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

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

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

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

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.

- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.

- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

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

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE LA RED DE VOZ, DATOS Y VIDEO E IMPLEMENTACIÓN DE UN PROTOTIPO DEL SISTEMA DISEÑADO PARA EL COLEGIO NACIONAL EXPERIMENTAL "JUAN PÍO MONTÚFAR"

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

ALEXIS RENÁN PASPUEL CALVOPIÑA
alexis.paspuel@est.epn.edu.ec

DIRECTOR: ING. RODRIGO FABIÁN CHANCUSIG CHUQUILLA
rodrigch@panchonet.net

Quito, Diciembre 2014

DECLARACIÓN

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

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

_____

Alexis Renán Paspuel Calvopiña

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por **Alexis Renán Paspuel Calvopiña** bajo mi supervisión.

_____

Ing. Rodrigo Chancusig

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A mi director de tesis, Ing. Rodrigo Chancusig por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia, fundamentales para la concreción de este trabajo.

Al personal administrativo del Colegio Juan Pío Montufar, en especial a la Rectora por su constante apoyo y ánimo para realizar este proyecto.

A mis amigos que de una u otra manera han facilitado en el desarrollo del trabajo, en especial a David Alvarez que de manera desinteresada me brindo su ayuda, espero retribuirle de alguna manera.

Y finalmente, los más importantes mis padres Patricia y Galo, mis hermanos que fueron los que día a día soportaron los malos días, disfrutaron los buenos momentos a mi lado y ahora comparten esta alegría conmigo.

DEDICATORIA

Este trabajo se lo dedico en primer lugar a mis padres que me dieron la vida y que han estado conmigo en todo momento. Gracias por todo a mi madre y a mi padre, por darme una carrera para mi futuro y por tener esa confianza en mí, aunque hemos pasado momentos difíciles siempre han estado a mi lado apoyándome.

A mis hermanos por estar conmigo desde la niñez siendo uno de los motivos para superarme y apoyarme siempre, los quiero mucho.

A mis tíos Luz y Javier quienes fueron parte fundamental para poder continuar mis estudios.

A mi hijo Ronand Xavi que es el motivo para salir adelante, para guiarle en su crecimiento y estar juntos en todo momento.

A una persona especial en mi vida, Susan eres el apoyo de cada día.

A toda mi familia que ha estado siempre conmigo dándome fuerzas, en especial a mis abuelitas.

ÍNDICE DE CONTENIDO

DECLARACIÓN i
CERTIFICACIÓN ii
AGRADECIMIENTO iii
DEDICATORIA iv
ÍNDICE DE CONTENIDO v
ÍNDICE DE FIGURAS xiv
ÍNDICE DE TABLAS xviii
ÍNDICE DE ANEXOS xxi
RESUMEN xxii
PRESENTACIÓN xxiii
CAPITULO I 1
1. FUNDAMENTOS TEÓRICOS 1
1.1. SISTEMAS DE CABLEADO ESTRUCTURADO 1
1.1.1. PAR TRENZADO 2
1.1.2. FIBRA ÓPTICA 5
1.2. ELEMENTOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO 7
1.2.1. EL SISTEMA DE CABLEADO HORIZONTAL 7
1.2.1.1. Consideraciones de diseño 8
1.2.1.2. Topología 9
1.2.1.3. Distancias 9
1.2.2. CABLEADO VERTICAL, TRONCAL O BACKBONE 9
1.2.3. CUARTO DE ENTRADA DE SERVICIOS 11
1.2.4. SISTEMA DE PUESTA A TIERRA 12
1.2.4.1. Atenuación 12
1.2.4.2. Capacitancia 12
1.2.4.3. Impedancia y distorsión por retardo 13
1.3. ESTÁNDARES AMERICANOS PARA CABLEADO ESTRUCTURADO 14
1.4. REDES DE INFORMACIÓN 16
1.5. MODELO DE REFERENCIA ISO/OSI 17
1.5.1. CAPA APLICACIÓN 17
1.5.2. CAPA PRESENTACIÓN 17

1.5.3. CAPA SESIÓN 17
1.5.4. CAPA TRANSPORTE 18
1.5.5. CAPA DE RED 18
1.5.6. CAPA ENLACE 18
1.5.7. CAPA FÍSICA 18
1.6. ARQUITECTURA TCP/IP 18
1.6.1. CAPA APLICACIÓN 19
1.6.2. CAPA TRANSPORTE 19
1.6.3. CAPA INTERNET 20
1.6.4. CAPA ACCESO A LA RED 21
1.7. REDES DE AREA LOCAL 21
1.7.1. TOPOLOGIAS DE RED 21
1.7.2. SISTEMAS LAN 23
1.7.3. EQUIPOS ACTIVOS EN REDES LAN 25
1.7.3.1. Conmutador o Switch 25
1.7.3.2. Redes VLAN 26
1.7.4. PROTOCOLOS USADOS EN LOS SWITCHES 27
1.7.4.1. Spaning Tree Protocol 27
1.7.4.1.1. Elección del puente raíz 29
1.7.4.1.2. Elección de los puertos raíz 29
1.7.4.1.3. Elección de los puertos designados 30
1.7.4.1.4. Elección de los puertos designados 30
1.7.4.1.5. Inter Switch Link 31
1.7.4.1.6. Conmutador Capa 3 31
1.7.4.1.7. Paquete por paquete 32
1.7.4.1.8. Cut-through 32
1.8. REDES DE ÁREA LOCAL INALÁMBRICAS 33
1.8.1. FUNCIONAMIENTO 33
1.8.2. CONFIGURACIONES DE RED PARA RADIOFRECUENCIA 34
1.8.3. ASIGNACIÓN DE CANALES 34
1.8.4. ESTÁNDARES 802.11 35
1.8.4.1. Rango y flujo de datos 38
1.8.4.2. 802.11a 38

1.8.4.3. 802.11b 39
1.8.4.4. 802.11g 40
1.8.5. SEGURIDAD EN REDES INALÁMBRICAS 40
1.8.6. EQUIPOS DE COMUNICACIÓN INALÁMBRICA 41
1.8.7. Router WiFi 41
1.8.8. Dispositivos de Distribución o Red [9] 41
1.8.9. Dispositivos Terminales [9] 42
1.8.9.1. SERVICIOS DE RED 42
1.8.9.2. Intranet 42
1.8.9.3. Beneficios de la Intranet de los centros docentes 42
1.8.9.4. Foros, wikis, blogs y redes sociales dentro de las Intranets 43
1.8.9.5. Voz sobre IP 43
1.8.10. ELEMENTOS 44
1.8.10.1. El Cliente 44
1.8.10.2. Los Servidores 44
1.8.10.3. Los Gateways 44
1.8.10.4. Funcionalidad 45
1.8.10.5. Móvil 45
1.8.10.6. Repercusión en el comercio 45
1.8.10.7. Estándar VoIP (H.323) 46
1.8.10.8. Características Principales 46
1.8.10.9. Estándar VoIP (SIP) 46
1.8.10.10. Arquitectura de red 46
1.8.10.11. Parámetros de la VoIP 47
1.8.10.12. Códecs 47
1.8.10.13. Retardo o latencia 48
1.8.10.14. Pérdida de tramas (Frames Lost) 48
1.8.10.15. Calidad del servicio 48
1.8.10.16. Ventajas 49
1.8.10.17. Desventajas 49
1.8.10.18. Perspectivas de futuro 49
CAPÍTULO II 51
2. ANÁLISIS DE LA INFRAESTRUCTURA DE RED ACTUAL 51

2.1. ANÁLISIS DE LA INFRAESTRUCTURA DE LA RED 51
2.1.1. INTRODUCCIÓN 51
2.1.2. IDENTIFICACIÓN, DESCRIPCIÓN Y DIAGNÓSTICO DEL PROBLEMA 51
2.1.3. INSTALACIONES 52
2.1.4. ANÁLISIS DE LA TOPOLOGÍA DE LA RED DE DATOS 54
2.1.5. EQUIPAMIENTO 55
2.1.5.1. Equipos para la comunicación de datos 56
2.1.5.2. Servidor 60
2.1.5.3. Estaciones de trabajo 60
2.1.5.4. Equipos de impresión 65
2.1.6. DIRECCIONAMIENTO IP 67
2.2. SISTEMA DE CABLEADO ESTRUCTURADO ACTUAL 68
2.2.1. ÁREA DE TRABAJO 69
2.2.2. CABLEADO HORIZONTAL 69
2.2.3. CABLEADO VERTICAL 72
2.2.4. CUARTO DE TELECOMUNICACIONES, SALA DE EQUIPOS Y ACOMETIDA 72
2.2.5. REQUERIMIENTOS DE PUESTA A TIERRA 73
2.2.6. CANALIZACIONES 73
2.2.7. RESUMEN DE LOS PUNTOS DE CABLEADO DE LA INSTITUCIÓN ... 74
2.3. USUARIOS DE LA RED 74
2.3.1. USUARIOS ADMINISTRATIVOS 75
2.3.2. ESTUDIANTES 75
2.3.3. PROFESORES 76
2.3.4. RESUMEN DE LOS USUARIOS POTENCIALES DE LA RED 77
2.4. ANÁLISIS DE TRÁFICO Y ANCHO DE BANDA GENERADO POR LAS APLICACIONES 77
2.4.1. ANÁLISIS DE LAS APLICACIONES INSTALADAS EN LOS EQUIPOS DE LA RED 77
2.4.2. ESTUDIO DE TRÁFICO UTILIZADO EN LA RED 79
2.4.3. Utilizando Wireshark 80
2.4.4. UTILIZANDO LA HERRAMIENTA COLASOFT CAPSA 82
2.4.5. UTILIZANDO LA HERRAMIENTA NTOP 85

2.4.5.1. Tráfico IP 85
2.4.6. UTILIZANDO LA HERRAMIENTA IPSCANNER 87
2.5.3. ANÁLISIS DE SEGURIDAD EN LA RED LAN Y WLAN 87
2.4.3. ANÁLISIS DEL ANCHO DE BANDA 88
2.5. ANÁLISIS DE SERVICIOS 89
2.5.1. SERVICIOS DE RED REQUERIDOS 89
2.5.1.1. Servicios web 89
2.5.1.2. Servicios de nombre de dominio (DNS) 90
2.5.1.3. Servicio de correo electrónico 90
2.5.1.4. Servicio de archivos compartidos 90
2.5.1.5. Servicio de impresión 91
2.5.1.6. Servicio de antivirus 91
2.6. RED DE VOZ ACTUAL 91
2.6.1. DETALLE DE USUARIOS ACTUALES 91
2.7. RESUMEN DEL DIÁGNOSTICO DE LA RED 94
CAPITULO III 97
3. REDISEÑO DE LA RED COLEGIO EXPERIMENTAL JUAN PÍO MONTÚFAR (CEJPM) 97
3.1. VISIÓN GENERAL 97
3.1.1. INFRAESTRUCTURA DE LA RED 98
3.2. SERVICIOS QUE DISPONDRÁ LA RED INTERNA LOCAL INTRANET CEJPM 99
3.2.1. SERVICIO DE VoIP (Telefonía IP). 99
3.2.2. SERVICIO DE INTERNET 99
3.2.3. SERVICIO DE E-MAIL (CORREO ELECTRONICO). 100
3.2.4. SERVICIO DE VIGILANCIA A TRAVES DE VIDEO CON TECNOLOGÍA IP. 100
3.2.5. SERVICIOS VARIOS 101
3.3. DIMENSIONAMIENTO DE TRÁFICO POR SERVICIO 101
3.3.1. Tráfico para Video Vigilancia IP 101
3.3.1.1. Procesos básicos y parámetros que se deben considerar para transmitir video sobre redes IP 102
3.3.1.2. Algoritmos de Compresión 103

3.3.1.3. Dimensionamiento del ancho de Banda 105
3.3.1.4. Dimensionamiento de Almacenamiento 107
3.3.2. TRÁFICO PARA TELEFONÍA IP 107
3.3.2.1. Protocolos de Encapsulamiento para enviar Voz sobre una red IP 109
3.3.2.2. Líneas troncales hacia la PSTN 112
3.3.3. TRÁFICO PARA CORREO ELECTRÓNICO 114
3.3.4. TRÁFICO GENERADO POR PÁGINAS WEB 115
3.3.5. TRÁFICO GENERADO POR ACCEDER A LA BASE DE DATOS 116
3.3.6. TRÁFICO GENERADO POR MENSAJERÍA INSTANTÁNEA 116
3.3.7. TRÁFICO GENERADO POR IMPRESIÓN 117
3.3.8. TRÁFICO GENERADO POR DESCARGAR ARCHIVOS DE INTERNET 118
3.3.9. TRÁFICO POR APLICACIÓN Y SERVICIO 118
3.3.10. CONEXIÓN A INTERNET 119
3.3.11. PROYECCIÓN DE TRÁFICO 120
3.4. TECNOLOGÍA DE RED Y MEDIO DE COMUNICACION 121
3.5. DISEÑO DE LA RED PASIVA 121
3.5.1. INTRODUCCIÓN 121
3.5.2. DISTRIBUCIÓN DE LOS PUNTOS DE CABLEADO PARA LAS ÁREAS 122
3.5.2.1. Edificio Administrativo 124
3.5.2.2. Departamental 126
3.5.2.3. Laboratorios 127
3.5.2.4. Bloque Primeros y Segundos Cursos 128
3.5.2.5. Bloque Terceros y Cuartos Cursos 128
3.5.2.6. Bloque Quintos y Sextos Cursos 129
3.5.3. REQUERIMIENTOS DE LA INSTITUCIÓN 130
3.5.3.1. Cableado Horizontal 130
3.6. Cálculo de la Longitud del Cable 131
3.6.1. Cableado Vertical. (Backbone) 143
3.6.1.1. Cuarto de Telecomunicaciones 145
3.6.1.2. Sala de Equipos 148
3.6.1.3. Área de Trabajo 149

3.6.1.4. Canalizaciones y enrutamiento 149
3.6.1.5. Etiquetado 150
3.6.2. PRUEBAS DE CERTIFICACIÓN [19] 153
3.7. DISEÑO DE LA RED ACTIVA 155
3.7.1. DISEÑO LÓGICO DE LA RED 155
3.7.2. DMZ 157
3.7.2.1. VLANs 158
3.7.2.2. Direccionamiento IP 159
3.7.3. DISEÑO DE LA RED PARA DATOS 161
3.7.3.1. Estaciones de trabajo 161
3.8. EQUIPOS DE CONECTIVIDAD 162
3.8.1. CARACTERÍSTICAS DE LOS SWITCHES DE ACCESO 163
3.8.2. CARACTERÍSTICAS DE LOS SWITCH DE DISTRIBUCIÓN. 164
3.8.3. DIMENSIONAMIENTO DE SERVIDORES 164
3.8.3.1. Primer Servidor 165
3.8.3.2. Segundo Servidor 165
3.8.3.3. Requerimiento mínimo del Sistema Operativo de los servidores 167
3.8.4. DISEÑO DE LA RED PARA VOZ SOBRE IP 167
3.8.4.1. Telefonía IP basada en software libre 168
3.8.4.2. Herramienta Trixbox CE 170
3.8.4.3. Requerimientos de hardware y Software para la implementación 171
3.8.4.4. Centrales Telefónicas Comerciales IP basadas en Asterisk 171
3.8.4.5. Elastix 171
3.8.4.6. SwitchVox 173
3.8.4.7. Trixbox Pro 174
3.8.4.8. Requerimiento que debe cumplir la central comercial IP 175
3.8.4.9. Comparación de las dos soluciones propuestas 176
3.8.4.10. Selección de la solución a utilizarse en la CEJPM 176
3.8.4.11. Principales razones de la elección de Elastix 177
3.8.5. ACCESORIOS PARA LA TELEFONÍA IP 177
3.8.6. DISEÑO DE LA RED INALÁMBRICA 178
3.8.7. TIPO DE APLICACIONES SOPORTADAS 179

3.8.8. MATERIAL DE CONSTRUCCIÓN DE LAS ZONAS DE COBERTURA DE LA RED INALÁMBRICA 179
3.9. CANTIDAD DE USUARIOS 180
3.10. SELECIÓN DE LA TECNOLOGÍA A UTILIZAR 182
3.10.1. CANTIDAD Y UBICACIÓN DE LOS EQUIPOS (AP) 182
3.10.2. DIAGRAMA DE LA RED WLAN 188
3.10.3. CARACTERÍSTICAS MÍNIMAS QUE DEBEN CUMPLIR LOS AP 189
3.10.4. DISEÑO DE LA RED PARA VIDEO VIGILANCIA 189
3.10.4.1. Ubicación Física de las Cámaras IP 190
3.10.4.2. Diagrama de la red para video vigilancia 194
3.11. UPS PARA EL CUARTO DE EQUIPOS Y CLOSET DE TELECOMUNICACIONES 195
3.11.1. CARACTERÍSTICAS MÍNIMAS DE LOS UPS 195
3.12. SEGURIDAD DE LA RED 196
3.12.1.1. Estaciones de Trabajo 197
3.12.1.2. Equipo Activo de la Red 197
3.12.1.3. Router Inalámbrico D-LINK 197
3.12.1.4. Central Telefónica 197
3.12.2. POLÍTICAS FÍSICAS Y LÓGICAS 198
3.12.2.1. Red LAN 198
3.12.2.2. Red WLAN 200
3.12.3. SEGURIDAD PERIMETRAL 201
3.13. ADMINISTRACIÓN Y MONITORIZACIÓN DE LA RED 203
3.13.1. AXENCE NETTOOLS PRO 204
3.13.2. WHATSUP GOLD 204
3.14. RECOMENDACIÓN PARA LA SELECCIÓN DEL ANTIVIRUS 206
3.15. EQUIPOS Y MATERIALES 206
CAPITULO IV 212
4. Implementación de un prototipo, pruebas y resultados 212
4.1. PROTOTIPO DE PRUEBA 212
4.1.1. IMPLEMENTACIÓN DE LOS SERVIDORES DHCP, DNS Y PROXY .. 212
4.1.1.1. Instalación y Configuración del Sistema Operativo Red Hat 5 212

4.1.1.2. Configuración del servidor DHCP (Dynamic Host Configuration Protocol) 214
4.1.1.3. Configuración del servidor DNS 215
4.1.1.4. Configuración del servidor Proxy (Squid) 219
3.17.2 IMPLEMENTACIÓN DE LA CENTRAL TELEFÓNICA IP TRIXBOX CE 222
4.1.1.5. VMware 222
4.1.1.6. Instalación de VMware en Red Hat 222
4.1.1.6.1. Crear y configurar la maquina virtual Trixbox 223
4.1.1.6.2. Requisitos mínimos de Hardware para la instalación 224
4.1.1.6.3. Pasos para la instalación 224
4.1.1.7. Configuración de extensiones 226
4.1.1.8. Configuración de una Troncal 227
4.1.1.9. Teléfono 3CXPhone 227
4.1.1.9.1. Características del Teléfono 3CXPhone 228
4.1.1.9.2. Instalación del Teléfono 3CXphone 229
4.1.1.9.3. Configuración del Teléfono 3CXphone 229
4.1.1.10. Pruebas de funcionamiento realizadas 230
4.1.1.10.1. Crear y configurar la máquina virtual correo Zimbra 231
4.1.1.10.2. Instalación de zimbra open source 232
4.1.1.10.3. Configuración de zimbra 232
4.1.1.10.4. Intalación de zimbra only server 233
CAPÍTULO V 239
5. CONCLUSIONES Y RECOMENDACIONES 239
5.1. CONCLUSIONES 239
5.2. RECOMENDACIONES 242
REFERENCIAS BIBLIOGRÁFICAS 244

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1.1 Comparación entre los diversos tipos de fibra óptica 7
Figura 1.2 Comparación entre TCP/IP y ISO/OSI 21
Figura 1.3 Topología ESTRELLA 22
Figura 1.4 Topología BUS 23
Figura 1.5 Topología ANILLO 23
Figura 1.6 Parámetros capa física IEEE 802.3 24
Figura 1.7 Opciones de tecnologías para IEE 802.3 25
Figura 1.8 Red VLAN con uso de Switches 27
Figura 1.9 Diagrama de red para VoIP 44

CAPÍTULO II

Figura 2.1 Topología de Red del Colegio Experimental “Juan Pío Montufar” 55
Figura 2.2 Configuración de las propiedades IPv4 para la conexión a Internet ... 68
Figura 2.3 Faceplate Biblioteca 69
Figura 2.4 Cableado horizontal 70
Figura 2.5 Tráfico capturado con Wireshark 80
Figura 2.6 Tráfico de la red – wireshark 81
Figura 2.7 Capacidad del Canal 82
Figura 2.8 Tráfico Total – Colasoft Capsa 83
Figura 2.9 Tráfico por tamaño de Paquete 83
Figura 2.10 Tráfico por Protocolo 84
Figura 2.11 Tráfico – Ntop 85
Figura 2.12 Hosts Escaneados 87

CAPÍTULO III

Figura 3.1 Modelo del sistema de video vigilancia 103
Figura 3.2 Utilización de AB de algunos algoritmos de compresión de video 105
Figura 3.3 Cabecera de los protocolos utilizados para enviar voz sobre redes IP 110
Figura 3.4 Erlang B 113
Figura 3.5 Crecimiento promedio de una página web 115

Figura 3.6 Estimación de Tráfico a 5 años. 121
Figura 3.7 Ejemplo de identificación de un punto de red..... 151
Figuras 3.8 Valores mínimos aceptables para realizar las pruebas en cable UTP CAT 6. 154
Figura 3.9 Topología de la Red De Comunicaciones. 156
Figura 3.10 Diagrama de la red de Telefonía IP del CEJPM..... 169
Figura 3.11 Paquetes que incluye Asterisk 172
Figura 3.13 Salón de Actos Primer Piso..... 184
Figura 3.14 Departamento Médico Planta Baja..... 184
Figura 3.15 Sala de Lectura de Profesores Primer Piso 185
Figura 3.16 Laboratorio de Química Planta Baja..... 185
Figura 3.17 Laboratorio de Física Primer Piso 186
Figura 3.18 Laboratorio de Computación Primeros y Segundos Cursos..... 186
Figura 3.19 Laboratorio de Computación Terceros y Cuartos Cursos 187
Figura 3.20 Laboratorio de idiomas..... 187
Figura 3.21 Laboratorio de Computación Quintos y Sextos Cursos..... 187
Figura 3.22 Diagrama de la red WLAN 188
Figura 3.23 Ubicación de las Cámaras IP Biblioteca y Colecturía..... 190
Figura 3.24 Ubicación de las Cámaras IP Salón de Actos y Corredor 191
Figura 3.25 Ubicación de las Cámaras Departamento Médico 191
Figura 3.26 Ubicación de las Cámaras IP Corredor 191
Figura 3.27 Ubicación de las Cámaras IP Laboratorios de Biología y Química . 192
Figura 3.28 Ubicación de las Cámaras IP Área Laboratorios de CC.NN y Física 192
Figura 3.29 Ubicación de la Cámara IP Bloque de Aulas Primeros y Segundos Cursos..... 192
Figura 3.30 Ubicación de la Cámara IP Laboratorio de Computación Terceros y Cuartos Cursos 193
Figura 3.31 Ubicación de la Cámara IP Laboratorio de Idiomas 193
Figura 3.32 Ubicación de la Cámara IP Laboratorio de Computación Quintos y Sextos Cursos. 193
Figura 3.33 Diagrama de la red de Video Vigilancia 194

CAPÍTULO IV

Figura 4.1 Prototipo de prueba 212
Figura 4.2 inicio de la instalación de Red Hat 213
Figura 4.3 Selección de los servidores (Continuación) 213
Figura 4.4 Selección de servicios específicos (continuación) 214
Figura 4.5 Configuración del servidor DHCP 215
Figura 4.6 Prueba realizada (Continuación) 215
Figura 4.7 configuración del archivo */etc/hosts* 216
Figura 4.8 Configuración del archivo localdomain.zone 216
Figura 4.9 Configuración del archivo localhost.zone 217
Figura 4.10 Configuración del archivo named.conf 217
Figura 4.11 Configuración del archivo named.10.93.2 218
Figura 4.12 Configuración del archivo named.juanpiomontufar.edu.ec 218
Figura 4.13 Pruebas de DNS con nslookup. 219
Figura 4.14 habilitación de los puertos 220
Figura 4.15 Creación de Listas de Control de Acceso. 220
Figura 4.16 Configuración de acceso para los puertos. 221
Figura 4.17 Configuración de sitios web no deseados. 221
Figura 4.18 Ventana de instalación de Trixbox 225
Figura 4.19 Ingreso al sistema (continuación) 226
Figura 4.20 Extensiones configuradas 227
Figura 4.21 Configuración de 3CXPhone 229
Figura 4.22 Prueba de Comunicación 230
Figura 4.23 Prueba de Estado del Sistema (Continuación) 230
Figura 4.24 Deshabilitar paquetes antes de la instalación de Zimbra 233
Figura 4.25 Elección de los paquetes a instalar 234
Figura 4.26 Cambio de dominio para el servidor. 235
Figura 4.27 Elección de la zona horaria 235
Figura 4.28 Opciones de configuración de Mailbox 236
Figura 4.29 Comprobación del servidor Zimbra 237
En la Figura 4.30 se indica la pantalla de Administración vía Web de Zimbra. .. 237
Figura 4.30 Pantalla de administración vía Web de Zimbra 237

Figura 4.31 Interfaz Web de Zimbra 238

ÍNDICE DE TABLAS

CAPÍTULO I

Tabla 1.1 Clasificación por Categoría de Cables UTP 5
Tabla 1.2: Protocolos de capa aplicación 20
Tabla 1.3: Capas estándar 802.11 35
Tabla 1.4: Clases de Estándar 802.11 38
Tabla 1.5: Tipos de estándar WiFi 38
Tabla 1.6: Velocidades de TX y Rangos de distancia estándar 802.11a 39
Tabla 1.7: Velocidades de TX y Rangos de distancia estándar 802.11b 39
Tabla 1.8: Velocidades de TX y Rangos de distancia estándar 802.11g 40

CAPÍTULO II

Tabla 2.1 Áreas de la Institución 53
Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución 59
Tabla 2.3 Características de los Equipos de la Institución 65
Tabla 2.4 Características de las impresoras de la Institución 66
Tabla 2.5 Direccionamiento IP actual 67
Tabla 2.6 Disponibilidad de puertos de los equipos activos 71
Tabla 2.7 Número de estudiantes totales del Colegio Nacional Experimental “Juan Pío Montufar” Fuente: Secretaría 76
Tabla 2.8 Número de usuarios potenciales de la red 77
Tabla 2.9 Aplicaciones instaladas en las estaciones de trabajo 79
Tabla 2.10 Tráfico capturado con Wireshark 81
Tabla 2.11 Protocolos más utilizados en la Red 84
Tabla 2.12 Tráfico IP – Ntop 86
Tabla 2.13 Teléfonos del Colegio Experimental “Juan Pío Montúfar” 94

CAPÍTULO III

Tabla 3.1 protocolos utilizados para transmitir video sobre redes IP 102
Tabla 3.2. Características de los principales algoritmos de compresión de video. 104
Tabla 3.3 Códec utilizados en VoIP [13] 109

Tabla 3.4 Cabecera de los protocolos utilizados para enviar vos sobre redes IP 111
Tabla 3.5 tráfico proyectado para 5 años 114
Tabla 3.6 Tamaño de hojas de Word 117
Tabla 3.7 Ancho de banda total requerido de la red interna..... 119
Tabla 3.8 Capacidad requerida para el enlace a Internet..... 119
Tabla 3.9 Proyección de tráfico 120
Tabla 3.10 Distribución de Áreas Colegio Experimental “Juan Pio Montufar” 124
Tabla 3.11 Distribución de puntos de red. Edificio Administrativo 125
Tabla 3.12 Distribución de puntos de red. Edificio Departamental 127
Tabla 3.13 Distribución de puntos de red. Edificio de Laboratorios..... 127
Tabla 3.14 Distribución de puntos de red. Edificio Bloque de Aulas Primeros y Segundos Cursos 128
Tabla 3.15 Distribución de puntos de red. Edificio Bloque de Aulas Terceros y Cuartos Cursos 129
Tabla 3.16 Distribución de puntos de red. Edificio Bloque de Aulas Quintos y Sextos Cursos 130
Tabla 3.17 Cálculo de las distancias promedio en cada una de las áreas 133
Tabla 3.18 Cálculo de las corridas de cable, número de puntos y rollos a ser utilizados por cada área. 135
Tabla 3.19 Accesorios necesarios para la instalación del Sistema de Cableado Estructurado 137
Tabla 3.21 Resumen de la red pasiva Edificio Departamental..... 139
Tabla 3.22 Resumen de la red pasiva Edificio Laboratorios 140
Tabla 3.23 Resumen de la red pasiva del Bloque Primeros y Segundos Cursos141
Tabla 3.24 Resumen de la red pasiva del Bloque Terceros y Cuartos Cursos .. 142
Tabla 3.25 Resumen de la red pasiva del Bloque Quintos y Sextos Cursos..... 142
Tabla 3.26 Medidas de Fibra öptica para Backbone 143
Tabla 3.27 Parámetros Giga Ethernet para ancho de banda fibra óptica..... 145
Tabla 3.28 Ubicación de Salas de Equipos en cada una de las Áreas 146
Tabla 3.29 Dimensionamiento del Closet de Telecomunicaciones 148
Tabla 3.30 Dimensionamiento para el rack del cuarto de equipos. 148
Tabla 3.31 Etiquetado del cableado para las diferentes Áreas. 151

Tabla 3.32 Identificación de los departamentos de la CEJPM. 152
Tabla 3.33 Asignación de direcciones IP 160
Tabla 3.34 Asignación de direcciones IP por VLAN Utilizadas y Libres 161
Tabla 3.35 Características de los Switch de Acceso 163
Tabla 3.36 Características de los Switches de Core 164
Tabla 3.37 Características de los servidores..... 167
Tabla 3.38 Versiones disponibles de Elastix y sus características técnicas [22] 173
Tabla 3.39 Versiones disponibles de SwitchVox y sus características técnicas [23] 174
Tabla 3.40 Comparación de las centrales IP comerciales basadas en Asterisk 176
Tabla 3.41 Materiales que causan Interferencia..... 180
Tabla 3.42 Estándares IEEE 802.11 182
Tabla 3.43 Características mínimas de los Access Poits 189
Tabla 3.44 Elementos para el Cableado Estructurado 208
En la Tabla 3.45 se indica aquipos activos de la red..... 209
Tabla 3.45 Elementos activos de la red 211

CAPÍTULO IV

Tabla 4.1 DIAL PLAN 225

ÍNDICE DE ANEXOS

ANEXO A 248
ANEXO B 253
ANEXO C 259
ANEXO D 265
ANEXO E 266
ANEXO F..... 319
ANEXO G 320
ANEXO H 323

RESUMEN

En el primer capítulo se describen fundamentos teóricos de redes de comunicaciones, tecnología, áreas de cobertura y arquitectura que actualmente se emplean. Además se estudia el protocolo IP, la diferencia entre los protocolos SIP y H.323 como parte importante de la transmisión de voz en una central telefónica IP; aspectos que constituyen la base para el desarrollo del presente trabajo.

En el capítulo dos se estudia la situación actual de la red de comunicaciones del Colegio Experimental Juan Pío Montufar CEJPM, donde se verifica el cumplimiento de normas y estándares para la red pasiva; se realiza un análisis del tráfico de voz para determinar la cantidad de troncales telefónicas necesarias y también se realiza un análisis del tráfico de datos para determinar la capacidad del enlace de Internet. Se genera un diagnóstico de la red de comunicaciones.

En el tercer capítulo se realiza el rediseño de la red de comunicaciones, recomendando la utilización de equipos de red activos, administrables y que soporten protocolos que proporcionen calidad de servicio. Además, se analizan soluciones de telefonía open source y propietarias para el CEJPM. Se propone un modelo de red de comunicación convergente, donde se toma en cuenta la seguridad interna de la misma, de ahí la recomendación para la adquisición de un firewall.

En el cuarto capítulo se realiza un prototipo de la red, tomando en cuenta el servicio de voz y datos. Se dimensiona la central telefónica IP y se configura utilizando el software Elastix como alternativa de solución. Se implementan servicios de datos para realizar pruebas de ambos servicios voz y datos en la red convergente. Se realizara un presupuesto referencial del costo de los equipos activos de la red utilizados en el rediseño.

En el quinto capítulo se presentan las conclusiones y recomendaciones que se pueden proponer como resultado de este proyecto.

PRESENTACIÓN

EL Colegio Experimental Juan Pío Montufar CEJPM es una institución pública que permite formar bachilleres con un elevado sustento científico y que logren éxito en sus estudios superiores, fundamentados en la práctica cotidiana de sus valores humanos y en la adecuada interpretación de la realidad social, capaces de vivir en la armonía con la naturaleza y de contribuir al desarrollo sostenido del país.

Las estudiantes recurren a este establecimiento para poder continuar con sus estudios de bachillerato.

El objetivo del presente trabajo fue realizar un rediseño de toda la red de comunicaciones, donde se contemplan los elementos de cableado estructurado, se propone instalar los equipos de conectividad necesarios para mejorar y soportar el servicio de telefonía IP con calidad de servicio.

Con la finalidad de demostrar el trabajo realizado y por limitaciones de carácter financiero se logró implementar el prototipo de una central telefónica IP utilizando software libre, para comprobar todas las bondades del uso de este sistema de acuerdo con los resultados logrados se puede recomendar que a futuro se implemente una solución completa bajo esta plataforma.

Para brindar una solución de telefonía IP acorde a las necesidades del Colegio Experimental Juan Pío Montufar CEJPM se analizan alternativas libres y propietarias, comparando sus características, ventajas y precios, a fin de poder proponer la solución más apropiada.

CAPÍTULO I

1. FUNDAMENTOS TEÓRICOS

1.1. SISTEMAS DE CABLEADO ESTRUCTURADO

El cableado estructurado existencialmente es una red de cable única y compleja, con variaciones de alambre de cobre (pares trenzados sin blindar UTP[1]), cables de fibra óptica, bloques de conexión, y varios tipos de cables con diferentes terminaciones, conexiones y adaptadores [1]. Una de las ventajas del cableado estructurado es que permite la posibilidad de una administración simple y sistemática, permitiendo la localización de las personas y equipos en diferentes localizaciones.

Los sistemas de cableado para las telecomunicaciones y en especial para los edificios, es óptima para lograr brindar una gran variedad de servicios, sin necesidad de realizar grandes modificaciones, y en base a este concepto es posible el diseño de un cableado estructurado, con herramientas simples y sin requerimientos especiales, para su correcto funcionamiento. Los estándares son los principales garantizadores de que los sistemas se manejen de forma ordenada y a su vez soporten las necesidades en telecomunicaciones actuales y futuras, generalmente establecidas en un tiempo estimado de diez años [1].

El tendido exige una organización sistemática para cubrir las diversas áreas de un edificio en sus diferentes plantas y servicios. Es por eso que se debe tener en cuentas todos los factores limitantes del diseño y los impedimentos tecnológicos al momento de implantar una red de área local [1] para esto se deben tomar en cuenta los siguientes factores:

- Segmentación esquematizada del tráfico de la red.
- Establecimiento de la longitud máxima de los distintos segmentos de la red.

[1] **UTP,** Unshielded Twisted Pair

- Análisis de las interferencias electromagnéticas.
- Establecimiento de las necesidades de redes locales virtuales.

En cuestión de los medios de trasmisión más conocidos se conocen dos tipos de cables para los sistemas; la fibra óptica, y el par trenzado, y estos a su vez se subdividen en tres tipos [1]:

- Cables de par trenzado sin blindar (UTP) de 100 ohm y cuatro pares.
- Cables de par trenzado blindados (STP) de 150 ohm y cuatro pares.
- Cables de fibra óptica multimodo de 62.5/125 um y dos fibras.

1.1.1. PAR TRENZADO

El par trenzado es un tipo de conexión generalmente usado en telecomunicaciones, que está fundamentado en que dos conductores eléctricos que se encuentran aislados, son entrelazados con el objetivo de abolir las interferencias de fuentes externas y diafonía de los cables cercanos, este fue inventado por Alexander Graham Bell [2].

Existen los siguientes tipos de pares trenzados:

- Unshielded twisted pair UTP o par trenzado sin blindaje: Este tipo de cables trenzados se utilizan principalmente para tecnologías de redes locales. Son generalmente de bajo costo y de fácil manejo, sin embargo causan errores más frecuentes que otros tipos de redes locales, además de limitaciones físicas para las grandes distancias.
- Shielded twisted pair STP[2] o par trenzado blindado: Son cables de cobre aislados en una cubierta protectora y mantienen un número específico de trenzas por pie. STP hace referencia a la cantidad de aislamiento que se tienen alrededor de un conjunto de cables y por ello su resistencia al ruido. Estos comúnmente se los puede encontrar en redes como Ethernet o

[2] STP Shielded Twisted Pair

Token Ring, sin embargo este método es más caro que el anteriormente mencionado.

- Foiled twisted pair FTP[3] o par trenzado con blindaje global: Estos son cables que tienen una pantalla conductora global de manera trenzada. Tienen una mejor relación frente a interferencias y tienen una impedencia de 12 ohmios.

En la tabla 1.1 se indica la especificación 568A según el Commercial Building Wiring Standard de la Asociación Industrias Electrónicas e Industrias de las Telecomunicaciones (EIA/TIA) [2].

Categoría	**Ancho de banda (MHz)**	**Aplicaciones**	**Notas**
Categoría 1	0,4 MHz	Líneas telefónicas y módem de banda ancha.	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
Categoría 2	4 MHz	Cable para conexión de antiguos terminales como el IBM 3270.	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
Categoría	**Ancho de banda (MHz)**	**Aplicaciones**	**Notas**
Categoría 3	16 MHz	10BASE-T and 100BASE-T4 Ethernet	Descrito en la norma EIA/TIA-568. No es

[3] FTP Foiled Twisted Pair

			adecuado para transmisión de datos mayor a 16 Mbit/s.
Categoría 4	20 MHz	16 Mbit/s Token Ring	
Categoría 5	100 MHz	100BASE-TX y 1000BASE-T Ethernet	
Categoría 5e	100 MHz	100BASE-TX y 1000BASE-T Ethernet	Mejora del cable de Categoría 5. En la práctica es como la categoría anterior pero con mejores normas de prueba. Es adecuado para Gigabit Ethernet
Categoría 6	250 MHz	1000BASE-T Ethernet	Cable más comúnmente instalado en Finlandia según la norma SFS-EN 50173-1.
Categoría	**Ancho de banda (MHz)**	**Aplicaciones**	**Notas**
Categoría 6e	250 MHz (500MHz según otras fuentes)	10GBASE-T Ethernet (en desarrollo)	No es estandarizado. Lleva el sello del fabricante.
Categoría 7	600 MHz	En desarrollo. Aún sin aplicaciones.	Cable U/FTP (sin blindaje) de 4

			pares.
Categoría 7a	1200 MHz	Para servicios de telefonía, Televisión por cable y Ethernet 1000BASE-T en el mismo cable.	Cable S/FTP (pares blindados, cable blindado trenzado) de 4 pares. Norma en desarrollo.
Categoría 8	1200 MHz	Norma en desarrollo. Aún sin aplicaciones.	Cable S/FTP (pares blindados, cable blindado trenzado) de 4 pares.

Tabla 1.1 Clasificación por Categoría de Cables UTP

1.1.2. FIBRA ÓPTICA

Este medio de transmisión es usualmente utilizado en redes de datos; y consta de un hilo muy fino transparente, que es de vidrio o diferentes tipos de materiales plásticos, lo cual permite que se envíen impulsos de luz para la rápida transmisión de datos, esto permite una alta flexibilidad y un ángulo de reflexión total en base a la ley de Snell la luz puede formar parte de un láser o un led [3]. La fibra óptica es el medio de transmisión por excelencia, principalmente debido a que no se ve afectado por las interferencias electromagnéticas, además es posible su utilización para las redes locales, u otros similares donde se requiera la reducción de interferencias.

Las diversas trayectorias que puede tener un haz de luz en el interior de una fibra óptica se denominan como modos de propagación. Además esto se subdivide en el modo de propagación, en el cual existen dos: multimodo y monomodo.

Las fibras multimodos son aquellas en los que el haz de luz puede circular por más de un camino, haciendo que este no llegue de completo a la vez, es por ello

que una fibra multimodo puede tener más de mil de modos de propagación de luz. Estas fibras se usan comúnmente en la aplicación a corta distancia, en distancias que no superan el 1 km, haciendo de estas un método fácil y económico de diseño [3].

En base del tipo de refracción del núcleo, se han creado dos tipos de fibra multimodo [3]:

- Índice escalonado: Se caracteriza por un índice de refracción constante en la sección cilíndrica y posee una alta dispersión modal.
- Índice gradual: Se caracteriza por no ser constante y poseer una menor dispersión modal, además de que su núcleo está constituido por diferentes materiales.

Es importante tener en cuenta que según el sistema ISO[4] 11801 para la clasificación de fibras multimodo, según su ancho se establece el formato OM3, sobre multimo de láser, a los modos ya existentes OM1 y OM2 sobre el multimodo de LED [3].

- OM1: Fibra 62.5/125 µm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores
- OM2: Fibra 50/125 µm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores
- OM3: Fibra 50/125 µm, soporta hasta 10 Gigabit Ethernet (300 m), usan láser (VCSEL) como emisores.

[4] ISO: Insternational Organization for Standarization Organismo encargado de promover el desarrollo de normas internacionales de fabricación

En la figura 1.1 se indica la comparación entre los diversos tipos de fibra òptica:

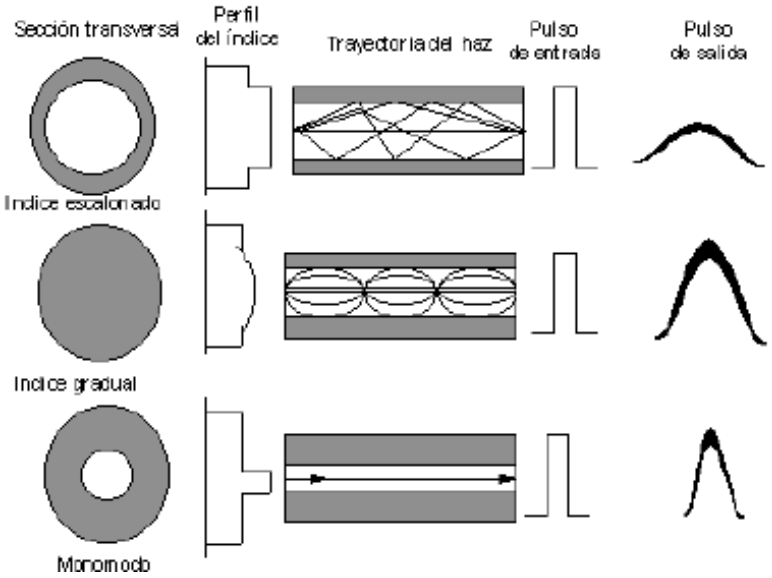


Figura 1.1 Comparación entre los diversos tipos de fibra óptica

1.2. ELEMENTOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO

Según la norma EIA/TIA[5] 568A se define al cableado horizontal de la siguiente manera.

1.2.1. EL SISTEMA DE CABLEADO HORIZONTAL

Es la parte del sistema cableado que se extiende desde el cuarto de telecomunicaciones hacia el área de trabajo o viceversa. Este consiste de dos elementos básicos [4]:

- Cable Horizontal y Hardware[6] de Conexión el que es también llamado cableado horizontal se encarga de otorgar los recursos básicos para transportar las diversas señales de telecomunicaciones entre en el área de

[5] EIA/TIA: Electronic Industries Alliance/Telecommunications Industry Association, estándares que tratan el cableado comercial para productos y servicios
[6] Hardware: se refiere a todas las partes tangibles de un sistema informático

trabajo y el cuarto de las telecomunicaciones. Sus componentes son los contenidos de las rutas y sus diversos espacios horizontales.

- Rutas y Espacios Horizontales son llamados también áreas de distribución horizontal, constan de las rutas y espacios que se utilizan para distribuir, y esquematizar de manera horizontal el hardware, entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estos espacios y rutas trazadas son los principales contenedores del cableado horizontal. Para estos espacios se recomienda:

    - En caso de existir cielo raso suspendido es recomendable la utilización de canaletas para la transportación de los cables horizontales.
    - Una tubería de ¾ in. por cada dos cables UTP.
    - Una tubería de 1 in. por cada cable de dos fibras ópticas.
    - Los radios mínimos de curvatura deben ser bien implementados.

El cableado horizontal debe incluir [4]:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo (WAO)[7].
- Los cables y conectores entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empalme (patch panels) y cables de empalme.

Adicional a todo esto se debe tener en cuenta ciertas consideraciones al momento de seleccionar el cableado horizontal.

1.2.1.1. Consideraciones de diseño

El costo del material es un factor fundamental, así como la mano de obra, retrasos, todo esto es necesario tener en cuenta para evitar los posibles cambios en los costos, y la suspensión de la obra por falta de presupuesto, es por ello que

[7] **WAO: Work Area Outlets** Cajas, placas y conectores de telecomunicaciones en el área de trabajo

se recomienda manejar una gama amplia de aplicaciones para el usuario. Además de mantener un diseño el cual facilite el mantenimiento, ampliación y modificación de las áreas de trabajo. También se deben considerar la incorporación de otros sistemas de información para la edificación, por tener algunos ejemplos, la televisión por cable, sistemas de control ambiental, sistemas de seguridad entre otros.

1.2.1.2. Topología

La norma EIA/TIA 568A hare referencia a una serie de recomendaciones acerca del cableado horizontal, entre las principales esta que el cableado debe tener una topología de estrella, lo que quiere decir que cada toma/conector de telecomunicaciones del área de trabajo debe tener una conexión en el cuarto de telecomunicaciones [4].

1.2.1.3. Distancias

Sin tomar en cuenta el medio usado, la distancia horizontal no de exceder los 90m. Medido desde la terminación mecánica del medio en la conexión horizontal desde el cuarto de telecomunicaciones hasta el área de trabajo. Tomando en cuenta que se recomienda la distancia que separa a los cables tanto desde el cuarto de telecomunicaciones como el área de trabajo con un distancia máxima de 10m, haciendo uso de cordones de parcheo, jumpers, y cables de equipo.

1.2.2. CABLEADO VERTICAL, TRONCAL O BACKBONE

El objetivo del cableado backbone[8] es el de otorgar interconexiones entre las diferentes áreas de servicio del edificio, entre cuartos de equipos y los cuartos de telecomunicaciones y cuartos de entrada de servicios. En el cableado del backbone se toma en cuenta las conexiones verticales entre los diferentes pisos del edificio, incluyendo los medios de transmisión, los puntos principales de conexión cruzada y las respectivas terminaciones mecánicas. El cableado vertical

[8] **Backbone**, se refiere al cableado troncal o subsistema vertical en una instalación de red de área local.

es el responsable de la interconexión de los distintos gabinetes de telecomunicaciones, y llevan la señal a la sala de equipamiento. En este medio del sistema de cableado, el costo es más alto por lo que en muchas ocasiones se recomienda el uso de instalaciones independientes de telefonía y datos. Además de que se ve reforzado por el hecho de que en caso de ser necesaria una sustitución del backbone su costo es relativamente bajo, reduciendo las incomodidades que este pudiera causar a los habitantes del edificio. El backbone telefónico se lo hace habitualmente con un cable telefónico de tipo multipar. Para determinar el backbone de datos es fundamental tener en cuenta cuál será la disposición física del equipamiento. Generalmente el backbone se realiza mediante un tendido en forma de estrella, lo que quiere decir que se interconectan todos con un gabinete central, donde se encuentra el equipamiento más complejo [4].

Para el backbone de datos se puede hacer uso de cables de tipo UTP, o a su vez con fibra óptica, estos tendrán un número definido de cables desde un gabinete a otro en una distribución tipo estrella.

En la actualidad la diferencia del costo que causa la utilización de sistemas de fibra óptica se compensa gracias a su mayor flexibilidad y a la posibilidad de crecimiento que permite este tipo de tecnología. Sin embargo para una configuración de tipo Ethernet mínima basta la utilización de cable de 2 fibras, es mejor usar un cable con una mayor cantidad, el cual puede ir de 6 a 12, lo que resulta más conveniente debido a que la diferencia en costos no es relevante y permite disponer de una más amplia reserva de conductores para evitar fallos, además de la proyección a futuro a las nuevas tecnologías así como sistemas FDDI[9] y sistemas resistentes a fallas

La norma EIA/TIA 568 prevé la ubicación de la transmisión de cableado vertical a horizontal, y la ubicación de los dispositivos necesarios, en habitaciones independientes con puerta destinada a tal fin, ubicadas por lo menos una por piso,

[9] **FDDI,** (Fiber Distributed Data Interface) es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica.

denominadas armarios de telecomunicaciones. Se utilizan gabinetes estándar de 19 pulgadas de ancho, con puertas, de aproximadamente 50 cm de profundidad y de una altura entre 1.5 y 2 metros. En dichos gabinetes se dispone generalmente de las siguientes secciones [4]:

- Acometida de los puestos de trabajo: 2 cables UTP llegan desde cada puesto de trabajo.
- Acometida del backbone telefónico: cable multipar que puede determinar en regletas de conexión o en patch panels.
- Acometida del backbone de datos: cables de fibra óptica que se llevan a una bandeja de conexión.
- Electrónica de la red de datos: Hubs, Switches, Bridges y otros dispositivos necesarios.
- Alimentación eléctrica para dichos dispositivos.
- Iluminación interna para facilitar la realización de trabajos en el gabinete.
- Ventilación a fin de mantener la temperatura interna dentro de límites aceptables [4].

1.2.3. CUARTO DE ENTRADA DE SERVICIOS

Este consiste de diferentes cables así como accesorios para la conexión y protección de los distintos dispositivos, además de las herramientas necesarias para la conexión entre la edificación a los servicios externos. Puede contener el punto de demarcación[10]. Adicionalmente brindan la protección eléctrica establecida por los códigos eléctricos aplicables. El diseño debe ser según la norma TIA/EIA-569-A. Los requerimientos de instalación son los siguientes [5]:

- Precauciones para el manejo de cables.
- Evitar las tensiones en el cable.
- Los cables deben evitar enrutarse en grupos muy apretados.

[10] Punto de Demarcación, es el punto en el que la red telefónica pública conmutada termina y se conecta con el cableado dentro de las instalaciones del cliente.

- Utilización de rutas de cable y accesorios adecuados (100 ohm UTP y ScTP.)
- Evitar giros con un ángulo mayor a 90 grados.

1.2.4. SISTEMA DE PUESTA A TIERRA

Los sistemas de puesta a tierra y de puenteo que están establecidos en el estándar ANSI/TIA/EIA-607 forman parte de un componente esencial de todo tipo de sistema de cableado estructurado moderno. Para esto el gabinete debe poseer una toma con acceso a tierra, y esta debe ser conectada a la tierra general de la edificación. Hay que tomar en cuenta que este cableado de tierra no siempre está estipulado en los planos del edificio, generalmente los cables de tierra son puestos a tierra en el subsuelo [1].

1.2.4.1. Atenuación

Las distintas señales de transmisión en largas distancias se encuentran sujetas a distorsión que es la pérdida de fuerza o amplitud de la señal. La atenuación es la razón principal de que el largo de las redes tenga varias restricciones. Si la señal se hace muy débil, el equipo receptor no interceptará bien o no reconocerá esta información. Esto causa errores, bajo desempeño al tener que retransmitir la señal [1]. Es por ello que la utilización de repetidores o amplificadores es esencial para extender las distancias de la red. Esta atenuación de la señal se mide mediante aparatos que inyectan una señal de prueba en un extremo del cable y la miden en el otro extremo.

1.2.4.2. Capacitancia

La capacitancia es uno de los causantes de la distinción de señal en el cable, regido específicamente por la relación entre mayor distancia de cable y menor espesor del aislante, mayor es la capacitancia, llegando así a causar más distorsión. La capacitancia en general es la unidad de medida de la energía que se encuentra almacenada dentro de un cable. Con la ayuda de los medidores de

cable se puede determinar si este ha sido roscado o estirado. La capacitancia del cable par trenzado en las redes está entre 17 y 20 pF[11] [1].

1.2.4.3. Impedancia y distorsión por retardo

Las distintas líneas de transmisión siempre tendrán en alguna porción ruido de fondo, principalmente generado por las diferentes fuentes externas o por la transmisión de las líneas adyacentes, mezclándose así con la señal transmitida. La distorsión que esta resultante puede ser menor, pero la atenuación provoca que la señal digital decaiga al mismo nivel de la señal de ruido. Aunque el nivel de la señal digital sea mayor al de la de ruido, este a medida que se acerca al receptor puede irse igualando. Una señal conformada por distintas frecuencias es propensa a tener una distorsión por el retardo que es causada por la impedancia, definida como la resistencia al cambio de las distintas frecuencias. Provocando que los diferentes componentes que estén en esa frecuencia contengan señales que lleguen a destiempo al receptor. Mediante el incremento de la frecuencia los efectos de interferencia aumentan, y los receptores empiezan a quedar imposibilitados para interpretar las señales de manera correcta. La forma más sencilla de disminuir estas interferencias es mediante la reducción del tamaño del cable. Teniendo en cuenta que la medición de la impedancia nos ayuda para encontrar las rutas o la falta de conexión. El cable tiene que poseer una impedancia de 100 ohm, en la frecuencia para la transmisión de datos.

Es fundamental mantener un nivel de señal mayo al nivel de ruido. Y la mayor fuente de distorsión de señal por parte de un cable trenzado es la interferencia. Dada esencialmente por la ruptura de los cables adyacentes siendo así un problema atípico del cableado, otro factor para tomar en cuenta es el ruido causado por las lámparas fluorescentes, microondas y distintos equipos de oficina.

[11] pF: Picofaradio, Unidad del Sistema Internacional de Unidades

Para la medición de la interferencia se envía una señal de un valor conocido por un extremo del cable y se la mide en los cables cercanos a fin de encontrar su nivel de ruido [1].

1.3. ESTÁNDARES AMERICANOS PARA CABLEADO ESTRUCTURADO

Entre los principales tenemos los siguientes:

- “TIA-526-7 “Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant “– OFSTP-7 - (February 2002)
- TIA-526-14-A Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant – OFSTP-14 - (August 1998)
- ANSI/TIA/EIA-568-B.1 de Alambrado de Telecomunicaciones para Edificios Comerciales, Parte 1: Requerimientos Generales, mayo de 2001.
- Adenda ANSI/TIA/EIA-568-B.1-1-2001, Adenda 1, Radio de Curvatura Mínimo para Cables de 4 Pares UTP y STP, julio de 2001.
- TIA/EIA-568-B.1-2 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 2 – Grounding and Bonding Requirements for Screened Balanced Twisted-Pair Horizontal Cabling - (February 2003)
- TIA/EIA-568-B.1-3 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 3 – Supportable Distances and Channel Attenuation for Optical Fiber Applications by Fiber Type - (February 2003)
- TIA/EIA-568-B.1-4 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 4 – Recognition of Category 6 and 850 nm Laser Optimized 50/125 μm Multimode Optical Fiber Cabling - (February 2003)
- TIA/EIA-568-B.1-5 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 5 –

Telecommunications Cabling for Telecommunications Enclosures – (March 2004).

- TIA/EIA-568-B.1-7 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 7 - Guidelines for Maintaining Polarity Using Array Connectors – (January 2006)
- TIA/EIA-568-B.2 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components - (December 2003)
- TIA/EIA-568-B.2-1 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 1 – Transmission Performance Specifications for 4-Pair 100 ohm Category 6 Cabling - (June 2002)
- TIA/EIA-568-B.2-2 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 2 – Revision of Sub-clauses - (December 2001)
- TIA/EIA-568-B.2-3 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 3 – Additional Considerations for Insertion Loss & Return Loss Pass/Fail Determination - (March 2002)
- TIA/EIA-568-B.2-4 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 4 – Solderless Connection Reliability Requirements for Copper Connecting Hardware - (June 2002)
- TIA/EIA-568-B.2-5 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 5 – Corrections to TIA/EIA-568-B.2 – (January 2003)
- TIA/EIA-568-B.2-6 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 6 – Category 6 Related Component Test Procedures – (December 2003)
- TIA/EIA-568-B.2-11 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 11 - Specification of 4-Pair UTP and SCTP Cabling – (December 2005)
- TIA/EIA-568-3 Optical Fiber Cabling Components Standard - (April 2002)

- TIA/EIA-568-3.1 Optical Fiber Cabling Components Standard – Addendum 1 – Additional Transmission Performance Specifications for 50/125 µm Optical Fiber Cables – (April 2002)
- TIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces - (October 2004)
- TIA-598-C Optical Fiber Cable Color Coding - (January 2005)
- TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure - (May 2002)
- J-STD-607-A Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications - (October 2002)
- TIA-758-A Customer-owned Outside Plant Telecommunications Infrastructure Standard – August 2004" [5]

1.4. REDES DE INFORMACIÓN

Se entiende a una red como un conjunto de dispositivos que se encuentran interconectados para el intercambio de comunicaciones a través de subredes de comunicaciones. Para facilitar el diseño de una manera más simple se opta por dividir en capas, las cuales están distribuidas en funciones independientes y de intercumunicarse entre si mediante protocolos. Y a este conjunto de capas y protocolos se lo llama arquitectura.

En base a la definición han existido dos tipos de arquitecturas que definen los estándares en comunicación. Los cuales se entienden como los protocolos TCP/IP[12] y los modelos de referencia ISO/OSI[13]. Teniendo en cuenta que TCP/IP es el tipo de arquitectura más utilizada mientras que el modelo OSI es más usado para las comunicaciones [5].

[12] **TCP/IP,** Transmission Control Protocol / Internet Protocol es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.
[13] **OSI,** Open SystemInterconnection 'interconexión de sistemas abiertos'

1.5. MODELO DE REFERENCIA ISO/OSI

Este modelo de referencia está desarrollado para los estándares de comunicación entre computadoras. Se conforma por siete capas principales las cuales son:

- Aplicación.
- Presentación.
- Sesión.
- Transporte
- Red
- Enlace.
- Física [5].

1.5.1. CAPA APLICACIÓN

Es la capa que se encuentra relacionada de manera directa al usuario y se encarga de brindar todos los servicios necesarios para el acceso de una red de información con una interfaz final.

1.5.2. CAPA PRESENTACIÓN

Es la encarga de proporcionar la independencia esencial para las aplicaciones respecto a la presentación y al formato de datos transmitidos, de manera que estos sean legibles en la capa aplicación, y a su vez estos puedan ser retransmitidos a través de la red.

1.5.3. CAPA SESIÓN

Es la que establece, gestiona y se encarga del cierre de las conexiones entre las aplicaciones que conforman la comunicación, también conocidas como sesiones.

1.5.4. CAPA TRANSPORTE

Otorga servicios con confiablidad y de manera transparente para los datos, entre los distintos extremo de la comunicación. Además se encarga de proveer los mecanismos de control de errores, que se encargan de verificar la información enviada y control del flujo entre el origen y destino.

1.5.5. CAPA DE RED

Otorga independencia a las capas con respecto a enrutamiento, conmutación e interconexión de las redes heterogéneas, también controla los proceso propios de la subred de comunicaciones. La unidad que maneja TX es el paquete.

1.5.6. CAPA ENLACE

Mantiene un nivel superior libre de errores, para la retransmisión de datos, ofreciendo un control de flujo y de errores a la capa de red. También soluciona problemas de pérdida, daños, direccionamiento, y secuenciamiento de tramas. La unidad representativa de TX es la trama.

1.5.7. CAPA FÍSICA

Mantiene la transición y recepción de los datos por medio de un canal de comunicación, y otorga características eléctricas, mecánicas y físicas, para la habilitación y mantenimiento de los enlaces físicos. La unidad usada para las TX es el bit.

1.6. ARQUITECTURA TCP/IP

Forma parte del conjunto de protocolos estándares a nivel de Internet sin que necesariamente existan modelos oficiales ISO/OSI, generalmente el número de capas definido es el 4 [5].

1.6.1. CAPA APLICACIÓN

Es la que se encuentra directamente relacionada con el usuario, utilizando protocolos de nivel alto con un respectivo número asignado de RFC[14].

1.6.2. CAPA TRANSPORTE

Se usan dos protocolos para la intercomunicación de un extremo a extremo, TCP (Transfer control Protocol) y UDP[15] (User Datagram Protocol).

TCP es uno de los protocolos de transmisión más confiable y está orientado a conexión. Otorga servicios de control de errores y su retransmisión.

UDP es un protocolo no confiable y no orientado a conexión, es usado en aplicaciones en las cuales la entrega debe ser más rápida.

En la tabla 1.2 se citan algunos protocolos de aplicación:

[14] **RFC,** Request for Comments son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc.
[15] **UDP,** User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI).

PROTOCOLO	FUNCIÓN	RFC	UDP/TCP
TELNET (TELetype NETwork)	Permite el acceso remoto a un equipo a través de la red.	*854*	*TCP*
SMTP (Simple Mail Transfer Protocol)	Permite el intercambio de correo electrónico basado en texto	*2821*	*TCP*
FTP (File Transfer Protocol)	Permite la transferencia de archivos basado en una arquitectura cliente - servidor	*2428*	*TCP*
TFTP (Trivial file transfer Protocol)	Es una versión reducida de *FTP*, permite el intercambio de archivos relativamente pequeños, por lo general asociado a la administración de dispositivos de red.	*1350*	*UDP*
DNS (Domain Name System)	Es un sistema de nomenclatura jerárquica de computadoras, que permite traducir nombres de dominio a direcciones IP.	*1034*	*TCP/UDP*
HTTP (HyperText Transfer Protocol)	Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, *proxies*) para comunicarse.	*1945*	*TCP*
DHCP (Dynamic Host Configuration Protocol)	Permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente	*2131*	*UDP*

Tabla 1.2: Protocolos de capa aplicación

1.6.3. CAPA INTERNET

El protocolo IP (Internet Protocol), es no confiable sin embargo se encarga del enrutamiento de los mensajes en la red, de la segmentación y el transporte de los datagramas, sin embargo deja el control de errores y de flujo en las capas superiores.

En estas capas se usan protocolos como el ICMP[16] el cual provee de mensajes de control para las capas superiores.

Otros protocolos usados son los ARP Address Resolution Protocol, y RARP Address Resolution Protocol. Es importante aclarar que estos protocolos sirven

[16] **ICMP,** Internet Control Message Protocol es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

para la determinación de direcciones IP por medio de las direcciones físicas y viceversa.

1.6.4. CAPA ACCESO A LA RED

Seguridad de transmisión de los paquetes IP a través de la red. En la figura 1.2 se indica la diferencia entre el modelo ISO/OSI y arquitectura TCP/IP:

Figura 1.2 Comparación entre TCP/IP y ISO/OSI

1.7. REDES DE AREA LOCAL

Se entiende como red LAN Local Area Network al conjunto de software y hardware que se encuentran interconectados entre sí, con el objetivo de compartir información dentro de un área establecida, en cientos de metros.

1.7.1. TOPOLOGIAS DE RED

Es la manera en que los dispositivos se entrelazan, para compartir un medio físico. La interconexión puede física o lógica.

Entre los diferentes tipos de topología que existen tenemos:

- Estrella.
- Bus.
- Anillo.

A continuación una descripción resumida de cada topología:

- Topología estrella; es la más común y se constituye de un concentrador en el que fluye la información, fácil de administrar e implementar.
- Topología Bus; todos los dispositivos se conectan al medio de transmisión, a través de coaxiales.
- Topología Anillo; los dispositivos se encuentran conectados en estrella, usando para la transmisión un permiso o Token, muy resistente a fallas y costoso.

  En la figura 1.3 se indica la representación de la topología estrella.

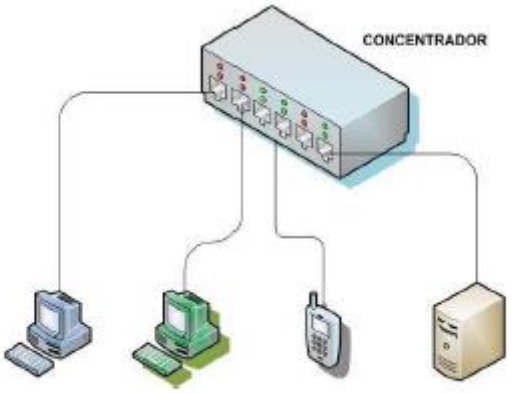


Figura 1.3 Topología ESTRELLA

En la figura 1.4 se indica la representación de la topología bus.

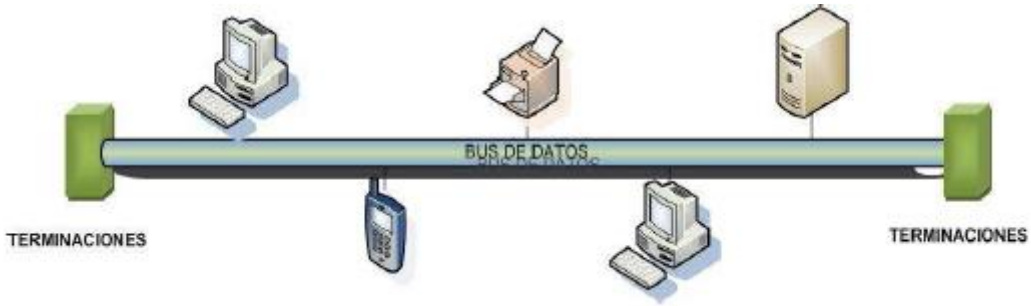


Figura 1.4 Topología BUS

En la figura 1.5 se indica la representación de la topología anillo.

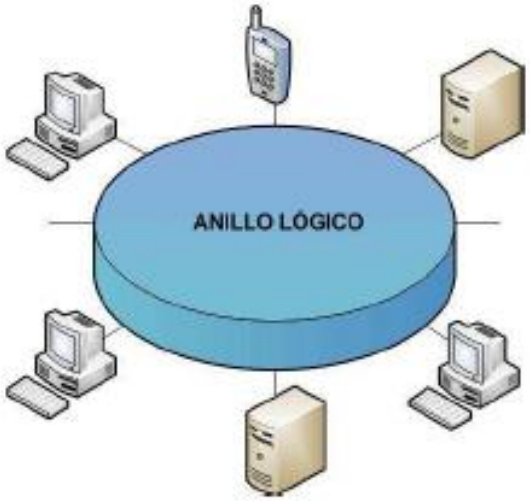


Figura 1.5 Topología ANILLO

1.7.2. SISTEMAS LAN

El modelo ISO-OSI posee diferentes funcionalidades, principalmente en capas superiores, que son independientes de la arquitectura mediante la cual estos sistemas transmiten sus datos de información. Por tanto, este modelo se reduce a 2 capas: la capa física y la capa de enlace.

La capa enlace esta subdividida en 2 subcapas: la de control lógico del enlace LLC[17] y la subcapa de control de acceso al medio.

[17] LLC Logical Link Control, define la forma en que los datos son transferidos sobre el medio físico

El estándar más usado es el 802.3 del IEEE, conocida como ETHERNET. Este define diferentes capas físicas, lo que permite tener un abanico de velocidades sobre diversos medios de TX. En la figura 1.6 se indica los parámetros de capa física IEEE 802.3, donde el método de señalización implica el uso de banda ancha o angosta para la comunicación.

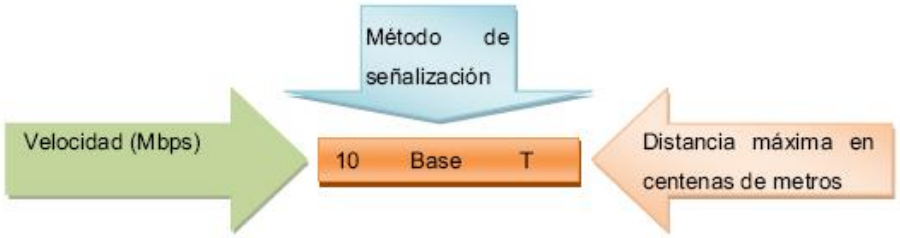


Figura 1.6 Parámetros capa física IEEE 802.3

Lo más común de estas redes es 10BASET, donde las estaciones se conectan a la red por medio de un concentrador de cableado, a través de la interfaz RJ45, usados con cables de categorías 3, 5 y 6 entre los más comunes.

En el desarrollo de ETHERNET una de las tecnologías más usadas actualmente es la de Fast Ethernet conocida como 100BASET, que conserva las características de la 10BASET, siendo su estándar el 802.3u.

Se considera finalmente la tecnología GIGABIT ETHERNET, compatible con los anteriores 10/100BASET. Tiene los siguientes estándares:

- 802.3z, Ethernet conmutada a 1 Gbps, que abarca las tecnologías 1000BASE-SX/LX/CX.
- 802.3ab, Ethernet conmutada a 1 Gbps, que abarca la tecnología 1000BASET.

En la figura 1.7 se indica las opciones de tecnologías para IEEE 802.3

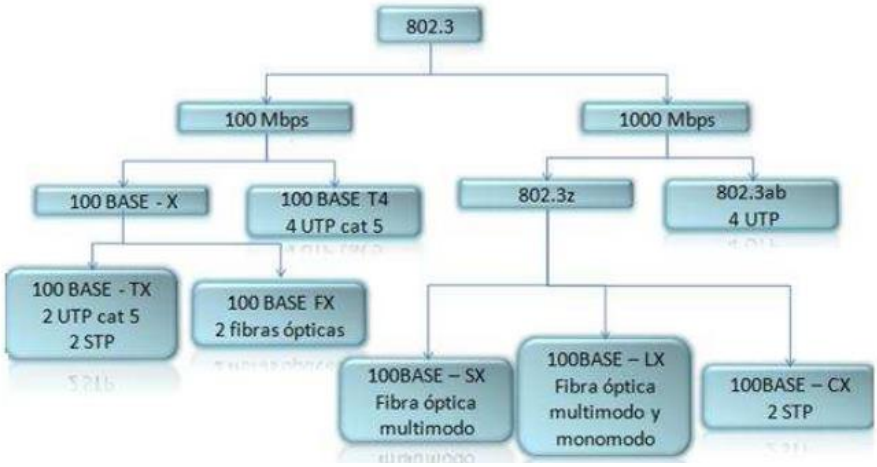


Figura 1.7 Opciones de tecnologías para IEE 802.3

1.7.3. EQUIPOS ACTIVOS EN REDES LAN

Los comités 802 del IEEE se concentran en la interfaz física relacionada con los niveles físicos y de enlace de datos del modelo OSI. Los productos que siguen las normas 802 incluyen tarjetas de la interfaz de red, routers bridges entre otros componentes utilizados para la creación de redes LAN de par trenzado y cable coaxial.

El nivel de enlace se divide en dos subniveles que son MAC y LLC. Los cuales se diferencian en la capa física en la subcapa MAC, sin embargo son compatibles en la subcapa de enlace. [6].

1.7.3.1. Conmutador o Switch

Es un dispositivo digital lógico de interconexión de equipos que opera en la capa enlace de datos del modelo OSI.
Un switch retransmite los paquetes hacia un puerto físico basado en información propia de la trama, esta acción se realiza mediante las direcciones físicas MAC[18] de los dispositivos conectados. Existen 3 métodos de conmutación: Cut & Through, Store & Forward y Fragment Free

18 MAC Media Access Control, es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

1.7.3.2. Redes VLAN

Una red VLAN[19] es un método para la creación de redes lógicamente independientes que forman parte de una red física. La unión de varias redes VLANs puede coexistir en un solo conmutador físico o en una red física. Además de ser útiles para la reducción del tamaño del dominio de difusión, ayudan a la administración de la red, separando segmentos lógicos de una red de área local.

Una VLAN es una red que es conformada por varios dispositivos de red que trabajan como si estuviesen conectados a un mismo conmutador, sin embargo pueden estar conectados físicamente a otros segmentos de una red local. Las VLAN son configuradas mediante software es por ello que son más flexibles en cuanto a su manejo. Otra de las grandes ventajas de las VLANs es cuando se mueve físicamente un computador a otra ubicación este sigue perteneciendo a la misma VLAN sin necesidad de cambiar la configuración IP del computador [6].

El protocolo de etiquetado que domina el mundo de las VLANs, es el IEEE 802.1Q, sin embargo sus antecesores protocolos propietarios son el ISL[20] y el VLT[21].

En sus inicios el principal problema que existió en la creación de redes fue el tamaño de los dominios de colisiones (Hubs), sin embargo esto se logró controlar mediante la inserción de los switches, aunque esto causo otro problema que fue el aumento de los dominios de difusión, para manejar esto se introdujo las VLANs. Otro de los usos para las VLANs es el de restringir y limitar el acceso a los recursos de red con independencia de la topología física de ésta [6].

En el ámbito de las VLAN, trunk (troncal) designa una conexión de red que transporta múltiples VLANs, las cuales son identificadas con etiquetas o tags [6].

19 VLAN Virtual Local Area Network, red de área local virtual) es un método para crear redes lógicas independientes dentro de una misma red física.
20 ISL Inter-Switch Link, protocol propietario de Cisco que mantiene información sobre VLANs en el tráfico entre routers y switches.
21 VLT Virtual LAN Trunk, protocolo propietario de 3COM.

En la figura 1.8 se indica la red VLAN con el uso de switches

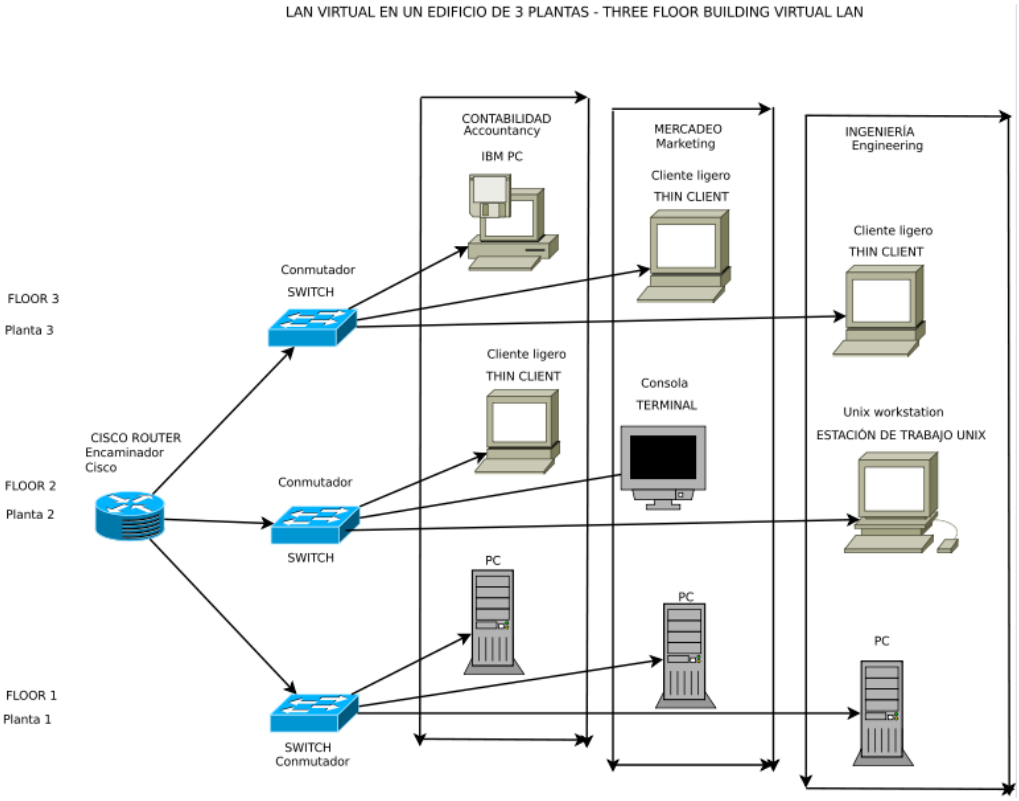


Figura 1.8 Red VLAN con uso de Switches

1.7.4. PROTOCOLOS USADOS EN LOS SWITCHES

1.7.4.1. Spaning Tree Protocol

Spanning Tree Protocol STP corresponde al protocolo de capa 2 del modelo OSI, teniendo dos versiones correspondientes al STP: 1) original (DEC STP) y 2) estandarizada por el IEEE[22] (IEEE 802.1D); mismos que no son compatibles por lo que es recomendable la utilización de versiones estandarizadas por la IEEE [7].

La función corresponde a la gestión de la presencia de bucles en topologías de red, debido a enlaces redundantes que garantizan la disponibilidad de conexiones; El protocolo permite activar y desactivar automáticamente los enlaces de conexión, grantizando que la topología se encuentre libre de bucles.

IEEE Institute of Electrical and Electronics Engineer: Instituto de Ingeniería Eléctrica y Electrónica

La existencia de rutas alternativas con respecto a una misma maquina o segmentos de red de destino, dan la posibilidad de generación de bucles infinitos, mismas que son necearias para la generación de redundacias y estableciendo una mayor fiabilidad de la red, en el caso de la existencia de varios enlaces, y uno de ellos falle, el otro enlace puede seguir soportando el tráfico de red.

Los dispositivos de interconexión de nivel de enlace de datos buscan enviar indefinidamente tramas Broadcast[23] y multicast debido a la existencia de bucles en la topología de la red, consumiendo el ancho de banda en la red y CPU de los dispositivos de enrutamiento, provocando la degradación de la red con la posibilidad de quedar inutilizable en corto tiempo. La inexistencia de un campo TTL (Time to live, tiempo de vida) en las tramas de capa 2 llevan a quedarse atrapadas indefinidamente hasta que se rompa el bucle; en el caso del router se puede evitar este tipo de problemas. La solución es permitir la existencia de enlaces físicos redundates, pero creando una topología lógica libres de bucles.

El STP permite calcular una ruta única libre de bucles, manteniendo los enlances redundantes desactivados como reserva, que serán activados en el caso de la existencia de fallas. En el caso de que la configuración de STP cambie o un segmento de la red redundante se vuelve inalcanzable, el algoritmo reconfigura nuevamente los enlaces y restablece la conectividad, entra a funcionar uno de los enlaces de reserva.

La existencia de multiples variantes del Spaning Tree Protocol, permitio remplazar el uso del STP original, ocacionado por el tiempo que tarda el algoritmo utilizados en converger [7]; una de las variantes es el Rapid Spaning Tree Protocol RSTP. El árbol de expansión (Spaning Tree) permanece vigente hasta que ocurre un cambio en la topología, esta situaciónque el protocolo es capaz de detectar de forma automática, llegando a expansiones del árbol en cinco minutos. Cuando ocurre uno de estos cambios. El puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

Broadcast: transmisión de datos recibidos por los dispositivos en una red

Los puentes se comunican mediante mensajes de configuración denominados Bridge Protocol Data Units (BPDU)[24].

1.7.4.1.1. Elección del puente raíz

Entre las decisiones que se deben tomar los switches de la red es indentificar el puente raíz, esto afectará un flujo de tráfico. Al encender un switch, supone que es el switch raíz enviando las BPDU que contiene la dirección MAC de sí mismo tanto en el BID raíz como emisor. El BID es el Bridge Identifier: Bidge Priority + Bridge Mac Address. En donde el Bridge Priority corresponde al valor configurable con se encuentra por defecto establecido en 32768 y el Bridge Mac Address es la dirección MAC del puente [7].

Cada uno de los switch busca remplazar el BID de la raíz más alta por los BID de la raíz más baja en los BPDU enviados. Todos los switches reciben las BPDU y determinan que el switch con valor de BID raíz es el más bajo será el puente raíz. Se puede establecer la prioridad del switch en un valor más pequeño que el valor por defecto, lo que hace que el BID sea más pequeño, mismos que solo debe ser implementado mediante un conocimiento a profundidad en la existencia del flujo de tráfico de la red [7].

1.7.4.1.2. Elección de los puertos raíz

Cuando se alegido el puente raíz, se debe calcular el puerto raíz para el resto de los puentes que no son raíz. El procedimiento a seguir es el mismo: entre todos los puertos del puente, se escoge como puerto raíz el puerto que tenga el menor costo hasta el puente raíz. En caso de que existan dos o más puertos con el mismo costo hacia el puente raíz, se utiliza la prioridad del puerto para establecer la raíz.

[24] Bridge Protocol Data Units (BPDU): Tramas que contienen información del protocolo tipo Spanning tree

1.7.4.1.3. Elección de los puertos designados

Posterior a la elección del puente raíz se preocede a calcular el puerto raíz para los demás puentes que no son raíz. El mismo procedimiento en todos los puentes es el mismo, se escoge como puerto raíz el puerto que tenga el menor costo hacia el puente raíz de entre todos los puertos del puente. En caso de que existan dos o más puertos con el mismo costo hacia el puente raíz, se procede a utilizar la prioridad del puerto para definir la raíz.

1.7.4.1.4. Elección de los puertos designados

Después de tener el puente raíz y los puertos raíz de los otros puentes se procede a calcular los puertos designados de cada segmento de red. En cada enlace que exista entre dos switches habrá un puerto desigando, será elegido el puerto de switch que poseea un menor costo para llegar al puente raíz, mismo que se encuentra relacionado al tipo de enlace existente en el puerto (Ethernet, Fast Ethernet, Gigabit Ethernet). Cada enlace tendrá distinto costo administrativo, siendo el de menor valor el puerto con mayor velocidad; en caso de exitir una igualdad entre los costos administrativos que tienen los dos switches para llegar al root bridge, se procede a elegir como designet port, el puerto del switch que tenga menor Bridge ID (BID). Los puertos que no son elegidos como raíz ni como designados deberán ser bloqueados.
La topologia puede cambiar por [7]:

- Se desactiva o se bloquea el puerto
- Un puerto bloqueado o desactivdado se activa

La introducción de un BPDU para la notificacion de cambios en la topología se realiza para detectar posibles anomalías en switch, con el fin de notificar al puerte raíz, mediante el envio de TCN[25] en su puerto raíz durante un intervalo de tiempo, mismo que no contiene información, realizando un acuse de recibido del cambio producido en la topología, hasta que se obtenga una respuesta por el puente raíz.

25 TCN: Es una BPDU muy simple que no contiene información y se envía durante el intervalo de tiempos de saludo.

Los puertos pueden encontrarse en los siguientes estados [7]:

- Bloqueo: Sucede cuando las tramas de datos no permiten actualizar las tablas de direcciones descartando las tramas de datos, recibiendo BPDU's, sin la capacidad de enviar una respuesta.
- Escucha: Ocurre cuando los switches establecen la existencia de una ruta alternativa hacia el puente raíz, revisando el coste, en caso de ser mayor el estado se bloquea y las tramas se descarta sin actualizar las tablas ARP[26].
- Aprendizaje: Estado en que las tramas de datos son descartadas pero son actualizadas las tablas de direcciones MAC procesando las BPDU.
- Envio: Estado en que los puertos tienen la capacidad de enviar y recibir datos, actualizando las tablas de direcciones MAC[27] mediante el procesamiento de las BPDU.
- Desactivado: Se establece cuando un puerto es deshabilitado o existe una falla sin el procesamiento del BPDU.

1.7.4.1.5. Inter Switch Link

El tráfico existente entre los routers y switches que contiene la informacion sobre las VLANs corresponden al protocolo propietario de Cisco y es identificado como Inter Switch Link (ISL), metodo que solo se encuentra soportado por equipos CISCO mediante enlaces Fast y Gigabit Ethernet. El tamaño de las tramas ISL puede variar entre 94 y 1548 bytes debido a la sobrecarga que el protocolo crea en la encapsulación.
Compite con el protocolo libre (no propietario) de IEEE 802.1Q.

1.7.4.1.6. Conmutador Capa 3

Los dispositivos lógicos de interconexión de redes se conocen como conmutador o swith y operan en la capa del enlace de datos, su función es la interconexión de

[26] ARP: protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware
[27] MAC: Identificador de control de acceso medio

dos o mas segmento de red pasando datos entre segmentos de acuerdo a la dirección MAC de destino de las distintas tramas en la red. El commutador es utilizado para conectar multiples redes funcionando como un filtro que mejora el rendimiento y seguridad del área local de la red.
El conmutador CAPA 3, tiene como funciones tradicionales el correspondiente al de capa 2, además de integrar funciones de routing o enrutamiento, validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicional (RIP, OSPF, etc.) y la definición de redes virtuales (VLAN) sin el requerimiento de un router externo [7].

Los switches de capa 3 permiten la unión de segmentos de diferentes dominios de difusión o broadcast, segmentando las redes LAN en las que la utilización de switches de capa 2 implicaría una pérdida de rendimiento y eficiencia debido a la cantidad de broadcasts; además se puede establecer que un switch de capa 3 utiliza técnicas de enrutamiento de manera escalable.

Entre los comuntadores de capa 3 se puede establecer [7]:

1.7.4.1.7. Paquete por paquete

Corresponde a un tipo especial de conmutador Store-and-Forward, almacena y examina el paquete, calculando el CRC y decodificando la cabecera de la capa de red definiendo la ruta a través del protocolo de enrutamiento adoptado.

1.7.4.1.8. Cut-through

El Cut-through es un conmutador que determina la dirección de destino mediante la revisión de los primeros campos a través de los headers de capa 2 y 3, estableciendo la conexión punto a punto que permite generar una alta tasa de transferecia de paquetes.

El Multi Protocolo Over ATM (MPOA)[28], aprobado como estándar, limitado por los backbones ATM, es complejo al ser implementado mismo que se refleja en la generación de altos costos.

1.8. REDES DE ÁREA LOCAL INALÁMBRICAS

Las Wireless Local Area Network (WLAN[29]) corresponden a las redes inalámbricas para áreas locales, establecidas por la comunicación de datos mediante radiofrecuencia minimizando la conexión de cableados, con el fin de compartir accesos a Internet [1].

1.8.1. FUNCIONAMIENTO

Son empleados para transportar información entre puntos mediante la utilización de ondas de radio, las cuales son las portadoras de radio sobre las que va la información, su función es llevar la energía a un receptor remoto; los datos a transmitir se superponen a la portadora de radio y así pueden ser extraídos exactamente en el receptor final.

Este proceso es conocido como modulación de portadora por la información que esta siendo transmitida; si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos, el receptor se sitúa en una determinada frecuencia, frecuencia de portadora, ignorando el resto.

En la configuración LAN los puntos de acceso se conectan mediante un cableado normalizado, recibiendo la información, almacenándola y transmientiendo mediante una conección de red cableada fija que puede soportar un pequeño grupo de usuarios. [1].

[28] MPOA: Multi protocol Over ATM protocolo que habilita servicios ATM para integrarse con LANs que usan Ethernet, token ring o protocolos TCP/IP.
[29] WLAN: Wireless Local Area Network

1.8.2. CONFIGURACIONES DE RED PARA RADIOFRECUENCIA

Una configuración básica puede ser entre dos ordenadores con tarjetas WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área de cobertura; esto es conocido comoo red pear to pear.

Mediante la instalación de un punto de acceso se puede duplicar la distancia de comunicación que en zonas abiertas puede alcanzar 150 m generando alcances finitos, que son conectados a una red cableada, permitiendo el acceso a los recursos existentes en el servidor que gestionen el tráfico en la red, en el caso de un campus universitario es necesario la implementacion de un mayor punto de acceso que permitan cubrir las áreas evitando los cortes por accesos, mismo que se conoce como roaming.

Con el fin de evitar los posibles problemas en la topología, es necesario definir el diseño de la red wireless, buscando cubrir el mayor número de puntos, extendiendo el alcance de la red LAN. La antena direccional es un componente que se debe considerar en el equipo de la WLAN.

1.8.3. ASIGNACIÓN DE CANALES

Los estándares 802.11b y 802.11g utilizan la banda de 2,4 – 2,5 Ghz. Permitiendo la asignación de 11 canales utilizables por equipos WIFI, los cuales pueden configurarse. Estos 11 canales no son completamente independientes canales contiguos se superponen y producen interferencias, en la práctica sólo se pueden utilizar 3 canales en forma simultánea 1,6 y 11. Esta asignación de canales se hace sólo en el punto de acceso, pues los clientes automáticamente detectan el canal, excepto si se forma una red ad hoc[30] o punto a punto cuando no existe punto de acceso. [1].

30 Ad Hoc: Es un tipo de red inalámbrica decentralizada.

1.8.4. ESTÁNDARES 802.11

El estándar 802.11 define los niveles inferiores del modelo OSI mediante para las conexiones inalámbricas que utilizan ondas electromagnéticas. Por ejemplo:

- La capa física a veces abreviada capa PHY[31] ofrece tres tipos de codificación de información.
- La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico LLC y control de acceso al medio MAC.

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos, la capa enlace de datos define la interfaz entre el bus del equipo y la capa física.

El estándar 802.11 esta conformada por tres capas físicas que establecen modos de transmisión alternativos. En la tabla 1.3 se indica las capas del estándar 802.11.

Capa de enlace de datos (MAC)	802.2
	802.11
Capa física (PHY)	DSSS FHSS Infrarrojo

Tabla 1.3: Capas estándar 802.11

El estándar 802.11 permite la generación de un ancho de banda de 1 a 2 Mbps, el estándar original se ha modificado para optimizar el ancho de banda, incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11. En la tabla 1.4 se indica las distintas modificaciones del estándar 802.11 y sus significados. [1]

31 PHY Physical layer

Nombre del estándar	Nombre	Descripción
802.11a	Wifi5	El estándar 802.11 (llamado WiFi 5) permite un ancho de banda superior (Rendimiento total máximo 54 Mbps, en la práctica 30 Mbps). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Wifi	El estándar 802.11 es el más utilizado actualmente. Rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) con un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de

		transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.
802.11g		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h		El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i		El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las

		tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir		El estándar 802.11r se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j		El estándar 802.11j es para la regulación japonesa lo que el 802.11h es para la regulación europea.

Tabla 1.4: Clases de Estándar 802.11

1.8.4.1. Rango y flujo de datos

Los estandres físicos (802.11a, 802.11b y 802.11g) corresponden a las modificaciones del estándar 802.11 permitiendo alcanzar variaciones en la velocidad en la transferencia de datos.
El la tabla 1.5 se indica los tipos de estándar WiFi:

Estándar	Frecuencia	Velocidad	Rango
WiFi a (802.11a)	5 GHz	54 Mbps	10 m
WiFi b (802.11b)	2,4 GHz	11 Mbps	100 m
WiFi g (802.11g)	2,4 GHz	54 Mbps	100 m

Tabla 1.5: Tipos de estándar WiFi

1.8.4.2. 802.11a

Se basa en la tecnología OFDM[32] multiplexación por división de frecuencias ortogonales, que permite transmitir mediante 8 canales no superpuestos en un rango de frecuencia de 5GHz [8], compatibles con dispositivos de banda dual [8].
El la tabla 1.6 se indica las velocidades de transmisión y rangos de distancia del estándar 802.11a:

32 OFDM: Orthogonal Frequency Division Multiplexing

Velocidad hipotética (en ambientes cerrados)	Rango
54 Mbps	10 m
48 Mbps	17 m
36 Mbps	25 m
24 Mbps	30 m
12 Mbps	50 m
6 Mbps	70 m

Tabla 1.6: Velocidades de TX y Rangos de distancia estándar 802.11a

1.8.4.3. 802.11b

Permite la transmisión en un rango de 100 metros en espacios cerrados y de más de 200 al aire libre, podría cubrir mayores distancias con el uso de antenas direccionales; a una transferencia de datos máximo de 11 Mbps [8].

El la tabla 1.7 se indica las velocidades de transmisión y rangos de distancia del estándar 802.11b:

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbps	50 m	200 m
5,5 Mbps	75 m	300 m
2 Mbps	100 m	400 m
1 Mbps	150 m	500 m

Tabla 1.7: Velocidades de TX y Rangos de distancia estándar 802.11b

1.8.4.4. 802.11g

Permite un máximo de transferencia de 54 Mbps, comparables a los del estándar 802.11b. Utiliza un rango de frecuencia de 2.4 GHz y con una codificación de OFDM [8].

El la tabla 1.8 se indica las velocidades de transmisión y rangos de distancia del estándar 802.11g:

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbps	27 m	75 m
48 Mbps	29 m	100 m
36 Mbps	30 m	120 m
24 Mbps	42 m	140 m
18 Mbps	55 m	180 m
12 Mbps	64 m	250 m
9 Mbps	75 m	350 m
6 Mbps	90 m	400 m

Tabla 1.8: Velocidades de TX y Rangos de distancia estándar 802.11g

1.8.5. SEGURIDAD EN REDES INALÁMBRICAS

La tecnología Wi-Fi presenta problemas generados por la saturación del espectro radioeléctrico establecido en las conexiones de larga distancia mayores a 100 metros, con la capacidad de conectar ordenadores en distancias reducidas con el reiesgo de sufrir interferencias. Una gran cantidad de redes instaladas son vulnerables al convertirse en redes abiertas sin protección de la información que transfieren. Para los problemas presentados se puede solucionar mediante la utilización de protocolos cifrados como WEP[33], WPA[34] o WPA2[35] porporcionado por los dispositivos inalámbricos [8]:

33 WEP Wired Equivalent Privacy, es un sistema de cifrado incluido en el estándar IEEE 802.11
34 WPA Wi-Fi Protected Access, es un sistema para proteger redes inalámbricas, corrige las deficiencias de WEP.
35 WPA2 Wi-Fi Protected Access 2, creado para corregir las vulnerabilidades de WPA.

- WEP, cifrados entre 64 y 128 bits con niveles de seguridad que codifican los datos mediante claves con varios tipos de vulnerabilidades de las mismas.
- WPA, generadas con claves conformadas por dígitos alfanuméricos dinámicos.
- IPSEC[36], (túneles IP) en caso de VPN[37] y el conjunto de estándares IEEE 802.1x, que permite la autentificación y autorización de usuarios.
- MAC, permite el acceso solo a los dispositivos autorizados a la red.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible para otros usuarios.
- WPA2, (estándar 802.11i) protocolo de seguridad que necesita hardware y software compatible, es el protocolo más seguro para redes Wi-Fi.

En general se puede definir que no existen alternativas fiables ya que cualquier cosa utilizada puede ser vulnerable.

1.8.6. EQUIPOS DE COMUNICACIÓN INALÁMBRICA

Los dispositivos Wi-Fi, pueden ser clasificados como dispositivos de distribución o red, entre los que se tienen Puntos de Acceso, Repetidores y dispositivos terminales como tarjetas receptoras (PCI, PCMCIA y USB).

1.8.7. Router WiFi

1.8.8. Dispositivos de Distribución o Red [9]

- Los puntos de acceso permiten conectar dispositivos en forma inalámbrica a una red existente, pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.

36 IPSEC Internet Protocol Security
37 VPN Virtual Private Network, permite una extensión segura de la LAN sobre una red pública.

- Los router inalámbricos son dispositivos diseñados para redes pequeñas (hogares o pequeñas oficinas), permiten la interconección de puntos de acceso con un switch para conectar equipos vía cable.
- Los repetidores inalámbricos sirven para extender la cobertura de redes inalámbricas, conectadas a una red existente creando una señal limpia.

1.8.9. Dispositivos Terminales [9]

- Tarjetas PCI para Wi-Fi que se integran a los ordenadores, también incluyen las tarjetas MiniPCI.
- Tarjetas PCMCIA son tarjetas capaces de llegar hasta la b de Wi-Fi, limitando la velocidad de transmisión.
- Tarjetas USB para Wi-Fi son tarjetas con el estándar 802.11N (Wireless-N) que es el estándar liberado para redes inalámbricas.
- Impresoras, cámaras Web y otros periféricos, permitiendo el ahorro de cableado en las instalaciones de redes.

1.8.9.1. SERVICIOS DE RED

1.8.9.2. Intranet

Es una red de computadoras que utilizan tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y operacionales. Intranet se utiliza en oposición a Internet.

1.8.9.3. Beneficios de la Intranet de los centros docentes

- Capacidad para compartir recursos.
- Alojamiento de páginas web.
- Servicios de almacenamiento de información.
- Servicio de correo electrónico.
- Foros, canales bidireccionales de comunicación.

- Realización de diversos trabajos como gestión de tutoría, test, periódicos; gestiones de secretaria y dirección; biblioteca; y gestiones administrativas [10].

1.8.9.4. Foros, wikis, blogs y redes sociales dentro de las Intranets

Una Intranet (Red Interna) contiene servidores de archivos, impresión, correos, Telefonía IP, Web con herramientas de comunicación e información como: Foros, wikis, blogs y redes sociales.

Las aplicaciones Web se alimentan de modelos de comunicación como foros, wikis, blogs y redes sociales, con impacto en la comunicación interna y objetivos ajustados a la innovación, mejora permanente y gestión del conocimiento [10].

1.8.9.5. Voz sobre IP

La Voz sobre IP, Voz IP, VozIP, VoIP (Voice over IP), son recursos que posibilitan que la señal de voz se traslade mediante un protocolo IP, en forma digital en paquetes de datos, en lugar de enviarla por la telefonía convencional como las redes PSTN (Public Switched Telephone Network, Red Telefónica Pública Conmutada) [11].

- VoIP corresponde al conjunto de normas, dispositivos, protocolos, en la tecnología que permite comunicar voz sobre el protocolo IP.
- Telefonía sobre IP conforma el servicio telefónico disponible al público, con numeración E.164[38], realizado con tecnología de VoIP.

38 E.164, Plan Internacional de numeración de telecomunicaciones públicas.

En la figura 1.9 se indica un digrama de red para voz sobre IP

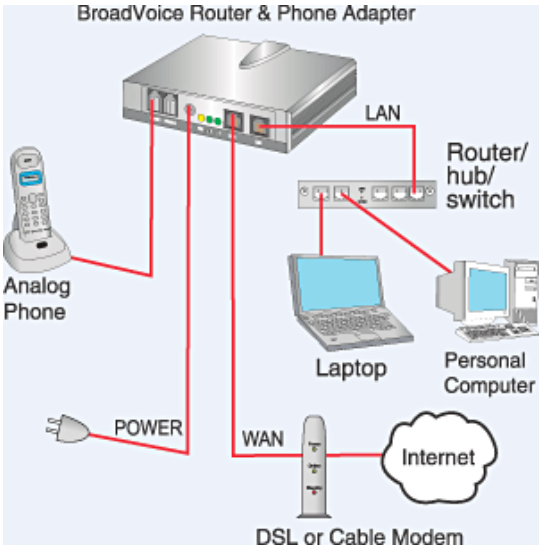


Figura 1.9 Diagrama de red para VoIP

1.8.10. ELEMENTOS

1.8.10.1. El Cliente

El cliente establece y origina llamadas de voz que se codifica, empaqueta y decodifica a través de los altavoces o audífonos. Un Cliente puede ser un usuario de alguna empresa que comercialice servicios de telefonía sobre IP.

1.8.10.2. Los Servidores

Gestionan las operaciones de base de datos, como la contabilidad, recolección, enrutamiento, administración y control del servicio, y registro de usuarios, etc.

1.8.10.3. Los Gateways

Brindan un puente de comunicación entre usuarios, su función proveer interfaces con la telefonía tradicional, como una plataforma para los usuarios. Se utilizan para terminar la llamada, es decir el cliente la origina y Gateway termina la llamada.

1.8.10.4. Funcionalidad

VoIP facilita tareas realizadas por redes telefónicas comunes[11]:

- Las llamadas telefónicas pueden ser enrutadas a un teléfono VoIP.
- Números telefónicos gratuitos VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países.
- Los agentes de call center pueden trabajar en cualquier lugar con conexión a Internet.
- Paquetes de VoIP incluyen servicios como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamada.

1.8.10.5. Móvil

Los usuarios de VoIP pueden seguir haciendo y recibiendo llamadas al viajar de la siguiente forma[11]:

- Los subscriptores pueden hacer y recibir llamadas locales fuera de su localidad, cobrada como llamada local mediante conexión a Internet.
- Los usuarios de Mensajería Instantánea basada en servicios de VoIP pueden hacer y recibir llamadas telefónicas en cualquier parte.
- Los teléfonos VoIP pueden incluir videoconferencias, intercambio de datos y mensajes, audio conferencias, administración de libros de direcciones e intercambio de información.

1.8.10.6. Repercusión en el comercio

La Voz sobre IP está bajando los costos de las comunicaciones, mejorando la relación entre proveedores y clientes, integrando aplicaciones en portales web, de forma que los usuarios pueden establecer relaciones con una empresa en concreto a través de un operador de Voz IP.

1.8.10.7. Estándar VoIP (H.323)

Establecido en 1996 por la UIT (Unión Internacional de Telecomunicaciones) suministra a los diversos fabricantes una serie de normas para que puedan evolucionar en conjunto.

1.8.10.8. Características Principales

Por su estructura el estándar proporciona las ventajas [11]:

- Control el tráfico de la red.
- Integración con las grandes redes de IP actuales.
- Independencia del hardware utilizado.
- Implementar software como hardware, eliminando el impacto para el usuario común.
- Integración de Vídeo.
- Proporciona enlace a redes de telefonía tradicional.
- Software instalable en pequeños servidores.

1.8.10.9. Estándar VoIP (SIP)

(Session Initiation Protocol) "Protocolo de Inicio de Sesión" es un protocolo que en la actualidad es mayormente utilizado. VoIP es un una tecnología que usa Protocolos de Internet (IP) mediante comprencion y descomprecion eficiente de paquetes de datos o datagramas, permitiendo la comunicación a través de una red como la de Internet prestando servicios de telefonía o videoconferencia.

1.8.10.10. Arquitectura de red

El Estándar define tres elementos fundamentales en la estructura [11]:

- Terminales: son sustitutos de los teléfonos, pueden implementar software como en hardware.

- Gatekeepers: son el centro de la organización VoIP, sustitutos de las actuales centrales.
- Gateways: son enlaces con la red telefónica tradicional.

Protocolos de VoIP: son lenguajes utilizados por distintos dispositivos VoIP para su conexión, definiendo la eficacia y complejidad de la comunicación: [11]

- Por orden de antigüedad:
  - H.323 - Protocolo definido por la ITU-T;
  - SIP - Protocolo definido por la IETF;
  - Megaco (También conocido como H.248) y MGCP - Protocolos de control;
  - UNIStim - Protocolo propiedad de Nortel (Avaya);
  - Skinny Client Control Protocol - Protocolo propiedad de Cisco;
  - MiNet - Protocolo propiedad de Mitel;
  - CorNet-IP - Protocolo propiedad de Siemens;
  - IAX - Protocolo original entre PBXs Asterisk;
  - Skype - Protocolo propietario peer-to-peer;
  - IAX2 - Protocolo para la comunicación entre PBXs Asterisk;
  - Jingle - Protocolo abierto utilizado en tecnología XMPP;
  - MGCP- Protocolo propietario de Cisco;
  - weSIP- Protocolo licencia gratuita de VozTelecom.

1.8.10.11. Parámetros de la VoIP

El principal problema que presenta VoIP como las aplicaciones de IP es la de garantizar la calidad de servicio de Internet que soporta "mejor esfuerzo" (best effort) y limita el ancho de banda en la ruta.

1.8.10.12. Códecs

Para codificación de voz y transmisión por red IP, se usa códecs que garantiza la codificación y compresión del audio o video antes de generar un sonido o imagen

utilizable. El ancho de banda depende del Códec utilizado misma que varia según la calidad de los datos transmitidos. Entre los codecs más utilizados esta [11]:

- G.711: bit-rate de 56 o 64 Kbps.
- G.722: bit-rate de 48, 56 o 64 Kbps.
- G.723: bit-rate de 5,3 o 6,4 Kbps.
- G.728: bit-rate de 16 Kbps.
- G.729: bit-rate de 8 o 13 Kbps.

1.8.10.13. Retardo o latencia

Una vez establecidos los retardos de tránsito y procesado se considera aceptable por debajo de los 150 ms.

1.8.10.14. Pérdida de tramas (Frames Lost)

Durante el transito de tramas por la red IP pueden perderse por congestión en la red o corrupción de datos, ocasionando retardos adicionales, motivo por el cual los terminales de voz retransmiten con perdidas, también llamadas Frame Erasures. El efecto de las tramas perdidas depende de como se gestionen las Frame Erasures. Una estrategia es reproducir las muestras de voz previas, usuando sistemas de interpolación, técnica conocida como Packet Loss Concealment (PLC) [11].

1.8.10.15. Calidad del servicio

La calidad de este servicio se logra bajo los siguientes criterios [11]:

- Supresión de silencios.
- Aplicación de estándares RTP/RTCP.
- Priorización de paquetes CQ (Custom Queuing), PQ (Priority Queuing), WFQ (Weight Fair Queuing) y DiffServ
- Implantación de IPv6.

1.8.10.16. Ventajas

- Evita los cargos altos de telefonía.
- Ahorros en costo al utilizar una misma red para voz y datos
- Permite que la voz se codifique en paquetes de datos [11].

Hay dos tipos de servicio de PSTN a VoIP:

- Discado Entrante Directo (Direct Inward Dialling: DID)
- Números de acceso (DID conecta a quien hace la llamada directamente con el usuario VoIP).

Los Números de acceso son cobrados como una llamada local para quien hizo la llamada desde la PSTN y gratis para el usuario de VoIP, llegando a ser hasta 100 veces más económicos que los precios de un operador locales.

1.8.10.17. Desventajas

- La calidad de transmisión es inferior a la telefónica
- VoIP no es el protocolo sino la red IP
- Latencia, 200ms (milisegundos) de pausa en la transmisión
- VoIP debe controlar el uso de la red para garantizar una transmisión de calidad.
- Robo de Datos
- Virus en el sistema.

1.8.10.18. Perspectivas de futuro

El creciente desarrollo en el ancho de banda a nivel mundial y la optimización de equipos de capa 2 y 3, garantizan que el QoS (Quality of Service) de los servicios de voz, en el futuro de la Voz sobre IP sea muy prometedor [11].

La tecnología utiliza sistemas operativos (Windows/Linux) desplegando problemas de estabilidad.

Las aplicaciones extras se pueden obtener en centrales IP y tradicionales, mismas que pueden incorporar la tecnología VoIP a sus necesidades.

CAPÍTULO II

2. ANÁLISIS DE LA INFRAESTRUCTURA DE RED ACTUAL

2.1. ANÁLISIS DE LA INFRAESTRUCTURA DE LA RED

2.1.1. INTRODUCCIÓN

El Colegio Nacional Experimental “Juan Pío Montufar” es una Institución de enseñanza media y superior con una trayectoria de 71 años al servicio de la población de la ciudad de Quito y del país. En los últimos años se ha logrado un avance en la infraestructura fruto de la gestión institucional y representantes de los alumnos.

En la actualidad se busca implementar un sistema que permita acceder y sistematizar la información razón por la cual el personal administrativo, profesores, padres de familia y alumnos ven la necesidad de contar con una infraestructura de red para permitir la gestión y la comunicación de los diferentes actores que forman parte de la institución educativa.

2.1.2. IDENTIFICACIÓN, DESCRIPCIÓN Y DIAGNÓSTICO DEL PROBLEMA

El Colegio Nacional Experimental “Juan Pío Montufar” en una Institución educativa pública, laica, dedicada a la formación humana y profesional, sustentada en las áreas de ciencia, técnica, tecnología, cultura y sociedad.

Satisface las demandas sociales del país con formación de ciudadanos, líderes y libres, con pensamiento crítico, creativo, con espíritu solidario, ético, cívico y conciencia social que aporten al mejoramiento de la calidad de vida de los ecuatorianos y hagan posible la consecución de la justicia social; se distingue por

su calidad profesional y académica de su personal, en la prestación de servicios a los sectores populares de la población ecuatoriana.

En esta misión el Colegio debe enfrentarse a situaciones y escenarios cada vez más diversos, con integración desde el ámbito administrativo hasta el organizativo sin dejar de lado el aspecto académico base fundamental del trabajo de la institución, lo que hace fundamental e indiscutible la modernización del colegio, que actualmente no cuenta con los recursos tecnológicos necesarios para estar a la par de estos nuevos retos y desarrollar adecuadamente su labor.

En un mundo tan desarrollado como el actual, los recursos de información son tan amplios que van más allá de lo que se puede imaginar. El desarrollo tecnológico en el país ha cobrado gran importancia, sobre todo en el área de las comunicaciones, lo que se ve reflejado en los modernos sistemas que han implementado las diferentes organizaciones públicas y privadas para este fin. Es importante mencionar que las comunicaciones juegan un papel indispensable en el desarrollo de todas las instituciones educativas y por consiguiente en el desarrollo de un país.

2.1.3. INSTALACIONES

El Colegio Nacional Experimental" Juan Pío Montufar" posee un campus de 8 hectáreas dentro del cual se encuentran distribuidas diferentes áreas a fin de cumplir con su misión dentro de la sociedad. Las mismas que se señalan a continuación:

- Ambiental
- Audio-Visuales
- Auditorio
- Biblioteca
- DOBE
- Investigación
- Médico-Dental

- Secretaría
- Laboratorio de Biología
- Laboratorios de Computación
- Laboratorio de Física
- Laboratorio de Química
- Laboratorio de Ciencias Naturales

Si bien su distribución dentro del campus es diversa, estas pueden ser agrupadas en áreas funcionales las cuales poseen una relación directa en su trabajo, tal como se especifica en la tabla 2.1.

Área Administrativa	• Oficinas Administrativas: Rectorado, Vicerrectorado, Secretarías • Inspección General • Inspección de Cursos
Área Educativa	• Laboratorios de Computación • Laboratorio de Biología • Laboratorio de Física • Laboratorio de Química • Laboratorio de Ciencias Naturales • Bloque de aulas
Otras Áreas	• Bar y Asociaciones • Biblioteca • Centro Médico y Bodegas Generales • Educación Física • Parqueaderos • Salón de actos • Departamento de Orientación y Bienestar Estudiantil DOBE

Tabla 2.1 Áreas de la Institución

2.1.4. ANÁLISIS DE LA TOPOLOGÍA DE LA RED DE DATOS

La red de la Institución, durante este tiempo de funcionamiento, ha crecido de manera desordenada, sin la documentación ni administración adecuada debido a lo cual los equipos no se encuentran conectados apropiadamente. Entre los problemas encontrados se pueden describir siguientes:

Se instalan nuevos puntos de red o equipos que muchas veces no cumplen las normas establecidas y peor aún tienen la debida etiquetación, estos puntos son conectados a cualquier puerto que esté disponible en ese momento.

Los equipos detallados en la figura 2.1 están interconectados mediante una topología física en estrella con tecnología Fast Ethernet, mediante cables categoría 5e y categoría 6. Los equipos presentan múltiples conexiones entre sí por lo que no se puede definir una topología específica, debido al desorden de la red. Tampoco se encuentra basada en algún tipo de modelo donde por ejemplo se puedan definir niveles como acceso, distribución o núcleo, por lo que no se encuentran definidas funciones de red como VLANs seguridad entre otros.

El enlace a Internet se encuentra contratado mediante un enlace asimétrico Gubernamental gratuito de 2 Mbps de la Corporación Nacional de Telecomunicaciones y otro enlace de 2 Mbps que provee SURATEL este último sirve solo para el servidor web. El enlace de SURATEL llega al router 2 y este a su vez se conecta al computador que cumple la función de servidor web. El enlace de CNT llega al router 1 ubicado en la Sala de Internet, este se encuentra conectado al switch 1, en la misma sala, al que a su vez está conectado en cascada al switch 2 en Colecturía, el switch 3 en la Biblioteca y el switch 4 en la Inspección General, del switch 4 se conectan un Access Point en el Departamento Médico, y la antena omnidireccional de la que sale a un router 3 y de este sale al switch 5 este a su vez se conecta con el switch 6 en el laboratorio de Informática M-3 de terceros y cuartos cursos, al switch 6 se conectan los switch 7, 8 y 9 dentro del mismo laboratorio de informática M-3. Al switch 6 también se conectan

los switch 10 y 11 que están en el laboratorio de Inglés y al switch 12 que está en laboratorio de Informática M-2 de primeros y segundos cursos.

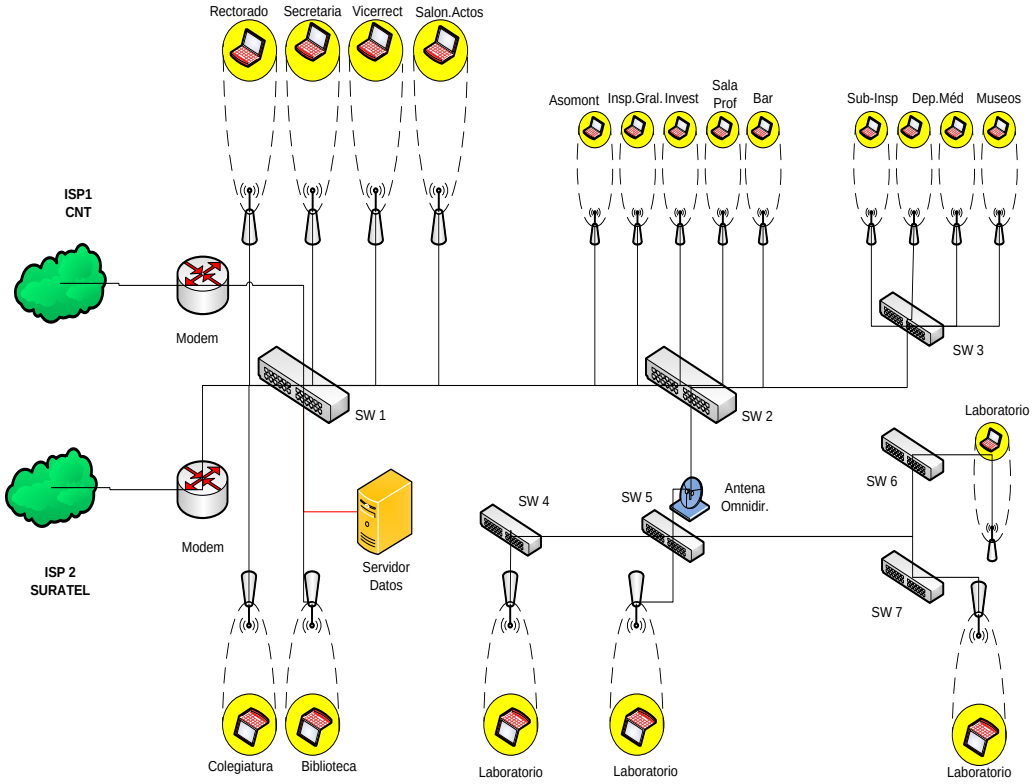


Figura 2.1 Topología de Red del Colegio Experimental "Juan Pío Montufar"

2.1.5. EQUIPAMIENTO

Con el propósito de brindar una idea general acerca de la situación actual de la red de comunicaciones de la institución se realizó un inventario de los equipos que actualmente cuenta la institución. La red de datos se encuentra funcionando de manera independiente de la red de voz por lo que el análisis se realiza de la misma manera.

Dentro del área administrativa del campus, se encuentran los equipos de comunicación, en la secretaria que no es un lugar apropiado para el alojamiento de equipos, ya que no cuentan con una infraestructura adecuada de una sala de equipos o cuarto de telecomunicaciones (rack para equipos, ambientes de acceso restringidos, controles de temperatura, etc.).

El acceso a estas áreas es libre lo que resulta una falla de seguridad debido a que cualquier persona puede ingresar y sustraer cualquiera de ellos. Además no se existe una adecuada documentación de la situación actual de los equipos, así como la función que desempeñan dentro de la red, lo que dificulta la administración de la misma.

2.1.5.1. Equipos para la comunicación de datos

Los equipos de la red corresponden a diversos fabricantes: Huawei, Zyxel, D-Link, CNet, Linksys de los cuales la marca preponderante es la marca D-Link sin embargo esta amalgama de marcas no se encuentra debidamente especificada. A continuación en la tabla 2.2 se presenta una descripción de los equipos que actualmente brindan servicios a los usuarios de la red.

	MARCA	FUNCIÓN	UBICACIÓN	PUERTOS	EQUIPO
Router 1	Modem Huawei echolife hg520c de CNT	Enlace del servicio de Internet	Secretaria	4 Puertos Fast Ethernet 1 Puerto ADSL	
Router 2	ZyXEL P-600 Series Model Number	Enlace del servicio de Internet	Secretaria	4 Puertos Ethernet 1 Puerto DSL 1 CON/AUX	
Router 3	Terraza	Interconexión de Bloques de	Terraza de Bloque de aulas de 5tos	4 Puertos Ethernet 1 Puerto	

		aulas	y 6tos cursos	DSL 1 CON/AUX	
SW 1	D-Link DES-1024Rt 10/100 Fast Ethernet Switch	SW de core Interconecta a los switches de otras áreas hacia el servidor y hacia el internet	Secretaria	24 Puertos Fast Ethernet	
SW 2	Advantek Networks	Interconexión de switches	Colecturía	8 puertos	
SW3	Lynksys SR224	Interconexión de Internet para la biblioteca	Biblioteca	24 pt 10/100 Switch	
SW 4	CNet Power Switch C517-1600	Interconexión de switches	Inspección General	16 Puertos 1x….16x	
Access Point 2	D-Link AirPlus Xtreme G	Conexión de Internet para el	Departmento Médico	1 LAN	

	Wireless Access Point DWL-2100Ap 192-200-200-253	Departamento Médico			
Access Point 1	Lynk Sys Wireless-G Access Point with SES	Conexión de Internet para la biblioteca	Biblioteca	1 LAN	
SW 5	Terraza	Interconexión de switches	Terraza de Bloque de aulas de 5tos y 6tos cursos	8 puertos	
SW 6	Advantek Networks	Interconexión de switches	Laboratorio de Informática M-3	8 puertos	
SW 7	D-Link DES-1024R+ 10/100 Fast Ethernet	Interconexión de Internet para el laboratorio de Informática	Laboratorio de Informática M-3	24 pt 10/100 Switch	
SW 8	D-Link DES-1016D 10/100 Fast	Interconexión de Internet para el laboratorio	Laboratorio de Informática M-3	16 pt 10/100 Switch	

	Ethernet	de Informática			
SW 9	D-Link DES-1016D 10/100 Fast Ethernet	Interconexión de Internet para el laboratorio de Informática	Laboratorio de Informática M-3	16 pt 10/100 Switch	
SW 10	D-Link DES-1016D 10/100 Fast Ethernet	Interconexión de Internet para el laboratorio de Informática	Laboratorio de Inglés	16 pt 10/100 Switch	
SW 11	D-Link DES-1016D 10/100 Fast Ethernet	Interconexión de Internet para el laboratorio de Informática	Laboratorio de Ingés	16 pt 10/100 Switch	

Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución

Los equipos que se encuentran funcionando en la institución no cumplen con requisitos mínimos, como por ejemplo ser administrables. El switch 1 que hace la función de switch de core es de muy baja capacidad, lo que reduce el nivel de optimización de las conexiones y no permite utilizar funciones propias de un equipo de este nivel, por lo que resulta erróneo afirmar que es una red completamente estructurada.

2.1.5.2. Servidor

En la red de la institución actualmente se encuentra operando un computador que realiza las funciones de servidor web, sin embargo este equipo no cumple con la características para trabajar adecuadamente dentro de una red convergente como la que se plantea diseñar para la institución, debido a que posee características similares a las estaciones de trabajo y no resulta adecuado para el alojamiento de servicios.

El actual equipo que funciona como servidor, es una estación de trabajo normal adaptado con los programas necesarios para su funcionamiento, que a pesar de encontrarse en producción actualmente no es la opción más recomendable, en cualquier momento este puede dejar de funcionar. Además este equipo no posee características como redundancia de fuente o protecciones adicionales que brindan confiabilidad en un equipo dedicado exclusivamente como servidor.

Marca:	Clon
Ubicación:	Secretaría
Procesador:	Intel Xeon CPU
Memoria:	6 GB
Tarjeta de Red:	Gigabit Ethernet Broadcon Gigabit Ethernet NetXtreme #2
Plataforma:	Windows Server 2008 R2 Enterprise
Función:	Aloja el servidor del sistema de información académica de la Institución que básicamente sirve para la asignación de notas mensualmente a los estudiantes.

2.1.5.3. Estaciones de trabajo

Las estaciones de trabajo de la Institución poseen diferentes características de acuerdo al área a la que sirven. De los cuatro laboratorios de computación en la Institución, solo el laboratorio de inglés tiene acceso a la red completamente los otros dos tienen acceso pero solo ocho computadores y el otro laboratorio no

tiene acceso a la red. Mientras en las otras salas los equipos son utilizados para la utilización de aplicaciones de escritorio entre las que podemos mencionar paquetes ofimáticos.

En las secretarías, en su mayoría, también se trabaja con equipos que no tienen acceso a la red de la institución, sin embargo estos equipos deben ser tomados en cuenta debido a que se espera tener una interconexión de todas las estaciones de trabajo a la red de datos, no tiene creados cuentas de usuario, todos poseen una cuenta con privilegios de administrador, además no existe ningún control sobre el software que posee cada usuario. A través del campus se encuentran diferentes equipos para el trabajo del departamento de la Institución que en su gran mayoría no se encuentran conectados a la red, por lo que su solicitud para poder ingresar a la misma es una constante. En la tabla 2.3 se encuentran especificadas las características de las computadoras de uso permanente en la Institución.

Cantidad	**Sistema Operativo**	**Procesador**		**Memoria RAM**	**Tarjeta de Red / (Acceso a la Red)**	**Ubicación**
		Marca	**Velocidad**			
4	Microsoft Windows XP Professional	Intel Celeron	2.50 GHz	256 MB	Adaptador Fast Ethernet PCI CNet Pro 200 / (No)	Laboratorio M-3 1ros y 2dos Cursos
1	Microsoft Windows XP Professional	Intel Celeron	2.50 GHz	256 MB	No tiene / (No)	
1	Microsoft Windows XP Professional	Intel Celeron	1.60 GHz	512 MB	Realtek RTL8139/810x Familily Fast Ethernet / (No)	
3	Microsoft Windows XP Professional	Intel Celeron	2.50 GHz	256 MB	No tiene / (No)	
1	Microsoft Windows XP Professional	Intel Celeron	1.60 GHz	512 MB	Adaptador Fast Ethernet VIA / (No)	

2	Microsoft Windows XP Professional	Intel Celeron	1.60 GHz	1 GB	No tiene / (No)	
2	Microsoft Windows XP Professional	Intel Celeron	1.60 GHz	512 MG	No tiene / (No)	
1	Microsoft Windows XP Professional	Intel Celeron	2.50 GHz	512 MB	No tiene / (No)	
2	Microsoft Windows XP Professional	Intel Celeron	2.50 GHz	512 MB	Adaptador Fast Ethernet PCI CNet Pro 200 / (No)	
6	Microsoft Windows XP Professional	Pentium 4	2.8 GHz	512 RAM	NIC Fast Ethernet PCI Family RTL8139 de Realtek/ (No)	
5	Microsoft Windows XP Professional	Intel Core 2 Duo	2.6 GHz	1 GB	No tiene / (No)	
2	Microsoft Windows XP Professional	Intel Core 2 Duo	2.6 GHz	1 GB	Atheros AR 5005 GS Wireless Network Adapter / Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC / (No)	
5	Microsoft Windows XP Professional	Pentium Dual Core	3.0 GHz	2 GB	No tiene / (No)	
1	Microsoft Windows XP Professional	Pentium Dual Core	2.7 GHz	512 MB	No tiene / (No)	
2	Microsoft	Pentium	2.7 GHz	1 GB	No tiene / (No)	

	Windows XP Professional	Dual Core				
1	Microsoft Windows XP Professional	Pentium Dual Core	3 GHz	2 GB	Realtek RTL8139/810x Family Fast Ethernet NIC	

Total Equipos Laboratorio Primeros y Segundos Cursos

Cantidad	Sistema Operativo	Procesador		Memoria RAM	Tarjeta de Red / (Acceso a la Red)	Ubicación
		Marca	Velocidad			
50	Microsoft Windows XP Professional	Intel Celeron	2.8 GHz	256 MB	Adaptador Fast Ethernet VIA PCI 10/100 mB / (No)	Laboratorio M-2 de Informática 3ros y 4tos Cursos
1	Microsoft Windows XP Professional	Xeon	3.06 GHz	256 MB	No tiene / (No)	

Total Equipos Laboratorio Terceros y Cuartos Cursos

Cantidad	Sistema Operativo	Procesador		Memoria RAM	Tarjeta de Red / (Acceso a la Red)	Ubicación
		Marca	Velocidad			
22	Microsoft Windows XP Professional	Intel Atom	1.6 GHz	1 GB	No tiene / (No)	Laboratorio M-1 5tos y 6tos Cursos
3	Microsoft Windows XP Colossus	Intel Atom	1.6 GHz	1 GB	Realtek RTL8139/810 x Family Fast Ethernet / Atheros AR5007G Wireless	

					Network Adapter / (Si)	
1	Microsoft Windows XP Professional	Pentium Dual Core	2.7 GHz	1 GB	No tiene / (No)	
2	Microsoft Windows XP Professional	Intel Atom	1.6 GHz	1 GB	Realtek RTL8168/811 PCI-E Gigabit Ethernet / Atheros AR50076 Wireless Network / (No)	
7	Microsoft Windows XP Professional	Pentium Dual Core	1.6 GHz	1 GB	No tiene / (No)	
1	Microsoft Windows XP Colossus	Intel Atom	2.8 GHz	2 GB	Realtek RTL8139/810 x Familily Fast Ethernet / Atheros AR5007G Wireless Network Adapter / (Si)	
4	Microsoft Windows XP Professional	Intel Celeron	2.5 GHz	512 MB	No tiene / (No)	
4	Microsoft Windows XP Professional	Intel Celeron	1.6 GHz	512 MB	No tiene / (No)	
1	Microsoft	Intel Celeron	2.5 GHz	512 MB	Adaptador	

	Windows XP Professional				Fast Ethernet PCI CNet Pro 200	
2	Microsoft Windows XP Professional	Pentium Dual Core	2.7 GHz	1 GB	No tiene / (No)	
1	Microsoft Windows XP Professional	Pentium Dual Core	2.7 GHz	1 GB	No tiene / (No)	
1	Microsoft Windows XP Colossus	Intel Atom	1.6 GHz	1 GB	No tiene / (No)	

Total Equipos Laboratorio Quintos y Sextos Cursos

Tabla 2.3 Características de los Equipos de la Institución

2.1.5.4. Equipos de impresión

La Institución cuenta con impresoras para el uso administrativo en las diferentes oficinas del área. Todas están conectadas directamente a una estación de trabajo a pesar de que algunas de ellas tienen funciones de red y no son aprovechadas lo que hace que sean ineficientes en términos de optimización. A continuación; en la Tabla 2.4 se presenta una lista de los equipos de impresión existentes.

Equipo	Marca	Soporte para conexión a la red	Cantidad
	HP Laser Jet 2600n	Si	1

	Samsung SCx-4300	No	5
	Samsung ML-2010	No	1
	Samsung ML-1740	No	1
	Samsung SCX-4216F	No	1
	Epson LX-810	No	2
	Epson LX-300	No	2
	Lexmark X364 dn	Si	1
	Canon MP 250	No	1

Tabla 2.4 Características de las impresoras de la Institución

El servicio de impresión puede ser optimizado de gran manera mediante la red de datos por medio de la cual una impresora puede ser compartida para el uso de la misma por varios usuarios, lo cual además de optimizar el tiempo de acceso a ellas representa un significativo ahorro de recursos.

2.1.6. DIRECCIONAMIENTO IP

Las direcciones IP son asignadas de forma dinámica utilizando una dirección clase A (10.20.8.0/24), como se mencionó anteriormente, otra falencia dentro de esta red es el hecho de que no se encuentra segmentada, es decir, no existen VLANs o subredes. Todos los usuarios se encuentran dentro de la misma red, lo cual es una falla tanto para el aspecto administrativo como de seguridad. En la tabla 2.5 se presenta la actual distribución de direcciones IP.

Direcciones IP asignadas		
Departamento	**Computador**	**Dirección IP**
Rectorado	Dra. Fanny Rodríguez	10.8.200.14
Vicerrectorado	Msc Miguel Lema	10.8.200.25
Secretarío Rectorado	Dr. Napoleón Pozo	10.8.200.27
Secretaría Vicerrector	Econ. Ana Marcillo	10.8.200.26
Secretaria 1	Lic verónica Espinosa	10.8.200.85
Secretaria 2	Lic. Susana Sanchez	10.8.200.19
Administrador de la Red	Ing. Francisco Erazo	10.8.200.10
Inspector	Dr. Mario Sarzosa	10.8.200.80
Departamento Médico	Dra. Teresa Carrillo	10.8.200.11
Colecturía	Lcdo Francisco Enalada	10.8.200.12
Biblioteca	Alt. Santiago Fiallos	10.8.200.13
Lab M3 1ros y 2dos		10.8.200.30….50
Lab M2 3ros y 4tos		10.8.200.50….60
Lab M1 5tos y 6tos		10.8.200.60….70
Lab de Inglés		10.8.200.100…150

Tabla 2.5 Direccionamiento IP actual

Todos los equipos del Colegio acceden al Internet por medio del router de la CNT con la dirección IP 10.8.200.3. Actualmente algunas direcciones IP son asignadas por el administrador de la red, sin embrago estas no tienen ningún orden específico o alguna diferenciación entre las áreas o lugares donde se encuentran los equipos, además que estas direcciones IP no se encuentran documentadas.

En la figura 2.2 se indica la configuración de las propiedades IPv4 para la conexión a Internet de una tarjeta de red.

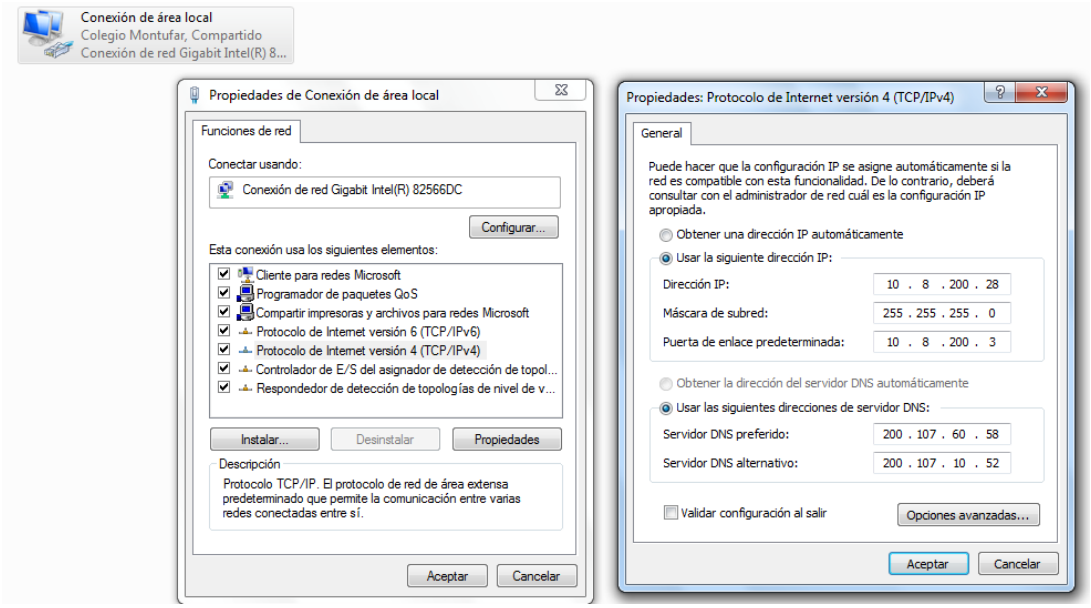


Figura 2.2 Configuración de las propiedades IPv4 para la conexión a Internet

2.2. SISTEMA DE CABLEADO ESTRUCTURADO ACTUAL

Actualmente el Colegio Experimental “Juan Pío Montufar” no goza de los estándares internacionales ANSI/TIA/EIA para el Sistema de Cableado Estructurado. Es un cableado de topología estrella jerárquica. La Institución cuenta con una Sala de Equipos que no brinda las comodidades necesarias para un buen funcionamiento, los equipos activos no poseen ninguna protección eléctrica, no hay una adecuada conexión a tierra, tampoco utiliza UPS. En base a lo expuesto se puede concluir que ninguna parte del sistema se encuentra apropiadamente certificada.

Se realizó una inspección visual de todas las instalaciones, aéreas de trabajo y laboratorios para conocer exactamente donde existe cableado estructurado y donde resulta primordial implementarlo, así como prever el lugar donde se pueden ubicar los Equipos y el Cuarto de Telecomunicaciones.

2.2.1. ÁREA DE TRABAJO

Se compone de todos los equipos, terminales, jacks que se conectan a la toma de información. Se analizó las estaciones de trabajo dentro de la intranet, las cuales se detallaron anteriormente indicando sus características técnicas. En el análisis de las estaciones se comprobó que todos los equipos eran computadores, y que no existían teléfonos IP, ni impresoras IP conectadas actualmente a la red.

Además se puede observar los terminales (Faceplates) en la biblioteca para conectar directamente los dispositivos al sistema.
En la figura 2.3 se indica un faceplate del Área Biblioteca de la Intitución.

Figura 2.3 Faceplate Biblioteca

2.2.2. CABLEADO HORIZONTAL

Comprende la conexión desde el cuarto de Telecomunicaciones hasta los faceplates. El cable viaja directamente a los faceplates utilizando cable UTP categoría 5e. En los laboratorios de informática los cables viajan por canaletas

hacia los faceplates para luego usar patch cords hacia los computadores como se observa en la figura 2.4

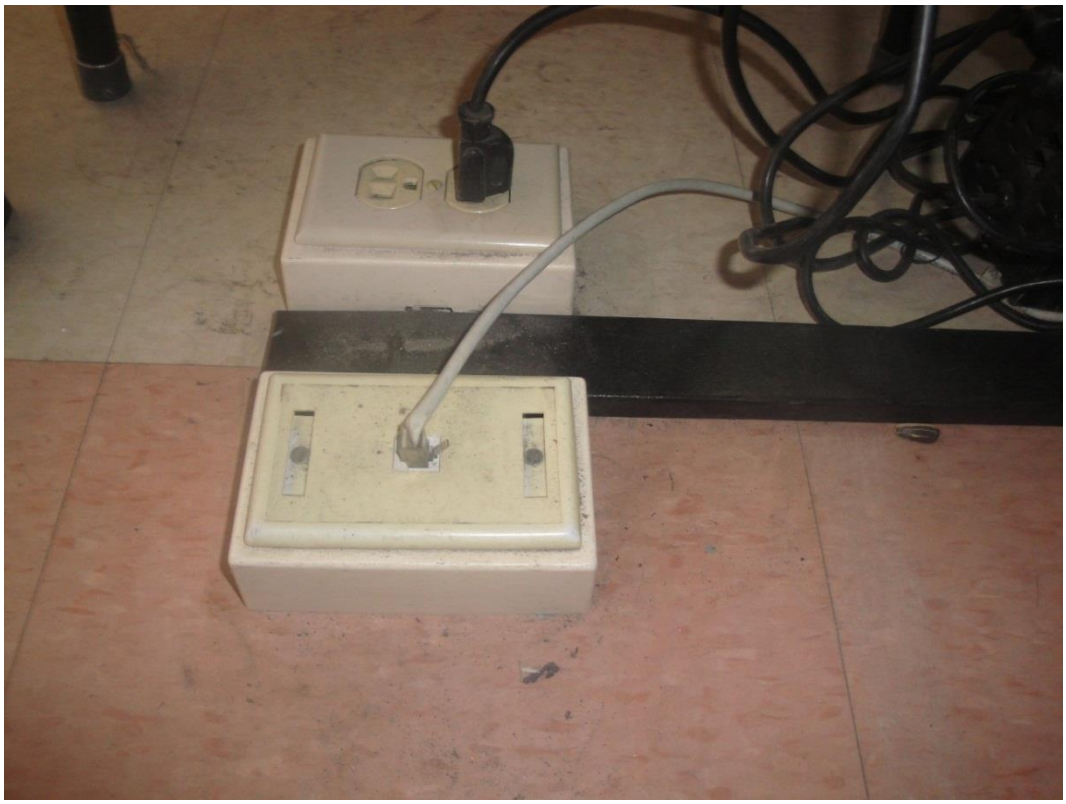


Figura 2.4 Cableado horizontal

Los equipos activos que se están utilizando se enumeran a continuación en la tabla 2.6 donde se indica los puertos disponibles y ocupados.

EQUIPOS ACTIVOS		
	Puertos Ocupados	**Puertos Disponibles**
Modem Huawei echolife hg520c de CNT	4	0
ZyXEL P-600 Series Model Number	1	0
D-Link DES-1024Rt 10/100 Fast Ethernet Switch	18	6

CNet Power Switch C517-1600	5	3
D-Link AirPlus Xtreme G Wireless Access Point DWL-2100Ap 192-200-200-253	1	0
LynkSys Wireless-G Access Point with SES	1	0
LINKSYS SR 224	16	8
D-Link DES-1024R+ 10/100 Fast Ethernet	16	8
D-Link DES-1016D 10/100 Fast Ethernet	10	6
D-Link DES-1016D 10/100 Fast Ethernet	10	6

Tabla 2.6 Disponibilidad de puertos de los equipos activos

De la tabla anterior se determina que los Switchs D-Link pueden ser reutilizados para el diseño de la red de área local, como switches de acceso, ya que sus especificaciones indican que no son administrables y servirán para conectar a los usuarios finales.

2.2.3. CABLEADO VERTICAL

El cableado vertical no cumple con el estándar ANSI/TIA/EIA 568 B.2 para conectar el backbone de la red, este subsistema tiene una interconexión en estrella, se toma como referencia que la altura del bloque es de 15 metros, puesto que en la planta baja se encuentran dos switches. Únicamente este subsistema se conecta a los equipo de comunicación mediante un cable UTP categoría 5e de cuatro pares. La distancia entre los equipos activos desde el primer piso hasta el cuarto de telecomunicaciones en la biblioteca es de aproximadamente 20 metros.

2.2.4. CUARTO DE TELECOMUNICACIONES, SALA DE EQUIPOS Y ACOMETIDA

El cuarto de telecomunicaciones se ubica en el primer piso, dentro de la secretaria sin embargo existen otros Cuartos de Telecomunicaciones en la planta baja, en los laboratorios de informática de: 3ros y 4tos cursos el cual alberga tres switches D-LINK y en 5tos y 6tos el cual alberga dos switches D-Link, en el laboratorio de inglés el cual alberga tres switches D-LINK. Los dos Cuartos de Telecomunicaciones tienen un área aproximada de 15 metros cuadrados. Solamente existe una persona autorizada para la administración del mismo. Esta instalación no cumple con la norma ANSI/TIA/EIA 569 para un Cuarto de Telecomunicaciones.

En el Cuarto de Telecomunicaciones de la Biblioteca existe un patch panel de 24 puertos que se ubica en un bastidor el cual se utiliza principalmente para alojar a los switches D-LINK. Ninguno de los equipos de networking está conectado a un equipo UPS (Uninterruptible Power Supply), todos ellos se conectan directamente a la red pública de energía por lo que sí existe una descarga eléctrica podrían dañarse. Adicionalmente el cuarto utilizado no posee un adecuado sistema de aire acondicionado que brinde el nivel de humedad adecuado y que evite cualquier problema de calentamiento. Como también no posee una conexión de puesta a tierra.

La acometida o entrada de servicios hacia la Institución no se encuentra especificada. Los servicios llegan a través de cables sueltos según el proveedor de servicios ha supuesto conveniente el momento de la instalación.

2.2.5. REQUERIMIENTOS DE PUESTA A TIERRA

El sistema de conexión a tierra para el diseño del cableado estructurado es fundamental para proteger la vida útil de los equipos así como para preservar la vida del personal que manipula el mismo. La mayoría de casos de daños a los equipos se debe a variaciones de voltaje debido a malas conexiones de puesta a tierra o en su defecto defectuosas conexiones.

Por este motivo un sistema de puesta a tierra es fundamental para la infraestructura del Colegio y el cuarto de Telecomunicaciones debe necesariamente contar con una Barra de tierra principal de telecomunicaciones (TMGB) como lo indica la norma de cableado estructurado correspondiente a los sistemas de puesta a tierra. Actualmente no existe el sistema de puesta a tierra en el Colegio.

2.2.6. CANALIZACIONES

Las canaletas que se emplean en el cableado del Colegio son de plástico PVC lisas normales de una vía de 60 mm x 40 mm (base x alto), se debe acotar que no están instaladas cajas ni terminaciones.

Para todo el Colegio se tiene una independencia entre el cableado eléctrico y los espacios que ofrecen el cableado estructurado, lo cual disminuyen interferencias eléctricas.

No se utiliza techo falso en ninguna de las instalaciones de Rectorado, Vicerrectorado, Secretarias, Contabilidad, Laboratorios. El cableado únicamente viaja a través de la loza o a su vez está direccionado por las paredes laterales de

los edificios y llega directamente a un switch o a un computador según sea el caso.

2.2.7. RESUMEN DE LOS PUNTOS DE CABLEADO DE LA INSTITUCIÓN

Como se indicó anteriormente, en el Colegio la conexión actual de la red no cumple con las normas de Cableado Estructurado, una de las razones es que las salidas de telecomunicaciones en las áreas de trabajo no se encuentran debidamente terminadas en faceplates, debido a que el sistema de cableado no se encuentra certificado, el servicio llega a las estaciones simplemente a través de cables directamente conectados a los switch.

Como se explica más adelante, en el literal 2.3 los usuarios potenciales de la red superan ampliamente al número total de puntos actuales en servicio, además que a excepción de Inspección General y los laboratorios de informática, todos los demás se encuentran en el edificio administrativo, esto implica que las demás áreas del colegio tiene acceso ilimitado a la red en la Institución por lo que resulta imperiosa la necesidad de la implementación de la red de datos.

2.3. USUARIOS DE LA RED

Los usuarios de la red se ha considerado conveniente dividirlos por grupos para una fácil clasificación de los mismos. Los grupos considerados en este análisis son los siguientes:

- Administrativos
- Profesores
- Estudiantes
- Periféricos

2.3.1. USUARIOS ADMINISTRATIVOS

En el sector administrativo cuenta con 31 personas entre los que se encuentran los siguientes usuarios:

- Autoridades
- Secretarias y Personal Contable
- Personal de Bodega y biblioteca
- Inspecciones

Las autoridades y secretarias se encuentran en su mayoría trabajando en el área administrativa, en este sector a cada usuario se le asigna una computadora, sin embargo cabe resaltar que no todos los usuarios tienen acceso a la red. Por lo que resulta indispensable que todos ellos puedan tener acceso a la Intranet como a Internet.

Los usuarios que poseen acceso a Internet no poseen restricciones de uso para la red lo cual es una falla grave respecto de la seguridad. De los mencionados dentro de usuarios administrativos existen algunos que tiene acceso a la red y otros que no debido a que se encuentran distribuidos en diferentes sitios del campus por lo que no poseen puntos de red razón por la cual no acceden a la misma.

2.3.2. ESTUDIANTES

Los estudiantes se encuentran divididos en los siguientes grupos:

- Sección Diurna
    - Ciclo Básico (Vespertino)
    - Ciclo Diversificado (Diurno)
- Sección Nocturna

Casi la totalidad de los estudiantes que accede a la red lo hace por medio de las computadoras ubicadas en la sala de Internet que tienen instaladas el sistema operativo (Windows XP). El número de computadores ubicados para este fin es de 8. En la tabla 2.7 se muestra el número de estudiantes del Colegio que vendrían a ser potenciales usuarios de la red.

Sección Diurna		Sección Nocturna	TOTAL
Ciclo Básico	Ciclo Diversificado		
1392	1283	714	3389

Tabla 2.7 Número de estudiantes totales del Colegio Nacional Experimental "Juan Pío Montufar" Fuente: Secretaría

Los estudiantes no acceden completamente a los servicios dentro de la Institución, el uso de Internet en la sala es limitado en comparación al número de estudiantes. El acceso a ciertas aplicaciones y páginas web se encuentra restringido por el administrador. Esta realidad es la que se intenta cambiar y masificar el uso de la red e Internet para todos los usuarios de la Institución.

2.3.3. PROFESORES

El colegio cuenta con 106 profesores no poseen puntos de red exclusivos, sin embargo acceden a la red desde la Sala de Internet en la Biblioteca y los laboratorios que poseen acceso a la red que se conectan por medio de conexión cableada. Además cabe resaltar que el uso de los profesores de la red es mayormente para el registro de calificaciones mensuales a través de un sistema instalado en el servidor Windows server 2008 ubicado en secretaría y conectado a Internet a través de una dirección pública, y casi todos lo realizan desde la Sala de Internet de la Biblioteca. El acceso de los profesores a los recursos es indispensable para poderles dar herramientas adecuadas para realizar su labor educativa.

Finalmente como periféricos se toma en cuenta las impresoras para el uso administrativo en cada una de las oficinas. No existe ninguna impresora compartida todas están directamente conectadas a la computadora. No existe ningún otro tipo de periféricos conectados a la red del Colegio. El uso de estos dispositivos a través de la red significaría el aprovechamiento de recursos y la inclusión de otros servicios como almacenamiento compartido, video seguridad entre otros.

2.3.4. RESUMEN DE LOS USUARIOS POTENCIALES DE LA RED

Se presenta en la tabla 2.8 un resumen con los usuarios potenciales de la red y el grupo al que pertenecen, es decir todos aquellos que hipotéticamente harían uso de la red de datos del Colegio, para indicar la relación entre los usuarios actuales.

ADMINIISTRATIVOS	PROFESORES	ESTUDIANTES	TOTAL
31	106	3389	3526

Tabla 2.8 Número de usuarios potenciales de la red

2.4. ANÁLISIS DE TRÁFICO Y ANCHO DE BANDA GENERADO POR LAS APLICACIONES

A fin de realizar un completo análisis de la situación actual de la red resulta conveniente el tener una visión del tráfico actual que generan las aplicaciones instaladas, así como las que podrían causar tráfico en la implementación futura de la red de datos multiservicios. Estas harán uso de la red para sus actualizaciones así como para el uso compartido mediante un servidor de aplicaciones.

2.4.1. ANÁLISIS DE LAS APLICACIONES INSTALADAS EN LOS EQUIPOS DE LA RED

Dentro del análisis de la situación actual de la red es conveniente realizar un reconocimiento de las aplicaciones que están utilizando en las estaciones de

trabajo y en el servidor. En base a esta recopilación se puede determinar cuál es la vida útil de las computadoras y sus componentes para un adecuado funcionamiento de las aplicaciones utilizadas.

Las aplicaciones de software, con las que se trabaja en el Colegio, cuentan con su respectiva licencia y es responsabilidad únicamente de la persona encargada de la administración de la red de la instalación de las mismas. Todas las estaciones de trabajo se encuentran funcionando bajo la plataforma de Windows. En la tabla 2.9 se muestra un resumen de las aplicaciones encontradas en los equipos del Colegio.

	Descripción	**Fabricante**	**Observaciones**
Mozila Firefox	Navegar web	Mozilla	
Microsoft Internet Explorer	Navegar web	Microsoft	
Avira Antivir Personal	Antivirus	GMBH	
Windows Live Messenger	Mensajería Instantánea	Microsoft	
Acrobat Reader 5.0 X	Visualización de archivos PDF	Adobe	
Adobe Flash Player	Reproducción Multimedia	Adobe	
J2SE Runtime Enviroment 5.0 Update 6	Desarrollo de software y acces a aplicaciones Java	Sun Microsystems	

WinRar	Software de compresión de datos	RAR Lab	
Microsoft Office Professional 2007	Suite de oficina (Word, Excel, PowerPoint)		
Inglés Your Way 2.0	Curso de Inglés		Instalado en los laboratorios de Inglés
Wireshark	Herraminta de Monitoreo de Tráfico de red		Instalado para la medición de tráfico en este proyecto.
Colasoft Capsa	Analizador de Red		Instalado para la medición de tráfico en este proyecto.

Tabla 2.9 Aplicaciones instaladas en las estaciones de trabajo

2.4.2. ESTUDIO DE TRÁFICO UTILIZADO EN LA RED

Posteriormente se ha realizado el estudio de tráfico utilizado por la red en el enlace al ISP, a fin de determinar qué tan aprovechada está la capacidad de dicho enlace en función de las aplicaciones que son requeridas por el colegio para el desarrollo de sus actividades. Para esto se utilizó Wireshark, Colasoft Capsa, Ntop, IP Scanner.

En el Colegio se utiliza una dirección de red clase A 10.8.200.0 con máscara 255.255.255.0, asignando mediante un servidor DHCP del router para asignar dinámicamente a las estaciones de trabajo conectadas a la red.

Para determinar el tráfico y las vulnerabilidades de la red se utilizó algunas herramientas como: Colasoft capsa, Wireshark, Ntop e IP Scanner obteniendo los siguientes resultados.

2.4.3. Utilizando Wireshark

En la figura 2.5 se indica el tráfico capturado con Wireshark.

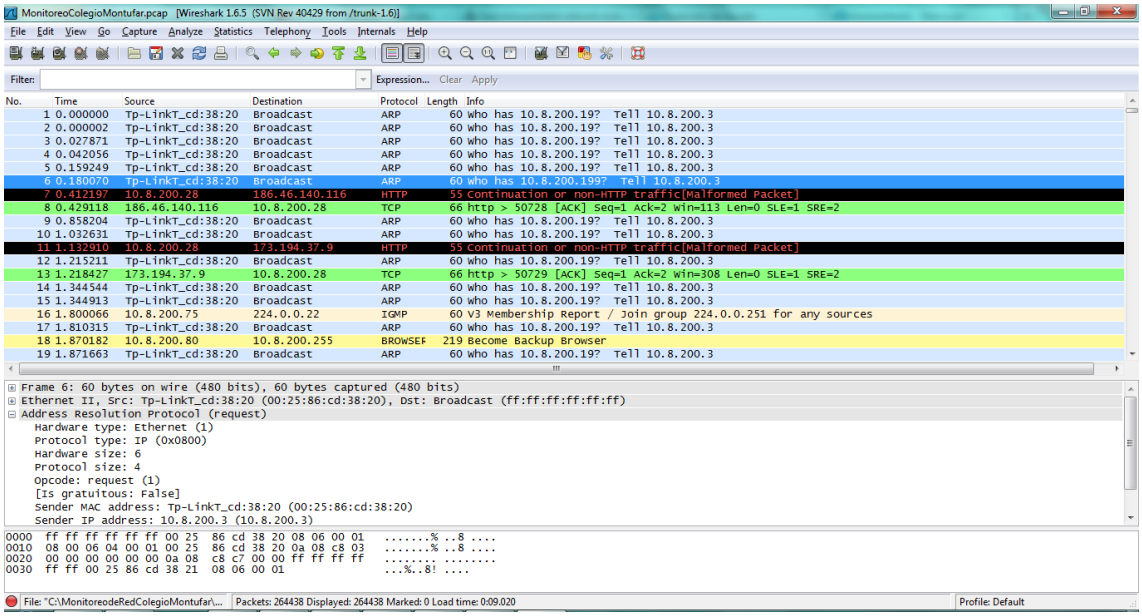


Figura 2.5 Tráfico capturado con Wireshark

Para este propósito se conectó una computadora al switch 3 Linksys SR224 de la biblioteca que a su vez está conectado al switch de core.

Las mediciones se realizaron en época de exámenes desde la 08:00 H hasta las 14:00 H, porque en este tiempo se tiene concurrencia de tráfico.

La medición se realizó durante dos semanas, teniendo como resultado los datos de la figura 2.6

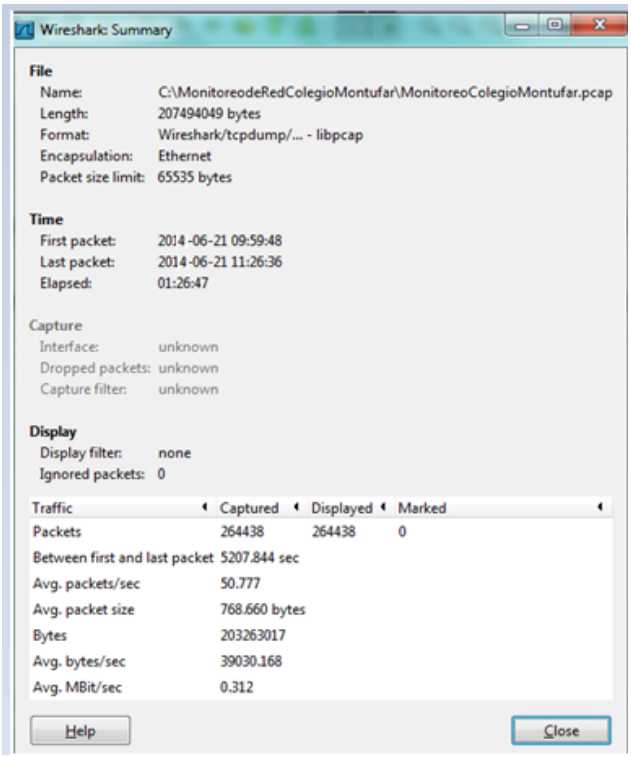


Figura 2.6 Tráfico de la red – wireshark

Con estos valores obtenidos se puede calcular el valor pico

$$\text{Capacidad} = \frac{\#\,de\ bits}{tiempo\ de\ transmisión} \quad \text{Ec 2.4.3.1}$$

$$\text{Capacidad} = \frac{\#depaquetesxtamaño(paquete)x8}{tiempo\ de\ transmisión}$$

$$\text{Capacidad} = \frac{264438(768.660)8}{5207.844}$$

$$\text{Capacidad} = 312.24\ \text{Kbps}$$

En la tabla 2.10 se indica el Tráfico capturado con Wireshark

	LUNES	MARTES	MIÈRCOLES	JUEVES	VIERNES
Capacidad (Kbps)	299.342	308.90	312.24	298.437	300.583

Tabla 2.10 Tráfico capturado con Wireshark

En la figura 2.7 se indica la Capacidad del Canal.

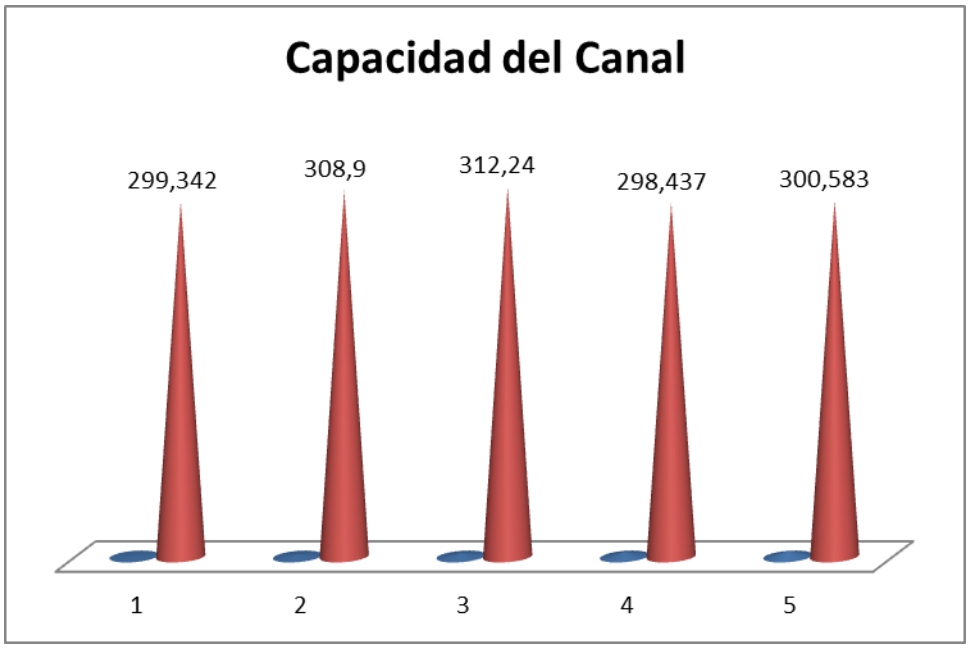


Figura 2.7 Capacidad del Canal

2.4.4. UTILIZANDO LA HERRAMIENTA COLASOFT CAPSA

Se ha monitorizado y analizado todo el tráfico que circula por una red local capturando sus paquetes TCP/IP en tiempo real.

Para conocer protocolos, tramas y estimar el tráfico que transmiten y reciben los hosts del Colegio Experimental “Juan Pío Montufar”, se utilizó el programa Colasoft Capsa 7 Free. Este programa es un poderoso sniffer que monitorea y analiza todo el tráfico que circula por una red local capturando sus paquetes TCP/IP en tiempo real, a continuación se muestran las imágenes del resultado del análisis con el snnifer.

En la figura 2.8 se indica el Tráfico Total- Colasoft Capsa.

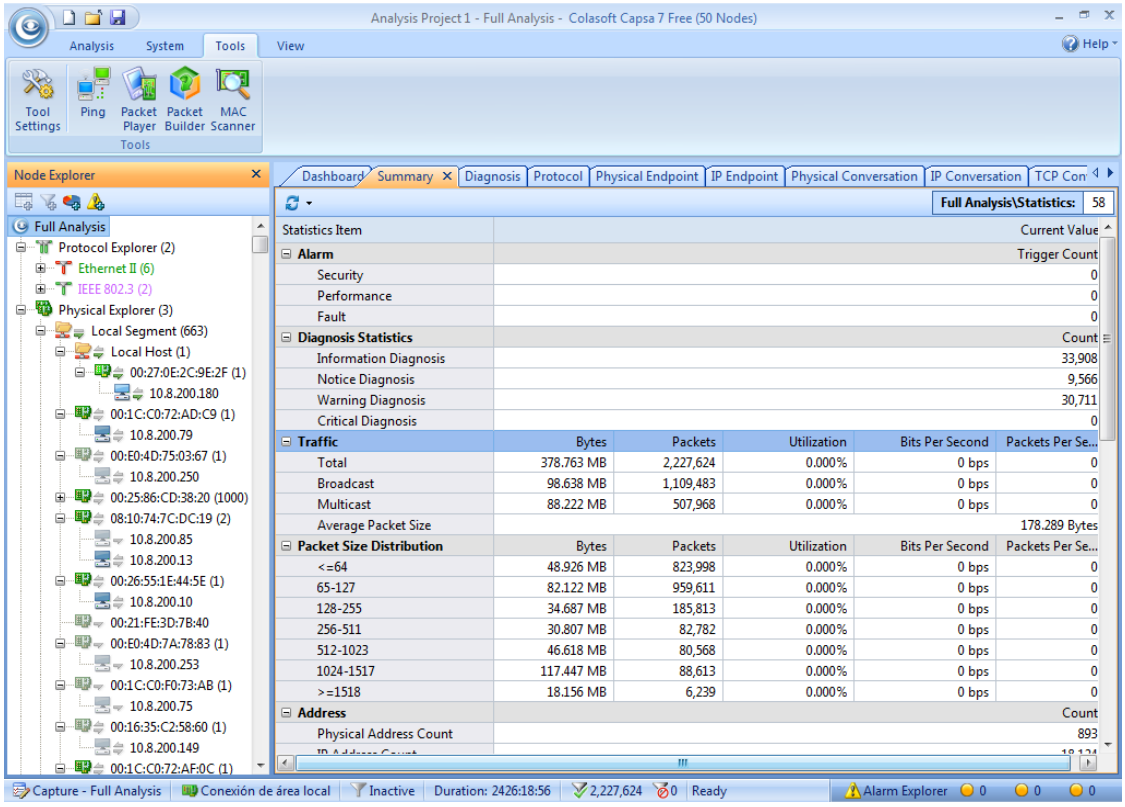


Figura 2.8 Tráfico Total – Colasoft Capsa

En la figura 2.9 se indica Tráfico por tamaño de Paquete.

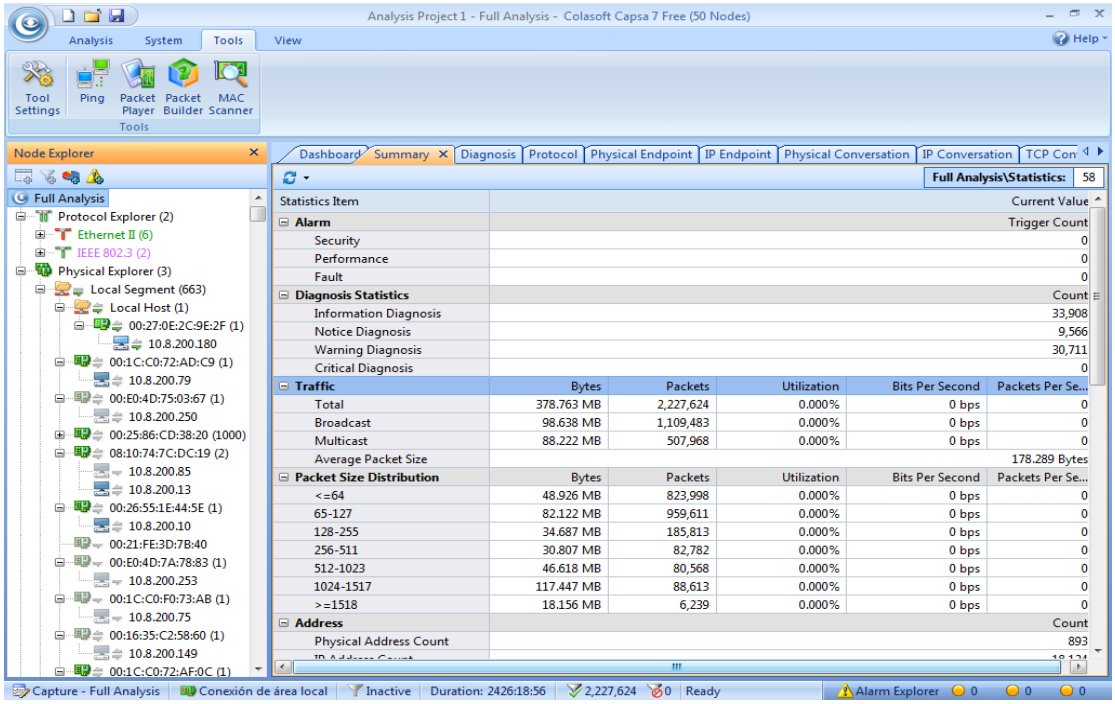


Figura 2.9 Tráfico por tamaño de Paquete

En la figura 2.10 se indica el Tráfico por Protocolo.

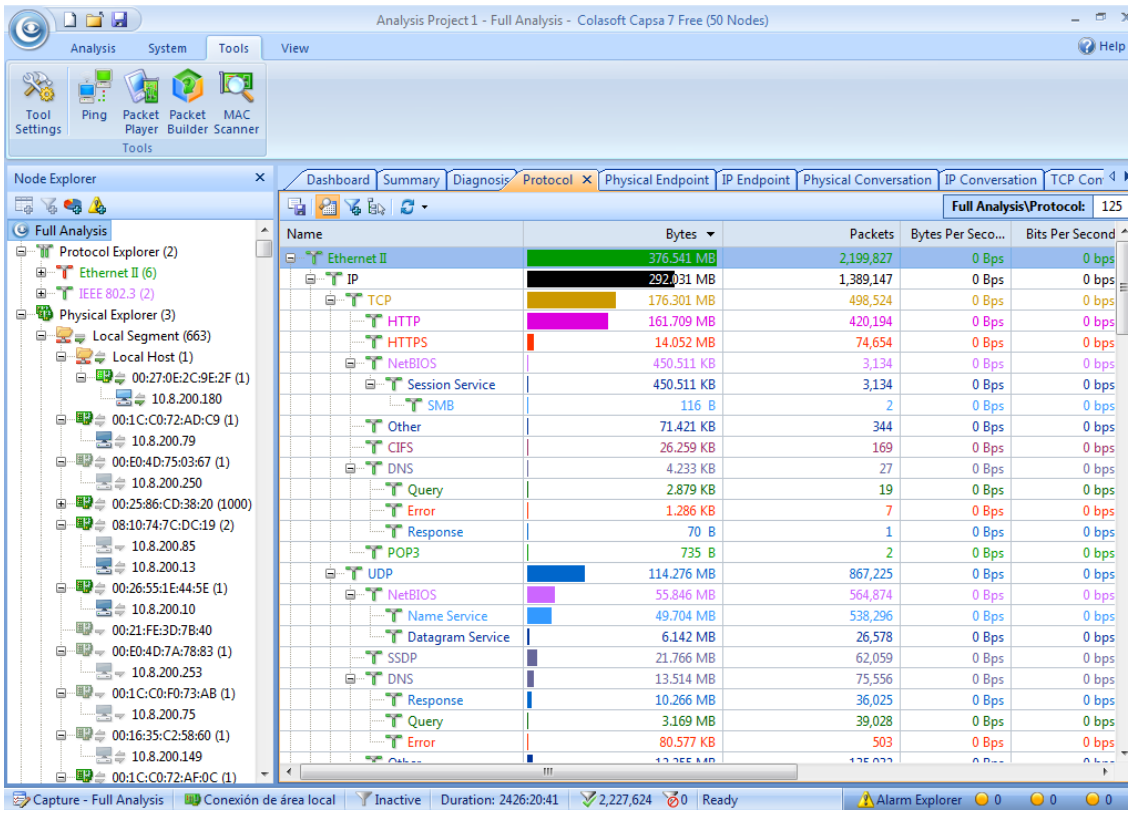


Figura 2.10 Tráfico por Protocolo

En la figura 2.7, 2.8, 2.9 se puede apreciar el tráfico total, el tamaño de los packetes TCP y los protocolos IP más utilizados en la red, junto con la cantidad de bytes transmitidos por cada uno de ellos.

En la tabla 2.11 se indica los Protocolos más utilizados en la Red.

Protocolo	Tamaño (Bytes)
TCP ---- HTTP	161.709 MBytes
TCP ---- HTTPS	14.052 MBytes
TCP ---- NetBios	450.511 KBytes
IP ---- UDP	114.276 MBytes

Tabla 2.11 Protocolos más utilizados en la Red

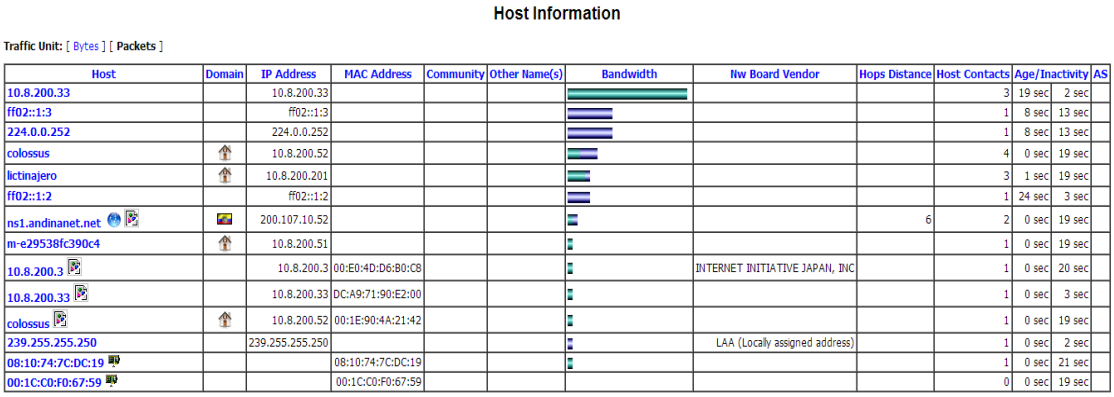
Como se muestra en la Figura 2.7 el número total de packtes capturados es de 2’227 624 y un total de tráfico de 378763 MBytes.

En la figura 2.9 se puede apreciar que el protocolo más usado es:
TCP ---- HTTP con 161709 MBytes.
En el Anexo A se muestran más pantallas del snnifer Colasoft Capsa 7.0 Free, similares a las de las dos figuras anteriores con más especificaciones.

2.4.5. UTILIZANDO LA HERRAMIENTA NTOP

Se obtuvo los siguientes valores de tráfico y el número de estaciones de trabajo conectadas con su respectivo tráfico generado.

En la figura 2.11 se indica el Tráfico- Ntop.



Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Community	Other Name(s)	Bandwidth	Nw Board Vendor	Hops Distance	Host Contacts	Age/Inactivity	AS
10.8.200.33		10.8.200.33							3	19 sec	2 sec	
ff02::1:3		ff02::1:3							1	8 sec	13 sec	
224.0.0.252		224.0.0.252							1	8 sec	13 sec	
colossus		10.8.200.52							4	0 sec	19 sec	
lictinajero		10.8.200.201							3	1 sec	19 sec	
ff02::1:2		ff02::1:2							1	24 sec	3 sec	
ns1.andinanet.net		200.107.10.52						6	2	0 sec	19 sec	
m-e29538fc390c4		10.8.200.51							1	0 sec	19 sec	
10.8.200.3		10.8.200.3	00:E0:4D:D6:B0:C8				INTERNET INITIATIVE JAPAN, INC		1	0 sec	20 sec	
10.8.200.33		10.8.200.33	DC:A9:71:90:E2:00						1	0 sec	3 sec	
colossus		10.8.200.52	00:1E:90:4A:21:42						1	0 sec	19 sec	
239.255.255.250		239.255.255.250					LAA (Locally assigned address)		1	0 sec	2 sec	
08:10:74:7C:DC:19			08:10:74:7C:DC:19						1	0 sec	21 sec	
00:1C:C0:F0:67:59			00:1C:C0:F0:67:59						0	0 sec	19 sec	

Figura 2.11 Tráfico – Ntop

De acuerdo a la figura 2.11 se tiene un bajo tráfico, debido a que no se tiene servicios locales en la red. Se tiene un mayor tráfico a la hora en que los estudiantes tienen computación en los laboratorios de informática.

2.4.5.1. Tráfico IP

En la tabla 2.12 se detalla el tráfico IP que se ha capturado con la herramienta NTOP. Se visualiza el tráfico generado por cada estación de trabajo que está conectada a la red LAN. Se observa la cantidad de datos que se transmiten con su respectivo porcentaje.

En la tabla 2.12 se indica el Tráfico IP- Ntop

Hosts	Datos	
colossus	4.6 KBytes	18.1 %
10.8.200.33	4.2 KBytes	16.8 %
ff02::1:2	2.3 KBytes	9.3 %
ff02::1:3	2.0 KBytes	8.0 %
workgroup	1.7 KBytes	6.8 %
ns1.andinanet.net	1.7 KBytes	6.7 %
10.8.200.33	1.6 KBytes	6.4 %
239.255.255.250	1.1 KBytes	4.5 %
secretaria2	1.0 KBytes	4.1 %
10.8.200.15	901	3.5 %
pc4495-024	652	2.5 %
secrec	634	2.5 %
lictinajero	616	2.4 %
inspgen	427	1.7 %
08:10:74:7C:DC:19	414	1.6 %
10.8.200.3	322	1.3 %
m-e29538fc390c4	258	1.0 %
colossus	168	0.7 %
10.8.200.250	92	0.4 %
10.8.200.3	60	0.2 %
224.0.0.251	60	0.2 %
all-systems.mcast.net	60	0.2 %
239.255.255.253	60	0.2 %
serv-jpm	60	0.2 %
secrec	46	0.2 %
m-e29538fc390c4	46	0.2 %
inspgen	46	0.2 %
10.8.200.33	46	0.2 %

Tabla 2.12 Tráfico IP – Ntop.

2.4.6. UTILIZANDO LA HERRAMIENTA IPSCANNER

Esta herramienta fue utilizada para descubrir las estaciones de trabajo que están conectadas y los puertos que tienen habilitados y deshabilitados, en la figura 2.12 se detalla un ejemplo de lo que se encontró al realizar un escaneo. Esta información se encuentra en el ANEXO B

En la figura 2.12 se indica los Hosts Escaneados.

Status	Name	IP	NetBIOS name	NetBIOS group	MAC address	User	Comments
Dead	SECREC	10.8.200.19			00:1C:C0:72:7B:45		
Dead	VICERRECTOR-PC	10.8.200.25			00:1C:C0:74:DC:C7		
Dead	SVICER	10.8.200.26			00:0B:6A:A6:62:A0		
Dead	RECTORADO-PC	10.8.200.14			00:1C:C0:F0:73:B4		
Dead	PC4495-017	10.8.200.50			00:18:E7:56:CC:17		
Dead	10.8.200.55	10.8.200.55			00:1E:90:4A:DB:10		
Dead	Marlon-PC	10.8.200.93			00:16:76:CE:F9:46		
Dead	PC4495-024	10.8.200.126			00:1E:90:4A:E0:F5		
Dead	LICPATRICIO	10.8.200.202			00:16:76:A4:2E:25		
Dead	10.8.200.210	10.8.200.210			00:16:76:A4:2C:C0		
Dead	10.8.200.211	10.8.200.211			00:18:E7:56:CB:FD		
Dead	10.8.200.212	10.8.200.212			94:00:70:62:25:BD		
Dead	10.8.200.214	10.8.200.214			00:23:76:0D:AB:AB		
Dead	10.8.200.213	10.8.200.213			14:36:05:8C:9B:1F		
Dead	10.8.200.217	10.8.200.217			30:17:C8:3F:AC:22		
Dead	Teacher-PC	10.8.200.225			00:18:E7:56:CB:FE		
Dead	COLOSSUS	10.8.200.226			00:30:67:A3:D7:B7		
Dead	10.8.200.230	10.8.200.230			9C:4A:7B:6E:8C:02		
Dead	10.8.200.240	10.8.200.240			00:BE:13:0C:E3:95		
Dead	PANKUADOR-PC	10.8.200.235			00:1D:E0:9A:59:21		
Dead	10.8.200.249	10.8.200.249			28:D1:AF:16:A7:34		
Alive	MONTUFARSEC-PC	10.8.200.28	MONTUFARSEC-PC	WORKGROUP	00:1C:C0:72:7B:33	MONTUFAR SEC	

Figura 2.12 Hosts Escaneados

Al realizar el escaneo de las estaciones de trabajo conectadas a la red, se ingreso como parámetro la dirección de red 10.8.200.0/24 hasta la 10.8.200.254/24 buscando cada una de las direcciones dentro de esta red, debido a que todas las PC están conectadas se tiene el resultado de “Alive” y en donde se encuentra respuesta son todas las conectadas a la red.

2.5.3. ANÁLISIS DE SEGURIDAD EN LA RED LAN Y WLAN

Al realizar el análisis de seguridad que se tiene en la red, se encontró las siguientes vulnerabilidades:

- No existe VLAN, por lo que los estudiantes pueden ver los archivos que están compartidos por el personal administrativo y docente.

- El administrador de la red usa el software deep freeze en todas la estaciones de trabajo para proteger las máquinas ya que al momento de instalar cualquier programa si se reinicia la máquina esta se restaura inmediatamente.
- El router tiene habilitado DHCP para la red WLAN ya que no es recomendable por seguridad.
- En caso de existir un ataque al router la red se quedaría sin funcionamiento ya que es el encargado del direccionamiento dinámico.
- No se tiene un antivirus centralizado para que actualice a las estaciones de trabajo de forma continua para brindar mayor seguridad.
- No se tiene un servidor proxy para restringir el acceso a sitios no deseados.
- Para el acceso inalámbrico se requiere de una contraseña, el adquirir dicha contraseña se puede ingresar con todos los privilegios, esto es un riesgo para la seguridad de la red LAN.
- Los puertos de los switchs que no están utilizados, están habilitados por lo que cualquier usuario puede conectarse y tener acceso a la red.
- No cuentan con un sistema de gestión de red para realizar un monitoreo continuo de la red.
- Para configurar el router se ingresa mediante la dirección IP 10.8.200.3 dentro de la interfaz web se solicita usuario y contraseña de administrador.
- Los usuarios ingresan como administradores lo cual es un riesgo para la seguridad interna.

2.4.3. ANÁLISIS DEL ANCHO DE BANDA

Para la salida a Internet el Colegio cuenta con dos planes compartidos, el primero es un plan gubernamental gratuito provisto por la CNT de 2 Mbps tipo ADSL (Línea de Subscriptor Digital Asimétrica) y el otro es un plan provisto por SURATEL de 2 Mbps con un dirección IP 186.66.129.218 con máscara de red 255.255.255.248, Gateway 186.66.129.217 y los DNSs 200.63.212.110, 200.25.144.1

El hecho de que el enlace sea asimétrico, significa que se tiene diferente ancho de banda en el canal hacia y desde el Internet, siendo la velocidad de dowstream (bajada) mayor que la velocidad de upstream (subida).

2.5. ANÁLISIS DE SERVICIOS

El Colegio Experimental “Juan Pío Montufar” posee un servidor, utilizado como servidor de notas en línea.

2.5.1. SERVICIOS DE RED REQUERIDOS

En una infraestructura de comunicaciones es imprescindible contar con los servicios de intranet para los usuarios de las diferentes Áreas. El Colegio Experimental “Juan Pío Montúfar” requiere de servicios de Intranet e Internet para satisfacer las necesidades de los usuarios. A continuación se hace referencia a los servicios requeridos por los usuarios de acuerdo a las necesidades propias de una entidad educativa.

2.5.1.1. Servicios web

Dentro de los recursos del Colegio se detalla que tiene un Servidor Web que se utiliza para el ingreso y consulta de notas por parte de los profesores y estudiantes respectivamente. Es por eso que El Colegio Experimental “Juan Pío Montúfar” tiene la disposición de tener su propio sitio WEB para publicar la información relevante como congresos, autoridades, cronograma de actividades para inscripciones y matrículas, etc. Además el sitio Web servirá para educación virtual, e-learning, para que estudiantes, profesores o las diferentes áreas del Colegio diseñe su propio blog para informar a sus alumnos de los horarios de prácticas en los laboratorios, pruebas teóricas y prácticas, y enlaces educativos a diversas dependencias.

2.5.1.2. Servicios de nombre de dominio (DNS)

Actualmente en la red del Colegio Experimental “Juan Pío Montufar” no existe una gran cantidad de computadores, servidores y periféricos por lo que un servidor DNS (Domain Name System) local no fue estimado. Pero para facilitar referirse a los dispositivos y otros periféricos se considera el dimensionamiento de un servidor DNS local para resolver nombres de servicios internos, así como para la administración de las computadoras. Se toma en cuenta este servicio ya que el direccionamiento es estático y que para los usuarios es más sencillo aprender un nombre que una dirección IP. El servidor local ayudará a resolver inconvenientes con las aplicaciones que se manejen en la Intranet. El dominio del Colegio será @juanpiomontufar.edu.ec

2.5.1.3. Servicio de correo electrónico

El correo electrónico es una herramienta imprescindible tanto para el trabajo como para la comunicación más aún en una Institución como esta que trabaja con gran número de estudiantes, profesores y personal administrativo. Por lo cual se requiere disponer de una herramienta flexible, y accesible desde cualquier lugar que se encuentre. Este servicio proporcionará la creación de cuentas para los profesores y personal administrativo así como su adecuado seguimiento a las colas de correo, aumentar la capacidad de la cuenta del usuario, resetear los password de las cuentas personales.

Para esto se configurara una plataforma de mensajería electrónica, usando la version open source de zimbra.

2.5.1.4. Servicio de archivos compartidos

Es necesario un servidor donde se pueda compartir información entre los diferentes miembros del Colegio (profesores, alumnos y empleados) y asegurar que la información esté disponible. El servicio mantendrá los archivos en un lugar específico, todos los documentos como formularios, normativas, notificaciones,

formato de prácticas, de solicitudes de inscripciones etc, para que los usuarios los descarguen o realicen una copia de seguridad.

2.5.1.5. Servicio de impresión

Existe una gran cantidad de impresoras conectadas a cada una de las máquinas en las diferentes áreas lo cual genera un gasto innecesario. Se dispondrá de un servicio de impresión con capacidad de almacenamiento que gestionará los archivos en las colas para ser impresos. Así se logrará asignar una impresora a un grupo de usuarios que la podrán utilizar optimizando el uso de recursos.

2.5.1.6. Servicio de antivirus

Las aplicaciones que los usuarios manejarán para acceder a recursos hacia el Internet o la Intranet deberán ser escaneados por un servidor de antivirus. Así toda la información sea texto o multimedia no se verá afectada a posibles ataques maliciosos que perjudiquen las comunicaciones y los demás servicios a ser implementados.

2.6. RED DE VOZ ACTUAL

En la topología de la red de voz, se identificó que el sistema telefónico no cuenta con ninguna central telefónica, tienen contratado ocho líneas telefónicas independientes para todo el Colegio.

2.6.1. DETALLE DE USUARIOS ACTUALES

Actualmente se encuentran conectadas en total 8 líneas telefónicas directas para servicios internos del Colegio, las cuales se encuentran distribuidas a través del campus de forma dispersa, conectadas hacia la red telefónica pública por medio de la Corporación Nacional de Telecomunicaciones.

La distribución del número de teléfonos por departamento del campus se detalla en la Tabla 2.13.

Número	Departamento	Personal	Teléfono. Directo	Cargo
1	Rectorado	Dra. Fanny Rodriguez	3131-380	Rectora
2	Vicerrectorado	Msc Miguel Lema Econ. Ana Marcillo	3131-721	Vicerrector Asistente y 1ROS
3	Inspección General	Dr. Mario Sarzosa Lcda. Cecilia Rivadeneira	3130-303	Inspector General Asistente y 3ROS
4	Subispección	Lcdo Carlos Ruano	3130-135	Subispector
5	Secretaria	Lic. Susana Sanchez Lic. Verónica Espinoza Sra. Magaly Vizcarra Alt. Santiago Fiallos	Telefax 3131-262	Asistente Rectorado y 4TOS Asistente y 5TOS Asistente y 2DOS Sistemas y 6TOS
6	Colecturía	Lcdo. Francisco	3131-399	Colector E

		Encalada Lic. María Oña Lcdo Ramiro Monje Alt. Santiago Fiallos		Contadora Guarda almacen Sistemas y 6TOS
7	Dep. Médico Dental	Dra. Teresa Carrillo Dra. Rubi Rivadeneira Lcda. Rosario Reina Dr. Tito Rendon Dra. Rosario Sanchez Dr. Julio Ortiz Sra. Mercedes Torres	3130-295	Médico Diurno Médico Diurno Enfermera Médico Noc. Odontóloga Odontólogo y Noc. Auxiliar
8	Departamento de Orientación	Dr. Wilson Gavilanes	3131-646	Director y Sociólogo

	y Bienestar Estudiantil DOBE	Dr. Vicente Cazco		5TOS Sicólogo 1ROS
		Lcdo. Patricio Jimenez		Sicólogo 2ROS
		Lcdo. Lenin Moreno		Sicólogo 3ROS
		Msc. Luis Campoverde		Sicólogo 4ROS
		Lcda. María Santana		Sicólogo 6ROS
		Lcda. Magdalena Aguirre		Trabajo Social D
		Lcda. Patricia Castillo		Trabajo Social B

Tabla 2.13 Teléfonos del Colegio Experimental "Juan Pío Montúfar"

2.7. RESUMEN DEL DIÁGNOSTICO DE LA RED

A lo largo de este capítulo se ha analizado el estado actual de la red de datos del Colegio Experimental "Juan Pío Montúfar", finalmente se presenta a manera de resumen los puntos principales analizados en este capítulo.

Con respecto a la topología y funcionamiento lógico de la red, ésta se encuentra actualmente desorganizada, no existe una jerarquía para interconexión de los equipos, no existe ningún tipo de restricción para la

comunicación de los diferentes integrantes de la red. El equipamiento del Colegio no es el adecuado, ninguno de los equipos es administrable y no se han tomado en cuenta las características mínimas para su adecuado funcionamiento.

Los servicios que se encuentran en funcionamiento son: el servidor de notas, que es brindado por una empresa externa al Colegio. El servidor actual es una computadora personal adaptada para su funcionamiento, no está dimensionado en función de la carga que va a soportar, razón por la cual en cualquier momento podría existir una falla del sistema que podría terminar en pérdida de información.

Los equipos finales de usuario encontrados en el Colegio son las estaciones de trabajo y las impresoras. Las estaciones de trabajo en su mayoría son demasiado antiguas, lo que hace que su trabajo sea ineficiente y no tienen acceso a la red.

Las impresoras son para el uso local lo que representa un desperdicio de recursos al tener que conectar una impresora por cada computador que la necesite.

El colegio no cuenta con una central telefónica, por lo que tienen contratado líneas telefónicas directas.

El cableado actual no cumple con la normas de los sistemas de Cableado Estructurado, no existe una Sala de Equipos y el enrutamiento es hecho de manera precaria en función de las necesidades inmediatas de los usuarios de la red, este sistema llega a muy pocos usuarios y no es escalable o flexible. El cableado vertical es inexistente debido a que las estaciones de trabajo se conectan directamente a los equipos ubicados en la sala de internet donde se encuentran los equipos de interconectividad. No existe una adecuada conexión a Tierra ni protecciones para los equipos por lo que una falla en el sistema eléctrico podría dejar sin funcionamiento a todo el sistema.

El número de usuarios potenciales de la red es muy grande con respecto a los usuarios actuales de la red porque en general la mayoría de integrantes del Colegio no tienen acceso a ésta. Los usuarios que tienen acceso a la red, no tienen una cultura de uso, a más de que no existen políticas de uso que regulen el acceso a la red. Los usuarios inalámbricos son prácticamente los de los laboratorios de informática ya que las algunas computadoras poseen tarjetas inalámbricas.

Las aplicaciones usadas en el Colegio son de carácter local, no existe ninguna aplicación instalada para su funcionamiento en red, debido a esto el tráfico local no existe, el único tráfico que circula en la red es el que va hacia el Internet, el cual es subutilizado debido a que las características de los equipos no son las más recomendadas, además que en su gran mayoría no es utilizado con labores acorde a la misión de la comunidad educativa.

CAPÍTULO III

3. REDISEÑO DE LA RED COLEGIO EXPERIMENTAL JUAN PÍO MONTÚFAR (CEJPM)

3.1. VISIÓN GENERAL

Para que el rendimiento y desarrollo tecnológico de la Institución Educativa este siempre mejorando, se requiere tener disponible una red con alta seguridad, que pueda ser escalable y en la que converjan varios servicios y beneficios, mediante la cual se quiere cumplir con las necesidades actuales y tener una idea del crecimiento para el tiempo posterior, ofreciendo a los clientes internos o externos de la Institución, servicios varios que puedan ser fácilmente accedidos y de buena calidad.

Se desarrolla el rediseño de la red, para brindar una total solución de interconectividad entre las diferentes aulas, laboratorios, centros de reuniones, etc. Para todo esto se tiene planificado tener variados servicios que soportaría la red tales como: Voz sobre IP (telefonía), navegación y descargas en Internet, interconectividad a través de red LAN/WLAN, vigilancia de seguridad con video, mails y correos, Intranet, etc.

Luego de la revisión y verificación del anterior capítulo, se ha llegado a la conclusión que el CEJPM tiene las siguientes necesidades tecnológicas: vigilancia y seguridad multimedia, interconectividad general, otros servicios; los que se deben contemplar a continuación:

- La vigilancia y seguridad multimedia, mediante cámaras con circuito cerrado CCTV, para mejorar la seguridad en el ingreso y salida del Colegio, esto cubrirá las necesidades de integridad personal y material para personal docente, administrativo y estudiantil.

- En sitios muy importantes como puntos de reunión, aulas virtuales, sala de profesores, biblioteca y bar es necesario tener servicio de Internet inalámbrico disponible para la navegación y conectividad a los usuarios internos y externos.
- Los puntos de trabajo o estaciones deben tener interconectividad a la red local, para que todo el personal administrativo, docente, estudiantil y externo tengan accesibilidad a servicios y aplicaciones tales como Intranet e Internet.
- Para obtener un mejor desempeño de la red de voz existente, se debe tener acceso a equipos que permitan acceder a la tecnología de VoIP, para esto es necesario contemplar el diseño de la telefonía IP.
- Tener un sistema de cableado estructurado que cumpla con estándares de calidad y funcionalidad, para disponibilidad de crecimientos de red futuros.
- Para mejorar seguridad, flexibilidad y desempeño de la red; es necesario tener disponibilidad de redes privadas virtuales VLANs , para segmentar los servicios , teniéndose una VLAN para voz sobre IP, una VLAN para cámaras y una VLAN para datos.
- Se requiere un establecimiento de políticas de seguridad en el acceso a la red interna y externa, en el que se puedan restringir las cuentas de usuarios de acuerdo a las aplicaciones justificados por competencia de funciones.
- Es crucial, tener la disponibilidad de tener servidores para Web, correos electrónicos, Bases de Datos, DNS, Proxy, DHCP, Firewalls para tener una red LAN/WLAN con calidad, seguridad y tecnología actual.

3.1.1. INFRAESTRUCTURA DE LA RED

En función a lo analizado en el capítulo 2, y de acuerdo a las necesidades del Colegio, se desarrolla un análisis de los servicios que tendrá la red, mediante lo cual se realiza el diseño de infraestructura de la misma.

3.2. SERVICIOS QUE DISPONDRÁ LA RED INTERNA LOCAL INTRANET CEJPM

3.2.1. SERVICIO DE VoIP (Telefonía IP).

Usando la infraestructura actual mediante nuevos dispositivos de telefonía, y usando el protocolo IP, se pueden tener los siguientes beneficios:

- La implementación e integración de una central IP tiene un costo efectivo respecto a tener una central telefónica analógica.
- Existe una mejor escalabilidad y un número menor de conexiones adicionales, lo cual conlleva a tener un costo menor para la implementación de la misma.
- Cumpliendo algunos requisitos técnicos, se pueden tener terminales de voz multivendor, obteniéndose así flexibilidad de fabricantes en esta tecnología.
- Se ahorra nueva infraestructura de cableado y se obtiene un beneficio de menor costo para la gestión de la red completa, teniéndose además una administración centralizada.
- Se pretenden mejores servicios que la telefonía tradicional y mejor seguridad para los usuarios, a través de procesos como la autenticación, codificación, digitalización de la información.

Este servicio es requerido por la Institución, debido a que actualmente cuenta con 10 líneas telefónicas independientes que abastecen a pocos usuarios y pocas localidades internas de la institución.

3.2.2. SERVICIO DE INTERNET

Este servicio será proporcionado para todos los usuarios conectados a la red LAN y WLAN, ofreciendo calidad, alta disponibilidad, para mejorar el acceso a la información evolucionando el desarrollo académico de personal docente, estudiantil y administrativo.

El área estudiantil y docente, desarrollará el área académica, con la facilidad de acceso a la red INTERNET, optimizará el estudio e investigación de información para cada una de sus materias.

3.2.3. SERVICIO DE E-MAIL (CORREO ELECTRÓNICO).

El correo electrónico es necesario para dar servicio a todos los usuarios de la Institución para que puedan enviar, recibir mensajes, descargar y cargar archivos dentro y fuera del CEJPM de forma sencilla y rápida, con el uso de programas instalados en cada PC.

El CEJPM actualmente no cuenta con correo electrónico Institucional, los usuarios para enviar un archivo dentro de la Institución utilizan correos externos como yahoo, hotmail, gmail entre otros.

Como observación principal, se tiene que este servicio es proporcionado por las empresas proveedoras de Internet, pero no obstante, este puede ser implementado en la Intranet mediante el uso de un servidor de correo y con el uso de aplicaciones clientes de correo en cada uno de los usuarios.

3.2.4. SERVICIO DE VIGILANCIA A TRAVES DE VIDEO CON TECNOLOGÍA IP.

La tecnología avanzada permite ahora la convergencia de red a través de unificación de servicios tales como la video vigilancia IP, usando el protocolo TCP/IP, solamente necesitándose una cámara de video IP, puerto disponible y la interconectividad, basándose en un lugar donde se requiera este servicio.

Los dispositivos de A/V comunican la información centralizados en un servidor, al cual se tiene acceso de forma interna (INTRANET) y externa (INTERNET), en el que se deberán tomar en cuenta políticas de seguridad de acceso y parámetros de circuito cerrado para seguridad de la institución.

El objetivo de brindar este servicio en la CEJPM, es proveer un sistema de monitoreo para la seguridad en el ingreso y salida de la Institución, necesario debido al alto índice de inseguridad que existe actualmente en la ciudad de Quito.

3.2.5. SERVICIOS VARIOS

Adicionalmente, se ofrecerá otros servicios como son la implementación de un servidor de impresión, fax y servidor de carga y descarga de archivos.

3.3. DIMENSIONAMIENTO DE TRÁFICO POR SERVICIO

Se realiza por servicio a ofrecerse y de acuerdo a las tabulaciones de datos de ingreso que se tengan de los estimados que se obtengan, para el dimensionamiento de red.

3.3.1. Tráfico para Video Vigilancia IP

Se realiza una descripción de los protocolos y procesos que rigen estos servicios, posteriormente se hará una introducción al dimensionamiento de tráfico.

En la tabla 3.1 se indica los protocolos utilizados para transmitir video sobre redes IP.

Protocolos Utilizados Para Video IP	Protocolos de Transporte	Puerto	Características
FTP	TCP	21	Transfiere las imágenes desde la cámara hacia el servidor
SNMP	TCP	25	Es utilizado para enviar notificaciones de alarma al correo electrónico
HTTP	TCP	80	Es el encargado de transferir el video desde el dispositivo de red (cámara), el cual funciona básicamente como servidor web que pone el video a disposición del usuario o del servidor de aplicaciones que lo solicita.

HTTPS	TCP	443	Tiene las mismas funciones que el protocolo HTTP pero adicionalmente proporciona seguridad
RTP	UDP/TCP	No está definido	Es utilizado para la entrega de audio y de video en la red IP, utilizado en sistemas multimedio o videoconferencia Transmite video basado en el estándar H.264/MPEG. Además, RTP proporciona numeración y señalización de paquetes para el ensamblado de forma correcta de los paquetes en el destino.
RTSP	TCP	554	Permite la configuración y el control de sesiones multimedia RTP:

Tabla 3.1 protocolos utilizados para transmitir video sobre redes IP

3.3.1.1. Procesos básicos y parámetros que se deben considerar para transmitir video sobre redes IP

Los procesos básicos para desarrollar un sistema de IP de seguridad y vigilancia mediante video son:

- Codificación, Decodificación y Compresión de datos de video.

Este proceso se realiza en el dispositivo de cámara IP o en el servidor de video, teniéndose que la codificación es el proceso mediante el cual una señal analógica se digitaliza y comprime para luego ser transmitida por la red IP, mientras que la decodificación de video es la traducción de la información con el fin de ser visualizada desde un dispositivo o interfaz traductor (Computador) y mediante el uso de un programa de monitoreo de video.

La compresión se basa en aplicar un algoritmo al video original para crear un archivo comprimido. Para obtener el archivo original se aplica el algoritmo inverso. Tomando en cuenta esto, cuanto más avanzado sea el algoritmo de compresión, menor será el ancho de banda requerido para transmitir video sobre la red.

Al codificador y decodificador se los denomina códecs de video. Los códecs de video de estándares diferentes no suelen ser compatibles entre sí.

- Transmisión y flujo de datos IP

Es la transmisión que se realiza desde el dispositivo de la cámara, la cual captura las imágenes y las envía a través de la red hacia un servidor de almacenamiento, para luego ser visualizado o monitoreado desde una PC.

- Grabación

La grabación o almacenamiento del video se lo realiza en servidores tales como NAS o RAS.
En la figura 3.1 se indica el modelo del sistema de video vigilancia

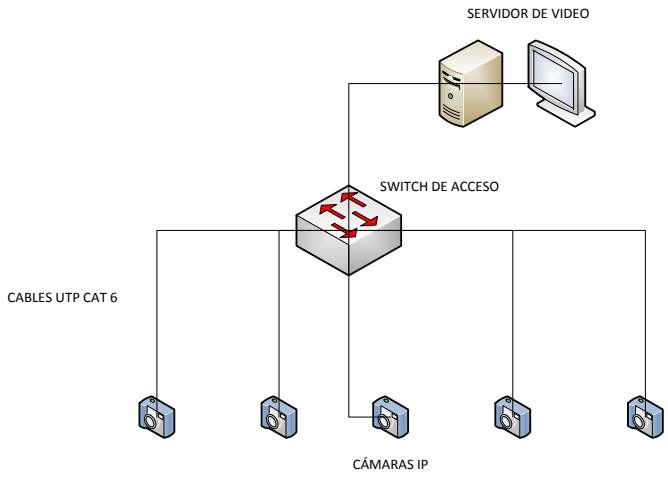


Figura 3.1 modelo del sistema de video vigilancia

3.3.1.2. Algoritmos de Compresión

Cada sistema de vigilancia o cámara IP utiliza diferentes tipos de compresión, la mayoría de los dispositivos soportan varios tipos de compresión dando la flexibilidad de elegir el más adecuado, entre los formatos de compresión de video más utilizados se tiene:

- M-JPEG[39]
- MPEG-4
- H.264 que es la versión 10 de MPEG-4.

Para este caso se escogió la compresión que proporciona MPEG-4 debido a que este sistema permite un alto grado de compresión manteniendo una buena calidad de video y utilizando un menor ancho de banda en relación a M-JPEG.

Cabe indicar que el algoritmo de compresión H.264 o MPEG-4 AVC, proporciona mejores características que MPEG-4, aumentando la compresión, manteniendo la calidad de video, disminuyendo el uso de ancho de banda y utilizando un menor espacio de almacenamiento sin embargo no está muy difundido en el mercado por lo que se tienen pocos equipos que soporten este tipo de compresión. Esta es la razón principal por la que no se escogió este algoritmo de compresión.

En la tabla 3.2 se indica las Características de los principales algoritmos de compresión de video.

	M-JPEG	**MPEG**	**H.264**
Compresión	Espacial	Espacial/Temporal	Espacial/Temporal
Calidad de la imagen	Grande	Pequeña	Pequeña
Pérdida	Con perdidas	Con perdidas	Con perdidas
Tamaño de los Archivos	Grande	Pequeño	Pequeño
Resolución	640X480	720X576	352X288
Tamaño de la Matriz	8X8	16X16	8X8
Ratio	20:1 y 40:1	100:1 variable	100:01:00
AB (Mbps)	2.5	1.86	0.546
Ips	25	30	20
Aplicaciones	Transmisión de video	Transmisión de video, TV	Video conferencia

Tabla 3.2. Características de los principales algoritmos de compresión de video.

[39] M-PEG Moving Pictures Experts Group: es un Grupo de Trabajo de expertos para establecer estándares para el audio y la transmisión video.

En la figura 3.2 se indica la Utilización de AB de algunos algoritmos de compresión de video.

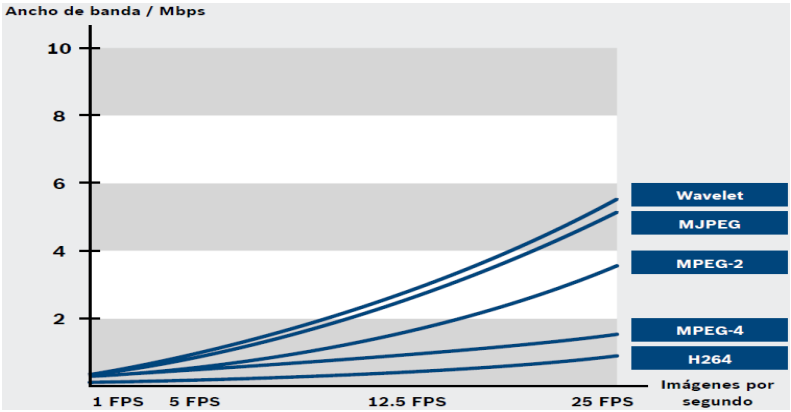


Figura 3.2 Utilización de AB de algunos algoritmos de compresión de video

Para realizar el análisis de ancho de banda requerido en la transmisión de video sobre una red IP, se consideran algunos parámetros fundamentales tales como:

- Número de imágenes por segundo
- Algoritmo de compresión
- Encapsulamiento de video
- Número de cámaras IP

3.3.1.3. Dimensionamiento del ancho de Banda

De acuerdo a los parámetros y procesos descritos en la tabla 3.2, los cuales se utilizan para determinar el ancho de banda necesario, se tiene la siguiente ecuación [12].

$$AB(bps) = \left[\frac{tamaño\ imagen * profundidad\ del\ color * \#\ imágenes\ por\ segundo}{Factor\ de\ compresión}\right]$$

Ecuación 1

Descripción de las variables utilizadas en la ecuación.

- **width * height** = tamaño de la imagen (pixeles)
- **Color bit depth** = Profundidad del color utilizado para las imágenes, 8 bits para codificar cada uno de los tres colores RGB.
- **Ips** = Número de Imágenes por segundo
- **Factor de compresión** = Factor de compresión de imágenes de video.

En la actualidad se puede encontrar diferentes tipos de cámaras IP, las que en su mayoría cumplen con las mínimas características técnicas requeridas.

- 25/30 Ips con una resolución de 160X120
- 25/30 Ips con una resolución de 320X240
- 10/25 Ips con una resolución de 640X480
- Compresión M-JPEG y MPEG-4

El estándar de compresión MPEG-4 soporta un factor de compresión que está en el rango de 70:1 (Movimiento) a 200:1(Estático), considerando que no va a existir un movimiento continuo se va a seleccionar un factor de compresión de 140.

$$AB(bps) = \left[\frac{640 * 480 * 24 * 15}{140}\right]$$

$$AB(bps) = 789.94 \ \ kbps$$

$$AB(Cámara\ IP) = AB(Video) + AB(Voz)$$

$$AB(Cámaras\ IP) = 789.94 + 64$$

$$AB(Cámaras\ IP) = 853.94\ kbps$$

El ancho de banda requerido es de 853.94 Kbps por cada cámara a utilizar, tomando en cuenta que son 14 cámaras se obtiene lo siguiente

$$AB(Cámaras\ IP) = Número\ Total\ de\ Cámaras * AB(Cámara)$$

$$AB(Cámaras\ IP) = \ \ 14 * (853.94)kbps$$

$$AB(Cámaras\ IP) = \ 11955.16\ kbps$$

3.3.1.4. Dimensionamiento de Almacenamiento

En base al ancho de banda requerido, se procede a calcular el espacio de almacenamiento necesario.

$$11955.16\frac{bits}{segundo} * \frac{1\ Byte}{8\ bits} * \frac{3600\ segundos}{1\ hora} * \frac{1}{1000} * \frac{1}{1000} = 5.38\ GB\frac{GB}{hora}$$

Se necesita aproximadamente 6 GB por cada hora de actividad, para la adquisición de las cámaras IP una de las características principales es que se enciendan y capturen video solo si hay actividad caso contrario se deben poner en estado de reposo.

Tomando en cuenta que las cámaras IP solo capturan video si existe actividad y que el CEJPM está abierto frecuentemente de 7:00 am a 8:00 pm, donde se tiene un flujo continuo de grabación de 7:00 am a 8:00 pm, obteniendo un tiempo promedio de grabación de 13 horas por día los 30 días al mes, se necesita un disco duro de almacenamiento de:

$$6.0\ GB\frac{GB}{hora} * \frac{13}{día} * \frac{30}{mes} = 2340.0\ GB$$

Para el almacenamiento de video, se puede utilizar un servidor normal, el cual tenga una capacidad de 2.5 TB, sin embargo existen servidores especiales para almacenamiento de información tales como los NAS y los SAN.

3.3.2. TRÁFICO PARA TELEFONÍA IP

Para realizar el dimensionamiento de tráfico de voz sobre una red IP, se han tomado en cuenta 4 factores principales:

- Códec a utilizar
- El tamaño del paquete de datos de voz
- Utilización de compresión de la cabecera RTP
- Supresión de silencio.

Los códecs de voz son dispositivos que convierten la señal analógica en digital. Además, permiten comprimir la señal, disminuyendo significativamente el ancho de banda requerido para enviar paquetes de voz por la red IP.

En la tabla 3.3 se realiza una descripción de los códecs más utilizados para transmitir VoIP.

Códec	Modulación	Ancho de Banda (Kbps)	Frecuencia de Muestreo (KHz)	Observaciones
G.711	PCM	64	8	Existen 2 versiones para muestrear la señal u-law (US y Japón) y a-law (Europa)
G.721	ADPCM	32	8	Obsoleta
G.722	7 kHz codificación de audio dentro de 64 kbit/s	64	16	Se basa en dividir La frecuencia de muestreo en dos bandas cada una usando ADPCM
G.722.1	Codificación a 24 y 32 kbit/s	24/32	16	Describe un algoritmo Wideband proporcionando un AB de 50 a 7000 Hz
G.723	Codificación de 24 y 40 kbit/s para aplicaciones en circuitos digitales.	24/40	8	Obsoleta y diferente de G.723.1.
G.723.1	Codec de audio de baja velocidad en aplicaciones multimedia.	5.6/6.3	8	Es parte de H.324. y es utilizada para videoconferencia
G.726	ADPCM	16/24/32/40	8	Reemplaza a G.721 y G.723.

G.727	ADPCM	variable		Relacionada con G.726.
G.728	Codificación de señales de voz mediante la utilización de la técnica de predicción lineal con excitación por código de bajo retardo	16	8	CELP.
G.729	CS-ACELP	8	8	Tiene un bajo requerimiento de ancho de banda y Bajo retardo (15 ms)

Tabla 3.3 Códec utilizados en VoIP [13]

Por lo que será utilizado para este dimensionamiento, de acuerdo a las características de los códecs más utilizados en telefonía IP, el que cuenta con un ancho de banda relativamente bajo y mantiene una buena calidad de voz es el G.729.

Para el envío de voz sobre redes IP, es necesario estructurar la información mediante paquetes, donde el ancho de banda requerido dependerá de la sobrecarga que generen estos paquetes.

3.3.2.1. Protocolos de Encapsulamiento para enviar Voz sobre una red IP

Para enviar VoIP sobre una red LAN mediante tramas Ethernet se utiliza el protocolo RTP (Real Time Protocol). El cual es encapsulado en el protocolo UDP (User Datagram Protocol), para luego ser encapsulado sobre IP, el que es encargado de llevar la información sobre Ethernet.

En la figura 3.3 se indica la Cabecera de los protocolos utilizados para enviar voz sobre redes IP.

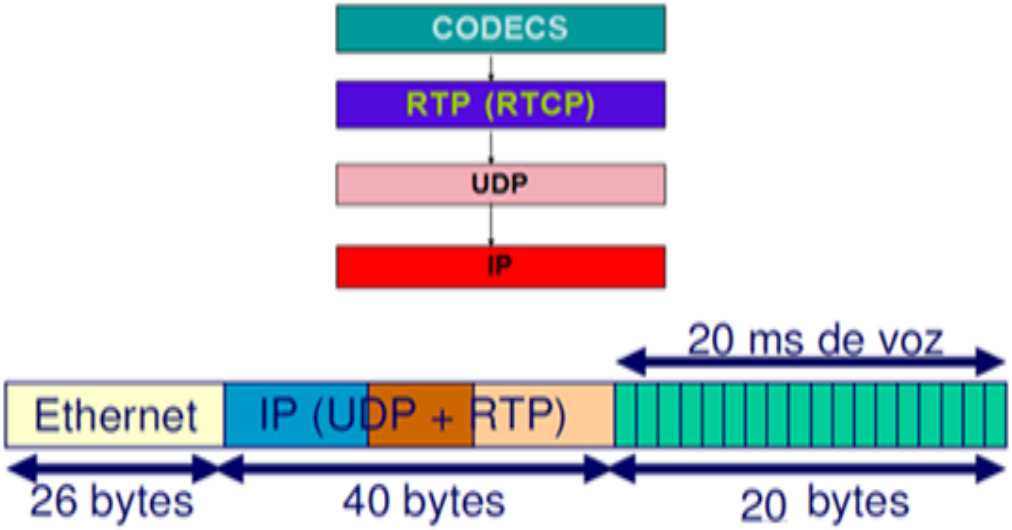


Figura 3.3 Cabecera de los protocolos utilizados para enviar voz sobre redes IP

Con la siguiente ecuación se puede determinar el ancho de banda necesario para transmitir paquetes de voz sobre una red IP [12].

$$AB_{canal} = AB_{codec} \frac{longitud\ de\ sobrecara + longitud\ de\ encapsulamiento}{longitud\ de\ sobrecarga}$$

Ecuación 2

Donde cada variable representa lo siguiente:

- **$AB_{códec}$** = Ancho de banda del códec seleccionado.
- **Longitud de sobrecarga** = Tamaño del payload de la trama.
- **Longitud de encapsulamiento** = Tamaño de la cabecera de la trama.

Con la ecuación anterior se obtiene la capacidad requerida por canal: sin embargo, la capacidad real para cada conversación será el doble del valor obtenido, debido a que la conversación se la realiza en sentido bidireccional.

Para obtener la capacidad real por conversación se va a utilizar la siguiente ecuación.

$$C_{capacidad\ real\ por\ conversación} = 2 * C_{canal}$$

En la tabla 3.4 se tiene una descripción detallada de las cabeceras de los protocolos que se encapsulan en el protocolo IP.

Cabecera RTP	12 Bytes
Cabecera UDP	8 Bytes
Cabecera IP	20 Bytes
Payload (Voz)	20 Bytes
Cabecera Ethernet	26 Bytes
Longitud de Sobrecarga	20 Bytes
Longitud de Encapsulamiento	66 Bytes
Ancho de banda del códec	8 Kbps

Tabla 3.4 Cabecera de los protocolos utilizados para enviar vos sobre redes IP

$$AB_{canal} = 8\ kbps \frac{20\ Bytes + 66\ Btes}{20\ Bytes}$$

$$AB_{canal} = 34.4\ kbps$$

$$C_{capacidad\ real\ por\ conversación} = 2 * 34.4\ kbps$$

$$C_{capacidad\ real\ por\ conversación} = 68.8\ kbps$$

Tomando en cuenta que el CEJPM tiene un requerimiento de 40 puntos para voz, por lo que el ancho de banda total mínimo necesario es:

$$ABTotal = 40 * 68.8\ Kbps$$

$$ABTotal = 2752\ Kbps$$

3.3.2.2. Líneas troncales hacia la PSTN

Para determinar el flujo de tráfico que circula a través de la central telefónica se va a utilizar la siguiente ecuación [14].

$$A=C*T \text{ (Erlang)}$$

Ecuación 3

Definición de las variables utilizadas en la ecuación.

- **A** = Intensidad de tráfico o velocidad de flujo de llamadas, este valor es dado en Erlangs.
- **C** = Número de llamadas originadas durante horas pico
- **T** = Tiempo promedio que dura una llamada.

Con los datos obtenidos en el capítulo 2, se va a realizar una aproximación del tráfico que va a circular por la central telefónica. Además, cabe mencionar que la Institución cuenta con 8 líneas telefónicas directas con CNT, sin tenerse la necesidad de más extensiones adicionales.

Los datos obtenidos fueron de 10 llamadas por hora con una duración promedio de 3 minutos.

$$A = 10\frac{llamadas}{hora} * \frac{1\ hora}{60\ minutos} * 3\frac{minutos}{1\ llamada}\ (Erlangs)$$

$$A = 0.5\ (Erlangs)$$

La intensidad de tráfico calculado es de 0.5 Erlangs[40], tomando en cuenta el valor 0.01 (Este valor es recomendado para telefonía) de la probabilidad de pérdida

[40] Erlang representa la cantidad de intensidad de tráfico transportado por un canal de voz.

(GoS)[41] y utilizando la gráfica de Erlang B, se determina 4 canales de voz necesarios para el CEJPM. (Figura 3.4)

En la figura 3.4 serepresenta Erlang B

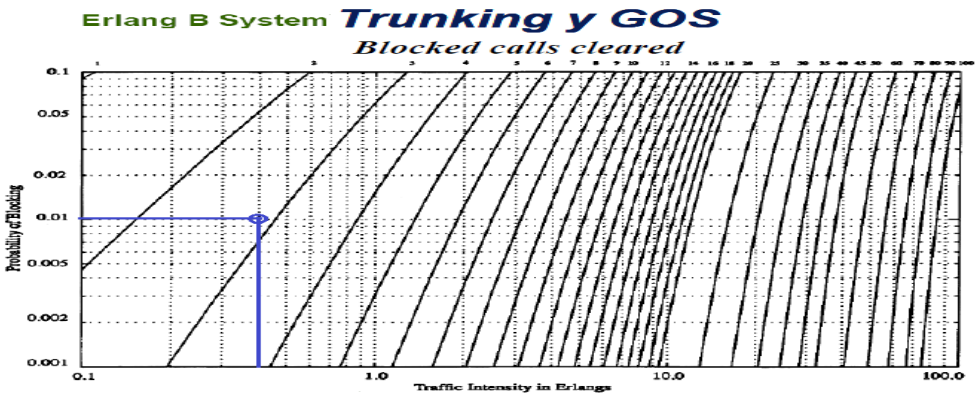


Figura 3.4 Erlang B

De acuerdo a los datos obtenidos se procederá a proyectar el tráfico telefónico a un periodo de 5 años, para lo cual se utiliza la siguiente ecuación.

$$A_f = A_0(1 + f_c)^n$$

Ecuación 4

Variables de la ecuación.

- A_f = Tráfico final
- A_o = Tráfico inicial
- f_c = Factor de crecimiento anual
- n = Número de años

Considerando un crecimiento anual del 1% durante un período de 5 años se tendrá un tráfico de 0.525 Erlangs, por lo que los cuatro canales de voz soportarán esta cantidad de tráfico generada.

[41] GoS (Grade of Service) Es una medida de la habilidad del usuario para acceder a un sistema que utiliza Trunking.

$$Af = 0.5(1 + 0.01)^5$$

$$Af = 0.525\ Erlangs$$

En la tabla 3.5 se detalla la cantidad de tráfico proyectado por año durante los 5 primeros años.

Año	A (Erlangs)	Número de Troncales
0	0.5000	4
1	0.5050	4
2	0.5101	4
3	0.5151	4
4	0.5203	4
5	0.5255	4

Tabla 3.5 tráfico proyectado para 5 años

3.3.3. TRÁFICO PARA CORREO ELECTRÓNICO

Para calcular el ancho de banda necesario para enviar y recibir un correo electrónico, se toma como referencia lo siguiente. Un mensaje de correo electrónico Institucional tiene un peso promedio de 50 KB y que el usuario revise el mail cada 40 minutos [15].

Cabe indicar que los usuarios que dispondrán de correo electrónico Institucional son 137 dentro de los cuales se encuentran los administrativos y profesores.

A continuación se detalla el cálculo utilizado para determinar el volumen de correo electrónico:

$$AB_{(por\ usuario)} = \frac{50\ KB}{1\ mail} * \frac{8\ bits}{1\ byte} * \frac{1\ mail}{40\ minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(por\ usuario)} = 0.167\ Kbps$$

$$AB_{(total\ correo\ electrónico)} = 0.167 * (137)\ Kbps$$

$$AB_{(total\ correo\ electrónico)} = 22.83\ Kbps$$

3.3.4. TRÁFICO GENERADO POR PÁGINAS WEB

Todos los usuarios que estén conectados a la red de la CEJPM deben tener el servicio de acceso a Internet, se estima que cada usuario visite 12 páginas web por hora y considerando la información de la figura 3.5, donde se detalla el tamaño promedio de una página web con relación al número de objetos que tiene. Una página web simple tiene un peso promedio de 350 KB [16].

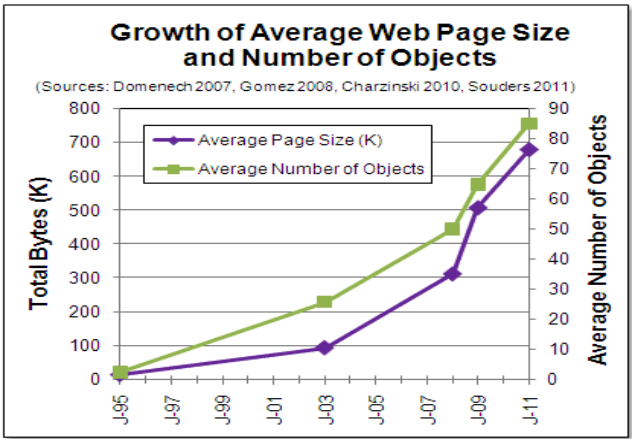


Figura 3.5 crecimiento promedio de una página web [17]

A continuación se realiza el cálculo para determinar el ancho de banda requerido.

$$AB_{(por\ usuario\ conectado\ al\ internet)} = \frac{350\ KB}{1\ página} * \frac{8\ bits}{1\ byte} * \frac{12\ página}{1\ hora} * \frac{1\ hora}{3600\ segundos}$$

$$AB_{(por\ usuario\ conectado\ al\ internet)} = 9.33\ Kbps$$

Una vez calculado el ancho de banda requerido por cada usuario para visitar una página web se procede a calcular la correspondiente para todos los usuarios que tendrán acceso a este servicio. Sin embargo, no todos los usuarios estarán navegando en Internet de forma simultánea por lo que se utiliza un índice de simultaneidad del 40%. Si tomamos en cuenta los 137 usuarios administrativos y profesores, el 40% seria 55 usuarios simultáneos.

$$AB\ (total\ para\ navegar\ en\ internet) = 55 * 9.33\ Kbps$$

$$AB_{(total\ para\ navegar\ en\ internet)} = 513.15Kbps$$

3.3.5. TRÁFICO GENERADO POR ACCEDER A LA BASE DE DATOS

Antes de calcular el tráfico que se genera al subir las notas a la base de datos, es necesario indicar que los profesores actualmente no cuentan con este servicio, por lo que las calificaciones las sube cada profesor al servidor para que sean almacenadas en la base de datos. Sin embargo: en este diseño se considera este tráfico ya que la Institución requiere dicho servicio.

Los docentes para subir la información al Sistema contarán con la siguiente infraestructura, 40 computadores del laboratorio de computación primeros y segundos cursos y 4 computadores en la sala de profesores, de acuerdo a la información de las tablas 3.12 y 3.14. Los computadores de los otros laboratorios de computación solo estarán disponibles para dictar clases.

En base al estudio realizado en el capítulo 2, donde se indica que existen 106 profesores. La duración de recreo es de 40 minutos, tomando como referencia un peso promedio de 50 KB para cada consulta a la base de datos [12].

$$AB_{(Académico)} = \frac{50\ KB}{1\ usuario} * \frac{8\ bits}{1\ byte} * \frac{106\ usuarios}{40\ minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Académico)} = 17.7Kbps$$

3.3.6. TRÁFICO GENERADO POR MENSAJERÍA INSTANTÁNEA

En la actualidad el uso de chat es muy utilizado tanto por los administrativos como por los estudiantes, por lo que será considerado para el diseño de la red. Se tiene 273 puertos para datos y un mensaje tiene un peso aproximado de 1KB por cada mensaje donde cada usuario envía uno cada minuto aproximadamente se requiere el ancho de banda detallado a continuación [18].

$$AB_{(Messenger)} = \frac{1KB}{1\ mensaje} * \frac{8\ bits}{1\ byte} * \frac{1\ mensaje}{1minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Messenger)} = 0.13\ Kbps$$

$$AB(Total) = 273 * 0.13\ Kbps$$

$$AB(Total) = 35.49\ Kbps$$

3.3.7. TRÁFICO GENERADO POR IMPRESIÓN

Para determinar el ancho de banda necesario para enviar una hoja de datos a imprimir se verificó el tamaño de diferentes archivos de una hoja del programa editor de texto ofimático Word, obteniendo los datos detallados en la siguiente tabla (3.6).

	Peso (KB)
Peso de una hoja de Word con diferente contenido	150
	23.1
	34.7
	22
Peso promedio	**57.45**

Tabla 3.6 Tamaño de hojas de Word

Se hace una estimación de que cada usuario imprimirá 8 hojas por hora donde cada hoja tiene un peso aproximado de 57.45 KB y que son 7 usuarios que utilizarán este servicio se necesitará el siguiente ancho de banda.

$$AB\ (Impresión) = 7\frac{57.45KB}{1\ hoja} * \frac{8\ bits}{1\ byte} * \frac{8hojas}{1hora} * \frac{1hora}{3600segundos}$$

$$AB\ (Impresión) = 7{,}15Kbps$$

3.3.8. TRÁFICO GENERADO POR DESCARGAR ARCHIVOS DE INTERNET

Para descargar un archivo desde Internet se utiliza 2 factores, el tamaño del archivo y el tiempo de descarga de dicho archivo. Un archivo de 1MB se descarga en un tiempo aceptable de un minuto, por lo que se requiere del siguiente ancho de banda.

$$AB_{(Descarga)} = T_{archivo} * t_{descarga}$$

$$AB_{(Descarga)} = \frac{1000\ KB}{1\ minuto} * \frac{8\ bits}{1\ byte} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Descarga)} = 16.7\ Kbps$$

Cabe indicar que no todos los usuarios conectados a Internet descargarán un archivo de forma simultánea, razón por la cual solo se calcula el ancho de banda requerido por los usuarios del Área Biblioteca que son 10. Se toma como referencia esta área porque es utilizado para que los estudiantes realicen investigación utilizando Internet.

$$AB\ (Descarga) = 10 * 16.7Kbps$$

$$AB\ (Descarga) = 167Kbps$$

3.3.9. TRÁFICO POR APLICACIÓN Y SERVICIO

En la tabla 3.7 se realiza un detalle del tráfico total requerido para todos los servicios y aplicaciones que se prestarán en la red de del CEJPM.

APLICACIÓN	CAPACIDAD REQUERIDA (Kbps)
Correo Electrónico	22.83
Páginas Web	513.15
Base de Datos	17.7
Mensajería Instantánea	35.49
Impresión	7.15

Descargar Archivos de Internet	167
TOTAL APLICACIONES	***763.32***
SERVICIOS	
Telefonía IP	2752
Video Vigilancia IP	11955.16
TOTAL SERVICIOS	14707.16
TOTAL GENERAL	**15470.48**

Tabla 3.7 Ancho de banda total requerido de la red interna

Se requiere una capacidad para la red interna de la Institución de aproximadamente 16 Mbps (**15.47 Mbps calculado)**, para prestar todos los servicios requeridos.

3.3.10. CONEXIÓN A INTERNET

Para calcular la capacidad requerida para el enlace a Internet, se toma en cuenta el tráfico generado por acceder a las páginas web, descargas de Internet y mensajería instantánea, lo cual se detalla en la tabla 3.8.

APLICACIÓN	CAPACIDAD REQUERIDA (Kbps)
Páginas Web	513.15
Mensajería Instantánea	35.49
Descargar Archivos de Internet	167
TOTAL	***715.64***

Tabla 3.8 Capacidad requerida para el enlace a Internet

De acuerdo a la información de la tabla 3.8 se requiere un enlace con una capacidad de 715.64 Kbps; sin embargo, los ISP (Proveedores de Servicio de Internet) ofrecen enlaces con capacidades estándar de 1 Mbps, el cual puede ser simétrico (1:1).

El CEJPM para la salida a Internet, cuenta con dos planes compartidos, el primero es un plan gubernamental gratuito provisto por la CNT de 2 Mbps tipo ADSL (Línea de Subscriptor Digital Asimétrica) 1:1 y el otro es un plan provisto por SURATEL de 2 Mbps con un dirección IP 186.66.129.218 con máscara de red

255.255.255.248, Gateway 186.66.129.217 y DNSs 200.63.212.110, 200.25.144.1.

3.3.11. PROYECCIÓN DE TRÁFICO

Al realizar un diseño de red se debe tomar en cuenta una estimación de tráfico futuro. Esto es primordial para asegurar un correcto funcionamiento de la red. El crecimiento de tráfico se debe al aumento de personal y actualización tecnológica.

El rediseño se lo realizó para todos los usuarios actuales, de acuerdo a la tabla 2.8, sin embargo, cada año se puede tener un aumento del personal administrativo o docente, para lo cual se considera un crecimiento del 1% anual de incremento de tráfico.
El tráfico que va existir en la red de acuerdo a la descripción anterior es de 15.47 Mbps, para calcular el crecimiento futuro, se utiliza la siguiente ecuación, la cual fue especificada en la ecuación 4.

$$A_f = A_0(1 + f_c)^n$$

$$A_f = 15.46(1 + 0.01)^5$$

$$A_{f0-10} = 16.24\ Mbps$$

En la tabla 3.9, se detalla el tráfico proyectado durante 5 años.

Años	Tráfico Final (Mbps)
1	15.61
2	15.76
3	15.92
4	16.07
5	16,24

Tabla 3.9 Proyección de tráfico

En la figura 3.6 se realiza el incremento de tráfico durante los próximos 5 años.

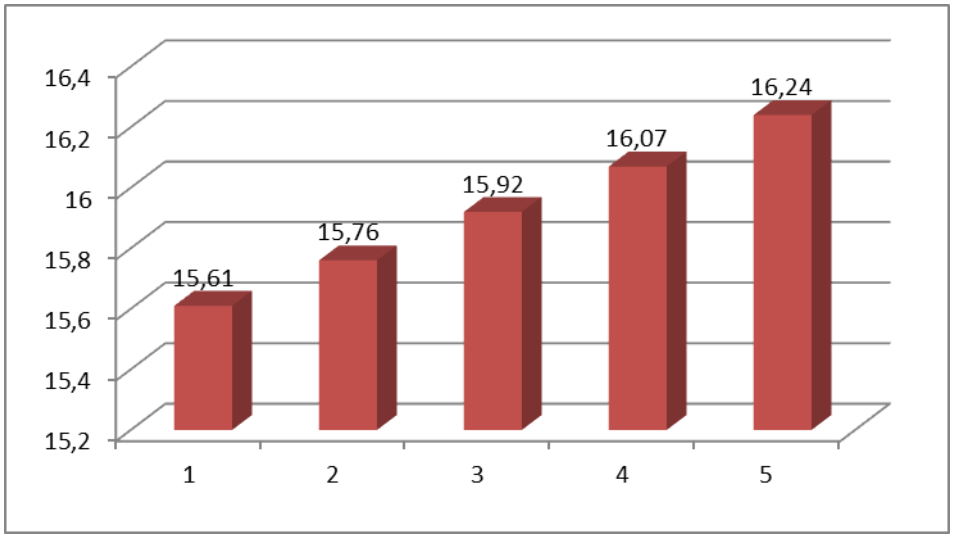


Figura 3.6 Estimación de Tráfico a 5 años.

3.4. TECNOLOGÍA DE RED Y MEDIO DE COMUNICACION

El CEJPM requiere contar con una red eficiente para prestar los servicios internos y externos optimizando recursos y mejorando el nivel educativo de los estudiantes.

De acuerdo a los servicios y aplicaciones que requiere la CEJPM se necesita contar con un medio de comunicación que soporte un gran ancho de banda por lo que se va a utilizar cable UTP CAT 6 con tecnología Gigabit Ethernet.

3.5. DISEÑO DE LA RED PASIVA

3.5.1. INTRODUCCIÓN

El Sistema de Cableado Estructurado brinda una perspectiva para crear un sistema organizado que el Administrador, usuario, técnicos y cualquier persona pueda fácilmente identificar, comprender o modificar cuando lo desee. El cableado garantiza eficiencia, efectividad, escalabilidad, ya que cuando se realiza el diseño se toma en cuenta que el modelo dura alrededor de 15 años. Unos de los objetivos que se pretende con esto es encontrar una solución óptima que permita interconectar todos los dispositivos, y al mismo tiempo cumplir con las

normas y estándares internacionales que permitan admitir tecnologías actuales y futuras.

Además con el cableado estructurado se planifica y se proyecta brindar conectividad teniendo en cuenta el crecimiento de usuarios en la intranet. La infraestructura de cableado conserva la libertad de elegir múltiples proveedores ofreciendo así la posibilidad de realizar modificaciones fácilmente y a bajo costo. Todo cambio que se quiera implementar será independiente del tipo de aplicación así como de los equipos de conectividad utilizados. Las salidas (outlets) garantizarán que cualquier movimiento se lo pueda hacer sin modificar el cableado existente.

La infraestructura actual de la red del Colegio Nacional Experimental “Juan Pío Montufar” no tiene una administración adecuada de su Cableado Estructurado. El presente diseño se enfocará a brindar todos los servicios necesarios que el Colegio utilizará a largo plazo.

Todos los edificios en los que funcionan estas dependencias tienen dos plantas, a excepción del bloque de aulas de los primeros y segundos cursos que tiene tres plantas. Cada una de estas áreas y edificios tienen requerimientos para el cableado estructurado y se describen a continuación para cada uno.

3.5.2. DISTRIBUCIÓN DE LOS PUNTOS DE CABLEADO PARA LAS ÁREAS

Debido al extenso campus del Colegio, éste ha sido dividido en diferentes áreas para brindar todos los servicios. En cada una de estas áreas se ubicará un Cuarto de Telecomunicaciones para el acceso a la información.

Si bien su distribución dentro del campus es diversa, estas pueden ser agrupadas en áreas funcionales las cuales poseen una relación directa en su trabajo, tal como se especifica en la tabla 3.10.

Área Administrativa	Planta Baja	- Biblioteca - Colecturía - Guarda-Almacén - Bodegas Generales
	Primer Piso	- Secretaria General - Salón de actos - Rectorado - Secretarias - Sistemas - Vicerrectorado - Secretaria Vicerrectorado - DOBE
Área Departamental	Planta Baja	- Sub-Inspección General - Departamento Médico - Sala de Música - Departamento de Cultura Física
	Primer Piso	- Sala de Lectura de Profesores - Inspección General - Departamento de Mejoramiento de la Calidad de la Educación - Sala de Profesores - Bar
Laboratorios	Planta Baja	- Laboratorio de Biología - Laboratorio de Química

	Primer Piso	✚ Laboratorio de Ciencias Naturales ✚ Laboratorio de Física
Bloque Primeros y Segundos Cursos	Planta Baja	✚ Laboratorio de Computación Primeros y Segundos Cursos ✚ Bar
	Primer Piso	✚ Bloque de Aulas
	Segundo Piso	✚ Bloque de Aulas
Bloque Terceros y Cuartos Cursos	Planta Baja	✚ Laboratorio de Computación Terceros y Cuartos Cursos ✚ Bloque de Aulas
	Primer Piso	✚ Laboratorio de Idiomas ✚ Sala de Idioma Extranjero ✚ Sala de Francés ✚ Bloque se Aulas
Bloque Quintos y Sextos Cursos	Planta Baja	✚ Boque de Aulas
	Primer Piso	✚ Laboratorio de Computación Quintos y Sextos Cursos.

Tabla 3.10 Distribución de Áreas Colegio Experimental "Juan Pio Montufar"

3.5.2.1. Edificio Administrativo

El edificio Administrativo está conformado por dos plantas, en la planta baja se encuentran la Biblioteca, Colecturía, Guarda-Almacén y Bodegas. En el primer piso se encuentran las oficinas de Rectorado y Vicerrectorado, Secretaría General, Salón de Actos, Secretarías, Sistemas, DOBE. De lo expuesto

anteriormente se resume en la tabla 3.11, los puntos de voz y datos a instalar así como el porcentaje de crecimiento.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total
Baja	Biblioteca	9	1	10
	Colecturía	4	3	7
	Guarda-Almacén	1	1	2
	Bodegas	1	1	2
Primer Piso	Secretaría General	3	2	5
	Salón de Actos	1	1	2
	Rectorado	1	2	3
	Secretarías	3	2	5
	Sistemas	1	1	2
	Vicerrectorado	2	2	4
	Secretaría de Vicerrectorado	1	1	2
	DOBE	4	4	8
	Cámaras	4	-	4
	Access Point	2		2
TOTAL		**37**	**21**	**58**
			25% Crecimiento	14

Tabla 3.11 Distribución de puntos de red. Edificio Administrativo

Para cada una de estas Áreas se proyecta un crecimiento de un 25 % este valor es para asegurar que las áreas tengan disponibilidad de acceso por un período de 10 años, de esta forma se provee que existan los suficientes puertos en los equipos y además el suficiente espacio en la ductería, ya que cuando entre en funcionamiento la red tendrá mayor demanda para los usuarios de todo el Colegio. Este valor ha sido determinado a partir de reuniones con las autoridades y profesores sobre las proyecciones de crecimiento esperadas en el Colegio, debido al incremento de estudiantes es necesesario el contrato de nuevo personal

para las diferentes áreas con las que cuenta el Colegio por ejemplo: Biblioteca, Colecturía, Secretarías, Departamento Médico, Profesores, etc.

En este edificio se tiene un total de 58 puntos de red, debido a la proyección se estima que se debe considerar 14 puntos adicionales para esta Área.

3.5.2.2. Departamental

El Área departamental presenta en la planta baja la Sub-Inspección, Departamento Médico, Sala de Música, Departamento de Cultura Física. En el primer piso la Sala de Lectura de Profesores, Inspección General, Departamento de Mejoramiento de la Calidad de la Educación, Sala de Profesores, Bar. En la Tabla 3.12 se indica la distribución de puntos de red para el edificio Departamental.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total
Baja	Sub-Inspección	1	1	2
	Departamento Médico	2	2	4
	Sala de Música	1	1	2
	Departamento de Cultura Física	1	1	2
Primer Piso	Sala de Lectura de Profesores	2	2	4
	Inspección General	1	1	2
	Departamento de Mejoramiento de la Calidad de la Educación	2	2	4
	Cámaras	2	-	2
	Access Point	2	-	2
TOTAL		**14**	**10**	**24**

	25% Crecimiento	6

Tabla 3.12 Distribución de puntos de red. Edificio Departamental

3.5.2.3. Laboratorios

En planta baja tenemos los laboratorios de Biología y Química. En el primer piso el Laboratorio de Ciencias Naturales y de Física. En la Tabla 3.13 se indica la distribución de puntos de red para el edificio Laboratorios.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total
Baja	Laboratorio de Bilogía	3	1	4
	Laboratorio de Química	2	1	3
Primer Piso	Laboratorio de Ciencias Naturales	3	1	4
	Laboratorio de Física	2	1	3
	Cámaras	4	-	4
	Laboratorios	2	-	2
TOTAL		**16**	**4**	**20**
			25% Crecimiento	5

Tabla 3.13 Distribución de puntos de red. Edificio de Laboratorios

3.5.2.4. Bloque Primeros y Segundos Cursos

En planta baja tenemos el Laboratorio de Computación de Primeros y Segundos Cursos. En el primer piso y segundo piso tenemos el Bloque de 7 Aulas en cada piso.

En la Tabla 3.14 se indica la distribución de puntos de red para el Bloque Primeros y Segundos Cursos.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total
Baja	Laboratorio de Computación Primeros y Segundos Cursos	39	1	40
Primer Piso	Bloque de Aulas	7	-	7
Segundo Piso	Bloque de Aulas	7	-	7
	Cámaras	1	-	1
	Access Point	1	-	1
TOTAL		**55**	**1**	**56**
			25% Crecimiento	14

Tabla 3.14 Distribución de puntos de red. Edificio Bloque de Aulas Primeros y Segundos Cursos

3.5.2.5. Bloque Terceros y Cuartos Cursos

En planta baja tenemos el Laboratorio de Computación de Terceros y Cuartos Cursos y el Bloque de Aulas de Terceros y Cuartos Cursos. En el primer piso tenemos el Laboratorio de Idiomas, Sala de Idioma Extranjero, Sala de francés y el Bloque de Aulas.

En la Tabla 3.15 se indica la distribución de puntos de red para el Bloque Terceros y Cuartos Cursos.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total
Baja	Laboratorio de computación Terceros y Cuartos Cursos	24	1	25
	Bloque de Aulas	7	-	7
Primer Piso	Laboratorio de Idiomas	39	-	39
	Sala de Idioma Extranjero	1	1	2
	Sala de Francés	1	1	2
	Bloque de Aulas	7	-	7
	Cámaras	2	-	2
	Access Point	2	-	2
TOTAL		**83**	**3**	**86**
			25% Crecimiento	21

Tabla 3.15 Distribución de puntos de red. Edificio Bloque de Aulas Terceros y Cuartos Cursos

3.5.2.6. Bloque Quintos y Sextos Cursos

En planta baja tenemos Bloque de Aulas de Quintos y Sextos Cursos. En el primer piso está el Laboratorio de Computación de Quintos y Sextos Cursos.
En la Tabla 3.16 se indica la distribución de puntos de red para el Bloque Quintos y Sextos Cursos.

Planta	Área de Trabajo	Puntos de Red	Puntos de Voz	Total

Baja	Bloque de Aulas	7	-	7
Primer Piso	Laboratorio de Computación Quintos y Sextos Cursos.	12	1	13
	Bloque de Aulas	7	-	7
	Cámaras	1	-	1
	Access Point	1	-	1
TOTAL		**28**	**1**	**29**
			25% Crecimiento	7

Tabla 3.16 Distribución de puntos de red. Edificio Bloque de Aulas Quintos y Sextos Cursos

En el Anexo C se presenta los puntos de red con su respectiva nomeclatura.

3.5.3. REQUERIMIENTOS DE LA INSTITUCIÓN

De acuerdo a la descripción en el capítulo 2, el Cableado Estructurado no posee ninguna topología, ni se rige a ninguna norma por lo que no se puede identificar adecuadamente los subsistemas que lo componen, en base a estas consideraciones es necesario su rediseño.

3.5.3.1. Cableado Horizontal

Primeramente se debe anotar que no se puede reutilizar la infraestructura existente del Sistema de Cableado Estructurado, puesto que el cableado no cumple con ninguna de las normas internacionales establecidas.

Partiendo de esto se concluye que para el cableado horizontal se utilizará cable UTP CAT 6, que comprende el tendido desde el área de trabajo hacia los switches de acceso. Esta recomendación se basa de acuerdo al análisis de tráfico del capítulo 2 y el cálculo de ancho de banda por aplicación de la tabla 3.7. Este medio de transmisión mejorará el rendimiento de la red para soportar voz, datos y video sin ningún inconveniente.

Para la asignación de puntos de red se tomo en cuenta un crecimiento total del 25% por áreas donde se cuenta con espacio suficiente para incrementar equipos de acuerdo a lo requerido.

3.6. Cálculo de la Longitud del Cable

Para la instalación de los puntos de voz, datos y cámaras se considera que se instalarán en un total de 273 puntos de red. Para el cálculo de los rollos de cable, se basa en la recomendación de la norma EIA/TIA 568C.2. Entre los aspectos más importantes a tomar en cuenta, es obtener la distancia mínima y máxima que recorrerá desde el cuarto de telecomunicaciones correspondiente hasta el área de trabajo, luego de lo cual se obtendrá el promedio.

Se contempla que la longitud de cable tiene 305 metros, esto es una medida estándar. El mínimo de puntos de red a instalarse para el cálculo de rollos de cable están descritos en las tablas del numeral 3.18. Se establece dejar un factor de holgura de 10% para contemplar el respectivo enrutamiento de subida y bajada hacia la salida de telecomunicaciones así como el gabinete.

Para el cálculo de la longitud promedio por punto, la fórmula a utilizarse sería

$$Lprom = \frac{Lmax + Lmin}{2} + 10\%\ holgura$$

A continuación, se presenta el cálculo de las distancias promedio de acuerdo a los planos del anexo D.

En la tabla 3.17 se indica el cálculo de las distancias promedio en cada una de las áreas de la Institución.

Área	Distancia Máxima [m]	Distancia Mínima [m]	Distancia Promedio [m]	Distancia Promedio + 10 % holgura [m]
Administrativo Planta baja	38.21	11.81	25.01	27.51
Administrativo Primer Piso	37.02	5.46	21.24	23.36
Departamental Planta Baja	46.48	11.62	29.05	31.95
Departamental Primer Piso	41.17	8.67	24.92	27.41
Laboratorios Planta Baja	25.97	10.96	18.46	20.30
Laboratorios Primer Piso	30.97	10.62	20.79	22.86
Bloque Primeros y Segundos Cursos Planta Baja	22.80	6.21	14.50	15.95
Bloque Primeros Y Segundos Cursos Primer Piso	84.80	11.54	48.17	52.98
Bloque Primeros y Segundos Cursos	89.96	21.55	55.75	61.32

Segundo Piso				
Bloque Terceros y Cuartos Cursos Planta Baja	69.71	8.74	39.22	43.14
Bloque Terceros y Cuartos Cursos Primer Piso	72.73	11.86	42.29	46.51
Bloque Quintos y Sextos Cursos Planta Baja	68.49	9.98	39.23	43.15
Bloque Quintos y Sextos Cursos Primer Piso	73.35	14.60	43.97	48.36

Tabla 3.17 Cálculo de las distancias promedio en cada una de las áreas

Determinadas las distancias promedio de las diferentes áreas, se calcula el número de corridas de cable que se van a tener por cada rollo, mediante la siguiente ecuación. Se tomará como ejemplo los valores del área administrativa en la planta baja.

$$\#\ de\ Corridas = \frac{longitud\ de\ cable\ por\ rollo}{distancia\ promedio} = \frac{305\ [m]}{27.51\ [m]} = 11.86$$

El valor calculado de la ecuación, se aproxima por debajo puesto existe un segmento del rollo de cable que no se utiliza, este segmento es el sobrante. Con este valor, finalmente se calcula el número de rollos a ser utilizados en cada área.

$$\#\ de\ Rollos = \frac{Número\ de\ puntos\ a\ instalar}{\#\ de\ corridas\ por\ rollo} = \frac{22\ [m]}{11\ [m]} = 2\ Rollos\ Administrativo\ Planta\ Baja$$

El valor que da como resultado esta ecuación se aproxima por arriba puesto que se desea obtener un número de rollos de valor entero. Los resultados del número de corridas por rollo, el número de puntos a instalarse (datos, voz y cámaras); además el número de rollos necesarios, se los puede observar en la tabla 3.18.

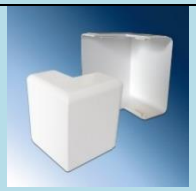
Área	Distancia Promedio + 10% holgura [m]	Número de corridas por rollo	Número de puntos a instalarse	Número de Rollos.
Administrativo Planta Baja	27.51	11	22	2
Administrativo Primer Piso	23.36	13	36	3
Departamental Planta Baja	31.95	9	11	2
Departamental Primer Piso	27.41	11	13	2
Laboratorios Planta Baja	20.30	15	8	1
Laboratorios Primer Piso	22.86	13	12	1
Bloque Primeros y Segundos Cursos Planta Baja	15.95	19	41	3
Bloque Primeros Y Segundos Cursos Primer	52.98	5	7	2

Piso				
Bloque Primeros y Segundos Cursos Segundo Piso	61.32	4	8	2
Bloque Terceros y Cuartos Cursos Planta Baja	43.14	7	33	5
Bloque Terceros y Cuartos Cursos Primer Piso	46.51	6	53	9
Bloque Quintos y Sextos Cursos Planta Baja	43.15	7	7	1
Bloque Quintos y Sextos Cursos Primer Piso	48.36	6	22	4

Tabla 3.18 Cálculo de las corridas de cable, número de puntos y rollos a ser utilizados por cada área.

Es imprescindible el uso de accesorios como se detallan en la tabla 3.19, para la instalación del cableado estructurado.

Accesorios	**Medidas**	**Gráfico**
Caja sobrepuesta de plástico		

Canaleta Plástica Decorativa	100 x 45 [2m] 60 x 40 [2m] 40 x 25 [2m]	
Angulo Interno	100 x 45 60 x 40 40 x 25	
Sección T para canaleta	100 x 45 60 x 40 40 x 25	
Jack CAT 6 Salida de telecomunicaciones		
Patch Panel CAT 6	24 puertos	
Face plate Doble		
Face Plate Simple		
Patch Cord UTP CAT 6		
Organizadores horizontales		

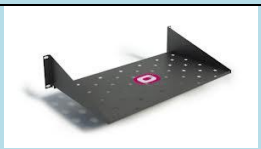
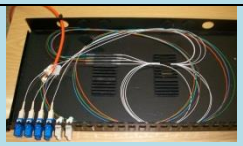
Tubo Conduit EMT	12,7 mm (1”) x 3m 25.4 mm (2”) x 3m	
Bandeja de Cables		
Rack cerrado de Piso	42	
Gabinetes abatibles de pared	12 18	
Bandeja de Fibra Óptica		
Patch Cord Fibra Óptica LC-SC		

Tabla 3.19 Accesorios necesarios para la instalación del Sistema de Cableado Estructurado

En las siguientes tablas se observa los diferentes elementos a utilizar en la red pasiva por cada Área del Colegio Experimental Juan Pío Montufar, se puede ver la descripción de los elementos a usar. En las cotizaciones del ANEXO E se muestra los precios de los materiales para la red pasiva.

En la tabla 3.20 se indica el resumen de materiales para la red pasiva del Edificio Administrativo.

Descripción	
Cable UTP CAT AWG 4 pares (1 Rollo)	5 rollos
Caja Sobrepuesta de 40 mm de plástico	
Canaleta Plástica Decorativa 100x45 2m	
Canaleta Plástica Decorativa 60x40 2m	
Canaleta Plástica Decorativa 40x25 2m	
Angulo Interno 100x45	
Angulo Interno 60x40	
Angulo Interno 40x25	
Sección T para canaleta 100x45	
Sección T para canaleta 60x40	
Sección T para canaleta 40x25	
Jack CAT 6 Salida de Telecomunicaciones	
Jack CAT 6 Patch Panel	
Face plate Doble	
Face plate Simple	
Patch Panel Modular de 24 puertos	
Patch Cord UTP 3 ft CAT 6	
Patch Cord UTP 7 ft CAT 6	
Organizadores horizontales	
Tubo Conduit EMT de (11/4”) x 3m	
Tubo Conduit EMT de (1”)x 3m	
Tubo Conduit EMT de (¾”) x 3m	
Gabinete Abatible de 18 UR	
CABLE Fibra Óptica Multimodo 50 125 um 6 HILOS (1 metro)	
Bandeja de Fibra Óptica SC	
Patch Cord Fibra Óptica LC-SC	

Tabla 3.20 Resumen de la red pasiva Edificio Administrativo

En la tabla 3.21 se indica el resumen de materiales para la red pasiva del Edificio Departamental.

Descripción	
Cable UTP CAT 6 23 AWG 4 PARES 1 Rollo	4 rollos
Caja sobrepuesta de 40 mm de plástico	
Canaleta Plástica Decorativa 100x45 2m	
Canaleta Plástica Decorativa 60x40 2m	
Canaleta Plástica Decorativa 40x25 2m	
Angulo Interno 100x45	
Angulo Interno 60x40	
Angulo Interno 40x25	
Sección T para canaleta 100x45	
Sección T para canaleta 60x40	
Sección T para canaleta 40x25	
Jack CAT 6 Salida de telecomunicaciones	
Jack CAT 6 Patch Panel	
Face plate Doble	
Face plate Simple	
Patch Panel Modular de 24 puertos	
Patch Cord UTP 3 ft CAT 6	
Patch Cord UTP 7 ft CAT 6	
Organizadores horizontales	
Tubo Conduit EMT de (11/4”) x 3m	
Tubo Conduit EMT de (1”) x 3m	
Tubo Conduit EMT de (3/4) x 3m	
Gabinete Abatible de 18 UR	
Cable Fibra optica Multimodo 50/125 um 6 HILOS (1 metro)	
Bandeja de Fibra Optica SC	
Patch Cord Fibra Optica LC- SC	

Tabla 3.21 Resumen de la red pasiva Edificio Departamental

En la tabla 3.22 se indica el resumen de materiales para la red pasiva del Edificio Laboratorios.

Descripción	
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	2 rollos
Caja sobrepuesta de 40 mm de plástico	
Canaleta Plástica Decorativa 40x25 2m	
Angulo Interno 40x25	
Sección T porta canaletas 40x25	
Jack CAT 6 Salida de telecomunicaciones	
Jack CAT 6 Patch Panel	
Face plate Doble	
Face plate Simple	
Patch Panel Modular de 24 puertos	
Patch Cord UTP 3 ft CAT 6	
Patch Cord UTP 7 ft CAT 6	
Organizadores Horizontales	
Tubo Conduit EMT DE (¾”) x 3m	
Gabinete Abatible de 12 UR	
Bandeja de Fibra Óptica SC	
PATCH Cord Fibra Óptica LC.SC	

Tabla 3.22 Resumen de la red pasiva Edificio Laboratorios

En la tabla 3.23 se indica el resumen de materiales para la red pasiva del Bloque Primeros y Segundos Cursos.

Descripción	
Cable UTP CAT 623 awg 4 pares (1 Rollo)	7 rollos
Caja sobrepuesta de 40mm de plástico	
Canaleta Plastica Decorativa 40x25m	
Angulo Interno 40x25	
Sección T porta canaleta 40x25	
Jact CAT 6 Salida de telecomunicaciones	

Jack CAT 6 Patch Panel
Face plate Doble
Face Plate Simple
Patch Panel Modular de 24 puertos
Patch Cord UTP 3 ft CAT 6
Patch Cord UTP 7 ft CAT 6
Organizadores Horizontales
Tubo Conduit EMT DE (1 ¼”) x 3m
Gabinete Abatible de 12 UR
Cable Fibra óptica Multimodo 50/125 um 6 Hilos (1 metro)
Bandeja de Fibra Optica SC
PATCH Cord Fibra óptica LC.SC

Tabla 3.23 Resumen de la red pasiva del Bloque Primeros y Segundos Cursos

En la tabla 3.24 se indica el resumen de materiales para la red pasiva del Bloque Terceros y Cuartos Cursos.

Descripción	
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	14 rollos
Caja sobrepuesta de 40mm de plástico	
Canaleta Plástica Decorativa 40x25 2m	
Angulo Interno 40x25	
Jack CAT 6 Salida de telecomunicaciones	
Jack CAT 6 Patch Panel	
Face plate Doble	
Face plate Simple	
Patch Panel Modular de 24 puertos	
Patch Cord UTP 3 FT CAT 6	
Patch Cord UTP 7 FT CAT 6	
Organizadores Horizontales	
Tubo Conduit EMT de (11/4”) x 3m	

Tubo Conduit EMT de 34 x 3m
Gabinete Abatible de 18 UR
Bandeja de Fibra Óptica SC
Patch Cord Fibra Óptica LC.SC

Tabla 3.24 Resumen de la red pasiva del Bloque Terceros y Cuartos Cursos

En la tabla 3.25 se indica el resumen de materiales para la red pasiva del Bloque Quintos y Sextos Cursos.

Descripción	
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	5 rollos
Caja sobrepuesta de 40mm de plástico	
Canaleta Plástica Decorativa 40x25 2m	
Angulo Interno 40x25	
Jack CAT 6 Salida de telecomunicaciones	
Jack CAT 6 Patch Panel	
Face plate Doble	
Face plate Simple	
Patch Panel Modular de 24 puertos	
Patch Cord UTP 3 FT CAT 6	
Patch Cord UTP 7 FT CAT 6	
Organizadores Horizontales	
Tubo Conduit EMT de (11/4”) x 3m	
Tubo Conduit EMT de 34 x 3m	
Gabinete Abatible de 18 UR	
Bandeja de Fibra Optica SC	
Patch Cord Fibra óptica LC.SC	

Tabla 3.25 Resumen de la red pasiva del Bloque Quintos y Sextos Cursos

3.6.1. Cableado Vertical. (Backbone)

Para este subsistema se desarrollará un esquema jerárquico en estrella con dos niveles de interconexión, la fibra recorrerá desde los switches en cada una de las áreas hasta los switches del core.

El cable a utilizarse será fibra óptica multimodo de 50/125 (micrometros) um de 6 hilos. Por cada enlace se debe considerar los siguientes aspectos, cada enlace utiliza 2 hilos, uno para transmisión y otro para recepción; además se debe considerar el doble de hilos para redundancia.

A continuación se muestra la cantidad de fibra óptica multimodo que se utilizará para el backbone con un 25% de holgura.

En la tabla 3.26 se indica las Medidas de Fibra óptica para Backbone.

RUTA	**Cantidad [m]**	**Holgura 25% [m]**
Ruta A Edificio Administrativo – Bloque Primeros y Segundos Cursos	40	50
Ruta B Edificio Administrativo – Bloque Quitos y Sextos Cursos	110	138
Ruta C Edificio Administrativo – Bloque Terceros y Cuartos Cursos	140	175
Ruta D Edificio Administrativo – Edificio Laboratorios	168	210
Ruta E Edificio Administrativo – Edicifico Depertamental	87	109

Tabla 3.26 Medidas de Fibra öptica para Backbone

Considerando esto, por cada enlace se necesita fibra óptica de 6 hilos de los cuales serán utilizados 4 hilos con lo que los dos hilos restantes estarían disponibles para futuras expansiones del servicio de la red, algún corte o algún problema con alguno de los hilos.

El tener enlaces de fibra de 6 hilos brinda independencia de cada uno de los enlaces, o que brinda un nivel de seguridad adicional a la red, protegiendo al backbone de algún tipo de intrusión o daño que pueda suceder.
Entre los factores para la elección de fibra óptica como medio de transmisión para backbone, se puede mencionar:

- Debido a las distancias que en algunos casos exceden los 100 metros que se considera para medios de transmisión de cobre.
- Para proteger el medio de transmisión, debido a que en su mayor parte estos enlaces atraviesan áreas abiertas que están expuestas a condiciones ambientales variantes y que serían puntos vulnerables en la red.
- El uso de fibra óptica para la interconexión de los switches, evitará que se generen cuellos de botella en la red y optimizará el rendimiento; además que en un sistema de backbone las velocidades se ajustan al enlace de menor capacidad por lo que es preferible tener el mismo sistema de transmisión en los enlaces.
- El cableado vertical se rige bajo la norma EIA/TIA 569-C.3, que especifica el cableado con fibra óptica. La fibra óptica a utilizarse debe ser protegida para ambientes externos, el enrutamiento de la fibra óptica será a través de tubería, de esta forma se protege que el medio transmisor sea manipulado por personas ajenas o sufra algún problema.
- La distancia máxima a cubrir con este medio de transmisión será de 300 metros con lo cual si se observa la tabla 3.27, la fibra deberá tener un diámetro de 50 micrones para soportar un ancho de banda de 1 Gbps. Debido a esta información la fibra óptica deberá ser multimodo 1000 Base SX en la ventana de 850 (nanometros) nm.

En la tabla 3.27 se indica los Parámetros Giga Ethernet para ancho de banda fibra óptica.

Características	1000 Base-SX	1000 Base-LX			
Longitud de onda	850	1300			
Tipo de FO	62,5	50	62,5	50	Monomodo
Ancho de Banda [MHz/Km]	160-200	400-500	500	400-500	s/d
Distancia [m]	220-275	500-550	550	550	5000
Pérdida del link [dB]	3,2-3,2	3,4-3,9	4	2,4-3,5	4,7

Tabla 3.27 Parámetros Giga Ethernet para ancho de banda fibra óptica.

3.6.1.1. Cuarto de Telecomunicaciones

En Colegio cuenta con área física muy extensa por lo que es necesario ubicar varios Cuartos de Telecomunicaciones en cada una de las áreas para brindar un acceso a todos los usuarios de la red, puesto que en la Norma EIA/TIA 569-C, se recomienda que la distancia máxima desde los Cuartos de Telecomunicaciones hasta la estación de trabajo no debe sobrepasar los 100 metros, incluidos los patch cords.

La Sala de Equipos se localiza en el primer piso del Edificio Administrativo, siendo este el punto central al cual los diferentes Cuartos de Telecomunicaciones de todo el campus se conectarán. A continuación, en la tabla 3.28, se detalla la ubicación de los Cuartos de Telecomunicaciones a través del campus.

En la tabla 3.28 se indica la Ubicación de Salas de Equipos en cada una de las Áreas.

ÁREA		UBICACIÓN CUARTOS DE TELECOMUNICACIONES
Administrativa	Colecturía	Planta Baja
	Sistemas	Primer Piso
Departamental	Departamento Médico	Planta Baja
	Inspección General	Primer Piso
Laboratorios	Laboratorio de Química	Planta Baja
	Laboratorio de Ciencias Naturales	Primer Piso

Bloque Primeros y Segundos Cursos	Laboratorio de Computación Primeros y Segundos Cursos	Planta Baja
	Aula	Primer Piso
	Aula	Segundo Piso
Bloque Terceros y Cuartos Cursos	Aula	Planta Baja
	Aula	Primer Piso
Bloque Quintos y Sextos Cursos	Aula	Planta Baja
	Aula	Primer Piso

Tabla 3.28 Ubicación de Salas de Equipos en cada una de las Áreas

El Cuarto de Telecomunicaciones es un espacio centralizado de uso específico para el equipo de telecomunicaciones, terminaciones mecánicas y el cableado de interconexión. Las características de un cuarto de telecomunicaciones deben cumplir la norma EIA/TIA 568-C.

Para el dimensionamiento de los closets se tomará en cuenta las medidas en unidades (U) para cada elemento, como se detalla en la tabla 3.29. Además, se debe considerar que los equipos no se pueden colocar montados por lo que se debe dejar espacio que permita la libre circulación del aire para que los equipos trabajen con una temperatura adecuada.

Adicionalmente, es recomendable dejar un espacio de crecimiento de 4 U[42] unidades para la ubicación de nuevos equipos si así lo requiere el crecimiento del Colegio.

En la tabla 3.29 se indica el Dimensionamiento del Closet de Telecomunicaciones.

ÁREA	ELEMENTO	CANTIDAD	UNIDADES (U)
DEPARTAMENTAL	Switch de Acceso 48p	1	1
	Organizador horizontal	2	4
	Organizador vertical	2	0
	Patch Panel Fibra Óptica	1	1
	Patch Panel 48p	1	2

[42] U: unidad rack es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 pulgadas de ancho.

	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	4	4
TOTAL			**15**
LABORATORIOS	Switch de Acceso 48p	1	1
	Organizador horizontal	2	4
	Organizador vertical	2	0
	Patch Panel Fibra Óptica	1	1
	Patch Panel 48p	1	2
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	4	4
TOTAL			**15**
BLOQUE PRIMEROS Y SEGUNDOS CURSOS	Switch de Acceso 48p	2	2
	Organizador horizontal	2	4
	Organizador vertical	2	0
	Patch Panel Fibra Óptica	1	1
	Patch Panel 48p	2	4
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	4	4
Total			**18**
BLOQUE TERCEROS Y CUARTOS CURSOS	Switch de Acceso 48p	2	2
	Switch de Acceso 24p	1	1
	Organizador horizontal	3	6
	Organizador vertical	2	0
	Patch Panel Fibra Óptica	1	1
	Patch Panel 48p	2	4
	Patch Panel 24p	1	2
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	4	4
TOTAL			**23**
BLOQUE QUINTOS Y SEXTOS CURSOS	Switch de Acceso 48p	1	1
	Organizador horizontal	1	2
	Organizador vertical	2	0
	Patch Panel Fibra Óptica	1	1

	Patch Panel 48p	1	2
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	4	4
TOTAL			**13**

Tabla 3.29 Dimensionamiento del Closet de Telecomunicaciones

3.6.1.2. Sala de Equipos

Este subsistema está ubicado en el departamento administrativo y deberá cumplir con las especificaciones de acuerdo a las normas ANSI/TIA/EIA 568-B y ANSI/TIA/EIA 569-A.

En el cuarto de equipos se utilizara un rack abierto con sus respectivos organizadores horizontales y verticales, este rack tiene mayor tamaño de los detallados anteriormente, las características se las detalla en la tabla 3.30.
Para el diseño de este rack se debe considerar si es el caso, servidores y otros dispositivos utilizados en el cuarto de equipos.
En la tabla 3.30 se indica el Dimensionamiento para el rack del cuarto de equipos.

ÁREA	ELEMENTO	CANTIDAD	UNIDADES (U)
ADMINISTRATIVO	Switch de Core 1 24p	1	1
	Switch de Core 2 24p	1	1
	Switch de Acceso 48p	1	1
	Switch de Acceso 24p	1	1
	Organizador horizontal	7	14
	Organizador vertical	2	0
	Patch Panel Fibra Óptica 24p - ODF	2	2
	Patch Panel 48p CAT 6	1	2
	Patch Panel 24p CAT 6	7	7
	Panel de Alimentación AC	2	2
	Servidores	3	8
	Crecimiento	2	2
TOTAL			**41**

Tabla 3.30 Dimensionamiento para el rack del cuarto de equipos.

3.6.1.3. Área de Trabajo

El área de trabajo comprende el recorrido desde la salida de telecomunicaciones o Faceplate hasta llegar al equipo final de usuario. El área de trabajo comprende principalmente computadores, impresoras, teléfonos entre otros.
Cada área de trabajo constara de una salida doble de telecomunicaciones, una para datos y otra para voz, o una simple para datos de acuerdo a las necesidades del usuario.

En los ambientes como son laboratorios dentro de la institución se ubicarán puntos dobles, debido a que un punto de datos será para uso exclusivo de los docentes y como requerimiento del instituto se debe disponer una extensión telefónica. Los faceplates deben tener conectores hembras RJ45, y también deben soportar etiquetas individuales para su correcta administración. Los faceplates se ubicaran a una distancia de 40 cm medidos desde el suelo, para evitar posibles daños.

La conectorización de los equipos en las áreas de trabajo a un punto de red sea esta voz o datos, se la realizara mediante un patch cord certificado CAT 6 de tres metros de longitud. La terminación de estos debe ser de acuerdo a la norma T568B.
Ninguno de los patch cords existentes en la red del Colegio cumple con las normas, por lo cual es necesario el cambio de los actuales. De igual forma los patch cords para la interconexión entre equipos de networking[43] y patch panels en los Cuartos de Telecomunicaciones, deberán ser certificados tanto para cable UTP CAT 6, como para la fibra óptica multimodo.

3.6.1.4. Canalizaciones y enrutamiento

De acuerdo a la inspección de la infraestructura de las oficinas, aulas, y laboratorios, se establece que las canalizaciones más adecuadas en estos espacios es utilizar canaletas decorativas. Toda la ductería superficial para el

cableado vertical y horizontal se debe instalar previamente, siguiendo la norma EIA/TIA 569A.

Las canaletas decorativas deben contener los elementos necesarios para los montajes de curvas, dando cumplimiento así a la norma establecida. Todas las canaletas que bajen desde el tumbado de las aulas, laboratorios y oficinas serán plásticas y retardantes al fuego. En los planos del cableado estructurado correspondiente al ANEXO D se especifica la ruta a seguir para la conexión, y más adelante, se detalla la cantidad y características tanto de las canaletas y accesorios a utilizarse.

3.6.1.5. Etiquetado

Se rige bajo el estándar EIA/TIA 606, que norma la correcta y adecuada identificación de cada uno de los Subsistemas de Cableado Estructurado. El etiquetado será en ambos extremos del cable, en los faceplates y en los patch panels de los Cuartos de Telecomunicaciones.
Los cables que conectan el subsistema de cableado horizontal y vertical debe ser rotulados con una etiqueta sobre el conductor para conocer a que patch panel y área pertenece. Las etiquetas del faceplate y del patch panel serán adhesivas.

Para diferenciar la salida de datos de la de voz, se recomienda establecer el siguiente formato para reconocer a que rack de telecomunicaciones está conectado dependiendo del área en la que se que se encuentra.

En la tabla 3.31 se indica el Etiquetado del cableado para las diferentes Áreas.

Área	**Identificación**
Administrativo	A
Departamental	D
Laboratorios	L
Bloque Primeros y Segundos Cursos	PS
Bloque Terceros y Cuartos Cursos	TC

Bloque Quintos y Sextos Cursos	QS

Tabla 3.31 Etiquetado del cableado para las diferentes Áreas.

Luego se procede a identificar al patch panel al cual se encuentra conectado el punto de red en el correspondiente rack de telecomunicaciones, en forma descendente de arriba hacia abajo.

Después se realiza el etiquetado del puerto al cual está conectado en el patch panel y finalmente determinar si se trata de un punto de voz o de datos. En la figura 3.7, se muestra un ejemplo que explica en detalle la identificación.

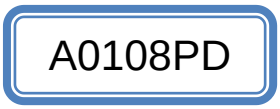


Figura 3.7 Ejemplo de identificación de un punto de red

- **A:** Área Administrativo.
- **01:** pertenece al Patch Panel 1 del Área antes mencionada.
- **08:** Puerto al que se conecta en el Patch Panel.
- **PD:** Punto de Datos.
- **PV:** Punto de Voz

Este esquema de etiquetación se propone para los puntos de voz y datos, además que permite al administrador identificar fácilmente y detectar posibles fallas en lo concerniente al cableado.

Una vez terminada la instalación del Sistema de Cableado Estructurado, es importante que una empresa certifique todos los puntos de red, a través del equipo diseñado para el efecto. El equipo certificador debe presentar un informe detallado indicando los principales parámetros tomando en consideración los mismos que garantizan el correcto desempeño de la red multiservicios.

Para realizar toda la etiquetación se va a utilizar la siguiente identificación para cada área de trabajo la cual se detalla a continuación:

En la tabla 3.32 se indica la Identificación de los departamentos de la CEJPM.

Departamento	Identificación
Biblioteca	BI
Colecturía	CO
Guarda-Almacen	GA
Bodegas	BO
Secretaria General	SG
Salon de Actos	SA
Rectorado	RE
Secretarias	SE
Sistemas	SI
Vicerrectorado	VI
Secretaria Vicerrectorado	SV
DOBE	DB
Sub-Inspección	SI
Departamento Médico	DM
Sala de Música	SM
Departamento de Cultura Física	DCF
Sala Lectura Profesores	SP
Inspección General	IG
Depertamento Mejoramiento de la Calidad de la Educación	DME
Laboratorio de Biología	LB
Laboratorio de Química	LQ
Laboratorio de CCNN	LC
Laboratorio de Física	LF

Tabla 3.32 Identificación de los departamentos de la CEJPM.

En el **ANEXO C,** se detalla la ubicación de todos los puntos de datos y de voz con su respectiva nomenclatura.

3.6.2. PRUEBAS DE CERTIFICACIÓN [19]

Para garantizar un correcto funcionamiento de la red LAN se debe realizar pruebas del cableado tanto vertical como horizontal.

La norma TIA/EIA TSB-67 es utilizada para especificaciones de rendimiento de transmisión para pruebas de campo solo para el medio de transmisión UTP. Dicha norma específica las siguientes pruebas.

- Mapa de Alambrado
- Longitud.
- Atenuación
- Pérdidas de Inserción
- Next.
- PS Next
- ELFext
- PS ELFext
- Pérdidas por Retorno.
- Tiempo de Propagación.

En la figura 3.7 se especifica los valores mínimos aceptados para realizar las pruebas a realizarse de cable de cobre de 4 pares a 250 MHz

En la figura 3.8 se indica los Valores mínimos aceptables para realizar las pruebas en cable UTP CAT 6.

Category 6 Permanent Link

Frequency (MHz)	Insertion Loss (dB)	NEXT* (dB)	PSNEXT (dB)	ELFEXT* (dB)	PSELFEXT (dB)	Return Loss (dB)
1.0	1.9	65.0	62.0	64.2	61.2	19.1
4.0	3.5	64.1	61.8	52.1	49.1	21.0
8.0	5.0	59.4	57.0	46.1	43.1	21.0
10.0	5.5	57.8	55.5	44.2	41.2	21.0
16.0	7.0	54.6	52.2	40.1	37.1	20.0
20.0	7.9	53.1	50.7	38.2	35.2	19.5
25.0	8.9	51.5	49.1	36.2	33.2	19.0
31.25	10.0	50.0	47.5	34.3	31.3	18.5
62.5	14.4	45.1	42.7	28.3	25.3	16.0
100.0	18.6	41.8	39.3	24.2	21.2	14.0
200.0	27.4	36.9	34.3	18.2	15.2	11.0
250.0	31.1	35.3	32.7	16.2	13.2	10.0

Category 6 Permanent Link

Maximum Cat 6 permanent link propagation delay: less than 498 ns at 10 MHz

Maximum Cat 6 permanent link delay skew: less than 44 ns/100 m at 10 MHz

Category 6 Channel

Frequency (MHz)	Insertion Loss (dB)	NEXT* (dB)	PSNEXT (dB)	ELFEXT* (dB)	PSELFEXT (dB)	Return Loss (dB)
1.0	2.1	65.0	62.0	63.3	60.3	19.0
4.0	4.0	63.0	60.5	51.2	48.2	19.0
8.0	5.7	58.2	55.6	45.2	42.2	19.0
10.0	6.3	56.6	54.0	43.3	40.3	19.0
16.0	8.0	53.2	50.6	39.2	36.2	18.0
20.0	9.0	51.6	49.0	37.2	34.2	17.5
25.0	10.1	50.0	47.3	35.3	32.3	17.0
31.25	11.4	48.4	45.7	33.4	30.4	16.5
62.5	16.5	43.4	40.6	27.3	24.3	14.0
100.0	21.3	39.9	37.1	23.3	20.3	12.0
200.0	31.5	34.8	31.9	17.2	14.2	9.0
250.0	35.9	33.1	30.2	15.3	12.3	8.0

Category 6 Channel

Maximum Cat 6 channel propagation delay: less than 555 ns at 10 MHz

Maximum Cat 6 channel delay skew: less than 50 ns/100m at 10 MHz

Category 6 Connecting Hardware

Frequency (MHz)	Insertion Loss (dB)	NEXT (dB)	FEXT (dB)	Return Loss (dB)
1.0	0.10	75.0	75.0	30.0
4.0	0.10	75.0	71.1	30.0
8.0	0.10	75.0	65.0	30.0
10.0	0.10	74.0	63.1	30.0
16.0	0.10	69.9	59.0	30.0
20.0	0.10	68.0	57.1	30.0
25.0	0.10	66.0	55.1	30.0
31.25	0.11	64.1	53.2	30.0
62.5	0.16	58.1	47.2	28.1
100.0	0.20	54.0	43.1	24.0
200.0	0.28	48.0	37.1	18.0
250.0	0.32	46.0	35.1	16.0

Category 6 Connecting Hardware

Figuras 3.8 Valores mínimos aceptables para realizar las pruebas en cable UTP CAT 6.

3.7. DISEÑO DE LA RED ACTIVA

3.7.1. DISEÑO LÓGICO DE LA RED

El alcance propuesto para la red de comunicaciones del Colegio Juan Pío Montúfar, es utilizar tecnología tipo Giga Ethernet para el backone en la topología en estrella, que interconecta las diferentes áreas del campus. Y para los enlaces de acceso a las computadoras y teléfonos IP se utilizará tecnología tipo Ethernet Conmutada a 100 Mbps.

Debido al extenso campus del Colegio se agrupó en 6 Áreas para formar los enlaces de fibra óptica con el Switch de Core, estas áreas son: Administrativo, Departamental, Laboratorios, Bloque Primeros y Segundos Cursos, Bloque Terceros y Cuartos Cursos, Bloque Quintos y Sextos Cursos.

Todas estas conexiones desde los switches de core a cada una de las seis áreas serán mediante fibra óptica multimodo.

A continuación indica el gráfico de la red propuesta para el Colegio Experimental Juan Pío Montúfar.

En la figura 3.9 se indica el esquema de red propuesta.

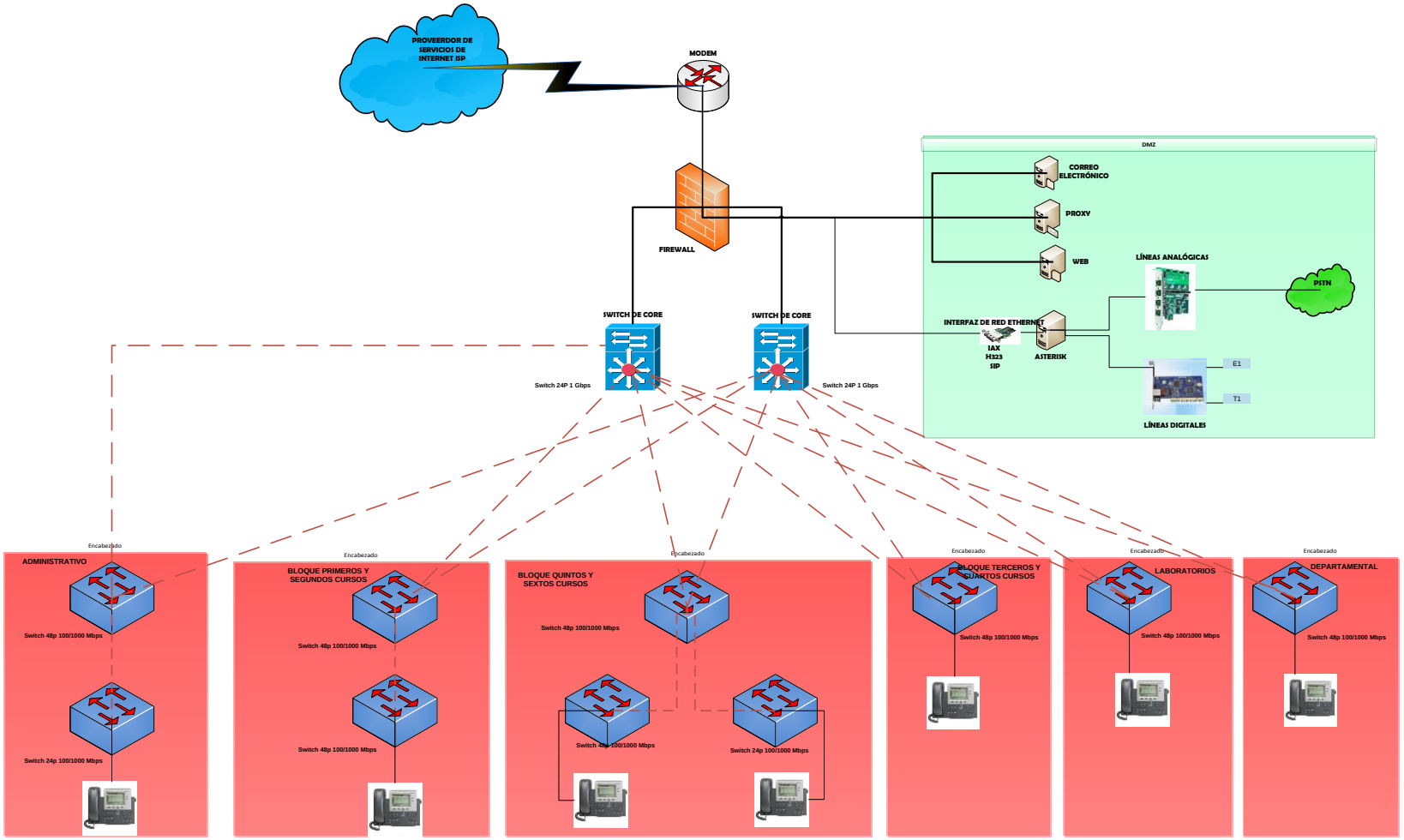


Figura 3.9 Topología de la Red De Comunicaciones.

Mediante este esquema se tiene dos switch de core de iguales características, los que proporcionarán balanceo de carga entre los enlaces y redundancia en caso de falla.

Estos equipos serán los encargados de procesar toda la información y direccionarla de una forma adecuada a los dispositivos finales. Estos equipos proveerán características de capa 3, además de contar con doble fuente de poder.

3.7.2. DMZ

La zona desmilitarizada brinda seguridad a los usuarios de la red, asignándoles niveles de confianza. Para este diseño se considera la DMZ, ya que los usuarios internos y externos necesitarán acceder a los servicios del Colegio. Con lo cual la granja de servidores (DNS, Servidor de Notas, Web, Correo Electrónico, etc) se establece una red separada para no comprometer la seguridad de la información y de los equipos internos.

Puesto que la DMZ contiene los servidores que brindan toda la información a los usuarios, la solución de firewall puede ser implementada tanto en hardware como en software, por lo que se decide aplicar una tecnología basada en hardware, con un equipo especializado en seguridad, debido a las prestaciones más altas que ofrece un dispositivo de estas características.

Este dispositivo bloqueará y filtrará el tráfico en función de las cabeceras de los paquetes; además filtrará los paquetes por estado de conexión, es decir tomará en consideración los datos de la capa aplicación, examinando todo el flujo de datos y verificando con las políticas permisivas o restrictivas de seguridad a implemenarse. Mediante el uso de este equipo se optimizará el acceso de los usuarios a las aplicaciones que necesiten evitando los riesgos de seguridad y los cuellos de botella.

3.7.2.1. VLANs

Las VLANs permiten crear redes de forma lógica y no física, reduciendo con esto el tamaño de los dominios de difusión, mejorando así la administración de los recursos prestados por una red.

Para tener un control óptimo, mejorar la gestión y administración de la red se crearán varias VLANs. De acuerdo al tipo de información que comparten en común cierto grupo de usuarios.
Las VLANs que se crearán están detalladas a continuación:

- Administración

  Es cualquier vlan que el administrador configura para acceder a la administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración.

- Telefonía IP

  Incluye todos los usuarios que tienen una extensión telefónica. El número de usuarios que pertenecen a esta VLAN son 40.

- Cámaras

  Está conformada por todas las cámaras instaladas en puntos estratégicos del CEJPM, consta de 14 usuarios.

- Educativo

  Está conformada por los laboratorios y la biblioteca para prestar servicio al área estudiantil, consta de 219 estaciones de trabajo disponibles.

- Servidores

Esta VLAN es la más importante para evitar que usuarios no autorizados tengan acceso a los servidores. Los cuales son aproximadamente 8.

- Visitantes

Esta VLAN es creada para todos los visitantes que se conecten a la red de forma inalámbrica.

3.7.2.2. Direccionamiento IP

En el Colegio existirán 273 puntos de red divididos en puntos de voz, datos y video, los cuales servirán para conectar PCs, teléfonos, cámaras IP, etc. Por lo cual se decide utilizar VLSM (Máscaras de subred de longitud variable), además para el todo el direccionamiento se establece una dirección clase A privada que es la 10.93.2.0 255.255.255.0

Una vez definidas las VLANs principales que se deben crear en el Colegio y con el número de usuarios que pertenecen a cada una de éstas, se realiza el direccionamiento IP.

La CEJPM estará conformada por 6 VLANs. Las que permitirán proporcionar cierta clase de seguridad a los datos. Además, posibilitan la agrupación de dispositivos de red en una misma subred independientemente de que se encuentren o no en el mismo sector físico.

En la tabla 3.33 se detalla las direcciones IP para cada subred y la asignación a cada VLAN.

VLAN	Nombre de Vlan	Subred	1° Dir. IP	Ult. Dir. IP	Broadcast	Mask Subred
Administración	**JPMADM**	**10.93.1.0**	10.93.1.1	10.93.1.254	10.93.1.255	255.255.255.0
Educativo	**JPMEDU**	**10.93.2.0**	10.93.2.1	10.93.2.254	192.168.2.255	255.255.255.0
Telefonía	**JPMTELEFONIA**	**10.93.3.0**	10.93.3.1	10.93.3.62	10.93.3.63	255.255.255.192
Cámaras	**JPMCAMARAS**	**10.93.3.64**	10.93.3.65	10.93.3.78	10.93.3.79	255.255.255.240
Servidores	**JPMSERVIDORES**	**10.93.3.80**	10.93.3.81	10.93.3.94	10.93.3.95	255.255.255.240
Visitantes	**JPMVISITAS**	**10.93.4.0**	10.93.4.1	10.93.4.254	10.93.4.255	255.255.255.0

Tabla 3.33 Asignación de direcciones IP

La primera dirección IP de cada rango de host válidos se designa como dirección para el default Gateway.

Adicionalmente, en la tabla 3.34 se detalla la cantidad de direcciones IP designadas a cada VLAN considerando las direcciones IP que están libres para uso futuro.

VLAN	Cantidad de Direcciones IP			
	Totales	Utilizadas	Libres	% Utilización
Educativo	**253**	219	34	86.56%
Telefonía	**64**	40	24	62.5%
Cámaras	**16**	14	2	87.5%
Servidores	**16**	8	8	50%
Administración	**253**	12	241	4.74%

Tabla 3.34 Asignación de direcciones IP por VLAN Utilizadas y Libres

3.7.3. DISEÑO DE LA RED PARA DATOS

Para realizar el diseño de la red de datos se consideran los equipos de Internetworking, servidores y estaciones de trabajo que estarán conectados a la red interactuando entre sí para brindar un servicio de eficiente al usuario final.

3.7.3.1. Estaciones de trabajo

Las estaciones de trabajo son los dispositivos que interactúan de forma directa con los usuarios de la red, los cuales acceden a todos los servicios que presta la red mediante estos dispositivos.

En el capítulo 2, se menciona que todos los equipos utilizan el Sistema Operativo Windows en sus diferentes versiones con sus respectivas aplicaciones de acuerdo al grupo de usuarios al que pertenezca.

3.8. EQUIPOS DE CONECTIVIDAD

Para la elección del switch se tomará en cuenta dos parámetros técnicos tales como: velocidad de backplane y protocolos de la red.
Para calcular el backplane de los switch se considera el número de puertos y la velocidad que tenga cada uno de ellos. Es decir, para un switch de 24 puertos con una velocidad de 100 Mbps y 2 puertos Full dúplex a 1000 Mbps, para este caso el backplane de ser de (24x100 Mbps + 2x1000 Mbps)(2) = 8.8 Gbps.

Las características a enumerar son especialmente para que los equipos de conmutación trabajen en capa dos y tres. Los puertos de los switches deberán ser de tecnología Ethernet conmutada a 10/100/1000 Mbps, que permitan que cualquier dispositivo que se conecte al switch, sense la interfaz y negocie automáticamente el método de intercambio de información. Algunos equipos necesitan de puertos con módulos de fibra óptica.

Los switches deben soportar ciertos protocolos de red de acuerdo al nivel de capa de red al que pertenezcan, para este caso en particular capa de acceso y de core, los protocolos se detallan a continuación.

- RIP (Routing Information Protocol): Es un protocolo de enrutamiento que permite intercambiar información sobre redes IP.
- OSPF (Open Shortest Path First): Es un protocolo de enrutamiento que permite determinar la ruta más corta.
- RMON (Remote Monitoring): Este protocolo permite monitorizar los switch de forma remota.
- DHCP (Dynamic Host Configuration Protocol): Es utilizado para asignar de forma dinámica las direcciones IP en la red.
- STP (Spanning Tree Protocol): Este protocolo es utilizado para activar o desactivar de forma automática enlaces redundantes para no generar bucles locales en la red.
- RSTP (Rapid Spanning Tree Protocol): Es una variante del protocolo STP por lo que realiza las mismas funciones a diferencia que utiliza un menor

tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

- TELNET (Telecommunication Network): Permite la administración remota de los switches.
- $SNMP_{V\ (1,2,3)}$ (Simple Network Management Protocol): Es un protocolo utilizado para administrar la red

3.8.1. CARACTERÍSTICAS DE LOS SWITCHES DE ACCESO

Después de realizar un análisis de requerimientos en el CEJPM, se determinó que se requiere 273 puntos de red, se recomienda utilizar 2 switches de acceso de 24 puertos, 8 switches de acceso de 48 puertos y 2 switches de distribución de 24 puertos.

Este dispositivo es el encargado de conectar todos los host, teléfonos IP, cámaras IP, impresoras entre otros por lo que debe tener varios puertos para interconectar todo los equipos presentes en el CEJPM.
Las características que deben tener los switches de acceso están detalladas en la tabla 3.35.

	CARACTERÍSTICAS
Switch de Acceso	· 24 / 48 puertos *de* 10/100 Mbps full dúplex · 4 puerto de fibra óptica Giga Ethernet · Auto negociación de la velocidad de los puertos · Apilable · Administrable mediante consola o vía interfaz Web · Conmutación a nivel de capa 2 · Debe soportar el protocolos IP, STP, RSTP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional) · Soporte de VLANs IEEE 802.1q · Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC. · Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. · Velocidad de backplane mínima de 8.8 Gbps · IP versión 4 y 6 · Soporte de 8000 direcciones MAC · Soporte de paquetes de telefonía IP (VoIP) · PoE norma IEEE 802.3af

Tabla 3.35 Características de los Switch de Acceso

3.8.2. CARACTERÍSTICAS DE LOS SWITCH DE DISTRIBUCIÓN.

Estos dispositivos son los encargados de recoger los datos de los switches de capa de acceso y retransmitirlos a la capa núcleo, admiten funciones de capa 3. Las características técnicas están detalladas en la tabla 3.36.

	CARACTERÍSTICAS
Switches de Core	· 24 puertos *de* fibra óptica · Auto negociación de la velocidad de los puertos · Apilable · Administrable mediante consola o vía interfaz Web · Conmutación a nivel de capa 2, 3 y 4 · Debe soportar el protocolos IP, STP, RSTP, RIPv1 y 2, DHCP, Telnet y $SNMP_{V\ (1,\ 2\ y\ 3)}$, $OSPF_{V\ (2\ y\ 3)}$, $RMON_{V\ (2\ y\ 3)}$ entre Otros. · Manejo y Administración de VLANs IEEE 802.1q · Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL) a nivel 2, 3 y 4, prevención mediante (DoS) y filtrado basado en MAC. · Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. · Velocidad de backplane mínima de 88 Gbps · IP versión 4 y 6 · Manejo, priorización y clasificación de tráfico VoIP

Tabla 3.36 Características de los Switches de Core

Los precios de los equipos de Networking, Antivirus y Firewall se encuentran en las proformas que se detallan en el **ANEXO E**

3.8.3. DIMENSIONAMIENTO DE SERVIDORES

Una vez descritos anteriormente los servicios principales que requiere el CEJPM se procede a dimensionar los servidores necesarios para soportar dichos servicios.

En el capítulo 2 se especificó que el CEJPM cuenta con un computador adaptado con las funciones de servidor el cual esta prestando los servicios de servidor de notas [20].

3.8.3.1. Primer Servidor

Este servidor será utilizado para implementar los siguientes servicios: DHCP, DNS, WEB y Proxy, se realizó esta agrupación debido a que estos servicios tienen algunas similitudes en cuanto a los servicios que prestan en la red.

Para implementar cada servicio se requiere como mínimo: un procesador de 250 Mhz, 256 MB de RAM y 8 GB de espacio en disco duro, tomando en cuenta que el servidor tiene un procesador de 2.66 GHz con una memoria que puede expandirse hasta 16 GB y un disco duro de 1 TB, todos los servicios trabajarán sin problema alguno.

A continuación se realiza el cálculo para determinar la velocidad de procesamiento y la capacidad de memoria requerida, si se utiliza los 4 servicios de forma simultánea.

$$Procesador = 4x250\ GHz$$

$$Procesador = 1.000\ GHz$$

$$Memoria_{RAM} = 4x256\ MB$$

$$Memoria_{RAM} = 1024\ MB$$

La capacidad de almacenamiento mínima necesaria es de 32 GB para implementar dichos servicios.

3.8.3.2. Segundo Servidor

Este servidor estará dedicado para los siguientes servicios: correo electrónico y servidor de impresión. Este servidor tiene las mismas características del primer servidor.

A continuación se realiza el cálculo para determinar la velocidad de procesamiento y la capacidad de memoria requerida si se utiliza los 2 servicios de forma simultánea.

$$Procesador = 2x250\ GHz$$

$$Procesador = 500\ GHz$$

$$Memoria_{RAM} = 2x256\ MB$$

$$Memoria_{RAM} = 512\ MB$$

Adema, Con los datos obtenidos anteriormente se calcula la capacidad de almacenamiento necesario de correo electrónico requerido por los 137 usuarios en 8 horas laborables los 22 días al mes.

$$AB_{(total\ correo\ electrónico)} = 22.83\ Kbps$$

$$C_{(Almacenamiento)} = 22.83\ Kbps \frac{1\ Byte}{8\ bits} * 3600s$$

$$C_{(correo\ electrónico)} = 10.03\ MB/hora$$

$$C_{(correo\ electrónico)} = 20.68\ GB/año$$

La capacidad de almacenamiento mínima necesaria es de 21 GB para implementar dichos servicios.

Este servidor también será utilizado para almacenar la información enviada por las 14 cámaras IP, la capacidad requerida es de 2340.0 GB.

Se debe adquirir un servidor con discos duros de 500 GB de almacenamiento

3.8.3.3. Requerimiento mínimo del Sistema Operativo de los servidores

Esta serie de servidores soportan sistemas operativos Linux y Windows por lo que se debe tomar en cuenta los requerimientos mínimos para instalar dichos sistemas operativos donde se van a implementar los servicios.

Linux (Red Hat, Suse) [21]

- **Procesador:** AMD Duron, Athlon o Intel Celeron, Pentium IV o superior **Memoria RAM:** Mínimo: 256 MB recomendado: 512 MB o superior
- **Disco duro:** Mínimo: 500MB Recomendado: 4GB o superior

Windows Server 2008

- **Procesador:** Mínimo: 1 GHz, Recomendado 2 GHz o superior
- **Memoria RAM:** Mínimo: 512 MB, Recomendado 1 GB o superior
- **Disco Duro:** Mínimo: 8 GB, Recomendado 40 GB o superior

En la tabla 3.37 se especifica en forma detallada las principales características requeridas para los servidores.

Servidores	Procesador (Estándar)	Memoria RAM (Estándar)	HD
Primer	2.6 GHz	4 GB	500 GB
Segundo	2.6 GHz	4 GB	1 TB

Tabla 3.37 Características de los servidores

3.8.4. DISEÑO DE LA RED PARA VOZ SOBRE IP

Para realizar el diseño de la red telefónica IP para el CEJPM se analizará una solución que se plantea para prestar Telefonía IP mediante el uso de software libre utilizando Trixbox CE que está basado en Asterisk y es de distribución gratuita. Por lo que se requiere solo un equipo para ser implementado.

3.8.4.1. Telefonía IP basada en software libre

En esta solución se utiliza de hardware un servidor equipado con tarjetas PCI[44] las cuales permiten la comunicación de la red telefónica interna con la red telefónica PSTN. Para el software se utiliza una herramienta de licencia GPL[45] denominada Asterisk la cual es reconocida por sus excelentes características para implementar una Centralita IP.

[44] *Peripheral Component Interconnect* (PCI): Es un bus de ordenador estándar que es utilizado para conectar dispositivos periféricos de forma directa a la placa base de un servidor o pc.
[45] GPL: General Public Licence

En la figura 3.10 se presenta un diagrama de la red de Telefonía IP utilizando un servidor Asterisk el cual hace las funciones de una central telefónica IP.

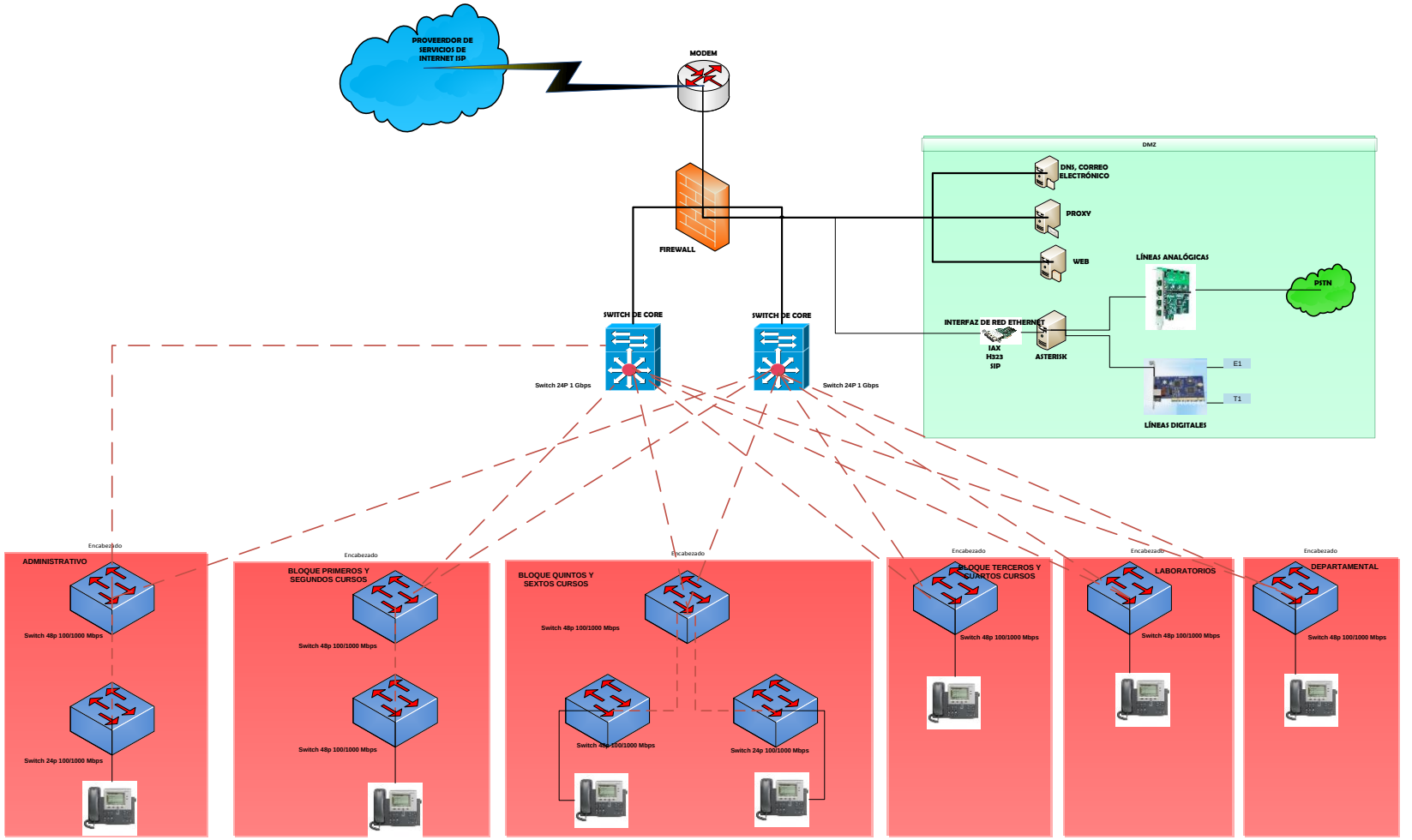


Figura 3.10 Diagrama de la red de Telefonía IP del CEJPM

Asterisk es una PBX en versión digital, fue creado utilizando la plataforma de Linux y Unix, permitiendo la conexión de diferentes interfaces de comunicación ya sean estas digitales o analógicas.

Esta herramienta provee algunos servicios tales como: directorios, cola de llamadas, conferencias, video conferencias, reconocimiento de voz, administradores únicos de llamadas, llamadas salientes y entrantes. Además, maneja varios tipos de protocolos para IP, SIP, H.323, ADSI, IAX, IVR.

3.8.4.2. Herramienta Trixbox CE

Empezó en el año 2004 como un proyecto IP-PBX llamado Asterisk@Home. El cual se convirtió en la distribución más popular para implementar centrales IP. Esta versión se caracteriza por dos pilares importantes; su flexibilidad para satisfacer las necesidades de los clientes, y por ser gratuita.

Esta herramienta esta implementada en una distribución del sistema operativo Linux (Centos), es una central telefónica IP basada en software utilizando el código abierto Asterisk, al ser una central telefónica realiza las mismas funciones de una central convencional. Además, tiene varias características que solo utilizan sistemas propietarios. Además, Trixbox incluye lo siguiente:

- Servidor Web Apache, con soporte a PHP y Perl
- Administración de Base de Datos
- Correo de Voz e integración de este con el email
- Integración fax-a-email
- Autoconfiguración del hardware Zaptel de Digium
- Text-to-Speech en inglés.

La aplicación que se va a utilizar es Trixbox CE porque es la versión comunitaria de Trixbox y es un sistema basado en software libre, por lo que tiene algunas ventajas.

- No necesita licencia por lo que es una disminución de costos para la Institución
- Tiene una ambiente grafico facilitando la administración de la centralita IP
- Tiene soporte de la comunidad la cual se encuentra en continua investigación y desarrollo mejorando el esta aplicación
- Se tiene acceso al código fuente permitiendo el acceso a la configuración de acuerdo a las necesidades de la Institución

3.8.4.3. Requerimientos de hardware y Software para la implementación

Para la implementación de la central IP trixbox, se requiere de un servidor o una PC que cumpla con las características detalladas a continuación.

- Sistema operativo Linux (Centos 5.x)
- Procesador 2 GHz o superior
- RAM 512
- Disco Duro 250 GB
- Tarjeta de red 10/100/1000 Mbps
- Software Trixbox CE
- Tarjeta PCI de 4 Puertos FXO y FXS.

3.8.4.4. Centrales Telefónicas Comerciales IP basadas en Asterisk

Existen algunas centrales telefónicas comerciales que se basan en el sistema Asterisk tales como Elastix, SwitchVox y Trixbox Pro, cada una de estas opciones posee excelentes características para trabajar como una central telefónica que incluso las hace competitivas con sistemas telefónicos propietarios tales como Cisco.

3.8.4.5. Elastix

Fue creado y actualmente es mantenido por la empresa PaloSanto Solution empezando como una interfaz de reporte de llamadas para Asterisk para

posteriormente ser liberado en el 2006 para luego convertirse en una central telefónica basada en Asterisk, que no solo provee telefonía si no que también integra otros medios de comunicación para hacer más eficiente y productivo su entorno de trabajo.

Elastix incluye en su paquete los siguientes medios de comunicación, los cuales se detallan en la figura 3.11.

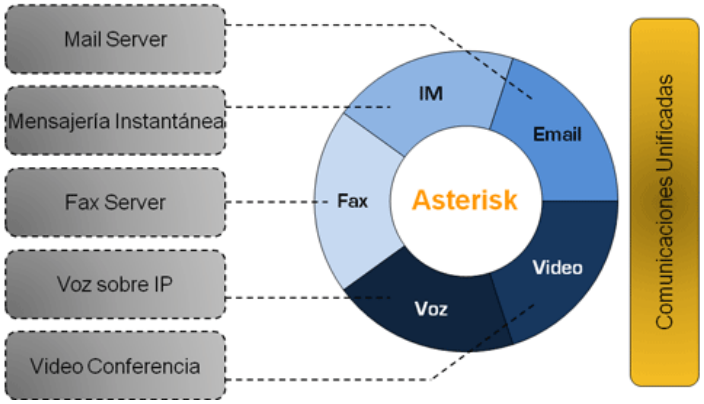
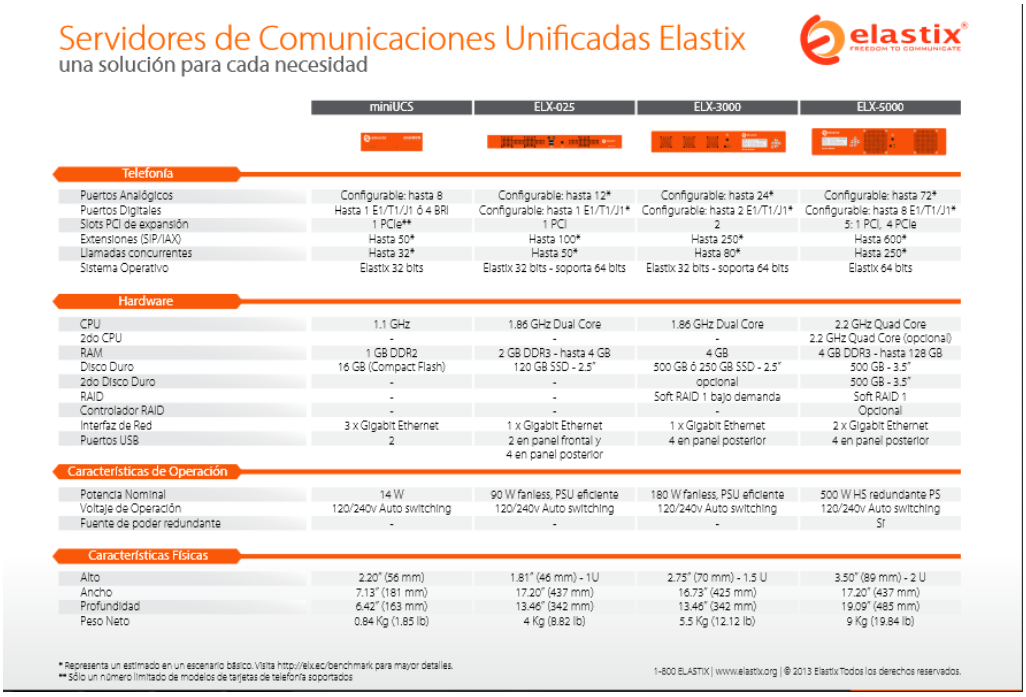


Figura 3.11 Paquetes que incluye Asterisk

Elastix es una herramienta de código abierto distribuida bajo licencia GPLv2. Por lo que no tiene un costo relacionado con licenciamiento o funcionalidades haciendo que las versiones disponibles de Elastix sean versiones completas sin limitación de uso, permitiendo que cualquier empresa pueda utilizarlo sin ninguna restricción.

En la tabla 3.38 se detalla las versiones disponibles de *Elastix*, detallando sus principales características técnicas.



Servidores de Comunicaciones Unificadas Elastix
una solución para cada necesidad

elastix
FREEDOM TO COMMUNICATE

	miniUCS	ELX-025	ELX-3000	ELX-5000
Telefonía				
Puertos Analógicos	Configurable: hasta 8	Configurable: hasta 12*	Configurable: hasta 24*	Configurable: hasta 72*
Puertos Digitales	Hasta 1 E1/T1/J1 ó 4 BRI	Configurable: hasta 1 E1/T1/J1*	Configurable: hasta 2 E1/T1/J1*	Configurable: hasta 8 E1/T1/J1*
Slots PCI de expansión	1 PCIe**	1 PCI	2	5: 1 PCI, 4 PCIe
Extensiones (SIP/IAX)	Hasta 50*	Hasta 100*	Hasta 250*	Hasta 600*
Llamadas concurrentes	Hasta 32*	Hasta 50*	Hasta 80*	Hasta 250*
Sistema Operativo	Elastix 32 bits	Elastix 32 bits - soporta 64 bits	Elastix 32 bits - soporta 64 bits	Elastix 64 bits
Hardware				
CPU	1.1 GHz	1.86 GHz Dual Core	1.86 GHz Dual Core	2.2 GHz Quad Core
2do CPU	-	-	-	2.2 GHz Quad Core (opcional)
RAM	1 GB DDR2	2 GB DDR3 - hasta 4 GB	4 GB	4 GB DDR3 - hasta 128 GB
Disco Duro	16 GB (Compact Flash)	120 GB SSD - 2.5"	500 GB ó 250 GB SSD - 2.5"	500 GB - 3.5"
2do Disco Duro	-	-	opcional	500 GB - 3.5"
RAID	-	-	Soft RAID 1 bajo demanda	Soft RAID 1
Controlador RAID	-	-	-	Opcional
Interfaz de Red	3 x Gigabit Ethernet	1 x Gigabit Ethernet	1 x Gigabit Ethernet	2 x Gigabit Ethernet
Puertos USB	2	2 en panel frontal y 4 en panel posterior	4 en panel posterior	4 en panel posterior
Características de Operación				
Potencia Nominal	14 W	90 W fanless, PSU eficiente	180 W fanless, PSU eficiente	500 W HS redundante PS
Voltaje de Operación	120/240v Auto switching	120/240v Auto switching	120/240v Auto switching	120/240v Auto switching
Fuente de poder redundante	-	-	-	Sí
Características Físicas				
Alto	2.20" (56 mm)	1.81" (46 mm) - 1U	2.75" (70 mm) - 1.5 U	3.50" (89 mm) - 2 U
Ancho	7.13" (181 mm)	17.20" (437 mm)	16.73" (425 mm)	17.20" (437 mm)
Profundidad	6.42" (163 mm)	13.46" (342 mm)	13.46" (342 mm)	19.09" (485 mm)
Peso Neto	0.84 Kg (1.85 lb)	4 Kg (8.82 lb)	5.5 Kg (12.12 lb)	9 Kg (19.84 lb)

* Representa un estimado en un escenario básico. Visita http://elx.ec/benchmark para mayor detalles.
** Sólo un número limitado de modelos de tarjetas de telefonía soportados

1-800 ELASTIX | www.elastix.org | © 2013 Elastix Todos los derechos reservados.

Tabla 3.38 Versiones disponibles de Elastix y sus características técnicas [22]

3.8.4.6. SwitchVox

El sistema SwitchVox de Digium, que es el creador de *Asterisk*, es más que un sistema telefónico tradicional, es un sistema de comunicaciones unificadas asequibles que tiene integrado todas las comunicaciones de una empresa, incluyendo teléfono, fax, chat y combinaciones en web.

SwitchVox es identificado como una de las centrales telefónicas IP más innovadoras y robustas que existen en el mercado, por la facilidad que ofrece para integrarse a servicios *web* tales como *Salesforce*, *Google Maps*, entre otras.

En la tabla 3.39 se indica las Versiones disponibles de SwitchVox y sus características técnicas [23].

Imagen			
Función	**SwitchVox SMB AA65 Appliance**	**SwitchVox SMB AA305 Appliance**	**SwitchVox SMB AA355 Appliance**
Ideal para	Empresas pequeñas	Empresas medianas	Empresas medianas y grandes
Usuarios	Hasta 30	Hasta 150	Hasta 400
Llamadas simultaneas	Hasta 12	Hasta 45	Hasta 75
Ranuras de expansión	Dos	Tres	Tres
Grabaciones	“Hasta 5 llamadas grabadas simultáneamente	Hasta 10 llamadas grabadas simultáneamente	Hasta 20 llamadas grabadas simultáneamente
Conferencia	Hasta 5 usuarios de conferencia simultáneos	Hasta 15 usuarios de conferencia simultáneos	Hasta 30 usuarios de conferencia simultáneos
Peso	15 Lbs.	30 Lbs.	48 Lbs.
Fuente de alimentación	220 W	300 W	500 W
Slot para tarjetas de telefonía	2	2	2
Soporte de tarjetas de telefonía	B410P, TDM410, TDM800, TE122(only one TE122 supported)	TDM410, TDM800, TDM2400, TE122, TE205/207, TE405/407, B410P	TDM410, TDM800, TDM2400, TE122, TE205/207, TE405/407, B410P
Opciones de garantía:	Garantía estándar de 1 año Garantía extendida a 3 años	Garantía estándar de 1 año Garantía extendida a 3 años	Garantía estándar de 1 año Garantía extendida a 3 años
Soporte de Idioma	Inglés, italiano y español	Inglés, italiano y español	Inglés, italiano y español

Tabla 3.39 Versiones disponibles de SwitchVox y sus características técnicas [23]

3.8.4.7. Trixbox Pro

Trixbox Pro es una solución denominada "hibrid-hosted", esto significa que el cliente puede realizar un monitoreo 24/7, y le permite administrar la central desde

cualquier lugar y actualizaciones del software de manera automática. Trixbox Pro, es una versión empresarial la cual ha sido comercializada desde el 2004 permitiendo enviar/recibir más de 120 millones de llamadas por día. Trixbox Pro posee 3 versiones:

- Standard Edition (SE)
  Es una solución de telefonía IP basada en Asterisk mejorada para ofrecer mayor fiabilidad y escalabilidad. Además, Trixbox Pro SE incluye: una interfaz gráfica, voicemail basado en web, reportes de llamadas, clickto-call, integración con Outlook, gráficos de recursos en tiempo real, alertas del sistema, configuración auto-card y VoIP trunking.
- Enterprise Edition (EE)
  Trixbox Pro EE tiene todas las características de Trixbox Standard Edition. Sin embargo, incluye nuevas funcionalidades tales como: puentes para conferencia, multiples auto attendants, paging, permisos de grupo entre otras. Además tiene incluido HUD Pro el cual añade administración presencial, control de llamadas drag and drop, chat corporativo privado, alertas interactivas y más.
- Call Center Edition (CCE)
  Trixbox Pro CCE fue desarrollado basándose en los anteriores estándares por lo que tiene todas sus funcionalidades añadiendo nuevas tales como: ACD[46] e IVR[47] con colas ilimitadas, estadísticas en tiempo real de colas, reportes gráficos, acceso basado en web a grabaciones.

3.8.4.8. Requerimiento que debe cumplir la central comercial IP

En caso de que la elección sea adquirir una central telefónica comercial basada en Asterisk debe cumplir los siguientes requerimientos.

- 3 interfaces FXO con la red PSTN
- Soporte para más de 40 Usuarios

[46] Automatic Call Distributor (ACD): es un proceso utilizado para distribuir las llamadas que llegan a los sistemas de atención.
[47] Contestador Automático (IVR): guía a los que llamen según las opciones predeterminadas.

- Protocolos de señalización
- Control de llamadas
- IVR
- Correo de voz
- Administración vía web
- Distribución automática de llamadas
- Soporte de códecs G.729a
- Soporta Auto negociación de códec

3.8.4.9. Comparación de las dos soluciones propuestas

Luego de haber detallado las centrales IP comerciales basadas en Asterisk se realiza una comparación de aquellas que cumplen con las características requeridas por el CEJPM, y que se detallan en la tabla 3.40.

IPPBX	Elastix	SwitchVox	Trixbox Pro
Distribución	ELX-025	SwitchVox SMB AA65 Appliance	Standard Edition (SE)

Tabla 3.40 Comparación de las centrales IP comerciales basadas en Asterisk

3.8.4.10. Selección de la solución a utilizarse en la CEJPM

Una vez presentadas y analizadas las dos propuestas utilizadas las cuales son: Trixbox CE y Centrales telefónicas IP comerciales basadas en Asterisk, se recomienda utilizar en el CEJPM una IPPBX comercial Elastix. Por cuestión de soporte, esto seria una ventaja ya que el soporte seria local a diferencia de un proveedor que se encuentre fuera del país.

Otra de las razones por la que se decidió por Elastix es la gran acogida que ha tenido a nivel nacional e internacional siendo nominada a premios de *software* libre.

3.8.4.11. Principales razones de la elección de Elastix

Elastix es un software aplicativo que tiene integrado las mejores herramientas disponibles para un central telefónica. Además cuenta con un conjunto de utilidades que permiten la creación de módulos haciendo de este uno de los mejores paquetes de software de código abierto.

Cabe indicar que Elastix ofrece confiabilidad, modularidad, robustez y una interfaz simple y fácil de usar.

La empresa PaloSanto Solution ofrece en sus productos un período de garantía, tiempo en el cual se evalúa la central telefónica y en caso de alguna eventualidad se puede reportar para solicitar una solución inmediata.

Al adquirir una central telefónica Elastix, PaloSanto Solution ofrece capacitación para los usuarios comunes y para el administrador. Además, la empresa ofrece soporte y mantenimiento continuo preventivo, este servicio incluye actualizaciones de archivos y consultas vía mail o telefónico.

3.8.5. ACCESORIOS PARA LA TELEFONÍA IP

La CEJPM requiere 40 extensiones para dar servicio de telefonía a los usuarios administrativos de la Institución, por lo que se debe adquirir 40 teléfonos IP los cuales deben cumplir con las siguientes características básicas detalladas a continuación.

- 2 puertos Fast Ethernet (100Mbps)
- PoE support (802.3af)
- Soporte de códecs G.729
- Soporte DHCP

- QoS (802.1p)
- Soporte de capa 2 (802.1q VLAN, 802.1p)
- Soporte de cancelado de eco
- Calidad de voz
- Identificador de llamadas
- Llamada en espera
- Transferencia de llamadas

Adicionalmente, existe software como softphone que realiza las funciones de un teléfono IP, el cual puede ser instalado en cualquier estación de trabajo utilizando un micrófono con audífonos.
Los precios de los equipos de Telefonía IP se encuentran en las proformas que se detallan en el **ANEXO E**

3.8.6. DISEÑO DE LA RED INALÁMBRICA

Las redes inalámbricas brindan movilidad a los usuarios y sirven como complemento a la red cableada cuando el acceso a esta en ciertos lugares no es posible, además brindan una solución para conexiones que se van a realizar de manera temporal.

La red inalámbrica brinda los mismos servicios que la red cableada; razón por la cual se tomará en cuenta sistemas de seguridad con autenticación de usuarios, cifrado de información, etc.
El Colegio Experimental Juan Pío Montúfar, dispone de una red cableada más no de una red inalámbrica. Como se ha descrito en el capítulo 2, las instalaciones del Colegio disponen de un cableado estructurado precario para su red.

La posible integración de nuevos usuarios, y las cambiantes necesidades departamentales, que eventualmente modifican la ubicación física de los miembros de la comunidad educativa, podrían generar un gran problema en la creación de nuevos puntos de red, o movimiento de los mismos por lo que se

considera necesario brindar servicios de acceso inalámbrico a los usuarios que así lo requieran.

Con el propósito de disponer de un sistema de acceso inalámbrico para los equipos, solucionar los problemas de movilidad de los departamentos, y abaratar los costos de incluir nuevos usuarios a la red, se determina que la mejor opción es la creación de una red inalámbrica que coexista con la red cableada que actualmente se dispone.

Se proveerá servicios de red inalámbrica para sectores como: Biblioteca, Salón de Actos, Departamento Médico, Sala de Profesores, Laboratorio de Biología, Laboratorio de Física, Laboratorio de Computación Primeros y Segundos Cursos, Laboratorio de Computación Terceros y Cuartos Cursos, Sala de Idioma Extranjero, Laboratorio de Computación Quintos y Sextos Cursos.

3.8.7. TIPO DE APLICACIONES SOPORTADAS

Las aplicaciones que se ejecutarán sobre la red inalámbrica serán las mismas que las indicadas para la red cableada: acceso web, correo electrónico, descarga de archivos, etc. Con las consideraciones relativas a una red inalámbrica como por ejemplo que su velocidad de acceso dependerá de la distancia al punto de acceso.

El tráfico cursado a través de la red inalámbrica será en su mayoría para el acceso a Internet tanto de los usuarios permanentes como de los temporales.

3.8.8. MATERIAL DE CONSTRUCCIÓN DE LAS ZONAS DE COBERTURA DE LA RED INALÁMBRICA

Toda la infraestructura de la Institución está compuesta por: loza de cemento, delimitación de aulas es de ladrillo con un espesor de 24 cm, las oficinas están separadas por vidrio con madera de 10 cm.

En la tabla 3.41 se muestra la atenuación que sufre la señal al pasar por estos obstáculos.

MATERIAL	EJEMPLO	INTERFERENCIA
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metales	Vigas, armarios	Muy Alta

Tabla 3.41 Materiales que causan Interferencia

Bibliografia: GOMEZ Fernando, “Diseño, estudio y análisis de costos de una red inalambrica para el sistema de comunicaciones interno de PETROECUADOR ”

3.9. CANTIDAD DE USUARIOS

Al realizar el diseño de una red WLAN es importante conocer la cantidad de usuarios que se van a conectar a esta red para acceder a los servicios que proporciona.

Para determinar un aproximado de usuarios simultáneos que se conectarán a la red inalámbrica se considera los siguientes aspectos.

- El CEJPM tiene 106 docentes que requieren subir las notas a la base de datos a más de investigar y actualizarse para mejorar el nivel educativo de los estudiantes, para determinar el número de docentes que van a utilizar la red inalámbrica se toma en cuenta que no todos los profesores disponen de una computadora portátil. Por lo que no todos los 106 docentes se

conectarán de forma simultánea. Además, se dispone de 3 computadores en la sala de profesores quedando la necesidad del servicio para el resto de docentes.

- En el colegio trabajan un número fijo de personal administrativo y de acuerdo al espacio físico dedicado a este departamento es difícil asumir un crecimiento de personal.
- En la biblioteca se cuenta con 10 computadoras. Sin embargo: en la actualidad los estudiantes no llevan computadores portátiles debido a que en esta no se presta este servicio.
- Este servicio será más utilizado por los estudiantes de bachillerato para realizar consultas y son aproximadamente 300 de los cuales no todos cuentan con equipos portátiles razón por la cual se toma un porcentaje del 25% dando un valor de 75 usuarios simultáneos.

De acuerdo a estas premisas, se tendrán aproximadamente 94 usuarios simultáneos conectados a la red inalámbrica en el peor de los casos.

3.10. SELECIÓN DE LA TECNOLOGÍA A UTILIZAR

Los estándares de las redes inalámbricas IEEE 802.11 que se pueden utilizar para el diseño se detallan en la tabla 3.42.

Parámetros	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frecuencia	5 GHz	2.4 GHz	2.4 GHz
Ancho de Banda	300 MHz	83.5 MHz	83.5 MHz
Modulación	OFDM	DSSS	OFDM
Número de Canales	6	3	3
AB por Canal	20MHz	22MHz	22MHz
Tasa de Transmisión	54 Mbps	Variada 1,2,5.5 y 11 Mbps	54 Mbps
U. Simultáneos	64	32	50
Distancia exteriores	30 m a 54 Mbps	120 m a 11 Mbps	Km con antenas parabólicas
	300m a 6Mbps	460 m a 1 Mbps	
Distancia interiores	12 m a 54 Mbps	30 m a 11 Mbps	30 Mbps a 50 m
	90m a 6Mbps	90 m a 1 Mbps	

Tabla 3.42 Estándares IEEE 802.11

En este diseño se va a utilizar IEEE 802.11g por su cobertura y tasa de transmisión que ofrece el estándar en interiores y por el número de usuarios simultáneos especificados en el literal anterior.

Como no se encontraron otras redes inalámbricas en las cercanías se van a utilizar los canales 1, 6 y 11 para evitar las interferencias entre ellos. Para cumplir con las condiciones mínimas de diseño de la red WLAN se necesita tener por lo menos una velocidad de 4Mbps.

3.10.1. CANTIDAD Y UBICACIÓN DE LOS EQUIPOS (AP)

Para determinar el número de AP necesarios para cubrir los sitios que requiere el CEJPM se consideró lo siguiente:

- El número de usuarios que se van a conectar en la red en cada área, el cual se detalló en el literal 3.4.1 (Arriba)
- Los obstáculos que se tienen por área de cobertura por los cuales tiene que atravesar la señal sufriendo cierto grado de atenuación disminuyendo el alcance de la señal.
- Elegir los puntos de acceso, ya que deben cumplir ciertos parámetros tales como: potencia de la señal la cual sea suficiente para cubrir el área a servir.

De acuerdo a las consideraciones anteriores se requiere de 10 AP dos por cada área los cuales utilizarán los canales de frecuencia 1, 6 y 11, y estarán ubicados de acuerdo a las siguientes figuras.

A continuación la ubicación de los Access point en el Área Administrativa del Colegi. En la figura 3.12 se indica la ubicación del Access Point, resaltado en azul dentro del Área Biblioteca en la planta baja.

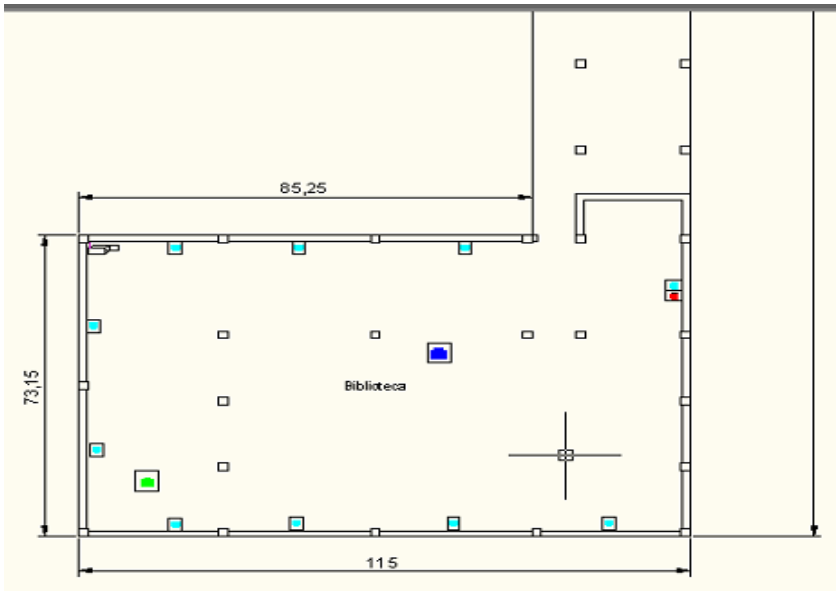


Figura 3.12 Biblioteca Planta Baja.

La figura 3.13 muetra la ubicación del Access Point en el Área de Salón de Actos en primer piso.

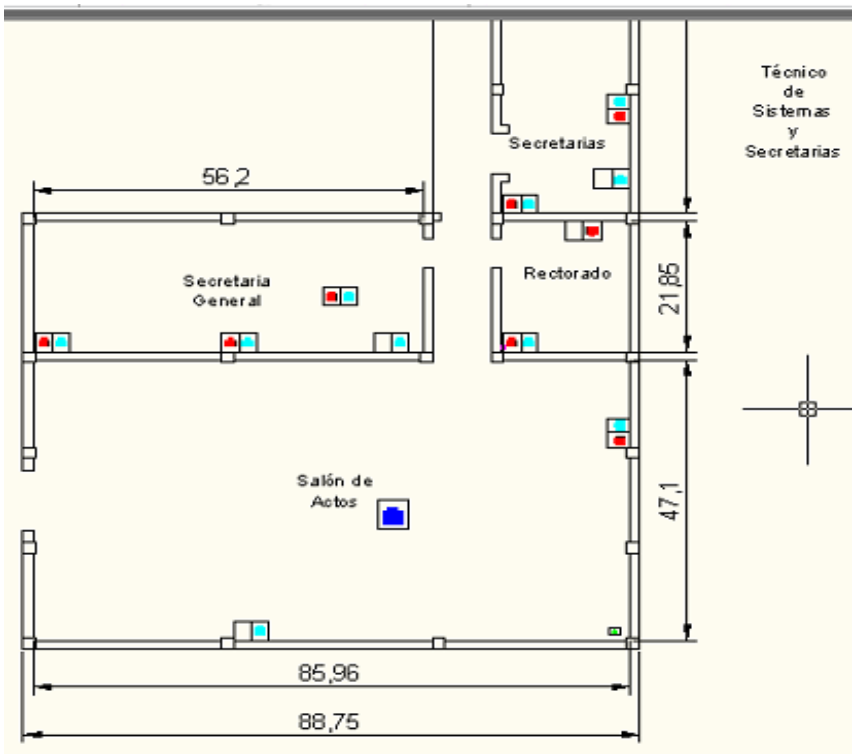


Figura 3.13 Salón de Actos Primer Piso

A continuación la ubicación de los Access Point en el Área Departamental del Colegio, están ubicados en el Departamento Médico en planta baja. (Figura 3.14).

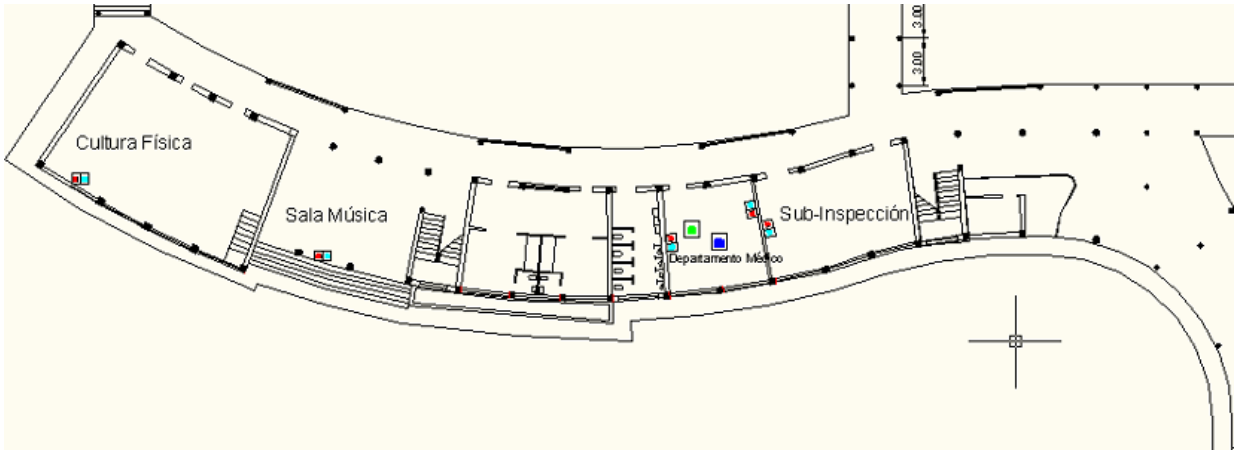


Figura 3.14 Departamento Médico Planta Baja

La siguiente figura muetra la ubicación del Access Point en el Área de Sala de Lectura de Profesores en primer piso. (Figura 3.15).

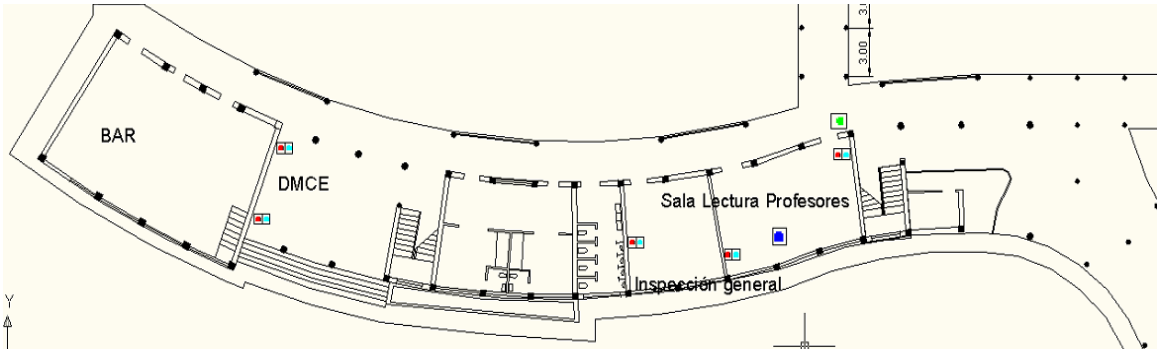


Figura 3.15 Sala de Lectura de Profesores Primer Piso

A continuación la ubicación de los Access Point en el Área Laboratorios del Colegio, están ubicados en el Laboratorio de Química en planta baja. (Figura 3.16)

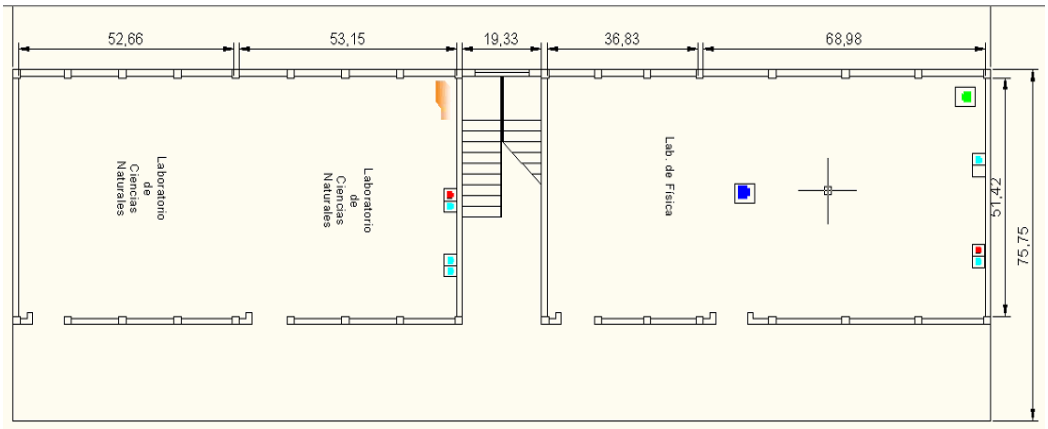


Figura 3.16 Laboratorio de Química Planta Baja

La siguiente figura muetra la ubicación del Access Point en el Laboratorios de Física en primer piso. (Figura 3.17).

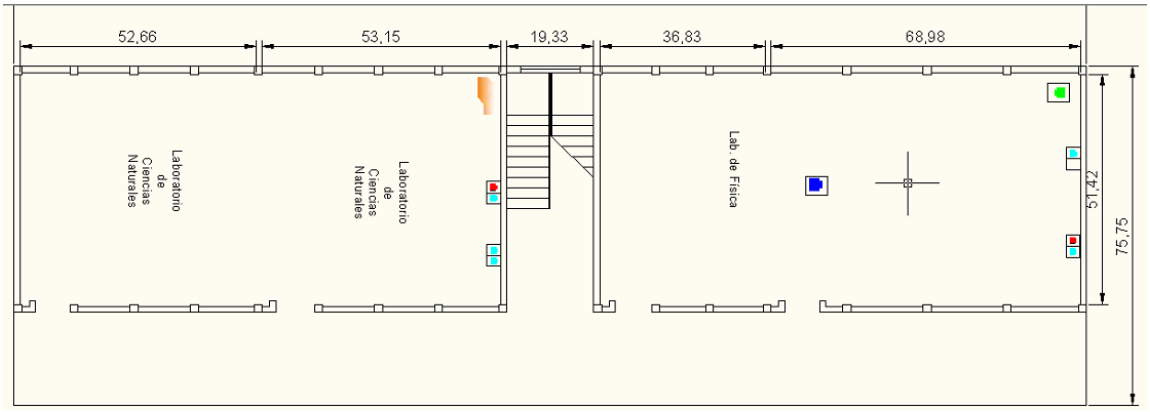


Figura 3.17 Laboratorio de Física Primer Piso

A continuación la ubicación del Access Point en el Bloque Primeros y Segundos Cursos está dentro del Laboratorio Computación. (Figura 3.18).

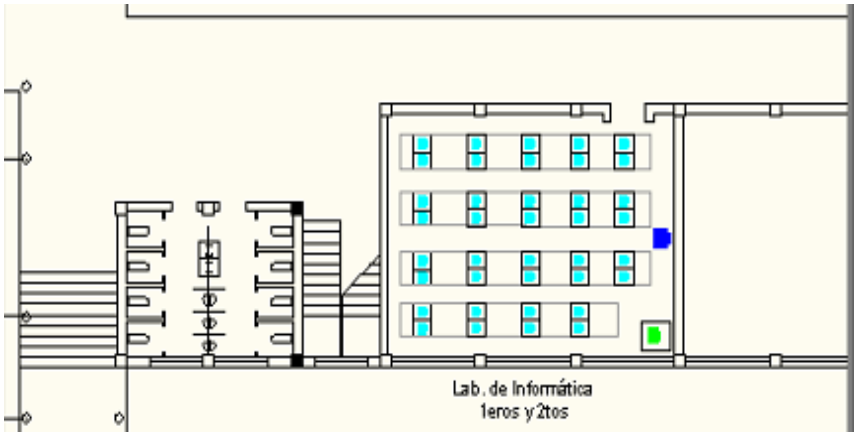


Figura 3.18 Laboratorio de Computación Primeros y Segundos Cursos

A continuación la ubicación de los Access Point en el Bloque Terceros y Cuartos Cursos están ubicados en el Laboratorio Computación en planta baja. (Figura 3.19).

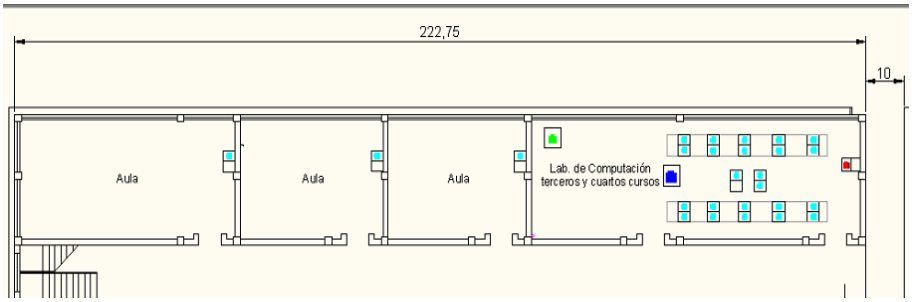


Figura 3.19 Laboratorio de Computación Terceros y Cuartos Cursos

La siguiente figura muetra la ubicación del Access Point en el Laboratorios de Idiomas en primer piso. (Figura 3.20).

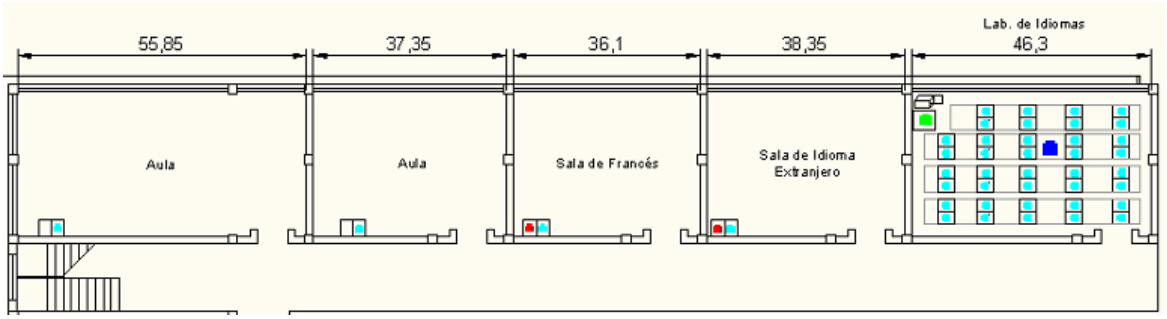


Figura 3.20 Laboratorio de idiomas

A continuación la ubicación del Access Point en el Bloque Quintos y Sextos Cursos está ubicado en el Laboratorio Computación en el primer piso. (Figura 3.21).

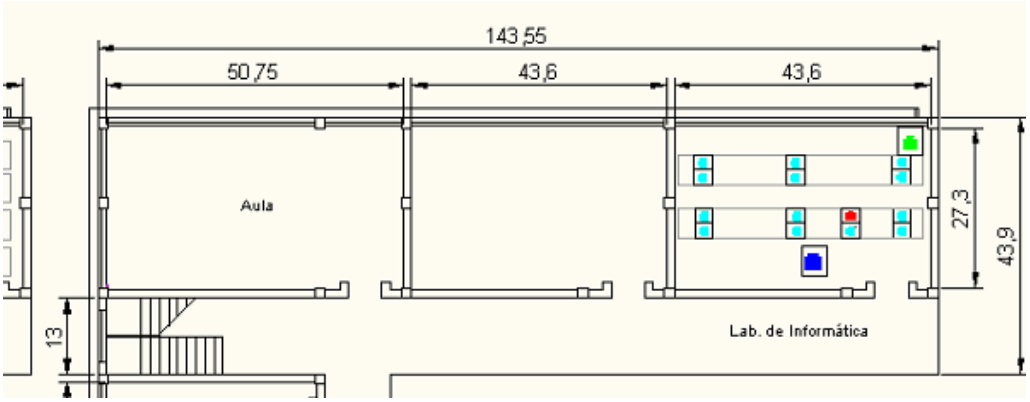


Figura 3.21 Laboratorio de Computación Quintos y Sextos Cursos.

3.10.2. DIAGRAMA DE LA RED WLAN

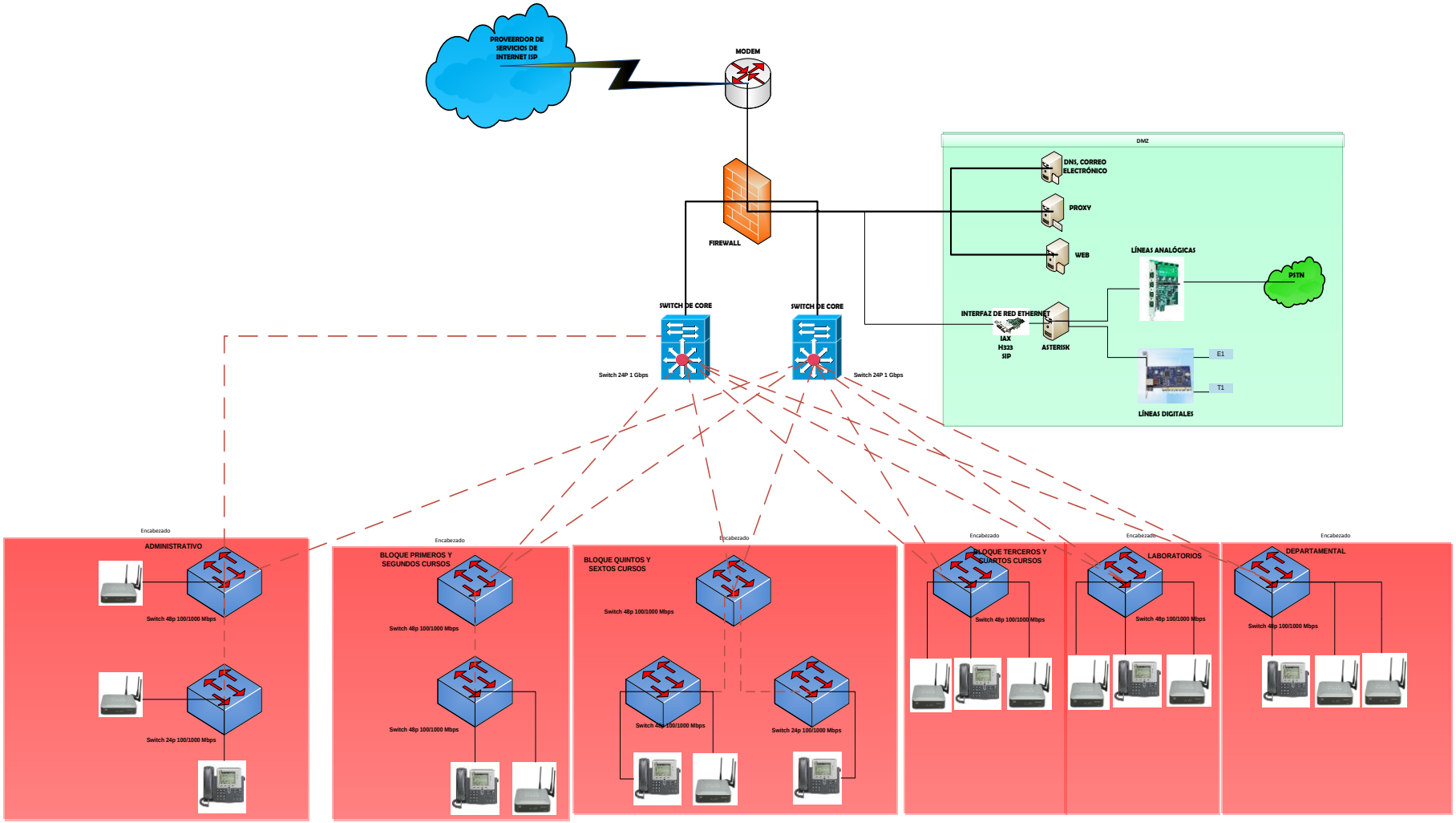


Figura 3.22 Diagrama de la red WLAN

En la figura 3.22 se indica el diseño de la red WLAN.

3.10.3. CARACTERÍSTICAS MÍNIMAS QUE DEBEN CUMPLIR LOS AP

Los equipos a ser utilizados deberán cumplir al menos con los requerimientos mínimos descritos en la tabla 3.43

Velocidad de transmisión	54 Mbps
Protocolo de interconexión	IEEE802.11g, IEEE802.11n
Protocolo de gestión	SNMP, HTTP
Algoritmo de cifrado	SHA, MD5, AES
Encriptación	TLS, PEAT, TTLS, TKIP, WPA, WPA2
Método de autenticación	RADIUS
Interfaces	Ethernet RJ45 (10 BaseT/100BaseTX)
Cumplimiento de normas	IEEE 802.11x, 802.11g, 802.11n, 802.af, 802.3u, 802.1q, 802.1p
Características adicionales	Filtrado de direcciones, firewall, DHCP
Protecciones contra condiciones ambientales variantes para los Access point a ser ubicados en exteriores.	

Tabla 3.43 Características mínimas de los Access Poits

Los precios de los equipos de la red WLAN se encuentran en las proformas que se detallan en el **ANEXO E.**

3.10.4. DISEÑO DE LA RED PARA VIDEO VIGILANCIA

Con el sistema de video vigilancia se tendrá monitoreado los lugares de mayor riesgo que tiene la CEJPM proporcionando monitoreo continuo.

En el literal 3.4, se especificó que se va a utilizar el servidor para el almacenamiento y monitoreo de las cámaras IP que estarán conectadas a la red.

3.10.4.1. Ubicación Física de las Cámaras IP

Las cámaras IP estarán ubicadas de la siguiente manera: 1 en cada acceso al Colegio para tener un mayor control del ingreso y salida del personal administrativo, estudiantes, docentes, padres de familia y particulares.
Las cámaras se ubicaran en las Áreas: Administrativa en la Biblioteca, Colecturía, Sistemas y Corredor del Bloque en el primer piso; Departamental en el Departamento Médico, y Corredor del Bloque del primer piso; Área de Laboratorios en el Laboratorio de Biología, Química, Ciencias Naturales y Física; Área Bloque de Aulas Primeros y Segundos Cursos en el Laboratorio de Computación, Área Bloque de Aulas Terceros y Cuartos Cursos en el Laboratorio de Computación y Laboratorio de Idiomas, Área Bloque de Aulas Quintos y Sextos Cursos en el Laboratorio de Computación, necesarias para monitorear el acceso y brindar mayor seguridad a los equipos de networking, servidores, en los laboratorios se encuentra una alta concentración de computadoras, material de laboratorios, entre otros.

A continuación la ubicación de las Cámaras IP en el Área Administrativa del Colegio, dentro de Biblioteca y Colecturía. Los puntos de red de color verde representan las cámaras IP. (Figura 3.23).

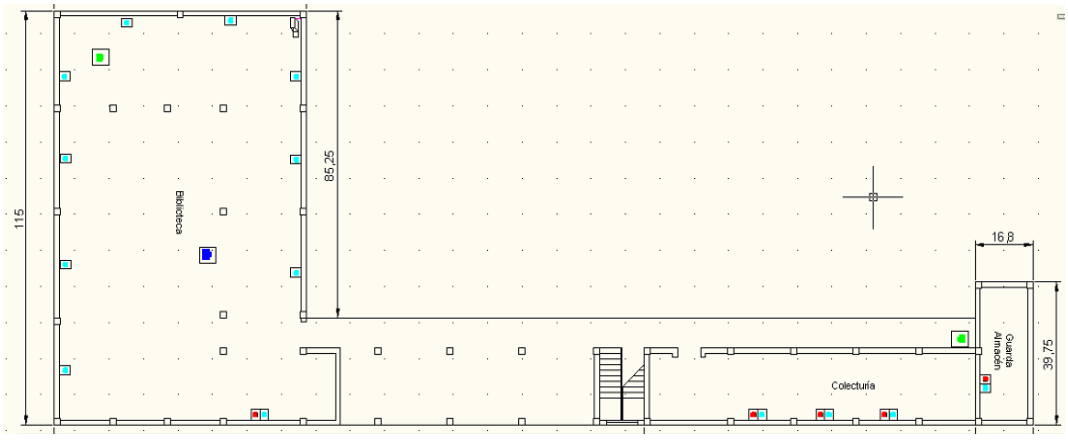


Figura 3.23 Ubicación de las Cámaras IP Biblioteca y Colecturía

A continuación las cámaras en el primer piso del área Administrativa dentro de Sistemas y Corredor del Bloque. (Figura 3.24).

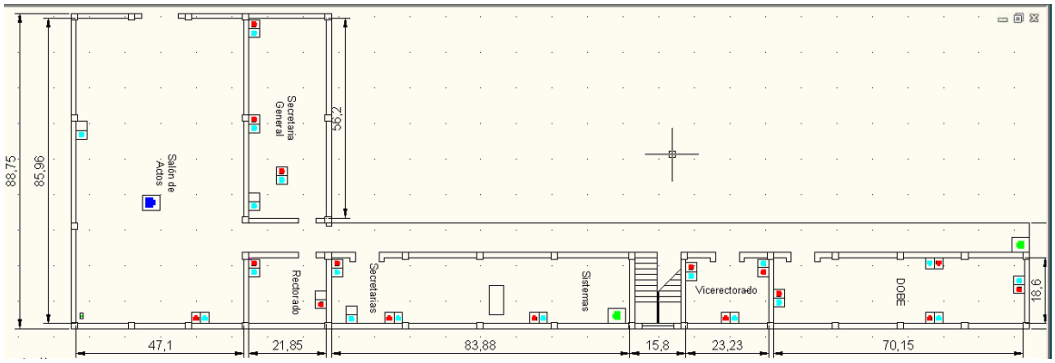


Figura 3.24 Ubicación de las Cámaras IP Salón de Actos y Corredor

A continuación la ubicación de las Cámaras IP en el Área Departamental en planta baja dentro del Departamento Médico. (Figura 3.25).

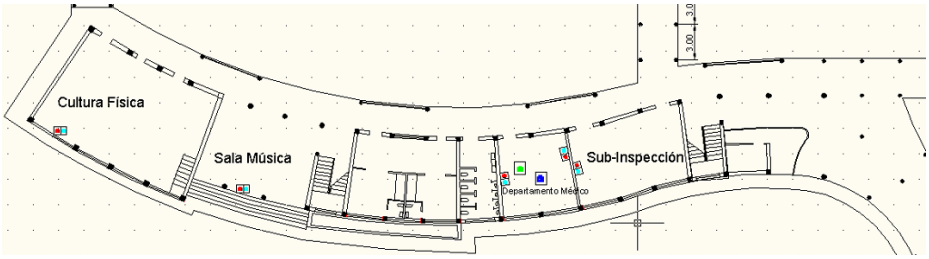


Figura 3.25 Ubicación de las Cámaras Departamento Médico

A continuación la ubicación de las Cámaras IP en el Área Departamental en el primer piso en el Corredor del Bloque. (Figura 3.26).

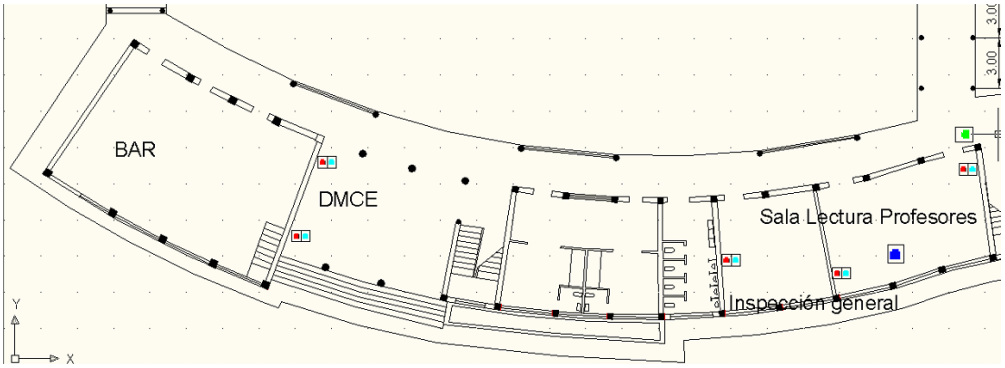


Figura 3.26 Ubicación de las Cámaras IP Corredor

A continuación la ubicación de las Cámaras IP en planta baja del Área Laboratorios del Colegio, dentro de los Laboratorios de Biología y Química. (Figura 3.27).

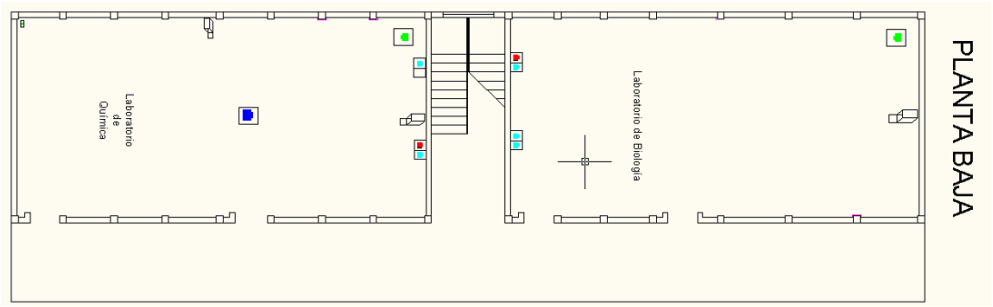


Figura 3.27 Ubicación de las Cámaras IP Laboratorios de Biología y Química

A continuación la ubicación de las Cámaras IP en el primer piso en el Área Laboratorios del Colegio, dentro de los Laboratorios de Ciencias Naturales y Física. (Figura 3.28).

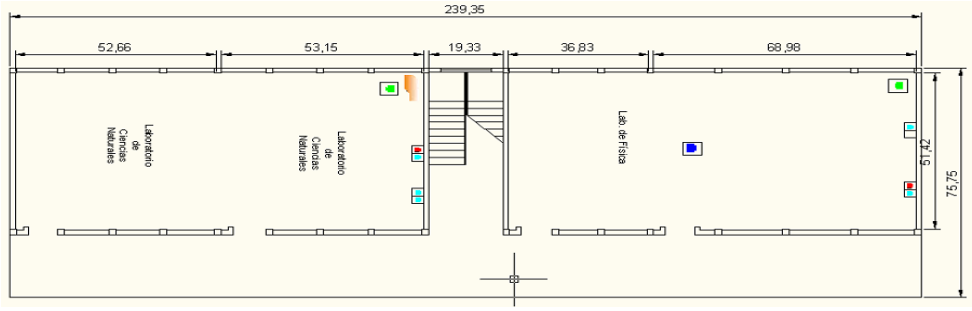


Figura 3.28 Ubicación de las Cámaras IP Área Laboratorios de CC.NN y Física

A continuación la ubicación de la Cámara IP en el Bloque de Primeros y Segundos Cursos del Colegio, dentro del Laboratorio de Computación. (Figura 3.29).

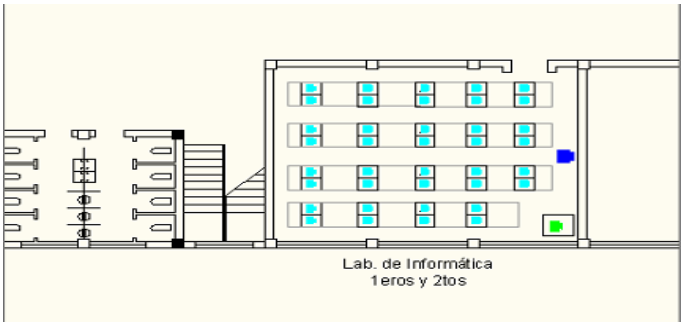


Figura 3.29 Ubicación de la Cámara IP Bloque de Aulas Primeros y Segundos Cursos

A continuación la ubicación de la Cámara IP en planta baja del Bloque de Terceros y Cuartos Cursos del Colegio, dentro del Laboratorio de Computación. (Figura 3.30).

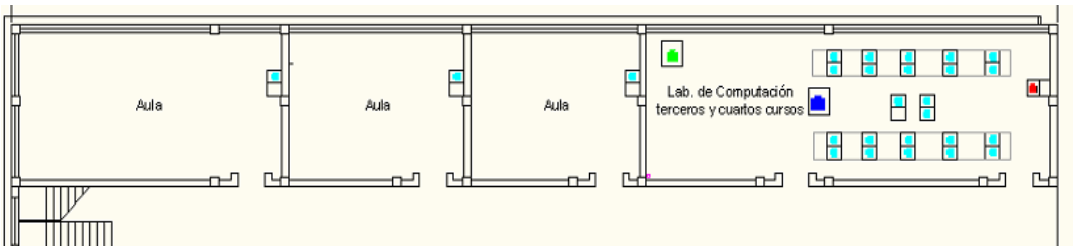


Figura 3.30 Ubicación de la Cámara IP Laboratorio de Computación Terceros y Cuartos Cursos

A continuación la ubicación de la Cámara IP en el primer piso del Bloque de Terceros y Cuartos Cursos del Colegio, dentro del Laboratorio de Idiomas. (Figura 3.31).

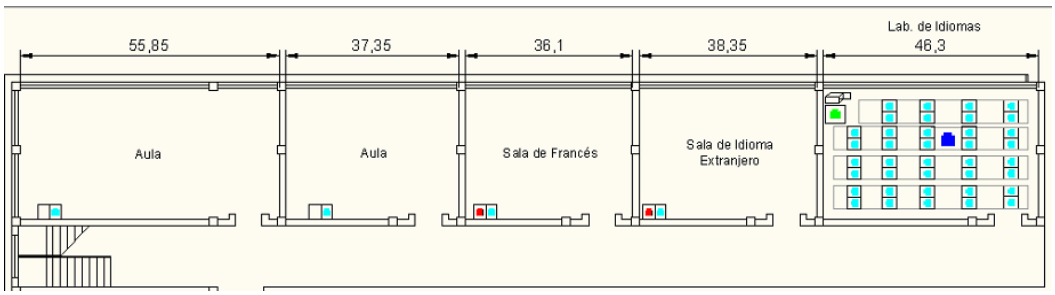


Figura 3.31 Ubicación de la Cámara IP Laboratorio de Idiomas

A continuación la ubicación de la Cámaras IP en el Bloque de Quintos y Sextos Cursos del Colegio, dentro del Laboratorio de Computación. (Figura 3.32).

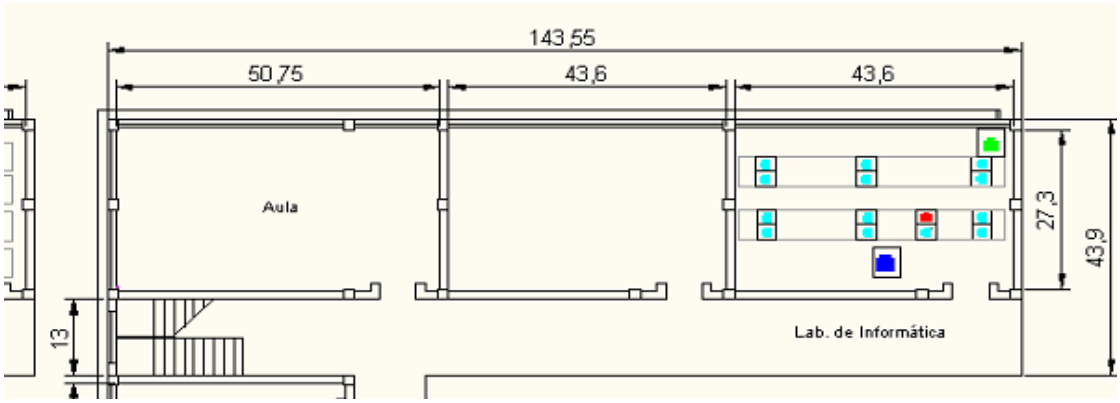


Figura 3.32 Ubicación de la Cámara IP Laboratorio de Computación Quintos y Sextos Cursos.

3.10.4.2. Diagrama de la red para video vigilancia

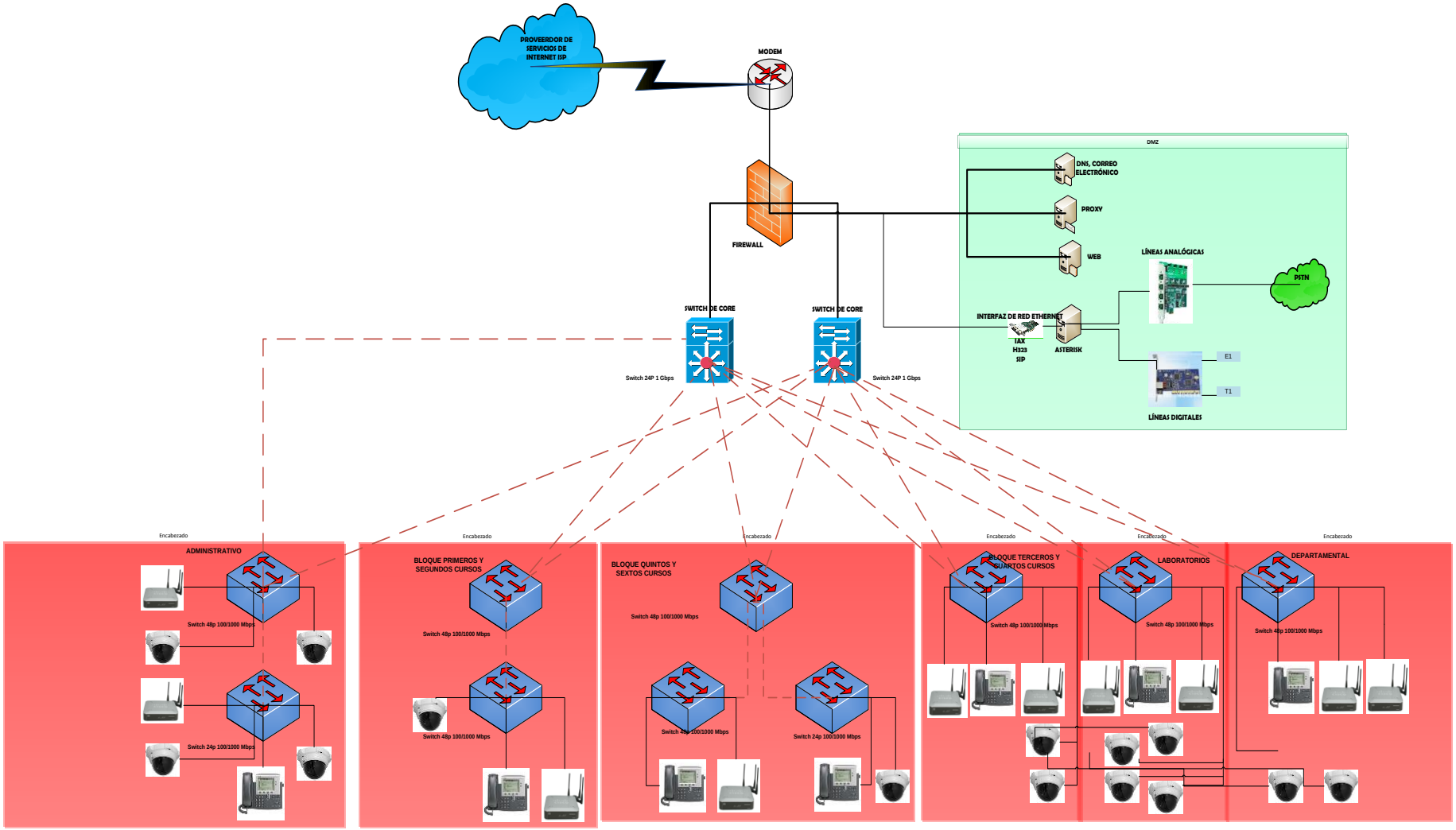


Figura 3.33 Diagrama de la red de Video Vigilancia

En la figura e.33 se indica el diagrama del diseño de la red de Video Vigilancia IP. Para la selección de las cámaras IP se tomará en cuentas los siguientes parámetros técnicos detallados a continuación:

- Un puerto 10/100 Fast Ethernet
- Protocolos TCP/IP, ARP, ICMP, HTTP, TELNET, SNMP Y DHCP
- Movimiento horizontal de cobertura 90°
- Detección de movimiento tanto de día como de noche (VMD) (Opcional)
- Formato de compresión MPEG-4 ó H.264
- Resolución de 640X480 pixeles ó superior
- Autenticación de usuario.
- Deberán soportar PoE norma IEEE 802.3af (Opcional)

Los precios de los equipos de la red de Videovilgilancia IP se encuentran en las proformas que se detallan en el **ANEXO E.**

3.11. UPS PARA EL CUARTO DE EQUIPOS Y CLOSET DE TELECOMUNICACIONES

Es necesario considerar el tiempo que los UPS pueden suministrar energía a los dispositivos que estén conectados después de que exista un corte del suministro eléctrico.

La capacidad del UPS es la suma de las potencias consumidas por los dispositivos a este conectados más un 40% adicional para que el equipo no trabaje al máximo de su capacidad; sin embargo, este es un sistema de emergencia por lo que no se puede seguir con las actividades normales en la Institución si existe un corte del suministro eléctrico.

3.11.1. CARACTERÍSTICAS MÍNIMAS DE LOS UPS

Deben cumplir los siguientes requerimientos mínimos para su adquisición.

- La capacidad debe ser de al menos 1000 VA o superior
- Tener una alimentación monofásica de 110 V y 60 Hz.
- Deben ser para montaje sobre *rack.*
- Smart.

3.12. SEGURIDAD DE LA RED

La implementación de una nueva red de datos para la Institución, además de aportar una amplia gama de servicios de los que se beneficie la Institución, trae también responsabilidades inherentes tanto a los usuarios de la red como al personal encargado del área de redes de la Institución. Para el correcto funcionamiento de la red y para garantizar su uso responsable de la misma.
Para tener un buen nivel de seguridad en el CEJPM es necesario cumplir con los siguientes requisitos: confidencialidad, autenticación, integridad, y disponibilidad de los datos. Para esto se debe crear ACLs, VLANs y adquirir algunos equipos que proporcionen seguridad adicional a la red tales como: Firewall, antivirus y equipos de autenticación de usuarios. Para que esto funcione correctamente, hay que tener políticas de seguridad adecuadas en la Institución.

Implementar un esquema de seguridad en la Institución conlleva a crear políticas que permitan disminuir el riego de un ataque tanto interno como externo garantizando un correcto funcionamiento de los servicios y aplicaciones que ofrece la red.

Debido a que siempre existirán ataques a las redes informáticas se debe formular políticas que vayan de acorde a la situación actual de la Institución y al desarrollo tecnológico. Además, dichas políticas deben ser evaluadas y actualizadas periódicamente para disminuir el riesgo de un posible ataque.

Antes de desarrollar las políticas de seguridad es necesario identificar los activos que deben ser protegidos para luego identificar las vulnerabilidades y los tipos de ataques a los que estarían expuestos.

3.12.1. ACTIVOS Y SUS VULNERABILIDADES

A continuación se detallan los activos y sus vulnerabilidades a los que se les implementaran ciertas políticas de acceso para protegerlos.

3.12.1.1. Estaciones de Trabajo

- Todos los usuarios tienen permisos de administrador
- No tiene restricciones de instalación y uso de programas que pueden dañar el equipo.

3.12.1.2. Equipo Activo de la Red

- Tienen la configuración por defecto
- Todos los puertos están habilitados.
- No utilizan VLANs por lo que tiene un solo dominio de broadcast
- Los closets de telecomunicaciones donde están ubicados no tiene cerradura
- Existen equipos que a los cuales tiene acceso todos los usuarios

3.12.1.3. Router Inalámbrico D-LINK

- Tiene habilitado el servidor DHCP
- Un AP está ubicado en un lugar accesible para algunos usuarios
- Utiliza WEP para autenticar a los usuarios, el cual no es recomendable para una Institución.

3.12.1.4. Central Telefónica

- Está ubicada en la recepción por lo que no cuenta con ningún nivel de seguridad.
- No dispone de ningún software para administrar la red telefónica.

Después de haber encontrado algunas vulnerabilidades que tiene la red actual se determina las políticas de seguridad físicas y lógicas que deben ser implementadas en la CEJPM.

Las políticas físicas son aquellas que se aplican al hardware de la red y al acceso indebido de personal no autorizado a ciertas localidades de la Institución. Al hablar de hardware es referirse por ejemplo seguridad en los puertos o interfaces de los equipos de Internetworking.

Las políticas lógicas son las que permiten o deniegan el acceso a los equipos mediante el uso de contraseñas, creación de usuarios con diferentes prioridades y configuración de los equipos de Internetworking

3.12.2. POLÍTICAS FÍSICAS Y LÓGICAS

3.12.2.1. Red LAN

Las políticas de seguridad físicas y lógicas sugeridas para la Institución son las siguientes:

- El cuarto de equipos y closets de telecomunicaciones tienen que estar cerrados con llave para controlar el acceso no autorizado a los equipos, y los usuarios con acceso deben llevar un registro de la hora de ingreso y salida detallando las modificaciones o monitoreo que realizaron.
- Los puertos de los switches (Acceso y Core) que no están siendo utilizados deben estar apagados, para evitar que cualquier usuario se conecte a la red sin autorización y si es requerido habilitar un puerto debe realizarse una solicitud por escrito al administrador de la red, el cual tiene que llevar un registro de la persona que solicito dicho servicio y la modificación que realizo en el equipo.
- Se debe configurar los puertos o interfaces de los equipos de Internetworking de tal forma que no sea posible conectar AP (Puntos de

Acceso) o switch en las salidas de telecomunicaciones que están destinadas a conectar ya sea estaciones de trabajo o teléfonos IP.

- Se deben crear VLANS de acuerdo al esquema detallado anteriormente en el direccionamiento IP.
- El control de flujo de tráfico en los equipos de Internetworking debe realizarse mediante la creación de ACLs.
- Realizar de forma periódica respaldo de la configuración de los equipos y de la información de la CEJPM, esta información es necesario en caso de emergencia.
- Cuando exista cambio de personal administrativo o de administración de la red se debe quitar todos los privilegios que el usuario tenía anteriormente y asignarle los nuevos permisos de acuerdo al tipo de usuario al que pertenezca.
- Los videos almacenados en el servidor de las cámaras IP solo puede ser administrada por el administrador de la red, pero si puede ser monitoreada por el usuario a cargo de la seguridad física de la Institución.
- Todos los cambios que se realicen en los servidores y en la configuración de los equipos debe ser registrado con hora y fecha indicando la razón y el usuario responsable de dichos cambios.
- La actualización de datos, y de configuración de servidores y equipos debe ser realizada en un horario fuera del laboral para no causar pérdidas de tiempo a los trabajadores y estudiantes de la Institución.
- Se debe utilizar un mecanismo de autenticación de usuarios utilizando control de acceso (Active Directory), mediante el cual se pueda adherir a un dominio común todas las estaciones de trabajo, para tener un mejor control de los mismos.
- Configuración adecuada del perfil de usuario, debido a que en este se define los permisos para modificar las configuraciones, archivos, parámetros del sistema operativo, servidores y equipos de Internetworking; razón por la cual cada usuario es responsable de los cambios que realice según su permiso y de administrar su contraseña.
- Se debe configurar los equipos y sistemas para actualizar la contraseña de forma mensual, activando el número de intentos erróneos de contraseña a

tres veces pasado esto el equipo debe bloquearse temporalmente. Además determinar la longitud de la contraseña.

- La navegación en Internet debe ser exclusivamente para investigación o para cumplir algunas actividades de la Institución más no para algún uso comercial, utilizar un servidor proxy para limitar el acceso a páginas que no tengan relación a esta actividad.
- El uso del correo electrónico Institucional debe ser únicamente para labores relacionadas a la CEJPM, no se deben enviar ni recibir correos con contenido de imágenes y videos
- Mediante la utilización de un firewall se deben bloquear todos los puertos que no se van a utilizar para disminuir posibles ataques.
- Utilizar un antivirus centralizado de tipo empresarial para proteger a toda la red de virus, gusanos y troyanos, indicando a los usuarios que reporten cualquier anomalía que tenga que ver con el ingreso de virus en el sistema.
- Los usuarios deben analizar con el antivirus las unidades extraíbles antes de abrir cualquier archivo.
- El administrador de la red debe hacer un seguimiento continuo de los logs generados por el sistema para estar enterado de todo lo que sucede en la red.
- En cuanto a la información que se considere de un alto grado de privacidad se debe cifrada para evitar un posible robo o alteración del contenido.
- El administrador de la red debe crear un cronograma de mantenimiento preventivo de hardware y software de todos los equipos conectados a la red y los de la red para mantenerlos en un óptimo funcionamiento.

3.12.2.2. Red WLAN

- Cambiar el nombre por defecto SSID por otro que no tenga relación con la Institución.
- Desactivar el broadcast SSID para evitar que la red sea encontrada e identificada fácilmente.
- Configurar a los equipos (AP) para realizar autenticación mediante filtrado MAC y cifrado de datos utilizando WPA con PSK.

- Realizar mantenimiento continuo de los puntos de acceso
- Crear un VLAN.

Adicionalmente, cabe indicar que para obtener una mejor seguridad se contará con un firewall el cual será en encargado de filtrar el tráfico interno y externo de acuerdo a las políticas de seguridad que se mencionaron anteriormente.

La sanción por el incumplimiento de las políticas físicas será una llamado de atención a los responsables (el usuario que permitió el ingreso y el que ingreso), en caso de ser reincidente la falta se le realizará un llamado de atención escrita por parte de la rectora de la Institución.
Para el caso del incumplimiento de las políticas lógicas, el o los usuarios perderán momentáneamente el acceso a la red obligándolos a un cambio de la contraseña, en caso de ser reincidente la falta se realizará un llamado de atención verbal por parte de la rectora de la Institución.

3.12.3. SEGURIDAD PERIMETRAL

Para brindar seguridad perimetral a la red de la CEJPM se utilizará un UTM[48] (Unified Threat Management Security Appliance) que es un dispositivo que tiene integrado varios servicios de seguridad. Los dispositivo UTM por lo general son equipos Appliance, lo que significa que son diseñados pasa realizar una función en concreto es decir equipos dedicados.

Estos equipos disponen de distintos interfaces de Red, que pueden utilizarse para diversas funciones o zonas que son:

- Zonas LAN
- Zonas WAN
- Zonas DMZ
- Zonas VPN

[48] UTM Unified Threat Management, dispositivo que permite la gestión unificada de amenazas.

Son equipos que ofrecen una solución integrada compuesta de diversos módulos. A continuación se citan los módulos más comunes:

- Antivirus
- Antispam
- Antispyware
- IDS
- IPS
- Firewall
- QoS
- NAT
- VPN

Existen varias empresas en el mercado que ofrecen equipos UTM, a continuación se menciona algunas tales como:

- D-Link
- Fortigate
- Ziwall
- Astaro
- Endian
- Security Point
- Check Point
- Cisco

Las características básicas que debe cumplir el UTM a elegir son:

- Firewall Throughput: 1000 Mbps o superior
- VPN Performance: 300 Mbps (3DES/AES) o superior
- 2 puertos WAN
- puertos LAN
    - 1 Puerto DMZ

- IPS
- Antivirus
- Antispam
- VPN
- NAT IPSec
- VLAN
- Políticas basadas en Routing
- Soportar VPN PPTP, IPSec, and L2TP + IPSec sin depender de un esquema de licenciamiento por usuario
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
- Aceleración por Hardware
- Filtrado a nivel de capa 7
- IGMP v3
- Prioridad de ancho de banda
- Balanceo dinámico de ancho de banda
- Alta disponibilidad (HA)

3.13. ADMINISTRACIÓN Y MONITORIZACIÓN DE LA RED

Para realizar la administración y monitoreo de todos los equipos de red y estaciones de trabajo se puede utilizar software libre o comercial, el cual ayudará al administrador de la red a tener un menor tiempo de respuesta en caso de presentarse algún inconveniente con algún equipo. Manteniendo la red operable y segura.

En cuanto a herramientas para administrar una red existe una gran variedad en el mercado, pero para la Institución se va a tomar en cuenta Net Tools y WhatsUp Gold, las características de cada uno se detallan a continuación: sin embargo, en el **ANEXO F** se presenta un análisis de las dos alternativas de software mencionadas para la administración de redes.

3.13.1. AXENCE NETTOOLS PRO

Axence NetTools Pro es una herramienta de distribución gratuita utilizada para la monitorización, seguridad y administración de redes locales y tiene incluido las siguientes herramientas:

NetWatch, esta herramienta es utilizada para monitorear la disponibilidad de hosts.

- WinTools, con esta herramienta se puede ver las características de algún equipo en la red.
- NetStat, permite revisar los paquetes de entrada y salida en la red.
- Local info, para ver información detallada del equipo local.
- Network scanner, escanea la red para descubrir todos los nodos de la red.
- Service & port scanner, para obtener información sobre los servicios y puertos.
- TCP/IP workshop, prueba diferentes servicios con este tool
- SNMP Browser y otras herramientas para lanzar Trazas, Pings, entre otros.

Esta herramienta tiene una interfaz gráfica bien amigable por lo que es muy fácil su manipulación para monitorear la red local.

3.13.2. WHATSUP GOLD

WhatsUp Gold [24] ofrece monitoreo de aplicaciones y de redes de forma fácil mediante la interfaz web permitiendo un control total de la infraestructura y aplicaciones de la red. Además, provee una fácil configuración, escalabilidad y simplicidad.

WhatsUp Gold permite aislar los problemas de la red y proporciona visibilidad y comprensión sobre rendimiento y disponibilidad de la red. A continuación se detalla algunas funciones que realiza son:

- Identifica y mapea los dispositivos de la red
- Envía notificaciones cuando un dispositivo falla
- Almacena información de forma periódica de la red para generar reportes
- Proporciona monitoreo continuo de la red de forma local o remota.
- Identificación y Mapeo Dinámico descubriendo la red en minutos utilizando ayudantes de instalación intuitivos para rastrear routers, switches, servidores, impresoras, host y otros dispositivos conectados a la red. Toda la información obtenida es almacenada en una base de datos para luego ser utilizada para una mejor gestión y generación de reportes.
- Realiza la identificación y mapeo de direcciones MAC y direcciones IP, descubriendo la conectividad entre los puertos de un switch y los dispositivos conectados, optimizando la localización de recursos.
- Para una mejor administración envía alertas vía correo electrónico, beeper, SMS, audio y las respectivas alertas que son enviadas a la bandeja de tareas del Sistema.
- Monitoreo de SNMP y WMI

Además de utilizar SNMP v1/2/3 para monitoreo y reportes, también utiliza el WMI[49] de Microsoft para obtener información histórica y en tiempo real sobre todos los dispositivos Windows de la red.

En función de las características técnicas y económicas de cada una de las herramientas antes mencionadas se recomienda utilizar Axence *Net Tools Pro* para la administración de la red CEJPM.

Cabe, indicar que WhatsUp Gold tiene mejores características técnicas para administrar una red, pero se escogió Axence NetTools Pro porque es de libre distribución y fácil de manipular. Además, la red de la CEJPM es una red pequeña por lo que no requiere una herramienta avanzada para su administración.

[49] (WMI) Windows® Management Instrumentation: es un estándar de Microsoft Windows para obtener información de sistemas bajo Windows.

3.14. RECOMENDACIÓN PARA LA SELECCIÓN DEL ANTIVIRUS

Es recomendable adquirir un antivirus de tipo empresarial para mantener la CEJPM libre de virus, gusanos, spam, entre otros. Estos antivirus tienen la ventaja de gestionar las actualizaciones y buscar virus de manera centralizada disminuyendo la carga de la red.

La mayoría de riesgos en seguridad informática se encuentran al interior de la red empresarial, sea por infiltraciones exitosas originadas fuera de la organización, o por ataques internos. Estas amenazas pueden tomar múltiples formas, desde infecciones de virus hasta robo de información confidencial. Para controlarlas, hace falta amplia funcionalidad, incluyendo:

- Control antimalware
- Monitoreo de usuarios
- Administración de políticas
- Administración de Hardware y Software

En el **ANEXO G** se realiza un análisis de tres alternativas de antivirus del tipo empresarial, los cuales pertenecen a los fabricantes Panda, Kaspersky y Symantec.
En función de las características de cada uno de los antivirus antes mencionados se recomienda utilizar el antivirus Kaspersky en la red CEJPM.

3.15. EQUIPOS Y MATERIALES

Después de haber presentado todo los elementos que se requieren para implementar el cableado estructurado en la CEJPM, en la tabla 3.44, se detalla la cantidad total de todos los accesorios que serán utilizados en la implementación del cableado estructurado
Los equipos seleccionados se detallan en las tablas 3.44 y 3.45 y sus características técnicas se especifican en el **ANEXO H**.

Adicionalmente, en la tabla 3.44 se detallan los elementos requeridos para la red pasiva del CEJPM.

NÚMERO	ÍTEMS	DESCRIPCIÖN	CANTIDAD (U)
1	Jacks	Cat 6	
2	Face Plate	Dobles	
		Simples	
3	Canaleta Plástica	32x12	
		40x24	
		40x40	
		60x40	
4	Codo Interno	32x12	
		40x24	
		40x40	
		60x40	
5	Codo Externo	32x12	
		40x24	
		40x40	
		60x40	
6	Codo Plano	32x12	
		40x25	
		40x40	
7	Derivación en T	40x25	
		40x40	
		60x40	
8	Terminación	32x12	
9	Cable UTP CAT 6	Bobina de 305 m	37
10	Fibra Óptica Multimodo	OM1 Ruta A	50 m
11	Fibra Óptica Multimodo	OM1 Ruta B	138 m
12	Fibra Óptica Multimodo	OM1 Ruta C	175 m

13	Fibra Óptica Multimodo	OM1 Ruta D	210 m
14	Fibra Óptica Multimodo	OM1 Ruta E	109 m
15	Conduit Metálico 3 m	¾	
		1	
		1 1/4	
16	Codos Metálicos	¾	
		1	
		1 1/4	
17	Cajetines	De paso 20x20	
18	Patch Cord de 3 m	Cat 6	275
19	Patch Cord de Fibra Óptica	LC-LC	14
20	SFP	1000BASE-SX SFP transceiver module MMF 850nm DOM	28
21	Patch Panel	Cat 6, 24p	8
22	Patch Panel	Cat 6, 48p	7
23	ODF	Interconexión de Fibra	6
24	Organizador	Horizontal	17
25	Organizador	Vertical	24
26	Panel de Alimentación	AC	7
27	Closet de Telecomunicaciones	13	1
		15	2
		23	2
28	Rack Abierto	42 U	1

Tabla 3.44 Elementos para el Cableado Estructurado

En la Tabla 3.45 se indica aquipos activos de la red.

NÚMERO	ÍTEMS	DESCRIPCIÓN	CANTIDAD
1	Switch de Acceso	24 puertos *de* 10/100 Mbps full dúplex 2 puertos Uplink *de* 10/100 /1000 Mbps full dúplex Auto negociación de la velocidad de los puertos Apilable Administrable mediante consola o vía interfaz Web Conmutación a nivel de capa 2 Debe soportar el protocolos IP, STP, RSTP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional) Soporte de VLANs IEEE 802.1q Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC. Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. Velocidad de backplane mínima de 8.8 Gbps IP versión 4 y 6 Soporte de 8000 direcciones MAC Soporte de paquetes de telefonía IP (VoIP) PoE norma IEEE 802.3af	2
1	Switch de Acceso	48 puertos *de* 10/100 Mbps full dúplex 2 puertos Uplink *de* 10/100 /1000 Mbps full dúplex Auto negociación de la velocidad de los puertos Apilable Administrable mediante consola o vía interfaz Web Conmutación a nivel de capa 2 Debe soportar el protocolos IP, STP, RSTP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional) Soporte de VLANs IEEE 802.1q Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC. Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. Velocidad de backplane mínima de 8.8 Gbps IP versión 4 y 6 Soporte de 8000 direcciones MAC Soporte de paquetes de telefonía IP (VoIP) PoE norma IEEE 802.3af	6

2	Switch de Core	- 24 puertos *de* 10/100/1000 Mbps full dúplex - Auto negociación de la velocidad de los puertos - Apilable - Administrable mediante consola o vía interfaz Web - Conmutación a nivel de capa 2,3 y 4 - Debe soportar el protocolos IP, STP, RSTP, RIPv1 y 2, DHCP, Telnet y SNMPV (1, 2 y 3), OSPFV (2 y 3), RMONV (2 y 3) entre Otros. - Manejo y Administración de VLANs IEEE 802.1q - Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL) a nivel 2,3 y 4, prevención mediante (DoS) y filtrado basado en MAC. - Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. - Velocidad de backplane mínima de 88 Gbps - IP versión 4 y 6 - Manejo, priorización y clasificación de tráfico VoIP	2
3	Access Point	- Tasa de transmisión de 54 Mbps - Protocolo de gestión: SNMP (v1, v2, v3) - IEEE 802.3af - Algoritmo de cifrado DES y AES - Filtrado MAC - Soporte estándares: IEEE 802.11g, IEEE 802.11e, IEEE 802.11q y IEEE 802.11x - 1 interfaz Fast Ethernet - Configuración de SSID - Soporte de VLANs - Certificación Wi-Fi	10
5	Central Telefónica IP	- Interfaces FXO (3) y FXS - Soporte mínimo para 40 Usuarios - Protocolos de señalización - Control de llamadas - IVR - Correo de voz - Administración vía web - Distribución automática de llamadas - Soporte de códecs G.729a - Soporta Auto negociación de códec - Software basado en Asterisk (Elastix)	1

4	Teléfonos IP	• Conector RJ45 • PoE support (802.3af) • Soporte de códecs G.729 • Soporte DHCP • QoS (802.1p) • Compatibilidad con protocolos de administración • Calidad de voz • Identificador de llamadas • Llamada en espera • Transferencia de llamadas	40
5	Cámaras IP	• Un puerto 10/100 Fast Ethernet • Protocolos TCP/IP, ARP, ICMP, HTTP, TELNET, SNMP Y DHCP • Movimiento horizontal de cobertura 90° • Detección de movimiento tanto de día como de noche (VMD) • Formato de compresión MPEG-4 ó H.264 • Resolución de 640X480 pixeles ó superior • Autenticación de usuario. • Deberán soportar PoE norma IEEE 802.3af • Administrables	16
4	Servidores	• Procesador: 2.6 GHz o superior, • Memoria RAM: 2 GHz o superior • Disco Duro: Mínimo: 640 GB o superior • Tarjeta de red 10/100/1000 Mbps	2
8	Firewall	• Firewall Throughput: 1000 Mbps o superior • VPN Performance: 300 Mbps (3DES/AES) o superior • 2 puertos WAN • 3 puertos LAN • 1 Puerto DMZ • IPS • Antivirus • Antispam • VPN • NAT IPSec • VLAN • Políticas basadas en Routing • Soportar VPN PPTP, IPSec, and L2TP + IPSec sin depender de un esquema de licenciamiento por usuario • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES • Aceleración por Hardware • Filtrado a nivel de capa 7 • IGMP v3 • Prioridad de ancho de banda • Balanceo dinámico de ancho de banda • Alta disponibilidad (HA)	1

Tabla 3.45 Elementos activos de la red

CAPÍTULO IV

4. Implementación de un prototipo, pruebas y resultados

4.1. PROTOTIPO DE PRUEBA

El diagrama del prototipo de prueba se detalla en la figura 4.1.

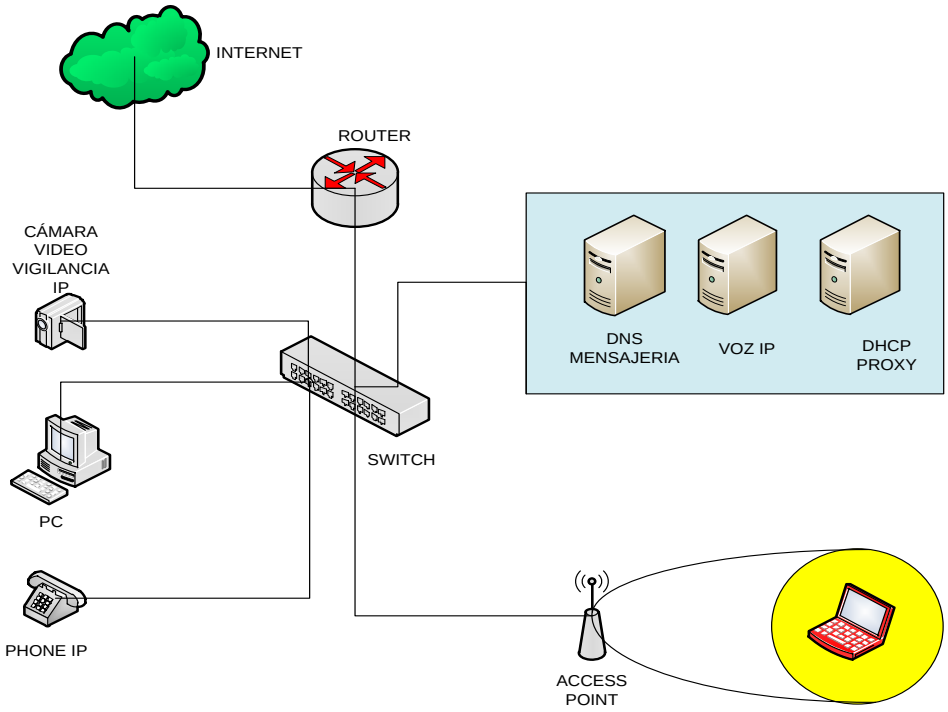


Figura 4.1 Prototipo de prueba

4.1.1. IMPLEMENTACIÓN DE LOS SERVIDORES DHCP, DNS Y PROXY

Para la instalación de los servidores DHCP, DNS y Proxy se utilizará el sistema operativo Red Hat 5

4.1.1.1. Instalación y Configuración del Sistema Operativo Red Hat 5

A continuación se detallan los pasos más importantes para instalar y configurar Red Hat 5.

Al empezar la instalación es recomendable presionar ***Enter*** para instalar desde cero el sistema operativo como se indica en la figura 4.2.

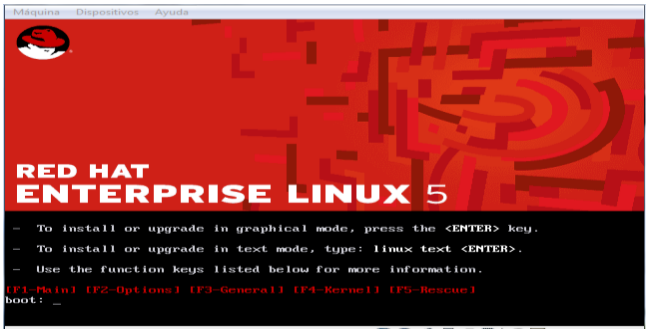


Figura 4.2 inicio de la instalación de Red Hat

Otra parte importante en la instalación es la elección de los servidores que se desea instalar, para este caso se requiere los servidores DNS, DHCP y Proxy como se indica en la figura 4.3.

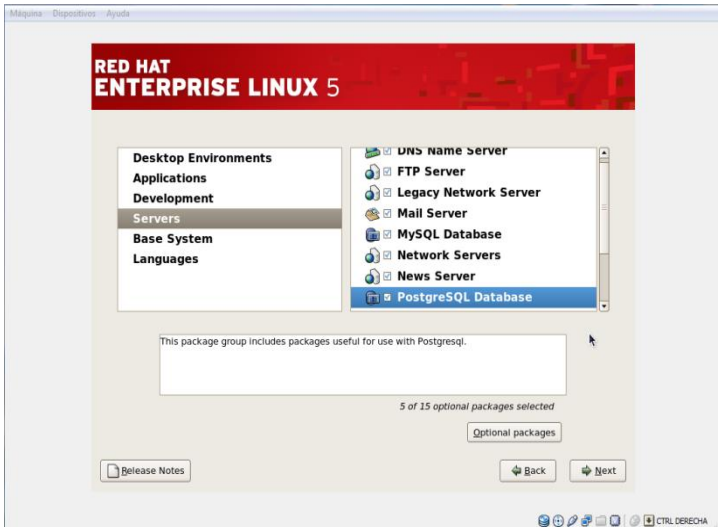


Figura 4.3 Selección de los servidores (Continuación)

Al finalizar la instalación es importante seleccionar servicios específicos que el firewall deje pasar y para que filtre acceso no autorizado como se indica en la figura 4.4

Figura 4.4 Selección de servicios específicos (continuación)

4.1.1.2. Configuración del servidor DHCP (Dynamic Host Configuration Protocol)

DHCP es un estándar TCP/IP creado para simplificar la configuración IP de los equipos de una red. Debido a que la asignación de direcciones IP es de forma automática sin necesidad de hacerlo manualmente.

Para configurar un servidor DHCP se modifica el archivo ubicado en /etc/**dhcpd.conf**

En la figura 4.5 se detalla la configuración realizada en el archivo. En el cual se utilizó la dirección IP privada 10.93.2.0 con máscara 255.255.255.0 con el rango de direcciones que va desde la 10.93.2.100 hasta la 10.93.2.114, la dirección broadcast es la 10.93.2.255 y la de Gateway será la 10.93.2.1

Los parámetros que se configuran son los siguientes:

- option routers (Esta es la dirección del servidor)
- option subnet-mask (Para la máscara de red)
- option domain-name (Nombre del dominio)
- Range (Rango de direcciones IP)

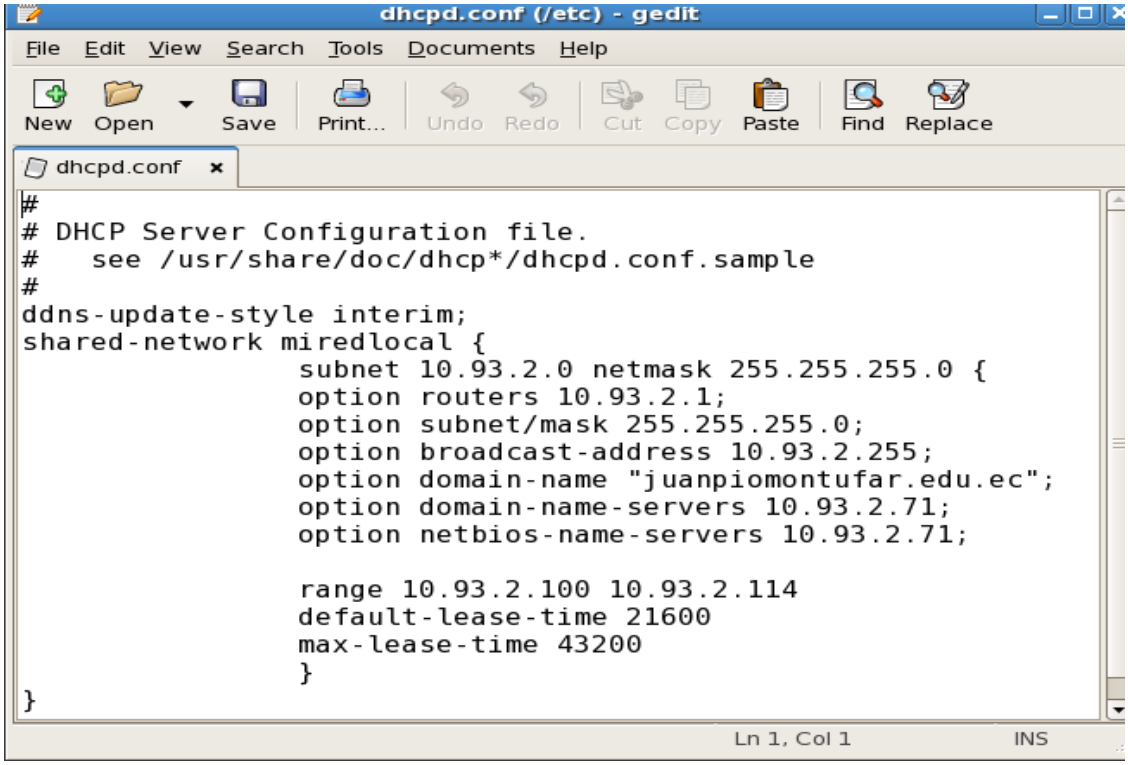


Figura 4.5 Configuración del servidor DHCP

Para realizar la comprobación del servidor DHCP se utilizó el comando ***ipconfig*** en una computadora que tiene el sistema operativo Windows, lo cual se indica en la figura 4.6.

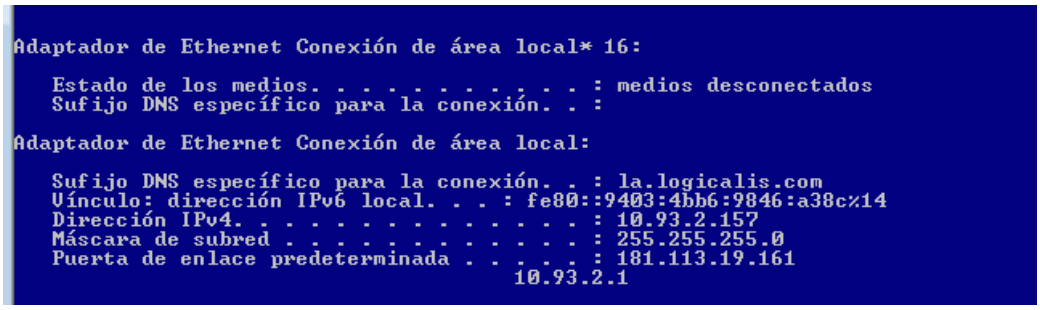


Figura 4.6 Prueba realizada (Continuación)

4.1.1.3. Configuración del servidor DNS

Un servidor DNS permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan las direcciones IP y los nombres de las PCs pertenecientes a su dominio.

Los servidores DNS se encuentran de forma jerárquica de modo que si el servidor local no puede resolver una petición, este lo traslada al DNS superior.

Primero se realiza la configuración del fichero ***/etc/hosts***, agregando el nombre del equipo que desempeñara la función de servidor DNS así como también la dirección IP asignada a ese equipo como se detalla en la figura 4.7.

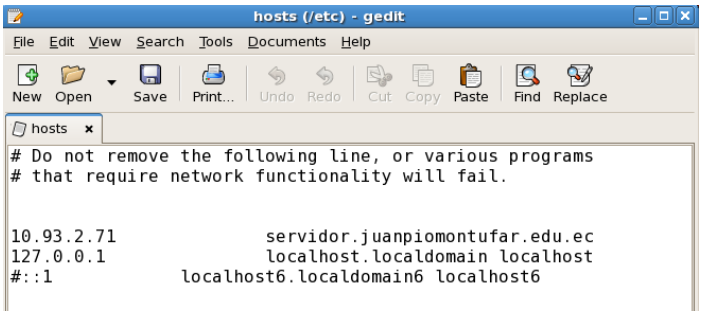


Figura 4.7 configuración del archivo */etc/hosts*

Ficheros de configuración del DNS

Los siguientes archivos deben ser creados y configurados como se detallan en las figuras 4.8, 4.9, 4.10, 4.11 y 4.12.

- /var/named/chroot/etc: aquí se crea el archivo “named.conf”.
- /var/named/chroot/var/named: creación de los ficheros de zona que son invocados por named.conf.

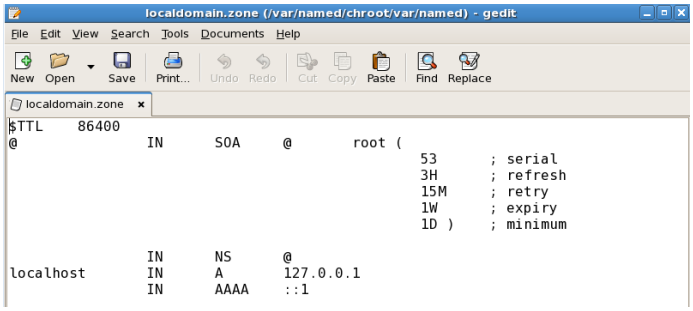


Figura 4.8 Configuración del archivo localdomain.zone

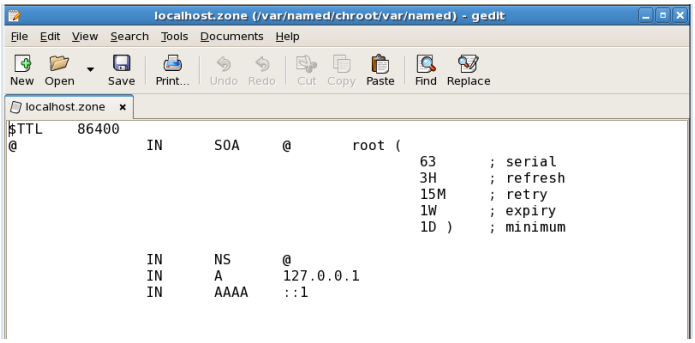


Figura 4.9 Configuración del archivo localhost.zone

Generación del fichero “named.conf” dentro de la ruta “/var/named/chroot/etc/”:

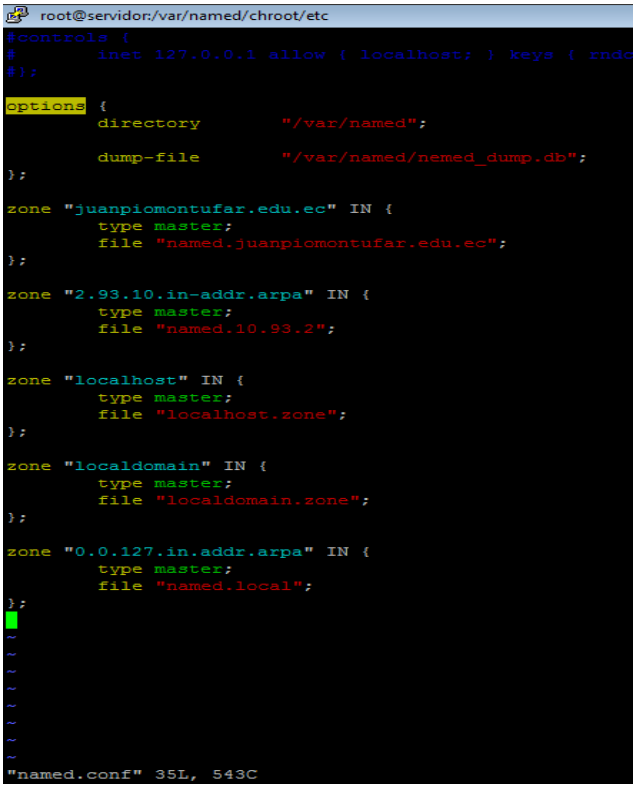


Figura 4.10 Configuración del archivo named.conf

Generación del fichero para la resolución de la zona inversa “named.10.93.2” dentro de la ruta “/var/named/chroot/var/named/”

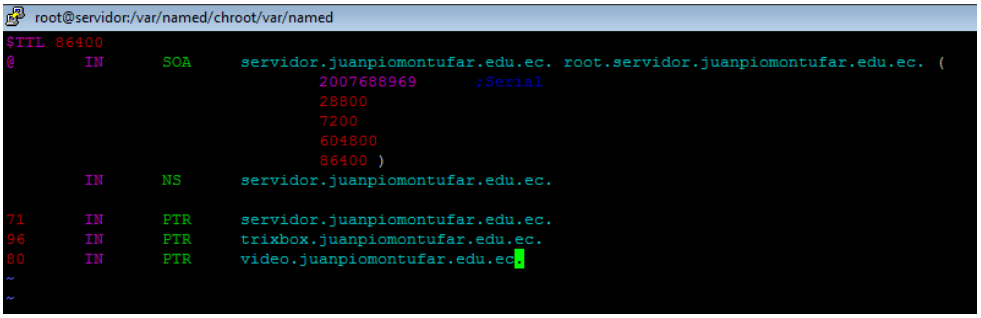


Figura 4.11 Configuración del archivo named.10.93.2

Generación del fichero para la resolución de la zona directa "named.juanpiomontufar.edu.ec" dentro de la ruta "/var/named/chroot/var/named/"

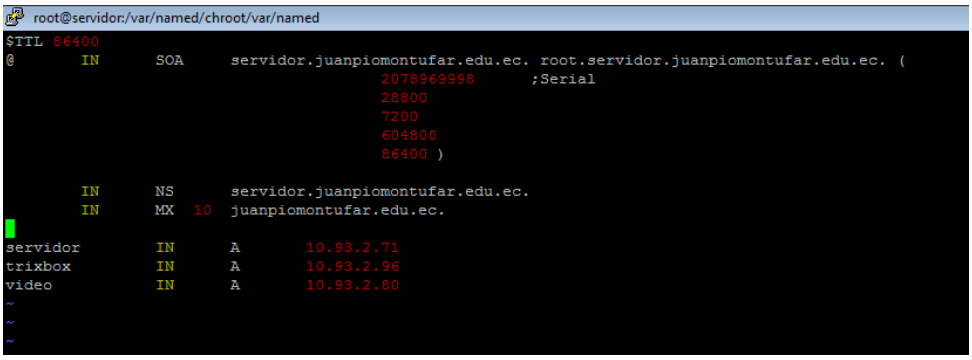


Figura 4.12 Configuración del archivo named.juanpiomontufar.edu.ec

Para comprobar el correcto funcionamiento del servidor se utiliza el comando ***nslookup.***

Primeramente se consulta el nombre correspondiente a la dirección IP 10.93.2.71 obteniendo como respuesta el nombre servidor.juanpiomontufar.edu.ec.

Luego se consulta la dirección IP correspondiente al nombre servidor.juanpiomontufar.edu.ec, esto se indica en la figura 4.13.

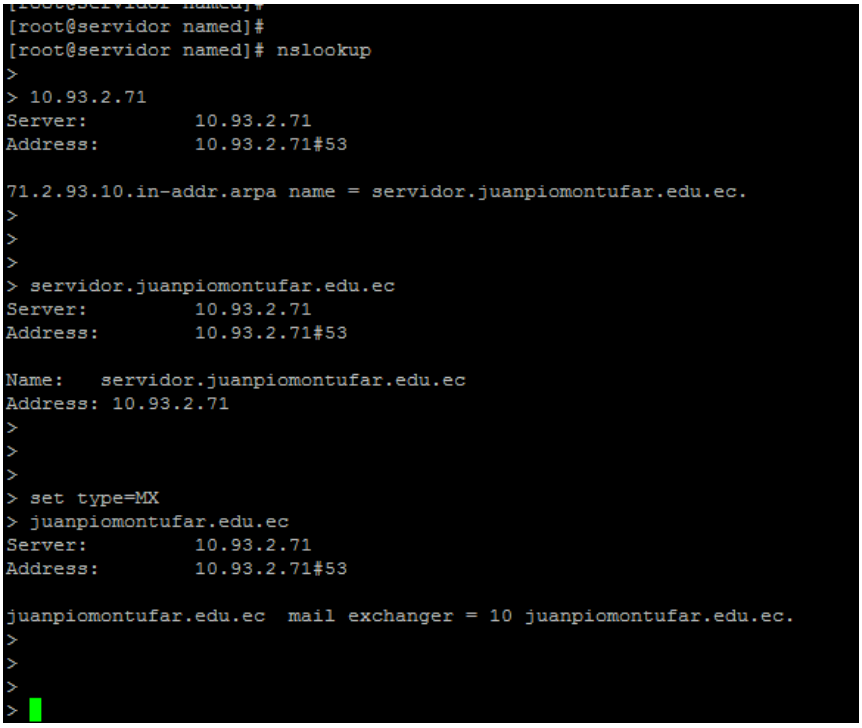


Figura 4.13 Pruebas de DNS con nslookup.

4.1.1.4. Configuración del servidor Proxy (Squid)

Squid es un software utilizado como servidor proxy, es de libre distribución y está basado en UNIX. Además ofrece confiabilidad, robustez y versatilidad convirtiéndolo en uno de los más populares.

Squid también puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de red para los protocolos HTTP, FTP, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS, filtración de contenido y control de acceso por IP y por usuario.

La configuración se la realizo en el fichero ***squid.conf*** localizado en la ruta ***/etc/squid/squid.conf*** como se detalla en la figura 4.14.

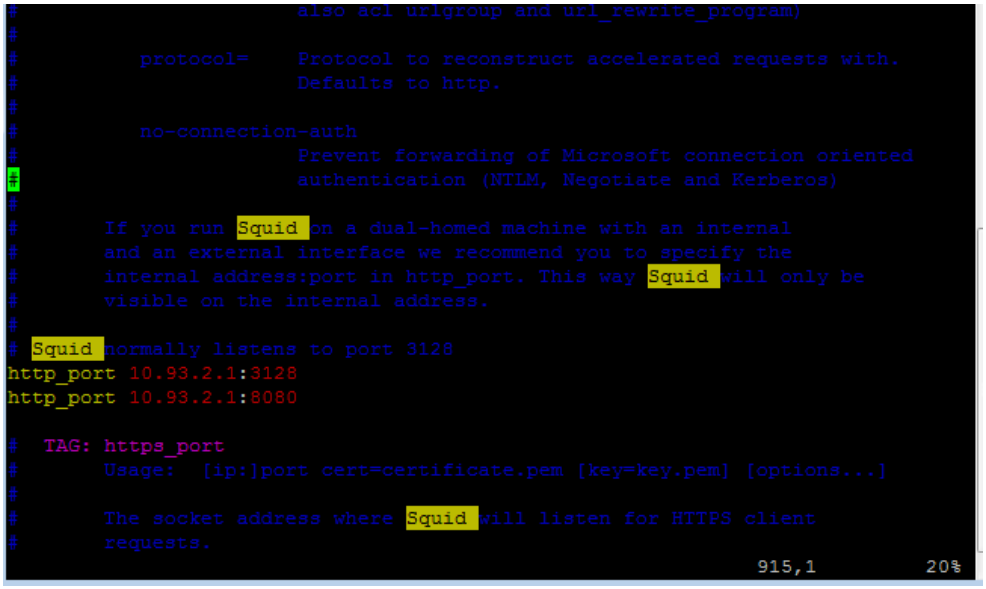


Figura 4.14 habilitación de los puertos

Creación de las ACLs para el control. (Figura 4.15).

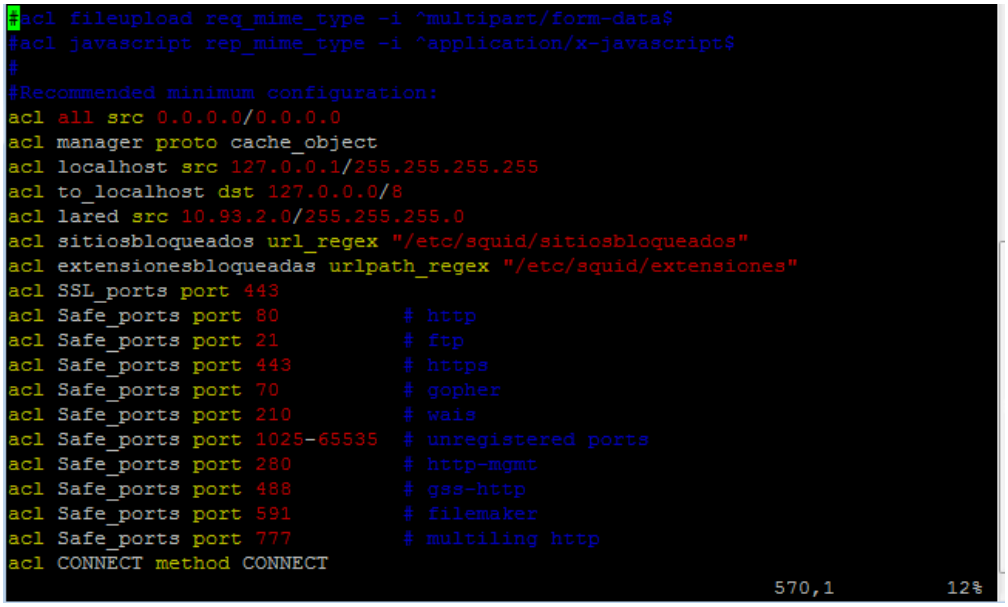


Figura 4.15 Creación de Listas de Control de Acceso.

En la figura 4.16 se crean las reglas para el control de acceso.

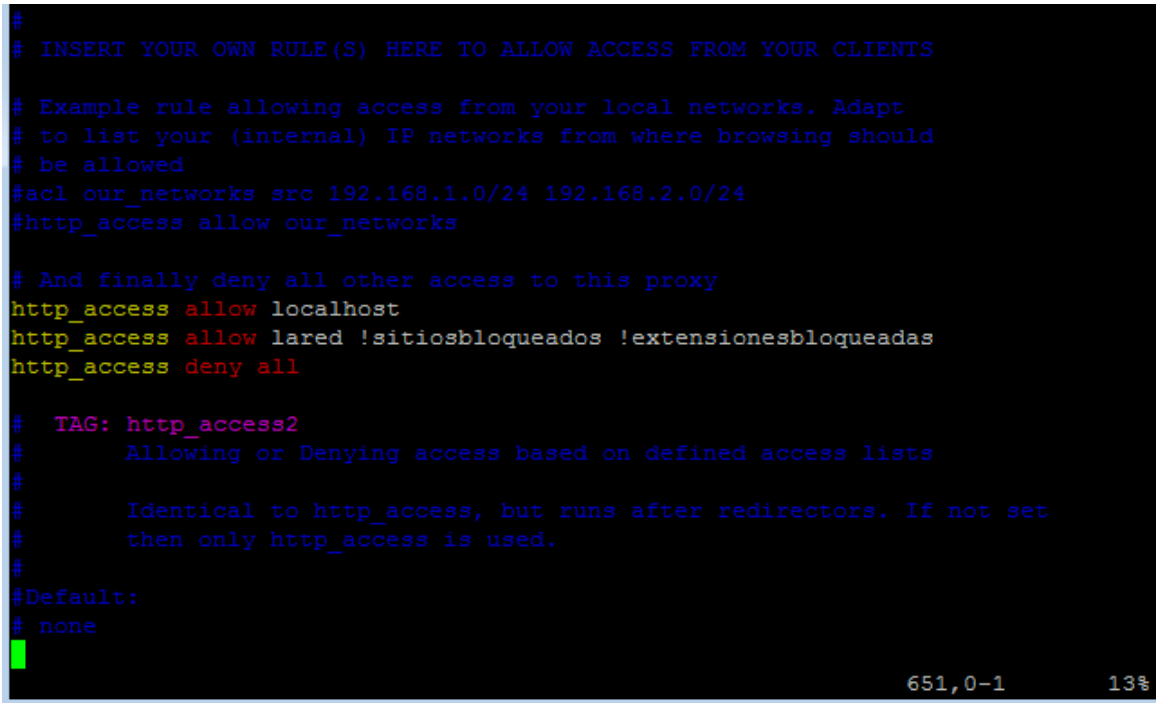


Figura 4.16 Configuración de acceso para los puertos.

Creación de los ficheros ***sitiosbloqueados*** para restringir sitios web no deseados por la Institución y de extensionesbloqueadas para que los usuarios no puedan descargar archivos con las extensiones guardadas en dicho fichero. (Figura 4.17).

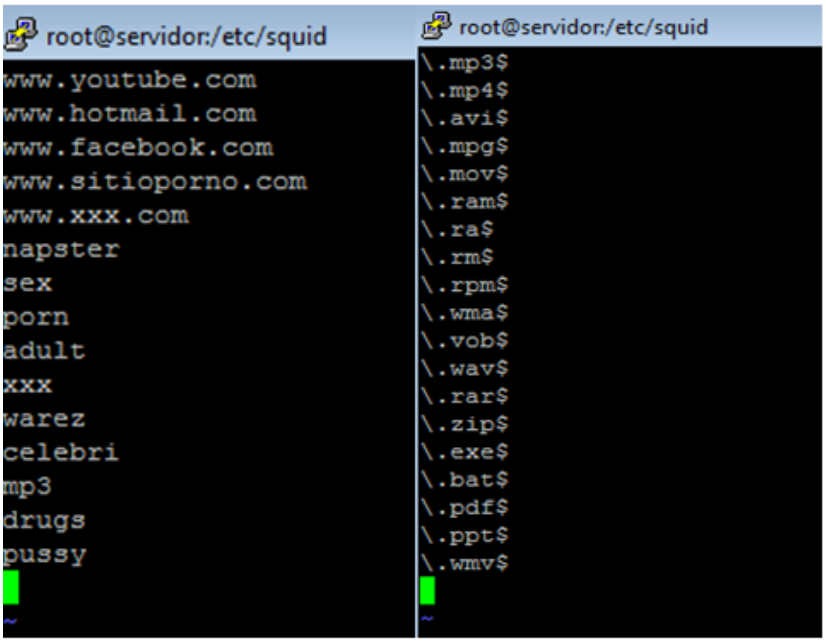


Figura 4.17 Configuración de sitios web no deseados.

3.17.2 IMPLEMENTACIÓN DE LA CENTRAL TELEFÓNICA IP TRIXBOX CE

Trixbox es una distribución ideal para pequeñas empresas donde no se requiere un gran número de extensiones. Además, su ambiente gráfico permite una fácil instalación y configuración sin necesidad de tener gran conocimiento en el sistema operativo Linux y mucho menos en Asterisk.

Los componentes que vienen incluidos en Trixbox son:

- Linux Centos como Sistema Operacional
- Asterisk el cual es el núcleo de la telefonía
- Drivers Zapata telephone
- Librería para soporte RDSI (Requerido para las tarjetas FXO/FXI)
- FreePBX entorno gráfico para la configuración mediante interfaz web
- FOP (Flap Operator Panel) para monitoreo de Asterisk
- Web Meet Control: es el administrador para salas de conferencias

La instalación se la realizará en una máquina virtual utilizando VMware ESXi 4.1.0 en el sistema operativo Red Hat.

4.1.1.5. VMware

VMware es una aplicación que permite ejecutar diferentes Sistemas Operativos simultáneamente en el mismo equipo de manera virtual. VMware ofrece un buen desempeño con servidores.

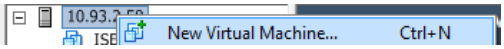
4.1.1.6. Instalación de VMware en Red Hat

Para instalar VMware ESXi en el servidor físico se descarga la versión más reciente desde la dirección *http://www.vmware.com* y se realiza los siguientes pasos:

- Grabar en un CD/DVD la imagen .iso
- La instalación es en modo texto
- Pulsamos F11 para aceptar la EULA
- Seleccionamos el disco donde instalaremos ESXi, pulsamos F1, en nuestro caso al tener solo uno no es necesario, pulsamos “Enter”.
- Selleccionamos el idioma.
- Introducimos la clave de root, la cual debe poseer siete caracteres como mínimo
- Confirmamos la instalación pulsando “F11”.
- Una vez instalada, pulsamos “Enter” para reiniciar.
- Pulsamos “F2” para configurar la IP estática para ser administrador por vSphere Client o el cliente web, nos autenticamos con root y el pass configurado en la instalación.
- Con la indicación de la IP estática se finaliza la instalación.

4.1.1.6.1. Crear y configurar la maquina virtual Trixbox

La creación de una maquina virtual en Vmware es bien sencillo solo se realiza los siguientes pasos:

- Hacer click derecho en la IP del servidor en el icono, seleccionamos New Virtual Machine 

- Seleccionar la configuración para la máquina virtual
- Nombre de la máquina virtual
- Selecionar el datastore, en el que se almacenaran los archivos de la máquina virtual
- Nombre y tipo de Sistema Operativo
- Tamaño del HD
- Instalar e iniciar la máquina virtual.
- Es posible modificar las características de la maquina virtual una vez creada e instalada.

4.1.1.6.2. Requisitos mínimos de Hardware para la instalación

Se requiere de un PC o servidor que cumpla con las siguientes características:

- Pentium IV de 1.8 GHz
- Memoria de 512 MB
- HD de 8 GB
- Tarjeta de re 10/100 Mbps
- Unidad CD-ROM

4.1.1.6.3. Pasos para la instalación

Para una correcta instalación de Trixbox se efectúa 2 pasos previos que son importantes, primero saber el número de usuarios que requieren telefonía y el segundo consiste en definir qué tipo de servicios se brindará a los usuarios.

La primera actividad se le conoce como “Planificar el plan de marcación” ó DIAL PLAN, que para este caso se definirá de la forma que esta detallado en la tabla 4.1.

PLAN DE MARCADO		
EXTENSIONES POR DEFAULT	#	Directorio Telefónico del Sistema
	*43	Prueba de echo de llamadas
	*52	Extension no disponible OFF
	*53	Extension no disponible ON
	*60	Hora del sistema
	*65	Prueba de sonido audible de la extensión
	*69	Ultimo número que ha llamado
	*70	Llamada en espera ON
	*71	Llamada en espera OFF
	*72	Desvió de llamada ON
	*73	Desvío de llamada OFF
	*77	Grabar mensaje de IVR

	*78	Opción de “No molestar” ON
	*79	Opción de “No molestar” OFF
	*91	Teléfono ocupado no disponible ON
	*92	Teléfono ocupado no disponible OFF
	*97	Cambiar el mensaje de bienvenida del buzón
	*98	Acceso al buzón de mensajes
	*99	Oír la grabación de mensaje de IVR
	70	Poner en espera de transferencia de llamada PARKING
EXTENSIONES PROPIAS	500	Alexis Paspuel
	501	Fanny Rodriguez
	512	Miguel Lema

Tabla 4.1 DIAL PLAN

Luego de tener bien claro los pasos previos mencionados en la tabla 4.18 se realiza la instalación de la central telefónica IP.

Figura 4.18 Ventana de instalación de Trixbox

Instalar el sistema Trixbox es muy sencillo ya que no requiere ningún nivel avanzado porque solo pide se ingrese:

- Idioma del teclado
- Uso horario

- IP fija o estática la cual puede ser configurada luego de la instalación utilizando el comando ***system-config-network***
- Password para acceder al sistema

Una vez terminada la instalación, el sistema pide el nombre de usuario que sería ***root*** y el password ingresado durante la instalación y, el servidor está listo para ser configurado, para ello se ingresa desde un browser con la dirección IP que se asigno para este caso http://10.93.2.96 luego para se accede al sistema como usuario maint y password password como se indica en la figura 4.19.

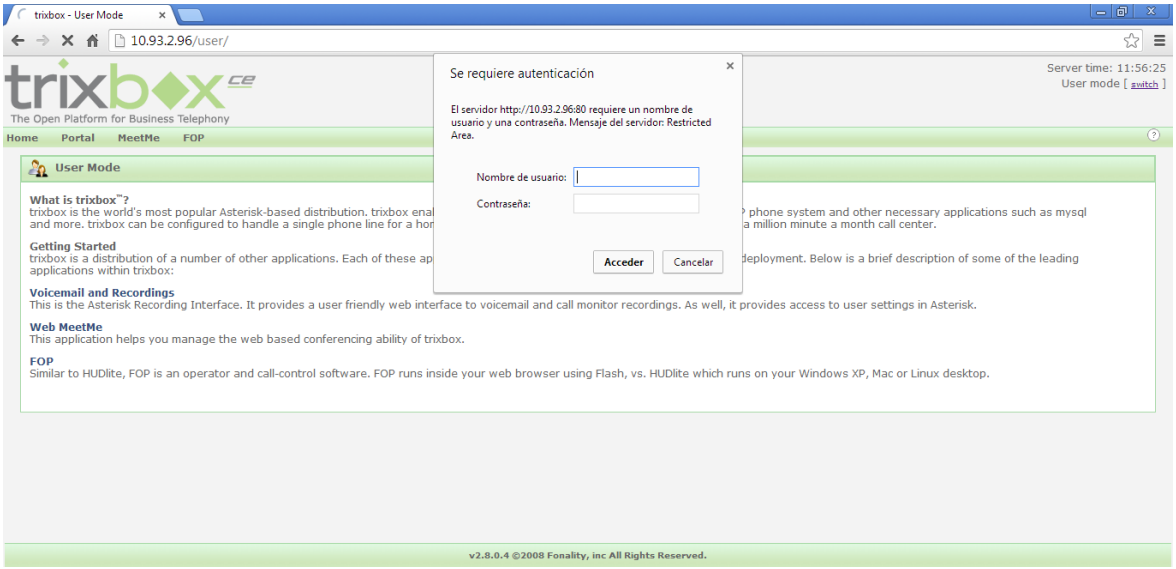
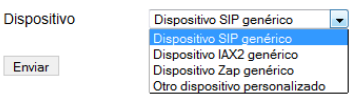


Figura 4.19 Ingreso al sistema (continuación)

4.1.1.7. Configuración de extensiones

Pasos para configurar una extensión: (Figura 4.20).

- Ingresar a PBX y setting PBX
- Ingresar a la opción de extensiones y seleccionar el tipo de extensión a crear



- Los datos básicos a ingresar son: extensión del usuario y nombre para mostrar en la pantalla del teléfono 3CX

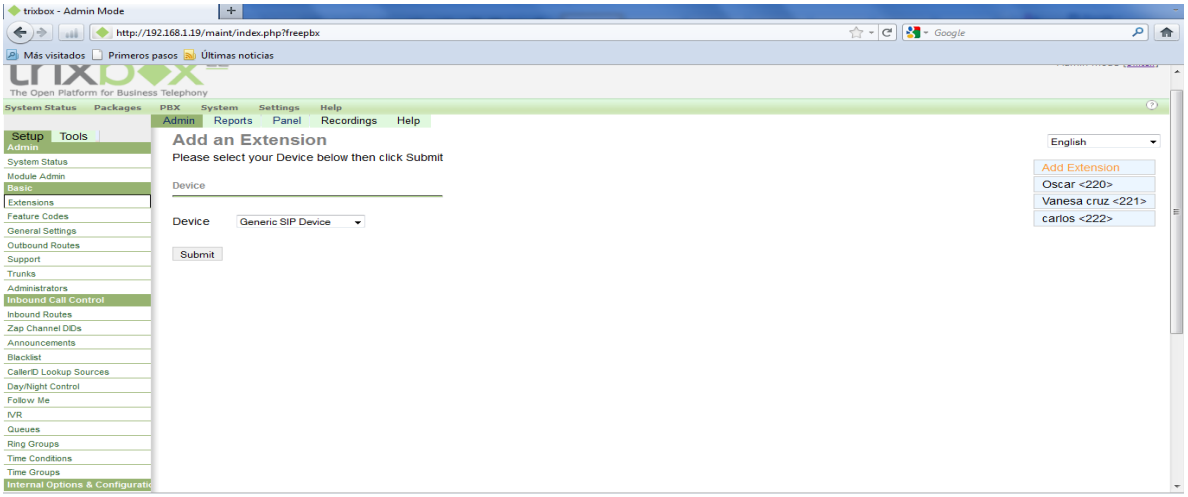


Figura 4.20 Extensiones configuradas

4.1.1.8. Configuración de una Troncal

Trixbox CE tiene varias opciones para crear líneas troncales que son:

- Añadir línea troncal Zap (Modo de compatibilidad con DAHDI)
- Añadir línea troncal IAX2
- Añadir línea troncal SIP
- Añadir línea troncal ENUM
- Añadir línea troncal DUNDi
- Añadir línea troncal personalizada

Para este proyecto se escoge la primera opción debido a que la tarjeta instalada en la PC es analógica.

4.1.1.9. Teléfono 3CXPhone

Teléfono 3CX [25] es completamente gratuito para usuarios individuales y para empresas incluyendo entidades comerciales. Todas las características incluyendo transferencia de llamada, están habilitadas. Esto facilita a las empresas, la instalación en cualquier escritorio de Windows, sin tener que preocuparse acerca del costo o problemas de administración de licencias. Además, cuenta con una interfaz intuitiva y fácil de usar.

Teléfono 3CX está disponible en 3 versiones:

- Para Microsoft Windows XP, Vista y 7
- Dispositivos basados en Android 1.6, 2.1, 2.2 tales como Google Nexus, Sony Xperia, Motorola Droid o Samsung Galaxy e Iphone 3G, 3GS 4, 4S, 5, 5S y 5C

4.1.1.9.1. Características del Teléfono 3CXPhone

Las características del teléfono 3CXPhone son:

- Habilidad para grabar llamadas al disco con un solo clic de un botón.
- Teléfono 3CX es un teléfono SIP que puede ser aprovisionado fácilmente en toda la red. A través de un URL,
- Aplicación pequeña y rápida
- Habilidad para trasferir llamadas o ponerlas en espera
- Multi-líneas (Windows)
- Soporta múltiples perfiles SIP
- Muestra registro / historial de llamadas personales
- Soporta & adhiere a los estándares RFC SIP
- Soporta G.711 (Ley-A y Ley-u), GSM y codecs Speex
- Soporte STUN para NAT/firewall traversal
- Archivo de instalación provisto como MSI para fácil despliegue (Windows)
- Funciona perfectamente como teléfono SIP con la Central Telefónica 3CX para Windows, la cual es una central SIP basada en software que reemplaza completamente una central telefónica propietaria tradicional.

4.1.1.9.2. Instalación del Teléfono 3CXphone

La instalación es bien sencilla, se descarga la aplicación desde http://www.3cx.es y se realiza los siguientes pasos:

- Ejecutar la aplicación y seleccionar Next (Pantalla de bienvenida)
- Aceptar las condiciones y Next
- Ingresar el directorio donde se va a instalar 3CXPhone
- Finalizar

4.1.1.9.3. Configuración del Teléfono 3CXphone

Para configurar 3CXPhone se realiza los siguientes pasos (Figura 4.21)

- Click en la pestaña
- En el menú ingresar a la opción Accounts

- Crear una nueva cuenta
- Ingresar el nombre, número de extensión, password, ID y la dirección IP de la central telefónica.

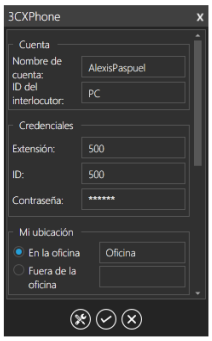


Figura 4.21 Configuración de 3CXPhone

4.1.1.10. Pruebas de funcionamiento realizadas

Se realizó una llamada al usuario que tiene asignado la extensión 103. (Figura 4.22).

Figura 4.22 Prueba de Comunicación

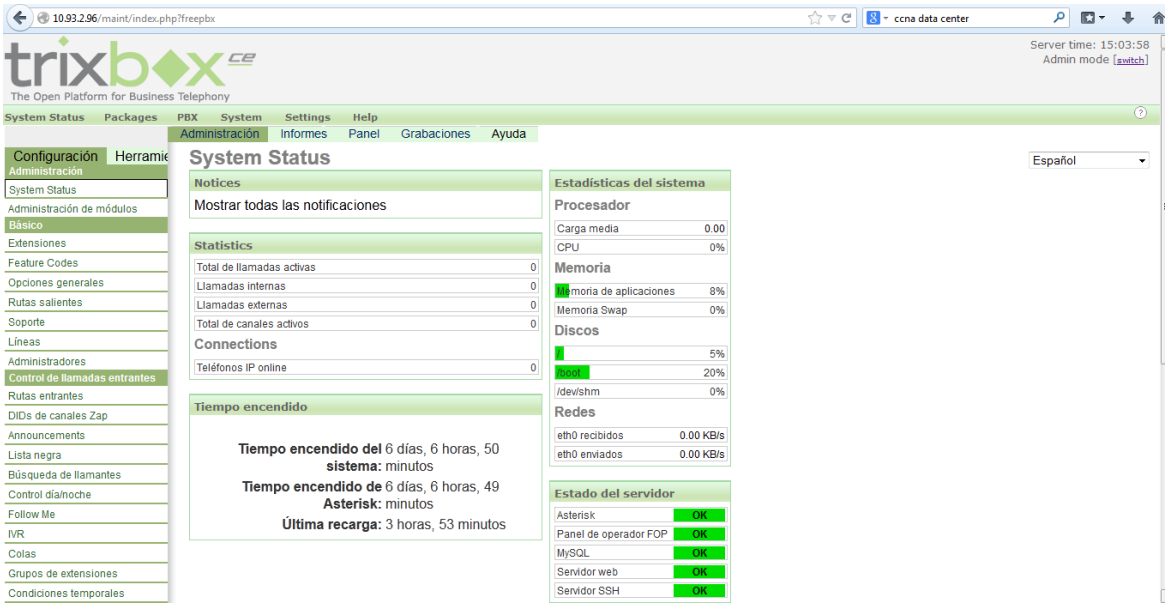


Figura 4.23 Prueba de Estado del Sistema (Continuación)

4.1.1.10.1. Crear y configurar la máquina virtual correo Zimbra

Zimbra es una plataforma que trabaja sobre Linux, permite tener funcionalidades de correo electrónico seguro a través de una interfaz web amigable con el usuario y el administrador del sistema.

Componentes de Zimbra:

LDAP: Protocolo Ligero de Acceso a Directorios. Es un sistema de directorio, que permite que los usuarios se almacenen un una base de datos y se autentiquen a través de este protocolo.

Mailbox: Servidor donde se almacenan los correos electrónicos.

MTA: Mail Tranfer Agent, es un servidor de correo electrónico que permite enviar y recibir correo.

Zimlets: Paquetes Open Source utilizados e implementados por Zimbra para sus aplicaciones.

IMAP y POP3: Protocolos de acceso a mensajes guardados en un ordenador.
RSS: Formato XML para compartir contenido en el Internet, permite recibir actualizaciones de páginas que web sin tener que acceder a ellas una por una.

CALDav: Estándar de Internet, que permite a un usuario tener acceso a información de un servidor remoto.

ZCS: Versión gratuita de Zimbra.

GAL: Lista de Direcciones Global. Es el grupo de direcciones que utiliza Zimbra para acceder al directorio de los usuarios de la empresa, almacenado en LDAP.

LMTP: Protocolo de transporte local de correo, es una variación del SMTP que se utiliza para entornos donde no se tiene un MTA.

Archivo CVS: Archivo de arquitectura plana separado por comas.

Amavis: Paquete integrador de ClamAV, Spamassassin y Postfix, utilizado por el servidor de Zimbra.

4.1.1.10.2. *Instalación de zimbra open source*

Se instalara zimbra Open Source en un solo servidor, dentro del cual estará LDAP, mailbox y MTA.

Uno de los requisitos fundamentales antes de la instalación de Zimbra es tener correctamente configurado un servidor de DNS, con el nombre del dominio que alojará, el dominio será "juanpiomontufar.edu.ec". Ver el apartado 3.13.1.3 Configuración de Servidor DNS.

4.1.1.10.3. Configuración de zimbra

Previo a la instalación se deben habilitar y deshabilitar los servicios que se necesiten con el comando ntsysv. Se deben deshabilitar: bluethooth, cups, isdn, pcmcia, sendmail, nfs, acpid, apmd, ip6tables, kudzu, nfslogk, portmap, rhnsd, rcpgssd, yum-updatesd, isdn, ldap, postfix, avahi-daemon, setroubleshoot.

En la siguiente figura de indica la deshabilitación de servicios previo a la instalación de zimbra.

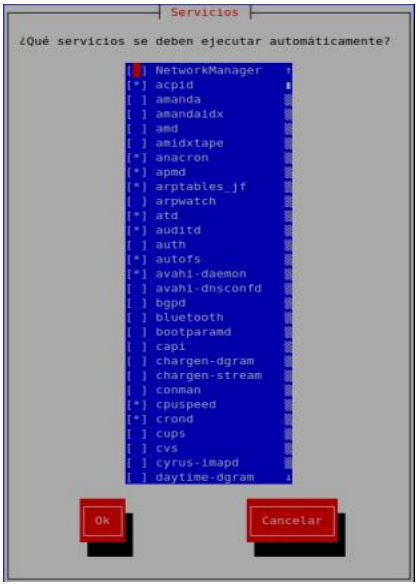


Figura 4.24 Deshabilitar paquetes previo la instalación de Zimbra

Se debe deshabilitar SELinux. Para ello se debe modificar el archivo /etc/selinux/config, en la línea SELINUX=disabled.

Se debe detener los servicios para evitar problemas en la instalación, principalmente sendmail. Para esto se digitan los comandos

Chkconfig –level 2345 sendmail off service sendmail stop

4.1.1.10.4. Intalación de zimbra only server

Se debe descargar de la página http://www.zimbra.com, la versión open source edition 7.0.0 de 32 bits. Se debe tener presente que el mismo paquete servirá para instalar los tres tipos de servidores: LDAP, Mailbox y MTA.

Se debe desempaquetar la aplicación con el comando.

#tar –xzvf zcs-7.0.0_GA_3077.RHEL5.20110127201734 (2).tgz

Se ejecuta el archivo **"./install.sh"** ubicado en el directorio de zimbra, que fue descomprimido con anterioridad. Con este archivo se abre un cuadro de dialogo

donde se debe aceptar las condiciones de licenciamiento y la instalación de los paquetes que Zimbra pueda requerir, en este caso zimbra-ldap, zimbra-logger, zimbra-mta, zimbra-snmp, zimbra-store, zimbra-apache, zimbra-spell. El componente zimbra-core se instalará por defecto en todos los servidores.

En la Figura 4.25 se indica la elección de los paquetes a instalar.

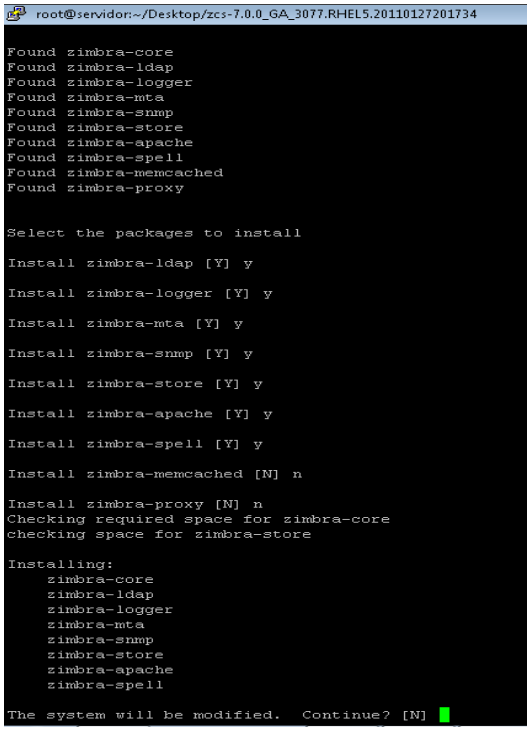


Figura 4.25 Elección de los paquetes a instalar

Aparecerá en el cuadro de dialogo una opción para cambiar el nombre de dominio con el que trabaja el servido DNS, en este caso será juanpiomontufar.edu.ec (Figura 4.26).

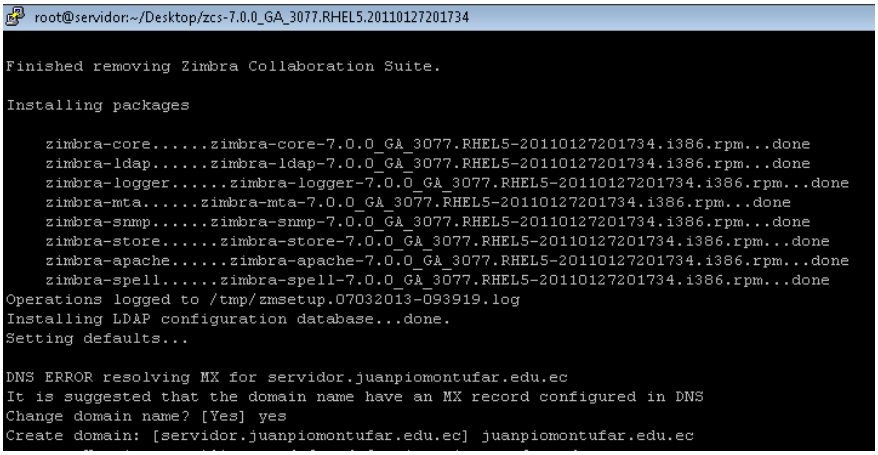


Figura 4.26 Cambio de dominio para el servidor.

Aparecerán las opciones en un menú para la configuración de los diferentes servicios.

Se configurará primero el servidor LDAP, para lo cual se coloca el número 1. Para ingresar a la configuración común, en las opciones del menú, se debe cambiar la contraseña de acceso a Ldap con la opción 4 y elegir la zona horaria en la que se va a trabajar con la opción 6. Luego de esto se coloca la opción r para regresar al menú principal.

Menú para la elección de la zona horaria. Para el caso de Ecuador es el número 11. (Figura 4.27).

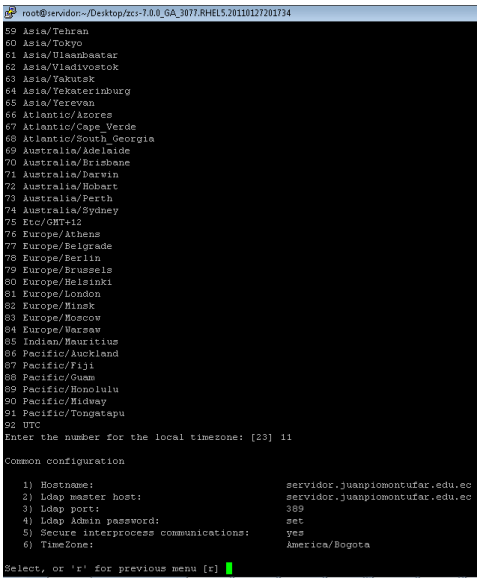


Figura 4.27 Elección de la zona horaria

Con la opción “3” se entra a la configuración de zimbra-store, con la opción 3 y 4 se debe modificar el usuario y el password del administrador. Y con la opción 12 cambiamos el web server mode a both, para tener acceso con el protocolo http y https.

3) Admin user to create: admin@juanpiomontufar.edu.ec

4) Admin Password: montufar

12) Web server mode: both

Todas las opciones marcadas con * son de carácter obligatorio.

Es importante recordar la contraseña de administrador asignada ya que es la que se utilizará para acceder al sistema posteriormente. (Figura 4.28).

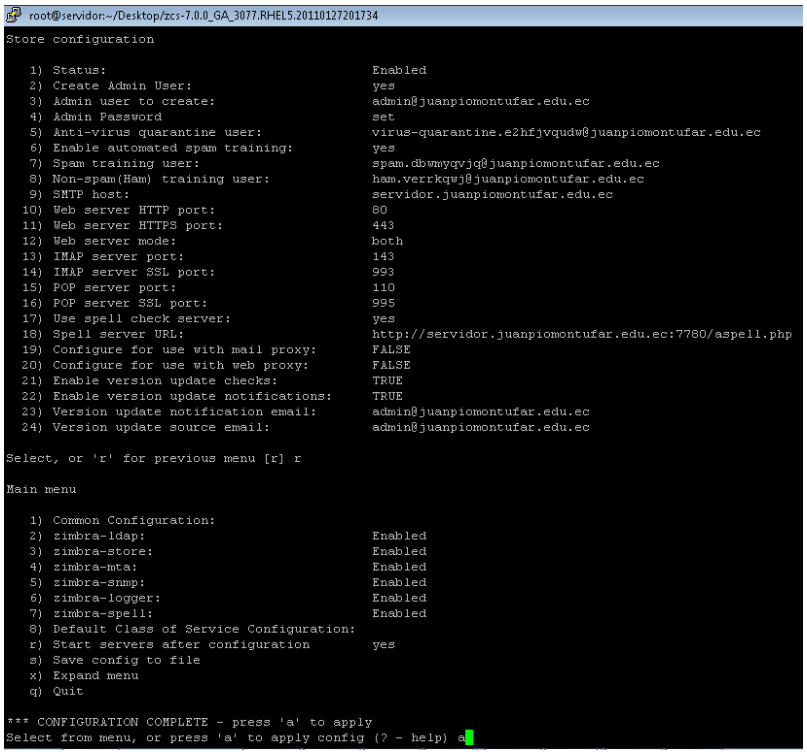


Figura 4.28 Opciones de configuración de Mailbox

Para volver al menú principal se pulsa “r” y se aplica la configuración pulsando “a”. Una vez aplicada la configuración finalizará la instalación de este servidor.

Aparecerá la opción de notificar a Zimbra de la instalación se colocará yes.

Para verificar que los servicios se encuentren corriendo de manera exitosa se ingresa como usuario zimbra y se utiliza el comando “zmcontrol status”. Para iniciar los servicios se utiliza el comando “zmcontrol start”, para reiniciarlos “zmcontrol restart” (Figura 4.29).

su –l zimbra zmcontrol status

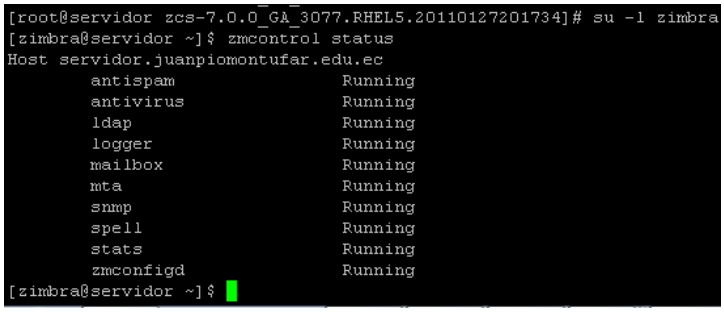


Figura 4.29 Comprobación del servidor Zimbra

Una vez montado el servidor podemos ingresar en la consola de administración vía: https://servidor.juanpiomontufar.edu.ec:7071/zimbraAdmin

En la Figura 4.30 se indica la pantalla de Administración vía Web de Zimbra.

Figura 4.30 Pantalla de administración vía Web de Zimbra

Una vez ingresado el usuario y password que configuramos en el menú del Store, se observa los servicios de zimbra corriendo. (Figura 4.31)

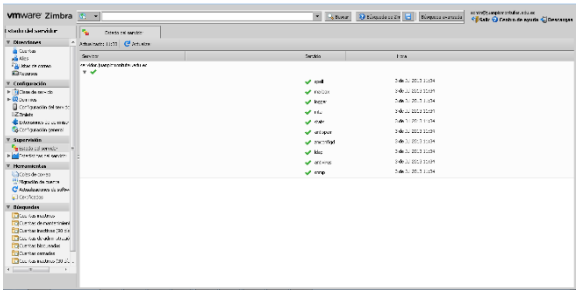


Figura 4.31 Interfaz Web de Zimbra

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Mejorar la infraestructura de comunicación en el CEJPM es urgente para poder brindar un mejor servicio a la ciudadanía a través de un sistema de comunicaciones actualizado y eficiente.
- El cableado estructurado del CEJPM debe ser parcialmente cambiado puesto que para su instalación no se han tomado en cuenta normas que garanticen el buen funcionamiento del cableado estructurado, a pesar de que se cuenta con cable UTP categoría 5e, la instalación no fue adecuada y no se realizaron pruebas de certificación, sin embargo se verificó el estado de los mismos para identificar los puntos de red que se encuentran en mal estado.
- Se obtuvo información importante acerca del tráfico telefónico a través de la encuesta realizada a los funcionarios del CEJPM, donde se determinó que son necesarias cuatro troncales telefónicas para cubrir la demanda de llamadas en el día y la hora más cargada.
- La migración hacia la telefonía IP tiene varios beneficios entre ellos económicos esto es debido a que si se requieren nuevas extensiones no es necesario realizar un nuevo cableado ni adquirir nuevos módulos para adaptar a la central telefónica en caso de un crecimiento futuro.
- Los equipos de Networking instalados en la institución son de marca D-Link y tienen las mínimas características por lo que no cumplen con lo requerido para la nueva red propuesta. Sin embargo debido al alto costo que tienen los equipos sugeridos se pueden utilizar para conectar estaciones de trabajo en algunos laboratorios hasta adquirir los nuevos equipos.
- La infraestructura de cableado estructurado contará con enlaces redundantes para el caso del cableado vertical, esto evitara que la

conexión entre los departamentos no se vea afectada de forma simultánea ya que siempre existirá un enlace en estado pasivo listo para entrar en funcionamiento.

- Con respecto a la seguridad informática el CEJPM no cuenta con un antivirus centralizado que ofrezca seguridad al sistema. Por ello se propone la adquisición de un antivirus implementado de forma centralizada para mantener a la red libre de virus, gusanos, spam entre otras. Además, disminuye el tráfico de la red debido a que las actualizaciones se las realiza en horas no laborables.
- Debido a la inseguridad informática que existe se utilizará un equipo que brinde seguridad perimetral el cual tenga incluido algunos módulos tales como: antivirus, IPS/IDS, Firewall, VPN, Web Filtering que se actualicen de forma automática para tener seguridad completa durante todo el tiempo.
- No se puede hablar del sistema de telefonía IP de manera independiente de la red de datos ya que se demostró en el prototipo de la red que ambos servicios pueden converger de manera adecuada sin degradar el rendimiento de la red.
- Se pudo determinar en base al análisis comparativo de las alternativas de soluciones de Telefonía IP que el principal parámetro de discrepancia es el costo de la solución, de mantenimiento, de actualización, lo que da una ventaja importante a la hora de escoger una alternativa, sin embargo ésta solución estaría orientada a lo que son las PYMES donde se utilice exclusivamente el servicio de telefonía IP.
- Después de comparar las características de los equipos de conectividad de las diferentes marcas que existen en el mercado, se obtuvo que cumplen con los requerimientos necesarios para formar parte de la nueva red de comunicaciones, sin embargo se escogió la opción de la marca CISCO por la compatibilidad y homogeneidad de los equipos que se van a reutilizar en la red de comunicaciones.
- La calidad de la voz durante una llamada telefónica externa depende de la capacidad del ancho de banda, de las características del terminal IP y de las características de la red donde se dará prioridad a este servicio.

- Las condiciones de operación que las empresas exigen al cliente son las recomendaciones que se han analizado durante el rediseño de la red y mientras no se cumplas éstas ningún proveedor de tecnología de telecomunicaciones garantizarán el óptimo funcionamiento de la solución presentada.
- Para la solución de Elastix deberían considerarse las mismas condiciones de operación, sin embargo al tratarse de software libre se lo puede implementar sin considerar las condiciones de operación y no se podría tener los resultados esperados.
- La nueva red contará con los servicios básicos tales como: correo, DNS, DHCP, firewall, proxy, servidor de archivos entre otros y además, brindará una plataforma adecuada para una futura implantación de servicios tales como educación virtual, repositorio digital para que los estudiantes puedan acceder a información relacionada con las materias recibidas, sistema de matriculación en línea entre otras.

5.2. RECOMENDACIONES

- Se recomienda exigir al proveedor del servicio de Internet que se tiene contratado un plan corporativo de 2 Mbps y se debe cumplir con el requerimiento puesto que durante las pruebas realizadas para la medición de la velocidad se obtuvieron valores inferiores a 1Mbps de tráfico consumido durante horas laborables y no laborables.
- Se recomienda que todos los puertos de red que no están siendo utilizados sean bloqueados y si un usuario requiere utilizar dicho puerto debe presentar un documento firmado por la rectora de la institución indicando el motivo por el cual requiere conectarse a dicho puerto.
- Se determinó que se requieren cuatro troncales analógicas para cubrir la demanda de tráfico telefónico en el CEJPM y se recomienda cancelar las líneas restantes que no se encuentren utilizando.
- Para este proyecto se recomienda adquirir una central telefónica IP basada en Asterisk como por ejemplo Elastix o Trixbox CE porque no necesitan licencia además, son fáciles de configurar y prestan los mismos o mejores servicios que una central propietaria.
- Se recomienda agilitar la gestión para la adquisición de un equipo de seguridad para protección de la red interna puesto que no existe un control de acceso en la navegación y como se observó se utilizan programas de descarga masiva que degradan la red y además proveerá de puertos adicionales para definir la DMZ.
- Se recomienda que se tenga la documentación de la red de comunicaciones actualizada para identificar de manera rápida posibles errores de conectividad o cambios en las estaciones de trabajo de un área a otra.
- Se recomienda tomar en cuenta las características de los equipos activos en caso de renovar los que actualmente se utilizan, ya que para poder implementar la segmentación propuesta en el rediseño de la red, y tener VLANs de voz y datos es necesaria la adquisición de equipos nuevos.

- Se recomienda que se instale el sistema de puesta a tierra para la infraestructura de telecomunicaciones y garantizar el buen funcionamiento de los equipos de conectividad.
- Se recomienda llevar un registro con hora, fecha y el motivo de ingreso al personal que accede al cuarto de equipos, esto es necesario para saber las modificaciones que se realizan en la red.
- Se recomienda realizar un mantenimiento mensual tanto de hardware como de software de los siguientes equipos: servidores, estaciones de trabajo, teléfonos IP, cámaras IP y equipos de Networking, dicho mantenimiento estará a cargo del personal de sistemas. Esto es necesario para aumentar el tiempo de vida útil de los dispositivos y así recuperar la inversión que tiene este proyecto.

REFERENCIAS BIBLIOGRÁFICAS

PROYECTOS DE TITULACIÓN

[12] D. Pozo, Estudio y diseño de una red de voz y datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, Video seguridad y Videoconferencia, Escuela Politécnica Nacional, p. 79.

[16] M. Herrera , Ingeniería de detalle para el diseño de una Intranet con conexión a Internet para aplicaciones de voz, Datos y Video utilizando la arquitectura TCP/IP,, Quito: Escuela Politecnica Nacional, 2004, p. 79.

[20] A. Muñoz y W. Leiva, Ingeniería de detalle para el diseño de la red para voz y datos, acceso remoto e intranet para la empresa Acurio & Asociados, Quito: Escuela Politecnica Nacional, 2011, p. 160.

[32] D. Aveiga y L. Cadena , Diseno de la red de telefonia IP y su integración con la red de datos para la comunicación de la matriz con las sucursales de importadora Vega S.A., Quito, 2010.

[33] M. Caiza y P. Cruz, Diseno de una red convergente para brindar una soluci6n de voz y datos de laboratorios life a nivel nacional, Quito, 2011.

[34] J. Bazurto y D. Mena, Rediseno de la red del lnstituto Tecnológico Superior Central Tecnico, Quito, 2011.

[35] R. Alvear y D. Méndez, Análisis de tráfico y diseño de una solución telefónica IP para la empresa Pinturas Cóndor S.A., Quito, 2009.

FOLLETOS

[14] R. Freeman, Ingeniería de sistemas de telecomunicaciones, Mexico: John Wiley & Sons, 2012.

[19] S. Sinche, Folleto Sobre Cableado Estructurado., Quito, 2008.

[26] H. Aulestia, Telefonía, Quito, 2010.

[27] CIERTE, Curso De Telefonía IP, Quito, 2011.

[28] F. Flores, Cableado Estructurado, Quito, 2008.

[29] P. Hidalgo, Redes de Área Extendida (WAN), Quito, 2009.

[30] J. Ibujés, Curso De Voip, Quito, 2007.

[31] M. Vinueza, Redes de Área Local (LAN), Quito, 2008.

INTERNET

[1] J. Cuesta, «Lineamientos para proyectos de cableado,» Universidad Nacional de Colombia, 2009. [En línea]. Available: http://www.dnic.unal.edu.co/docts/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf.

[2] Ingeniatic, «Cable de par trenzado,» 2014. [En línea]. Available: http://ingeniatic.euitt.upm.es/index.php/multimedia/videos/item/745-cable-de-par-trenzado.

[3] Ecured, «Fibra optica,» 2014. [En línea]. Available: http://www.ecured.cu/index.php/Fibra_%C3%B3ptica.

[4] C. Chavez y M. Gomez, «Cableado horizontal y vertical,» 2009. [En línea]. Available: http://es.slideshare.net/krosuarezjc/cableado-horizontal-y-vertical.

[5] Mindomo, «Redes Mind Map,» 2010. [En línea]. Available: https://www.mindomo.com/mindmap/redes-527de9aeb03d4204889f51cdc3b6815e.

[6] Universidad Nacional de Quilmes, «Comunicacion de datos,» 2009. [En línea]. Available: http://iaci.unq.edu.ar/materias/comunicacion/archivos/apuntes/Apunte%20Redes.pdf.

[7] E. Gutierrez, «Spaning Tree,» UNEFA, [En línea]. Available: http://sistemamid.com/preview.php?a=3841.

[8] D. Nosferatus, «Estandares de protocolo 802.11,» 2010. [En línea]. Available: http://es.slideshare.net/DAVIDNOSFERATUS/estandares-protocolo-80211.

[9] ICTEA, «Que es el Wifi,» 2006. [En línea]. Available:

http://www.ictea.com/cs/knowledgebase.php?action=displayarticle&id=274.

[10] K. Avalos, «Beneficios de la intranet,» 2007. [En línea]. Available: https://sites.google.com/site/portafoliokevinavalos/unidad-tres/a-redes-informaticas/tipos-de-redes/por-grado-de-difucion/intranet.

[11] V. Sanchez, «Servicio de vecnologia de Voz IP - VoIP,» 2013. [En línea]. Available: http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CEoQFjAI&url=http%3A%2F%2Fvicentesanchezsri.files.wordpress.com%2F2013%2F03%2Fservicio-de-tecnologc3ada-de-voz-ip-voip.pptx&ei=xQfIU9bXL-S-sQSZ6YHQDg&usg=AFQjCNGxT6oPXW56Da645Nu1ZarTFD.

[13] OZVOIP, «VoIP,» 2014. [En línea]. Available: http://www.ozvoip.com/codecs.php.

[15] Microsoft, «Volumen de correo electronico,» 2010. [En línea]. Available: http://technet.microsoft.com/es-es/library/cc745931.aspx.

[17] Maxglaser, «Tamano de las paginas web,» 2003. [En línea]. Available: http://www.maxglaser.net/el-tamano-de-las-paginas-web-se-ha-triplicado-desde-el-2003/.

[18] Movistar, «Soporte de Internet,» 2014. [En línea]. Available: http://www.movistar.com.ve/particulares/Internet/soporte_preguntas_frecuentes.asp.

[21] Linux, «Configuracion de equipos,» 2009. [En línea]. Available: http://www.configurarequipos.com/doc835.html.

[22] Elatrix, «Servidores de comunicacion,» 2011. [En línea]. Available: http://elastix.org/images/documentation/elx-a-flyer_esp.pdf.

[23] Dimgium, «Switch vox,» 2013. [En línea]. Available: http://www.digium.com/switchvox.

[24] Ipswitch, «Whats upp,» 2011. [En línea]. Available:

http://www.ipswitch.com/international/spanish/whatsupgold.asp.

[25] 3CX, «3CX,» 2014. [En línea]. Available: http://www.3cx.es.

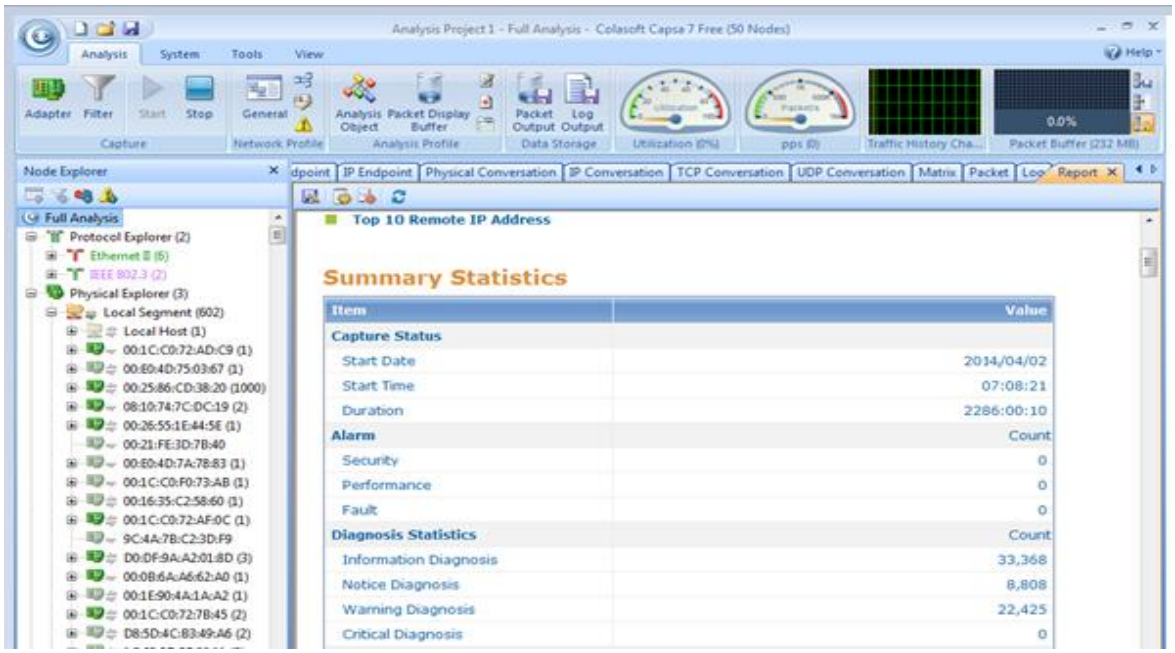
ANEXOS

ANEXO A

Se ha monitorizado y analizado todo el tráfico que circula por una red local capturando sus paquetes TCP/IP en tiempo real.

Para conocer protocolos, tramas y estimar el tráfico que transmiten y reciben los hosts del Colegio Experimental “Juan Pío Montufar” se utilizó el programa Colasoft Capsa 7 Free. Este programa es un poderoso sniffer que monitoriza y analiza todo el tráfico que circula por una red local capturando sus paquetes TCP/IP en tiempo real, a continuación se muestran las imágenes del resultado del análisis con el snnifer:

En la siguiente figura se muestra un resumen del status de la captura, fecha y hora de inicio de la captura, duración de la captura. Alarmas, estadísticas de diagnóstico:



A continuación en resumen del tráfico total, broadcast, multicast. Distribución por tamaño de paquete:

Traffic	Bytes	Packets	Utility	bps	pps
Total	309.118 MB	1,742,722	0.002%	2.304 Kbps	3
Broadcast	76.035 MB	817,423	0.002%	2.304 Kbps	3
Multicast	61.423 MB	359,995	0.000%	0 bps	0
Average Packet Size					185.993 Bytes
Packet Size Distribution	Bytes	Packets	Utility	bps	pps
<=64	35.550 MB	603,276	0.000%	0 bps	0
65-127	67.937 MB	791,373	0.002%	2.304 Kbps	3
128-255	24.350 MB	132,192	0.000%	0 bps	0
256-511	26.053 MB	70,559	0.000%	0 bps	0
512-1023	37.244 MB	63,477	0.000%	0 bps	0
1024-1517	100.096 MB	75,703	0.000%	0 bps	0
>=1518	17.889 MB	6,142	0.000%	0 bps	0

A continuación el número de direcciones físicas e IP. El total de protocolos. El tipo de conversación TCP y UDP:

Address	Count
Physical Address Count	824
IP Address Count	11,748
Local IP Address Count	294
Remote IP Address Count	11,454
Protocol	Count
Total Protocols	82
Datalink Protocols	9
Network Protocols	12
Transport Protocols	3
Session Protocols	3
Presentation Protocols	9
Application Protocols	46
Conversation	Count
Physical Conversation	2,109
IP Conversation	12,631
TCP Conversation	23,177
UDP Conversation	79,247

A continuación en resumen de la cantidad de establecimiento de la conexión. Análisis de DNS, Email, FTP, HTTP

TCP	Count
TCP SYN Sent	23,506
TCP SYNACK Sent	23,387
TCP FIN Sent	51,926
TCP Reset Sent	13,607
DNS Analysis	Count
DNS Query	37,506
DNS Response	35,168
Email Analysis	Count
SMTP Connection	0
POP3 Connection	2
FTP Analysis	Count
FTP Upload	0
FTP Download	0
HTTP Analysis	Count
HTTP Request	18,341
HTTP Requested	0
HTTP Connection	36,406

A continuación los protocolos de las capas Aplicación, Trasporte, Red y Enlace:

Diagnosis Statistics

Name	Counts
All Diagnosis	62,764
Application Layer	7,408
DNS Server Slow Response	274
DNS Host or Domain Does Not Exist	389
DNS Server Error	7
HTTP Client Error	707
HTTP Suspicious Conversation	410
HTTP Request Page Not Found	1
HTTP Server Slow Response	5,620
Transport Layer	42,209
TCP Connection Refused	2
TCP Connection Retry	527
TCP Retransmission	1,748
TCP Slow Response	28,968
TCP Duplicated Acknowledgement	10,964
Network Layer	2,716
Illegal IP Checksum	3
IP Address Conflict	2,684
ICMP Host Unreachable	12
ICMP Port Unreachable	17
Data Link Layer	10,431
ARP Request Storm	365
ARP Scan	10,065
ARP Too Many Active Response	1

A continuación el nombre y porcentaje de estadísticas de los protocolos más usados dentro de la red:

Protocols Statistics

Name	Percentage		Bytes	Packets
Ethernet II		99.500	307.573 MB	1,723,181
IP		81.776	252.786 MB	1,209,157
UDP		30.473	94.198 MB	721,999
NetBIOS		15.404	47.616 MB	485,561
Name Service		13.895	42.952 MB	465,420
Datagram Service		1.509	4.665 MB	20,141
SSDP		5.095	15.749 MB	45,536
Other		2.746	8.487 MB	94,415
DNS		4.212	13.020 MB	72,668
Response		3.207	9.915 MB	34,772
Query		0.985	3.043 MB	37,502
Error		0.020	62.907 KB	394
BOOTP		2.970	9.182 MB	21,733
DHCP		2.970	9.182 MB	21,733
RTP		0.034	108.087 KB	1,575

A continuación el top 10 protocolos de aplicaciones

Top 10 Application Protocols

Name	Percentage		Bytes	Packets
HTTP		46.481	143.681 MB	391,726
NetBIOS		15.491	47.886 MB	487,478
SSDP		11.385	35.192 MB	104,163
UDP - Other		7.197	22.246 MB	208,370
DNS		4.329	13.382 MB	74,123
HTTPS		4.274	13.210 MB	70,975
BOOTP		2.970	9.182 MB	21,733
NBIPX		0.229	724.189 KB	5,812
RIPX		0.113	356.242 KB	5,695
SAP		0.084	266.188 KB	4,259

A continuación el top 10 direcciones físicas, indicando el porcentaje de entrada y de salida:

Top 10 Physical Address

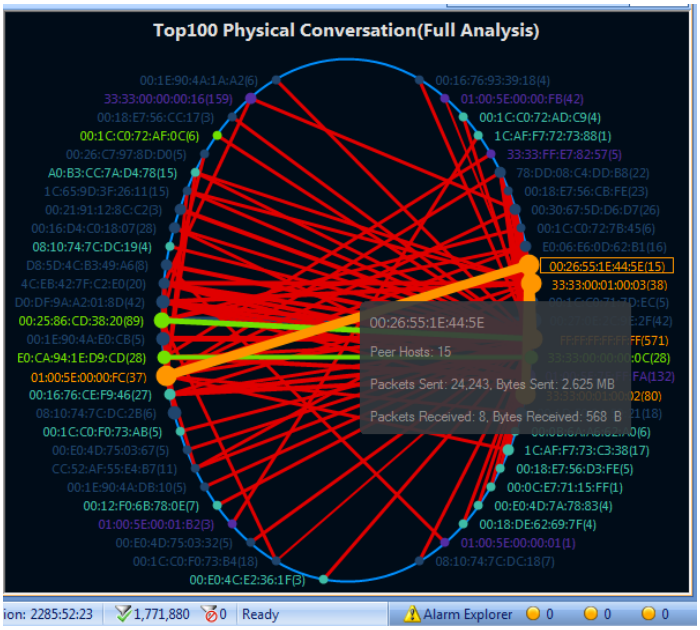
Name	Percentage Inbound	Percentage Outbound	Bytes	Packets
00:25:86:CD:38:20	26.830	73.170	187.929 MB	797,293
00:27:0E:2C:9E:2F	67.468	32.532	162.506 MB	568,781
FF:FF:FF:FF:FF:FF	100.000	0.000	76.035 MB	817,423
00:1E:90:4A:E0:CB	0.007	99.993	22.647 MB	247,115
33:33:00:00:00:0C	100.000	0.000	21.632 MB	61,130
D0:DF:9A:A2:01:8D	0.040	99.960	20.867 MB	133,379
01:00:5E:7F:FF:FA	100.000	0.000	17.631 MB	49,801
E0:CA:94:1E:D9:CD	0.060	99.940	13.048 MB	54,513
08:10:74:7C:DC:2B	97.199	2.801	10.256 MB	9,352
4C:EB:42:7F:C2:E0	0.614	99.386	9.162 MB	78,969

A continuación el top 10 direcciones IP, indicando el porcentaje de entrada y de salida:

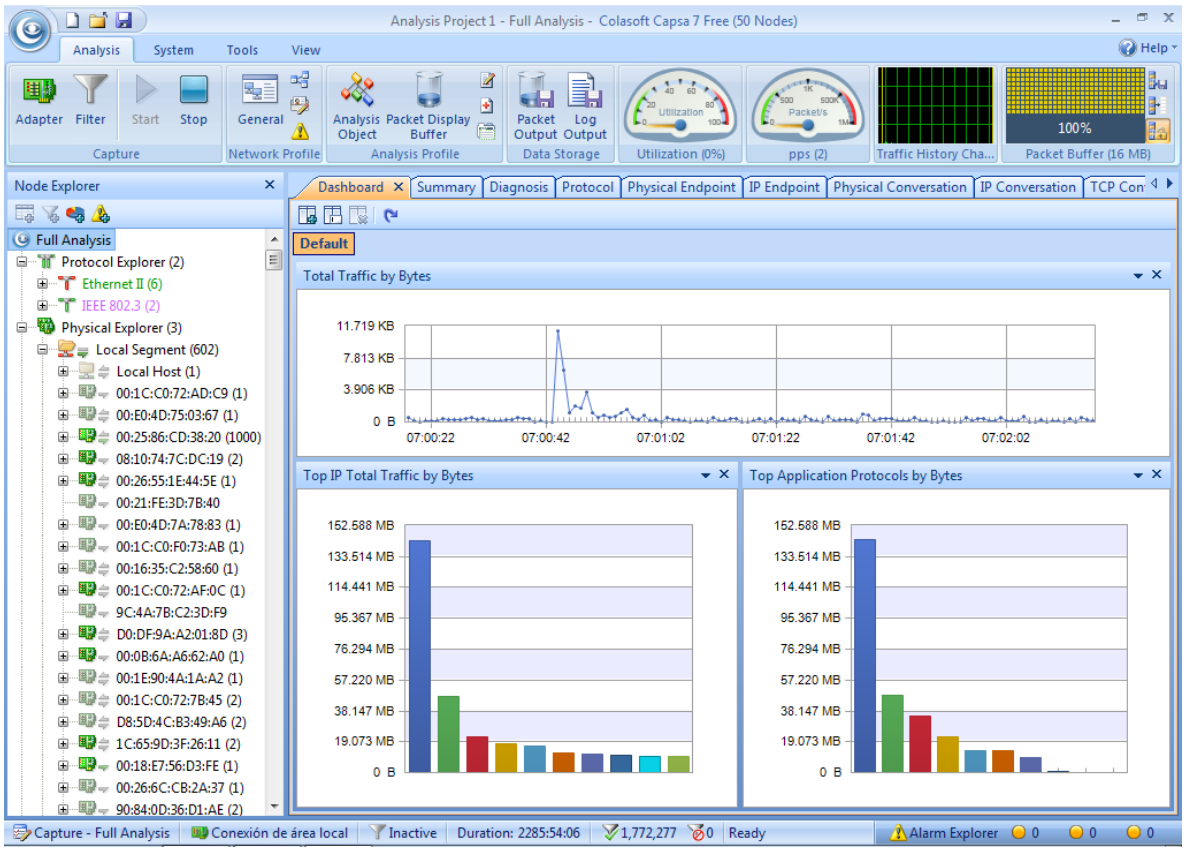
Top 10 IP Address

Name	Percentage Inbound	Percentage Outbound	Bytes	Packets
10.8.200.180	76.008	23.992	143.324 MB	531,170
10.8.200.255	100.000	0.000	46.813 MB	478,090
10.8.200.27	0.013	99.987	22.394 MB	244,113
239.255.255.250	100.000	0.000	17.631 MB	49,801
65.55.17.78	10.275	89.725	16.439 MB	26,163
65.55.17.75	10.288	89.712	12.321 MB	19,672
200.107.60.58	21.175	78.825	11.263 MB	58,883
10.8.200.18	0.001	99.999	10.642 MB	77,368
10.8.200.221	98.467	1.533	10.125 MB	8,249
31.12.64.27	0.000	100.000	9.965 MB	7,167

A continuación el top 10 de conversaciones por dirección física, indicando la cantidad de paquetes enviados y recibidos:



A continuación el top 10 del tráfico total IP y protocolos de aplicación por bytes, de manera gráfica:



ANEXO B

Para conocer el Status, Name, Dirección IP, Netbios Name, Netbios Group, MAC address, User y Comments de las computadoras conectadas a la red del Colegio Experimental Juan Pío Montufar se utilizó el programa IPScanner.

Status	Name	IP	NetBIOS name	NetBIOS group	MAC address	User	Comments
Dead	RECTORADO-PC	10.8.200.14			00:1C:C0:F0:73:B4		
Dead	10.8.200.185	10.8.200.185			84:C9:B2:7B:58:73		
Dead	10.8.200.213	10.8.200.213			14:36:05:8C:9B:1F		
Dead	10.8.200.214	10.8.200.214			00:23:76:0D:AB:AB		
Dead	10.8.200.217	10.8.200.217			30:17:C8:3F:AC:22		
Dead	PERSONAL-0E3DFD	10.8.200.218			00:21:97:83:C6:4D		
Dead	Teacher-PC	10.8.200.225			00:18:E7:56:CB:FE		
Alive	MONTUFARSEC-PC	10.8.200.28	MONTUFARSEC-PC	WORKGROUP	00:1C:C0:72:7B:33	MONTUFAR SEC	
	Shared folder:						
	ADMIN$						
	C$						
	D$						
	E$						
	F$						
	G$						
	IPC$						
	Users						
	Radmin ports:						
	80						
Alive	SECRETARIA2	10.8.200.85			08:10:74:7C:DC:19	SECRETARIA2$	
	Shared folder:						
	IPC$						
	D$						
	print$						
	C						
	Mis documentos						
	DATOS SERVIDOR						

	ADMIN$						
	C$						
	EpsonLX300						
Alive	M-E29538FC390C4	10.8.200.51			00:E0:4D:75:03:30	M-E29538FC390C4$	
	Shared folder:						
	IPC$						
	print$						
	SamsungM						
	ADMIN$						
	C$						
Alive	SECRET2	10.8.200.27			08:10:74:7C:DC:18		
Alive	PERSONAL-2DE009	10.8.200.79	PERSONAL-2DE009	INICIOMS	00:1C:C0:72:AD:C9	PERSONAL-2DE009$	
	Shared folder:						
	Impresora						
	IPC$						
	D$						
	print$						
	EpsonFX-1180						
	FX-1180						
	Documentos c						
	ADMIN$						
	C$						
	Impresora2						
	Impresora3						
Alive	SVICER	10.8.200.26			00:0B:6A:A6:62:A0	SVICER$	
	Shared folder:						
	IPC$						
	print$						
	EpsonLX-810						
	DATOS SERVIDOR						
	ADMIN$						
	C$						
Alive	PC40	10.8.200.131	PC40	MH	00:E0:4C:E2:35:2F	PC40$	
	Shared folder:						
	E$						
	IPC$						
	ADMIN$						
	C$						

Alive	PC41	10.8.200.130			00:14:2A:61:53:2B	PC41$	
	Shared folder:						
	IPC$						
	D$						
	ADMIN$						
	IMG						
	C$						
Alive	LICTINAJERO	10.8.200.201	LICTINAJERO	REM 1	00:1C:C0:F0:67:59		
Alive	SERLAB2	10.8.200.233	SERLAB2	REM 1	00:30:67:5D:D6:D7		
Alive	COLOSSUS	10.8.200.226			00:30:67:A3:D7:B7		
Alive	COLEGIO-FE9F887	10.8.200.241			00:11:11:4A:25:B8		
Alive	10.8.200.55	10.8.200.55			00:1E:90:4A:DB:10		
Alive	M-160D9C7A6C1A4	10.8.200.250			00:E0:4D:75:03:67		
Alive	M-7874095577EF4	10.8.200.253			00:E0:4D:7A:78:83		
Alive	M-D1CD5AC670284	10.8.200.254			00:E0:4D:75:03:32		
Alive	10.8.200.4	10.8.200.4			00:17:61:10:13:2F		
	Http:						
	(no title)						
	Radmin ports:						
							23
							80
Alive	10.8.200.43	10.8.200.43			1C:AF:F7:72:73:88		
	Http:						
	DWL-2100AP						
	Radmin ports:						
							23
							80
Alive	10.8.200.211	10.8.200.211			00:18:E7:56:CB:FD		

Alive	10.8.200.47	10.8.200.47			1C:AF:F7:69:61:6B		
	Http:						
	DWL-2100AP						
	Https:						
	(no title)						
	Radmin ports:						
	23						
	80						
Alive	10.8.200.5	10.8.200.5			00:21:91:12:8B:A1		
	Radmin ports:						
	80						
Alive	10.8.200.21	10.8.200.21			00:21:91:12:8C:6E		
	Radmin ports:						
	80						
Alive	10.8.200.240	10.8.200.240			00:BE:13:0C:E3:95		
Alive	INSPGEN	10.8.200.80	INSPGEN	REM 1	00:1E:90:4A:1A:A2		
Alive	SERV-JPM	10.8.200.10	SERV-JPM	REM1	00:26:55:1E:44:5E		
	Http:						
	IIS7						
	Radmin ports:						
	80						
Alive	FRANCISCOENCAL	10.8.200.227			00:1C:C0:72:BB:0B	FRANCISCOENCAL$	
	Shared folder:						
	Samsung ML-1740 Series						
	IPC$						
	D$						
	print$						
	EpsonFX-1180						
	Documentos c						
	ADMIN$						
	C$						
	Impresora3						
	Radmin ports:						
	21						
Alive	Marlon-PC	10.8.200.93			00:16:76:CE:F9:46		

Alive	COLECTURIA2	10.8.200.72	COLECTURIA 2	WORKGR OUP	00:1C:C0:71:7D:EC	COLECT URIA2$	
	Shared folder:						
	IPC$						
	D$						
	print$						
	ADMIN$						
	C$						
	EpsonLQ						
	SAMSUNG ML-1740 SERIES						
Alive	SECREC	10.8.200.19			00:1C:C0:72:7B:45	SECREC $	
	Shared folder:						
	IPC$						
	D$						
	print$						
	ADMIN$						
	C$						
	EpsonFX						
Alive	PC4495-024	10.8.200.126	PC4495-024	REM	00:1E:90:4A:E0:F5	PC4495-024$	
	Shared folder:						
	E$						
	IPC$						
	print$						
	SamsungM						
	ADMIN$						
	C$						
	Samsung scx-4300 series						
Alive	COLECTURIA	10.8.200.228			00:1C:C0:72:AF:0C	COLECT URIA$	
	Shared folder:						
	IPC$						
	D$						
	print$						
	Documentos c						
	ADMIN$						
	C$						
	SamsungS						
	Impresora2						
Alive	LICPATRICIO	10.8.200.202			00:16:76:A4:2E:25	LICPATR ICIO$	
	Shared folder:						
	Impresora						

	IPC$						
	print$						
	Documentos c						
	ADMIN$						
	H$						
	C$						
	SamsungS						
Alive	10.8.200.3	10.8.200.3			00:25:86:CD:38:20		
	Radmin ports:						
	80						
Alive	PC4495-017	10.8.200.50			00:18:E7:56:CC:17		
Alive	10.8.200.75	10.8.200.75			00:1C:C0:F0:73:AB		
Alive	10.8.200.31	10.8.200.31			00:1E:90:4A:1A:BB		
Alive	10.8.200.199	10.8.200.199			00:1E:90:4A:1A:A2		
Alive	VICERRECTOR-PC	10.8.200.25			00:1C:C0:74:DC:C7		
Alive	10.8.200.212	10.8.200.212			94:00:70:62:25:BD		
Alive	10.8.200.210	10.8.200.210			00:16:76:A4:2C:C0		
Alive	10.8.200.230	10.8.200.230			9C:4A:7B:6E:8C:02		
Alive	10.8.200.249	10.8.200.249			28:D1:AF:16:A7:34		
Alive	PANKUADOR-PC	10.8.200.235			00:1D:E0:9A:59:21		

ANEXO C

A continuación se presentan los puntos de red con su respectiva nomenclatura de acuerdo al área y departamento donde se encuentran ubicados:

Departamento	Puerto de datos	Puerto de Voz	Puerto de Video
Biblioteca	BI-01A-01-PD01	BI-02-01-PV01	CAM1-02-ABI
	BI-01A-02-PD02	-	-
	BI-01A-03-PD03	-	-
	BI-01A-04-PD04	-	-
	BI-01A-05-PD05	-	-
	BI-01A-06-PD06	-	-
	BI-01A-07-PD07	-	-
	BI-01A-08-PD08	-	-
	BI-01A-09-PD09	-	-
Colecturía	CO-01A-10-PD10	CO-02-02-PV02	CAM2-02-ACO
	CO-01A-11-PD11	CO-02-03-PV03	-
	CO-01A-12-PD12	CO-02-04-PV04	-
	CO-01A-13-PD13	-	-
Guarda-Almacén	GA-01A-14-PD14	GA-02-05-PV05	-
Bodegas	BO-01A-15-PD15	BO-02-06-PV06	-
Secretaria General	SG-01A-16-PD16	SG-02-07-PV07	-
	SG-01A-17-PD17	SG-02-08-PV08	-
	SG-01A-18-PD18	-	-
Salón de Actos	SA-01A-19-PD19	SA-02-09-PV09	-
Rectorado	RE-01A-20-PD20	RE-02-10-PV10	-
		RE-02-11-PV11	-
Secretarias	SE-01A-21-PD21	SE-02-12-PV12	-
	SE-01A-22-PD22	SE-02-13-PV13	-
	SE-01A-23-PD23	-	-
Sistemas	SI-01A-24-PD24	SI-02-14-PV14	CAM3-02-ASI
Vicerrectorado	VI-01B-25-PD25	VI-02-15-PV15	-
	VI-01B-26-PD26	VI-02-16-PV16	-
Secretaria de Vicerrectorado	SV-01B-27-PD27	SV-02-17-PV17	-
DOBE	DB-01B-28-PD28	DB-02-18-PV18	-
	DB-01B-29-PD29	DB-02-19-PV19	-
	DB-01B-30-PD30	DB-02-20-PV20	-

Corredor Bloque	DB-01B-31-PD31	DB-02-21-PV21	-
	-	-	CAM4-02-ACB

Nomenclatura de los Puntos de Datos, Voz y Video del Área Administrativa

Para el área Departamental se muestra en la siguiente tabla:

Departamento	Puerto de datos	Puerto de Voz	Puerto de Video
Sub-Inspección	SI-01A-01-PD01	SI-02-01-PV01	-
Departamento Médico	DM-01A-02-PD02	DM-02-02-PV02	CAM5-02-DDM
	DM-01A-03-PD03	DM-02-03-PV03	-
Sala de Música	SM-01A-04-PD04	SM-02-04-PV04	-
Departamento de Cultura Física	DCF-01A-05-PD05	DCF-02-05-PV05	-
Sala de Lectura de Profesores	SP-01A-06-PD06	SP-02-06-PV06	-
	SP-01A-07-PD07	SP-02-07-PV-07	-
Inspección General	IG-01A-08-PD08	IG-02-08-PV-08	-
Departamento de Mejoramiento de la Calidad de la Educación	DME-01A-09-PD09	DME-02-09-PV-09	-
Corredor Bloque	-	-	CAM6-02-DDME

Nomenclatura de los Puntos de Datos, Voz y Video del Área Departamental

Para el Área Laboratorios se muestra en la siguiente tabla:

Departamento	Puerto de datos	Puerto de Voz	Puerto de Video
Laboratorio de Biología	LB-01A-01-PD01	LB-02-01-PV01	-
	LB-01A-02-PD02	LB-02-02-PV02	CAM7-02-LLB
	LB-01A-03-PD03	LB-02-03-PV03	-
Laboratorio de Química	LQ-01A-04-PD04	LQ-02-04-PV04	CAM8-02-LLQ
	LQ-01A-05-PD05	LQ-02-05-PV05	-
Laboratorio de Ciencias Naturales	LC-01A-06-PD06	LC-02-06-PV06	CAM9-02-LLC
	LC-01A-07-PD07	LC-02-07-PV-07	-
Laboratorio de Física	LF-01A-08-PD08	LF-02-08-PV-08	CAM10-02-LLF
	LF-01A-09-PD09	LF-02-09-PV-09	-
	LF-01A-10-PD10	LF-02-10-PV-10	

Nomenclatura de los Puntos de Datos, Voz y Video del Área Laboratorios

Para el Área Bloque Primeros y Segundos Cursos se muestra en la siguiente tabla:

	Patch Pannel A de 48 p	Patch Pannel B de 48 p
Lab. De Computación Primeros y segundos Cursos	BPS-LCPSA-PD01	BPS-LCPSCB-PD25
	BPS-LCPSA-PD02	BPS-LCPSCB-PD26
	BPS-LCPSA-PD03	BPS-LCPSCB-PD27
	BPS-LCPSA-PD04	BPS-LCPSCB-PD28
	BPS-LCPSA-PD05	BPS-LCPSCB-PD29
	BPS-LCPSA-PD06	BPS-LCPSCB-PD30
	BPS-LCPSA-PD07	BPS-LCPSCB-PD31
	BPS-LCPSA-PD08	BPS-LCPSCB-PD32
	BPS-LCPSA-PD09	BPS-LCPSCB-PD33
	BPS-LCPSA-PD10	BPS-LCPSCB-PD34
	BPS-LCPSA-PD11	BPS-LCPSCB-PD35
	BPS-LCPSA-PD12	BPS-LCPSCB-PD36
	BPS-LCPSA-PD13	BPS-LCPSCB-PD37
	BPS-LCPSA-PD14	BPS-LCPSCB-PD38
	BPS-LCPSA-PD15	BPS-LCPSCB-PD39
	BPS-LCPSA-PD16	BPS-LCPSCB-PV40
	BPS-LCPSA-PD17	CAM11-LCPSCB-41
	BPS-LCPSA-PD18	P42 No asignado
	BPS-LCPSA-PD19	P43 No asignado
	BPS-LCPSA-PD20	P44 No asignado
	BPS-LCPSA-PD21	P45 No asignado
	BPS-LCPSA-PD22	P46 No asignado
	BPS-LCPSA-PD23	P47 No asignado
	BPS-LCPSA-PD24	P48 No asignado

Nomenclatura de los Puntos de Datos, Voz y Video del Laboratorio de Computación Primeros y Segundos Cursos.

Para el Área Bloque Terceros y Cuartos Cursos se muestran en las siguientes tablas:

	Patch Pannel A de 48 p	Patch Pannel B de 48 p
Lab. De Idiomas	BTC-LIA-PD01	BTC-LIB-PD25
	BTC-LIA-PD02	BTC-LIB-PD26
	BTC-LIA-PD03	BTC-LIB-PD27
	BTC-LIA-PD04	BTC-LIB-PD28
	BTC-LIA-PD05	BTC-LIB-PD29
	BTC-LIA-PD06	BTC-LIB-PD30
	BTC-LIA-PD07	BTC-LIB-PD31
	BTC-LIA-PD08	BTC-LIB-PD32
	BTC-LIA-PD09	BTC-LIB-PD33
	BTC-LIA-PD10	BTC-LIB-PD34
	BTC-LIA-PD11	BTC-LIB-PD35
	BTC-LIA-PD12	BTC-LIB-PD36
	BTC-LIA-PD13	BTC-LIB-PD37
	BTC-LIA-PD14	BTC-LIB-PD38
	BTC-LIA-PD15	BTC-LIB-PD39
	BTC-LIA-PD16	
	BTC-LIA-PD17	BTC-B1-PD40
	BTC-LIA-PD18	BTC-B2-PD41
	BTC-LIA-PD19	BTC-B3-PD42
	BTC-LIA-PD20	BTC-B4-PD43
	BTC-LIA-PD21	BTC-B5-PD44
	BTC-LIA-PD22	BTC-B6-PD45
	BTC-LIA-PD23	BTC-B7-PD46
	BTC-LIA-PD24	CAM12-LCTCB-47

Nomenclatura de los Puntos de Datos, Voz y Video del Laboratorio de Idiomas y Aulas.

Lab. De Computación Terceros y Cuartos Cursos	**Patch Pannel C de 24 p**	
	BTC-LCTCC-PD01	
	BTC-LCTCC-PD02	
	BTC-LCTCC-PD03	
	BTC-LCTCC-PD04	
	BTC-LCTCC-PD05	
	BTC-LCTCC-PD06	
	BTC-LCTCC-PD07	
	BTC-LCTCC-PD08	
	BTC-LCTCC-PD09	
	BTC-LCTCC-PD10	
	BTC-LCTCC-PD11	
	BTC-LCTCC-PD12	
	BTC-LCTCC-PD13	
	BTC-LCTCC-PD14	
	BTC-LCTCC-PD15	
	BTC-LCTCC-PD16	
	BTC-LCTCC-PD17	
	BTC-LCTCC-PD18	
	BTC-LCTCC-PD19	
	BTC-LCTCC-PD20	
	BTC-LCTCC-PD21	
	BTC-LCTCC-PD22	
	BTC-LCTCC-PV23	
	CAM13-LCTCC-24	

Nomenclatura de los Puntos de Datos, Voz y Video del Laboratorio de Computación Terceros y Cuartos Cursos

Para el Área Bloque Quintos y Sextos Cursos se muestran en las siguientes tablas:

	Patch Pannel A de 48 p	Patch Pannel B de 48 p
Lab. De Computación Quintos y Sextos Cursos	BQS-LCQSA-PD01	
	BQS-LCQSA-PD02	
	BQS-LCQSA-PD03	
	BQS-LCQSA-PD04	
	BQS-LCQSA-PD05	
	BQS-LCQSA-PD06	
	BQS-LCQSA-PD07	
	BQS-LCQSA-PD08	
	BQS-LCQSA-PD09	
	BQS-LCQSA-PD10	
	BQS-LCQSA-PD11	
	BQS-LCQSA-PD12	
	BQS-LCQSA-PD13	
	BQS-LCQSA-PV14	
	CAM14-LCQSA-15	

Nomenclatura de los Puntos de Datos, Voz y Video del Laboratorio de Computación Quintos y Sextos Cursos

ANEXO D

PLANOS ARQUITECTÓNICOS

ANEXO E

PaloSanto Solutions
OPENSOURCE INNOVATION
www.palosanto.com

MegaTelCon S.A.
TELECOMUNICACIONES Y CONECTIVIDAD

elastix
FREEDOM TO COMUNICATE

Oficina Quito
Ave. Julio Zaldumbide N25-82 y Valladolid,
1er. Piso (Sector Hotel Quito - La Floresta)
Telefax: 2901733 / 6001980 / 6001981

Oficina Guayaquil
Cdla. Nueva Kennedy, Calle E #222
Teléfonos: 228-3268 / 229-4440
Fax: 228-4356

Quito, 4 de Agosto de 2014

PROPUESTA ECONÓMICA

PaloSanto Solutions propone una solución telefónica **Elastix** totalmente basada en IP y con soporte para todos los requerimientos solicitados:

CANT.	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
	MATRIZ		
1	**Servidor Elastix ELX-25 (New)** – Servidor IPPBX puede soportar en un nivel óptimo hasta 50 llamadas concurrentes y 100 extensiones registradas. Incluye Disco estado sólido 120GB.	$1,200.00	$1,200.00
1	**Gateway Sangoma 8 FXO**	$786.00	$786.00
39	**Teléfono Básicos Elastix LXP-200**	$100.00	$3,900.00
1	**Teléfono Ejecutivos Grandstream GXP-2100**	$130.00	$130.00
1	**Teléfono Ejecutivos Grandstream GXP-2160**	$170.00	$170.00
1	**Servicios Elastix – Configuración IPPBX Elastix**. Incluye instalación Elastix 2.4, configuración de IVRs (pre-atendedor), grupos de atención (ACDs) planes de marcado, restricciones o niveles de servicio, rutas entrantes y salientes. Incluye capacitación para Personal Técnico y Usuarios Finales. Configuración de troncales.	$1,920.00	$1,920.00
	SOPORTE POST IMPLEMENTACIÓN		
1	**Plan Anual de Soporte – 12 horas de servicio post implementación** - El plan incluye: Soporte Técnico Correctivo por 1 año en esquema 8x5 (días laborables y horario de oficina). En casos de soporte fuera de estos horarios, en fines de semana o feriados el consumo de horas es doble. Soporte remoto (acceso remoto seguro SSH al server IPPBX). Tiempos de respuesta acordes a la criticidad del servicio (al menos 4 horas de SLA).	$720.00	$720.00
		SUBTOTAL	***$8,826.00***
		IVA 12 %	$1,059.12
		TOTAL US$	**$9,885.12**

PaloSanto Solutions
OPENSOURCE INNOVATION
www.palosanto.com

MegaTelCon S.A.
TELECOMUNICACIONES Y CONECTIVIDAD

elastix
FREEDOM TO COMUNICATE

Oficina Quito
Ave. Julio Zaldumbide N25-82 y Valladolid,
1er. Piso (Sector Hotel Quito - La Floresta)
Telefax: 2901733 / 6001980 / 6001981

Oficina Guayaquil
Cdla. Nueva Kennedy, Calle E #222
Teléfonos: 228-3268 / 229-4440
Fax: 228-4356

TERMINOS Y CONDICIONES

Forma de pago:	70% anticipado y 30% con la firma de las respectivas actas de entrega y recepción del proyecto.
Validez de la oferta:	30 días
Tiempo Entrega Equipos:	Máximo 10 días hábiles luego de recibir el anticipo.
Tiempo Entrega Servicio:	Máximo 5 días hábiles luego de la entrega equipos.
Garantía:	1 año, pero se puede extender a 3 años con un cargo adicional del 18%.
Observaciones:	• Esta propuesta no incluye ningún otro producto o servicio que no esté explícitamente detallado.

Será un placer servirle, quedamos a la espera de su confirmación de la oferta. Cualquier inquietud o comentario no dude en contactarme.

Muy Atentamente,

Ing. Steven Flores J.
Gerente de Negocios y Proyectos
MEGATELCON S. A. - PaloSanto Solutions
Telf.: +593 2 6001980 (1) Ext: 705
www.palosanto.com
www.elastix.org

elastix
FREEDOM TO COMUNICATE

2010 INTERNET TELEPHONY PRODUCT OF THE YEAR

¡Mucho mejor! ECUADOR

BIOMETRIK
Soluciones Tecnológicas

COTIZACIÓN

Nro.: 201311046
Fecha: 12/08/2014

Nombre: Alexis Paspuel
Compañía: Colegio Experimental Juan Pío Montúfar
Teléfono: 0984464122
Ciudad: Quito - Ecuador **Email:** alexspaspuel@hotmail.com

De acuerdo a su solicitud de cotización enviamos nuestra proforma del equipo requerido:
Instalación 1 Puerta:

Cámaras IP:

Ítem	Descripción	Cantidad	P. Unitario $	Total $
1	DS-7608NI-ST Series NVR HIKVISION **NVR 8CH P/CAMARAS IP HIKVISION. ACEPTA ONVIF HASTA 40 MB** Canales de Video: 8ch Entradas: LAN / serial Grabación: MJPEG / MPEG4 / **H.264** Backup: Vía USB Salida de Video: VGA,HDMI, BNC Conexión: 10/100/1000Mbps TCP/IP HDD: Hasta 2HDD (Hasta 3TBC/U) Incluye: Software de monitoreo remoto hasta 64ch Alimentación: 110V	1	451,00	451,00
2	**HDD-2TB-DVR** DISCO DURO **SATA 2TB (2000GB) ESPECIAL PARA DVR** 	1	165,00	165,00
3	**DS-2CD2412FI-WNS** HIKVISION **CAMARA IP INALAMBRICA CON IR DIA/NOCHE C/ICR 1,3 M-PIXEL C/AUDIO,(3GPP) WIDE DYNAMIC RANGE (WDR-D), ESCANEO PROGRESIVO** 250,56 **280,63** Dual **Stream** Res: 1280X960 a 12,5FPS - 1280x960 a 25FPS / 0,01 Lux . (2,8mm). Compresión Dual-Codec (MJPEG / H.264) Stream de Video: Dual Conexión: TCP/IP, POE. Alimentación 5V. Sensor de movimiento. In/Out Incluye: Software de 64ch. Lente y soporte	4	320,00	1.280,00

Quito- Ecuador

4	**DS-2CD2112-I** HIKVISION **CAMARA IP DOMO ANTIVANDALICA CON IR DIA/NOCHE C/ICR 1.3 M-PIXEL, (3GPP) WIDE DYNAMIC RANGE (WDR-D), ESCANEO PROGRESIVO** Res: 1280 X 960 a 30FPS - 1280x720 a 30FPS / 0,01 Lux . (2,8mm). Compresión Dual-Codec (MJPEG / MPEG4 / H.264) Stream de Video: Dual Conexión: TCP/IP, POE. Alimentación 12V. Incluye: Software de 64ch. Lente.	4	262,00	1.048,00
5	**DS-2CD2132-I** HIKVISION **CAMARA IP DOMO ANTIVANDALICA CON IR DIA/NOCHE C/ICR 3 M-PIXEL, (3GPP) WIDE DYNAMIC RANGE (WDR-D), ESCANEO PROGRESIVO** Res: 1920x1080 a 30FPS - 2048x1536 a 15FPS / 0,05 Lux . (2,8mm). Compresión Dual-Codec (MJPEG / MPEG4 / H.264) Stream de Video: Dual Conexión: TCP/IP, POE. Alimentación 12V. Incluye: Software de 64ch. Lente.	4	334,00	1.336,00

Condiciones Comerciales

Validez de la oferta: 15 días.
Garantía: 12 meses.
Forma de Pago: Contra entrega.
Tiempo de Entrega: Inmediata. Sujeto a stock.
Observaciones:
-El equipo se entregará en sus oficinas de Quito.

Le agradecemos nos haya brindado la posibilidad de cotizar nuestros productos. En caso de necesitar alguna aclaración, nuestro departamento de ventas estará gustoso de atenderles.

Maribel Menacho
Ejecutiva de Ventas
Correo Electrónico: mmenacho@biometrik.com.bo

Cliente:	CEJPM
Proyecto:	RED LAN
País:	Ecuador
Fecha de Creación:	19/06/2014
Creado por:	David Zambonino
Moneda:	USD
Lista de Precios:	Global PriceList-Latin America

LOGICALIS
Business and technology working as one

Nº	Número de Parte	Descripción	Cantidad	Precio Unit	Precio Lista	PVP
Productos						
1.0	WS-C2960+24PC-L	Catalyst 2960 Plus 24 10/100 PoE + 2 T/SFP LAN Base	2	2.495,00	4.990,00	3.293,40
1.1	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00	0,00
2.0	WS-C2960+48PST-L	Catalyst 2960 Plus 48 10/100 PoE + 2 1000BT +2 SFP LAN Base	6	4.295,00	25.770,00	17.008,20
2.1	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	6	0,00	0,00	0,00
3.0	WS-C3750X-24S-S	Catalyst 3750X 24 Port GE SFP IP Base	2	20.000,00	40.000,00	26.400,00
3.1	CAB-3KX-AC	AC Power Cord for Catalyst 3K-X (North America)	4	0,00	0,00	0,00
3.2	C3KX-PWR-350WAC/2	Catalyst 3K-X 350W AC Secondary Power Supply	2	500,00	1.000,00	660,00
3.3	S375XVK9T-15002SE	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2	0,00	0,00	0,00
3.4	CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	2	0,00	0,00	0,00
3.5	CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	2	0,00	0,00	0,00
3.6	C3KX-PWR-350WAC	Catalyst 3K-X 350W AC Power Supply	2	0,00	0,00	0,00
4.0	AIR-CAP1602E-AK910	802.11a/g/n Ctrlr-based AP Ext Ant A Reg Domain 10 APs	1	7.950,00	7.950,00	5.247,00
4.1	AIR-AP-T-RAIL-F	Ceiling Grid Clip for Aironet APs - Flush Mount	10	0,00	0,00	0,00
4.2	AIR-CHNL-ADAPTER	T-Rail Channel Adapter for Cisco Aironet Access Points	10	5,00	50,00	33,00
4.3	AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	10	0,00	0,00	0,00
4.4	AIR-ANT2524DW-R	2.4 GHz 2 dBi/5 GHz 4 dBi Dipole Ant. White RP-TNC	30	39,00	1.170,00	772,20
4.5	AIR-CAP1602E-ABULK	BOM Level AP1600e Bulk PID for A reg domain	10	0,00	0,00	0,00
4.6	SWAP1600-RCOVRY-K9	Cisco 1600 Series IOS WIRELESS LAN RECOVERY	1	0,00	0,00	0,00
4.7	AIR-OPT60-DHCP	Service Provider Option 60 for Vendor Class Identifier	1	0,00	0,00	0,00
5.0	BE6K-8T-BDL-XU=	Cisco BE6000 Medium Density Server Export Unrestricted SW	1	9.400,00	9.400,00	6.204,00
5.1	CAB-N5K6A-NA	Power Cord 200/240V 6A North America	1	0,00	0,00	0,00
5.2	BE6K-SW-9X10X-XU	Cisco Business Edition 6000 - Sw App 9X 10X Unrestricted	1	0,00	0,00	0,00
5.3	CIT-PSU-BLKP	Power Supply Blanking Panel/Filler	1	0,00	0,00	0,00
5.4	CIT-SD-16G-C220	16GB SD Card Module for C220 servers	1	0,00	0,00	0,00
5.5	CTI-VCSC-BE6K-PAK	Config Only E-Delivery VCS Control PAK PID	1	0,00	0,00	0,00
5.6	LIC-SW-VMVCS	Software Release Key for Virtual VCS Application	1	0,00	0,00	0,00
5.7	LIC-VCS-10+	Video Comm Server 10 Add Non-traversal Network Calls	1	0,00	0,00	0,00
5.8	LIC-VCS-GW	Enable GW Feature (H323-SIP)	1	0,00	0,00	0,00
5.9	LIC-VCSE-5+	Video Communication Server - 5 Traversal Calls	1	0,00	0,00	0,00
5.10	R2XX-RAID10	Enable RAID 10 Setting	1	0,00	0,00	0,00
5.11	UC-A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF Hot Plug/Drive Sled Mounted	4	0,00	0,00	0,00
5.12	UC-CPU-E5-2609	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1066MHz	2	0,00	0,00	0,00
5.13	UC-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/Dual Rank/1.35v	4	0,00	0,00	0,00
5.14	UC-PSU-650W	650W Power Supply Unit For UCSC C220 Rack Server	1	0,00	0,00	0,00
5.15	UC-RAID-9271	MegaRAID 9271-8i + Battery Backup for C240 and C220	1	0,00	0,00	0,00
5.16	VMW-VSS-HYP-K9	Cisco UC Virt. Hypervisor 5.x (2-socket)	1	0,00	0,00	0,00
5.17	VMW-VSS-SNS	Cisco UC Virt. Hypervisor 5.x - SnS	1	0,00	0,00	0,00
6.0	C2921-CME-SRST/K9	CUBE10	1	5.195,00	5.195,00	3.428,70
6.1	S29UK9-15204M	Cisco 2901-2921 IOS UNIVERSAL	1	0,00	0,00	0,00
6.2	SL-29-APP-K9	AppX License for Cisco 2900 Series	1	1.000,00	1.000,00	660,00
6.3	FL-CME	Cisco Communications Manager Express License	1	0,00	0,00	0,00
6.4	FL-C2921-WAASX	WAASX Feature License RTU (Paper) for 2921	1	0,00	0,00	0,00
6.5	PWR-2921-51-AC	Cisco 2921/2951 AC Power Supply	1	0,00	0,00	0,00
6.6	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	1	0,00	0,00	0,00
6.7	FL-CME-SRST-25	Communication Manager Express or SRST - 25 seat license	1	0,00	0,00	0,00
6.8	FL-CUBEE-5	Unified Border Element Enterprise License - 5 sessions	2	0,00	0,00	0,00
6.9	PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	1	0,00	0,00	0,00
6.10	SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1	0,00	0,00	0,00
6.11	SL-29-UC-K9	Unified Communication License for Cisco 2901-2951	1	0,00	0,00	0,00
6.12	SL-29-DATA-K9	Data License for Cisco 2901-2951	1	0,00	0,00	0,00
6.13	WAAS-RTU-1300	WAAS and VWAAS Right to Use for 1300 connections	1	0,00	0,00	0,00
6.14	HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	4	0,00	0,00	0,00
6.15	ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	1	0,00	0,00	0,00
6.16	MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)	1	0,00	0,00	0,00
6.17	MEM-CF-256MB	256MB Compact Flash for Cisco 1900 2900 3900 ISR	1	0,00	0,00	0,00
6.18	PVDM3-32	32-channel high-density voice and video DSP module	1	0,00	0,00	0,00
6.19	SM-D-BLANK	Blank faceplate for DW slot on Cisco 2951 and 3925	1	0,00	0,00	0,00
6.20	SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900/3900/4400 ISR	1	0,00	0,00	0,00
7.0	CP-7962G	Cisco UC Phone 7962	40	495,00	19.800,00	13.068,00
7.1	SW-CCM-UL-7962	CUCM 3.x or 4.x RTU lic. for single IP Phone 7962	40	200,00	8.000,00	5.280,00
8.0	CIVS-IPC-4500E	Cisco 4500E IP Camera HD Day/Night	16	1.800,00	28.800,00	19.008,00
8.1	CIVS-IPCA-PWR12V	Cisco IP Camera Power Supply	16	60,00	960,00	633,60
8.2	CIVS-IPC-VFM28-12	Cisco IP Camera Lens Megapixel 2.8-12mm Fujinon	16	295,00	4.720,00	3.115,20
8.3	FL-CVA-CP-4500	Cisco Video Analytics - Counting Plus Package	16	100,00	1.600,00	1.056,00
9.0	UCS-SPR-C220-E1	RAILS	2	5.193,00	10.386,00	6.854,76

9.1	UCS-CPU-E52609B	2.50 GHz E5-2609 v2/80W 4C/10MB Cache/DDR3 1333MHz	4	0,00	0,00	0,00
9.2	UCS-MR-1X082RZ-A	8GB DDR3-1866-MHz RDIMM/PC3-14900/dual rank/x4/1.5v	4	0,00	0,00	0,00
9.3	A03-D1TBSATA	1TB 6Gb SATA 7.2K RPM SFF HDD/hot plug/drive sled mounted	2	974,00	1.948,00	1.285,68
9.4	CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	4	0,00	0,00	0,00
9.5	UCSC-PSU-650W	650W power supply for C-series rack servers	4	0,00	0,00	0,00
9.6	UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	2	0,00	0,00	0,00
9.7	UCS-SD-16G	16GB SD Card module for UCS Servers	2	0,00	0,00	0,00
9.8	N20-BBLKD	UCS 2.5 inch HDD blanking panel	14	0,00	0,00	0,00
9.9	UCSC-HS-C220M3	Heat Sink for UCS C220 M3 Rack Server	4	0,00	0,00	0,00
9.10	UCSC-PCIF-01F	Full height PCIe filler for C-Series	2	0,00	0,00	0,00
9.11	UCSC-PCIF-01H	Half height PCIe filler for UCS	2	0,00	0,00	0,00
9.12	UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	2	0,00	0,00	0,00
10.0	ASA5545-IPS-K9	ASA 5545-X with IPS SW 8GE Data 1GE Mgmt AC 3DES/AES	2	31.995,00	63.990,00	42.233,40
10.1	ASA-IC-6GE-CU-C	ASA 5545-X/5555-X Interface Card 6-port 10/100/1000 RJ-45	2	5.000,00	10.000,00	6.600,00
10.2	SF-ASA-X-9.1-K8	ASA 9.1 Software Image for ASA 5500-X Series5585-X & ASA-SM	2	0,00	0,00	0,00
10.3	SF-ASAIPS64-7.1-K9	ASA 5500-X IPS Software 7.1 for IPS SSP	2	0,00	0,00	0,00
10.4	ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2	1.500,00	3.000,00	1.980,00
10.5	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00	0,00
10.6	ASA5545-IPS-SSP	ASA 5545-X IPS SSP License	2	0,00	0,00	0,00
10.7	ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows Solaris Linux Mac)	2	0,00	0,00	0,00
10.8	ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2	0,00	0,00	0,00
10.9	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2	0,00	0,00	0,00
10.10	ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2	0,00	0,00	0,00
10.11	ASA5545-MB	^ASA 5545 IPS Part Number with which PCB Serial is associated	2	0,00	0,00	0,00
10.12	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00	0,00
					Subtotal de Equipos (USD)	164.821,14
Servicios Cisco						
1.0.1	CON-PSRT-WSC2964L	PRTNR SS 8X5XNBD Catalyst 2960 Plus 24 10/100 PoE + 2 T/S	2	82,72	165,44	95,96
2.0.1	CON-PSRT-WSC296TL	PRTNR SS 8X5XNBD Catalyst 2960 Plus 48 10/100 PoE + 2 100	6	141,99	851,94	494,13
3.0.1	CON-PSRT-C375X24S	PRTNR SS 8X5XNBD Catalyst 3750X 24 Port GE SFP IP Base	2	1.045,11	2.090,22	1.212,33
4.0.1	CON-PSRT-C162EA10	PRTNR SS 8X5XNBD 802.11a/g/n Ctlr-ba	1	0,00	0,00	0,00
4.5.0.1	CON-PSRT-C162EABK	PRTNR SS 8X5XNBD BOM Level AP1600e Bu	10	17,48	174,80	101,38
5.0.1	CON-PSUP-BE6KSTXU	PRTNR SUP 24X7X4 Cisco BE 6000 UCS C Server 9.0-XU SW	1	210,22	210,22	121,93
6.0.1	CON-PSRT-2921CMST	PRTNR SS 8X5XNBD 2921 Voice Bundle w/ UC License PAK	1	302,74	302,74	175,59
7.0.1	CON-PSRT-CP7962	PRTNR SS 8X5XNBD Cisco Unified IP Phone 7962	40	5,54	221,60	128,53
8.0.1	CON-SNT-CIVSIP45	SMARTNET 8X5XNBD Cisco 4500E IP Camera HD Day/Night	16	173,25	2.772,00	1.607,76
8.3.0.1	CON-SNT-CP4500	SMARTNET 8X5XNBD Cisco Video Analytics - Counting Plus Pa	16	9,63	154,08	89,37
9.0.1	CON-PSW2-SRC220E1	8	2	168,23	336,46	195,15
10.0.1	CON-PSUP-A45IPS9	PRTNR SUP 24X7X4 ASA 5545-X with IPS SW 8GE Data 1GE M	2	1.662,96	3.325,92	1.929,03
10.1.0.1	CON-PSUP-ASACUC1	PRTNR SUP 24X7X4 ASA 5545-X/5555-X In	2	527,88	1.055,76	612,34
					Subtotal de Servicios (USD)	6.783,50
					Total (Cisco)(USD)	171.584,64
Cableado Estructurado						
11.0	CAB-CM-100	Feet	37	394,68	14.603,16	5.549,20
12.0	CAB-FH26	Bobina de fibra óptica 62.5/125 multimodo 2.0 mm duplex de 300 m	5	1.267,92	6.339,62	3.867,17
13.0	CAB-CM-5PACK-EPCB7F	Feet	55	43,55	2.395,07	910,13
14.0	CAB-2M-FPCLC	2M Multimode Duplex Fiber Optic Cable (62.5/125) - LC to LC	14	126,13	1.765,76	1.077,12
15.0	DP24688TGY	Panel	8	553,32	4.426,59	2.700,22
16.0	CPPKLTP48WBLY	Panduit - CPPKLTP48WBLY - 48-p Panel 110mod 8w8p T568a/b Cat6 Xp7 Giga-ch Tx-6 T3 Kit Blk 2rms Wlb Rohs	7	773,80	5.416,58	3.304,11
17.0	WMP1E	Panduit Patchlink 19" Cable Manager Front Only - 2 Ru	17	130,42	2.217,07	1.352,41
18.0	FMT1	Panduit FMT1 Rack Mount Fiber Tray	6	276,69	1.660,13	1.012,68
19.0	FAP6WEIDLC	Panduit FAP6WEIDLC Multi-Mode 6-Port Fiber Adapter Panel with Phosphor Bronze Split Sleeve, Electric Ivory	6	179,42	1.076,55	656,70
20.0	WMPVF45E	Panduit WMPVF45E Vertical Cable Manager, Black	24	339,41	8.145,78	4.968,93
21.0	M8X2	Furman M-8X2 Merit Series 8 Outlet Power Conditioner and Surge Protector	7	154,44	1.081,08	724,32
22.0	SRW18US	Tripp Lite SRW18US 18U Wall Mount Rack Enclosure Server Cabinet Door/Sides, Hinged	3	1.467,18	4.401,54	2.949,03
23.0	SRW26US	Tripp Lite SRW26US 26U Wall Mount Rack Enclosure Server Cabinet Door/Sides, Hinged	2	1.976,83	3.953,66	2.648,95
24.0	SR48UBEXPNDNR3	Tripp Lite SR48UBEXPNDNR3 48U OPEN RACK 4POST SVR CABINET HEAVY DUTY CASTER	1	2.690,09	2.690,09	1.802,36
25.0	75-100BL	ADANAC R034PEB-SP100F 100' Reel, 3/4" Split Convoluted Wire Conduit	125	63,30	7.912,91	5.301,65
26.0	50-100BL	Drossbach R012PEBS100 1/2" x 100' Black Corrugated Tubing/Split Loom	125	53,42	6.677,39	4.473,85
27.0	R100PEBS	ADANAC R100PEB-S0050F 50' Reel, 1" Split Convoluted Wire Conduit	125	63,66	7.957,95	5.331,83
28.0	ABR14 x 50	Flexible Conduit, 1 1/4in, 50Ft, Aluminum	125	230,17	28.771,25	6.617,39
29.0	CJ6X88TGBL	Jack RJ 45 Cat. 6A,10 Gb/sde 8posiciones y 8hilos color negro	672	4,79	3.221,30	2.158,27
30.0	CFPE1IWY	Face PlateEjecutivo de 2salidas	336	4,79	1.609,44	1.078,32
31.0	CAB_CAN_PAN3012	Canaleta Plástica 30x12	250	9,01	2.252,25	1.509,01
32.0	CAB_CAN_PAN4024	Canaleta Plástica 40x24	250	10,99	2.747,75	1.840,99
33.0	CAB_CAN_PAN4040	Canaleta Plástica 40x40	250	21,62	5.405,40	3.621,62
34.0	CAB_CAN_PAN6040	Canaleta Plástica 60x40	250	36,69	9.172,80	6.145,78
35.0	CAB_CAN_ACC_PAN3012	Accesorios de Canaleta 30x12	680	1,80	1.225,22	820,90
36.0	CAB_CAN_ACC_PAN4024	Accesorios de Canaleta 40x24	680	3,60	2.450,45	1.641,80
37.0	CAB_CAN_ACC_PAN4040	Accesorios de Canaleta 40x40	680	5,41	3.675,67	2.462,70

TOTALTEK
tecnología y servicio

Número:	AV00832
Fecha:	19-jun-14
Cliente:	CEJPM
Descripción:	Networking

Responsable: AV

Equipamiento Wireless Cisco

Cotización Venta - Instalación Equipos de Networking Y Cableado

Núero de Parte	Descripción	Cantidad	Precio Unit	PVP
WS-C2960+24PC-L	Catalyst 2960 Plus 24 10/100 PoE + 2 T/SFP LAN Base	2	2.495,00	4.990,00
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00
WS-C2960+48PST-L	Catalyst 2960 Plus 48 10/100 PoE + 2 1000BT +2 SFP LAN Base	6	4.295,00	25.770,00
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	6	0,00	0,00
WS-C3750X-24S-S	Catalyst 3750X 24 Port GE SFP IP Base	2	20.000,00	40.000,00
CAB-3KX-AC	AC Power Cord for Catalyst 3K-X (North America)	4	0,00	0,00
C3KX-PWR-350WAC/2	Catalyst 3K-X 350W AC Secondary Power Supply	2	500,00	1.000,00
S375XVK9T-15002SE	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2	0,00	0,00
CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	2	0,00	0,00
CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	2	0,00	0,00
C3KX-PWR-350WAC	Catalyst 3K-X 350W AC Power Supply	2	0,00	0,00
AIR-CAP1602E-AK910	802.11a/g/n Ctrlr-based AP Ext Ant A Reg Domain 10 APs	1	7.950,00	7.950,00
AIR-AP-T-RAIL-F	Ceiling Grid Clip for Aironet APs - Flush Mount	10	0,00	0,00
AIR-CHNL-ADAPTER	T-Rail Channel Adapter for Cisco Aironet Access Points	10	5,00	50,00
AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	10	0,00	0,00
AIR-ANT2524DW-R	2.4 GHz 2 dBi/5 GHz 4 dBi Dipole Ant. White RP-TNC	30	39,00	1.170,00
AIR-CAP1602E-ABULK	BOM Level AP1600e Bulk PID for A reg domain	10	0,00	0,00
SWAP1600-RCOVRY-K9	Cisco 1600 Series IOS WIRELESS LAN RECOVERY	1	0,00	0,00
AIR-OPT60-DHCP	Service Provider Option 60 for Vendor Class Identifier	1	0,00	0,00
BE6K-ST-BDL-XU=	Cisco BE6000 Medium Density Server Export Unrestricted SW	1	9.400,00	9.400,00
CAB-N5K6A-NA	Power Cord 200/240V 6A North America	1	0,00	0,00
BE6K-SW-9X10X-XU	Cisco Business Edition 6000 - Sw App 9X 10X Unrestricted	1	0,00	0,00
CIT-PSU-BLKP	Power Supply Blanking Panel/Filler	1	0,00	0,00
CIT-SD-16G-C220	16GB SD Card Module for C220 servers	1	0,00	0,00
CTI-VCSC-BE6K-PAK	Config Only E-Delivery VCS Control PAK PID	1	0,00	0,00
LIC-SW-VMVCS	Software Release Key for Virtual VCS Application	1	0,00	0,00
LIC-VCS-10+	Video Comm Server 10 Add Non-traversal Network Calls	1	0,00	0,00
LIC-VCS-GW	Enable GW Feature (H323-SIP)	1	0,00	0,00
LIC-VCSE-5+	Video Communication Server - 5 Traversal Calls	1	0,00	0,00
R2XX-RAID10	Enable RAID 10 Setting	1	0,00	0,00
UC-A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF Hot Plug/Drive Sled Mounted	4	0,00	0,00
UC-CPU-E5-2609	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1066MHz	2	0,00	0,00
UC-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/Dual Rank/1.35v	4	0,00	0,00
UC-PSU-650W	650W Power Supply Unit For UCSC C220 Rack Server	1	0,00	0,00
UC-RAID-9271	MegaRAID 9271-8i + Battery Backup for C240 and C220	1	0,00	0,00
VMW-VS5-HYP-K9	Cisco UC Virt. Hypervisor 5.x (2-socket)	1	0,00	0,00
VMW-VS5-SNS	Cisco UC Virt. Hypervisor 5.x - SnS	1	0,00	0,00
C2921-CME-SRST/K9	CUBE10	1	5.195,00	5.195,00
S29UK9-15204M	Cisco 2901-2921 IOS UNIVERSAL	1	0,00	0,00
SL-29-APP-K9	AppX License for Cisco 2900 Series	1	1.000,00	1.000,00
FL-CME	Cisco Communications Manager Express License	1	0,00	0,00
FL-C2921-WAASX	WAASX Feature License RTU (Paper) for 2921	1	0,00	0,00
PWR-2921-51-AC	Cisco 2921/2951 AC Power Supply	1	0,00	0,00

CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	1	0,00	0,00
FL-CME-SRST-25	Communication Manager Express or SRST - 25 seat license	1	0,00	0,00
FL-CUBEE-5	Unified Border Element Enterprise License - 5 sessions	2	0,00	0,00
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	1	0,00	0,00
SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1	0,00	0,00
SL-29-UC-K9	Unified Communication License for Cisco 2901-2951	1	0,00	0,00
SL-29-DATA-K9	Data License for Cisco 2901-2951	1	0,00	0,00
WAAS-RTU-1300	WAAS and VWAAS Right to Use for 1300 connections	1	0,00	0,00
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	4	0,00	0,00
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	1	0,00	0,00
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)	1	0,00	0,00
MEM-CF-256MB	256MB Compact Flash for Cisco 1900 2900 3900 ISR	1	0,00	0,00
PVDM3-32	32-channel high-density voice and video DSP module	1	0,00	0,00
SM-D-BLANK	Blank faceplate for DW slot on Cisco 2951 and 3925	1	0,00	0,00
SM-S-BLANK	Removable faceplate for SM slot on Cisco 290039004400 ISR	1	0,00	0,00
CP-7962G	Cisco UC Phone 7962	40	495,00	19.800,00
SW-CCM-UL-7962	CUCM 3.x or 4.x RTU lic. for single IP Phone 7962	40	200,00	8.000,00
CIVS-IPC-4500E	Cisco 4500E IP Camera HD Day/Night	16	1.800,00	28.800,00
CIVS-IPCA-PWR12V	Cisco IP Camera Power Supply	16	60,00	960,00
CIVS-IPC-VFM28-12	Cisco IP Camera Lens Megapixel 2.8-12mm Fujinon	16	295,00	4.720,00
FL-CVA-CP-4500	Cisco Video Analytics - Counting Plus Package	16	100,00	1.600,00
UCS-SPR-C220-E1	RAILS	2	5.193,00	10.386,00
UCS-CPU-E52609B	2.50 GHz E5-2609 v2/80W 4C/10MB Cache/DDR3 1333MHz	4	0,00	0,00
UCS-MR-1X082RZ-A	8GB DDR3-1866-MHz RDIMM/PC3-14900/dual rank/x4/1.5v	4	0,00	0,00
A03-D1TBSATA	1TB 6Gb SATA 7.2K RPM SFF HDD/hot plug/drive sled mounted	2	974,00	1.948,00
CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	4	0,00	0,00
UCSC-PSU-650W	650W power supply for C-series rack servers	4	0,00	0,00
UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	2	0,00	0,00
UCS-SD-16G	16GB SD Card module for UCS Servers	2	0,00	0,00
N20-BBLKD	UCS 2.5 inch HDD blanking panel	14	0,00	0,00
UCSC-HS-C220M3	Heat Sink for UCS C220 M3 Rack Server	4	0,00	0,00
UCSC-PCIF-01F	Full height PCIe filler for C-Series	2	0,00	0,00
UCSC-PCIF-01H	Half height PCIe filler for UCS	2	0,00	0,00
UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	2	0,00	0,00
ASA5545-IPS-K9	ASA 5545-X with IPS SW 8GE Data 1GE Mgmt AC 3DES/AES	2	31.995,00	63.990,00
ASA-IC-6GE-CU-C	ASA 5545-X/5555-X Interface Card 6-port 10/100/1000 RJ-45	2	5.000,00	10.000,00
SF-ASA-X-9.1-K8	ASA 9.1 Software Image for ASA 5500-X Series5585-X & ASA-SM	2	0,00	0,00
SF-ASAIPS64-7.1-K9	ASA 5500-X IPS Software 7.1 for IPS SSP	2	0,00	0,00
ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2	1.500,00	3.000,00
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00
ASA5545-IPS-SSP	ASA 5545-X IPS SSP License	2	0,00	0,00
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows Solaris Linux Mac)	2	0,00	0,00
ASA-PWR-AC	ASA 5545-X/5555-X AC Power Supply	2	0,00	0,00
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2	0,00	0,00
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2	0,00	0,00
ASA5545-MB	^ASA 5545 IPS Part Number with which PCB Serial is associated	2	0,00	0,00
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2	0,00	0,00
			Subtotal	***249.729,00***

Núero de Parte	Descripción	Cantidad	Precio	PVP
CON-PSRT-WSC2964L	PRTNR SS 8X5XNBD Catalyst 2960 Plus 24 10/100 PoE + 2 T/S	2	82,72	69,48
CON-PSRT-WSC296TL	PRTNR SS 8X5XNBD Catalyst 2960 Plus 48 10/100 PoE + 2 100	6	141,99	357,81
CON-PSRT-C375X24S	PRTNR SS 8X5XNBD Catalyst 3750X 24 Port GE SFP IP Base	2	1.045,11	877,89
CON-PSRT-C162EA10	PRTNR SS 8X5XNBD 802.11a/g/n Ctrlr-ba	1	0,00	0,00
CON-PSRT-C162EABK	PRTNR SS 8X5XNBD BOM Level AP1600e Bu	10	17,48	73,42
CON-PSUP-BE6KSTXU	PRTNR SUP 24X7X4 Cisco BE 6000 UCS C Server 9.0-XU SW	1	210,22	88,29
CON-PSRT-2921CMST	PRTNR SS 8X5XNBD 2921 Voice Bundle w/ UC License PAK	1	302,74	127,15
CON-PSRT-CP7962	PRTNR SS 8X5XNBD Cisco Unified IP Phone 7962	40	5,54	93,07
CON-SNT-CIVSIP45	SMARTNET 8X5XNBD Cisco 4500E IP Camera HD Day/Night	16	173,25	1.164,24
CON-SNT-CP4500	SMARTNET 8X5XNBD Cisco Video Analytics - Counting Plus Pa	16	9,63	64,71

CON-PSW2-SRC220E1	PSS 8	2	168,23	141,31
CON-PSUP-A45IPS9	PRTNR SUP 24X7X4 ASA 5545-X with IPS SW 8GE Data 1GE M	2	1.662,96	1.396,89
CON-PSUP-ASACUC1	PRTNR SUP 24X7X4 ASA 5545-X/5555-X In	2	527,88	443,42
			Subtotal	*4.897,68*
			S1	*254.626,68*

Núero de Parte	Descripción	Cantidad	Precio	PVP
CAB-CM-100	Feet	37	394,68	3.358,73
CAB-FH26	Bobina de fibra óptica 62.5/125 multimodo 2.0 mm duplex de 300 m	5	1.267,92	3.676,98
CAB-CM-5PACK-EPCB7F	7 Feet	55	43,55	550,87
CAB-2M-FPCLC	2M Multimode Duplex Fiber Optic Cable (62.5/125) - LC to LC	14	126,13	1.024,14
DP24688TGY	Panel	8	553,32	2.567,42
CPPKLTP48WBLY	Panduit - CPPKLTP48WBLY - 48-p Panel 110mod 8w8p T568a/b Cat6 Xp7 Giga-ch Tx-6 T3 Kit Blk 2rms Wlb Rohs	7	773,80	3.141,62
WMP1E	Panduit PatchInk 19" Cable Manager Front Only - 2 Ru	17	130,42	1.285,90
FMT1	Panduit FMT1 Rack Mount Fiber Tray	6	276,69	962,87
FAP6WEIDLC	Panduit FAP6WEIDLC Multi-Mode 6-Port Fiber Adapter Panel with Phosphor Bronze Split Sleeve, Electric Ivory	6	179,42	624,40
WMPVF45E	Panduit WMPVF45E Vertical Cable Manager, Black	24	339,41	2.851,02
M8X2	Furman M-8X2 Merit Series 8 Outlet Power Conditioner and Surge Protector	7	154,44	378,38
SRW18US	Tripp Lite SRW18US 18U Wall Mount Rack Enclosure Server Cabinet Door/Sides, Hinged	3	1.467,18	1.540,54
SRW26US	Tripp Lite SRW26US 26U Wall Mount Rack Enclosure Server Cabinet Door/Sides, Hinged	2	1.976,83	1.383,78
SR48UBEXPNDNR3	Tripp Lite SR48UBEXPNDNR3 48U OPEN RACK 4POST SVR CABINET HEAVY DUTY CASTER	1	2.690,09	941,53
75-100BL	ADANAC R034PEB-SP100F 100' Reel, 3/4" Split Convoluted Wire Conduit	125	63,30	2.769,52
50-100BL	Drossbach R012PEBS100 1/2" x 100' Black Corrugated Tubing/Split Loom	125	53,42	2.337,08
R100PEBS	ADANAC R100PEB-S0050F 50' Reel, 1" Split Convoluted Wire Conduit	125	63,66	2.785,28
ABR14 x 50	Flexible Conduit, 1 1/4in, 50Ft, Aluminum	125	230,17	6.517,39
CJ6X88TGBL	Jack RJ 45 Cat. 6A10 Gb/sde 8posiciones y 8ilos color negro	672	4,79	1.127,45
CFPE1IWY	Face PlatEjecutivo de 2alidas	336	4,79	563,30
CAB_CAN_PAN3012	Canaleta Plástica 30x12	250	9,01	1.509,01
CAB_CAN_PAN4024	Canaleta Plástica 40x24	250	10,99	1.840,99
CAB_CAN_PAN4040	Canaleta Plástica 40x40	250	21,62	3.621,62
CAB_CAN_PAN6040	Canaleta Plástica 60x40	250	36,69	6.145,78
CAB_CAN_ACC_PAN3012	Accesorios de Canaleta 30x12	680	1,80	820,90
CAB_CAN_ACC_PAN4024	Accesorios de Canaleta 40x24	680	3,60	1.641,80
CAB_CAN_ACC_PAN4040	Accesorios de Canaleta 40x40	680	5,41	2.462,70
CAB_CAN_ACC_PAN6040	Accesorios de Canaleta 60x40	680	9,01	4.104,50
			Subtotal	**62.635,50**
			S2	*62.635,50*

Núero de Parte	Descripción	Cantidad	Precio	PVP
	Instalación de la solución	1	13.000,00	8.710,00
			Subtotal	**8.710,00**
			S3	*8.710,00*
			Gran Total	**325972,18**

Oferta Seguridad Perimetral
Sophos 320

Preparada para:

COLEGIO EXPERIMENTAL JUAN PIO MONTUFAR

Junio, 2014

Quito, 26 de Junio de 2014

Ingeniero
Alexis Paspuel
Ing. Sistemas Colegio Experimental Juan Pío Montufar
COLEGIO EXPERIMENTAL
JUAN PIO MONTUFAR
Quito - Ecuador

Apreciado Ingeniero:

GMS agradece la oportunidad de presentarle esta oferta de soluciones informáticas. Somos una empresa de consultoría de TI con más de 30 años de experiencia, durante los cuales hemos podido atender a muchas de las compañías más importantes de la región. Nuestras soluciones cubren las más altas exigencias de nuestros clientes, y nos caracterizamos por cumplir proyectos de alta complejidad. Asumimos el papel de socio estratégico para establecer relaciones exitosas a largo plazo.

Esperamos que esta propuesta sea de su conveniencia y quedo a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Atentamente,

Leonardo Peña C.
Asesor Comercial
leonardo.pena@gms.com.ec
Oficina: 02 3993 000 ext 7513
Celular: 09 58788506
www.gms.com.ec
Quito – Guayaquil – Cuenca – Bogotá

I. Información sobre GMS

Perfil empresarial

Fundada en 1978, GMS es una de las empresas de consultoría informática de mayor trayectoria en la región. Nuestra misión es potenciar la habilidad empresarial de nuestros clientes hacia la excelencia, a través de tecnología de vanguardia, sistemas y servicios de alta calidad. Medimos nuestros resultados según los que obtienen nuestros clientes, ya que nos consideramos sus socios de negocio para asegurar el mejor retorno sobre las inversiones que realizan con nosotros.

Nuestro principal diferenciador es nuestro personal, y definimos nuestra identidad de ***genteinteligente*** a base de los equipos de trabajo que formamos con nuestros clientes. Profesionales altamente capacitados de GMS participan de la mano con sus contrapartes en las empresas que apoyamos para entender a fondo sus requerimientos y definir las soluciones más inteligentes a cada entorno particular. Esta cooperación es la base sobre la cual construimos relaciones a largo plazo que permiten lograr los mejores resultados.

A partir de nuestro personal, hemos formado un portafolio de productos y servicios que nos permite ofrecer soluciones integradas de seguridad informática, telecomunicaciones, administración de infraestructura TI y cloud services. Estas soluciones se complementan con servicios de consultoría en estrategias y normas de TI y seguridad, y servicios de desarrollo de aplicaciones. Con nuestro apoyo, su empresa puede dejar en el pasado preocupaciones como incompatibilidad entre herramientas o rendición de cuentas con diversos proveedores que no logran responsabilizarse de la operación global de su red empresarial.

Sistemas de gestión

Para asegurar los niveles de servicio que requieren las empresas más exigentes, GMS opera con un sistema de gestión ITIL para el control de actividades y requerimientos. En el mismo, hemos habilitado un portal web que permite a nuestros clientes revisar el historial de los trabajos realizados para ellos, ingresar nuevas solicitudes, y hacer un seguimiento sobre el avance de las mismas. El sistema también permite registrar los niveles de satisfacción ante los soportes entregados, con lo cual mantenemos un control para asegurar un mejoramiento continuo.

Todos nuestros servicios cuentan con esquemas de escalamiento. Estos aseguran redundancia en canales de comunicación para que los clientes puedan aprovechar del soporte 7x24 ofrecido por GMS. Adicionalmente establecen tiempos de respuesta para distintos tipos de requerimientos, incluyendo los mecanismos de apoyo por parte de fabricantes internacionales, según el caso. La combinación de estos elementos permite a GMS otorgar niveles de atención y apoyo que marcan la diferencia.

Clientes destacados

Nuestro mayor logro ha sido conseguir y mantener la confianza de nuestros clientes. Más de 2.000 empresas han decidido trabajar con GMS. Entre algunas que lideran sus respectivos sectores se encuentran las siguientes:

Sector Financiero:

- Aseguradora del Sur
- Asociación de Bancos Privados del Ecuador
- Banco Amazonas
- Banco de Loja
- Banco del Austro
- Banco del Pacífico
- Banco Internacional
- Banco Territorial
- Cooperativa de Ahorro y Crédito Ejército Nacional
- Cooperativa de Ahorro y Crédito San Francisco
- Cooperativa Juventud Ecuatoriana Progresista
- Helm Bank
- Raul Coka Barriga Seguros
- ZHM Seguros y Reaseguros

Manufactura y Consumo Masivo:

- Chalde & Chalde
- DANEC
- Endesa / Grupo Durini
- Industrias Ales
- INGESA
- La Fabril
- LEVAPAN
- Manufacturas Americanas
- Mercantil Garzozi & Garbu
- Neypiex
- Novopan / Pelikano
- Plásticos Ecuatorianos
- REYBANPAC
- ZaiMella

Educación:

- Colegio Tomás Moro
- Escuela Politécnica del Ejército
- Escuela Politécnica Nacional
- Universidad Católica Santiago de Guayaquil
- Universidad de las Américas
- Universidad de Milagro – UNEMI
- Universidad Estatal de Bolívar
- Universidad San Francisco de Quito
- Universidad Tecnológica Equinoccial

Gobierno:

- Armada del Ecuador
- Consorcio Nacional de Telecomunicaciones - CNT
- Fuerza Aérea del Ecuador
- H. Consejo Provincial del Guayas
- H. Consejo Provincial de Pichincha
- Instituto Ecuatoriano de Seguridad Social
- Ministerio de Coordinación de Desarrollo Social
- Ministerio de Relaciones Exteriores
- Servicio de Rentas Internas

Servicios:

- Adecco
- AviancaTaca / Aerogal
- Cobiscorp
- Ernst & Young
- INMEDICAL
- Hospital Metropolitano
- Hotel Howard Johnson
- Multitrabajos.com
- Pérez Bustamante y Ponce
- Ils Servilogistics
- Junta de Beneficencia de Guayaquil
- Transoceánica

Medios de Comunicación y Publicidad:

- Canal 1
- Diario EL UNIVERSO
- Cybergulas (gulatelefonica.com.ec)
- EDIMPRES (Diario Hoy, TV Hoy, Newsweek)
- Editores Nacionales (Vistazo, América Economía, etc.)
- Impulso Comunicadores (Ecuadorinmediato.com)
- Gráficos Nacionales (Diario Extra)
- Induvallas
- Grupo EL COMERCIO
- Grupo K
- Rivas Herrera Young & Rubicam
- Sonorama

Energía y Petróleos:

- CELEC
- CNEL
- Compañía de Petróleos de los Ríos - Petroríos
- Consejo Nacional de Electricidad
- Empresa Eléctrica Regional Centro Sur
- Empresa Eléctrica de Riobamba
- EP Petroecuador
- Grupo Azul
- Lutexsa Industrial – TERPEL
- Operaciones Río Napo
- P & S – Petróleos y Servicios
- SERTECPET
- SINOPEC International Petroleum Service Ecuador
- Sipetrol

Comercialización:

- Almacenes La Ganga
- Autolasa
- Comercial JAHER
- Comercial Kywi
- Consorcio NOBIS
- Distribuidora Farmacéutica - DIFARE
- Firmesa Industrial
- Grupo KFC
- Marcimex
- Motransa – Mitsubishi
- IIASA Caterpillar
- Juan Marcet
- Tiendas Industriales Asociadas - TIA
- Toyota del Ecuador

Servicios y Soluciones

En un entorno empresarial cada día más interconectado, se ha vuelto indispensable asegurar una correcta integración entre los componentes que sustentan la información de su negocio: telecomunicaciones, seguridad informática y aplicaciones. GMS ofrece experiencia y soluciones del más alto nivel en cada una de estas áreas, para asegurar a su empresa la correcta coordinación y óptimo funcionamiento de las mismas.

Consultoría

Las decisiones de inversión en soluciones informáticas deben basarse en una visión clara de los problemas, sus impactos y sus soluciones, para así asegurar que generen un retorno para la empresa. GMS puede ayudar a lograr este objetivo a través de servicios de consultoría, sea esta en relación a procesos TICS, seguridades o infraestructura.

Consultoría

Áreas de competencia en procesos TICS:
Estrategia de servicios basada en Buenas Prácticas ITIL
Alineación de TICS con estrategias corporativas
Definición de proyectos y construcción de mapas de ruta
Definición de políticas de buen uso de TICS

Áreas de competencia en seguridades:
Sistemas de Gestión de Seguridad de Información (SGSI), incluyendo ISO 27000
Clasificación de información
Continuidad de negocio
Ethical Hacking

Áreas de competencia en infraestructura:
Auditoría de hardware y software
Optimización de uso de recursos tecnológicos (ej. ancho de banda)
Análisis de retorno sobre la inversión (ROI) en proyectos de infraestructura

Seguridad Informática

La evolución de amenazas informáticas exige cubrir cada vez más frentes, sean capas de infraestructura dentro de nuestra red o dispositivos fuera de ella. Ofrecemos una amplia gama de soluciones especializadas para que su organización no sea vulnerada por el eslabón más débil de la seguridad:

Astaro hoy forma parte de Sophos, una de las empresas más grandes de seguridad informática a nivel mundial con más de 25 años de experiencia y aproximadamente 2.000 empleados. Astaro (Sophos UTM) protege a más de 100.000 redes, sean de PYMES, gobiernos, multinacionales o TELCOS, con una solución robusta e integral para la seguridad perimetral. Sophos UTM cuenta con diversas certificaciones y reconocimientos, incluyendo la distinción como líder en el Cuadrante Mágico de Gartner de soluciones UTM.

DigitalStakeout ofrece servicios de ciberinteligencia que permiten proteger su red institucional o corporativa y salvaguardar su reputación en línea. Con el monitoreo de reputación y tráfico de miles de millones de IP's a nivel mundial, DigitalStakeout puede identificar la fuente y naturaleza de amenazas que afectan a su red. Sus motores de escaneo de redes sociales y sitios de phishing pueden ayudarle a asegurar que su identidad en Internet no sea vulnerada.

Kaspersky Lab es uno de los líderes mundiales en seguridad interna, especialista en tecnología antimalware. Fundada en Moscú en 1997, hoy protege a más de 300 millones de usuarios por todo el mundo. Su tecnología es regularmente premiada por analistas y publicaciones de renombre como Virus Bulletin, ICSA Labs, AV Comparatives (el cual le otorgó el premio de Antivirus del Año 2011), y Gartner, quien considera a Kaspersky Lab entre los líderes de su cuadrante de proveedores antimalware.

Qualys es el líder mundial en soluciones de gestión de vulnerabilidades y compliance, reconocido como tal por múltiples analistas incluyendo Gartner. Sus soluciones están en uso por miles de empresas en cerca de 100 países, incluyendo más de la mitad de las empresas en el Forbes Global 100. Su tecnología permite escanear vulnerabilidades en IP's internas, IP's externas y aplicaciones web, además de realizar escaneos de cumplimiento de políticas, incluyendo normas internacionales como PCI.

Safend, empresa especializada en soluciones DLP (prevención de fugas de información), fue fundada en Israel en el año 2003, y ahora es subsidiaria de Wave Systems, empresa líder en seguridad basada en hardware. Sus soluciones se destacan por su facilidad de uso y permiten inspeccionar el contenido del tráfico en un endpoint para asegurar su cumplimiento con políticas granulares de control de confidencialidad, además de manejar la encripción de datos y el uso de puertos, medios removibles y conexiones inalámbricas.

Transecq es una empresa que ha liderado la innovación en soluciones de seguridad móvil para bancos, operadoras móviles, instituciones de salud, entre otras. Ofrece una plataforma segura sobre la cual se pueden activar módulos tales como autenticación de doble factor o banca móvil. La

tecnología de Transecq (en proceso de patente global), permite identificar al usuario y su teléfono inteligente de forma única, con comunicación cifrada sobre plataforma de datos, lo cual da un nivel de seguridad previamente inalcanzable en el ámbito móvil.

Telecomunicaciones

GMS es el primer pionero en servicio de Internet Seguro y enlaces de datos con las seguridades más desarrolladas del país. Esto permite a su empresa tener un acceso protegido contra hackers, virus, spam, entre otros, lo cual además optimiza su tráfico. Adicionalmente ofrecemos equipos y servicios de telepresencia, ideales para maximizar las ventajas que su empresa recibe de las telecomunicaciones contratadas.

La experiencia de GMS en el manejo de redes, seguridades y aplicaciones nos permite asesorar a su empresa para la puesta en marcha del mejor esquema de conectividad. Con alianzas estratégicas con múltiples carriers, podemos lograr las combinaciones óptimas en costo y tecnología para beneficio de su compañía. Adicionalmente proveemos soluciones que le permiten acceder a esquemas muy eficientes de alta disponibilidad.

Vidyo, Inc. es una empresa con soluciones revolucionarias de videoconferencia y telepresencia. Considerado por analistas como alterador de las reglas de juego de la industria, Vidyo no solo ofrece su propia gama de equipos, sino también soluciones basadas en software que permiten a los clientes aprovechar su infraestructura existente. Fue fundada en EEUU en el año 2004 por expertos pioneros en tecnologías de videoconferencia.

Administración de Infraestructura TI

Las inversiones en TICS son significativas y es necesario maximizar su retorno por medio de una acertada administración. GMS ofrece soluciones de fabricantes especializados, sea en modalidad de compra de las mismas o por medio de servicios gerenciados / outsourcing.

Allot Communications es un proveedor líder de soluciones inteligentes de optimización IP, tanto para empresas como para operadores móviles e ISP's. Fundada en 1996 con origen en Israel, hoy cuenta con oficinas en 14 países y clientes alrededor de todo el mundo. Su tecnología propietaria DART para la administración dinámica de ancho de banda permite visibilidad y administración total sobre aplicación, usuario y topología.

Aranda Software Corp. ofrece soluciones de administración de infraestructura TI que permiten aplicar las mejores prácticas de gestión ITIL. Es uno de los contados fabricantes a nivel mundial que cuenta una plataforma de Service Desk con más de 10 procesos certificados ITIL por Pink Elephant. La misma se integra con su producto de Asset Management para una administración unificada.

Desarrollo de software

Sea que requiera servicios o herramientas, GMS puede aportar mucho a los proyectos de desarrollo de aplicaciones en su empresa o institución.

Con un equipo humano con estándares elevados, metodologías formales en las fases de análisis, diseño, programación, pruebas e implementación,

y el uso de herramientas avanzadas, GMS es su socio ideal para enfrentar su próximo proyecto. Sea el desarrollo de su nuevo sistema back-office, la creación de un portal de reportes, o simplemente un servicio de acompañamiento, GMS puede marcar la diferencia.

GeneXus es la primera herramienta inteligente para crear, desarrollar y mantener en forma automática aplicaciones multiplataforma. Con GX, las puede adaptar fácilmente a los cambios del negocio y las nuevas posibilidades brindadas por la evolución tecnológica. GX es producto de la empresa Uruguaya Artech, fundada en 1988 con oficinas en Brasil, México, Japón y China para soportar a miles de clientes a nivel mundial.

Cloud Services

El avance del cloud computing es una tendencia inevitable y GMS puede ayudar a su empresa a aprovecharla.

GMS ofrece infraestructura en nubes locales que le permite a su empresa o institución ganar economías de escala y optimizar los costos de propiedad de equipamiento propio, sin la incomodidad de ceder control a un tercero distante. Si requiere proveer servicios vía Internet a sus clientes, también podemos apoyarle para habilitar su propia nube para ellos, siempre con el respaldo que permite nuestra experiencia en seguridad TI.

Reconocimientos

Gracias al compromiso con nuestros clientes, el nivel de nuestras soluciones, y nuestros sistemas de gestión, GMS ha logrado reconocimientos internacionales que son motivo de gran orgullo para nosotros. Entre ellos, se destacan los siguientes:

- **Kaspersky Lab**
  2007: Partner del Año, Latinoamérica
  2008: Spirit of Kaspersky
  2009: Partner del Año, Latinoamérica
  2010: Partner del Año, Latinoamérica
  2010-2011: Consejo Consultivo de Partners
  2011: Number 1 Club
  2011: Partner del Año (Enterprise), Mercados Emergentes (Latinoamérica + África + Medio Oriente + Europa del Este)

- **Astaro / Sophos**
  2010: Partner del Año, Sudamérica Hispana
  2011: Partner del Año (Sophos UTM), Latinoamérica

- **Asociación Brasilera de Calidad (ABIQUA)**
  2010: Premio Panamericano de Calidad 2010

II. Información sobre soluciones ofertadas

Sophos UMT – Astaro

Sophos UTM es una solución de seguridad que le proporciona una cobertura total del perímetro con gestión unificada de amenazas en la plataforma de su elección. Ya sea como hardware, software o como un dispositivo virtual, todos éstos cuentan con las mismas funcionalidades, tienen idéntica interfaz de usuario y se pueden desplegar en múltiples configuraciones.

Los módulos de Network, Mail y Web pueden ser añadidos de manera flexible a su plataforma de despliegue, dependiendo de sus necesidades empresariales. Cada aplicación ofrece un paquete completo de los mejores módulos de seguridad en su clase que aseguran una protección completa e integrada para su área de elección.

Sophos UTM es compatible con una serie de accesorios, entre las que se incluyen herramientas gratuitas para administración central, reportes y acceso remoto.

Perfil empresarial

Sophos es una compañía británica que ofrece las soluciones de seguridad para Internet más completas y fáciles de usar disponibles actualmente, al combinar las mejores aplicaciones del mercado y un rendimiento a nivel corporativo. Sophos cuenta con oficinas en todo el mundo y sus centros de operaciones están en Oxford (Inglaterra) y Boston (EE.UU.)

Sus galardonados productos proporcionan la protección más reciente con el mejor costo / beneficio. Su oferta de soluciones en software, hardware y virtual appliance proporcionan a los usuarios la flexibilidad necesaria para satisfacer una amplia variedad de escenarios de despliegue. Distribuidos a través de una creciente red de más de 2.500 partners a nivel mundial, los productos de Sophos protegen hoy en día más de 100.000 redes para más de 47.000 clientes en 60 países.

Sophos UTM mantiene presencia en Ecuador desde el año 2004 y se ha convertido en una excelente alternativa para empresas medianas y grandes, cuando se trata de maximizar la protección de sus redes con presupuestos limitados.

Sophos UTM tiene certificaciones ICSA, Common Criteria, y esta posicionado dentro del cuadrante de líderes en Gartner. Con sus funcionalidades superiores y su interface de usuario intuitiva, las soluciones de Sophos han sido elogiadas internacionalmente por publicaciones líderes en seguridad IT.

Ventajas principales de Sophos UTM - Astaro

Las innovaciones de Sophos han dado a las opciones de seguridad un nuevo significado. Una vez elegida la plataforma para Sophos UTM Gateway (appliance, software o appliance virtual) se está en capacidad de añadir cualquier combinación de las aplicaciones que tiene a su disposición, de modo que cuando una compañía esté enfrentando nuevos retos, ésta tenga la libertad de adaptar su seguridad perimetral a voluntad.

Hardware Appliance Software Appliance Virtual Appliance

El esquema de funcionamiento de Sophos UTM incluye 6 módulos funcionales, cada uno con distintas alternativas y funcionalidades de acuerdo a las necesidades del cliente:

- **Essential Protection** es una versión libre del Sophos UTM y ofrece funciones básicas de seguridad para ayudarle a proteger su red empresarial. Con esta herramienta puede empezar a poner en práctica un firewall libre en el ambiente IT de su empresa sin cargos ni compromisos.
- **Network Protection** incluye características totalmente integradas como un firewall configurado combinado con un sistema de Protección contra Intrusos (IPS), Denegación de Servicio (DoS), muchas herramientas de direccionamiento de tráfico y NAT, y mucho más.
- **Email Protection** asegura que el abuso al que el correo electrónico es sometido, tal como spam, virus y temas de privacidad, no afecte sus tareas de negocio diarias. A través de esta aplicación, los mensajes válidos son entregados apropiadamente y los empleados pueden encontrar lo que requieren sin ser expuestos a contenido peligrosos.
- **Web Protection** protege a sus empleados de amenazas y les permite aplicar condiciones de cómo y dónde pueden utilizar su tiempo en línea. Los programas espía (spyware) y virus son detenidos antes de que puedan entrar a la red y ocasionar daños. Todo es registrado y organizado en reportes detallados los cuales muestran que tan efectiva es su política, de modo que se puedan realizar ajustes.
- **Wireless Protection** Con Access Points (AP's) propietarios, provee administración centralizada y verdadera seguridad a redes inalámbricas. Soporta múltiples SSID's por equipo, roaming automático entre AP's, encripción avanzada y autenticación fuerte.
- **Web Server Protection** evita que su servidores de aplicaciones web sean víctimas de ataques modernos mediantes inyección de código SQL o XSS. Además asegura que los clientes que interactúan con sus aplicaciones web no puedan vulnerar debilidades de dichos servicios al forzar una interacción correcta con los servidores y protege a sus clientes mediante la generación de cookies firmadas digitalmente

Essential Network Firewall

Sophos UTM Essential Network Firewall ofrece funciones de seguridad básicas para ayudar a proteger una red corporativa. Sophos Essential Firewall protege un ilimitado número de direcciones IP y proporcionará indefinidamente las siguientes características

- Networking: Router de Internet Router, Bridging, servidor DNS & proxy, DynDNS, servidor DHCP & relay, soporte NTP, automatic QoS automatic
- Seguridad de Red: Firewall con Stateful Packet Inspection Firewall & Network Address translation (DNAT/SNAT/Masquerading)
- Acceso Remoto: soporte de PPTP y L2TP sobre IPSec (incluyendo soporte de iPhone)
- Registros / Informes: Registro complete en disco duro local, búsquedasg,reports en tiempo real para hardware, uso de la red y seguridad de la red, reports ejecutivos diarios
- Administración: GUI basada en web, asistente de instalación, respaldo y restauración de configuración, notificaciones administrativas, soporte SNMP, administración centralizada mediante Sophos UTM Manager.

Network Protection

El módulo de seguridad de red de Sophos permite controlar y proteger a la red corporativa de ataques de hackers, intrusos y controlar el acceso desde el Internet. Dentro de sus funciones principales se destacan las siguientes:

- Firewall: Un buen firewall puede detener eventos costosos que pueden llevar a una pérdida o robo de información, infección a estaciones de trabajo así como otros incidentes que pueden minar la productividad. Apropiadamente configurado, un firewall puede mantener protegido mucho de la operación de su empresa.

  El Firewall de Sophos Firewall incluye una combinación de múltiples herramientas ponderosas y características para controlar el flujo de información que circula desde el Internet a la red LAN y viceversa:
  - Stateful Packet Filter
  - Filtrado profundo de paquetes a nivel de aplicación
  - Administración flexible de reglas
  - Network Address Translation
- IPS / IDS: El Sistema de Prevención de Intrusos de Sophos UTM identifica y bloquea las amenazas ocultas en el tráfico entrante, y analiza el tráfico aprobado para proteger la red contra ataques externos. Esto permite separar el tráfico peligroso y mantener su red a salvo de agresiones externas.
- Control de DoS: Las conexiones de Internet son fácilmente localizadas y utilizadas maliciosamente incluso por los malwares más simples. La prevención mediante la Denegación de Servicio de Sophos mantiene sus recursos a salvo y sin daños durante estos ataques.
- Control de Ancho de Banda: El ancho de banda de Internet a menudo limita que tan rápido puede funcionar una red. Las empresas que aprovechan al máximo su ancho de banda disponible mantienen alta la productividad de sus empleados sin necesidad de que ellos experimenten demoras excesivas mientras trabajan.
- Autenticación de Directorio: La autenticación de directorio se enlaza con bases de datos externas y hace uso de sus usuarios y grupos en la configuración de seguridad. Una manera fácil de hacer que sus usuarios conecten sus VPNs con su misma clave de acceso.
- Portal de Usuario: El Portal de Usuario de Sophos es un centro autogestionado donde los empleados pueden trabajar con sus mensajes de email y tecnologías de acceso remoto previamente configuradas sin la necesidad de la ayuda de un Administrador.
- VPN para sucursales: Permite que los empleados de distintas oficinas envíen y reciban información por Internet a través de una conexión segura. Y es tan fácil de usar que podrá conectar varias sedes sin ningún tipo de experiencia en redes VPN.
- Portal VPN HTML5: Permite un acceso controlado a la red al personal informático que se encuentra fuera de la oficina y a terceros. Nuestro portal VPN HTML5 permite acceder a la red desde cualquier lugar.

Email Protection

El modulo Email Protection de Sophos permite el control del tráfico de correo electrónico desde y hacia la red corporativa, asegurando que spam, virus no se conviertan una amenaza para los usuarios. Dentro de sus características personales están:

- Anti Spam: Los correos no deseados o spam acarrean riesgos y roban valioso tiempo a sus empleados. Al utilizar el filtrado de correo de Sophos, todo el correo electrónico no deseado es detenido antes que estos sean entregados y copen espacio en los buzones de correo.
- Escaneo Antivirus: Desvía contenido malicioso o dañino a la entrada de la red usando un doble motor antivirus que funcionan en paralelo. Esto permite que el contenido sea escaneado y bloqueado antes que éste tenga oportunidad de entrar a la red.
- Encriptación de Correo: Los correos electrónicos están lejos de ser privados. Cualquiera ubicado entre el remitente y el destinatario puede interceptar, leer e incluso copiar o alterar su contenido. Sophos Email Encryption empaqueta sus mensajes de forma segura y los cierra con un sello de seguridad.
- Portal de Usuario: El Portal de Usuario de Sophos es un centro autogestionado donde los empleados pueden trabajar con sus mensajes de email y tecnologías de acceso remoto previamente configuradas sin la necesidad de la ayuda de un Administrador.

Web Server Protection

Web Server Protection de Sophos endurece sus servidores web para protegerlos de los ataques modernos y pérdida de información. Con esto se pueden ofrecer aplicaciones como Outlook Web Access (OWA) y protegerlo contra técnicas como Inyección SQL y Cross Site Scripting (XSS). Con esto se evita que hackers usen estos tipos de ataque para acceder a información sensible como tarjetas de crédito, información personal y números de identificación. Web Server Protection ayuda al cumplimiento de requisitos donde se requiere un firewall para aplicaciones web, como por ejemplo un PCI-DSS. Sus características principales son:

- Antivirus: Tiene dos motores de escaneo independientes que funcionan en paralelo para prevenir infecciones al tiempo de mantener a los usuarios y servidores a salvo. El contenido es escaneado y bloqueado en un punto central antes de que se le permita entrar o salir de la red.
- Endurecimiento URL: La característica de Sophos de endurecimiento de URLs permite mantener a los visitantes en áreas apropiadas y accediendo solamente a contenido al que están autorizados. Al forzarlos a interactuar con los servidores de la "forma correcta" esta característica evita que hackers creativos ejecuten operaciones inesperadas que puedan ser de riesgo.
- Firewall de Aplicaciones Web: Muchos métodos distintos pueden ser usados por visitantes maliciosos para probar silenciosamente los sitios y aplicaciones en la búsqueda de huecos de seguridad hasta que encuentren una debilidad. Esto evita que los hackers usen inyección SQL o XSS al monitorear su actividad y utilizando patrones para identificar sondas y ataques.
- Protección contra Cookies: Esta protección asegura que los comúnmente utilizados "paquetes de información" entregados a los visitantes por los servidores web no hayan sido alterados. Al ser firmada digitalmente cada cookie, se puede verificar la integridad de la información cuando esta regresa desde el usuario.
- Refuerzo de formularios: Verifica la información enviada a través de formularios por los usuarios que visitan los sitios web. De esta forma, evitamos que los usuarios envíen datos no válidos que pueden dañar los servidores o aprovechar cualquier vulnerabilidad presente.
- Refuerzo de direcciones web: Cuando los servidores web intentan interpretar direcciones web manipuladas, pueden crearse agujeros que sirven para acceder a los servidores. La tecnología de refuerzo de direcciones web controla las solicitudes que los visitantes pueden realizar, restringiéndolas exclusivamente a aquellas que son válidas.

Productos Complementarios

Sophos Mail Archiving

Los servidores de correo electrónico a menudo sufren de la pesada carga del crecimiento del tráfico de emails y los administradores luchan contra mayor demanda de cuotas de correo y capacidad de almacenamiento. A través de Sophos Mail Archiving se puede liberar valiosos recursos del servidor y tomar control de requerimientos de conformidad, al mismo tiempo que incrementa la productividad del usuario final. Todo esto se provee a través de un confiable servicio de hospedaje (hosted service), sin necesidad de hardware o software adicional. Sus características principales son:

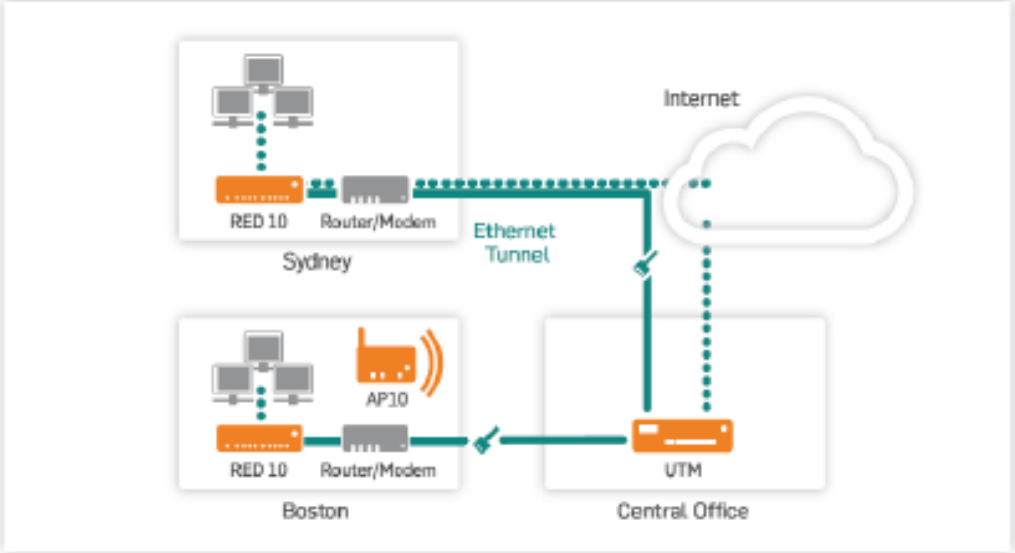
- Fácil Configuración: El configurar una solución de almacenamiento para correo electrónico usualmente toma un considerable tiempo y esfuerzo. Con Sophos Mail Archiving estará listo en minutos en lugar de horas o días.
- Conformidad: Es un hecho que en muchos países lo negocios están obligados a archivar correos electrónicos por muchos años debido a requerimientos legales. El servicio de Sophos Mail Archiving le permite decidir que necesita ser archivado y por cuanto tiempo.
- Descarga del Servidor de Correo: Recupere valiosos recursos de su servidor de mensajería al reducir el almacenamiento ocupado por correos mediante una vía segura y confiable para transferirlos al servicio de hospedaje de archivos.
- Ubicación Instantánea: Los mensajes pueden ser ubicados en segundos sin importar si los elementos de búsqueda son parte del título, cuerpo o adjunto de un correo electrónico.
- Plugin para Outlook: Con Sophos Mail Archiving se puede incrementar la productividad al utilizar complementos integrados de Outlook para búsquedas, sin necesidad de capacitación al usuario final.
- Eliminación de Necesidad de Archivo PST: Las cuotas de buzones de correo a menudo tientan al usuario final a almacenar sus correos en sus PCs particulares como archivos PST. Estos altos riesgos de pérdida de información y manejo ineficiente de los correos electrónicos pueden ser solucionados empezando porque un almacenamiento de correos electrónicos confiable elimina la necesidad de crear archivos PST.

Sophos RED

Sophos RED (Dispositivo Remoto de Ethernet) es la manera más fácil y asequible para dar seguridad a sucursales remotas. Se puede configurar centralizadamente a través de un Sophos UTM ubicado en la matriz el cual automáticamente distribuye la configuración al equipo Sophos RED. Al redireccionar todo el tráfico al Sophos UTM central, el Sophos RED proporciona completa seguridad de UTM aún para las oficinas más pequeñas o remotas. En contraste a equipos de seguridad estándar, Sophos RED no sólo proporciona una seguridad más fuerte, sino que también reduce el costo total de propiedad en un 80% ya que no requiere de conocimientos técnicos o mantenimientos periódicos en el sitio remoto.

- Completa Seguridad UTM: Con Sophos RED no se tiene que hacer compromisos con respecto a la seguridad de sucursales. Hasta las oficinas remotas más pequeñas están totalmente protegidas mediante las suscripciones de Network, Web y Mail del Sophos UMT en su oficina matriz.
- Administración Central Integrada: El Sophos UTM actúa como un controlador de los Sophos RED, administrando centralizadamente todos los equipos Sophos RED a través de un servicio de provisión basado en la nube. La configuración, registro y manejo de problemas se ejecuta completamente desde la matriz. No hay necesidad de administración individualizadas de equipos.
- Cable Virtual Ethernet: El Sohos RED actúa como un puerto de red remota conectado a través de un cable virtual Ethernet a su Sophos UTM. Toda la información transferida está protegida mediante una encriptación muy fuerte.

- Rápido Despliegue: Sophos RED es el primer gateway de seguridad completo que no requiere configuración local o conocimientos técnicos en el sitio remoto. La configuración se realiza en la oficina central y se distribuye automáticamente a todos los equipos Sophos RED. Esto permite despliegues masivos de hasta 100 equipos por día.



Deployment scenario of Sophos RED

Sophos VPN Clients

- El acceso remoto a las redes corporativas es una necesidad cada vez más cotidiana. Si bien Sophos UTM soporta conexiones VPN sin la necesidad de usar un cliente propietario, también ofrece sus alternativas SSL (sin costo) e IPSec (licenciado). Los Sophos VPN Client permiten accesos remotos de forma universal con seguridad, flexibilidad y mínima gestión administrativa. Tienen extensos mecanismos de protección para prevenir ataques en cualquier ambiente de acceso remoto, incluyendo soporte de OTP (One-Time Password tokens) y PKI (Public Key Infrastructure). Adicionalmente el cliente IPSec soporta autenticación vía PSK (Pre-Shared Key), smartcards, tokens y XAUTH.Completa Seguridad UTM: Con Sophos RED no se tiene que hacer compromisos con respecto a la seguridad de sucursales. Hasta las oficinas remotas más pequeñas están totalmente protegidas mediante las suscripciones de Network, Web y Mail del Sophos UTM en su oficina matriz.
- Cliente IPSec de Sophos: Cliente completo y de gran potencia para accesos remotos basados en IPsec desde equipos con sistemas operativos Windows XP, Windows Vista o Windows 7 (compatibilidad con 32 y 64 bits).
- Cliente SSL de Sophos: Cliente de acceso SSL transparente a todas las aplicaciones de la empresa fácil de usar (no se necesita ningún "Webifier"). Instalable en sistemas operativos Windows, Linux, Mac OS y UNIX.
- VPN con un solo clic: Los usuarios pueden descargar e instalar sus propios paquetes de VPN, incluidos el software, los archivos de configuración, las claves y los certificados, desde el portal para usuarios de Sophos UTM con un solo clic del ratón. La instalación completa del equipo cliente se realiza en cuestión de minutos sin que el usuario final necesite realizar ningún tipo de configuración.

Sophos UTM Manager

- Sea que tiene dos Sophos UTM o cientos de ellos, Sophos Command Center (SCC) le permitirá un gran ahorro de tiempo y esfuerzo. Proveedores de servicio y empresas con múltiples instalaciones utilizan el SCC para centralizar sus labores de configuración, mantenimiento, monitoreo y reportes por medio de una única consola web. El SCC permite una visibilidad completa de la infraestructura y de eventos en tiempo real con acceso según distintos perfiles de responsabilidad. Los administradores pueden desplegar actualizaciones, definiciones, reglas, túneles VPN, entre otros, y definir operaciones repetitivas según horarios. ¡Nunca había sido tan fácil manejar instalaciones multi-sitio!
- Monitorización en tiempo real
- Configuración central
- Informes

Certificaciones y Premios

Las soluciones para Internet de Sophos han sido probadas por las más representativas publicaciones de seguridad en la industria. Algunas de ellas son:

SC Magazine – Fabricante del año Mayo 2012

Sophos ganó el premio de Fabricante del Año en la revista SC Magazine Awards 2012 en reconocimiento a su alto nivel de satisfacción del cliente, la innovación constante, la influencia sobre la estrategia de seguridad de TI, y su posición de liderazgo en el mercado de protección de punto final y de datos. El premio fue anunciado en la 11 ª Conferencia Anual de Seguridad AusCERT Información.

CRN Tech Innovator award 2012

CRN reconoce Sophos UTM 9 como el ganador en la categoría Seguridad para el 2012 los premios Tech Innovator.

Sophos a Leader in 2012 Magic Quadrant

Febrero de 2012 - Evaluación basada en la integridad de visión y capacidad de ejecución.

El programa VMware Ready reconoce soluciones que son funcionales y optimizadas para plataformas VMware, y que por lo tanto están listas para ejecutar aplicaciones de misión crítica y operaciones con soporte total de VMware.

ICSA Labs probó y renovó la Certificación de Firewall Certification para la versión actual de Sophos UTM.

Sophos UTM se convirtió en el primer equipo de Administración Unificada de Amenazas (UTM) que recibió la certificación de Common Criteria de la Oficina Federal Alemana para la Seguridad de la Información. Esta certificación asegura a los clientes de los sistemas y procesos de Sophos han sido probados satisfactoriamente por laboratorios acreditados e independientes y que cumplent con estándares de seguridad IT.

InformationWeek - Finalista: Mejor de Interop 2010 (2010/04/16)

Sophos RED fue enunciado como Finalista en Los Premios Lo Mejor de Interop. Los Premios Lo Mejor de Interop Awards reconoce a los expositors que han realizado avances tecnológicos significativos en una categoría especifica

Sophos Receives 5 Star Rating from CRNCRN's 2012 Partner Program Guide

Sophos ofrece a los proveedores de soluciones, la información que necesitan para evaluar a los proveedores que ya trabajan o están considerando trabajar. Sophos recibió una calificación de 5 estrellas en la Guía del Socio Programa 2012.

Ventajas de Sophos UTM – Astaro Sophos Network Security

- Seguridad completa: gama completa de programas de seguridad, incluidos cortafuegos, VPN, prevención de intrusiones, protección del correo electrónico, filtrado web y restricción de aplicaciones.
- Protección en cualquier lugar: protección a los usuarios trabajen desde donde trabajen a través de la red, desde las estaciones de trabajo.
- VPN y Wi-Fi listos para usar: Facilidad de conectar las sucursales y a los usuarios que se desplazan en cuestión de minutos a través de nuestra VPN sin necesidad de configuración y las extensiones inalámbricas.
- El tamaño es lo de menos: Sophos ofrece la protección que necesita en el formato que desee: dispositivo, virtual, software o incluso en la nube.
- El sistema de prevención de intrusiones de Sophos identifica y bloquea las amenazas ocultas en el tráfico entrante, y analiza el tráfico aprobado para proteger la red contra ataques externos.

III. Planes de Soporte

GMS pone a disposición múltiples alternativas de soporte para ajustarse a las necesidades de cada cliente. Nuestro servicio es administrado sobre una herramienta certificada ITIL, lo que permite un óptimo seguimiento de cada requerimiento. Al ser cliente de GMS, automáticamente se obtiene acceso a este sistema, el cual incluye un portal web que permite visualizar el estado actual e histórico de cada ticket de servicio. Los servicios de soporte se prestan bajo modalidad 7x24.

Paquetes de horas prepagadas

Para clientes que requieren mayor flexibilidad en el uso de soporte, ofrecemos la alternativa de prepago de horas. Bajo esta modalidad, se puede contratar el volumen de horas deseadas en incrementos de 5 horas, a la tarifa preferencial de $50,00 cada una. Las horas pueden ser utilizadas en cualquier momento por un año calendario desde la fecha de su compra. En caso de consumir todas las horas disponibles, el cliente deberá contratar un nuevo paquete para mantener su tarifa preferencial o acceder a la tarifa regular de soporte sin plan.

Soporte sin plan

La mayor flexibilidad puede obtenerse al no optar por planes mensuales ni horas prepagadas. Nuestro soporte se mantiene disponible sin necesidad de ningún compromiso por parte del cliente a la tarifa regular de $80,00, aplicada únicamente al utilizar el servicio.

Contabilización de tiempo

- El tiempo de soporte entregado en sitio será contabilizado en incrementos de horas enteras, mientras que el soporte remoto (incluye telefónico) será contabilizado en incrementos de medias horas.
- Se define como horario de oficina el periodo entre las 8:00am y 6:00pm en días laborables. El tiempo de soporte entregado fuera de este horario será multiplicado por un factor de recargo, después de haber contabilizado el tiempo en sus respectivos incrementos. En caso de tener un plan mensual o paquete de horas prepagadas, el recargo será del 50% de tiempo adicional, mientras que si no se tiene plan alguno, el recargo será del 100%.
- Cualquier fracción resultante en los cálculos de tiempos será considerada en incrementos mínimos de media hora.
- No se contabiliza el tiempo de soporte entregado bajo garantía propia del servicio o producto adquirido, bajo las políticas de los fabricantes correspondientes. Tampoco se toma en cuenta el tiempo requerido para recibir e identificar el tipo de solicitud de soporte requerido por el cliente.
- Según las condiciones de compra de los servicios o productos adquiridos, es posible acceder a un cupo de horas. Cualquier contabilización de horas que podrían generar recargos para el cliente será aplicado primero al saldo disponible de dicho cupo.

IV. Propuesta Económica

1. *Licenciamiento Seguridad Perimetral*:

Descripción	1 año	3 años
SOPHOS UTM 320 TOTAL PROTECT **Ethernet interfaces**: 8xGigabit Ethernet **I/O ports**: 2xUSB, 1xCOM (RJ45), 1xVGA **LED display**: Power, HDD **Power supply**: 200W ATX: 100-240V, 50-60Hz, 3-6A **Usuarios**: hasta 200 usuarios *Servicios incluidos:* •***Sophos Network Protection:*** Protección y administración de red con IPS control DoS, Acceso Remoto, balanceo de enlaces WAN, QoS, Registro / Reporte, Administración •***Sophos Web Security:*** Filtrado URL, Protección contra Spyware, Escaneo Antivirus, Filtrado IM/P2P, Reportes de Usuarios. •**Sophos Mail Protection**: filtra el correo electrónico desde y hacia la red contra spam, virus y phishing. Adicionalmente puede permite encriptar el correo e incluye un portal de usuario para facilitar la autogestiónsin sobrecargar el administrador •***Sophos Webserver Protectition:*** Protege servidores de aplicaciones publicados en la web contra ataques avanzados como inyecciones SQL, y Cross Site Scripting. •***Sophos Wireless Protectition:*** Con Acces Points (APS) propietarios, provee administración centralizada y verdadera seguridad a redes inalámbricas. Soporta múltiples SSIDS por equipo, roaming automático entre AP´S encripción avanzada y autenticación fuerte	$ 4.300,00	$ 5.500,00
Instalación y configuración de la consola SOPHOS **Incluye: Aplicar las configuraciones, políticas y aplicaciones de toda la red del cliente.**	$ 800,00	$ 800,00
Capacitación Certificada para 1 persona (Fecha por Conformar) (Opcional)	$ 350,00	$ 350,00
Plan Soporte técnico 10 Horas por un año (Opcional)	$ 500,00	$ 500,00
TOTAL	**$ 5.950,00**	**$ 7.150,00**

Observaciones:

- El costo presentado no incluye el IVA.
- Esta oferta es válida por 30 días
- GMS entregará una cronograma de actividades de implementación, una vez adjudicado
- Tiempo de Entrega 15 días a partir de la firma del contrato.

V. Escalamiento de soporte y recomendaciones

Para asegurar la mejor experiencia de nuestros clientes con las soluciones que ofrecemos, preparamos documentos que explican los contactos y mecanismos de escalamiento de soporte, más las recomendaciones de uso de las herramientas implementadas.

Quito: 399-3000 Guayaquil: 263-0400 Cuenca: 410-3320 Bogotá: +57 1 744 3993

Soporte 24 horas: +593 9 983-9231

soportegms@gms.com.ec

Escalamiento de soporte

Impacto	Tiempo de Atención y Solución en horas*					
	1er Nivel		2do Nivel		3er Nivel / Proveedor	
	Atención	Solución	Atención	Solución	Atención	Solución
Critico	1	4	1	8	1	24
Alto	1	6	1	16	1	48
Medio Alto	2	8	2	36	2	96
Medio	4	16	4	48	4	120
Bajo	8	24	8	72	8	144

Impacto	Descripción
Critico	Afectación completa al cliente
Alto	Afectación a un grupo de cliente
Medio Alto	Afectación a un usuario
Medio	No afecta a usuarios - degradación de servicio
Bajo	No afecta a usuarios - Servicios complementarios

El documento completo de escalamiento será puesto a disposición del cliente a la entrega del servicio.

* Los valores expuestos se aseguran en un 90% de incidentes o requerimientos, en caso de requerir ampliación de estos plazos, esto será debidamente comunicado y acordado con el cliente. Los tiempos se comienzan a contabilizar desde el primer contacto efectivo con el Centro de Soporte de GMS.

VI. Anexo: Descripción de los Módulos

Essential Firewall
Un firewall de protección básica.

El producto incluye:

- **Networking**
  - Internet Router
  - Bridging
  - DNS server & proxy
  - DynDNS
  - DHCP server & relay
  - NTP support
  - automatic QoS
- **Network Security**
  - Stateful Packet Inspection Firewall & Network Address translation (DNAT/SNAT/Masquerading)
- **Remote Access**
  - : PPTP and L2TP over IPSec support (including iPhone support)
- **Logging/Reporting**
  - Full logging on local hard drive
  - Searching
  - Real-time reports for hardware
  - Network usage and network security
  - Daily executive reports
- **Management**
  - Web-based GUI in local languages
  - Setup wizard
  - Configuration backup & restore
  - Administrator notifications
  - SNMP support
  - Centralized management via Sophos UTM Manager

Network Protection
Un firewall avanzado que proporciona la mejor protección de seguridad.

El producto incluye:

- **Firewall**
  - Stateful Packet Filter
  - Security Proxies to Simplify Management
    - HTTP/S, FTP, FTP-over-HTTP, POP3, SMTP, DNS, Socks, Ident , NTP, generic
    - Transparent mode eases administration
  - Application-Level Deep Packet Filtering
    - Scans packet payloads to enforce protocol-specific rules
  - Flexible Rules Management
    - Can include hosts, networks, groups or vpn users
    - Automatic rule generation for application proxies and internal services
    - Time-based activation
    - Policy-based routing
    - Interface based rules
  - Network Address Translation
    - SNAT/DNAT
    - Masquerading

- **Intrusion Prevention**
  - Identifies and Blocks Application and Protocol Related Probes and Attacks through Deep Packet Inspection
  - Database of over 8,000 Patterns and Rules Including:
    - Probing, port scans, interrogations, host sweeps
    - Attacks on application vulnerabilities
    - Protocol exploitations
  - Intrusion Detection and Prevention

        - Notify administrator and/or block traffic immediately
    - Powerful Management Interface
        - One click to enable or disable complete rule sets e.g. for email- or webservers

- **DoS Protection**
    - DoS and DDoS (Distributed Denial of Service) / Flooding Protection
        - TCP SYN Flood Protection
        - UDP Flood Protection
        - ICMP Flood Protection
        - Based on Source and/or Destination IP Address
        - Adjustable maximum allowed packet rates
        - Adjustable logging level
    - Port-Scan Protection
        - Log, drop or reject detected port scan traffic
        - Adjustable logging level

- **Bandwidth Control**
    - Outbound Dynamic Bandwidth Reservation (Guaranteed Minimum, Maximum Limit) Based on:
        - Source/destination server or network
        - Service/Port
        - TOS/DSCP bits
        - Pre-defined traffic selectors for IM/P2P applications
    - Inbound Queuing Optimization via:
        - Stochastic Fairness Queuing (SFQ)
        - Random Early Detection (RED)
        - Proportional bandwidth shaping
        - Dynamically adapts amount of reserved bandwidth to available link speeds
    - Download Equalizer
        - Intelligently drops downlink packets to avoid network congestion
    - Upload Optimizer
        - Accelerates TCP handshake packets (SYN, ACK, ...)

- **Branch Office VPN**
    - Supports IPsec and SSL Protocols
        - IPSec offers high interoperability with other devices
        - SSL allows for easy setup between two Sophos UTM devices
        - Star, hub-and-spoke and fully meshed configurations
        - Nat-Traversal for establishing tunnels between NAT devices
    - Supports all Major Encryption and Many Authentication Methods
        - DES, 3DES, AES, Serpent, Blowfish, Twofish
        - MD5, SHA-1
        - XAUTH allows for integration of One-Time-Password systems
    - Full Public Key Infrastructure (PKI) Support
        - Via Internal or external certificate authority

- **SSL Remote Access**
    - Fully Transparent Access to Network Resources without Requiring any "Webifier" for Each Application
    - SSL encryption and Authentication Methods:
        - DES, AES (up to 256 bts)
        - MD5, SHA-1
    - Supports Feature Rich SSL VPN Clients:
        - Free Sophos SSL VPN Client (based on OpenVPN Client that runs on Windows, Linux, MacOSX,and many UNIX operating systems)
    - One-Click-Configuration via Sophos's UserPortal:
        - Download of SSL client software, configuration files, keys and certificates with a single mouse click
        - Automated installation and configuration of SSL client software within minutes
    - Automatic Split Tunneling
    - Automatic Network Configuration Update
    - IP Address Assignment via Virtual IP Pool
    - VPN Traffic Compression

VI. Anexo: Descripción de los Módulos

- **IPSec Remote Access**
  - Support of all Major IPSec Encryption and Many Authentication Methods:
    - DES, 3DES, AES, Serpent, Blowfish, Twofish
    - MD5, SHA-1
    - XAUTH allows for integration of One-Time-Password systems
  - Supported IPSec Clients:
    - Sophos Secure Client with integrated desktop firewall (runs on Windows XP, Windows Vista and Windows 7 based PCs)
    - Cisco IPSec client
  - One-Click-Configuration via Sophos's UserPortal:
    - Download of Sophos Secure Client software, configuration files, keys and certificates with a single mouse click
    - Automated installation and configuration of Sophos Secure Client software within minutes

- **Native Windows Remote Access**
  - PPTP (Point-To-Point Tunneling Protocol)
    - Supports strong encryption (128 bit)
    - Local or RADIUS based user authentication
    - Authentication protocols: MSCHAPv2
    - IP Address assignment via pool network or DHCP server
    - Supports native Windows and Apple iPhone client
  - L2TP (Layer-2-Tunneling Protocol) over IPSec
    - Authentication via pre-shared key or X.509 certificate
    - Local or RADIUS based user authentication
    - Authentication protocols: PAP, CHAP, MSCHAP, MSCHAPv2
    - IP Address assignment via pool network or DHCP server
    - Supports native Windows and Apple iPhone client

- **Directory Authentication**
  - Comprehensive Authentication Methods:
    - Active Directory
    - eDirectory
    - Radius
    - Tacacs+
    - LDAP Local
  - Single Sign-On (SSO) Support for Transparent Authentication:
    - Active Directory
    - eDirectory
  - Other Highlights:
    - Point & Click User Definitions via Graphical eDirectory and Active Directory Browsers
    - Automatic User Creation and Synchronization
    - User Pre-fetch at Configurable Intervals
    - Easy Server Connection Testing via "TEST" Button
    - Supports Windows Server 2008 Native Mode

- **UserPortal**
  - SMTP / POP3 Mail Quarantine
    - Search, view, release, download, delete and whitelist spam mails in your personalized quarantine
  - Individual Mail Log
    - Gain a quick overview over your complete email traffic
  - Personal Whitelist
    - Manage your personal email whitelist of sender addresses which should not be subject to spam scans
  - POP3 Account Management
    - Redirect POP3 email accounts through the Sophos UTM to take advantage of spam and virus scanning

- Remote Access Package Download including VPN Client Software, Config Files and Certificates for:
  - L2TP, PPTP, SSL, IPSec
- Comprehensive Language Support
  - Available in 15 local languages
  - Customizable HTML welcome page

Web Protection
Protege y dirige a los usuarios a medida que trabajan en línea.

El producto incluye:

- **URL Filtering**
  - Comprehensive Up-to-Date Database with 35+ Million Websites Covering over 3.9 Billion Web Pages in 96 Categories:
    - Nudity, gambling, criminal activities, shopping, drugs, job search, sports, entertainment, etc.
    - Additional categories can be created for individual customization
    - International content from hundreds of countries in 65 languages
    - Re-categorization via online form
  - Fast Response Times through Globally Distributed Database Replications
  - Filter Might also Consider Global Reputation
  - Whitelists and Blacklists to Tailor Access for Groups of Users
  - Many User Authentication Options
    - IP Address, Active Directory SSO, eDirectory SSO, LDAP, RADIUS/TACACS+
    - Time-based access policies

- **Spyware Protection**
  - Blocks (Unintentional) Downloads of Spyware, Adware, and Other Malicious Software
  - Prevents Infected Systems from Sending Information Back to the Spyware (Home) Servers
  - Checks Against a Database of Known Spyware URLs
  - Filters and Removes Active Content Such as Java, Active X, Flash, Cookies, VBScript or JavaScript

- **Antivirus Scanning**
  - Dual Independent Virus Scanners with Multiple Detection Methods
    - Virus signatures
    - Heuristic analysis
  - Scans HTTP, HTTPS, FTP, SMTP and POP3 Traffic
  - Scans Encrypted SMTP Traffic
  - Huge Signature Database
    - More than 800,000 virus signatures
    - Frequent automatic updates
  - Flexible Management
    - Can specify file formats (endings) and content (MIME type) to block
    - Emails and attachments can be dropped, rejected with message to sender, passed with a warning, or quarantined

- **IM/P2P Filtering**
  - Manages the Use of Instant Messaging Clients:
    - AOL IM, ICQ, MSN Messenger, Yahoo! Messenger, IRC, Google Talk/Jabber, Tencent QQ, Skype
  - Manages the Use of Peer-to-Peer Applications:
    - Applejuice, Ares, Bittorrent, Direct Connect, Edonkey, Gnutella, IMesh, MUTE, Manolito, Pando, Share, WinMX, Winny
  - Provides Flexible Control
    - Depending on application the administrator can decide to either allow or block it completely, block file transfers only or just log its usage
    - Specific users/IP addresses can be excluded from general rules
    - Specific hosts and networks can be excluded from IM/P2P control
  - Granular Bandwidth Control
    - Define max. allowed bandwidth per application

VI. Anexo: Descripción de los Módulos

- **User Reporting**
  - Inline Reports
    - Offer up-to-date statistical information for each security application, like Top Domains/Users by traffic or time spend, top email senders/receivers or top blocked attacks
  - Reporting Graphs
    - Provide RRD style flow graphs with daily, weekly, monthly and yearly statistics about hardware components such as CPU, RAM, and hard disk usage, IPS activity, and web usage by IP address or user name
  - Executive Reports
    - Includes a summary as well as mayn details about TOP-10 statistics taken from Inline reports and reporting graphs for over 60 areas
    - Can be generated at will and also emailed out to a list of users (e.g. admin and/or CEO) on configurable schedules
  - Report Anonymization
    - Hides user names and addresses within reports
    - Uses 4-eyes-principle to unhide selected names

    - Customizable html welcome page

VII. Alcance soporte Sophos UTM

Alcance soporte Sophos UTM			
Evento	**Con costo/o se descuenta de las horas de soporte**	**Sin costo/ sin descuento de las horas de soporte**	**Horas aproximadas de soporte**
Reinstalación por:			
Cambio de servidor	X		1
Problemas con el servidor (Appliance UTM)		X	1
Problemas con el servidor (Hardware del cliente)	X		1
Problemas del S.O. *		X	1
Reconfiguración del servidor *	X		1
Configuración de políticas (Network Protection)	X		1
Configuración de políticas (Web Protection)	X		1
Configuración de políticas (Mail Protection)	X		1
Configuración de Wireless Protection	X		1
Instalación de APs adicionales	X		1
Configuración del Webserver Protection	X		1
Configuración Alta Disponibilidad	X		1
Configuración Endpoint Protection	X		1
Configuración de Multipath (Redundancia de internet)	X		1
Revisión y auditoria de configuraciones *	X		2
Problemas de configuraciones *		X	2
Análisis de reportes	X		1
Actualizaciones			
Nuevas versiones	X		2
Nuevos parches		X	1
Capacitación			
Inducción de temas específicos	X		4
Inducción general (Personal nuevo, fuera del contrato)	X		2

Oferta de Kaspersky Endpoint Security For Business Select / Advanced

Preparada para:

COLEGIO EXPERIMENTAL JUAN PIO MONTUFAR

Junio, 2014

Quito, 26 de Junio de 2014

Ingeniero
Alexis Paspuel
Ing. Sistemas Colegio Experimental Juan Pío Montufar
COLEGIO EXPERIMENTAL
JUAN PIO MONTUFAR
Quito - Ecuador

Estimado Ingeniero:

GMS agradece la oportunidad de presentarle esta oferta de soluciones informáticas. Somos una empresa de consultoría de TI con más de 30 años de experiencia, durante los cuales hemos podido atender a muchas de las compañías más importantes de la región. Nuestras soluciones cubren las más altas exigencias de nuestros clientes, y nos caracterizamos por cumplir proyectos de alta complejidad. Asumimos el papel de socio estratégico para establecer relaciones exitosas a largo plazo.

Esperamos que esta propuesta sea de su conveniencia y quedo a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Atentamente,

Leonardo Peña
Asesor Comercial
leonardo.pena@gms.com.ec
Oficina: +593 2 399-3000 ext. 7513
Celular: 095 8788506
www.gms.com.ec
Quito – Guayaquil – Cuenca – Bogotá

1. Información sobre GMS

Perfil empresarial

Fundada en 1978, GMS es una de las empresas de consultoría informática de mayor trayectoria en la región. Nuestra misión es potenciar la habilidad empresarial de nuestros clientes hacia la excelencia, a través de tecnología de vanguardia, sistemas y servicios de alta calidad. Medimos nuestros resultados según los que obtienen nuestros clientes, ya que nos consideramos sus socios de negocio para asegurar el mejor retorno sobre las inversiones que realizan con nosotros.

Nuestro principal diferenciador es nuestro personal, y definimos nuestra identidad de ***genteinteligente*** a base de los equipos de trabajo que formamos con nuestros clientes. Profesionales altamente capacitados de GMS participan de la mano con sus contrapartes en las empresas que apoyamos para entender a fondo sus requerimientos y definir las soluciones más inteligentes a cada entorno particular. Esta cooperación es la base sobre la cual construimos relaciones a largo plazo que permiten lograr los mejores resultados.

A partir de nuestro personal, hemos formado un portafolio de productos y servicios que nos permite ofrecer soluciones integradas de seguridad informática, telecomunicaciones, administración de infraestructura TI y cloud services. Estas soluciones se complementan con servicios de consultoría en estrategias y normas de TI y seguridad, y servicios de desarrollo de aplicaciones. Con nuestro apoyo, su empresa puede dejar en el pasado preocupaciones como incompatibilidad entre herramientas o rendición de cuentas con diversos proveedores que no logran responsabilizarse de la operación global de su red empresarial.

Datos de la Empresa:

- Razón Social: Grupo Microsistemas Jovichsa SA
- RUC: 1790590542001
- Dirección: Av. Amazonas N42-88 y Tomás de Berlanga
- Teléfono: 399 3000

Sistemas de gestión

Para asegurar los niveles de servicio que requieren las empresas más exigentes, GMS opera con un sistema de gestión ITIL para el control de actividades y requerimientos. En el mismo, hemos habilitado un portal web que permite a nuestros clientes revisar el historial de los trabajos realizados para ellos, ingresar nuevas solicitudes, y hacer un seguimiento sobre el avance de las mismas. El sistema también permite registrar los niveles de satisfacción ante los soportes entregados, con lo cual mantenemos un control para asegurar un mejoramiento continuo.

Todos nuestros servicios cuentan con esquemas de escalamiento. Estos aseguran redundancia en canales de comunicación para que los clientes puedan aprovechar del soporte 7x24 ofrecido por GMS. Adicionalmente establecen tiempos de respuesta para distintos tipos de requerimientos, incluyendo los mecanismos de apoyo por parte de fabricantes internacionales, según el caso. La combinación de estos elementos permite a GMS otorgar niveles de atención y apoyo que marcan la diferencia.

Clientes destacados

Nuestro mayor logro ha sido conseguir y mantener la confianza de nuestros clientes. Más de 2.000 empresas han decidido trabajar con GMS. Entre algunas que lideran sus respectivos sectores se encuentran las siguientes:

Sector Financiero:

- Aseguradora del Sur
- Asociación de Bancos Privados del Ecuador
- Banco Amazonas
- Banco de Loja
- Banco del Austro
- Banco del Pacífico
- Banco Internacional
- Banco Territorial
- Cooperativa de Ahorro y Crédito Ejército Nacional
- Cooperativa de Ahorro y Crédito San Francisco
- Cooperativa Juventud Ecuatoriana Progresista
- Helm Bank
- Raul Coka Barriga Seguros
- ZHM Seguros y Reaseguros

Manufactura y Consumo Masivo:

- Chalde & Chalde
- DANEC
- Endesa / Grupo Durini
- Industrias Ales
- INGESA
- La Fabril
- LEVAPAN
- Manufacturas Americanas
- Mercantil Garzozi & Garbu
- Neyplex
- Novopan / Pelikano
- Plásticos Ecuatorianos
- REYBANPAC
- ZaiMella

Educación:

- Colegio Tomás Moro
- Escuela Politécnica del Ejército
- Escuela Politécnica Nacional
- Universidad Católica Santiago de Guayaquil
- Universidad de las Américas
- Universidad de Milagro – UNEMI
- Universidad Estatal de Bolívar
- Universidad San Francisco de Quito
- Universidad Tecnológica Equinoccial

Gobierno:

- Armada del Ecuador
- Consorcio Nacional de Telecomunicaciones - CNT
- Fuerza Aérea del Ecuador
- H. Consejo Provincial del Guayas
- H. Consejo Provincial de Pichincha
- Instituto Ecuatoriano de Seguridad Social
- Ministerio de Coordinación de Desarrollo Social
- Ministerio de Relaciones Exteriores
- Servicio de Rentas Internas

Servicios:

- Adecco
- AviancaTaca / Aerogal
- Cobiscorp
- Ernst & Young
- INMEDICAL
- Hospital Metropolitano
- Hotel Howard Johnson
- Multitrabajos.com
- Pérez Bustamante y Ponce
- Ils Servilogistics
- Junta de Beneficencia de Guayaquil
- Transoceánica

Medios de Comunicación y Publicidad:

- Canal 1
- Diario EL UNIVERSO
- Cybergulas (guiatelefonica.com.ec)
- EDIMPRES (Diario Hoy, TV Hoy, Newsweek)
- Editores Nacionales (Vistazo, América Economía, etc.)
- Impulso Comunicadores (Ecuadorinmediato.com)
- Gráficos Nacionales (Diario Extra)
- Induvallas
- Grupo EL COMERCIO
- Grupo K
- Rivas Herrera Young & Rubicam
- Sonorama

Energía y Petróleos:

- CELEC
- CNEL
- Compañía de Petróleos de los Ríos - Petroríos
- Consejo Nacional de Electricidad
- Empresa Eléctrica Regional Centro Sur
- Empresa Eléctrica de Riobamba
- EP Petroecuador
- Grupo Azul
- Lutexsa Industrial – TERPEL
- Operaciones Río Napo
- P & S – Petróleos y Servicios
- SERTECPET
- SINOPEC International Petroleum Service Ecuador
- Sipetrol

Comercialización:

- Almacenes La Ganga
- Autolasa
- Comercial JAHER
- Comercial Kywi
- Consorcio NOBIS
- Distribuidora Farmacéutica - DIFARE
- Firmesa Industrial
- Grupo KFC
- Marcimex
- Motransa – Mitsubishi
- IIASA Caterpillar
- Juan Marcet
- Tiendas Industriales Asociadas - TIA
- Toyota del Ecuador

Servicios y Soluciones

En un entorno empresarial cada día más interconectado, se ha vuelto indispensable asegurar una correcta integración entre los componentes que sustentan la información de su negocio: telecomunicaciones, seguridad informática y aplicaciones. GMS ofrece experiencia y soluciones del más alto nivel en cada una de estas áreas, para asegurar a su empresa la correcta coordinación y óptimo funcionamiento de las mismas.

Consultoría

Las decisiones de inversión en soluciones informáticas deben basarse en una visión clara de los problemas, sus impactos y sus soluciones, para así asegurar que generen un retorno para la empresa. GMS puede ayudar a lograr este objetivo a través de servicios de consultoría, sea esta en relación a procesos TICS, seguridades o infraestructura.

Consultoría

Áreas de competencia en procesos TICS:
Estrategia de servicios basada en Buenas Prácticas ITIL
Alineación de TICS con estrategias corporativas
Definición de proyectos y construcción de mapas de ruta
Definición de políticas de buen uso de TICS

Áreas de competencia en seguridades:
Sistemas de Gestión de Seguridad de Información (SGSI), incluyendo ISO 27000
Clasificación de información
Continuidad de negocio
Ethical Hacking

Áreas de competencia en infraestructura:
Auditoría de hardware y software
Optimización de uso de recursos tecnológicos (ej. ancho de banda)
Análisis de retorno sobre la inversión (ROI) en proyectos de infraestructura

Seguridad Informática

La evolución de amenazas informáticas exige cubrir cada vez más frentes, sean capas de infraestructura dentro de nuestra red o dispositivos fuera de ella. Ofrecemos una amplia gama de soluciones especializadas para que su organización no sea vulnerada por el eslabón más débil de la seguridad:

Astaro hoy forma parte de Sophos, una de las empresas más grandes de seguridad informática a nivel mundial con más de 25 años de experiencia y aproximadamente 2.000 empleados. Astaro (Sophos UTM) protege a más de 100.000 redes, sean de PYMES, gobiernos, multinacionales o TELCOS, con una solución robusta e integral para la seguridad perimetral. Sophos UTM cuenta con diversas certificaciones y reconocimientos, incluyendo la distinción como líder en el Cuadrante Mágico de Gartner de soluciones UTM.

DigitalStakeout ofrece servicios de ciberinteligencia que permiten proteger su red institucional o corporativa y salvaguardar su reputación en línea. Con el monitoreo de reputación y tráfico de miles de millones de IP's a nivel mundial, DigitalStakeout puede identificar la fuente y naturaleza de amenazas que afectan a su red. Sus motores de escaneo de redes sociales y sitios de phishing pueden ayudarle a asegurar que su identidad en Internet no sea vulnerada.

Kaspersky Lab es uno de los líderes mundiales en seguridad interna, especialista en tecnología antimalware. Fundada en Moscú en 1997, hoy protege a más de 300 millones de usuarios por todo el mundo. Su tecnología es regularmente premiada por analistas y publicaciones de renombre como Virus Bulletin, ICSA Labs, AV Comparatives (el cual le otorgó el premio de Antivirus del Año 2011), y Gartner, quien considera a Kaspersky Lab entre los líderes de su cuadrante de proveedores antimalware.

Qualys es el líder mundial en soluciones de gestión de vulnerabilidades y compliance, reconocido como tal por múltiples analistas incluyendo Gartner. Sus soluciones están en uso por miles de empresas en cerca de 100 países, incluyendo más de la mitad de las empresas en el Forbes Global 100. Su tecnología permite escanear vulnerabilidades en IP's internas, IP's externas y aplicaciones web, además de realizar escaneos de cumplimiento de políticas, incluyendo normas internacionales como PCI.

Safend, empresa especializada en soluciones DLP (prevención de fugas de información), fue fundada en Israel en el año 2003, y ahora es subsidiaria de Wave Systems, empresa líder en seguridad basada en hardware. Sus soluciones se destacan por su facilidad de uso y permiten inspeccionar el contenido del tráfico en un endpoint para asegurar su cumplimiento con políticas granulares de control de confidencialidad, además de manejar la encripción de datos y el uso de puertos, medios removibles y conexiones inalámbricas.

Transecq es una empresa que ha liderado la innovación en soluciones de seguridad móvil para bancos, operadoras móviles, instituciones de salud, entre otras. Ofrece una plataforma segura sobre la cual se pueden activar módulos tales como autenticación de doble factor o banca móvil. La tecnología de Transecq (en proceso de patente global), permite identificar al usuario y su teléfono inteligente de forma única, con comunicación cifrada sobre plataforma de datos, lo cual da un nivel de seguridad previamente inalcanzable en el ámbito móvil.

Telecomunicaciones

GMS es el primer pionero en servicio de Internet Seguro y enlaces de datos con las seguridades más desarrolladas del país. Esto permite a su empresa tener un acceso protegido contra hackers, virus, spam, entre otros, lo cual además optimiza su tráfico. Adicionalmente ofrecemos equipos y servicios de telepresencia, ideales para maximizar las ventajas que su empresa recibe de las telecomunicaciones contratadas.

La experiencia de GMS en el manejo de redes, seguridades y aplicaciones nos permite asesorar a su empresa para la puesta en marcha del mejor esquema de conectividad. Con alianzas estratégicas con múltiples carriers, podemos lograr las combinaciones óptimas en costo y tecnología para beneficio de su compañía. Adicionalmente proveemos soluciones que le permiten acceder a esquemas muy eficientes de alta disponibilidad.

Vidyo, Inc. es una empresa con soluciones revolucionarias de videoconferencia y telepresencia. Considerado por analistas como alterador de las reglas de juego de la industria, Vidyo no solo ofrece su propia gama de equipos, sino también soluciones basadas en software que permiten a los clientes aprovechar su infraestructura existente. Fue fundada en EEUU en el año 2004 por expertos pioneros en tecnologías de videoconferencia.

Administración de Infraestructura TI

Las inversiones en TICS son significativas y es necesario maximizar su retorno por medio de una acertada administración. GMS ofrece soluciones de fabricantes especializados, sea en modalidad de compra de las mismas o por medio de servicios gerenciados / outsourcing.

Allot Communications es un proveedor líder de soluciones inteligentes de optimización IP, tanto para empresas como para operadores móviles e ISP's. Fundada en 1996 con origen en Israel, hoy cuenta con oficinas en 14 países y clientes alrededor de todo el mundo. Su tecnología propietaria DART para la administración dinámica de ancho de banda permite visibilidad y administración total sobre aplicación, usuario y topología.

Aranda Software Corp. ofrece soluciones de administración de infraestructura TI que permiten aplicar las mejores prácticas de gestión ITIL. Es uno de los contados fabricantes a nivel mundial que cuenta una plataforma de Service Desk con más de 10 procesos certificados ITIL por Pink Elephant. La misma se integra con su producto de Asset Management para una administración unificada.

Desarrollo de software

Sea que requiera servicios o herramientas, GMS puede aportar mucho a los proyectos de desarrollo de aplicaciones en su empresa o institución.

Con un equipo humano con estándares elevados, metodologías formales en las fases de análisis, diseño, programación, pruebas e implementación, y el uso de herramientas avanzadas, GMS es su socio ideal para enfrentar su próximo proyecto. Sea el desarrollo de su nuevo sistema back-office, la creación de un portal de reportes, o simplemente un servicio de acompañamiento, GMS puede marcar la diferencia.

GeneXus es la primera herramienta inteligente para crear, desarrollar y mantener en forma automática aplicaciones multiplataforma. Con GX, las puede adaptar fácilmente a los cambios del negocio y las nuevas posibilidades brindadas por la evolución tecnológica. GX es producto de la empresa Uruguaya Artech, fundada en 1988 con oficinas en Brasil, México, Japón y China para soportar a miles de clientes a nivel mundial.

Cloud Services

El avance del cloud computing es una tendencia inevitable y GMS puede ayudar a su empresa a aprovecharla.

GMS ofrece infraestructura en nubes locales que le permite a su empresa o institución ganar economías de escala y optimizar los costos de propiedad de equipamiento propio, sin la incomodidad de ceder control a un tercero distante. Si requiere proveer servicios vía Internet a sus clientes, también podemos apoyarle para habilitar su propia nube para ellos, siempre con el respaldo que permite nuestra experiencia en seguridad TI.

Reconocimientos

Gracias al compromiso con nuestros clientes, el nivel de nuestras soluciones, y nuestros sistemas de gestión, GMS ha logrado reconocimientos internacionales que son motivo de gran orgullo para nosotros. Entre ellos, se destacan los siguientes:

- **Kaspersky Lab**
  2007: Partner del Año, Latinoamérica
  2008: Spirit of Kaspersky
  2009: Partner del Año, Latinoamérica
  2010: Partner del Año, Latinoamérica
  2010-2011: Consejo Consultivo de Partners
  2011: Number 1 Club
  2011: Partner del Año (Enterprise), Mercados Emergentes (Latinoamérica + África + Medio Oriente + Europa del Este)

- **Astaro / Sophos**
  2010: Partner del Año, Sudamérica Hispana
  2011: Partner del Año (Sophos UTM), Latinoamérica

- **Asociación Brasilera de Calidad (ABIQUA)**
  2010: Premio Panamericano de Calidad 2010

2. Información sobre soluciones ofertadas

1. Kaspersky

Kaspersky es una solución de seguridad TI de clase mundial que ofrece a su negocio un nuevo nivel de protección contra malware y otras amenazas. Mantenga la información sensible del negocio intacta, e incremente su productividad con menos esfuerzo y tiempo administrativo. Su diseño por capas permite cubrir cualquier tipo de dispositivo de red de una forma flexible a los requerimientos del cliente. Todo el tráfico entrante y saliente de estaciones de trabajo, teléfonos inteligentes, servidores y gateways, puede ser revisado contra contenido malicioso. Las soluciones de Kaspersky proveen lo último en rendimiento confiable y efectivo, con implementación sencilla, interfaz amigable y herramientas administrativas eficientes, para que su empresa pueda obtener los mejores resultados en protección antimalware.

Perfil empresarial

Kaspersky Lab es la empresa de soluciones antimalware de mayor crecimiento en el mundo. Desde su fundación en Moscú en 1997, ha crecido a ser una organización con más de 1.500 especialistas altamente calificados, con oficinas regionales para las Américas, Asia-Pacífico, Japón, Europa Occidental, y Europa Oriental / Medio Oriente / África. Sus operaciones abarcan más de 100 países, protegiendo a más de 250 millones de usuarios.

Kaspersky Lab es respetado por su innovación: fue el primero en ofrecer soluciones completas para las plataformas Linux, Unix y Netware; lidera el desarrollo de análisis heurístico de siguiente generación; es el más rápido en responder a nuevas amenazas; todo esto respaldado por múltiples patentes tecnológicas.

En Ecuador, Kaspersky Lab ha mantenido representación directa desde el año 2006. Su crecimiento ha sido extraordinario gracias a la calidad de sus soluciones y del soporte local. Actualmente Kaspersky protege a más de 2.000 empresas y 200.000 usuarios, incluyendo muchas de las organizaciones más grandes del país, tanto en el sector público como privado.

Entre múltiples certificaciones y reconocimientos que tiene el producto, se destacan las de analistas de virus como ICSA Labs, West Coast Labs, VB100, y AV Comparatives; publicaciones como SC Magazine, PC World, Computer Shopper, Computer Idea; y plataformas como Windows XP, Windows 7, SUSE y Red Hat.

Ventajas principales de Kaspersky

En la actualidad, Kaspersky Total Security for Business ofrece la más completa plataforma de protección y gestión del sector. Total Security for Business protege exhaustivamente la red y dispone de potentes herramientas de configuración para garantizar la productividad de los usuarios y la ausencia de amenazas del malware con independencia del dispositivo que utilicen o de su ubicación.

Kaspersky integro en su nueva plataforma potentes funciones empresariales en todos los niveles de protección, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

Una única consola de gestión
A través de un único "panel de control", el administrador puede ver y gestionar todo el sistema de seguridad: equipos virtuales y dispositivos tanto físicos como móviles.

Una única plataforma de seguridad
Kaspersky Lab ha desarrollado la consola, módulos de seguridad y herramientas de forma interna en lugar de adquirirlos de otras empresas.
Eso significa que los programadores que trabajan en el mismo código base han desarrollado tecnologías que interactúan entre sí y funcionan de forma conjunta. Esto se traduce en estabilidad, políticas integradas, generación de informes útiles y herramientas intuitivas.

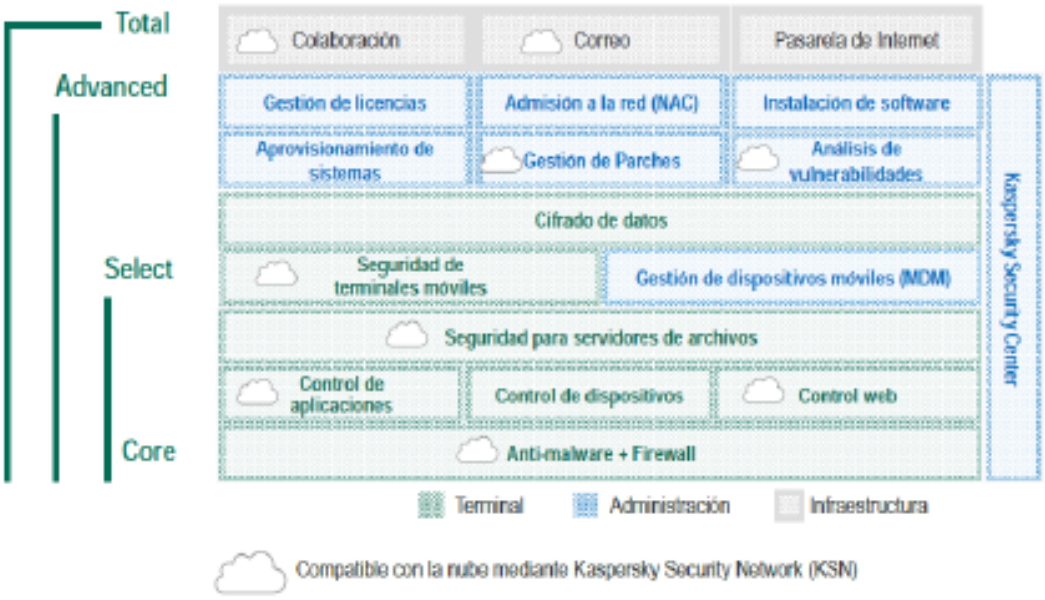
Un único costo
Todas las herramientas provienen de un único proveedor y se proporcionan mediante una única instalación, para que no tengas que pasar por un nuevo proceso de presupuestación y justificación para alinear tus riesgos de seguridad con tus objetivos empresariales.

La nueva plataforma de Kaspersky End Point Security for Business Incluye:

- Funciones de Seguridad Movil
- Protección para End Points
- Seguridad Web, para Colaboración y Correo
- Control de Endpoints
- Cifrado y Protección de Datos
- Configuración de sistema y Gestión de Parches

Kaspesky End Point Security for Business

Niveles progresivos con un gran número de características



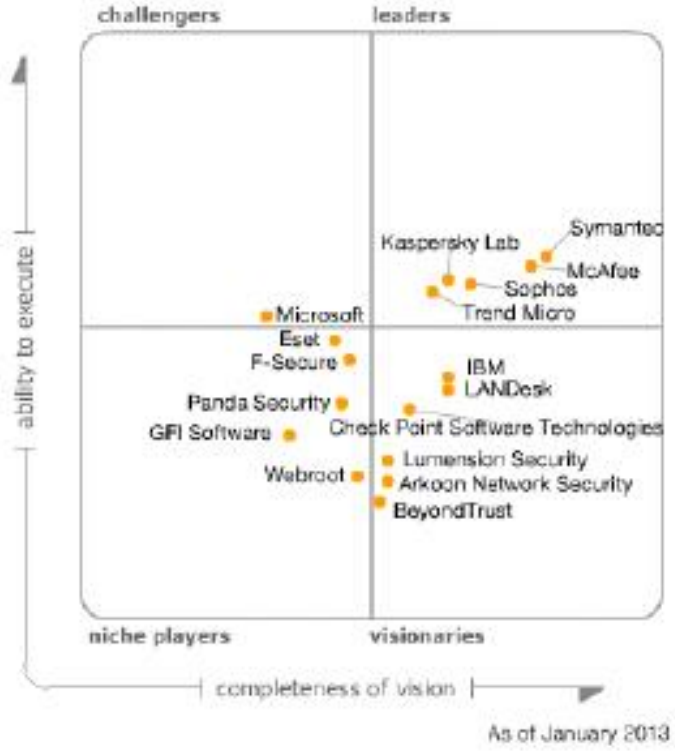
Soluciones adaptadas adiciones:
- Servidores de archivos
- Gestión de sistemas
- Almacenamiento
- Correo
- Móvil
- Virtualización
- Colaboración
- Pasarelas de Internet

Comparativos de analistas

- Gartner ubica a Kaspersky como líder en su cuadrante mágico de protección endpoint en el 2013

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Por qué Kaspersky para su negocio?

GALARDONADO ANTI-MALWARE

KASPERSKY INSIDE

Más de 80 proveedores de TI, seguridad de redes y comunicaciones han elegido incorporar la tecnología anti-malware de Kaspersky Lab dentro de sus propias soluciones, incluyendo Microsoft, IBM, Checkpoint y Juniper.

- AV Comparatives, Diciembre 2012, resultados de pruebas de detección total de amenazas: Kaspersky Lab obtuvo la calificación "TOP RATED" .

A continuación se detalla las conclusiones de los comparativos realizados durante el de 2012:

	File Detection Test March 2012	Proactive Test March 2012	Performance Test (Suite) May 2012	Real-World Test (March-June 2012)	Anti-Phishing test July 2012	File Detection test September 2012	Performance Test (AV) October 2012	Malware Removal Test October 2012	Real-World Test (August-November 2012)
Bitdefender	***	***	***	***	***	***	**	***	***
Kaspersky	***	***	***	***	***	***	**	***	***
F-Secure	***	***	***	***	***	***	**	**	**
AVIRA	***	***	***	**	**	***	**	**	**
BullGuard	***	***	**	**	***	***	*	**	***
ESET	***	***	***	**	*	**	***	**	**
G DATA	***	***	**	***	**	**	*	**	***
avast!	***	***	***	*	**	***	***	*	**
Panda	***	***	***	**		**	**	***	*
eScan	***	***	**	**	*	***	**		*
Sophos	***		***	*	***	**	**		*
Qihoo 360	*	*	***	***	*	tested	**		***
PC Tools	*	*	*	**	***	*	*	**	*
McAfee	**		**	*	***	***	**		tested
AVG	*	**	***	**	*	*	**	*	*
Trend Micro	*		**	*	***	***	*		**
Tencent QQ	**	**	***	*		***			**
Fortinet	**	*	*	tested	*	***	*	**	tested
GFI Vipre	*	*	**	*	*	**	*	**	tested
Webroot	*		***	tested	***	tested	***		tested
Microsoft	*	***				*	***		
AhnLab	tested	tested	**	tested		tested			tested

- West Coast Labs: Kaspersky Lab es actualmente uno de seis fabricantes que tiene la certificación "Checkmark Platinum".

- Kaspersky Lab ganó el premio VB100 por octava vez, complementando su certificación con Spam + Verified.

3. Planes de Soporte

GMS pone a disposición múltiples alternativas de soporte para ajustarse a las necesidades de cada cliente. Nuestro servicio es administrado sobre una herramienta certificada ITIL, lo que permite un óptimo seguimiento de cada requerimiento. Al ser cliente de GMS, automáticamente se obtiene acceso a este sistema, el cual incluye un portal web que permite visualizar el estado actual e histórico de cada ticket de servicio. Los servicios de soporte se prestan bajo modalidad 7x24.

Paquetes de horas prepagadas

Para clientes que requieren mayor flexibilidad en el uso de soporte, ofrecemos la alternativa de prepago de horas. Bajo esta modalidad, se puede contratar el volumen de horas deseadas en incrementos de 5 horas, a la tarifa preferencial de $50,00 cada una. Las horas pueden ser utilizadas en cualquier momento por un año calendario desde la fecha de su compra. En caso de consumir todas las horas disponibles, el cliente deberá contratar un nuevo paquete para mantener su tarifa preferencial o acceder a la tarifa regular de soporte sin plan.

Soporte sin plan

La mayor flexibilidad puede obtenerse al no optar por planes mensuales ni horas prepagadas. Nuestro soporte se mantiene disponible sin necesidad de ningún compromiso por parte del cliente a la tarifa regular de $80,00, aplicada únicamente al utilizar el servicio.

Contabilización de tiempo

- El tiempo de soporte entregado en sitio será contabilizado en incrementos de horas enteras, mientras que el soporte remoto (incluye telefónico) será contabilizado en incrementos de medias horas.

- Se define como horario de oficina el periodo entre las 8:00am y 6:00pm en días laborables. El tiempo de soporte entregado fuera de este horario será multiplicado por un factor de recargo, después de haber contabilizado el tiempo en sus respectivos incrementos. En caso de tener un plan mensual o paquete de horas prepagadas, el recargo será del 50% de tiempo adicional, mientras que si no se tiene plan alguno, el recargo será del 100%.

- Cualquier fracción resultante en los cálculos de tiempos será considerada en incrementos mínimos de media hora.

- No se contabiliza el tiempo de soporte entregado bajo garantía propia del servicio o producto adquirido, bajo las políticas de los fabricantes correspondientes. Tampoco se toma en cuenta el tiempo requerido para recibir e identificar el tipo de solicitud de soporte requerido por el cliente.

- Según las condiciones de compra de los servicios o productos adquiridos, es posible acceder a un cupo de horas. Cualquier contabilización de horas que podrían generar recargos para el cliente será aplicado primero al saldo disponible de dicho cupo.

4. Propuesta Económica

1. Licenciamiento de Kaspersky Capa Select:

Descripción	1 años	2 años	3 años
KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT 275 Licencias para protección de estaciones de trabajo, Servidores de Archivos, Móviles *El servicio incluye:* • Exploración de Antivirus para contenido del disco • Protección por ataques desde la red • Protección proactiva sobre las aplicaciones de Microsoft Office • Antihacker • Antispyware • Intercepción de virus de escritura • Actualización permanente y automática de firmas de virus • Consolas de administración centralizada para equipos dentro de la red • Administración de control de aplicaciones • Control Web • Manejo y administración de Móviles	$ 18,00	$ 26,00	$ 33,00
Total licenciamiento (275 Nodos)	$ 4.950,00	$ 7.150,00	$ 9.075,00
Instalación y configuración de la consola	Incluye	Incluye	Incluye
Capacitación durante la instalación	Incluye	Incluye	Incluye
Plan Soporte técnico 10 Horas (Opcional)	$ 500,00	$ 500,00	$ 500,00
TOTAL	**$ 5.450,00**	**$ 7.650,00**	**$ 9.575,00**

Observaciones:

- Los precios no incluyen IVA
- El precio ofertado incluye el número de consolas adicionales que el cliente desee sin costo adicional.

2. Licenciamiento de Kaspersky Capa Advanced:

Descripción	1 año	2 años	3 años
KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED 275 Licencias para protección de estaciones de trabajo, Servidores de Archivos, Móviles *El servicio incluye:* • Exploración de Antivirus para contenido del disco • Protección por ataques desde la red • Protección proactiva sobre las aplicaciones de Microsoft Office • Antihacker • Antispyware • Intercepción de virus de escritura • Actualización permanente y automática de firmas de virus • Consolas de administración centralizada para equipos dentro de la red • Administración de control de aplicaciones • Control Web • Manejo y administración de Móviles • Protección de Datos (encriptación) • Scan de Vulnerabilidades • Administración de parches • NAC • Software de instalación	$ 24,00	$ 34,00	$ 44,00
Total licenciamiento (275 Nodos)	$ 6.600,00	$ 9.350,00	$ 12.100,00
Instalación y configuración de consola	Incluye	Incluye	Incluye
Capacitación durante la instalación	Incluye	Incluye	Incluye
Plan Soporte técnico 10 Horas por un año (Opcional)	$ 500,00	$ 500,00	$ 500,00
TOTAL	**$ 7.100,00**	**$ 9.850,00**	**$ 12.600,00**

Observaciones:

- Los precios no incluyen IVA
- El precio ofertado incluye el número de consolas adicionales que el cliente desee sin costo adicional.

5. Escalamiento de soporte y recomendaciones

Para asegurar la mejor experiencia de nuestros clientes con las soluciones que ofrecemos, preparamos documentos que explican los contactos y mecanismos de escalamiento de soporte, más las recomendaciones de uso de las herramientas implementadas.

Quito: 399-3000 Guayaquil: 263-0400 Cuenca: 410-3320 Bogotá: +57 1 744 3993

Soporte 24 horas: +593 9 983-9231

soportegms@gms.com.ec

Escalamiento de soporte

Impacto	Tiempo de Atención y Solución en horas*					
	1er Nivel		2do Nivel		3er Nivel / Proveedor	
	Atención	Solución	Atención	Solución	Atención	Solución
Critico	1	4	1	8	1	24
Alto	1	6	1	16	1	48
Medio Alto	2	8	2	36	2	96
Medio	4	16	4	48	4	120
Bajo	8	24	8	72	8	144

Impacto	Descripción
Critico	Afectación completa al cliente
Alto	Afectación a un grupo de cliente
Medio Alto	Afectación a un usuario
Medio	No afecta a usuarios - degradación de servicio
Bajo	No afecta a usuarios - Servicios complementarios

El documento completo de escalamiento será puesto a disposición del cliente a la entrega del servicio.

* Los valores expuestos se aseguran en un 90% de incidentes o requerimientos, en caso de requerir ampliación de estos plazos, esto será debidamente comunicado y acordado con el cliente. Los tiempos se comienzan a contabilizar desde el primer contacto efectivo con el Centro de Soporte de GMS.

6. Requerimientos para la instalación

Estaciones de trabajo

- Estaciones de trabajo Windows
- Estaciones de trabajo Linux
- Estaciones de trabajo Mac

Servidores de archivos

- Servidores de archivos Windows
- Windows Server Enterprise Edition
- Servidores de archivos Linux
- Servidores de archivos para Novell Netware
- Servidores de archivos for Storage

Dispositivos móviles

- Kaspersky Tablet Security
- Kaspersky Mobile Security (Android)
- Kaspersky Mobile Security 9.0 (Symbian)
- Kaspersky Mobile Security 9.0 (WinMobile)
- Kaspersky Mobile Security 9.0 (BlackBerry)
- Kaspersky Password Manager 5.0

Kaspersky KryptoStorage**Administración**

- Administration Kit (Security Center)

Servidores de correo y Colaboración

- Kaspersky Security 8.0 for MS Exchange Server
- Kaspersky Security 5.5 for MS Exchange Server
- Kaspersky Security 8.0 for SharePoint Server
- Kaspersky Security 8.0 for Linux Mail Server
- Kaspersky Anti-Spam 3.0
- Kaspersky Anti-Virus 5.6 for Linux Mail Servers
- Kaspersky Mail Gateway 5.6
- Kaspersky Anti-Virus 8.0 for Lotus Domino

Gateways de Internet

- Kaspersky Anti-Virus 8.5 for MS ISA Server &
- Forefront TMG Standard Edition
- Kaspersky Anti-Virus 8.0 for MS ISA Server &
- Forefront TMG Standard Edition
- Kaspersky Anti-Virus 5.5 for Proxy Server

Anexo 1

7. Alcance del Soporte

	Alcance soporte Kaspersky		
Evento	**Con costo/o se descuenta de las horas de soporte**	**Sin costo/ sin descuento de las horas de soporte**	**Horas aproximadas de soporte**
Formateo del servidor	X		2
Problemas en el Sistema Operativo	X		2
Problemas consola no se conecta		X	3
Cambio de servidor de administración	X		1
Configuración de políticas	X		2
Configuración de tareas	X		1
Revisión y diagnóstico de informes	X		1
Despliegue de licencias		X	1
Revisión de eventos críticos		X	1
Problemas con actualizaciones			
Por inconvenientes con el canal de internet	X		2
Por inconvenientes con tareas de la consola		X	2
Estación de trabajo			
Reinstalación de antivirus por:			
Formateo del equipo	X		1
Problemas con el sistema operativo	X		1
Problemas desconocidos en el momento de la instalación		X	1
Pantalla azul		X	1
Malware *			
Revisión de muestras enviadas por el cliente		X	1
Toma de muestras		X	1
Capacitación			
Inducción de temas especializados	X		2
Inducción general de la consola	X		4
Inducción general de políticas de estaciones de trabajo	X		4
Inducción de proceso de instalación	X		4

* Con la toma de muestras de malware, generalmente se envía documentación de captura, o captura remota. En caso de que no pueda ser posible la captura, se realiza soporte remoto o se procederá con soporte presencial.

ANEXO F

Software para Administra redes de datos		
	WhatsUp Gold	**Axence NetTools Pro 4.8**
Características Principales	Monitorización de la 2 y 3 capa de red	Monitorización de la disponibilidad de hosts.
	Monitorización completa de todos los equipos conectados a la red	Visualización de todos los paquetes entrantes y salientes de la red
	Trabaja con el protocolo SNMP (V1, V2 y V3) para cualquier dispositivo que lo soporte	
	Reportes Predefinidos Sobre el Rendimiento del Sistema, Utilizando Contadores de WMI (Para redes Windows)	Escaneo de la red para descubrir todos los nodos que tiene la red
	Monitores y Reportes de Rendimiento Personalizados, Utilizando Cualquier Contador WMI	Crea una lista exhaustiva de información del sistema de computadoras con el sistema operativo Windows: detallando todos los procesos y servicios que se encuentran ejecutando, registro, eventos, discos, memoria ,etc.
	Adicione MIBs con simples “Drag-and-Drop”	Despliegue de la información local de un determinado host.
	Monitoreo de Contenido Web (HTTPS/HTTP)	TCP/IP WorkShop
	Monitoreo de ancho de banda de routers y análisis de tendencias	Escáner excautivo de la red
	Gestión de recursos /Reportes de buscador de direcciones MAC	Tiene alertas para indicar si un host no está trabajando adecuadamente
	Suite integrada de herramientas para la base de datos del WhatsUp	
	Asignación de recursos mediante priorización.	SNMP Browser y otras herramientas para lanzar Trazas, Pings, entre otros
	Solución de problemas en base a gráficos en tiempo real	

Tabla Comparación de herramientas de administración de red

ANEXO G

Antivirus Empresarial			
Versión	**Panda Security For Business**	**Kaspersky Enterprise Space Security.**	**Symantec™ Protection Suite Small Business Edition**
Características	Máximo nivel de protección frente amenazas sobre virus, gusanos, troyanos, Spyware, adware, rootkits, y phishing, incluyendo protección para ficheros y correo electrónico, descargas HTTP/FTP y mensajería instantánea. Protección optimizada para todos los EndPoints de la empresa. Provee bloque preventivo. Gestión centralizada y sencilla mediante la utilización de la herramienta AdminSecure. Optimización de recursos Reportes en tiempo real. Auditoría bajo demanda.	Protección anti-virus para nodos clave de la red: estaciones de trabajo, laptops, servidores de archivo y smartphones Un nuevo motor anti-virus que asegura el uso óptimo de los recursos Protección proactiva mejorada para estaciones de trabajo y servidores de archivo contra nuevos programas maliciosos Escaneo “sobre la marcha” de correos electrónicos y de tráfico de Internet Firewall personal para protección en cualquier tipo de red, incluyendo WiFi Protección local contra correos electrónicos no deseados y contra phishing Previene filtro de información de smartphones extraviados Protección para servidores de archivo que ejecutan Windows, Linux y Novell NetWare	Efectiva Protección contra virus, malware, apyware, spam y nuevas amenazas. Protección de estaciones de trabajo, mail, servidores y sistema de recuperación. Protección integrada. Seguridad Centralizada Seguridad más acelerada y efectiva recomendada para pequeñas y medianas empresas. Bloquea el 99% de Spam y protege el correo electrónico en Exchange Fácil administración optimizando optimizados. Además, Identificación y control del flujo de información

Componentes	Panda AdminSecure Panda security for desktops Panda security For File Servers Panda security ComandLine	Protección exhaustiva para servidores de terminales y para grupos de servidores Balanceo de carga de procesamientos del servidor Protección anti-virus para servidores de correo electrónico Sendmail, qmail, Postfix y Exim Escaneo de mensajes, bases de datos y otros objetos en servidores Lotus Notes/Domino Escaneo de todos los mensajes en servidores Microsoft Exchange, incluyendo carpetas públicas Bloquea envíos masivos de correos y epidemias de malware Soporte completo para sistemas de 64-bit	
		Exploración de Antivirus para contenido del disco Protección por ataques desde la red Protección proactiva sobre las aplicaciones de Microsoft Office Antihacker Antispam para cada máquina Antispyware Intercepción de virus de escritura Actualización permanente y automática de firmas de virus (hasta 3 veces al día)	Servidores y estaciones de trabajo. Servidor de administración de Endpoint Protection Small Business Edition. Mail Security para Exchange. Backup Exec System Recovery Desktop

		1 Consola de administración centralizada para equipos dentro de la red Soporte técnico 24x7x365	

Tabla Comparación de Antivirus empresariales

ANEXO H

DAP-2360

Key Features

For Business-Class Environments

- 2.4Ghz 802.11n Connectivity for Increased Network Capacity
- White Rugged Metal Plenum-rated Chassis
- Up to 26dbm High Power radio design
- Ideal for Indoor Deployments[1]
- Limited Lifetime Warranty[3]

Multiple Operation Modes

- Access Point
- Wireless Distribution System (WDS) /Bridge
- Point-to-Point
- Point-to-Multiple-Points
- WDS with AP
- Wireless Client

High Performance Connectivity

- IEEE 802.11n Wireless
- Up to 300Mbps[2]

Trusted Security Features

- WPA2™ - Enterprise/Personal
- WPA™ - Enterprise/Personal
- WPA2 - PSK/AES over WDS
- 64/128-bit WEP Encryption
- MAC Address Filtering
- NAP

Convenient Installation

- Supports 802.3af Power over Ethernet
- Wall Mounting Brackets Included

Easy Management

- Web Browser (HTTP) & HTTPS
- Telnet
- SNMP v1, v2c, and v3
- AP Manager II
- SSH
- D-View® 6.0
- AP Array

business

AirPremier® N PoE Access Point with Plenum-rated Chassis

Overview

The DAP-2360 is an 802.11n Plenum Rated PoE Access Point ideal for any network administrator to create or expand the capacity of their wireless network. This is especially applicable to wireless networks in high traffic areas such as airports, coffee shops, shopping centers, sporting venues, and campus deployments. At transfer rates of up to 300Mbps in the 2.4GHz frequency range, users are able to connect with legacy 802.11b/g adapters as well as the latest 802.11n adapters to enjoy faster downloads and instant communication.

Versatile Access Point

The DAP-2360 allows network administrators to deploy a highly manageable and extremely robust 802.11n wireless network. The included antennas are detachable and provide optimal wireless coverage in the 2.4GHz (802.11g and 802.11n) band using a high power single radio design to reduce dead spots and increase capacity. Enclosed in a white plenum-rated metal chassis, the DAP-2360 color allows the access point to easily blend into ceilings or walls and adheres to strict fire codes for placement in air passageways. For advanced installations, this high-speed Access Point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available.

Enhanced Performance

The DAP-2360 delivers reliable wireless performance with maximum wireless signal rates of up to 300Mbps[2] in the 2.4GHz wireless band. This, coupled with support for Wi-Fi Multimedia™ (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications. Additionally, the DAP-2360 supports load balancing features to ensure maximum performance by limiting the maximum number of users per Access Point.

Security

To help maintain a secure wireless network, the DAP-2360 provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server backend. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

The DAP-2360 includes support for up to 8 VLANs for implementing multiple SSIDs to further help segment users on the network. It also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

Multiple Operation Modes

To maximize total return on investment, the DAP-2360 can be configured to optimize network performance based on any one of its multiple operation modes: Access Point, Wireless Distribution System (WDS) with Access Point, WDS/Bridge (No AP Broadcasting) and Wireless Client. With WDS support, network administrators can set up multiple DAP-2360s throughout a facility and configure them to bridge with one another while also providing network access to individual clients. Also included are advanced features such as Load Balancing, which optimizes high network traffic volume, and redundancy for fail-safe wireless connectivity. Additionally, the DAP-2360 offers Spanning Tree Protocol support for greater efficiency and to avoid broadcast storms when used in WDS mode.

Network Management

Network administrators have multiple options for managing the DAP-2360 including Web (HTTP), Secure Sockets Later (SSL, which provides for a secure

D-Link®

connection to the Internet), Secure Shell (SSH, which provides for a secure channel between local and remote computers), and Telnet (bi-directional, eight-bit byte oriented communications facility). For advanced network management, administrators can use the D-Link AP Manager II or D-View management module to configure and manage multiple access points from a single location. In addition to a streamlined management process, the AP Manager II or D-View software provides network administrators with the means of verifying and conducting regular maintenance checks remotely, eliminating the need to send personnel out to physically verify proper operation. With 2.4GHz band functionality, PoE support, a plenum-rated chassis, extensive manageability, versatile operation modes, and solid security enhancements, the D-Link AirPremier N PoE Access Point (DAP-2360) provides SMB environments with a business-class solution for deploying a wireless network in the workplace.

Technical Specifications

Standards	• IEEE 802.11n • IEEE 802.11g • IEEE 802.3ab	• IEEE 802.3af • IEEE 802.3u • IEEE 802.3
Network Management	• Telnet - Secure (SSH) Telnet • Web Browser interface • HTTP - Secure HTTP (HTTPS) • SNMP Support	• D-View Module - Private MIB • AP Manager II • AP Array
Security	• WPA™-Personal • WPA-Enterprise • WPA2™-Personal • WPA2-Enterprise	• 64/128-bit WEP • SSID Broadcast Disable • MAC Address Access Control • Rogue AP Detection
VLAN/SSID Support	• 802.1q/Multiple SSID support up to 8	
Quality of Service (QoS)	• 4 Priority Queues • WMM Wireless Priority	
Wireless Frequency Range	• 2.4GHz to 2.4835GHz	
Operating Modes	• Access Point (AP) • WDS with AP	• WDS/Bridge (No AP Broadcast) • Wireless Client
Dipole Antenna Gain	• 5 dBi @ 2.4 GHz	
Maximum Transmit Output Power	• 26 dBm @ 2.4 GHz Dual Chain	
LEDs	• Power • LAN	• 2.4GHz
Maximum Power Consumption	• 9 Watts with PoE • 8 Watts without PoE	
Operating Voltage	• 48VDC +/- 10% for PoE or 5V/2.5A	
Temperature	• Operating: 32°F to 104°F (0°C to 40°C) • Storing: -4°F to 149°F (-20°C to 65°C)	
Humidity	• Operating: 10% ~ 90% (Non-condensing) • Storing: 5% ~ 95% (Non-condensing)	
Certifications	• FCC class B • IC	• UL 2043 • WiFi®
Weight	• 1.69 lb (768g)	
Dimensions (WxHxD)	• 6.5" x 7.4" x 1.5" (166mm x 188mm x 37mm)	
Warranty	• Limited Lifetime[3]	

[1] This unit is designed for indoor environments, you might violate local regulatory requirements by setting up this unit in outdoor environments.
[2] Maximum wireless signal rate derived from IEEE Standard 802.11g, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.
[3] Limited Lifetime warranty available only in the USA and Canada.

All references to speed and range are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

Updated 10-21-10

business

For more information
D-Link Systems | 17595 Mt. Herrmann Street | Fountain Valley, CA 92708 | 800.326.1688 | dlink.com

©2010 D-Link Corporation/D-Link Systems, Inc. All rights reserved.
D-Link, the D-Link logo and AirPremier are registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners. Visit www.dlink.com for more details.

D-Link®

D-Link®

DFL-260/860/1660/2560/2560G

NETDEFEND

INTEGRATED FIREWALL/VPN

- Powerful Firewall Engine
- Virtual Private Network (VPN) Security
- Granular Bandwidth Management
- 802.1Q VLAN Tagging
- D-Link End-to-End Security Solution (E2ES) Integration with ZoneDefense

ADVANCED FUNCTIONS

- Stateful Packet Inspection (SPI)
- Detect/Drop Intruding Packets
- Server Load Balancing
- Policy-Based Routing

UNIFIED THREAT MANAGEMENT

- Intrusion Prevention System (IPS)
- Antivirus (AV) Protection
- Web Content Filtering (WCF)
- Optional Service Subscriptions

VIRTUAL PRIVATE NETWORK (VPN)

- IPSec NAT Traversal
- VPN Hub and Spoke
- IPSec, PPTP, L2TP
- DES, 3DES, AES, Twofish, Blowfish, CAST-128 Encryption
- Automated Key Management via IKE/ISAKMP
- Aggressive/Main/Quick Negotiation

ENHANCED NETWORK SERVICES

- DHCP Server/Client/Relay
- IGMP V3
- H.323 NAT Traversal
- Robust Application Security for ALGs
- OSPF Dynamic Routing Protocol
- Run-Time Web-Based Authentication

NetDefend UTM Firewall Series

Today's continuously shifting security environment presents a challenge for small/home office networks with limited IT capabilities. Fortunately, the D-Link NetDefend Unified Threat Management (UTM) firewalls provide a powerful security solution to protect business networks from a wide variety of threats. UTM Firewalls offer a comprehensive defense against virus attacks, unauthorized intrusions, and harmful content, successfully enhancing fundamental capabilities for managing, monitoring, and maintaining a healthy network.

Enterprise-Class Firewall Security

NetDefend UTM Firewalls provide complete advanced security features to manage, monitor, and maintain a healthy and secure network. Network management features include: Remote Management, Bandwidth Control Policies, URL Black/White Lists, Access Policies and SNMP. For network monitoring, these firewalls support e-mail alerts, system logs, consistency checks and real-time statistics.

Unified Threat Management

NetDefend UTM Firewalls integrate an intrusion detection and prevention system, gateway antivirus, and content filtering for superior Layer 7 content inspection protection. An acceleration engine increases throughput, while the real-time update service keeps the IPS information, antivirus signatures, and URL databases current. Combined, these enhancements help to protect the office network from application exploits, network worms, malicious code attacks, and provide everything a business needs to safely manage employee Internet access.

Powerful VPN Performance

NetDefend UTM Firewalls offer an integrated VPN Client and Server. This allows remote offices to securely connect to a head office or a trusted partner network. Mobile users working from home or remote locations can also safely connect to the office network to access company data and e-mail. NetDefend UTM Firewalls have hardware-based VPN engines to support and manage a large number of VPN configurations. They support IPSec, PPTP, and L2TP protocols in Client/Server mode and can handle pass-through traffic as well. Advanced VPN configuration options include: DES/3DES/AES/Twofish/Blowfish/CAST-128 encryption, Manual or IKE/ISAKMP key management, Quick/Main/Aggressive Negotiation modes, and VPN authentication support using either an external RADIUS server or a large user database.

D-Link®

DFL-260/860/1660/2560/2560G

PERFORMANCE OPTIMIZATION

- UTM Acceleration Engine
- Multiple WAN Interfaces for Traffic Load Sharing

DFL-260

- Firewall Throughput: 80Mbps
- VPN Performance: 25Mbps (3DES/AES)
- 1 10/100 Ethernet WAN Ports
- 4 10/100 Ethernet LAN Ports
- 1 10/100 Ethernet DMZ Port

DFL-860

- Firewall Throughput: 150Mbps
- VPN Performance: 50Mbps (3DES/AES)
- 2 10/100 Ethernet WAN Ports
- 7 10/100 Ethernet LAN Ports
- 1 10/100 Ethernet DMZ Port

DFL-1660

- Firewall Throughput: 1.2Gbps
- VPN Performance: 350Mbps (3DES/AES)
- 6 Configurable Gigabit Ethernet Ports

DFL-2560(G)

- Firewall Throughput: 2Gbps
- VPN Performance: 1Gbps (3DES/AES)
- 10 Configurable Gigabit Ethernet Ports
- 4 SFP Ports (DFL-2560G)

NetDefend UTM Firewall Series

UTM Services

Maintaining an effective defense against the various threats originating from the Internet requires that all three databases used by the NetDefend UTM Firewalls are kept up-to-date. In order to provide a robust defense, D-Link offers optional NetDefend Firewall UTM Service subscriptions which include updates for each aspect of defense: Intrusion Prevention Systems (IPS), Antivirus and Web Content Filtering (WCF). NetDefend UTM Subscriptions ensure that each of the firewall's service databases are complete and effective.

Robust Intrusion Prevention

The NetDefend UTM Firewalls employ component-based signatures, a unique IPS technology which recognizes and protects against all varieties of known and unknown attacks. This system can address all critical aspects of an attack or potential attack including payload, NOP sled, infection, and exploits. In terms of signature coverage, the IPS database includes attack information and data from a global attack sensor-grid and exploits collected from public sites such as the National Vulnerability Database and Bugtrax. The NetDefend UTM Firewalls constantly create and optimize NetDefend signatures via the D-Link Auto-Signature Sensor System without overloading existing security appliances. These signatures ensure a high ratio of detection accuracy and a low ratio of false positives.

Stream-Based Virus Scanning

The NetDefend UTM Firewalls examine files of any size, using a stream-based virus scanning technology which eliminates the need to cache incoming files. This zero-cache scanning method not only increases inspection performance but also reduces network bottlenecks. NetDefend UTM firewalls use virus signatures from Kaspersky Labs to provide systems with reliable and accurate antivirus protection, as well as prompt signature updates. Consequentially, viruses and malware can be effectively blocked before they reach the network's desktops or mobile devices.

Web Content Filtering

Web Content Filtering helps administrators monitor, manage, and control employee usage of and access to the Internet. The NetDefend UTM Firewalls implement multiple global index servers with millions of URLs and real-time website data to enhance performance capacity and maximize service availability. These firewalls use highly granular policies and explicit black/white lists to control access to certain types of websites for any combination of users, interfaces and IP networks. The firewall can actively handle Internet content by stripping potential malicious objects, such as Java Applets, JavaScripts/VBScripts, ActiveX objects, and cookies.

NetDefend UTM Subscription

The standard NetDefend UTM Subscription provides your firewall with UTM service updates for 12 months starting from the day you activate or extend your service. The NetDefend UTM Subscription can be renewed regularly to provide your firewalls with the most up-to-date security service available from D-Link.

NetDefend Center: http://security.dlink.com.tw

NetDefend UTM Firewall Series

Powerful VPN Engine

Hardware-based data encryption and authentication for IPSec, PPTP, and L2TP in Client/Server mode enable fast and safe handling of VPN traffic.

Professional Intrusion Prevention System (IPS)

Automatic updates from a comprehensive IPS signature database focus on attack payloads to protect the network against zero-day attacks.

Real-Time Antivirus Inspection (AV)

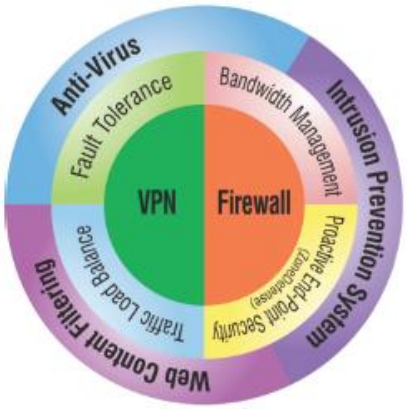
The antivirus engine scans using the most complete, most up-to-date antivirus signature database. Streaming-based pattern matching provides the effective protection against viruses.

Fast, Efficient Web Content Filtering

Multiple index server implementation, highly granular policies, black lists and active content handling enhance performance and effectiveness of web surfing control.

Acceleration Engine for Unified Threat Management

A powerful processor allows the firewall to carry out IPS and Antivirus scanning simultaneously without performance degradation.



Licensed for Unlimited Users

Optional subscription services for IPS, Antivirus Scanning, and Web Content Filtering are priced per firewall rather than per user, thus reducing the total cost of ownership for licensing.

WAN Link Load-Balancing and Fault-Tolerance

Multiple WAN ports support traffic load balancing and failover, thus guaranteeing Internet availability and bandwidth.

D-Link End-to-End Security (E2ES) Solution

The ZoneDefense mechanism operating in conjunction with D-Link xStack switches automatically quarantines infected workstations and prevents them from flooding the internal network with malicious traffic.

dlink™ green

D-Link Green Certified

The DFL-1660 and DFL-2560(G) have attained D-Link Green Certification. These firewalls are built with an 80 PLUS internal power supply. 80 PLUS certified power supplies offer increased reliability due to greater efficiency, and provide a reduced cost of ownership through longer equipment life. Additionally, 80 PLUS power supplies help to prevent pollution by limiting energy consumption, and run at a lower temperature to reduce cooling costs.

D-Link Green certified devices comply with RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) directives. RoHS directives restrict the use of specific hazardous materials during manufacturing, while WEEE implements standards for proper recycling and disposal. Together, these considerations make D-Link Green firewall products the environmentally responsible choice.

D-Link®

DFL-260/860/1660/2560/2560G

Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Interfaces	Ethernet	1 10/100 WAN Port 1 10/100 DMZ Port 4 10/100 LAN Ports	2 10/100 WAN Ports 1 10/100 DMZ Port 7 10/100 LAN Ports	6 Configurable Gigabit Ports	10 Configurable Gigabit Ports
	SFP	–	–	–	4 SFP Ports (DFL-2560G only)
	USB	–	–	2 USB Ports (reserved)	2 USB Ports (reserved)
	Console	1 DB-9 RS-232	1 DB-9 RS-232	1 DB-9 RS-232	1 DB-9 RS-232
System Performance[1]	Firewall Throughput[2]	80Mbps	150Mbps	1.2Gbps	2Gbps
	VPN Throughput[3]	25Mbps	50Mbps	350Mbps	1Gbps
	IPS Throughput[4]	20	40	400Mbps	600Mbps
	Antivirus Throughput[4]	10	20	225Mbps	450Mbps
	Concurrent Sessions	12,000	25,000	600,000	1,500,000
	Policies	500	1,000	4,000	6,000
Firewall System	Transparent Mode	✓	✓	✓	✓
	NAT, PAT	✓	✓	✓	✓
	Dynamic Routing Protocol	–	OSPF		
	H.323 NAT Traversal	✓	✓	✓	✓
	Time-Scheduled Policies	✓	✓	✓	✓
	Application Layer Gateway	✓	✓	✓	✓
	Proactive End-Point Security	–	ZoneDefense		
Networking	DHCP Server/Client	✓	✓	✓	✓
	DHCP Relay	✓	✓	✓	✓
	Policy-Based Routing	✓	✓	✓	✓
	IEEE 802.1q VLAN	8	16	1024	2048
	IP Multicast	IGMP v3			
Virtual Private Network (VPN)	Encryption Methods (DES/ 3DES/ AES/ Twofish/ Blowfish/ CAST-128)	✓	✓	✓	✓
	Dedicated VPN Tunnels	100	300	2,500	5,000
	PPTP/L2TP Server	✓	✓	✓	✓
	Hub and Spoke	✓	✓	✓	✓
	IPSec NAT Traversal	✓	✓	✓	✓

D-Link®

DFL-260/860/1660/2560/2560G

Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Traffic Load Balancing	Outbound Load Balancing	✓	✓	✓	✓
	Server Load Balancing	–	✓	✓	✓
	Outbound Load Balance Algorithms	Round-robin, Weight-based Round-robin, Destination-based, Spill-over			
	Traffic Redirect at Fail-Over	✓	✓	✓	✓
Bandwidth Management	Policy-Based Traffic Shaping	✓	✓	✓	✓
	Guaranteed Bandwidth	✓	✓	✓	✓
	Maximum Bandwidth	✓	✓	✓	✓
	Priority Bandwidth	✓	✓	✓	✓
	Dynamic Bandwidth Balancing	✓	✓	✓	✓
High Availability (HA)	WAN Fail-Over	✓	✓	✓	✓
	Active-Passive Mode	–	–	✓	✓
	Device Failure Detection	–	–	✓	✓
	Link Failure Detection	–	–	✓	✓
	FW/VPN Session SYN	–	–	✓	✓
Intrusion Detection & Prevention System (IDP/IPS)	Automatic Pattern Update	✓	✓	✓	✓
	DoS, DDoS Protection	✓	✓	✓	✓
	Attack Alarm via E-mail	✓	✓	✓	✓
	Advanced IDP/IPS Subscription	✓	✓	✓	✓
	IP Blacklist by Threshold or IDP/IPS	–	✓	✓	✓
Content Filtering	HTTP Type	URL Blacklist/Whitelist			
	Script Type	Java, Cookie, ActiveX, VB			
	E-mail Type	E-mail Blacklist/Whitelist			
	External Database Content Filtering	✓	✓	✓	✓

D-Link®

DFL-260/860/1660/2560/2560G

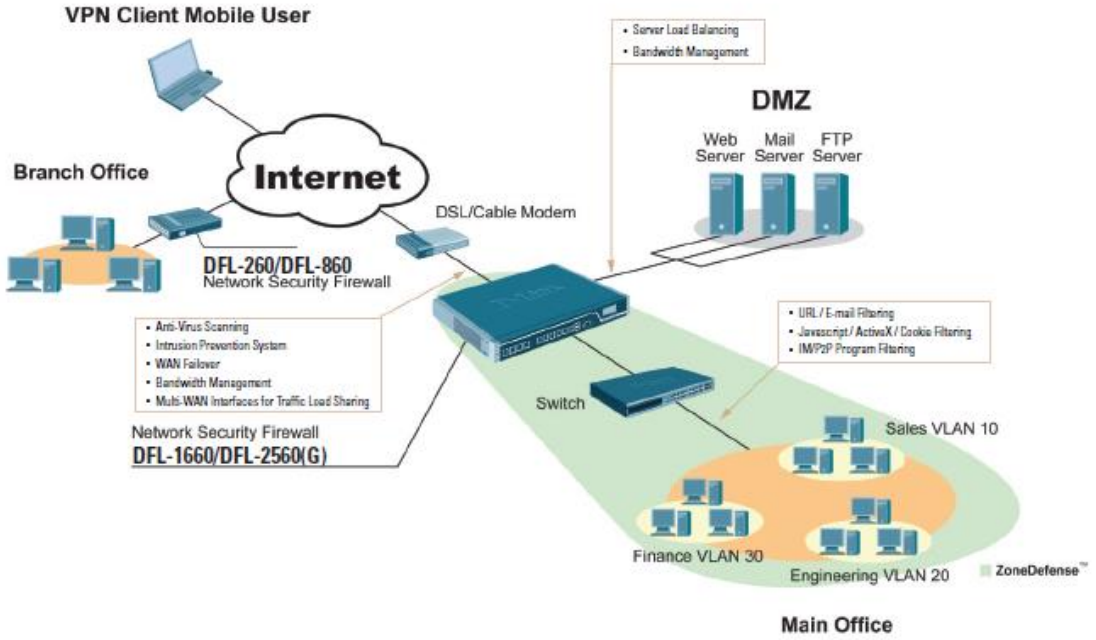
Technical Specifications		DFL-260	DFL-860	DFL-1660	DFL-2560(G)
Antivirus	Real Time AV Scanning	✓	✓	✓	✓
	Unlimited File Size	✓	✓	✓	✓
	Scans VPN Tunnels	✓	✓	✓	✓
	Supports Compressed Files	✓	✓	✓	✓
	Signature Licensor	Kaspersky			
	Automatic Pattern Update	✓	✓	✓	✓
Physical & Environmental	Power Suppy	External Power Adapter		80 PLUS Internal Power Supply	
	Dimensions	235 x 162 x 36 mm Desktop Size	280 x 214 x 44 mm Desktop Size	440 x 400 x 44 mm 19" Standard Rack-Mount	
	Operating Temperature	0° to 40° C			
	Storage Temperature	-20° to 70° C			
	Operating Humidity	5% to 95% non-condensing			
	EMI	FCC Class A CE Class A C-Tick VCCI			
	Safety	UL LVD (EN60950-1)	LVD (EN60950-1)	cUL, CB	
	MTBF	186,614 Hours	140,532 Hours	400,000 Hours	

[1] Actual performance may vary depending on network conditions and activated services.
[2] The maximum Firewall plaintext throughput is based on RFC2544 testing methodologies.
[3] VPN throughput is measured using UDP traffic at 1420 byte packet size adhering to RFC 2544.
[4] IPS and Anti-Virus performance test is based on HTTP protocol with a 1Mb file attachment run on the IXIA IxLoad. Testing is done with multiple flows through multiple port pairs.

D-Link®

DFL-260/860/1660/2560/2560G

Secure Network Implementation Using NetDefend™ UTM Firewalls



CE FC

D-Link Corporation
No. 289 Xinhu 3rd Road, Neihu, Taipei 114, Taiwan
Specifications are subject to change without notice.
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.
©2010 D-Link Corporation. All rights reserved.
Release 01 (August 2010)

FIREWALL

PaloSanto Solutions
OPEN SOURCE INNOVATION

FREEDOM TO COMMUNICATE

elastix®
FREEDOM TO COMMUNICATE

ELASTIX APPLIANCES SERIE ELX

Elastix instalado y listo para operación

La solución de telefonía que su empresa necesita debe integrar software estable con múltiple funcionalidad y hardware diseñado especialmente para garantizar el tráfico de llamadas requerido. Como un integrador u operador usted sabe que los negocios de Voz sobre IP requieren de hardware profesional con gran capacidad de soporte. Nosotros entendemos su negocio y queremos ayudarlo a crear la mejor solución posible para sus clientes o su empresa.

Elastix Appliance Serie ELX ofrece el servidor de comunicaciones ideal de acuerdo a sus necesidades con el cual usted estará seguro de contar con un equipo certificado y desarrollado pensando en satisfacer sus requerimientos de comunicación e ir más allá.

Características Generales

Diseño compacto y uniforme

El diseño de nuestros appliances es sencillo y compacto lo cual los hace portátiles y de fácil mantenimiento. Con carcasas metálicas de 1U, 1.5U y 3U tienen accesibilidad para expansiones usando puertos PCI o puertos USB utilizando *Channel Banks*.

Todos nuestros appliances son montables en rack lo cual permite integrarlos rápidamente a su infraestructura de red establecida.

Bajo consumo de poder

Nuestros appliances están diseñados para consumir la menor cantidad de poder necesario en condiciones normales. Por un lado esto permite un ahorro en energía y en gastos de operación del equipo y por otro contribuimos con la conservación del medio ambiente.

Capacidad de integración digital y analógica

Los appliance serie ELX integran tarjetas analógicas FXO/FXS y/o tarjetas digitales E1/T1, de acuerdo a su requerimiento, siempre asesorado por nuestro equipo técnico antes de empezar una implementación. Todo hardware viene integrado, pre-configurado y probado desde nuestras instalaciones.

ELX 025 - 4, 8, 12 - 1 E1/T1

ELX 3000 - 4, 8, 12, 16, 24 FXO - 1, 2 E1/T1

+1-877-ELASTIX www.elastix.org

PaloSanto Solutions
OPEN SOURCE INNOVATION

FREEDOM TO COMMUNICATE

elastix®
FREEDOM TO COMMUNICATE

ELASTIX APPLIANCES SERIE ELX

Software pre-instalado

Todos los modelos de nuestros appliance vienen con software Elastix pre instalado, dándole a usted una herramienta poderosa de negocios.

VoIP PBX

- Grabación de llamadas
- Voicemail
- IVR configurable y flexible
- Soporte para sintetización de voz
- Herramienta para crear extensiones por lotes
- Cancelador de eco integrado
- Provisionador de teléfonos vía Web
- Soporte para Video-teléfonos
- Interfaz de detección de hardware
- Servidor DHCP para asignación dinámica de IPs
- Panel de operador basado en Web
- Parqueo de llamadas
- Reporte de detalle de llamadas (CDRs)
- Tarifación con reporte de consumo por destino
- Reporte de uso de canales
- Soporte para colas de llamadas
- Centro de conferencias con salas virtuales
- Soporte para protocolos SIP e IAX, entre otros
  Codecs soportados: ADPCM, G.711 (A-Law & μ-Law), G.722, G.723.1 (pass through), G.726, G.729, GSM, entre otros
- Soporte para interfaces análogas FXS/FXO
- Soporte para interfaces digitales E1/T1/J1 a través de los protocolos PRI/BRI/R2
- Identificación de llamadas (Caller ID)
- Troncalización
- Rutas entrantes y salientes con configuración por coincidencia de patrones de marcado
- Soporte para *follow-me*
- Soporte para grupos de timbrado
- Soporte para paging e intercom
- Soporte para condiciones de tiempo
- Soporte para PINes de seguridad
- Soporte DISA
- Soporte Callback

Fax

- Servidor de fax administrable desde Web
- Visor de faxes integrado, pudiendo descargarse los faxes desde el Web en formato PDF
- Aplicación fax-a-email
- Personalización de faxes-a-email
- Control de acceso para clientes de fax
- Puede ser integrado con Winprint Hylafax

General

- Ayuda en línea embebida
- Disponible en 22 idiomas
- Monitor de recursos del sistema
- Configurador de parámetros de red
- Control de apagado/re-encendido de la central vía Web
- Manejo centralizado de usuarios y perfiles gracias al soporte de ACLs
- Administración centralizada de actualizaciones
- Soporte para backup/restore a través del Web
- Soporte para temas o skins
- Interfaz para configurar fecha, hora y uso horario de la central

+1-877-ELASTIX

www.elastix.org

PaloSanto Solutions
OPEN SOURCE INNOVATION

FREEDOM TO COMMUNICATE

elastix®
FREEDOM TO COMMUNICATE

ELASTIX APPLIANCES SERIE ELX

Software pre-instalado

Email

- Servidor de Email con soporte multidominio
- Administración centralizada vía Web
- Interfaz de configuración de *Relay*
- Cliente de Email basado en Web
- Soporte para cuotas
- Soporte *Antispam*

Colaboración

- Calendario integrado con PBX con soporte para recordatorios de voz
- Libreta telefónica *(Phonebook)* con capacidad *click-to-call*

Extras

- Integración con A2Billing para facturación
- CRM integrado: vTigerCRM y SugarCRM

Call Center

- Módulo de *Call Center* con marcador predictivo
- Soporte para campañas salientes y entrantes
- Formularios pueden ser asociados a campañas y diseñados a través de Web
- Un script puede ser asociado a una campaña
- Consola de agente con *pop- ups*
- Soporte para varios tipos de *breaks*
- Reportes avanzados

Mensajería instantánea

- Servidor de mensajería instantánea basado en OpenFire
- Cliente de mensajería instantánea Spark
- Inicio de llamadas desde Spark
- Servidor de mensajería es configurable desde Web
- Soporta grupos de usuarios
- Soporta conexión a otras redes de mensajería como MSN, Yahoo Messenger, GTalk, ICQ
- Reporte de sesiones de usuarios
- Soporta Jabber
- Soporta *plugins*
- Soporta LDAP
- Soporta conexiones server-to-server para compartir usuarios

Hardware Soportado

Soportamos el hardware telefónico de marcas probadas mundialmente. Sugerimos a nuestros clientes en sus implementaciones telefónicas los siguientes proveedores:

- **Teléfonos IP:**
  AASTRA, ATCOM, POLYCOM
- **Channel banks:**
  XORCOM, RHINO

PaloSanto Solutions
OPEN SOURCE INNOVATION

FREEDOM TO COMMUNICATE

elastix
FREEDOM TO COMMUNICATE

ELASTIX APPLIANCES SERIE ELX

	ELX-025	ELX-3000	ELX-5000
Telefonía			
Puertos Analógicos	Hasta 12	Hasta 24	Hasta 72
Puertos Digitales	Hasta 1 E1/T1/J1	Hasta 4 E1/T1/J1	Hasta 8 E1/T1/J1
Slots PCI de expansión	1	2	6: 3 PCI, 2(x8) PCIe, 1(x4)
Extensiones (SIP/IAX)	Hasta 100	Hasta 250	Hasta 600*
Llamadas concurrentes (máximo recomendado)	30	60	150*
Tiempo de soporte incluido	1 hora, 8x5 (-5GMT)	1 hora, 8x5 (-5GMT)	1 hora, 8x5 (-5GMT)
Hardware			
CPU	1.6 GHz Intel	2 x 1.6 GHz Dual Core Intel	1.86 GHz Dual Intel 64 bit Xeon
2do CPU	No	No	Si, hasta 4 núcleos Intel Xeon
RAM	1 GB	2GB	4 GB expandible a 48 GB
Hard Drive	250 GB	400 GB	1 TB de capacidad (2 x 500GB)
2do Hard Drive	No	Opcional	Opcional
RAID	No	Soft-RAID 1 (Opcional)	Soft-RAID por defecto
Tarjeta controladora de RAID	No	No	Opcional
Network Interface	10/100 Mbps	10/100 Mbps	2 x Gigabit Ethernet
Características de operación			
Potencia Nominal	90 W *fanless*, PSU eficiente	180 W PSU eficiente	Fuente redundante 500W HS
Voltaje de Operación	120-240 *Autoswitching*	120-240 *Autoswitching*	120-240 *Autoswitching*
Consumo de poder promedio	40 W *(low power)*	90 W	200 W
Fuente de poder redundante	No	No	Si
Sistema operativo	Elastix 32 bits	Elastix 32 bits	Elastix 64 bits
Características físicas			
Alto	1.75" (44.5 mm) - 1 U	2.63" (68 mm) - 1.5 U	3.46" (89 mm) - 2 U
Ancho	16.73" (425 mm)	16.73" (425 mm)	17.20" (437 mm)
Profundidad	11.96" (304 mm)	11.96" (304 mm)	14.45" (367 mm)
Montable en rack	Si	Si	Si - rack de 19"
Peso (Sistema básico)	4 Kg	5.5 Kg	9 Kg
Display LCD	No	20x4 chars. 5 botones de navegación	Si - Soporta Blacklight
Puertos USB	2 puertos en el panel frontal y 2 puertos en el panel posterior	4 puertos en panel posterior	4 puertos en panel posterior
Paneles LED frontales	Power/HDD	Power/HDD	Power/HDD
Extras			
Garantía	1 año	1 año	2 años
Garantía extendida	Opcional hasta 3 años	Opcional hasta 3 años	Opcional hasta 3 años
Rackmount/wallmount kit	Incluido	Incluido	Incluido
Cable de poder	Incluido	Incluido	Incluido
Quickstart Guide	Incluido	Incluido	Incluido

*Dependiendo del Número de CPUs y RAM

Guayaquil, Ecuador
Cdla. Nueva Kennedy, Calle E #222 y 9na Este
Telf: +593-4-2283268, +593-4-2294440
Email: ventas@palosanto.com

Quito, Ecuador
Av. De la República E703 y la Pradera, Edificio María Victoria 9no piso oficina N.904
Telf: +593-2-2901733, +593-2-6001980, +593-2-6001981
Email: ventasuio@palosanto.com

USA
2792 Belgravian Ct
Telf: +1-877-ELASTIX
San Jose, CA 95121
Email: sales@palosanto.com

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Advanced

Las herramientas de seguridad combinadas con funciones de optimización de TI abundan en esta valiosa gama de soluciones de Kaspersky Lab.

El nivel de protección Advanced de Kaspersky ofrece la solución de protección y gestión que tu organización necesita para aplicar la política de TI, mantener a los usuarios libres de malware, evitar las pérdidas accidentales de datos y, además, mejorar la eficacia en TI.

Las funciones de protección y gestión que necesitas.

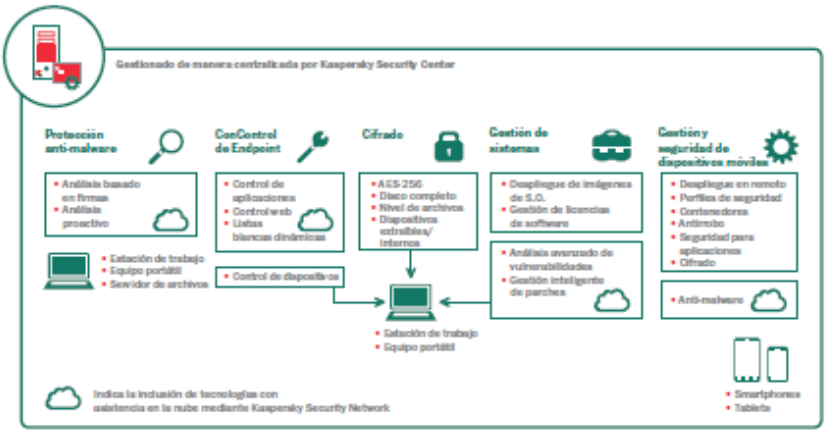
En Kaspersky hemos integrado potentes funciones empresariales en todos los niveles de protección de las soluciones que ofertamos, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

¿Qué nivel de protección es el más adecuado para ti?

- CORE
- SELECT
- **ADVANCED**
- TOTAL

FUNCIONES INCLUIDAS:

- ANTI-MALWARE
- FIREWALL
- PROTECCIÓN CON ASISTENCIA EN LA NUBE MEDIANTE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- MARCADO DE APLICACIONES EN LISTA BLANCA
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DE SERVIDORES DE ARCHIVOS
- MOBILE DEVICE MANAGEMENT (MDM)
- SEGURIDAD PARA DISPOSITIVOS MÓVILES (PARA TABLETS Y SMARTPHONES)
- CIFRADO
- CONFIGURACIÓN E IMPLEMENTACIÓN DE SISTEMAS
- CONTROL DE ADMISIÓN A LA RED
- ANÁLISIS AVANZADO DE VULNERABILIDADES
- GESTIÓN DE REVISIONES



LA ÚNICA PLATAFORMA DE SEGURIDAD DEL SECTOR

Una única consola de gestión
A través de un único "Panel de Control", el administrador puede ver y gestionar todo el sistema de seguridad: equipos virtuales y dispositivos tanto físicos como móviles.

Una única plataforma de seguridad
Kaspersky Lab ha desarrollado la consola, módulos de seguridad y herramientas de forma interna en lugar de adquirirlos de otras empresas. Eso significa que los programadores que trabajan en el mismo código base han desarrollado tecnologías que interactúan entre sí y funcionan de forma conjunta. Esto se traduce en estabilidad, políticas integradas, generación de informes útiles y herramientas intuitivas.

Un único coste
Todas las herramientas provienen de un único proveedor y se proporcionan mediante una única instalación, para que no tengas que pasar por un nuevo proceso de presupuestación y justificación para alinear tus riesgos de seguridad con tus objetivos empresariales.

CIFRADO Y PROTECCIÓN DE DATOS:

CIFRADO EXHAUSTIVO
Te permite elegir entre el cifrado a nivel de disco completo o el de archivo, respaldado por el algoritmo Advanced Encryption Standard (AES), con cifrado de 256 bits, para proteger información empresarial de vital importancia en caso de robo o pérdida de dispositivos.

COMPATIBILIDAD CON DISPOSITIVOS EXTRAÍBLES
Aumenta tu seguridad mediante políticas que aplican el cifrado de datos en dispositivos extraíbles.

USO SEGURO DE DATOS COMPARTIDOS
Significa que los usuarios pueden crear fácilmente paquetes cifrados y autoextraíbles para garantizar que los datos estén protegidos al compartirlos mediante dispositivos extraíbles, correo electrónico, redes o la web.

TRANSPARENCIA PARA USUARIOS FINALES
La solución de cifrado de Kaspersky es invisible para los usuarios y no tiene efectos negativos en la productividad. Sin repercusiones en la configuración de las aplicaciones ni en las actualizaciones.

CONTROL DE ENDPOINT

CONTROL DE APLICACIONES
Permite a los administradores de TI establecer políticas de autorización, bloqueo o regulación de aplicaciones (o categorías de aplicaciones).

CONTROL DE DISPOSITIVOS
Permite a los usuarios establecer, programar y aplicar políticas de control de dispositivos de almacenamiento extraíbles y otros dispositivos periféricos — conectados a un puerto USB o cualquier otro tipo de bus.

CONTROL WEB
Los controles de navegación basados en Endpoint hacen un seguimiento del usuario tanto en la red corporativa como fuera de ella, tanto para navegación peligrosa como para navegación no productiva.

LISTAS BLANCAS DINÁMICAS
El envío datos de reputación de archivos en tiempo real de Kaspersky Security Network permite garantizar que las aplicaciones aprobadas estén libres de malware, así como maximizar la productividad de los usuarios.

FUNCIONES DE PROTECCIÓN DE ENDPOINTS

ANTI-MALWARE PARA ENDPOINTS DE CALIDAD SUPERIOR
Métodos tradicionales de eficacia demostrada basados en firmas, proactivos y basados en la nube para la detección de amenazas de malware.

PROTECCIÓN CON ASISTENCIA EN LA NUBE
Kaspersky Security Network (KSN) ofrece una respuesta inmediata ante sospechas de amenazas, de forma mucho más rápida que los métodos de protección tradicionales. El tiempo de respuesta de KSN a una amenaza de malware puede ser de tan sólo 0,02 segundos.

NO TODAS LAS FUNCIONES SE ENCUENTRAN DISPONIBLES EN TODAS LAS PLATAFORMAS. Para obtener más información, consulta **www.kaspersky.es**

CONFIGURACIÓN DE SISTEMAS Y GESTIÓN DE REVISIONES:

GESTIÓN DE PARCHES
Análisis exhaustivo avanzado de vulnerabilidades combinado con distribución automatizada de parches.

DESPLIEGUE EN REMOTO DEL SOFTWARE
Implementación centralizada de software en los equipos cliente, incluso en sucursales.

NETWORK ADMISSION CONTROL (NAC)
Con control de admisión a la red (NAC), puedes crear una política de red de invitados. Los dispositivos invitados (incluidos los dispositivos móviles) se reconocen automáticamente y se envían a un portal de la empresa donde se habilitan las credenciales correctas para usarlos con los recursos que hayas aprobado.

DESPLIEGUE DE IMÁGENES DE SISTEMAS OPERATIVOS Y APLICACIONES
Fácil creación, almacenamiento y despliegue de imágenes de sistema desde una ubicación centralizada. Perfecto para migrar a Microsoft® Windows® 8.

GESTIÓN DE HARDWARE, SOFTWARE Y LICENCIAS
Los informes de inventario de hardware y software contribuyen a mantener el control de las obligaciones de licencia de software. Así podrás ahorrar costes gracias al abastecimiento central de derechos de software.

FUNCIONES DE SEGURIDAD MÓVIL:

INNOVADORAS TECNOLOGÍAS ANTI-MALWARE
La combinación de tecnologías de detección basadas en firma, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura y a tecnologías antispam.

DESPLIEGUE REMOTO DE APLICACIONES
Preconfigura e implementa aplicaciones de forma centralizada mediante SMS, correo electrónico y ordenadores.

HERRAMIENTAS ANTIRROBO REMOTAS
Las herramientas de vigilancia de SIM, bloqueo remoto, borrado y búsqueda evitan el acceso no autorizado a los datos de la empresa en caso de robo o pérdida de un dispositivo móvil.

CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES
Supervisa las aplicaciones instaladas en un dispositivo móvil, de acuerdo con las políticas de grupo predefinidas. Incluye un grupo de "aplicación obligatoria".

COMPATIBILIDAD CON LOS DISPOSITIVOS PERSONALES DE LOS EMPLEADOS
¿Iniciativa BYOD (trae tu propio dispositivo)? Los datos y las aplicaciones de la empresa permanecen aislados en contenedores cifrados de apariencia transparente para los usuarios. Estos datos se pueden borrar por separado.

CIFRADO Y PROTECCIÓN DE DATOS:

CIFRADO EXHAUSTIVO
Te permite elegir entre el cifrado a nivel de disco completo o el de archivo, respaldado por el algoritmo Advanced Encryption Standard (AES), con cifrado de 256 bits, para proteger información empresarial de vital importancia en caso de robo o pérdida de dispositivos.

COMPATIBILIDAD CON DISPOSITIVOS EXTRAÍBLES
Aumenta tu seguridad mediante políticas que aplican el cifrado de datos en dispositivos extraíbles.

USO SEGURO DE DATOS COMPARTIDOS
Significa que los usuarios pueden crear fácilmente paquetes cifrados y autoextraíbles para garantizar que los datos estén protegidos al compartirlos mediante dispositivos extraíbles, correo electrónico, redes o la web.

TRANSPARENCIA PARA USUARIOS FINALES
La solución de cifrado de Kaspersky es invisible para los usuarios y no tiene efectos negativos en la productividad. Sin repercusiones en la configuración de las aplicaciones ni en las actualizaciones.

CONTROL DE ENDPOINT

CONTROL DE APLICACIONES
Permite a los administradores de TI establecer políticas de autorización, bloqueo o regulación de aplicaciones (o categorías de aplicaciones).

CONTROL DE DISPOSITIVOS
Permite a los usuarios establecer, programar y aplicar políticas de control de dispositivos de almacenamiento extraíbles y otros dispositivos periféricos — conectados a un puerto USB o cualquier otro tipo de bus.

CONTROL WEB
Los controles de navegación basados en Endpoint hacen un seguimiento del usuario tanto en la red corporativa como fuera de ella, tanto para navegación peligrosa como para navegación no productiva.

LISTAS BLANCAS DINÁMICAS
El envío datos de reputación de archivos en tiempo real de Kaspersky Security Network permite garantizar que las aplicaciones aprobadas estén libres de malware, así como maximizar la productividad de los usuarios.

FUNCIONES DE PROTECCIÓN DE ENDPOINTS

ANTI-MALWARE PARA ENDPOINTS DE CALIDAD SUPERIOR
Métodos tradicionales de eficacia demostrada basados en firmas, proactivos y basados en la nube para la detección de amenazas de malware.

PROTECCIÓN CON ASISTENCIA EN LA NUBE
Kaspersky Security Network (KSN) ofrece una respuesta inmediata ante sospechas de amenazas, de forma mucho más rápida que los métodos de protección tradicionales. El tiempo de respuesta de KSN a una amenaza de malware puede ser de tan sólo 0,02 segundos.

NO TODAS LAS FUNCIONES SE ENCUENTRAN DISPONIBLES EN TODAS LAS PLATAFORMAS. Para obtener más información, consulta **www.kaspersky.es**

CONFIGURACIÓN DE SISTEMAS Y GESTIÓN DE REVISIONES:

GESTIÓN DE PARCHES
Análisis exhaustivo avanzado de vulnerabilidades combinado con distribución automatizada de parches.

DESPLIEGUE EN REMOTO DEL SOFTWARE
Implementación centralizada de software en los equipos cliente, incluso en sucursales.

NETWORK ADMISSION CONTROL (NAC)
Con control de admisión a la red (NAC), puedes crear una política de red de invitados. Los dispositivos invitados (incluidos los dispositivos móviles) se reconocen automáticamente y se envían a un portal de la empresa donde se habilitan las credenciales correctas para usarlos con los recursos que hayas aprobado.

DESPLIEGUE DE IMÁGENES DE SISTEMAS OPERATIVOS Y APLICACIONES
Fácil creación, almacenamiento y despliegue de imágenes de sistema desde una ubicación centralizada. Perfecto para migrar a Microsoft® Windows® 8.

GESTIÓN DE HARDWARE, SOFTWARE Y LICENCIAS
Los informes de inventario de hardware y software contribuyen a mantener el control de las obligaciones de licencia de software. Así podrás ahorrar costes gracias al abastecimiento central de derechos de software.

FUNCIONES DE SEGURIDAD MÓVIL:

INNOVADORAS TECNOLOGÍAS ANTI-MALWARE
La combinación de tecnologías de detección basadas en firma, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura y a tecnologías antispam.

DESPLIEGUE REMOTO DE APLICACIONES
Preconfigura e implementa aplicaciones de forma centralizada mediante SMS, correo electrónico y ordenadores.

HERRAMIENTAS ANTIRROBO REMOTAS
Las herramientas de vigilancia de SIM, bloqueo remoto, borrado y búsqueda evitan el acceso no autorizado a los datos de la empresa en caso de robo o pérdida de un dispositivo móvil.

CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES
Supervisa las aplicaciones instaladas en un dispositivo móvil, de acuerdo con las políticas de grupo predefinidas. Incluye un grupo de "aplicación obligatoria".

COMPATIBILIDAD CON LOS DISPOSITIVOS PERSONALES DE LOS EMPLEADOS
¿Iniciativa BYOD (trae tu propio dispositivo)? Los datos y las aplicaciones de la empresa permanecen aislados en contenedores cifrados de apariencia transparente para los usuarios. Estos datos se pueden borrar por separado.

KESB-ADV/Versión 0.2/Nov12/Global

© 2012 Kaspersky Lab ZAO. Todos los derechos reservados. Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios. Microsoft y Windows son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos o en otros países.

KASPERSKY lab

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Select

Herramientas para dar soporte a un personal laboral móvil, garantizar el cumplimiento con las políticas de seguridad de TI y bloquear el malware.

El nivel de protección "Select" de Kaspersky incluye implementación y protección para dispositivos móviles mediante Mobile Device Management (MDM) y funciones anti-malware para móviles. Las herramientas de control de terminales (web, dispositivos y aplicaciones) permiten a tu organización aplicar la política de TI, lo que mantiene seguros los elementos esenciales de tu entorno de TI.

Las funciones de protección y gestión que necesitas.

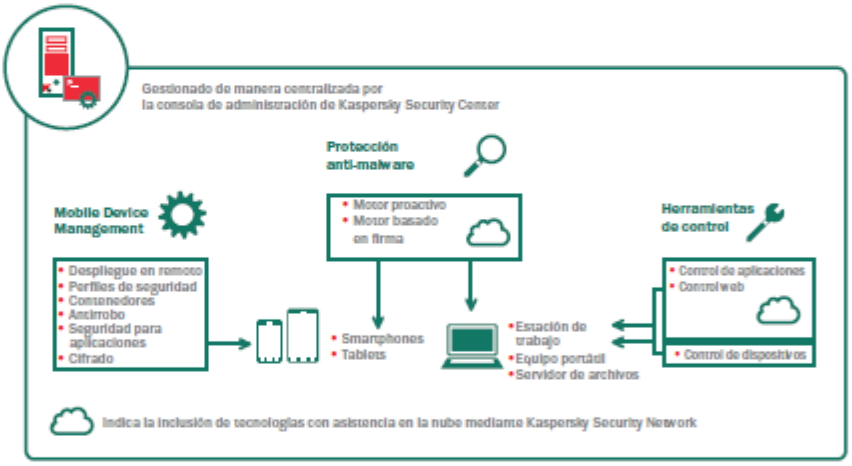
En Kaspersky hemos integrado potentes funciones empresariales en todos los niveles de protección de las soluciones que ofertamos, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

¿Qué nivel de protección es el más adecuado para ti?

- CORE
- **SELECT**
- ADVANCED
- TOTAL

FUNCIONES INCLUIDAS:

- ANTI-MALWARE
- FIREWALL
- PROTECCIÓN CON ASISTENCIA EN LA NUBE MEDIANTE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- MARCADO DE APLICACIONES EN LISTA BLANCA
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DE SERVIDORES DE ARCHIVOS
- MOBILE DEVICE MANAGEMENT
- SEGURIDAD PARA TERMINALES MÓVILES



FUNCIONES PRINCIPALES:

POTENTE ANTI-MALWARE PARA TERMINALES

El mejor motor de análisis de Kaspersky funciona en varios niveles del sistema operativo, eliminando el malware de raíz. Kaspersky Security Network (KSN) basado en la nube protege a los usuarios en tiempo real contra nuevas amenazas.

HERRAMIENTAS DE CONTROL FLEXIBLES Y CON GRAN NIVEL DE DETALLE

Una base de datos categorizada basada en la nube que enumera las aplicaciones y las páginas web seguras y no seguras permite al administrador definir y aplicar políticas para aplicaciones y navegación web, mientras que los controles con gran nivel de detalle garantizan que sólo los dispositivos específicos se puedan conectar a los equipos de la red.

EFICAZ IMPLEMENTACIÓN Y SEGURIDAD MÓVIL PARA SMARTPHONES Y TABLETS

La seguridad móvil basada en agentes está disponible para dispositivos móviles Android™, Blackberry®, Symbian y Windows® Mobile. Las políticas y el software para los dispositivos móviles se pueden implementar de forma segura de forma inalámbrica mediante Kaspersky MDM tanto en estos dispositivos como en dispositivos iOS.

ANALIZADOR DE VULNERABILIDADES

FUNCIONES DE PROTECCIÓN DE TERMINALES:

ACTUALIZACIONES FRECUENTES Y PROTECCIÓN BASADA EN FIRMAS
Método tradicional basado en firmas de eficacia demostrada para detectar amenazas de malware.

ANÁLISIS DE COMPORTAMIENTO DE SUPERVISOR DEL SISTEMA
Ofrece una protección proactiva contra amenazas que aún no se han registrado en las bases de datos de firmas.

PROTECCIÓN CON ASISTENCIA EN LA NUBE
Kaspersky Security Network (KSN) ofrece una respuesta inmediata ante sospechas de amenazas, de forma mucho más rápida que los métodos de protección tradicionales. El tiempo de respuesta de KSN a una amenaza de malware puede ser de tan sólo 0,02 segundos.

SISTEMA DE PREVENCIÓN DE INTRUSIONES BASADO EN HOST (HIPS) CON FIREWALL PERSONAL
Gracias a las reglas predefinidas para cientos de las aplicaciones más comúnmente utilizadas se reduce el tiempo invertido en la configuración del firewall.

CONTROL DE ENDPOINT

CONTROL DE APLICACIONES
Permite a los administradores de TI establecer políticas de autorización, bloqueo o regulación de aplicaciones (o categorías de aplicaciones).

CONTROL WEB
Significa que los controles de navegación basados en terminales hacen un seguimiento del usuario, tanto en la red empresarial como en itinerancia.

CONTROL DE DISPOSITIVOS
Permite a los usuarios establecer, programar y aplicar políticas de datos con controles para dispositivos de almacenamiento extraíbles y otros dispositivos periféricos conectados a un puerto USB o cualquier otro tipo de bus.

LISTAS BLANCAS DINÁMICAS
El envío datos de reputación de archivos en tiempo real de Kaspersky Security Network permite garantizar que las aplicaciones aprobadas estén libres de malware, así como maximizar la productividad de los usuarios.

FUNCIONES DE SEGURIDAD MÓVIL:

INNOVADORAS TECNOLOGÍAS ANTI-MALWARE
La combinación de tecnologías de detección basadas en firma, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura, a tecnologías antispam y a aplicaciones con tecnología sandbox.

IMPLEMENTACIÓN CON ABASTECIMIENTO INALÁMBRICO
Capacidad para preconfigurar e implementar aplicaciones de forma centralizada mediante el uso de SMS, correo electrónico y ordenadores.

HERRAMIENTAS ANTIRROBO REMOTAS
Las herramientas de vigilancia de SIM, bloqueo remoto, borrado y búsqueda evitan el acceso no autorizado a los datos de la empresa en caso de robo o pérdida de un dispositivo móvil.

CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES
Supervisa las aplicaciones instaladas en un dispositivo móvil, de acuerdo con las políticas de grupo predefinidas. Incluye un grupo de "aplicación obligatoria".

COMPATIBILIDAD CON LOS DISPOSITIVOS PERSONALES DE LOS EMPLEADOS
Los datos y las aplicaciones de la empresa permanecen aislados en contenedores cifrados de apariencia transparente para los usuarios. Estos datos se pueden borrar por separado.

LA ÚNICA PLATAFORMA DE SEGURIDAD DEL SECTOR.

Una única consola de gestión
A través de un único "panel de control", el administrador puede ver y gestionar todo el sistema de seguridad: equipos virtuales y dispositivos tanto físicos como móviles.

Una única plataforma de seguridad
Kaspersky Lab ha desarrollado nuestra consola, módulos de seguridad y herramientas de forma interna en lugar de adquirirlos de otras empresas. Eso significa que los programadores que trabajan en el mismo código base han desarrollado tecnologías que interactúan entre sí y funcionan de forma conjunta. Esto se traduce en estabilidad, políticas integradas, generación de informes útiles y herramientas intuitivas.

Un único coste
Todas las herramientas provienen de un único proveedor y se proporcionan mediante una única instalación, para que no tengas que pasar por un nuevo proceso de presupuestación y justificación para alinear tus riesgos de seguridad con tus objetivos empresariales.

NO TODAS LAS FUNCIONES SE ENCUENTRAN DISPONIBLES EN TODAS LAS PLATAFORMAS. Para obtener más información, consulta **www.kaspersky.es**

KESB-S/Versión 0.1/Nov12/Global

© 2012 Kaspersky Lab ZAO. Todos los derechos reservados. Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios. Windows

KASPERSKY

KD-DD61RC30-PT	Wired
KD-DD61RC30-PT-W	Wireless, Supports 802.11b/g protocol, 2.4GHZ, maximum wireless distance can be 100 meters, Supports WEP,WPA,WPA2,
Illumination	0.4Lux (Color)@F1.2; 0Lux(B/W)@IR on
Image sensor	1/4 OV CMOS Sensor,
Lens	Fixed Lens 6mm, IR distance: 10m
Video compression	H.264 Main Profile @Level 3/MJPEG
IR function	Built- in 10 pcs IR led and IR-cut set, IR distance: 10m
PAN/ TILT	Angle: horizontal 0º—355º, vertical 0º—90º Speed: horizontal 0º -15°/S , vertical 0º -15°/S
Video Definition	VGA : 640*480,1-30f/s QVGA : 320*240,1-30f/s QQVGA : 160*128,1-30f/s
Video Frame Rate	PAL: 1-25fps NTSC:1-30fps
Video Bit rate	32Kbps ~ 16Mbps
Audio Compression	G.726 , 32K bits
Audio Output	1channel, linear output,
Audio Input	1 channel external MIC interface(internal sound pick-up)
Video Output	With 1 channel CVBS analog video loop output
Title OSD	Supports channel name, date, and video stream information overlay; OSD location is adjustable
SD Card Interface	Support Video and Snapshots stored ,SD2.0 SDHC standard and maximum capacity:32GB
Network Interface	Self-adaption 10/100Mbps RJ45 port
Network protocol	TCP/IP、UDP、RTP、RTSP、RTCP、HTTP、DNS、DDNS、DHCP、FTP、NTP、PPPOE、SMTP、UPNP
Serial port	1 channel RS485
Alarm Input	1channel input, NO/NC modes adjustable
Alarm Output	1 channel output, 120VAC 1A/24VDC 1A
E-mail Alarm	Support
FTP Protocol	Support
RTSP Protocol	Support
Mobile Monitor	Supports smart mobile monitor that is based on Windows Mobile, Symbian and iPhone platforms

Working Temperature	-10℃ - +55℃
Working Humidity	0% - 90%
Power Input	DC12V/1.0A
Power Consumption	9W (MAX)
Dimension	Φ164mm *113mm
Net weight	0.6kg
Package	10pcs/carton, 13kg/carton, 930x270x365 mm

Yealink
easy VoIP

SIP-T22P

Professional IP phone with 3 Lines & HD voice

Yealink SIP-T22P features intuitive user interface and enhanced functionality which make it easy for people to interact and maximize productivity. Yealink HD technology enables rich, clear, life-like voice communications, outsourced management options, flexible deployment and third-party communications applications. As a cost effective IP solution, it helps users to streamline business processes, delivery a powerful, security and consistent communication experience for small and large offices environment.

Key Features and Benefits

HD Audio

Yealink HD Voice refers to the combination of software and hardware design as well as the implementation of wideband technology to maximize the acoustic performance. Coupled with advanced acoustic clarity technology such as full duplex, echo cancellation, adaptive jitter buffer etc. Provide clearer, more lifelike voice communications.

Enhanced Call Management

The SIP-T22P supports vast productivity-enhancing feature such as XML Browser, call park, call pickup, BLF, call forward, call transfer, 3-way conference. Which make it the natural and obvious efficiency tool for today's busy small and large offices environment.

Efficient Installation and Provisioning

Integrated IEEE 802.3af Power-over-Ethernet allows easy deployment with centralized powering and backup.The SIP-T22P support the FTP, TFTP, HTTP, and HTTPS protocols for file provisioning and are configured by default to use Trivial File Transfer Protocol (TFTP), supports AES encrypted XML configuration file.

Highly secure transport and interoperability

The Communicator uses SIP over Transport Layer Security (TLS/SSL) to provide service providers the latest technology for enhanced network security. The range is certified compatible with 3CX, Asterisk and Broadsoft Broadworks, ensuring excellent compatibility with leading soft switch suppliers.

- > Yealink HD Voice
- > 132x64-pixel graphical LCD
- > Two-port 10/100 Ethernet Switch
- > PoE support
- > Up to 3 SIP accounts
- > Headset support
- > Wall mountable
- > Simple, flexible and secure provisioning options

Addr: 4th-5th Floor, South Building, No.63 Wanghai Road, 2nd Software Park, Xiamen, China
Web: www.yealink.com

Yealink

Web: www.yealink.com
Tel: +86-592-5702000
Email: sales@yealink.com

Yealink SIP-T22P Specification

Audio Features
- HD voice: HD handset, HD speaker
- Wideband codec: G.722
- Narrowband codec: G.711(A/μ), G.723.1, G.729AB, G.726, iLBC
- DTMF: In-band, Out-of-band(RFC 2833) and SIP INFO
- Full-duplex hands-free speakerphone with AEC
- VAD, CNG, AEC, PLC, AJB, AGC

Phone Features
- 3 SIP accounts
- Call hold, mute, DND
- One-touch speed dial, hotline
- Call forward, call waiting, call transfer
- Group listening, SMS
- Redial, call return, auto answer
- Local 3-way conferencing
- Direct IP call without SIP proxy
- Ring tone selection/import/delete
- Set date time manually or automatically
- Dial plan
- XML Browser, Action URL/URI

Directory
- Loal phonebook up to 1000 entries
- Black list
- XML/LDAP remote phonebook
- Intelligent search method
- Phonebook search/import/export
- Call history: dialed/received/missed/forwarded

IP-PBX Features
- Busy Lamp Field (BLF)
- Bridged Line Apperance(BLA)
- Anonymous call, anonymous call rejection
- Hot-desking, emergency call
- Message Waiting Indicator (MWI)
- Voice mail, call park, call pickup
- Intercom, paging, music on hold
- Call completion, call recording

Display and Indicator
- 132x64-pixel graphical LCD with backlight
- LED for call and message waiting indication
- One-color (green) illuminated LEDs for line status information
- Intuitive user interface with icons and soft keys
- National language selection
- Caller ID with name, number

Feature keys
- 3 line keys with LED
- 5 features keys: message, headset, redial, tran, hands-free speakerphone
- 6 navigation keys
- Volume control keys

Interface
- 2xRJ45 10/100M Ethernet ports
- Power over Ethernet (IEEE 802.3af), class 2
- 1xRJ9 (4P4C) handset port
- 1xRJ9 (4P4C) headset port

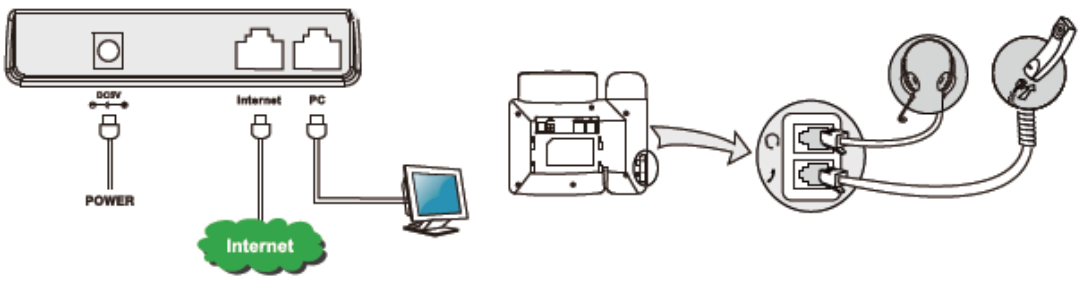
Other Physical Features
- Wall mountable
- External universal AC adapter (optional): AC 100~240V input and DC 5V/1.2A output
- Power consumption (PSU): 1.4-2.0W
- Power consumption (PoE): 2.1-2.9W
- Dimension(W*D*H*T): 209mm*188mm*150mm*41mm
- Operating humidity: 10~95%
- Operating temperature: -10~50°C

Management
- Configuration: browser/phone/auto-provision
- Auto provision via FTP/TFTP/HTTP/HTTPS for mass deploy
- Auto-provision with PnP
- Zero-sp-touch
- Phone lock for personal privacy protection
- Reset to factory, reboot
- Package tracing export, system log

Package Features
- Qty/CTN: 10 PCS
- N.W/CTN: 11.8 kg
- G.W/CTN: 13.0 kg
- Giftbox size: 220mm*241mm*105mm
- Carton Meas: 560mm*460mm*250mm

Network and Security
- SIP v1 (RFC2543), v2 (RFC3261)
- Call server redundancy supported
- NAT transverse: STUN mode
- Proxy mode and peer-to-peer SIP link mode
- IP assignment: static/DHCP
- HTTP/HTTPS web server
- Time and date synchronization using SNTP
- UDP/TCP/DNS-SRV(RFC 3263)
- QoS: 802.1p/Q tagging (VLAN), Layer 3 To DSCP
- SRTP for voice
- Transport Layer Security (TLS)
- HTTPS certificate manager
- AES encryption for configuration file
- Digest authentication using MD5/MD5-sess
- OpenVPN, IEEE802.1X
- IPv6

Certifications



Learn More
To find out how Yealink solutions can help your organization, visit us at www.yealink.com or mail to sales@yealink.com

Yealink
easy VoIP

SIP-T28P

Executive IP Phone with 6 Lines & HD Voice

The Yealink SIP-T28P represents the next generation VoIP phone which designed for the business user who needs rich telephony features, friendly UI and super voice quality. Yealink HD technology enables rich, clear, life-like voice communications. By the large, high-resolutiongraphical display, and together with all the 48 keys, SIP-T28P offers an excellent user experience to configure, make calls, express XML browser, etc. Moreover, to avoid problems with unwanted violations of your audio data, Yealink SIP-T28P supports the security standards TLS, SRTP, HTTPS, 802.1x, Open VPN and AES encryption which are necessary to protect against electronic eavesdropping and data theft.

Key Features and Benefits

HD Audio

Yealink HD Voice refers to the combination of software and hardware design as well as the implementation of wideband technology to maximizes the acoustic performance. Coupled with advanced acoustic clarity technology such as full duplex, echo cancellation, adaptive jitter buffer etc. Provide clearer, more lifelike voice communications.

A rich visual experience for applications

SIP-T28P Supports vast productivity-enhancing feature such as XML Browser, BLF, call forward, call transfer, 3-way conferencing, the 4 inch backlit display enables rich visual presentation and easier navigation of the menu, and together with all the 48 keys, SIP-T28P offers an excellent user experience to configure, make calls, etc.

Efficient Installation and Provisioning

Integrated IEEE 802.3af Power-over-Ethernet allows easy deployment with centralized powering and backup.The SIP-T28P support the FTP, TFTP, HTTP, and HTTPS protocols for file provisioning and are configured by default to use Trivial File Transfer Protocol (TFTP), supports AES encrypted XML configuration file.

Highly secure transport and interoperability

The Communicator uses SIP over Transport Layer Security (TLS/SSL) to provide service providers the latest technology for enhanced network security. The range is certified compatible with 3CX, Asterisk and BroadSoft Broadworks, ensuring excellent compatibility with leading soft switch suppliers.

- > Yealink HD Voice
- > 320x160-pixel graphical LCD
- > Two-port 10/100 Ethernet Switch
- > PoE support
- > Up to 6 SIP accounts
- > Headset, EHS support
- > Supports expansion modules
- > Simple, flexible and secure provisioning options

Addr: 4th-5th Floor, South Building, No.63 Wanghai Road, 2nd Software Park, Xiamen, China
Web: www.yealink.com
Tel: +86-592-5702000
Email: sales@yealink.com

Yealink
easy VoIP

SIP-T28P Specifications

Audio Features

> HD voice: HD handset, HD speaker
> Codecs: G.722, G.711(A/μ), G.723.1, G.729AB, G.726, iLBC
> DTMF: In-band, Out-of-band(RFC 2833) and SIP INFO
> Full-duplex hands-free speakerphone with AEC
> VAD, CNG, AEC, PLC, AJB, AGC

Phone Features

> 6 VoIP accounts
> Call hold, mute, DND
> One-touch speed dial, hotline
> Call forward, call waiting, call transfer
> Group listening, SMS
> Redial, call return, auto answer
> Local 3-way conferencing
> Direct IP call without SIP proxy
> Ring tone selection/import/delete
> Set date time manually or automatically
> Dial plan
> XML Browser
> Action URL/URI

Directory

> Loal phonebook up to 1000 entries
> Black list
> XML/LDAP remote phonebook
> Intelligent search method
> Phonebook search/import/export
> Call history: dialed/received/missed/forwarded

IP-PBX Features

> Busy Lamp Field (BLF)
> Bridged Line Apperance(BLA)
> Anonymous call, anonymous call rejection
> Hot-desking, emergency call
> Message Waiting Indicator (MWI)
> Voice mail
> Call park, call pickup
> Intercom, paging
> Music on hold
> Call completion
> Call recording

Display and Indicator

> 320x160-pixel graphical LCD with backlight
> LED for call and message waiting indication
> Dual-color (red or green) illuminated LEDs for line status information
> Intuitive user interface with icons and soft keys
> National language selection
> Caller ID with name, number

Feature keys

> 48 keys including 16 freely programmable keys
> 8 features keys: message, headset, hold, mute, tran, redial, conf, hands-free speakerphone
> 4 context-sensitive "soft" keys
> 6 navigation keys
> Volume control keys

Interface

> 2xRJ45 10/100M Ethernet ports
> Power over Ethernet (IEEE 802.3af), class 2
> 1xRJ9 (4P4C) handset port
> 1xRJ9 (4P4C) headset port
> 1XRJ12 (6P6C) EXT port:
Supports up to 6 Expansion Modules for an attendant console application

Other Physical Features

> External universal AC adapter (optional):
AC 100~240V input and DC 5V/1.2A output
> Power consumption (PSU): 1.3-2.1W
> Power consumption (PoE): 1.8-3.1W
> Dimension(W*D*H*T):
273mm*200mm*158mm*58.5mm
> Operating humidity: 10~95%
> Operating temperature: -10~50°C

Management

> Configuration: browser/phone/auto-provision
> Auto provision via FTP/TFTP/HTTP/HTTPS for mass deploy
> Auto-provision with PnP
> Zero-sp-touch, TR-069
> Phone lock for personal privacy protection
> Reset to factory, reboot
> Package tracing export, system log

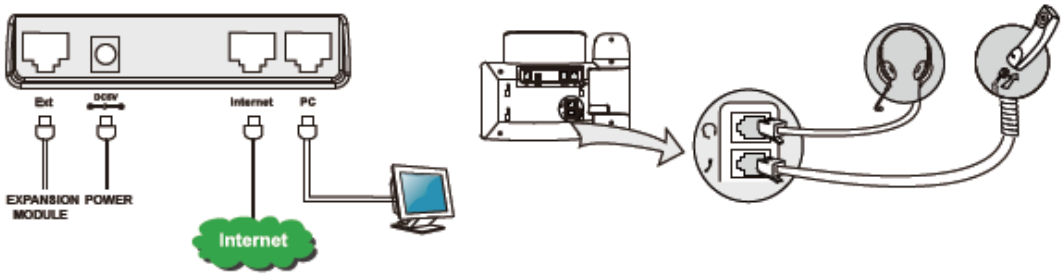
Network and Security

> SIP v1 (RFC2543), v2 (RFC3261)
> Call server redundancy supported
> NAT transverse: STUN mode
> Proxy mode and peer-to-peer SIP link mode
> IP assignment: static/DHCP/PPPoE
> HTTP/HTTPS web server
> Time and date synchronization using SNTP
> UDP/TCP/DNS-SRV(RFC 3263)
> QoS: 802.1p/Q tagging (VLAN), Layer 3 ToS DSCP
> SRTP for voice
> Transport Layer Security (TLS)
> HTTPS certificate manager
> AES encryption for configuration file
> Digest authentication using MD5/MD5-sess
> OpenVPN, IEEE802.1X
> IPv6

Package Features

> Qty/CTN: 5 PCS
> N.W/CTN: 6.9 KG
> G.W/CTN: 7.6 KG
> Giftbox size: 285mm * 240mm* 110mm
> Carton Meas: 580mm*295mm*250mm

Certifications



Learn More

To find out how Yealink solutions can help your organization, visit us at www.yealink.com or mail to sales@yealink.com

Addr: 4th-5th Floor, South Building, No.63 Wanghai Road, 2nd Software Park, Xiamen, China
Web: www.yealink.com
Tel: +86-592-5702000
Email: sales@yealink.com