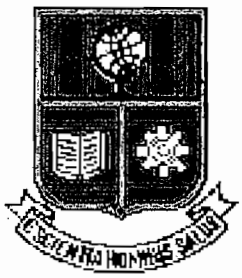
ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA



INGENIERÍA DE DETALLE PARA EL DISEÑO DE UNA INTRANET CON CONEXIÓN A INTERNET PARA APLICACIONES DE VOZ, DATOS Y VÍDEO UTILIZANDO LA ARQUITECTURA TCP/IP

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

MYRIAM PAULINA HERRERA MENA

WENDY PATRICIA HIDALGO ALOMOTO

DIRECTOR: ING. PABLO HIDALGO

Quito, Octubre 2004

DECLARACIÓN

Nosotros, Myriam Paulina Herrera Mena y Wendy Patricia Hidalgo Alomoto, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

Myriam Paulina Herrera Mena

Wendy Patricia Hidalgo Alomoto

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por las señoritas Myriam Paulina Herrera Mena y Wendy Patricia Hidalgo Alomoto, bajo mi supervisión.

Ing. Pablo Hidalgo
DIRECTOR DEL PROYECTO

DEDICATORIA

A mis queridos padres, Mariana y Galo, porque con su ejemplo y dedicación me enseñaron que no hay barreras cuando se lucha por un objetivo, gracias a su confianza y esfuerzo puedo hoy disfrutar de este sueño.

A mis hermanos, Maritza, Alex y Diana por permitirme disfrutar de esta linda familia de la cual me siento muy orgullosa.

Myriam Paulina

DEDICATORIA

A mi querido Jesús por ser ese amigo fiel que ha permanecido siempre conmigo

A mi amada familia por ser ese apoyo incondicional durante todos estos años

A todas las personas que han pasado por mi vida brindandome su amistad y dejándome enseñanzas valiosas

Wendy Patricia

AGRADECIMIENTO

Agradecemos a Dios por todo el amor que nos ha regalado a través de las innumerables situaciones y personas que ha puesto en nuestro camino. A la Comunidad Católica Verbum Dei por el apoyo y guía espiritual que nos han procurado en todo momento de nuestras vidas.

A nuestros amados padres por el cariño, la formación y el apoyo total que nos brindan; a nuestros hermanos por ser esos amigos sinceros e incondicionales.

A nuestros queridos amigos que por haber compartido nuestras alegrías y tristezas han hecho inolvidables los años vividos en esta universidad.

Al Ing. Pablo Hidalgo por su acertada dirección y por enseñarnos con su ejemplo que la honestidad y el trabajo son valores que debemos cultivar a diario.

Al Dr. Luis Corrales a los Ingenieros Carlos Egas, José Villacrés y Daniel Sánchez por el desinteresado asesoramiento prestado para la realización de este proyecto.

A todos aquellos familiares y personas que nos han brindado su mano amiga a lo largo de todo este tiempo.

Myriam Paulina

Wendy Patricia

ÍNDICE

Índice..... I
Resumen..... XI
Presentación..... XII

CAPÍTULO I

1 FUNDAMENTOS DE INTRANETS

1.1 ¿Qué es una Intranet?..... 2
1.2 Internet y el *World Wide Web*..... 3
1.2.1 ¿Qué es Internet?..... 3
1.2.2 Principales protocolos de la Arquitectura TCP/IP..... 6
1.2.3 *World Wide Web* (WWW)..... 9
1.2.3.1 URLs (Localizador Universal de Recursos)..... 10
1.3 Beneficios de una Intranet..... 11
1.4 Intranet vs Internet..... 13
1.5 Intranet vs Extranet..... 14
1.6 Servicios brindados por una Intranet..... 15
1.6.1 Servicio de correo..... 15
1.6.2 Servicio de archivos..... 15
1.6.3 Servicios *Web*..... 16
1.6.4 Servicios de audio..... 16
1.6.5 Servicios de vídeo..... 16
1.7 Componentes de una Intranet..... 17
1.7.1 Red de computadoras..... 18
1.7.2 Software de sistemas operativos..... 20
1.8 Administración de red..... 21
1.8.1 Administración de la configuración..... 21
1.8.2 Administración del contenido..... 23
1.8.3 Administración del rendimiento..... 24
1.8.4 Administración de fallas..... 25

1.8.5 Administración de la contabilidad.....25
1.8.6 Administración de la seguridad.....26
1.8.7 El *Webmaster*.....26
1.9 Seguridades de Intranet.....27
1.9.1 Seguridad interna.....28
1.9.2 Seguridad externa.....29
1.9.3 Cortafuegos o *Firewalls*.....31
1.9.4 Servidores *Proxy*.....35
1.10 El futuro de las Intranets.....37

CAPÍTULO II

INGENIERÍA AL DETALLE PARA EL DISEÑO DE LA INTRANET.....39
2.1 Servicios brindados por la Intranet.....43
2.1.1 Servicio de Internet.....43
2.1.2 Voz sobre IP (VoIP).....43
2.1.3 Vídeoconferencia.....44
2.1.4 Servicio de correo electrónico.....46
2.1.5 Servicio de *Chat*.....46
2.1.6 Servicios varios.....47
2.2 Análisis de requerimientos de la red.....47
2.2.1 Características de dimensionamiento del tráfico.....49
2.2.2 Determinación del volumen de información.....51
2.3 Diseño de la red de área local.....53
2.3.1 Topologías de red.....53
2.3.2 Tecnología de red.....56
2.3.3 Diseño de la red pasiva.....59
2.3.4 Diseño y dimensionamiento de la red activa.....68
2.4 Acceso a Internet.....75
2.4.1 Tecnología de transmisión.....77
2.4.2 Consideraciones de las tecnologías de acceso a Internet.....80
2.5 Proveedores de servicio a Internet (ISPs).....85
2.5.1 Acuerdos de nivel de servicio (SLA).....86
2.5.2 Parámetros para el análisis de calidad de servicios de los ISPs.....88

2.5.3 Análisis de la calidad de servicio de los ISPs en Quito.....90
2.6 Sistemas operativos y software de red.....93
2.6.1 Sistemas operativos.....94
2.6.2 Software para los servicios de la Intranet.....99
2.7 Configuración de Equipos.....101
2.7.1 Asignación de direcciones IP.....103
2.7.2 Configuración del *router*.....110
2.7.3 Configuración de servidores.....115
2.8 Administración y seguridad de la Intranet.....150
2.8.1 Administración de la Intranet.....150
2.8.2 Seguridad de la Intranet.....150
2.9 Diseños Complementarios.....152
2.9.1 Diseño de la iluminación.....152
2.9.2 Instalaciones eléctricas.....163

CAPÍTULO III

3 ANÁLISIS ECONÓMICO Y DE FACTIBILIDAD PARA LA INTRANET.....172
3.1 Estudio de mercado.....173
3.1.1 Definición y análisis del problema.....173
3.1.2 Definición de los servicios.....177
3.1.3 Investigación de mercado.....178
3.1.4 Usuarios del servicio.....187
3.1.5 Análisis de la demanda.....187
3.1.5.1 Demanda actual e histórica.....187
3.1.5.2 Proyección de la demanda.....189
3.2 Estudio financiero.....192
3.2.1 Inversiones.....193
3.2.2 Financiamiento de la inversión.....203
3.2.3 Presupuesto de costos y gastos.....204
3.2.4 Presupuesto de ventas.....207
3.2.5 Análisis del punto de equilibrio.....209
3.2.6 Flujo de caja proyectado.....210
3.2.7 Estados financieros proyectados.....213

3.3 Evaluación financiera del proyecto.....216
3.3.1 Período de recuperación del capital (TR).....216
3.3.2 Valor presente neto (VAN).....217
3.3.3 Tasa interna de retorno (TIR).....219
3.4 Análisis costo beneficio del proyecto.....220

CAPÍTULO IV

4 ESTUDIO LEGAL DE LA INTRANET.....222
4.1 Permisos legales.....222
4.2 Licencias y software.....224
4.3 Legislación para Voz sobre IP.....224
4.4 Trámites legales institucionales.....226
4.5 Trámites para servicios básicos.....229
4.5.1 Agua potable.....229
4.5.2 Servicio de energía eléctrica (Empresa Eléctrica Quito).....230
4.6 Constitución de una compañía.....231
4.6.1 Requisitos para el registro de la compañía en la Superintendencia de Compañías.....233

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES.....237
5.1 Conclusiones.....237
5.2 Recomendaciones.....241

GLOSARIO DE TÉRMINOS.....244

REFERENCIAS BIBLIOGRÁFICAS.....253

ANEXOS

A Estandar H323

B Resumen de las normas de cableado estructurado

C Distribución de salidas de telecomunicaciones

D Pruebas de certificación de cableado estructurado

E Configuración de *Netmeeting*

F Direccionamiento IP para los equipos de red LAN

G Resumen de comandos básicos de Linux

H Navegación Web de la Intranet

I Plan Administrativo de la Intranet

J Información general del programa *System Administrador Control* (SAC)

K Plan de seguridad para la Intranet

L Niveles de Iluminación

M Distribución de circuitos para instalaciones eléctricas

N Pruebas para instalaciones eléctricas

O Hojas técnicas de los equipos

P Planos de la Intranet

Q Métodos de proyección de la demanda

R Estrategias de *Marketing*

S Formularios

T Normativo para el apoyo a la presentación y administración de los proyectos y trabajos de extensión de la Escuela Politécnica Nacional

ÍNDICE DE TABLAS

CAPÍTULO I

FUNDAMENTOS DE INTRANETS

1.1 Diferencias entre Intranet, Internet y Extranet.....15

1.2 Componentes de una Intranet.....17

CAPÍTULO II

INGENIERÍA AL DETALLE PARA EL DISEÑO DE LA INTRANET

2.1 Características de tráfico para distintas aplicaciones.....51
2.2 Valores de tráfico estimado.....53
2.3 Ventajas y desventajas de las diferentes topologías de red.....56
2.4 Ventajas y desventajas de las alternativas de tecnologías de red LAN *Ethernet*.....60
2.5 Distribución de los puntos de telecomunicaciones.....62
2.6 Salidas de telecomunicaciones.....63
2.7 Cálculo de la longitud de cable UTP categoría 6.....65
2.8 Cálculo de la longitud de cable telefónico.....65
2.9 Resumen de materiales necesarios para cableado estructurado.....67
2.10 Características técnicas para el servidor proxy.....71
2.11 Características técnicas para los PCs de usuario.....71
2.12 Características técnicas para los PCs de administración y control.....72
2.13 Características técnicas para el servidor de e-mail.....74
2.14 Características y aplicaciones de las tecnologías WAN.....82
2.15 Características de los diferentes medios de transmisión.....84
2.16 Características de los diferentes ISPs de la Ciudad de Quito.....92
2.17 Cuadro comparativo de los sistemas operativos Windows vs UNIX.....97
2.18 Características de las versiones Windows.....98
2.19 Programas para vídeoconferencia a través de Internet.....100
2.20 Permisos de usuarios en Windows XP.....110
2.21 Puertos asignados para los diferentes servicios.....114
2.22 Direcciones para los interfaz de los servidores de red.....116
2.23 Análisis de riesgos de la Intranet.....152
2.24 Niveles de luz reflejada en materiales.....156
2.25 Niveles de luz reflejada en paredes y techos.....156
2.26 Cálculo de luminarias.....161
2.27 Cálculo de la demanda.....166
2.28 Valores de Ti.....166
2.29 Cálculo de conductores.....167
2.30 Protecciones para la instalación eléctrica.....170

2.31 Resumen de materiales necesarios para la instalación eléctrica 170

CAPÍTULO III

ANÁLISIS ECONÓMICO Y DE FACTIBILIDAD PARA LA INTRANET

3.1 Ingreso a la Escuela de Formación en Ciencias en los últimos tres años.....184
3.2 Ingreso a la Escuela de Ingeniería en los últimos tres años.....184
3.3 Ingreso a la Escuela de Formación Tecnológica de los últimos tres años.....184
3.4 Respuestas a la pregunta 1.....185
3.5 Respuestas a la pregunta 2.....185
3.6 Respuestas a la pregunta 3.....185
3.7 Respuestas a la pregunta 4.....186
3.8 Respuestas a la pregunta 5.....186
3.9 Respuestas a la pregunta 6.....186
3.10 Demanda actual e histórica de la población estudiantil.....188
3.11 Demanda real a centros de cómputo de la población estudiantil en la EPN.....189
3.12 Proyección de la demanda de la Escuela de Ciencias para un período de cuatro años.....191
3.13 Proyección de la demanda de la Escuela de Ingeniería para un período de..... ...191
cuatro años
314 Proyección de la demanda de la Escuela de Tecnología para un período..... ...192
de cuatro años
3.15 Costos de construcción y adecuación del local.....194
3.16 Resumen de costos de equipos de la red LAN.....195
3.17 Resumen de costos de equipos para la red WAN.....196
3.18 Cuadro de costos de materiales utilizados en instalaciones eléctricas 196
e iluminación
3.19 Resumen de materiales necesarios para la instalación de cableado.....197
estructurado
3.20 Resumen de costos de mano de obra.....197
3.21 Costos de muebles necesarios para la Intranet.....198
3.22 Costo de enceres necesarios en bar.....199
3.23 Dispositivos complementarios al diseño.....199
3.24 Resumen de los costos por licencias para los equipos de la Intranet.....200
3.25 Resumen de los costos de capital de trabajo sugerido 201

3.26 Inversión necesaria para la implementación del proyecto.....202
3.27 Equipos para vídeoconferencia grupal.....203
3.28 Costos fijos mensuales de la Intranet.....206
3.29 Costos variables mensuales de la Intranet.....206
3.30 Costos indirectos o gastos administrativos.....207
3.31 Porcentaje de ventas que se espera alcanzar.....207
3.32 Ingresos proyectados [Miles de USD].....208
3.33 Flujo de caja proyectada para la Intranet [Miles de USD].....212
3.34 Costos y gastos proyectados [Miles USD].....213
3.35 Balance general proyectado.....215
3.36 Reporte de índices financieros.....219

CAPITULO IV

ESTUDIO LEGAL DE LA INTRANET

4.1 Montos establecidos por la ley de contratación pública del Ecuador 228
para el llamado a concurso de oferentes
4.2 Número de socios o accionistas para la constitución de las compañías.....234
4.3 Valores mínimos a cancelarse para la constitución de las compañías.....234

ÍNDICE DE FIGURAS

CAPÍTULO I

FUNDAMENTOS DE INTRANETS

1.1 Una Intranet es la red de una compañía basada en la tecnología de Internet.....2
1.2 Conexión a Internet.....4
1.3 Intranet con acceso al Internet.....14
1.4 Red de computadoras.....18
1.5 Modelo de red Cliente – Servidor.....19
1.6 Respuesta de un servidor *Web* a la solicitud de un visualizador.....21
1.7 Papel del *Webmaster* en la compañía.....27

1.8 Red local protegida por *Firewall*..... 32
1.9 *Firewall* que separa a una red de su servidor *Web* actuando así como protector de la red local.....33
1.10 Servidor *Proxy*.....35

CAPÍTULO II

INGENIERÍA AL DETALLE PARA EL DISEÑO DE LA INTRANET

2.1 Distribución física del local.....42
2.2 Diagrama conceptual del diseño.....47
2.3 Estructura de una red VoIP.....44
2.4 Vídeoconferencia de escritorio.....45
2.5 Topologías físicas de red.....54
2.6 Transmisión de información en una red *Ethernet*.....57
2.7 Red *Ethernet* segmentada.....59
2.8 Diagrama lógico de la red.....61
2.9 Diagrama de la estructura interna de un *switch*.....68
2.10 Tarjeta de red NIC.....70
2.11 *Yap Max*.....72
2.12 Conexión a Internet.....76
2.13 Acceso a Internet *Frame Relay*.....78
2.14 Configuraciones de acceso dedicado a Internet.....79
2.15 Diagrama de bloques de la estructura interna del *router*.....84
2.16 Proveedor de servicio de Internet (ISP).....86
2.17 Límites de rendimiento del enlace de un ISP.....88
2.18 La velocidad de acceso está limitada por el ancho de banda más pequeño.....89
2.19 Distribución lógica de la Intranet.....103
2.20 Estaciones de trabajo con direcciones privadas accediendo a recursos de Internet.....105
2.21 Traductor de direcciones de red.....105
2.22 Traslación de de direcciones de red NAT.....106
2.23 Distribución de direcciones IP públicas.....107

2.24 Asignación de direcciones IP para la Intranet.....108
2.25 Pantalla para la configuración de las estaciones de trabajo en Windows XP...108
2.26 Pantalla de configuración de direcciones IP para estaciones de trabajo.....109
2.27 Registro de zona master.....119
2.28 Propiedades de zona master 120
2.29 Configuración para el registro DNS.....120
2.30 Propiedades para los registros A.....121
2.31 Ubicación del *firewall* en una red.....137
2.32 Ubicación del *firewall* en una red con DMZ.....137
2.33 Esquema de red con DMZ y dos *firewalls*.....138
2.34 Procesamiento de un paquete en el *kernel* con *IPtables*.....140
2.35 Pantalla de las propiedades del Servidor *Apache*.....147
2.36 Propiedades de *host* virtual 147
2.37 Página *Web* de la Intranet.....149
2.38 Página *Web* para ambiente privado de la Intranet.....149
2.39 Altura de montaje 158

CAPÍTULO III

ANÁLISIS ECONÓMICO Y DE FACTIBILIDAD PARA LA INTRANET

3.1 Punto de equilibrio para el servicio de acceso a Internet.....226

PRESENTACIÓN

El entusiasmo que se ha generado en torno a Internet ha motivado que las organizaciones busquen la mejor forma de aprovechar internamente los beneficios de esta tecnología, como son: fácil acceso, actualización inmediata y rápida difusión de la información.

La Intranet es una infraestructura basada en los estándares y protocolos de Internet que permite compartir información dentro de un grupo definido y limitado. Las expectativas de los usuarios finales de una Intranet son simplemente la facilidad de uso, la velocidad y la confiabilidad.

El presente proyecto de titulación propone una alternativa real de solución que responde a ciertas necesidades de la comunidad politécnica, tales como: navegación *Web*, *e-mail*, vídeoconferencia y acceso a información bibliográfica con calidad de servicio. Cabe mencionar que la solución propuesta analiza también aspectos económicos y legales necesarios para su implementación.

El diseño de una Intranet es un tema en el que intervienen varias disciplinas: cableado estructurado, levantamiento de servicios en la Intranet, configuración de elementos activos, dimensionamiento de la red WAN, establecimiento de seguridad física y lógica, planes de administración de red, diseño eléctrico y de iluminación, estudio de mercado, análisis financiero y el estudio legal.

Este documento ha sido preparado en un estilo que consideramos fácil de entender, con la finalidad de que pueda ser utilizado por personas involucradas en el área de redes y telecomunicaciones.

RESUMEN

La implementación masiva de Intranets con conexión a Internet sin un sustento técnico, ha llevado a los usuarios a soportar un servicio de acceso a Internet de muy mala calidad, frente a este problema el presente proyecto de titulación propone una alternativa real de solución.

Con la finalidad de presentar organizadamente el diseño de la Intranet, este proyecto está organizado en cuatro capítulos:

El capítulo uno describe las características de las Intranets, los protocolos en los que se fundamenta, proporciona criterios generales acerca de la administración y seguridad de la red y una descripción general de los servicios que brindar.

En el segundo capítulo se realiza el diseño sistemático y detallado de la Intranet, partiendo del análisis de requerimientos de red, los cuales permiten dimensionar el tráfico que tendrá que soportar.

Basados en este análisis se plantean cinco etapas para el diseño:

- Diseño de la red LAN
- Dimensionamiento del enlace a Internet
- Software y configuración de equipos de red
- Administración y seguridad de red
- Proyectos complementarios: instalaciones eléctrica e iluminación

El tercer capítulo realiza el estudio de factibilidad del proyecto, fundamentado en estudios de mercado, presupuesto referencial, consideraciones de gastos e ingresos esperados, que a su vez posibilitan plantear estados financieros proyectados y el tiempo de recuperación del capital.

En el cuarto capítulo se indican todos y cada uno de los permisos legales internos y externos, necesarios para que el proyecto sea legalmente establecido en la Institución educativa.

En el capítulo cinco se presentan las conclusiones y recomendaciones del proyecto de titulación.

Finalmente en los anexos se adjuntan documentos adicionales con la descripción detallada de los protocolos, normas vigentes, plan administrativo, plan de seguridad, etc. que complementan el entendimiento del proyecto.

CAPÍTULO 1

FUNDAMENTOS DE INTRANETS

FUNDAMENTOS DE INTRANETS

1.1 ¿QUÉ ES UNA INTRANET?

Una Intranet básicamente es tener una Internet dentro de una compañía, es decir emplear la misma tecnología que se utiliza en Internet (páginas, servidores *Web*, protocolos, etc) para fines específicos. Son redes privadas que utilizan estándares y protocolos de Internet y llevan la información a la interfaz intuitiva de *World Wide Web*[1], al igual que servicios almacenados a la red de área local LAN de una empresa (figura 1.1).

Con la utilización de una Intranet, la información en una red es fácil de acceder y una página es sencilla de implementar. Las intranets resultan atractivas por que reducen el costo de administración y mantenimiento de las redes internas y aumentan la productividad de los usuarios al proporcionar un acceso más eficiente a la información y a los servicios que necesitan.

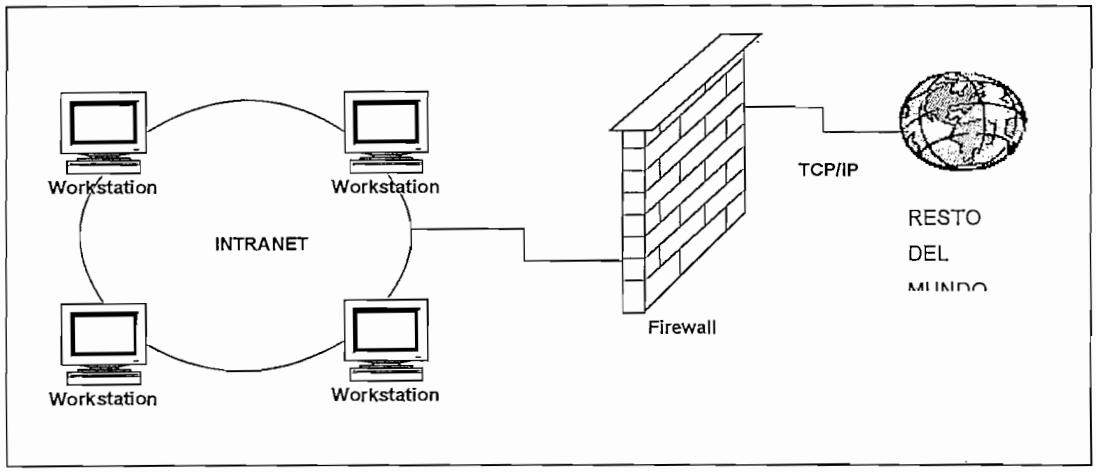


Figura 1.1 *Una Intranet es la red de una compañía basada en la tecnología de Internet. [1]*

En pocas palabras, una Intranet es una red de computadoras, que permite que los usuarios de una compañía compartan e intercambien información, correo electrónico e incluso documentos empresariales confidenciales.

[1] *World Wide Web*: es un conjunto de documentos enlazados entre sí y ubicados en la cima de Internet.

A primera vista, una Intranet puede parecer una red de área local de alcance empresarial. En algunos casos, es estrictamente una red de área local; sin embargo, los usuarios conectados a una Intranet trabajan a menudo en oficinas geográficamente dispersas, incluso en el mundo entero. Una de las características que distinguen a las Intranets de las redes tradicionales es que se basan en la pila de protocolos TCP/IP, que es el conjunto de reglas de software que controlan a Internet.

1.2 INTERNET Y EL *WORLD WIDE WEB*

Sin Internet y el *World Wide Web*, las Intranets no existirían. De la misma forma que las compañías utilizan Internet y el *World Wide Web* para las comunicaciones externas entre compañías, éstas han empezado ha adoptar las mismas herramientas para sus interconexiones internas. Las herramientas pioneras en Internet se han convertido en la base de la comunicación en una Intranet. Las herramientas de comunicación de "red" inter-compañía se han convertido en las herramientas de red intra-compañías.

1.2.1 ¿QUÉ ES INTERNET?

Internet es una red de redes. Actualmente conecta miles de redes para permitir compartir información y recursos a nivel mundial. Con Internet los usuarios pueden compartir, prácticamente, cualquier cosa almacenada en un archivo (figura 1.2).

Las comunicaciones en Internet son posibles entre redes de diferentes ambientes y plataformas. Este intercambio dinámico de datos se ha logrado debido al desarrollo de los protocolos[2] de comunicación.

Internet es una red global, en la cual cada computadora actúa como cliente o servidor. Internet consta de varios componentes interconectados:

[2] Protocolo: conjunto de reglas que permiten realizar una acción, son estándares aprobados por la comunidad mundial de Internet, representada en el IETF (*Internet Engineering Task Force*)

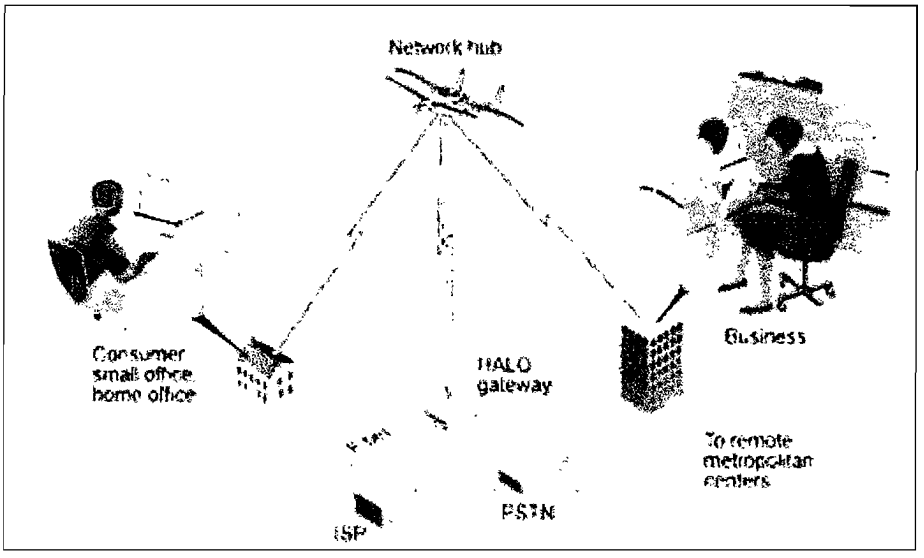


Figura 1.2. Conexión a Internet [31]

a. Backbones

Líneas de comunicación de alta velocidad y gran ancho de banda que unen *hosts* o redes.

b. Redes

Son sistemas de comunicación entre computadoras, que permiten compartir información y recursos. La topología o la forma de conexión de la red, depende de algunos aspectos como la distancia entre computadoras, el medio de comunicación utilizado y la velocidad del sistema.

c. Proveedores del Servicio de Internet (ISPs)

Son empresas que permiten el acceso a Internet.

d. Hosts

Computadoras cliente/servidor por medio de los cuales los usuarios acceden a los diferentes servicios locales o de Internet.

Cada computadora que se conecta directamente a una red es un *host*. Todos los *hosts* tienen una dirección de red única, ésta es comúnmente conocida como la dirección IP.

La arquitectura TCP/IP está conformada por un modelo de cuatro capas: *Host* Red, Red, Transporte y Aplicación.

Capa *Host* Red

Como base del modelo esta capa es responsable de colocar y recuperar los datos del medio físico.

Capa de Red

La capa de red es responsable de las funciones de direccionamiento, empaquetamiento y ruteo. Los protocolos más utilizados en esta capa son:

IP: rutea y direcciona paquetes entre los nodos y redes.

ARP: obtiene las direcciones de hardware de los nodos localizados en el mismo segmento.

ICMP: envía mensajes y reporta errores con respecto a la entrega de paquetes.

Capa Transporte

La capa de transporte provee la comunicación entre dos nodos; está formada por dos protocolos:

TCP: es un protocolo orientado a conexión. Establece comunicaciones confiables para aplicaciones que transfieren una gran cantidad de datos al mismo tiempo, o requieran una confirmación de los datos recibidos.

UDP: es un protocolo no orientado a conexión, no garantiza que los paquetes sean entregados. Las aplicaciones de UDP transfieren pequeñas cantidades de datos a la vez.

Capa de Aplicación

La capa de aplicación está en la parte superior del modelo. En esta capa las aplicaciones obtienen el acceso a la red.

Cuando una aplicación transmite datos a otro nodo, cada capa añade su propia información como un encabezado. Al ser recibido el paquete, la capa correspondiente remueve su encabezado y trata el resto del paquete como datos.

Las necesidades básicas que aparecen en el mundo real como el correo electrónico o el acceso a una computadora remota, condujeron a desarrollar protocolos de aplicación sobre los protocolos de transporte.

1.2.2 PRINCIPALES PROTOCOLOS DE LA ARQUITECTURA TCP/IP

a. Hypertext Transfer Protocol (HTTP)

El Protocolo de Transferencia de HiperTexto *(Hypertext Transfer Protocol)* es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes *Web* y los servidores HTTP.

HTTP se basa en sencillas operaciones de solicitud/respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su posible resultado. Todas las operaciones pueden adjuntar un objeto o recurso sobre el que actúan; cada objeto *Web* (documento HTML, fichero multimedia o aplicación CGI[3]) es conocido por su URL[4].

En pocas palabras, HTTP define las reglas que siguen los programas de software para intercambiar información a través del *Web*.

Entre las propiedades de HTTP se pueden destacar las siguientes:

- Un esquema de direccionamiento comprensible.
  Utiliza el *Universal Resource Identifier* (URI) para localizar sitios (URL) o nombres (URN) sobre los que hay que aplicar un método.
- Arquitectura Cliente-Servidor.

[3] CGI: *Common Gateway Interface* es una norma para establecer comunicación entre un servidor web y un programa
[4] URL: *Uniform Resource Locator* permite la localización de páginas Web a través del Internet

HTTP se basa en el paradigma solicitud/respuesta. El puerto de salida por defecto es el 80, pero se pueden utilizar otros.

- Es un protocolo no orientado a conexión.
  Después de que el servidor ha respondido la petición del cliente, se rompe la conexión entre ambos. Además no se guarda memoria del contexto de la conexión para futuras conexiones.
- Está abierto a nuevos tipos de datos.
  HTTP utiliza tipos MIME (*Multipart Internet Mail Extension*) para la determinación del tipo de datos que transporta. Cuando un servidor HTTP transmite información, de vuelta a un cliente incluye una cabecera que le indica sobre los tipos de datos que componen el documento. De la gestión de esos datos se encargan las utilidades que tenga el cliente (visor de imágenes, de vídeo, etc.)

b. Internet Relay Chat (IRC)

El protocolo IRC es un protocolo basado en modo texto, en un ambiente cliente - servidor.

IRC por si mismo es un sistema de teleconferencia diseñado para ejecutarse en varias computadoras en un ambiente distribuido.

Una instalación común involucra un solo servidor, convirtiéndose en un punto central para los clientes (u otros servidores).

c. Simple Mail Transfer Protocol (SMTP)

Todas las aplicaciones de correo que se ejecutan sobre la pila TCP/IP usan el protocolo simple de transporte de correo (SMTP) para transmitir los mensajes.

Este protocolo está diseñado para transferir correo de manera segura y eficiente. SMTP es independiente del servicio de transporte usado mientras se emplee un canal de transmisión para enviar y recibir: comandos, texto y confirmaciones.

Mientras las conexiones TCP transmiten *bytes*, los datos de SMTP se envían en caracteres ASCII de 7-bits.

d. Multipurpose Internet Mail Extensions (MIME)

Es otra de las facilidades útiles que se puede tener en aplicaciones de correo. MIME proporciona la capacidad de asociar archivos a los mensajes de correo. Por ejemplo permite asociar a un mensaje: hojas de cálculo, documentos, archivos de bases de datos, archivos de audio y de vídeo así como cualquier otro tipo de archivos. Quien recibe el mensaje usa una aplicación para ejecutar el archivo. Se puede usar esta capacidad para enviar propuestas, presupuestos y comentarios.

Una variación de este protocolo es el S / MIME, que proporciona una forma de cifrar los mensajes de correo desde que abandona la computadora del emisor hasta que llega al computador del receptor.

e. *Post Office Protocol* (POP3)

POP3 está diseñado para permitir el acceso dinámico y eficaz de las estaciones de trabajo (cliente) a un recipiente de mensajes en un *host* (servidor).

El servidor POP3 inicia el servicio monitoreando el puerto TCP 110. Cuando un cliente desea hacer uso del servicio, él establece una conexión con el servidor. Cuando la conexión es establecida, el servidor POP3 envía una confirmación. El cliente y el servidor POP3 entonces intercambian comandos y respuestas (respectivamente) hasta que la conexión sea cerrada o abortada.

e. *File Transfer Protocol (FTP)*

El protocolo de transferencia de archivos FTP es el protocolo estándar de TCP/IP para transportar archivos de un computador a otro. FTP define las reglas del protocolo mediante las que un computador servidor puede proveer datos o archivos a otros para su uso y mediante las que un computador cliente puede localizar y transmitir estos archivos. Con FTP un usuario se registra en el lugar en donde se realiza FTP en Internet y se le permite el acceso a ciertos archivos de ese lugar, una vez autenticado en forma apropiada.

1.2.3 *WORLD WIDE WEB* (WWW)

El *World Wide Web* es un medio de acceso a información en Internet. El WWW consiste en ordenadores conectados mediante hiperenlaces que permiten a los usuarios de Internet navegar de un lugar a otro.

El *World Wide Web* define un conjunto de documentos ligados entre sí y ubicados en la cima de Internet. Gracias a la vinculación de documentos entre sí, el *Web* facilita enormemente la localización de información por parte de sus usuarios. Los componentes del *Web* son los siguientes:

a. Visualizadores *Web* o *Web Browsers*

Para ver un documento *Web*, es necesario un *Web browser,* como el *Internet Explorer* o el *Netscape Navigator*. Un *browser* es una aplicación cliente que permite la comunicación de una computadora con el servidor *Web* u otros servidores de Internet como FTP.

Un visualizador también interpreta y despliega archivos de hipertexto, que integran texto, gráficos y sonidos.

b. Páginas *Web*

El *Web browser* interpreta y despliega las páginas *Web* obtenidas del servidor *Web*. Estas páginas cuentan con capacidades de hipertexto e hipermedia que incluyen diferentes tipos de archivos y pueden crear enlaces con otras páginas, este es el verdadero poder del WWW. El Lenguaje de Marcadores de Hipertexto (HTML) permite incrustar diferentes tipos de archivos y adjuntarlos con otros documentos.

Se puede afirmar que el HTML es una notación estándar usada para escribir páginas WWW. HTML permite definir la fuente, apariencia y color del texto, incrustar gráficos, sonidos, y enlaces de hipertexto, a través de un conjunto de etiquetas.

Cuando el visualizador recibe la página *Web* del servidor, interpreta las páginas HTML para desplegar la información.

c. Servidor *Web*

El servidor *Web*, almacena y administra las páginas *Web*. Los servidores *Web* se usan principalmente para mantener un directorio de páginas y lugares *Web* que permitan responder a las peticiones de los visualizadores e interactuar con el servidor.

Un servidor *Web* es un servidor de archivos, configurado con el hardware y software apropiados para responder a las peticiones de los clientes, mediante un visualizador. Esencialmente un servidor *Web* descarga páginas y aplicaciones *Web* hacia los usuarios.

Funcionamiento del WWW

Los pasos para obtener información del WWW son:

1. El Web *browser* solicita una página *Web* por medio de un URL.
2. Se establece una sesión entre el *browser* y el servidor por medio de HTTP.
3. El servidor contesta la solicitud de la página *Web* en formato HTML[5].
4. El *Web browser* interpreta el formato HTML y despliega la información.

1.2.3.1 URLs (Localizador Universal de Recursos)

El Localizador Universal de Recursos (URL) es la dirección de una página Web, un archivo, una base de datos, una petición u otro lugar de un servidor en cualquier parte del mundo.

Todos los recursos en Internet tienen una dirección "familiar" conocida como URL. La primera parte de un URL corresponde al protocolo del servicio usado. La segunda parte corresponde a una dirección IP. Los *routers* traducen una URL en una dirección numérica IP. El siguiente es un ejemplo:

http://www.ejemplo.edu/tesis/arq.html

[5] HTML: *Hyper Text Markup Language* es un lenguaje para estructurar documentos a partir de texto en World Wide Web

http: *Hypertext Transfer Protocol*
www.ejemplo.edu: URL de la red
tesis: Directorio
arq.html: Nombre del archivo en que está guardado el hypertexto

Una organización puede registrar su nombre de dominio dentro del *Internet Network Information Center (InterNIC)*, según el tipo de organización:

→ .gov: gobierno
→ .com: compañías comerciales
→ .edu: instituciones educacionales
→ .mil: militar
→ .net: proveedor de acceso a Internet
→ .org: organización sin fines de lucro
→ .int: internacional

Es importante mencionar que los URLs hacen diferencias entre mayúsculas y minúsculas.

1.3 BENEFICIOS DE UNA INTRANET

Una Intranet no es exclusiva para grandes redes, puede resultar de mucha utilidad para cualquier tipo de red. Una de las ventajas es manejar la información como si se tratase de páginas electrónicas del *Web*. La difusión de la información se hace por medio de la red y no por papeles y documentos impresos. Así toda la información importante para todos los empleados se maneja a través de ella, por ejemplo: el reglamento interno de trabajo, la cartera de clientes, el directorio interno, etc. Una Intranet otorga los siguientes beneficios:

a. Actualización

Acceso a la información en el momento en que se actualiza, por ejemplo cualquier cambio de precios será actualizado en un único sitio y la información aparecerá sin necesidad de que el usuario envíe un mensaje para que se la actualice.

b. Escalabilidad

Inicialmente puede ser una aplicación pequeña, y se construye de acuerdo a las necesidades de la empresa; según los requerimientos de la misma podrá crecer siendo su único límite la capacidad de almacenamiento.

c. Ahorro

El uso de útiles de oficina queda reducido al mínimo y esto justifica la inversión que se realizará para la Intranet.

d. Acceso

Se puede acceder a la información independientemente de su ubicación física al momento de consultarla, existe incluso la posibilidad de tener acceso a través de cualquier otro servidor de Internet previa identificación y validación del usuario para garantizar la seguridad de la información.

e. Centralización

Simplifica la búsqueda de la información, ya que todos los datos cronológicos de las operaciones de la empresa pueden ser buscados en un mismo servidor facilitando el trabajo incluso en casos de cambios de personal y reasignación de funciones que difícilmente se reflejan en todas las bases de datos de la empresa.

f. Fácil localización y confidencialidad

El uso de navegadores facilita el proceso de localización de documentos y permite a la vez un control sobre el acceso de las páginas *Web* internas. En un momento dado es posible impedir el acceso al personal que ha dejado de laborar en la empresa o que por alguna razón no debe tener acceso a la información.

g. Seguridad

Actualmente una de las mayores preocupaciones es la seguridad en el manejo de la información y la garantía de que personas ajenas a la empresa no puedan acceder a ella sin autorización. La Intranet provee los mecanismos de seguridad

adecuados, así los usuarios que tengan acceso a información confidencial estarán definidos dentro de los sistemas de seguridad del sistema operativo.

h. Enlaces

La búsqueda de la información se vuelve más eficiente al conectar documentos y datos mediante hipervínculos.

i. Búsqueda

Con la indexación automática los usuarios encuentran rápidamente documentos específicos o información general aunque el *Web* no esté organizado por temas o por autores.

j. Punto de entrada en común

Los usuarios no tienen que recordar si la información está guardada en una carpeta del servidor o distribuida como un memo impreso.

1.4 INTRANET vs INTERNET

Ya que mucha de esta tecnología es el resultado de Internet se podría a menudo observar a la Intranet y a Internet como afines, pero la mayor diferencia es que la Intranet pertenece a la empresa mientras que el Internet no.

Una de las ventajas de Intranet es que el personal trabaja con las mismas herramientas, y con los mismos formatos que se han usado, la diferencia radica en que se accede a la información interna o externa a través de una única interfaz.

Siendo de fácil implementación en una empresa, la Intranet tiene la gran ventaja de que su uso no requiere un valor adicional como sucede con el Internet, por el que se debe pagar un cierto costo de utilización a las empresas encargadas de distribuir este servicio.

La seguridad es otro factor primordial que diferencia a los dos tipos de redes, en el Internet se está expuesto a que cualquier persona pueda acceder a la

información que se está recibiendo o enviando por este medio, en cambio una Intranet puede tener un buen sistema de seguridad.

Las desventajas de una Intranet comparada con el Internet, es que la primera se queda en la empresa y no tiene visibilidad de lo que pasa fuera de ella. Los límites de su comunicación son los mismos de la empresa. Ésta es una limitación si la empresa requiere que sus clientes o proveedores interactúen en todas las decisiones de la compañía. En el caso de que esto sea requerido la empresa deberá plantear la necesidad de una Extranet como solución a mediano o largo plazo.

1.5 INTRANET vs EXTRANET

Una empresa hoy en día puede tener un sitio en donde los clientes consulten sus compras, sus productos, si todavía éstos existen en *stock* sin necesidad de estar en la empresa, inclusive sin estar en la misma ciudad. En este caso es conveniente el paso de una Intranet a una Extranet, que no es más que una apertura para el uso externo de la Intranet.

Extranet es entonces, una Intranet abierta al exterior. (figura 1.3)

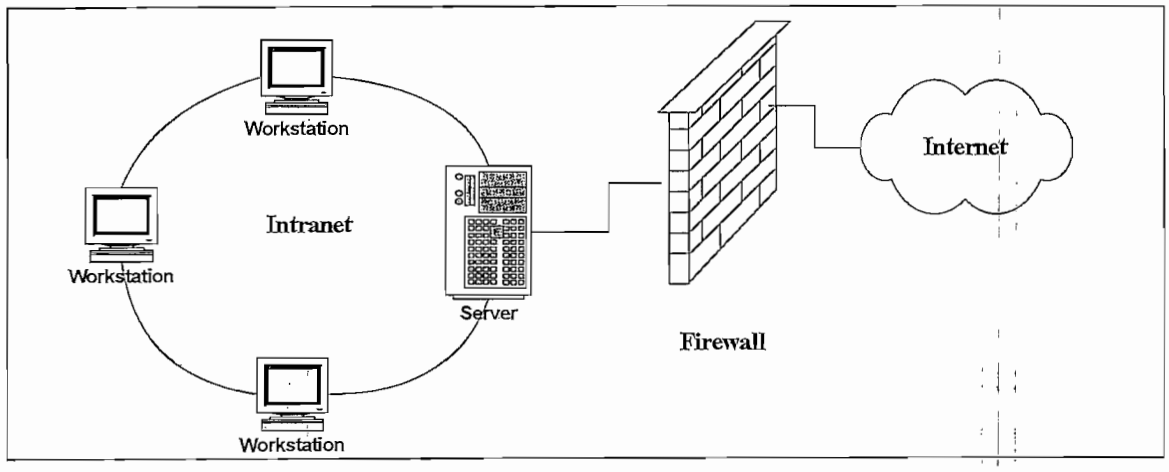


***Figura 1.3** Intranet con acceso al Internet [3]*

Una Extranet no es totalmente pública, por lo tanto es necesario identificar cuál es la información externa y cuál es la información interna.

La Extranet tiene mucho en común con la Intranet, aunque esta última haya sido definida con el propósito de dar servicio al interior de una compañía, su semejanza está en que las dos utilizan el *Word Wide Web* para satisfacer las necesidades de comunicación organizacional, sea interna o externa. La línea que diferencia la comunicación interna de la externa comienza a desaparecer pues hoy en día las organizaciones deben comunicarse tanto a nivel interno (miembros de la compañía) como externo (clientes y proveedores).

En la tabla 1.1 se muestran las diferencias de Intranet, Internet y Extranet.

	INTRANET	INTERNET	EXTRANET
Tipo de acceso	Privado	Abierto	Controlado
Usuarios	Miembros de la organización	Público	Socios de negocios
Tipo de información	Propietaria	General	Seleccionada

***Tabla 1.1** Diferencias entre Intranet, Internet y Extranet*

1.6 SERVICIOS BRINDADOS POR UNA INTRANET

Los servicios principales proporcionados por una Intranet son:

1.6.1 SERVICIOS DE CORREO

La Intranet brinda una magnífica oportunidad para implantar el servicio de correo. En primer lugar, se selecciona un paquete de correo que admita mensajes basados en navegadores de Internet, como: *Outlook Express* o Pegasus[6] . Si se opta por un paquete de correo comercial, se debe instalar SMTP[7] para el intercambio de correo entre la red y los clientes Internet. Estos servicios residirán en plataformas de servidores compartidos o dedicados.

1.6.2 SERVICIOS DE ARCHIVOS

Este servicio permite que un usuario de cualquier lugar de Internet establezca una sesión con un servidor de archivos y descargue la información que éste contiene.

[6] PEGASUS: Es un sistema de gestión de correo electrónico que puede utilizarse a nivel de usuarios individuales o en redes

[7] SMTP: *Simple Mail Transfer Protocol* permite el intercambio de correo electrónico

Se debe indicar que si se dispone de una red y un servidor dedicado, implícitamente ya se está suministrando un servicio de archivos.

1.6.3 SERVICIOS *WEB*

En este contexto se debe decidir si los servicios *Web* serán suministrados desde un servidor *Web* dedicado o desde un servidor de archivos existente. Se tendrá que optar por un servidor determinado, y esta elección influirá decisivamente sobre la selección de los paquetes de software asociados. Incluso puede ser necesario dotar al servidor de más espacio en disco y más memoria.

1.6.4 SERVICIOS DE AUDIO

Una de las ventajas que ofrece una Intranet es su amplio ancho de banda fiable y siempre disponible, esto permite contar con servicios en la Intranet que normalmente no se tiene en Internet. Uno de ellos es el servicio de audio, que puede incluir música o extractos de conferencia de la empresa.

Los servidores de audio acondicionan el hardware y el sistema operativo que puede manejarse, por tanto, si la elección del servicio de audio es un aspecto importante en la Intranet, deberá reconsiderarse el tipo de servidor seleccionado o añadirse una máquina dedicada.

1.6.5 SERVICIOS DE VÍDEO

Este servicio no está limitado en la Intranet por los condicionantes de ancho de banda, que sí se los tiene en Internet.

Los servidores de vídeo requieren más potencia que los servidores *Web* tradicionales y deben implementarse en una máquina dedicada. La capacidad de almacenamiento de un servidor de vídeo será también importante en el proceso de selección ya que los vídeos *clips* son archivos de gran tamaño. Un servidor de vídeo impone ciertas restricciones al hardware y al sistema operativo que se utilizarán. Si los servicios de vídeo se consideran suficientemente importantes en

la Intranet, se tendrá que analizar nuevamente la selección de los componentes o añadir un servidor dedicado con este propósito.

1.7 COMPONENTES DE UNA INTRANET

Para establecer una Intranet se necesitan los siguientes componentes:

HARDWARE

- Una red de computadoras para compartir recursos.

SOFTWARE

- Un sistema operativo de red que soporte el *stack* de protocolos TCP/IP
- Un software servidor que soporte solicitudes de protocolo de transferencia de hipertexto (http).
- Sistema operativo de computadoras cliente de escritorio, que ejecuten software, capaz de enviar y recibir paquetes de datos TCP/IP
- Software de *browsers* para computadoras cliente

En tabla 1.2 se muestran los componentes de una Intranet

Además de estos requerimientos de software y hardware, se debe conocer la forma de crear documentos en lenguaje HTML, los cuales permiten generar, editar y registrar el contenido de la Intranet.

COMPONENTES	OPCIONES
Navegadores *Web*	*Netscape Navigator, Internet Explorer*
Máquinas clientes	IBM, Compaq, *Macintosh*, etc.
Software para servidor Web	*Netscape Enterprice, Microsoft IIS, Apache*,etc
Protocolo de red	TCP/IP
Sistemas Operativos de red	*Unix, Windows* NT, *Netware*, Solaris, Aix,etc
Hardware para servidores	SUN, IBM, DELL, etc
Red física	Estrella, bus, anillo

***Tabla 1.2** Componentes de una Intranet [1]*

1.7.1 RED DE COMPUTADORAS

El primer requerimiento para establecer una Intranet es contar con una red de computadoras. La red es una colección de computadoras usualmente conectadas por cables; hoy en día, la mayoría de redes de computadoras son redes de área local (LAN), las cuales se encuentran dentro de un edificio. La mayor parte de las LAN se basan en el modelo cliente servidor, el cual usa una computadora central dedicada, llamada servidor para satisfacer las solicitudes del cliente (figura 1.4).

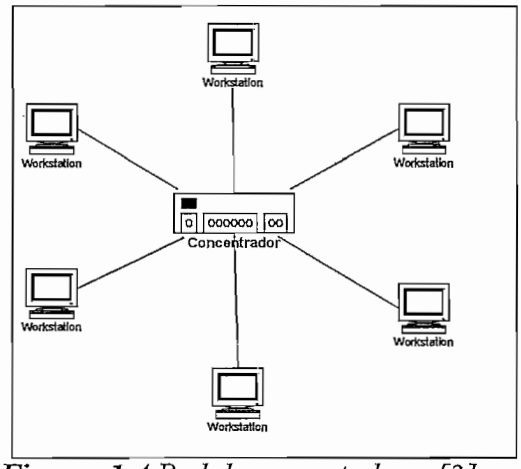


Figura 1.4 *Red de computadoras[3]*

a. Modelo cliente servidor

Una conexión de red consiste de dos computadoras que se comunican, así como la ruta entre ellas. El modelo computacional cliente servidor divide la comunicación de red en dos partes: la del cliente y la del servidor. Por definición el cliente solicita información o servicios del servidor y el servidor a su vez, responde las solicitudes del cliente. En muchos casos, cada parte de una conexión cliente servidor puede realizar ambas funciones. La figura 1.5 muestra un modelo de red cliente servidor.

Una aplicación servidor por lo general se inicializa a sí misma y después entra en reposo, empleando mucho de su tiempo simplemente en esperar una solicitud de una aplicación cliente.

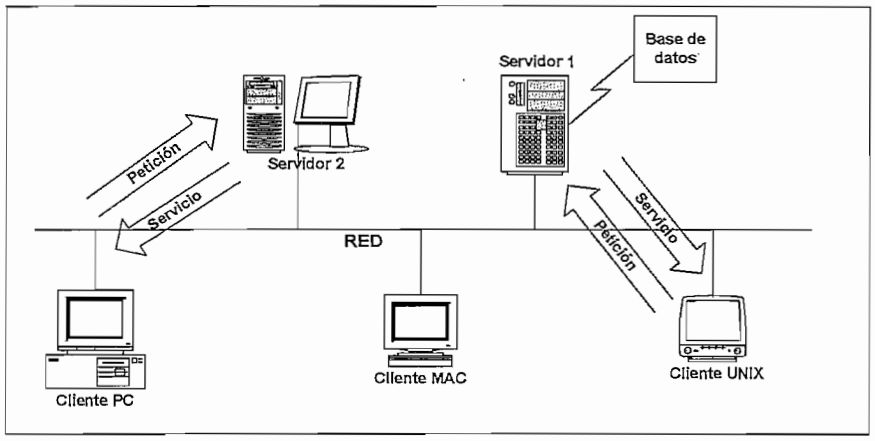


Figura 1.5 *Modelo de red Cliente – Servidor [3]*

El elemento básico de una red de cómputo es su conexión física de red que une entre sí a las computadoras a la red. Las topologías más comunes para la conexión física de las computadoras son: en bus, estrella y en anillo.

b. Creación de una red de cómputo

Para crear una red de cómputo se debe seleccionar varios componentes de red que determinarán el software y hardware que se pueden usar en la Intranet.

Para la conexión física entre computadoras, se necesita una tarjeta física de interfaz de red la cual reside en la computadora y presenta un interfaz en el que se puede insertar el cable de red. El tipo de tarjeta de red, establece el tipo de tecnología que se puede emplear.

La tecnología de red establece las reglas básicas para el uso de datos y regula el flujo de los mismos administrando la comunicación entre las computadoras de una red.

Las computadoras básicas en una red son los servidores que corren el sistema operativo de red y controlan la manera en que las computadoras de la red comparten los servicios del servidor. La carga (número de usuarios y tráfico en la red) del servidor de la Intranet influye en la selección de un tipo específico de procesador.

1.7.2 SOFTWARE DE SISTEMAS OPERATIVOS

a. Software de sistema operativo de red

Para que una serie de protocolos funcione adecuadamente y transfiera datos entre computadoras de una red, la red de cómputo debe correr un software especial llamado sistema operativo de red.

Los sistemas operativos de redes más difundidos son: Windows *Server* de *Microsoft* y *Linux.*

El sistema operativo de red controla la operación de un servidor, y hace uso de uno o más protocolos de red para transferir datos a y desde sus clientes.

b. Software de sistema operativo cliente

Las computadoras cliente pueden correr una gran variedad de sistemas operativos,
entre los que están Windows XP, 2000 y diversas versiones de los sistemas operativos de *Unix*. Para que el sistema operativo cliente pueda hacer uso de la red, se deben instalar controladores especiales que permitan a la tarjeta de interfaz de red de la computadora cliente comunicarse con la red.

c. Software para servidores *Web*

Las intranets se basan en el modelo de cómputo cliente servidor. Para disponer de una Intranet operativa, se debe contar con software servidor capaz de manejar solicitudes de los visualizadores, en la figura 1.6 se muestra el manejo de una solicitud de un visualizador *Web* por parte de un servidor para acceder a una página HTML estática.

En gran medida, la selección de un servidor *Web* de una Intranet es similar al de un servidor *Web* para un sitio de Internet; sin embargo, los servidores de Internet deben manejar una gran cantidad de solicitudes diarias y ocuparse de las cuestiones de seguridad. Por el contrario la mayoría de los servidores de Intranets empresariales no tendrán inicialmente tanto tráfico como los servidores de Internet.

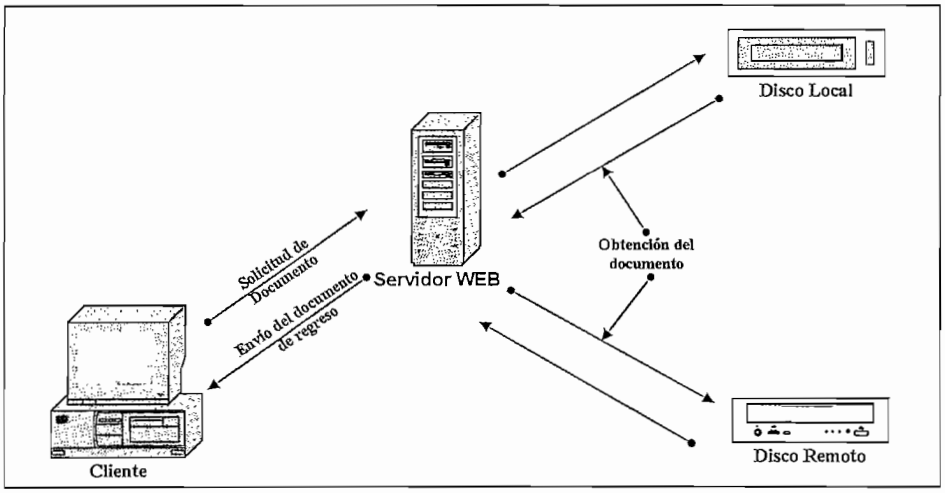


Figura 1.6 Respuesta de un servidor Web a la solicitud de un visualizador [3]

En consecuencia, primero se puede crear la Intranet con servidores fáciles de usar y mantener, para después transitar a servidores de alto rendimiento cuando el uso de la Intranet se incremente. A menudo, el desempeño de la Intranet depende más del desempeño de la máquina servidor que del software instalado en él. El software más utilizado actualmente es el Apache.

1.8 ADMINISTRACIÓN DE RED

El término administración de red es definido como la suma total de las políticas y procedimientos que intervienen en la planeación, configuración, control y monitoreo de los elementos que conforman una red, con el fin de asegurar el empleo eficiente y efectivo de sus recursos. La eficiencia de la red se verá reflejada en la calidad de los servicios ofrecidos.

A continuación se analizarán las áreas funcionales que se deben aplicar en la administración de red.

1.8.1 ADMINISTRACIÓN DE LA CONFIGURACIÓN

Las actividades ubicadas dentro del proceso de administración de la configuración son: planeación y diseño de la red, instalación y administración del software, administración de hardware, y el aprovisionamiento.

a. Planeación y diseño de la red

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

b. Selección de la infraestructura de red

Esta selección se debe realizar de acuerdo a las necesidades y a la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo. Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben estar sujetos todos los equipos que pretendan ser adquiridos.

c. Administración de hardware

Es la actividad responsable de mantener un registro detallado del hardware existente en la Intranet, así como de llevar un registro de los mantenimientos realizados.

d. Administración del software

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, mantiene un control sobre los programas que son creados para obtener información específica en los dispositivos.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son elementos que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de archivos.

e. Aprovisionamiento

Esta tarea tiene la función de asegurar los respaldos del software y la redundancia de los elementos de hardware más importantes de la red. Puede

llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, proporciona elementos físicos tales como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como por ejemplo versiones de sistema operativo, parches y aplicaciones. Además establece recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

f. Políticas y procedimientos relacionados

En este apartado se recomienda plantear, entre otros, los siguientes procedimientos y políticas:

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

1.8.2 ADMINISTRACIÓN DEL CONTENIDO

Integrar un sistema que proporcione administración del contenido de las páginas *web es* parte importante en el plan de la Intranet.

En la siguiente lista se identifican las tareas para la administración de contenido:

- Los usuarios deben tener la posibilidad de incorporar nuevos contenidos.
- Los usuarios deben tener la posibilidad de proteger su contenido contra cambios de otros usuarios.
- Los usuarios deben contar con un medio para actualizar el contenido ya existente.
- La Intranet debe disponer de un proceso de aprobación de contenido.
- La Intranet debe ofrecer un medio para controlar las revisiones de documentos, especialmente de documentos compartidos y además un medio sencillo para que los usuarios hagan pruebas con sus páginas *web*

Al formular políticas y procedimientos para el sistema de administración de contenido se debe identificar y asignar responsabilidades en todas las fases del proceso de desarrollo.

1.8.3 ADMINISTRACIÓN DEL RENDIMIENTO

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo; esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 3 etapas: monitoreo, análisis e interacción con otras áreas.

a. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red.

Se considera importante el uso de un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

b. Análisis

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

c. Interacción con otras áreas

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red, si se detecta saturación en los enlaces o un tráfico excesivo generado por o hacia un solo elemento se relaciona con la administración de seguridad, se vincula con la administración de la configuración cuando se realizan modificaciones en la

CAPÍTULO I
Ingeniería en Electrónica y Telecomunicaciones

configuración de algún dispositivo al momento de presentarse una falla que atente contra el rendimiento de la red.

1.8.4 ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y

configuración de algún dispositivo al momento de presentarse una falla que atente contra el rendimiento de la red.

1.8.4 ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases:

- *Monitoreo de alarmas.* Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- *Localización de fallas.* Determinar el origen de una falla.
- *Pruebas de diagnóstico.* Diseñar y realizar pruebas que apoyen la localización de una falla.
- *Corrección de fallas.* Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

1.8.5 ADMINISTRACIÓN DE LA CONTABILIDAD

Es el proceso de recolección de información para determinar los recursos utilizados por los elementos de la red, desde los equipos de interconexión hasta usuarios finales.

Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso es también llamado tarificación.

1.8.6 ADMINISTRACIÓN DE LA SEGURIDAD

Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso es también llamado tarificación.

1.8.6 ADMINISTRACIÓN DE LA SEGURIDAD

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red, así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

Una vez instalada la Intranet y en operación se debe concentrar esfuerzos en el mantenimiento del contenido y la capacitación de los empleados. La estrategia de actualización y mantenimiento del contenido es parte del sistema de administración de documentos, pero también se debe seleccionar responsables del contenido, que son individuos de diferentes departamentos o grupos encargados de la creación y mantenimiento del contenido específico

La responsabilidad global de la creación y el mantenimiento de servidores y servicios de la Intranet, recae en el administrador *Web*. El *Webmaster* es la persona o personas, cuya misión es instalar y mantener el sitio *Web* interno o externo de una empresa.

1.8.7 EL *WEBMASTER*

El *Webmaster* se encarga de mantener un buen funcionamiento de los servicios suministrados por la Intranet. Además, es responsable de la actualización del contenido de los sitios *Web* y de la permanente puesta al día en cuanto a nuevas tecnologías y sitios *Web* se refiere.

Las funciones del *Webmaster* pueden dividirse en relativas a la administración física y a la administración lógica. La administración física se aplica sobre el hardware del servidor *Web* y las tareas relacionadas que se requieren para mantener en buen estado tanto al servidor como a los servicios que ofrece. También se refiere a la infraestructura de la red en la que se incluyen las

estaciones de trabajo clientes y cualquier otro servicio de pasarela (anfitriones y dispositivos de acceso a Internet). En la administración lógica se contempla la seguridad de la Intranet, la creación y la dotación de contenidos del sitio *Web*. El esquema de direccionamiento TCP/IP y la administración de protocolos forman también parte de estas responsabilidades.

En la figura 1.7 se muestra el papel del *Webmaster* en la compañía.

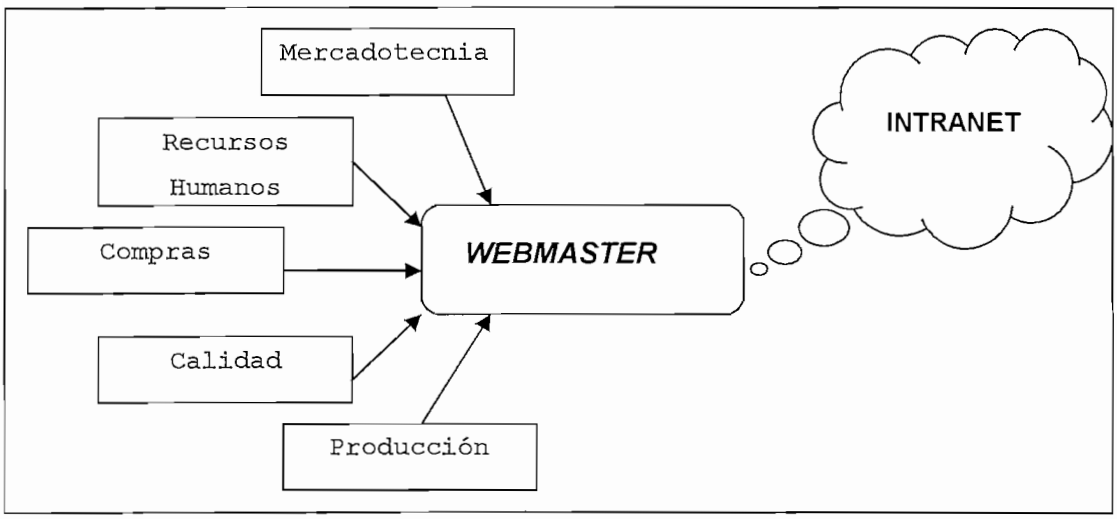


***Figura 1.7** Papel del Webmaster en la compañía.[1]*

1.9 SEGURIDADES DE INTRANET

La proliferación de Internet ha causado que una gran cantidad de empresas y organizaciones hayan conectado su red local a Internet, de forma no segura.

Más allá de la protección de la Intranet a través de un *firewall* o de otros dispositivos que limitan el acceso, están los siguientes aspectos claves:

- Seguridad integral de la Intranet y la conexión a Internet
- Procedimientos de seguridad, que no pasen por alto la seguridad física y los procedimientos de acreditación de empleados, socios y subcontratados.
- Gestión integral de la seguridad

- Una visión de la seguridad que abarque desde los servidores *Web* a los servidores de correo pasando por los servidores departamentales y las aplicaciones corporativas.

1.9.1 SEGURIDAD INTERNA

a. Amenazas internas

Los problemas de seguridad interna son probablemente los más comunes; usuarios de confianza con ciertos niveles de acceso a sistemas y hardware, pueden convertirse en la mayor amenaza si no se los monitorea cuidadosamente. El chequeo cuidadoso del ambiente referencia y trabajos anteriores, ayudará a prevenir el aparecimiento de una serie de amenazas

HARDWARE

El primer componente en el sistema de cómputo es el hardware que usa. Las amenazas más comunes son:

- Robo de computadora, impresora u otro recurso
- Interferencia de parte de un empleado descontento que puede causar daño en algún *switch* o inclusive cortar algún cable
- Destrucción de recursos por fuego, inundación o problemas eléctricos
- Desgaste y deterioro normal de los equipos. Este problema se puede disminuir con un programa de mantenimiento preventivo

SOFTWARE

El segundo componente del sistema es el software y las amenazas a éste son:

- Borrado de un programa sea por accidente o por intento malicioso
- Robo de un programa por parte de un usuario.
- Corrupción de un programa ya sea por falla de hardware o por virus.

1.9.2 SEGURIDAD EXTERNA

Para comprender los problemas y las vulnerabilidades que pueden presentarse en una red, primero se debe entender exactamente el término invasor o intruso denominado comúnmente *hacker*[8]. Este término actualmente se refiere a quien obtiene un acceso no autorizado a los sistemas de computación especialmente a aquellos que acceden remotamente.

Las compañías frecuentemente fallan en detectar incidentes en las seguridades de sus redes debido a que los sistemas administradores de la red no examinan el ingreso de los usuarios y no detecta la violación de las seguridades.

a. Amenazas externas

Algunas de las violaciones más frecuentes que se realizan a una red son:

Ataques basados en *passwords*

Una de las infiltraciones más comunes es averiguar la combinación correcta del nombre de usuario y el *password* y de esta manera ingresar a la red.

Algunas veces se logra conocer los *passwords* mediante el acceso a los correos electrónicos o por medio de la localización de los reportes de *passwords*. A veces se usa servicios como el TFTP[9] o el FTP[10] para acceder remotamente a los sistemas y obtener el archivo de *passwords* que aunque está encriptado puede descifrarse.

Ataques que utilizan el acceso del sistema operativo

Algunos sistemas operativos incluyendo Unix y Windows Server han diseñado sus sistemas de acceso con el fin de facilitar la interconectividad a otros sistemas o dominios. Para los sistemas conectados a Internet se suele permitir archivos denominados *trusted* que contienen los nombres de los servidores y algunas direcciones importantes y cualquier usuario de la organización podría acceder a

[8] *Hacker:* pirata informático capaz de entrar en sistemas cuyo acceso es restringido
[9] TFTP: *Trivial File Transfer Protocol*
[10] FTP: *File Transfer Protocol*

ellos sin necesidad de una contraseña; por tanto un intruso que adivine el nombre de un *host* podría tener acceso a los archivos *trusted*.

IP *SPOOFING*

Spoofing significa proveer una información falsa acerca de la identidad de una persona o de un *host* para obtener un acceso no autorizado a los sistemas o a los servicios que éstos poseen.

El primer paso consiste en identificar las dos máquinas que se atacará, entonces el intruso intentará establecer la conexión con la máquina B de manera que ésta crea que ha establecido la conexión con la máquina A cuando verdaderamente la máquina con la que se ha conectado es la máquina X del intruso. Este acoplamiento es creado por un mensaje de la máquina X que contiene la dirección origen de A.

La mejor defensa para este tipo de ataque es configurar los *routers* para rechazar algún paquete que sea enviado desde afuera de la red.

Robo de sesión

Este es un caso especial de *IP spoofing.* Aquí el intruso busca la existencia de una conexión entre dos servidores e intenta tomarlos. Luego de burlar el control del *firewall* el intruso verifica el funcionamiento de la red, de esta manera es capaz de determinar las secuencias de números usadas por las dos partes sin que los procesos que se están ejecutando en ese momento se detengan. Al tener analizada la conexión, el intruso puede generar un tráfico que aparentemente viene desde los dos servidores, "robando la sesión" desde uno de los dos individuos involucrados; hecho esto el intruso obtiene todos los privilegios de acceso como un usuario legítimo, y mientras el usuario verdadero es borrado de la conexión, el intruso puede seguir trabajando como un usuario.

Protegerse contra este tipo de ataque es muy difícil, aún la más efectiva autenticación no siempre es la más efectiva, podría mejorarse la protección de los

routers y *firewalls* removiendo por defecto cuentas que sean innecesarias, pero la mejor forma de protegerse sería el diseño de un sistema de encriptación.

Ataques a librerías compartidas

Algunos programas a menudo leen librerías compartidas y las ejecutan. Una técnica de los *hackers* es la de reemplazar los programas compartidos por otros programas con el propósito de tomar ventaja sobre ellos. Al reemplazar estos programas los *hackers* pueden dar acceso a la red a la persona que desean o pueden ejecutar programas que llamen a las librerías compartidas.

El mejor método de controlar este tipo de problema es el chequeo periódico de las librerías compartidas.

1.9.3 CORTAFUEGOS O *FIREWALLS*

El uso principal de los *firewalls* es el de prevenir ataques externos a la Intranet; su propósito es controlar daños o proteger a la red de un acceso no autorizado, pero su uso más general es regular el flujo de tráfico entre dos redes, es decir, mantener a los intrusos fuera del alcance de los trabajos que se realizan en la red. Los *firewalls* son instrumentos efectivos para implementar un control de acceso a la red; proveen protección contra ataques de protocolos individuales o aplicaciones, pueden ser efectivos contra ataques *spoofing* y son relativamente flexibles en su configuración por que proveen diferentes restricciones para cada tipo de tráfico de red.

Una de las mayores ventajas de los *firewalls* es proveer un solo punto dentro de la red para controlar la seguridad. Además proveen de un punto de administración puesto que es un lugar de restricciones para los servidores y se constituyen en un buen medio para el monitoreo de tráfico.

Algunos *firewalls* solamente permiten tráfico de correo a través de ellos de modo que protegen a la red de cualquier ataque distinto al de un servicio de *e-mail*. Otros *firewalls* proporcionan menos restricciones y bloquean servicios conocidos por sus constantes problemas de intrusión.

De la misma forma como el *firewall* presenta el único punto para la seguridad de la red, si éste es violado, la seguridad de todo el perímetro es rota y un intruso podría tener acceso a toda la red de la compañía. Por esta razón los *firewalls* más fuertes están compuestos de múltiples bloques de seguridad.

Los *firewalls* son también un sistema de seguridad a la hora de controlar estadísticas de usuarios que intentaron conectarse a la red y no lo consiguieron, el tráfico que atraviesa la misma, etc.

El uso más sencillo de los *firewalls* consiste en crear un "sitio interno", accesible sólo para los ordenadores pertenecientes a la red local. Para ello solo se requiere introducir el servidor, dentro del *firewall* (figura1.8).

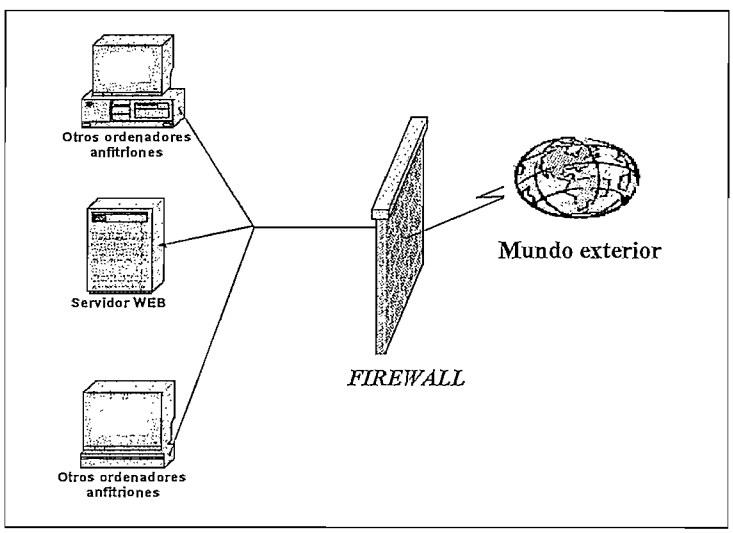


Figura 1.8 *Red local protegida por un firewall[1]*

Sin embargo, si se pretende poner el servidor a disposición de usuarios de todo el mundo será preciso situarlo fuera del *firewall*. Desde el punto de vista de la seguridad de la organización como conjunto, el lugar más seguro sería totalmente fuera de la red de área local (figura 1.9).

Esta configuración se conoce como "zona desmilitarizada" (DMZ), ya que el servidor queda como víctima, a expensas de ataques del exterior mientras el cortafuegos protege la seguridad de la red interna.

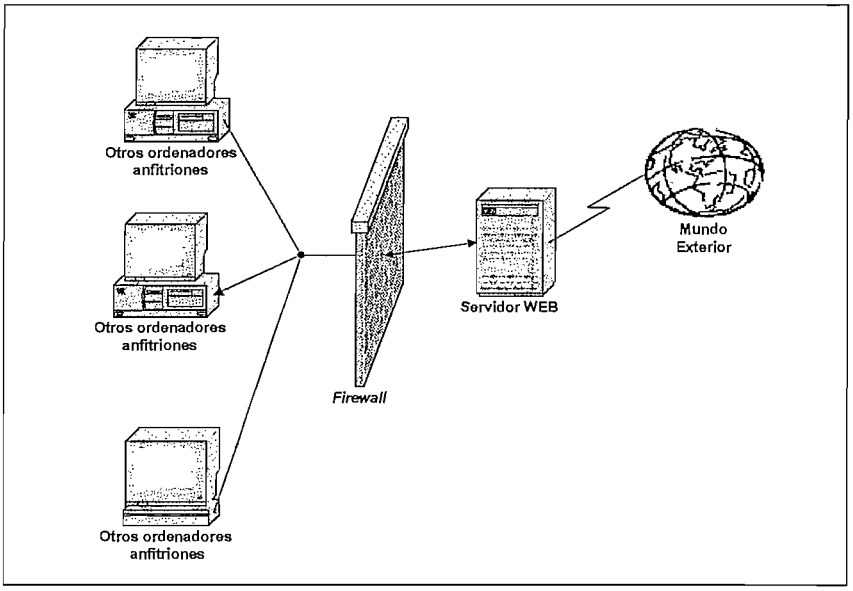


Figura 1.9 *Firewall que separa a una red de su servidor Web actuando así como protector de la red local[1]*

No es aconsejable trabajar con el servidor *Web* dentro del *firewall*; si se actúa así, cualquier fallo del servidor podría comprometer la seguridad de toda la organización.

Existen múltiples variantes de esta estructura básica alguna de las cuales incluyen arquitecturas con servidores internos y externos para permitir acceso universal a la información pública y al mismo tiempo mantener el acceso por red interna a los documentos privados.

Limitaciones

Contrario al pensamiento general, los *firewalls* no son la solución para todos los problemas de seguridad en una red. Los *firewalls* no pueden proteger a la red de ataques que se produzcan por caminos distintos al del *firewall* instalado; por ejemplo, una organización que posee datos clasificados no necesita un *firewall*, si no más bien puede optarse por no conectarse a Internet o se requiere el aislamiento de estos datos de la red corporativa.

Entre las tareas que los *firewalls* no pueden responder se tiene:

a. Integridad en los datos

Mientras los *firewalls* proveen indirectamente la integridad sobre algunos datos de la red, para evitar los ingresos no autorizados, muchas empresas usan los *firewalls* para protegerse de los virus. La verificación de todo el tráfico que ingresa para buscar un virus, demanda mucho tiempo y resulta casi imposible chequear cada archivo binario para analizar los virus conocidos.

La única forma real para chequear los virus que ingresan a la red, es la restricción del lugar de origen de los datos, verificarlos fuera de la línea y solo entonces enviarlos al usuario deseado.

b. Autentificación del origen de los datos

Un *firewall* solo tiene la posibilidad de mirar un paquete, este control sirve para verificar cómo fue creado el paquete. Una de las mayores inseguridades con TCP/IP es que se puede generar un mensaje con otra identidad.

c. Confidencialidad de los datos

A pesar de que la mayoría de proveedores de *firewalls* activan el tráfico encriptado entre dos *firewalls* esta capacidad requiere que cada red con la que se está comunicando tenga instalado el mismo tipo de *firewall*.

d. Protección contra ataques internos

El mejor *firewall* puede proteger a la red de un ataque de Internet pero no considera ningún ataque desde el interior. Es evidente que de nada sirve la instalación de un *firewall* si existen personas dentro de una organización que se dedican a pasar información a empresas competidoras.

Para mejorar la seguridad en la red se puede utilizar un *firewall* en conjunto con un servidor *proxy*, que proporcionará una puerta controlada, a través del *firewall* y hacia afuera de la red externa desprotegida.

1.9.4 SERVIDORES *PROXY*

Un servidor *Proxy* es una aplicación que media en el tráfico producido entre una red protegida e Internet. Se utilizan a menudo como sustitutos de los *routers,* controladores de tráfico, para prevenir directamente el tráfico que pasa entre las redes. La figura 1.10 muestra el funcionamiento del servidor Proxy.

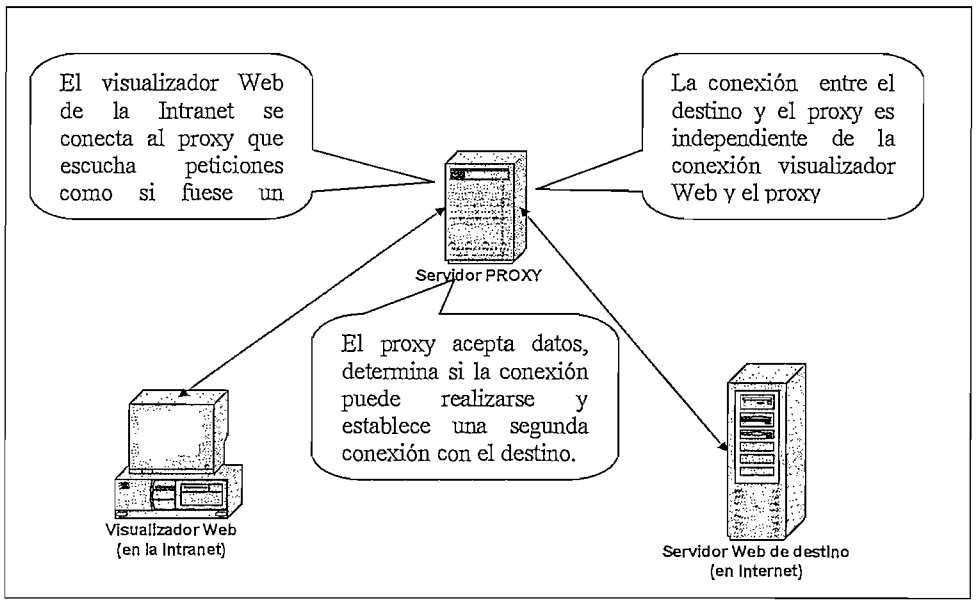


***Figura 1.10** Servidor Proxy [7]*

Un *Proxy* debe entender el protocolo de la aplicación que está siendo usado aunque también puede implementar protocolos específicos de seguridad.

Los servidores *proxy,* son aplicaciones específicas, cuyo proceso de conexión es el siguiente:

1. El usuario hace la conexión con el *proxy*
2. Aparece un menú que indica el lugar al cual quiere dirigirse.
3. El *proxy* consulta la lista de lugares permitidos para este usuario, en caso de no constar en ella, niega la conexión.

Ventajas

1. No requiere que los usuarios tengan acceso al sistema operativo, mediante este sistema pocas personas pueden acceder al mismo por lo que es difícil que se ingrese dentro de alguna máquina.
2. No requiere hacer algunas conexiones para llegar al destino.
3. Ofrece al usuario la ilusión de estar conectado directamente con el destino, de esta manera no es necesaria la transferencia de información entre el servidor y el *proxy*.
4. Oculta al *host* interno al que se quiere llegar.

Limitaciones

Existen dos limitaciones en un servidor *proxy:*

Una limitación del p*roxy* es que existe la posibilidad de que las páginas recuperadas de la memoria *cache* no estén actualizadas.

Por otro lado este tipo de aplicaciones servidores *proxy* requieren uno por cada tipo de aplicación, tales como *proxys* para TFTP, Telnet, HTTP y otras. Encontrar *proxys* que ofrezcan todos estos servicios resulta una tarea difícil; si un *proxy* no está disponible para algún servicio la solución al problema podría ser el uso de un *proxy* genérico.

Diferencias entre firewall y proxy

Un *firewall* funciona con cada uno de los paquetes. Sólo controla el tráfico de paquetes y reacciona de acuerdo con las reglas que se le da, no tiene en cuenta el contenido de los paquetes.

El *firewall* trabaja a nivel de capa 4, mientras que el *proxy* lo hace a nivel de capa aplicación.

1.10 EL FUTURO DE LAS INTRANETS

Los aspectos tecnológicos de una Intranet no son difíciles de entender; sin embargo, la tecnología de la Intranet y la información tecnológica en general, cambia tan rápidamente que mantenerse al día con las últimas soluciones de hardware y software requiere de un departamento a tiempo completo. Compañías tales como *Netscape* y *Microsoft*, están desarrollando rápidamente tecnologías clave de Intranet. Muchas compañías pronto comprenderán que transformar una Intranet estática utilizada para la edición HTML a una Intranet dinámica e interactiva es un gran reto. Los retos técnicos más importantes que enfrenta cualquier organización después de la puesta en marcha inicial de una Intranet son:

- Cómo convertir los documentos existentes en papel a documentos electrónicos para que puedan ser accedidos electrónicamente a través de una Intranet.
- Cómo conectar bases de datos existentes a la Intranet para ser accedidas por una amplia gama de plataformas de computación tales como: sistemas basados en Windows y MAC.
- Cómo mejorar de manera continua las características y capacidades de una Intranet para mantener a los empleados motivados en cuanto a su utilización.
- Cómo instalar múltiples servidores a través de varios departamentos.

Los paradigmas de Intranet y la aparición de la Extranet probablemente serán la plataforma de información de la próxima década. Las compañías que comprenden claramente sus propios "cuellos de botella" y adquieran tecnologías de Intranet apropiadas serán capaces de aprovechar las nuevas oportunidades. Las oportunidades competitivas que se pueden asumir con cambio en las plataformas de la información no ocurren a menudo y ya están generando una gran cantidad de nuevos productos. Las compañías han de considerar cuidadosamente los productos apropiados para resolver sus problemas; además, la competencia y las nuevas posibilidades que surgen de las tecnologías de Intranet harán desaparecer a las compañías que no quieren participar o que esperan mucho para iniciarse.

CAPÍTULO II

INGENIERÍA DE DETALLE PARA EL DISEÑO DE LA INTRANET

INGENIERÍA DE DETALLE PARA EL DISEÑO DE LA INTRANET

Una Intranet es una red privada, que utiliza el stack de protocolos TCP/IP de Internet para su transporte básico. Las Intranets permiten a los usuarios trabajar juntos de un modo más sencillo y efectivo, permitiendo colaborar en proyectos y compartir información.

Este capítulo presenta el diseño de una Intranet para la Escuela Politécnica Nacional, la cual funcionará de forma independiente a la estructura de la Polired, detalla claramente cada uno de los elementos que la conforman, como son: topología y tecnología de red, diseño de la red pasiva con el respectivo proyecto de cableado estructurado. Se realiza también un estudio de las tecnologías de transmisión con el fin de elegir la más adecuada para la comunicación a Internet, así como también el análisis de la calidad de servicio brindado por los ISPs en la ciudad de Quito en base a los SLAs (acuerdos de calidad de servicio) a fin de elegir la mejor alternativa para la Intranet.

La sección 2.6 se estudian los diferentes sistemas operativos de red para servidores y usuarios con el objeto de elegir los más adecuados en base a las necesidades presentadas, se propone las diferentes configuraciones para todos y cada uno de los equipos de red.

La administración y seguridad de la red también son parámetros considerados por cuanto constituyen una parte fundamental del buen funcionamiento de la red y garantiza continuidad del servicio. Finalmente se realizan los proyectos complementarios para el diseño de iluminación e instalaciones eléctricas de la red.

En vista de los beneficios que brinda una Intranet, la institución educativa ha destinado un área de 180 m^2, ubicada en la terraza del Edificio Quimica-Eléctrica, espacio físico que será distribuido de la siguiente manera:

- Tres salones que brindarán acceso a Internet, uno de los cuales prestará adicionalmente servicios de vídeoconferencia; éstos cuentan con un área aproximada de 30 m^2 cada uno y alojarán en promedio 14 máquinas por salón
- Se contará con cuatro cabinas telefónicas, con un área de alrededor de 4 m^2
- Un área de aproximadamente 16 m^2 destinada para la administración de la red
- Un área de control de acceso al local, para la cual se destina 16 m^2
- Un espacio físico de 30 m^2 para otros servicios

La distribución del espacio físico se muestra en la figura 2.1

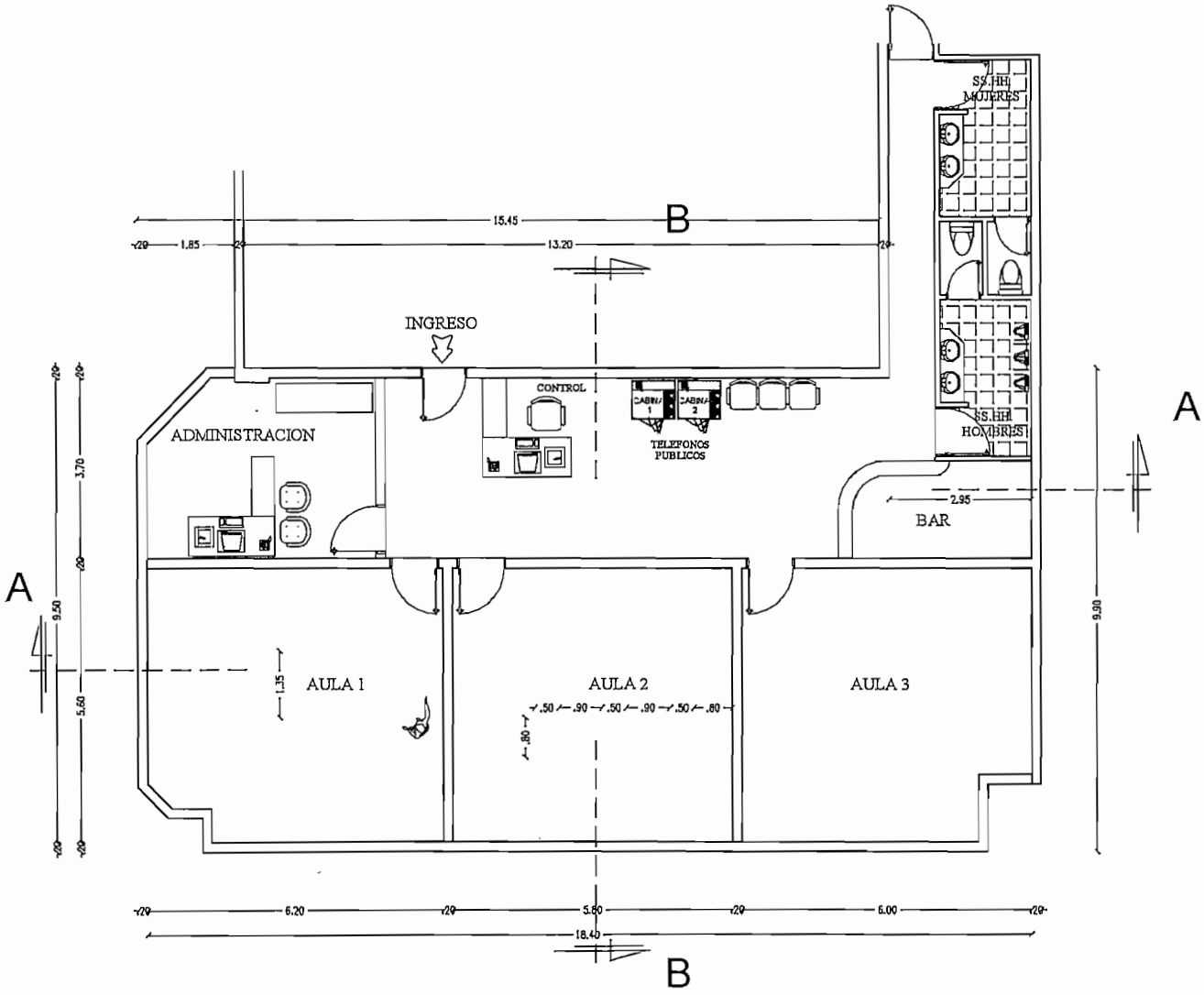
El buen desempeño de una Intranet depende en gran medida de la adecuada coordinación y buen funcionamiento de sus componentes; en vista de la diversidad de aspectos a tomarse en cuenta en el diseño, se plantean varios ítems referenciales que se indican en la figura 2.2, con el fin de lograr un entendimiento sistemático del presente proyecto.

El proceso de diseño de la red LAN, contempla la selección adecuada de la topología y tecnología a implementarse en base al análisis de requerimientos de usuarios y al tráfico que soportará la red, los cuales proporcionan pautas para la elección del enlace a Internet, que deberá considerar la calidad de servicio brindada por los ISPs[1].

El rendimiento máximo de la red no depende únicamente de su óptimo funcionamiento físico, sino también del nivel de seguridad y administración que se le pueda proporcionar y para ello se requiere la utilización de *routers, firewalls* y servidores correctamente configurados.

Sin duda los proyectos complementarios como: sistema eléctrico y de seguridad física garantizan una adecuada operación de la Intranet, por tanto son considerados parte del diseño.

[1] ISP: *Internet Service Provider* o Proveedor de Servicios de Internet



DISEÑO ARQUITECTONICO DE LA INTRANET

ESCALA :---------- 1:100

NOTAS TECNICAS Y SIMBOLOS

Escuela Politécnica Nacional

CARRERA
ING. ELECTRONICA Y TELECOMUNICACIONES

2004

TEMA:

DISEÑO DE UNA INTRANET PARA VOZ DATOS Y VIDEO SOBRE TCP/IP

FECHA: JULIO 2004	DIRECTOR:
HERRERA PAULINA	ING. PABLO HIDALGO
HIDALGO WENDY	ESCALA: 1:100
	LAMINA: 1/4

CONTIENE:

DISEÑO ARQUITECTONICO DE LA INTRANET

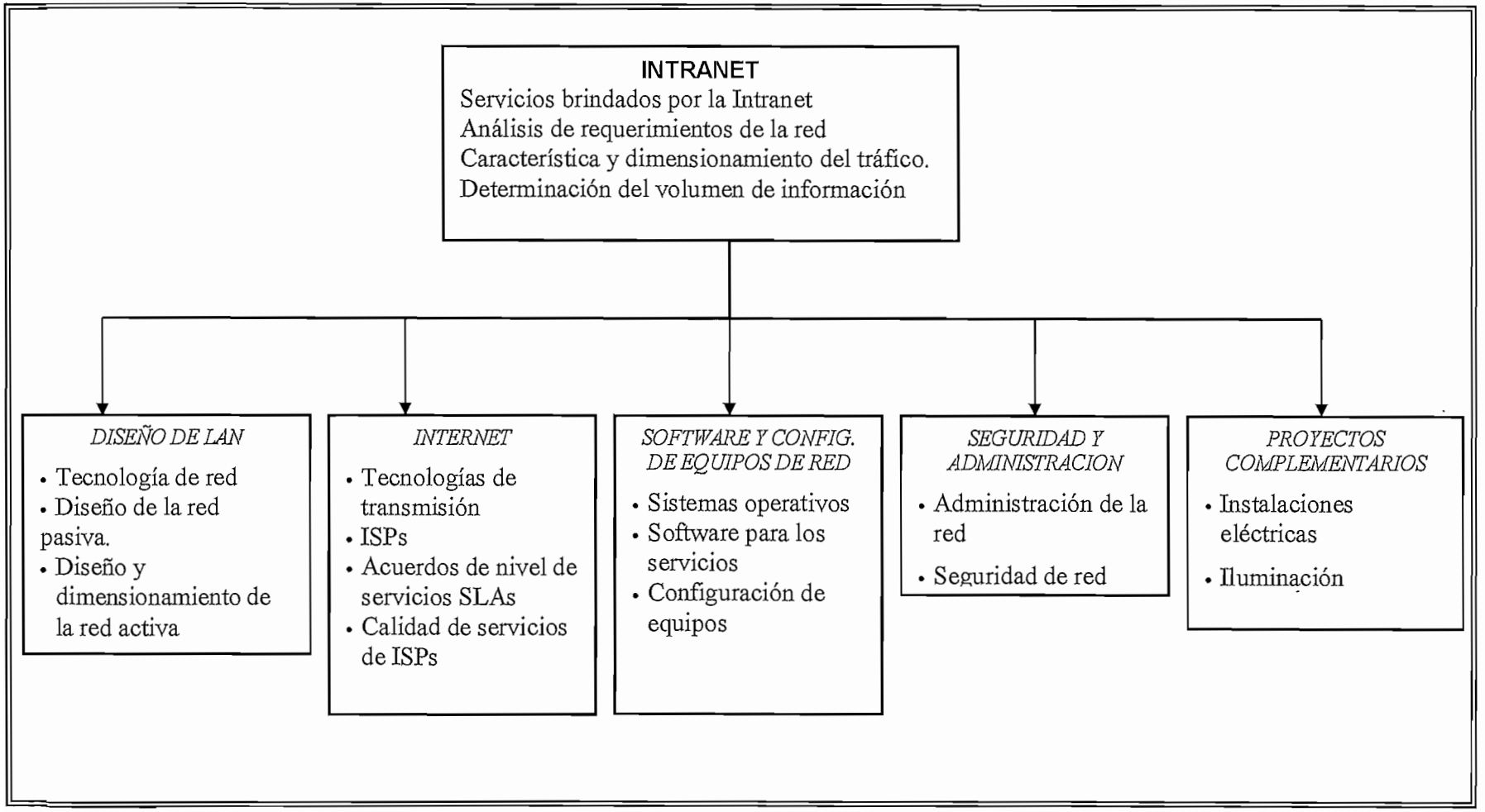


***Figura 2.2** Diagrama conceptual del diseño*

2.1 SERVICIOS BRINDADOS POR LA INTRANET

De acuerdo a los alcances planteados en el plan del proyecto de titulación la Intranet motivo de este estudio brindará los siguientes servicios:

2.1.1 SERVICIO DE INTERNET

La Intranet brindará servicios de calidad para el acceso a Internet con el objetivo de aprovechar todas las ventajas que ofrece esta red mundial al sector educativo.

Internet funciona con el modelo "Cliente/Servidor", lo que significa que en la red hay servidores que dan una información concreta en el momento que se solicite, y por otro lado están los clientes que piden dicha información.

La gama de servicios brindados por Internet son innumerables siendo los más usados: servicios de telefonía, vídeoconferencia, correo electrónico, w*orld wide web*, FTP, IRC, etc.

2.1.2 VOZ SOBRE IP (VoIP)

Al contar con una conexión de Internet se optimiza el uso de este recurso para la transmisión de voz digitalizada, lo cual permite reducir sustancialmente los costos de comunicación.

La voz que ingresa en el extremo receptor, se transforma por un programa en el computador o equipo del emisor, en pequeños paquetes de datos, que se transmiten por Internet empleando el mismo protocolo. Para hablar por Internet, existen varias alternativas:

De un PC a otro PC usando exclusivamente la red Internet
De un PC a un Teléfono normal que es lo más usual en VoIP
De un teléfono IP a otro teléfono IP
De un teléfono IP a un teléfono normal

Los dos últimos casos no requieren un PC. La comunicación es más directa y transparente.

En el caso de usar un PC, se requiere que el equipo tenga instalado un programa de telefonía IP como *Net2phone*, *MediaRingTalk* u otros similares y accesorios multimedia: tarjeta de sonido, micrófono y parlantes. Cada programa funciona con un determinado proveedor de telefonía IP.

Este proveedor se encarga de completar el circuito constituido por el PC, la red Internet, el *gateway*[2] en el punto final y la red telefónica normal en el mismo punto. La figura 2.3 muestra la estructura de una red VoIP.

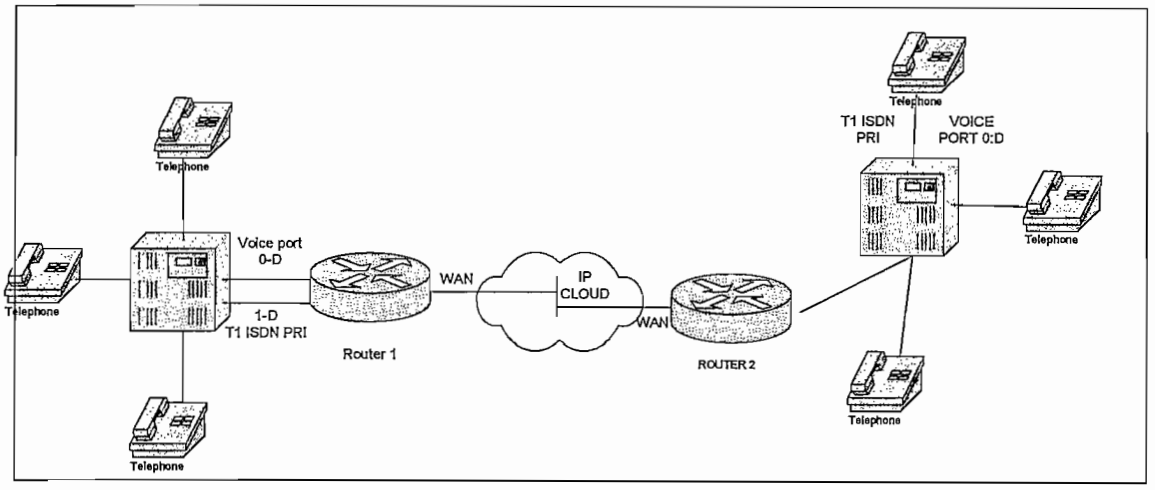


Figura 2.3 *Estructura de una red VoIP [34]*

Las cabinas telefónicas que brindarán este servicio en la Intranet para la Escuela Politécnica Nacional, utilizarán un ancho de banda de 17 Kbps por cabina y un contrato de intercomunicación con *Net2phone*, empresa autorizada para la transmisión de VoIP, la misma que permite comunicarse con cualquier lugar del mundo a través de su infraestructura de comunicación. Se plantea esta alternativa de solución, tomando en cuenta que a la fecha de realización del proyecto aún no existen reglamentos que normen el funcionamiento de VoIP en el Ecuador.

2.1.3 VÍDEOCONFERENCIA

Al contar con una conexión a Internet con suficiente ancho de banda se brindará también el servicio de vídeoconferencia de escritorio, que es esencialmente un computador con capacidades para vídeoconferencia. El vídeo de una localidad

[2] *Gateway:* Puerta de acceso a la red

remota aparece en el monitor de un computador de imagen en imagen (ver figura 2.4).

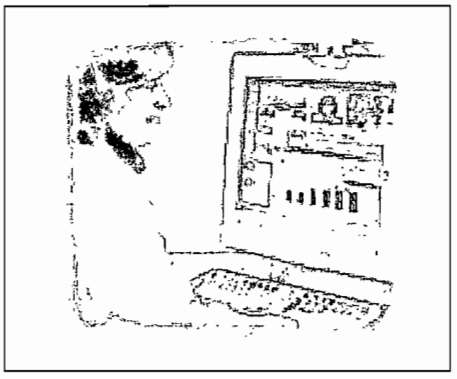


Figura 2.4 *Vídeoconferencia de escritorio [57]*

Una unidad de escritorio es usada para conferencias personales o de pequeños grupos de dos o tres participantes. Pueden ser utilizadas también para conferencias mediante Internet, pero con una baja calidad de imagen.

La mayoría de los sistemas de escritorio sólo trabajan con una velocidad de 128 Kbps, y algunos a 384 Kbps. Cabe mencionar que el ancho de banda requerido para la transmisión de vídeoconferencia, depende de la calidad de imagen y el servicio mismo brindado por el sistema; por ejemplo el envío de archivos o manejo de información crítica a través del mismo canal comunicación, demanda un mayor ancho de banda.

Existen estándares que permiten realizar estas aplicaciones utilizando una línea telefónica conmutada y un módem a 56 Kbps. Los sistemas considerados soportan los siguientes estándares:

- H.320 (comunicación sobre RDSI)
- H.323 (comunicación sobre TCP/IP)

Para proporcionar los servicios de vídeoconferencia y voz sobre IP, la Intranet a diseñarse utilizará el protocolo H.323 el cual se describe en el Anexo A.

Es necesario señalar que el ancho de banda utilizado para una sesión de vídeoconferencia sólo será utilizado cuando el usuario así lo requiera, caso contrario estará disponible para otro tipo de aplicaciones. Recalcando además que al momento de realizarse una sesión de vídeoconferencia todo el ancho de banda será utilizado para este efecto, es decir las máquinas de las salas no tendrán acceso a Internet en este lapso de tiempo.

2.1.4 SERVICIO DE CORREO ELECTRÓNICO

El correo electrónico permite enviar y recibir mensajes hacia y desde cualquier persona en el mundo con una dirección *e-mail*.

E-mail utiliza el protocolo *Simple Mail Transfer Protocol* (SMTP) para transportar correo a través de Internet. Los mensajes de *e-mail* normalmente son en modo texto, sin embargo también pueden incluir otros objetos y tipos de archivos. Para esto el cliente y el servidor deben soportar el protocolo *Multipurpose Internet Mail Extensions* (MIME).

Para este servicio se requiere de servidores de e-mail.

La Intranet contará con un servidor de *e-mail* que permitirá la creación y manejo de cuentas de *mail* de 10 MB, considerando que ésta es una capacidad razonable para el envío y recepción de mensajes.

2.1.5 SERVICIO DE *CHAT*

Internet Relay Chat (IRC) permite la comunicación con otra persona en un sitio diferente y es similar a una llamada telefónica, siendo la única diferencia el uso del teclado en lugar de un teléfono. IRC, mejor conocido como *chat*, ha sido uno de los servicios más populares de Internet. Normalmente el *chat* es usado con fines recreativos. Las personas pueden conversar de una gran variedad de temas a través de los foros de *chat*.

Los servidores dedicados de IRC son administrados por diferentes organizaciones alrededor del mundo, para soportar estos foros. El uso del *chat* puede ser con una o varias personas al mismo tiempo.

Los clientes de *chat* IRC pueden usar software como *Windows Messenger, Mirc, Yahoo Messenger, Tkirc, BitchX*, etc, de acuerdo al sistema operativo utilizado por el cliente.

Para este objetivo se contará con varias máquinas que dispondrán de una conexión de calidad a Internet.

2.1.6 SERVICIOS VARIOS

Adicionalmente la Intranet a diseñarse brindará el ingreso a computadores los cuales contarán con el hardware y software necesario para la realización de tareas y trabajos.

Igualmente no se dejarán de lado los servicios de impresión, *scanner*, y fax cuya finalidad es la de brindar todas las comodidades para la realización de tareas de la comunidad educativa.

2.2 ANÁLISIS DE REQUERIMIENTOS DE LA RED

Para que una LAN sea efectiva y sirva para las necesidades de los usuarios, debe diseñarse e implementarse de acuerdo con una serie de pasos sistemáticos planificados, que incluyen lo siguiente:

- Requisitos y expectativas de los usuarios
- Análisis de los requisitos
- Diseño de la estructura (es decir, la topología).
- Documentación de la implementación física y lógica

El primer paso para diseñar una red debe ser reunir datos acerca de la estructura de la organización. Esta información incluye el historial de la organización y su estado actual, el crecimiento proyectado, las políticas operativas y los procedimientos de administración.

En vista que esta Intranet es totalmente nueva e independiente de *la Polired no* se consideran datos históricos.

Es necesario también el análisis de los puntos de vista de las personas que utilizarán la red LAN y el contestar las siguientes preguntas proporcionará una clara visión de las expectativas de los usuarios de la red.

- ¿Quiénes son las personas que utilizarán la red?

Los usuarios potenciales de la red será un porcentaje de la población estudiantil de la Institución, los mismos que poseen niveles aceptables de conocimiento en el manejo de computadores.

- ¿Cuáles son las aplicaciones a las que se accederán?

La red prestará servicios de, acceso a *Internet*, voz sobre IP, *e-mail*, vídeoconferencia de escritorio, impresión y envío/recepción de fax.

- ¿Cuál es la expectativa de los usuarios respecto a estos servicios?

Acceso a Internet.- alta disponibilidad y rapidez a un bajo costo.
Voz sobre IP.- calidad de voz, confiabilidad, disponibilidad y costo moderado.
Servicio de *e-mail*.- gran capacidad de almacenamiento y confiabilidad.
Vídeoconferencia de escritorio.- alta resolución, gran velocidad de transmisión, disponibilidad y costo moderado.
Servicios de impresión y fax.- alta calidad, velocidad, disponibilidad y bajo costo.

- ¿Cuáles son las redes a las que se conectará?

Se plantea una red independiente conectada a un ISP con línea dedicada.

Respondiendo estas preguntas y otras preguntas similares, es posible determinar la disponibilidad para el diseño, entendiéndose con ello parámetros de tiempo de respuesta y acceso a recursos, además la capacitación necesaria y el número de personas requeridas para dar soporte a la red LAN.

El diseñador de una red de datos debe asimilar los requerimientos de los usuarios, e ir más allá que simplemente recopilar la información proporcionada por ellos, ya que ésta suele ser incompleta e inexacta. Estos dos puntos de vista son complementarios puesto que el usuario observa la red desde fuera, mientras que el diseñador mira la red desde adentro.

Es función del diseñador buscar la forma de viabilizar los requerimientos del usuario basado en criterios técnicos.

2.2.1 CARACTERÍSTICAS Y DIMENSIONAMIENTO DEL TRÁFICO

Es necesario determinar la carga de tráfico de red antes de desarrollar una estructura de red y adquirir *hardware*. Además, al analizar los requisitos técnicos, se debe estimar la carga de tráfico provocada por las aplicaciones, por ejemplo la cantidad de datos transmitidos en un segundo a través de la red.

Ciertos tipos de uso de red pueden generar grandes volúmenes de tráfico por lo tanto causar congestión, siendo las aplicaciones que usualmente congestionan la red las siguientes:

- Acceso a *Internet*
- Computadores que cargan *software* desde un sitio remoto
- Cualquier dispositivo que transmita imágenes o vídeo

Se debe calcular la peor carga de tráfico en la red durante las horas pico para los usuarios y durante servicios de red programados de forma regular, por ejemplo respaldos del servidor de *e-mail.*

Para poder dimensionar el tráfico generado por cada una de las aplicaciones, se debe tener en claro algunos conceptos, los mismos que se convierten en factores fundamentales a la hora de diseñar una red de datos; dichos conceptos tienen que ver con el comportamiento del tráfico, las tolerancias a retardos, el tiempo de respuesta y la cantidad máxima de información que se puede transmitir por un medio. Entre los factores a considerar están:

a. Burstiness

Factor que permite medir cuan frecuente es el envío de tráfico de una fuente de información. El factor de ráfaga se define como el cociente entre el pico y el promedio de tráfico enviado por una fuente en un período de tiempo determinado.

$$Burstiness = \frac{Tasa\_pico}{Tasa\_promedio}$$

Para un buen desempeño, la relación *burstiness* debe tender a 1 para asegurar que el tráfico real no exceda a las consideraciones de dimensionamiento del enlace, de esta manera se evita una exagerada congestión en la red.

b. Tolerancia al retardo

El nivel de tolerancia al retardo que puede soportar el tráfico dependerá directamente de las aplicaciones. El retardo puede tener muchas causas, las mismas que deberán ser analizadas en el diseño de la red, con el fin de determinar el retardo máximo que las aplicaciones y los usuarios mismos pueden tolerar.

c. Tiempo de respuesta

Los tiempos de respuesta son una consecuencia directa de las variaciones en el retardo; las aplicaciones que soportan tiempos de respuesta variables se las conoce como aplicaciones "*jitter*"[3].

d.* Capacidad y *Throughput

Throughput se refiere a la cantidad de información que se transmite por un medio en una unidad de tiempo, cabe indicar que el *throughput* no se refiere a las capacidades del canal de transmisión sino a las tasas de transmisión instantáneas que las aplicaciones generan.

La capacidad se refiere a la cantidad de recursos disponibles en un medio determinado. La capacidad se orienta más al canal de comunicación, mientras que el *throughput* tiene que ver con el usuario.

La variación de estos factores según las aplicaciones se muestra en la tabla 2.1

[3] *Jitter:* Fluctuación de fase causada por una inestabilidad en la señal de reloj.

Aplicación	Factor de ráfaga	Tolerancia al retardo	Tiempo de respuesta	Throughput
Correo electrónico	Alto	Alta	Diferido	4 a 20 Kbps
Voz	Medio	Baja	Tiempo real	4 a 64 Kbps
Transferencia de archivos	Frecuentemente alto	Alta	Diferido	10 Kbps a 600 Mbps
Transmisión de *web*	Alto	Alta	Diferido	64 Kbps a 1,5 Mbps
Transmisión de imágenes	Frecuentemente Alto	Baja	Tiempo real	256Kbps a 25 Mbps

Tabla 2.1 *Características de tráfico para distintas aplicaciones [23]*

2.2.2 DETERMINACIÓN DEL VOLUMEN DE INFORMACIÓN

De acuerdo a un muestreo realizado a los centros de cómputo de la Institución, se han considerado los siguientes criterios para cuantificar el tráfico diario de la red.

- Un 80% de los usuarios de la Intranet utilizará el servicio de Internet, los mismos que se estima accederán a un promedio de 20 páginas *web* por hora, las cuales tienen un peso aproximado de 25 Kbytes cada una.
- Para el acceso a *e-mail* se consideró que cada usuario revisa un promedio de tres *mails* por cada media hora cuyo peso individual oscila alrededor de 20 Kbytes cada una.
- Para el servicio de impresión se estima un promedio de 10 hojas de impresión (200 Kbytes cada hoja) por persona, con 5 personas accediendo a este servicio por hora.
- El tráfico de voz considera un ancho de banda constante de 17 Kbps por cabina telefónica con una ocupación total de 3 horas diarias.
- La carga diaria considera que la Intranet prestará sus servicios 10 horas diarias.
- Las actualizaciones y *backups* de la red se las realizará en horarios en que la red no esté abierta al público.

La carga diaria es calculada de la siguiente forma:

Tráfico de Internet

$$T_{diario} = (45 * 0.8) * \frac{25KB}{página} * \frac{20 páginas}{1hora} * \frac{10horas}{día}$$

$$T_{diario} = \frac{180MB}{día}$$

Tráfico de *e-mail*

$$T_{diario} = (45 * 0.8) * \frac{20KB}{mail} * \frac{3mails}{0.5hora} * \frac{10horas}{día}$$

$$T_{diario} = \frac{43.2MB}{día}$$

Tráfico usuario/servidor de impresión

$$T_{diario} = \frac{5usuarios}{hora} * \frac{20KB}{página} * \frac{10 páginas}{usuario} * \frac{10horas}{dia}$$

$$T_{diario} = \frac{10MB}{día}$$

Tráfico de voz

$$T_{diario} = 4cabinas * \frac{17Kbits}{cabina * s} * \frac{1Kbyte}{8Kbits} * \frac{3600s}{hora} * \frac{3horas}{día}$$

$$T_{diario} = \frac{91.8MB}{día}$$

Donde T = tráfico generado por la red

La tabla 2.2 muestra valores de tráfico estimados para el diseño.

Una vez determinados los requisitos generales para la red, el siguiente paso es decidir cuál será la topología de la red LAN que satisface los requisitos del usuario.

APLICACIÓN	CARGA GENERADA (diaria)
Usuario / servidor *Proxy*[4]	180.0 Mbytes
Usuario /servidor de *e-mail*	43.2 Mbytes
Servicio de Impresión	10.0 Mbytes
Tráfico de voz	91.8 Mbytes
TOTAL	279.1 Mbytes

Tabla 2.2 *Valores de tráfico estimados*

2.3 DISEÑO DE LA RED DE ÁREA LOCAL

2.3.1 TOPOLOGÍAS DE RED

Las topologías usuales de red LAN son: bus, árbol, anillo y estrella (ver figura 2.5).

a. Topología en bus y árbol

Ambas topologías se caracterizan por el uso de un medio multipunto. En el caso de la topología en bus, todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión a un medio de transmisión lineal o bus. En cada extremo del bus existe un terminador que absorbe las señales eliminándolas del bus.

La topología en árbol es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados que comienzan en un punto conocido como raíz o cabecera. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos.

b. Topología en anillo

La red consta de un conjunto de repetidores unidos por enlaces punto a punto, formando un bucle cerrado. Los enlaces son unidireccionales es decir los datos se transmiten en un solo sentido. Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él.

[4] *Proxy*: elemento de red que almacena las páginas Web solicitadas al servidor de Internet por los usuarios

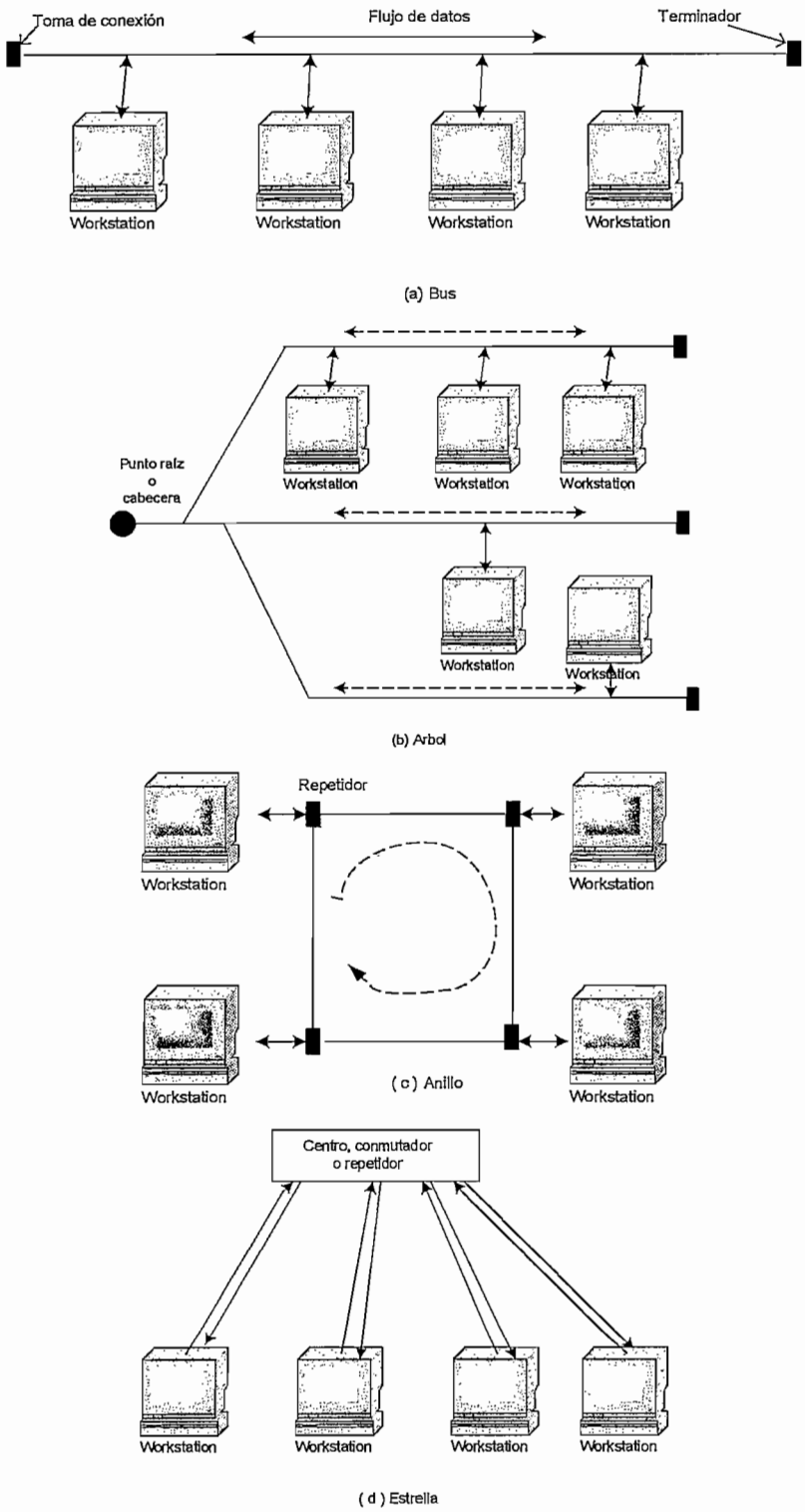


Figura 2.5 *Topologías físicas de red [7]*

c. Topología en estrella

En las redes LAN con topología en estrella cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción.

En general existen dos alternativas para el funcionamiento del nodo central. Una es el funcionamiento en modo difusión, en el que la transmisión de una trama por parte de una estación se envía sobre todos los enlaces de salida del nodo central.

Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación destino.

Una red puede tener un tipo de topología física y un tipo de topología lógica completamente distinto.

Si se consideran las ventajas y desventajas mostradas por la tabla 2.3 la opción más adecuada para el diseño de la Intranet es utilizar topología en estrella tanto física como lógica, debido a que se le considera como la más fácil de diseñar e instalar.

Esto se debe a que los medios de red parten directamente desde un concentrador central hacia cada área de estaciones de trabajo, adicionalmente su mantenimiento es sencillo, ya que la única área de concentración está ubicada en el punto central de la estrella.

Esta topología permite modificar con mayor facilidad el diseño y facilita realizar el diagnóstico por que si existe una falla en un tendido de cable solamente el dispositivo conectado a ese punto queda fuera de servicio.

En resumen, una topología en estrella brinda mayor confiabilidad, siendo éste uno de los requerimientos de los usuarios.

TOPOLOGIA	VENTAJAS	DESVENTAJAS
Bus o Árbol	▪ Fácil de implementar. ▪ No requiere acciones especiales para eliminar la trama del medio de transmisión.	▪ Gran posibilidad de colisión. ▪ Requiere mecanismos para regular la transmisión.
Anillo	▪ No existe colisiones. ▪ Es determinística. ▪ Puede manejar prioridades. ▪ Rendimiento excelente en condiciones de alta utilización de la red.	▪ Requiere técnicas de control de acceso al medio. ▪ Baja eficiencia en condiciones de baja carga. ▪ Naturaleza centralizada. ▪ Más costosa.
Estrella	▪ Ofrece escalabilidad ▪ Mejora la administración de la red. ▪ Fácil diseño e instalación. ▪ Fácil mantenimiento de la red. ▪ Mayor confiabilidad.	▪ Mayor número de equipos activos. ▪ Puede incrementar latencia. ▪ Mayor costo.

Tabla 2.3 *Ventajas y desventajas de las diferentes topologías de red*

2.3.2 TECNOLOGÍA DE RED

La tecnología de LAN más común para una red es *Ethernet*[5], ésta se utiliza para transportar datos entre dispositivos en una red, tal como computadoras, impresoras y servidores de archivos. Como aparece en la figura 2.6, todos los dispositivos se conectan al mismo medio de transmisión. Los medios *Ethernet* utilizan un método de *broadcast*[6] de trama de datos para transmitir y recibir datos a todos los dispositivos de la red.

Existe una gran variedad de estándares *Ethernet* que han evolucionado de acuerdo a las necesidades de los usuarios. Para este caso, tomando en cuenta la topología seleccionada, este universo de alternativas queda reducido a tres.

- ***Ethernet* 10 BaseT**

Utiliza una topología tipo estrella, emplea dos pares de cable UTP por cada DTE[7]

[5] *Ethernet:* Tecnología de red estandarizada por Comité de Normalización IEEE 802
[6] *Broadcast:* Información dirigida hacia todas las máquinas de una red de difusión
[7] DTE: *Data Terminal Equipment.*

conectado a la red, mismos que se conectan a un concentrador de cableado a través de interfaces RJ45.

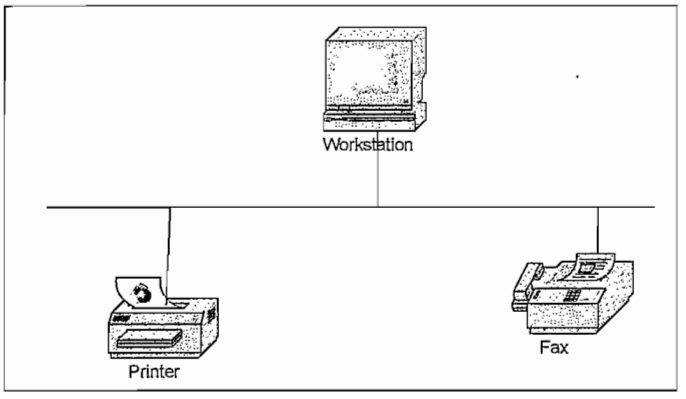


Figura 2.6 *Transmisión de información en una red Ethernet[6]*

- ***Ethernet* Conmutada**

Utiliza una topología tipo estrella, cada segmento de la red cuenta con un ancho de banda independiente de los demás para ello utiliza un *switch* como concentrador.

- **Fast Ethernet**

Es una red *Ethernet* conmutada que establece una velocidad de transmisión de 100 Mbps, en la que sigue siendo útil el método CSMA/CD[8], y el tamaño mínimo de trama de 512 bits, también conocida como 100BaseT. En la práctica cuenta con dos estándares en función del tipo de cable:

100BaseX : Para cables STP, UTP categoría 5 o superior y fibra óptica.
100 Base T4: Para cables de voz categoría 3 o superior

Aunque los *hubs* y los *switches* son dispositivos de red útiles y económicos, amplían los dominios de colisión y, por lo tanto, hacen que el desempeño de la red se vea afectado debido al exceso de colisiones.

El desempeño de una LAN *Ethernet* de medio compartido puede verse afectado de forma negativa por distintos factores:

[8] CSMA/CD: *Carrier Sense Multiple Access Collision Detect*

- La naturaleza de entrega de *broadcast* de trama de datos de las LAN *Ethernet*
- Los métodos de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) sólo permiten que una estación a la vez pueda transmitir.
- Las aplicaciones de multimedia con mayor demanda de ancho de banda, tales como vídeo e Internet, sumadas a la naturaleza de *broadcast* de *Ethernet*, pueden crear congestión de red.

Actualmente las redes están experimentando un aumento en la transmisión de archivos de gráficos, imágenes, vídeos con movimiento y aplicaciones de multimedia, así como un aumento en la cantidad de usuarios de red. Todos estos factores representan una exigencia aún mayor para la capacidad del ancho de banda; cada vez más personas utilizan la red para compartir grandes archivos, acceder a servidores de archivo y conectarse a Internet, lo que produce congestión de red, dando como resultado tiempos de respuesta más lentos, transferencias de archivos muy largas y usuarios de red menos productivos debido a los retardos de red.

Para aliviar la congestión de red, se necesita más ancho de banda o bien, el ancho de banda disponible debe usarse con mayor eficiencia.

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de red que pueden dividir los dominios. Los puentes, *switches* y *routers* son ejemplos de este tipo de dispositivo. Este proceso se denomina segmentación. Cada segmento utiliza el método de acceso CSMA/CD y mantiene el tráfico entre los usuarios del segmento. La figura 2.7 muestra un ejemplo de red *Ethernet* segmentada.

Dividiendo la red en varios segmentos, un administrador de red puede reducir la congestión de la red dentro de cada segmento. Al transmitir los datos dentro de un segmento, los dispositivos dentro de éste, comparten el mismo ancho de banda. En una LAN *Ethernet* segmentada, los datos que pasan entre segmentos

se transmiten a través del *backbone*[9] de la red utilizando un puente, *router* o *switch*.

En vista de las ventajas anteriormente expuestas se elige el uso de una red *Fast Ethernet* con topología estrella, que puede ser configurada de dos formas distintas:

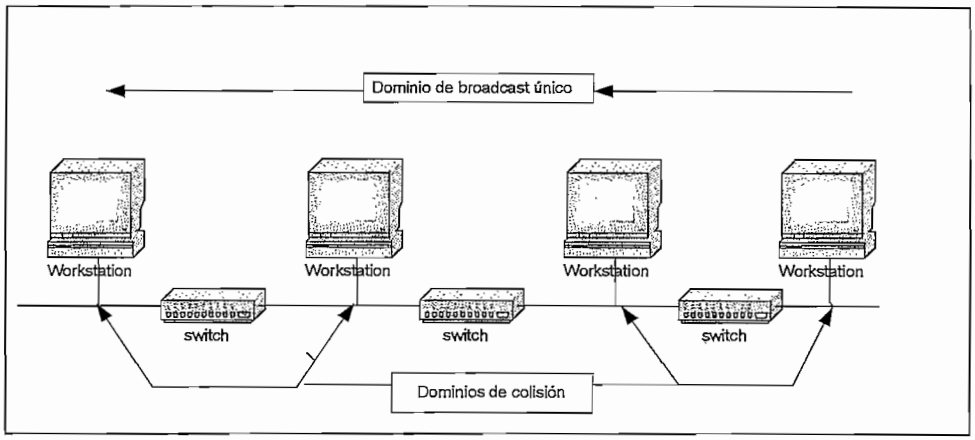


Figura 2.7 *Red Ethernet segmentada [6]*

Alternativa A.- Todos los usuarios y servidores pueden ser concentrados en un solo *switch Fast Ethernet* central.

Alternativa B.- Requiere el uso de tres *switches* (uno por sala), un *switch* central que se encargará de concentrar equipos de administración, control, servidores y además permite conectar a los *switches* de cada sala.

Considerando las ventajas y desventajas indicadas en la tabla 2.4, se elige la alternativa B, puesto que brinda mayor seguridad y confiabilidad a la red, siendo éstos los factores principales para el buen desempeño de la misma.

2.3.3 DISEÑO DE LA RED PASIVA

El cableado físico es uno de los componentes más importantes que se deben tener en cuenta al diseñar una red. Los temas de diseño incluyen el diagrama

[9] *Backbone:* Sistema de Cableado Estructurado vertical

lógico, el tipo de cableado que se debe utilizar y la estructura general del sistema de cableado estructurado.

ALTERNATIVA	VENTAJAS	DESVENTAJAS
Alternativa A	▪ Menor número de elementos de red ▪ Menor latencia ▪ Menor costo	▪ El *switch* se convierte en un punto de falla. ▪ Menor confiabilidad de la red ▪ Poca seguridad de acceso a servidores. ▪ Extensos dominios de colisión.
Alternativa B	▪ Estructura de red descentralizada. ▪ Gran confiabilidad. ▪ Mayor escalabilidad. ▪ Mayor seguridad de acceso a servidores. ▪ Menores dominios de colisión. ▪ Se puede establecer mayor número de prioridades de tráfico.	▪ Mayor número de elementos activos. ▪ Puede incrementar latencia. ▪ Mayor costo.

Tabla 2.4 *Ventajas y desventajas de las alternativas de tecnologías de red LAN Ethernet.*

El diagrama lógico es el modelo de topología de red sin todos los detalles de la ruta de instalación exacta del cableado. Es el mapa de ruta básico de la LAN. Los elementos del diagrama lógico incluyen:

- Las ubicaciones exactas de los centros de cableado MDF[10] e IDF[11].
- El tipo y la cantidad de cableado que se utiliza para interconectar los IDF con el MDF, así como también la cantidad de cables de reserva que hay disponibles para aumentar el ancho de banda entre los armarios.
- Documentación detallada sobre todos los tendidos de cable, los números de identificación y en cuál de los puertos del HCC[12] o VCC[13] termina el tendido de cableado.

Para este diseño se ha considerado el estándar TIA/EIA -568-B, (el resumen de la norma se presenta en el Anexo B), que especifica que cada dispositivo de la red

[10] MDF: punto de distribución principal del Sistema de Cableado Estructurado
[11] IDF: punto de distribución secundario del Sistema de Cableado Estructurado
[12] HCC: *Horizontal Cross Connect*
[13] VCC: *Vertical Cross Connect*

debe estar conectado a una ubicación central a través del cableado horizontal, siempre y cuando todos los *hosts* que necesitan acceder a la red estén ubicados dentro de un límite de distancia de hasta 100 metros.

La Intranet motivo de diseño, contará con un solo MDF, ubicado en el área de administración, debido a que:

- La distancia máxima entre el dispositivo de red y el MDF es de 25 m
- Todos los servidores de red son del tipo empresarial, y por lo tanto se considera conveniente ubicarlos en forma centralizada, en el sistema de distribución principal, de modo que resulten fáciles de administrar
- Se colocarán tres *switches,* uno por sala, ubicados en el *rack*
- La red contará únicamente con cableado horizontal el mismo que será tendido con cable UTP categoría 6, que ofrece 250 MHz de ancho de banda y que resulta suficiente para la red a la vez que no limita el uso de futuras tecnologías.

En la figura 2.8 se presenta un diagrama lógico de la red.

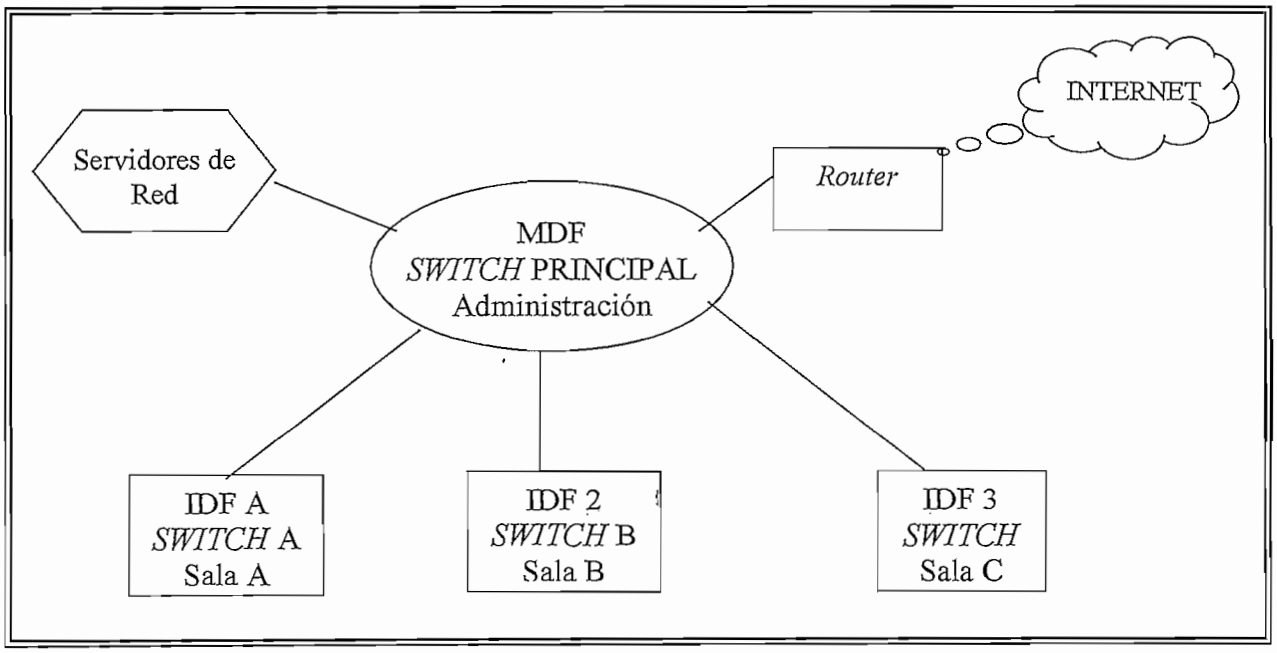


Figura 2.8 *Diagrama lógico de la red*

Una vez obtenido un esquema general de lo que será el sistema de cableado estructurado se inicia con el diseño al detalle, el cual está dividido en tres áreas: área de trabajo, cableado horizontal y closet de telecomunicaciones, tomando en cuenta los elementos que se encuentran dentro de ellas.

a. Área de trabajo

Está constituida por:

PUNTOS DE RED

El tendido de cableado estructurado abarca un área aproximada de 180 m^2 que se halla distribuida de la siguiente manera: tres salas de computadores con un promedio de catorce equipos cada una, una oficina para administración, dos cabinas telefónicas y un espacio asignado para el control de ingreso.

Se prevé la necesidad de 55 puntos, para lograr una cobertura total del lugar, considerando que la red no tendrá crecimiento, debido a que el espacio físico no lo permite por tener un área limitada; estos accesos serán distribuidos de la siguiente forma:

Voz	7 puntos
Datos	47 puntos
Vídeo	1 punto

La distribución de los puntos de red se realiza como lo indica la tabla 2.5.

DESCRIPCIÓN	DATOS	VOZ	VÍDEO	TOTAL
SALA A	14	1	1	16
SALA B	15	0	0	15
SALA C	13	0	0	13
ADMINISTRACIÓN	3	1	0	4
CONTROL	2	1	0	3
CABINAS TELEF.	0	4	0	4
TOTAL	47	7	1	55

Tabla 2.5 *Distribución de los puntos de telecomunicaciones*

SALIDA DE TELECOMUNICACIONES

Las salidas de telecomunicaciones están compuestas por: la placa, la caja y los *jacks*[14]; éstas estarán colocadas a una altura de 50 cm sobre el piso en el caso de las salidas de pared, mientras que para el caso de las salidas de piso, éstas irán sobre la canaleta utilizada. Las salidas simples y dobles contendrán *jacks* de 8 posiciones.

Para este diseño se considera que todas las salidas de telecomunicaciones serán de pared. El esquema de conexión escogido estará establecido por la norma T568B, cuyas especificaciones generales se indican en el Anexo B, mismo que será adoptado a lo largo de toda la instalación del cableado estructurado. El resumen de las salidas de telecomunicaciones y *patch cords*[15] se indican en el Anexo C.

La ubicación física de las salidas de telecomunicaciones se muestra en el plano de cableado indicado en el Anexo P.

DESCRIPCIÓN	SALIDAS DE PARED	TIPO
SALA A	16	Simple
SALA B	15	Simple
SALA C	13	Simple
ADMINISTRACIÓN	4	Simple
CONTROL	3	Simple
CABINAS TELEF.	4	Simple

Tabla 2.6 *Salidas de telecomunicaciones*

PATCH CORDS

Los *patch cords* destinados a las áreas de trabajo, deben tener una longitud máxima aproximada de 2 metros, con la cual se puede tener la suficiente flexibilidad para la conexión entre la salida de telecomunicaciones y la estación de trabajo.

[14] *Jack*: Terminal de conexión
[15] *Patch cords:* Segmento de cable UTP que conecta al *patch panel* con los dispositivos de red

Los *patch cords* deberán ser construidos con cable multifilar UTP categoría 6 de cuatro pares y con un conector RJ45.

b. Cableado horizontal

Para analizar el cableado horizontal es importante considerar:

CABLE

El medio de transmisión seleccionado es el cable UTP de cuatro pares categoría 6, pues resulta adecuado para soportar las aplicaciones de la Intranet y es de fácil instalación.

El cálculo de cableado horizontal se lo realiza de la siguiente forma, bajo la consideración que los puntos serán distribuidos equitativamente [17]

1. Ubicación de las salidas de información
2. Con la ayuda de los planos arquitectónicos se determina la ruta del cable
3. Establecer el área a servir para cada IDF o MDF.
4. Medir la distancia al punto más lejano.
5. Medir la distancia al punto más cercano.
6. Sumar las distancias y dividirlas para dos.
7. Añadir el 10% de holgura.
8. Añadir la holgura de terminación (2.5 m).
9. El número de corridas será calculado al dividir 305 m (longitud del rollo del cable), para el resultado de la suma de los literales 6, 7 y 8; aproximar al inmediato inferior.
10. Para obtener el número de rollos necesarios, se divide el número de salidas para el número de corridas por rollo, aproximar al inmediato superior.

Con los datos estimados en la tabla 2.7 se requieren un total de 2 rollos de cable UTP categoría 6.

DESCRIPCIÓN	SALA A	SALA B	SALA C	ADMINIST	CONTROL
Número de puntos	16	15	13	3	2
Punto más cercano [m]	1	6	11	1	6
Punto más lejano	6.5	12	16	3	7
Distancia promedio	3.75	9	13.5	2	6.5
Corridas por rollo	73	30	20	152	46
Rollos requeridos	0.21	0.5	0.7	0.1	0.1

Tabla 2.7 *Cálculo de la longitud de cable UTP categoría 6*

De acuerdo al cálculo realizado que se muestra en la tabla 2.8 la longitud de cable telefónico necesario para la red es de 43 m, ya que todas las salidas de voz se concentran en el *yap-max*[16] ubicado en la oficina de administración.

DESCRIPCIÓN	CABINAS	ADMINIST	CONTROL
Número de puntos	4	1	1
Punto más cercano [m]	7	1	6
Punto más lejano	8	3	7
Distancia promedio	8.5	2	6.5
Longitud del cable [m]	34	2	6.5

Tabla 2.8 *Cálculo de la longitud de cable telefónico*

MÉTODO DE DISTRIBUCIÓN

Por tratarse de un local en construcción se prevé la utilización de bandejas, las cuales estarán ubicadas sobre el techo falso y en pared se utilizarán tuberías PVC que tendrán un índice de ocupación del 40%, como lo establecen las recomendaciones de cableado estructurado.

c. Closet de telecomunicaciones

Los sitios destinados a funcionar como closet de telecomunicaciones deben adecuarse correctamente con ventilación, iluminación, seguridad, conexión a tierra y provisión continua y regulada de energía eléctrica (UPS).

[16] *Yap max:* equipo para la transmisión de voz sobre IP.

De acuerdo a las normas ANSI/EIA/TIA568 B y ANSI/EIA/TIA 569, es necesario un sólo closet de telecomunicaciones, debido a que la distancia no sobrepasa los 90 metros de tendido de cable y se cuenta con un número de puntos inferior a 200; el closet por cuestiones de seguridad y espacio físico se ubicará en la oficina de administración.

La ubicación de este closet se muestra en el plano de cableado indicado en el Anexo P. En esta área se deben considerar los siguientes elementos:

RACK

Por razones económicas se utilizará un *rack*[17] abierto con sus respectivos organizadores horizontales y verticales, en lugar de un gabinete o *rack* cerrado.

La altura de los *racks* se estandariza en: 2.1 metros (84 pulg) o 1.2 metros (48 pulg). En razón de la cantidad de elementos (*patch panels*[18], *switches*, organizadores horizontales, etc) que deberá albergar el *rack*, se escoge uno de 2.1 metros. Por otro lado, la diferencia económica al instalar un *rack* de 2.1 metros o de 1.2 metros no es muy significativa, y bien vale la pena asumirla, tomando en cuenta ciertas ventajas como: seguridad, comodidad y estética.

Para el *rack* se tendrá cuatro organizadores horizontales, un organizador vertical y seis bandejas: cuatro para los *switches*, una para el *yap max* y uno para el *router*, bajo la consideración de que estos equipos no serán necesariamente montables en *rack.*

PATCH PANELS

Se requieren 4 *patch panels* de 24 puertos. El *patch panel* de 24 puertos requiere un organizador horizontal de una unidad de *rack* (1 UR = 1.75 pulg) para realizar un adecuado manejo de los *patch cord.*

Se planea establecer un sobredimensionamiento aproximado del 15% en el número de puertos de los *patch panels*, con el objeto de suplir las fallas que pudiesen producirse en estos elementos.

---

[17] *Rack* estructura metálica utilizada para soportar varios dispositivos y *patch panels.*
[18] *Patch Panel*: paneles para la organización del cableado estructurado.

En resumen los materiales necesarios para la instalación del sistema de cableado estructurado se muestran en la tabla 2.9.

ELEMENTO	SALA A	SALA B	SALA C	ADMIN.	CABINAS	CONTROL	TOTAL
Patch cord 1.6 m	14	15	13	3	0	1	46
Patch cord 3 m	14	15	13	3	0	1	46
Cable UTP cat 6 [m]	64	152	213	31	0	31	491
Cable telefónico [m]	0	0	0	2	34	7	43
Plugs RJ-45	16	15	13	3	0	2	49
Plugs RJ-8	0	0	0	1	4	1	6
Rack de 2.1 metros	0	0	0	1	0	0	1
Bandejas	1	1	1	3	0	0	6
Organizadores horizontales	1	1	1	1	0	0	4
Organizadores verticales	0	0	0	1	0	0	1
Regletas o *patch panels* 24 puertos	1	1	1	1	0	0	4
Face plate	16	15	13	4	4	3	55
Cajetines simples	16	15	13	4	4	3	55
Número de ductos PVC rígidos de 2"	2	2	2	0	0	1	7
Número de ductos metálicos	5	4	4	0	0	0	13

Tabla 2.9 *Resumen de materiales necesarios para cableado estructurado*

El plano del sistema de cableado estructurado para la Intranet, se presenta en el Anexo P.

El último paso en el diseño de cableado estructurado consiste en realizar las pruebas de cableado respectivas, para garantizar su buen funcionamiento, la forma de realizar estas pruebas se las presenta en el Anexo D.

Para una mejor administración del sistema, el Anexo C presenta la información completa acerca de la distribución del cableado estructurado.

2.3.4 DISEÑO Y DIMENSIONAMIENTO DE LA RED ACTIVA

El diseño de la parte activa radica básicamente en el dimensionamiento de *switches,* el mismo que se lo hace en base a un análisis de las estaciones de trabajo y del tráfico previsto para la red.

a. SWITCHES

La función de los dispositivos de capa 2 en la red es suministrar control de flujo, detección de errores, corrección de errores y reducir la congestión en la red. Los dispositivos de esta capa determinan el tamaño de los dominios de colisión y los dominios de *broadcast* (ver figura 2.9).

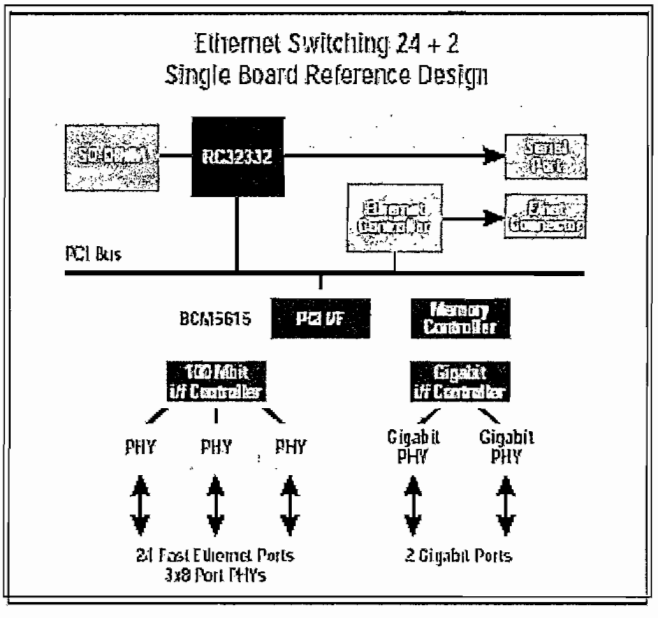


Figura 2.9 *Diagrama de la estructura interna de un switch*

Por las ventajas brindadas por el *switch* en lo que a conmutación se refiere se considera el uso de un *switch* por sala, tanto por el ancho de banda proporcionado como por su costo muy similar al de un *hub.*

De acuerdo a la carga estimada para la red, se requieren 4 *switches Fast Ethernet* estandarizados de 24 puertos 10/100 *autosensing*[19], no se considera

[19] *Auto sensing*: Detección automática de velocidades

necesaria la utilización de un puerto *up link*[20] 10/100/1000 debido a que eleva demasiado el costo de los equipos y se estima que el tráfico de la red no sobrepasa los niveles de *Fast Ethernet*.

Los requerimientos mínimos para los *switches* son:

24 puertos UTP (RJ45) *Ethernet full duplex*
6 Mbps de *Throughput*
460 Mbps de *Back plane*
2000 *Mac Address*
Soporte de *Switching* de Capa 2
Protocolo SNMP

b. Tarjetas de red (NIC's)

Una tarjeta de interfaz de red o NIC es un pequeño circuito impreso que se coloca en la ranura de expansión de un bus de la *motherboard* o dispositivo periférico de un computador. También se denomina adaptador de red (ver figura 2.10).

Las NIC's se consideran dispositivos de Capa 2 y en cualquier lugar del mundo lleva un nombre codificado único, denominado dirección de Control de acceso al medio (MAC[21]).

Para la red se requieren 48 tarjetas de red Fast Ethernet con interfaz RJ45, con soporte para protocolo TCP/IP, 44 para las estaciones de trabajo y 4 para los servidores las cuales deben tener las siguientes características:

Tecnología Ethernet 10/100 Mbps
Interfaz RJ45
Full duplex
Bus mastering[22]

[20] Puerto *Up link:* Puerto del switch de mayor velocidad, que permite conectarlo en cascada.
[21] MAC: *Medium Access Control*
[22] *Bus mastering:*Tecnología que reduce el tiempo de espera y acelera el rendimiento del sistema.

Parallel Tasking[23]

Es necesario aclarar que usualmente las tarjetas de red vienen integradas a las estaciones de trabajo.

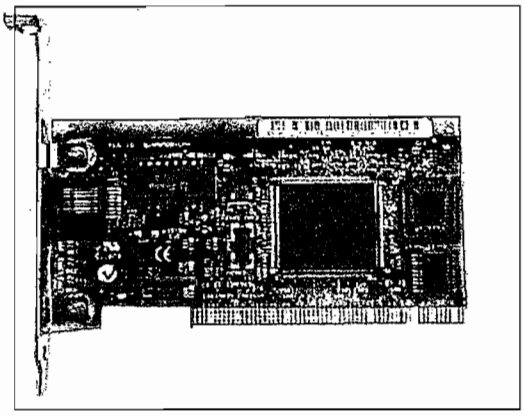


Figura 2.10 *Tarjeta de red (NIC)[16]*

c. Estaciones de trabajo

Las estaciones de trabajo conocidas también como *workstation* son puestos de trabajo que interactúan directamente con el cliente o usuario de la red y dependen de los servicios brindados por la red. Están constituidas por ordenadores personales que ejecutan gran cantidad de aplicaciones para procesamiento y transmisión de datos, útiles para el usuario.

La red trabajará con 44 estaciones, distribuidas de la siguiente forma:

Sala A:	14 máquinas
Sala B:	15 máquinas
Sala C:	13 máquinas
Control :	1 máquina
Administración:	1 máquina

Las tablas 2.10, 2.11 y 2.12 describen las características técnicas mínimas requeridas de cada una de las estaciones de trabajo:

[23] *Parallel Tasking:* Tecnología que permite procesar paralelamente.

- Máquina para servidor *Proxy* :

COMPONENTES	CARACTERÍSTICAS	
PROCESADOR	Velocidad Modelo CPU	2.6 GHz P IV
MEMORIA	RAM estándar	512 MB
DISCO DURO	Capacidad	80 GB
MONITOR	Monitor	17" CRT
2 TARJETAS DE RED	Velocidad	100 Mbps
SISTEMA OPERATIVO	Con soporte para protocolo TCP/IP	
UNIDAD DE CD-ROM	CDRW/DVD COMBO	
Posibilidad de futuras expansiones		

Tabla 2.10 *Características técnicas para el servidor proxy*

- Máquinas para usuarios de las salas:

COMPONENTES	CARACTERÍSTICAS	
PROCESADOR	Velocidad Modelo CPU	2.6 GHz P IV
MEMORIA	RAM estándar	256 MB
DISCO DURO	Capacidad	80 GB
MONITOR	Monitor	17" CRT
1 TARJETA DE RED	Velocidad	100 Mbps
SISTEMA OPERATIVO	Con soporte para protocolo TCP/IP	
UNIDAD DE CD-ROM	CD-ROM	
Posibilidad de futuras expansiones		

Tabla 2.11 *Características técnicas para los PCs de usuarios*

Posibilidades de futuras expansiones y sus respectivas tarjetas de red.

- Máquinas destinadas a la administración y control:

COMPONENTES	CARACTERÍSTICAS	
PROCESADOR	Velocidad Modelo CPU	2.6 GHz P IV
MEMORIA	RAM estándar	256 MB
DISCO DURO	Capacidad	120 GB
MONITOR	Monitor	17" CRT
1 TARJETA DE RED	Velocidad	100 Mbps
SISTEMA OPERATIVO	Con soporte para protocolo TCP/IP	
UNIDAD DE CD-ROM	CDRW/DVD COMBO	
Posibilidad de futuras expansiones		

Tabla 2.12 *Características técnicas para los PCs de administración y control*

Voz sobre IP (VoIP)

Para la VoIP se requiere la adquisición de un *Yap Max* 4 (figura 2.11) que permite la salida de la señal de voz digitalizada con formato IP hacia la red de Internet.

Figura 2.11 *Yap Max [33]*

Adicionalmente es necesario 2 telefónos convencionales los cuales irán directamente conectados al Yap Max.

Vídeoconferencia

El servicio de videoconferencia grupal deberá ser considerado para futuras inversiones por cuanto requiere de la adquisición de equipos especializados para este fin como son las cámaras *Policom View Station,* inicialmente se plantea dar

este servicio a través de *Web cams.* Las especificaciones técnicas de los equipos requeridos son:

CÁMARA "*Web cam*"

- Interfaz: USB.
- Resolución máxima del vídeo CIF (pixels): 352x288
- Número de colores (bits): 24
- Frecuencia máxima (fotogramas/segundo): 30
- Micrófono integrado: no.
- "Drivers" para Microsoft Windows.
- Software operativo.

Los requisitos que debe tener el PC que prestará el servicio de vídeoconferencia:

- Pentium IV
- 512 MB RAM
- 1 GB de espacio libre en disco.
- 1 puerto USB libre.
- Lector de CD o DVD.
- Capacidad de grabar y reproducir audio.
- Pantalla de 64000 colores.
- Windows 2000 o ME
- Conexión a Internet.

Correo electrónico

La Intranet diseñada, requiere de servidores *Web*, de y correo electrónico que *considerando* el tamaño de la red, pueden ser configurados en una misma máquina. Los servidores bajo condiciones óptimas deberían prestar servicios las 24 horas del día. Sin embargo el costo del hardware específico para estos tipos de servidores es muy elevado, por ello se plantea el uso de una PC normal con las características indicadas en la tabla 2.13.

COMPONENTES	CARACTERÍSTICAS	
PROCESADOR	Velocidad Modelo CPU	3 GHz P IV
BUS	Velocidad	133 MHz
MEMORIA	RAM estándar	512 MB
DISCO DURO	Capacidad	80 GB
MONITOR	Monitor	17" CRT
2 TARJETAS DE RED	Velocidad	100 Mbps
SISTEMA OPERATIVO	Con soporte para protocolo TCP/IP	
UNIDAD DE CD-ROM	CDRW/DVD COMBO	
Posibilidad de futuras expansiones		

Tabla 2.13 *Características técnicas para el servidor de e-mail*

Varios

Adicionalmente a los servicios de acceso a Internet, VoIP, *chat*, *e-mail* y vídeoconferencia, la Intranet ofrecerá servicios de impresión, escáner y fax a todos los usuarios de la red.

IMPRESORAS

Puerto USB

Resolución para impresión blanco y negro 1200x1200 pixeles

Resolución para impresión a color 4800x1200 pixeles

Impresión de páginas color 12 a 15 páginas por minuto

Impresión de páginas blanco y negro 17 a 21 páginas por minuto

SCANNER

Resolución de 1200x1200 [dpi] a 2400x2400 [dpi][24]

Velocidad *Preview* [seg.] 7 a 10 [seg.]

Puerto USB

Página completa

Color

[24] dpi: unidad de resolución de un *scanner*

FAX

Fax-Teléfono y copiadora.

Identificador de llamadas.

Papel normal.

Pantalla líquida.

Remarcado automático.

40 memorias para recepción de fax.

2.4 ACCESO A INTERNET

La red mundial Internet interconecta miles de redes con múltiples medios de transmisión y protocolos, es por ello que exige una gran cantidad de recursos y necesita tecnologías de red de alto desempeño.

Las comunicaciones en Internet son posibles entre redes de diferentes ambientes y plataformas como se indica en la figura 2.12. Este intercambio dinámico de datos se ha logrado debido al desarrollo de los protocolos de comunicación.

Como se indicó en la sección 2.3 los requisitos en cuanto a acceso de Internet son: alta velocidad de acceso, bajo retardo, baja tasa de bits errados, sin restricciones de protocolos y aplicaciones y el menor costo posible; éstos son parámetros que permiten la elección adecuada de la tecnología de transmisión. Para ello es necesario determinar las características de tráfico y el volumen de información saliente a Internet.

La capacidad total del canal se obtiene de la suma de la capacidad requerida para el tráfico hacia Internet más el tráfico generado por el servicio de VoIP.

Considerando que la red cuenta con un servidor *Proxy*, el mismo que posee memoria *caché* que almacena las páginas Web accedidas con mayor frecuencia, se estima que las peticiones reales salientes a Internet serán del 60% del tráfico simultáneo generado por la red hacia éste, mientras que el 40% restante obtendrá sus respuestas de la memoria *caché*.

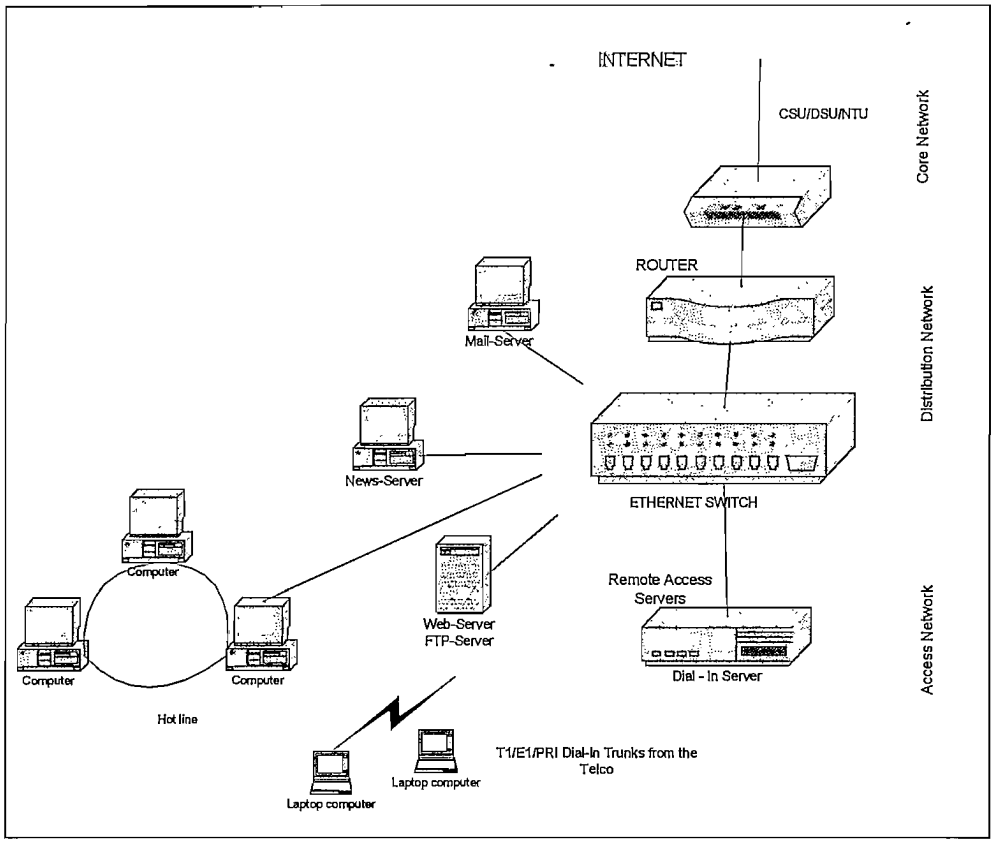


Figura 2.12 Conexión a Internet [32]

El cálculo de la capacidad del canal se realiza para las peores condiciones de tráfico, es decir cuando simultáneamente todas las máquinas se encuentren descargando páginas Web. Bajo estas condiciones se asume que una página Web con un peso promedio de 25 KB será descargada en 30 segundos.

La capacidad de canal requerida para la transmisión de VoIP es constante y tiene un valor de 17 Kbps por cabina telefónica.

$$C_{canal} = C_{Internet} + C_{VoIP}$$

$$C_{Internet} = 21 usuarios * \frac{25KB}{usuario} * \frac{8Kb}{1KB} * \frac{1}{30s}$$

$$C_{Internet} = 140Kbps$$

$$C_{VoIP} = 4Cabinas * \frac{17Kbps}{Cabina}$$

$$C_{VoIP} = 68Kbps$$

$$C_{canal} = 140Kbps + 68Kbps$$

$$C_{canal} = 208Kbps$$

Donde C = capacidad

Considerando que el cálculo realizado es para las peores condiciones de tráfico, es posible trabajar con un canal de 192 Kbps para la Intranet, cabe señalar que el servicio de vídeoconferencia grupal requerirá el uso de toda la capacidad del canal, es por ello que al momento de ofrecer este servicio será necesario desconectar del Internet a todas las máquinas de la red.

2.4.1 TECNOLOGÍAS DE TRANSMISIÓN

Servicios de conmutación de circuitos

- *RDSI (Red Digital de Servicios Integrados) de banda angosta*: Una tecnología versátil, de amplio uso e históricamente importante. Fue el primer servicio con marcación totalmente digital. Es de uso bastante generalizado, aunque varía considerablemente de un país a otro. El costo es moderado. Su capacidad es de 128 kbps para la BRI (Interfaz de Acceso Básico) de menor costo y de aproximadamente 3 Mbps para la PRI (Interfaz de Acceso Principal). El medio típico es el cable de cobre de par trenzado.

Servicios de conmutación por paquetes

- *X.25:* Tecnología más antigua pero que aún se la sigue utilizando, posee amplias capacidades de verificación de errores desde la época en que los enlaces de las WAN eran más susceptibles a los errores, lo que hace que su confiabilidad sea muy grande, pero al mismo tiempo limita su ancho de

banda. Su capacidad puede ser de 64 Kbps como máximo. Es ampliamente utilizada, y su costo es moderado. El medio típico es el cable de cobre de par trenzado.

- *Frame Relay*: Versión conmutada por paquetes del RDSI de banda angosta. Se ha transformado en una tecnología WAN sumamente popular por derecho propio. Es más eficiente que X.25, con servicios similares. Su capacidad máxima es de 1,544 Mbps. En los EE.UU. son muy populares las capacidades de 56 kbps y 384 kbps. Es de uso generalizado, el costo es de moderado a bajo. Entre los medios típicos se incluyen el cable de cobre de par trenzado y el cable de fibra óptica.

En la figura 2.13 se ilustra un modelo típico *Frame Relay* de acceso a Internet.

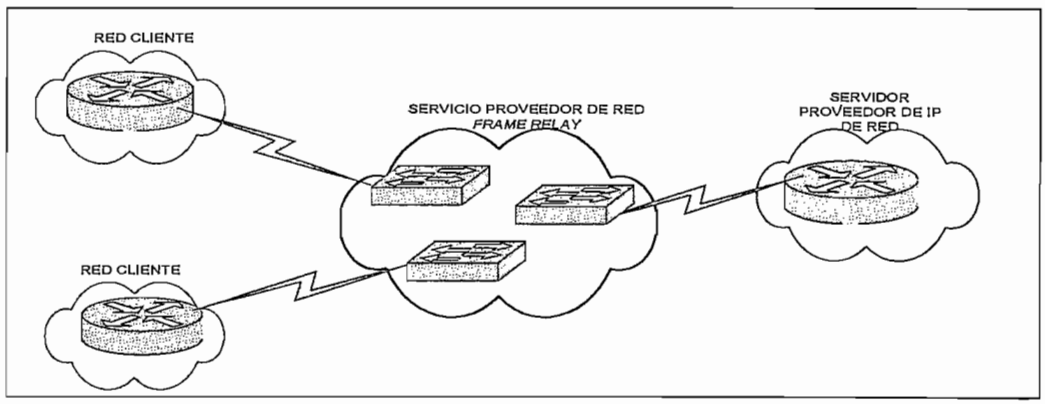


Figura 2.13 *Acceso a Internet Frame Relay [4]*

Servicios de conmutación por celdas

- *ATM (Modo de Transferencia Asíncrona):* Tiene una cercana relación con el RDSI de banda ancha. Es una tecnología WAN (e inclusive LAN) cuya importancia va en aumento. Utiliza tramas pequeñas, de longitud fija (53 bytes) para transportar los datos. Su capacidad actualmente es de 622 Mbps, y se están desarrollando velocidades mayores. Los medios típicos son el cable de cobre de par trenzado y el cable de fibra óptica. Su uso es generalizado y está en aumento; el costo es elevado.

Servicios digitales dedicados

El acceso dedicado a Internet se ofrece habitualmente a velocidades de 56 Kbps o 64 Kbps hasta velocidades de 2.048 Mbps. La Figura 2.14 ilustra la configuración típica de acceso dedicado a Internet.

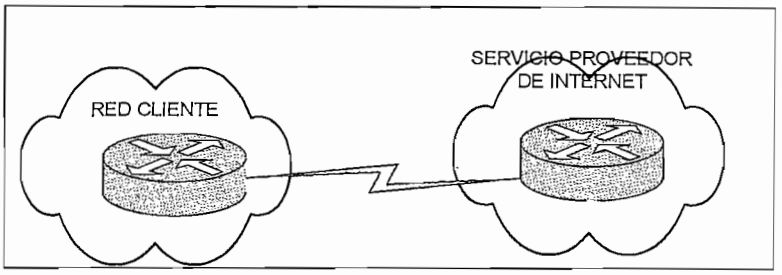


Figura 2.14 *Configuración de acceso dedicado a Internet [4]*

- *T1, T3, E1, E3:* La serie T de servicios en los EE.UU. y la serie E de servicios en Latinoamérica y Europa son tecnologías Wan sumamente importantes. Usan la multiplexación por división de tiempo para "dividir" y asignar ranuras de tiempo para la transmisión de datos; su capacidad correspondiente es:

  - T1: 1,544 Mbps
  - T3: 44,736 Mbps
  - E1: 2,048 Mbps
  - E3: 34,368 Mbps
  - Hay otras capacidades de banda disponibles

Los medios utilizados son normalmente el cable de cobre de par trenzado y fibra óptica. Su uso es muy generalizado; el costo es moderado.

- *xDSL (*Familia de tecnologías para línea digital de abonado): Tecnología nueva y en desarrollo para uso doméstico. Su ancho de banda disminuye a medida que aumenta la distancia desde el equipo de las compañías telefónicas. Las velocidades máximas de 51,84 Mbps son posibles en las cercanías de una central telefónica; son más comunes las velocidades mucho menores (desde 100 kbps hasta varios Mbps). Su uso es limitado

pero en rápido aumento; el costo es moderado y se reduce cada vez más. Entre las tecnologías DSL, se tiene:

- *HDSL*: DSL de alta velocidad
- *SDSL*: DSL de línea simétrica
- *ADSL*: DSL asimétrica
- *VDSL*: DSL de muy alta velocidad
- *RADSL*: DSL de velocidad adaptable

- *SONET (Red Óptica Síncrona)*: Conjunto de tecnologías de capa física de muy alta velocidad, diseñadas para fibra óptica, pero que también pueden funcionar con cables de cobre. Tiene una serie de velocidades de datos disponibles con designaciones especiales. Implementadas a diferentes niveles de OC (portadora óptica) desde los 51,84 Mbps (OC-1) hasta los 9,952 Mbps (OC-192). Puede alcanzar estas impresionantes velocidades de datos mediante el uso de multiplexación por división de longitud de onda (WDM), en la que los láser configurados para colores ligeramente diferentes (longitudes de onda) envían enormes cantidades de datos ópticamente; su uso es generalizado entre las entidades de *backbone* de Internet. El costo es elevado: no es una tecnología que se pueda usar a nivel doméstico.

2.4.2 CONSIDERACIONES DE LAS TECNOLOGÍAS DE ACCESO A INTERNET

Servicios Dedicados

Las conexiones de acceso dedicado se utilizan cuando el ancho de banda que se va a usar es previsible y el acceso a la red es lo suficientemente alto para justificar una línea de estas características, 24 horas al día.

El mayor inconveniente del acceso dedicado es su costo, que normalmente es más alto comparado con otros métodos de acceso.

Normalmente el acceso dedicado a Internet implica la terminación del circuito físico en el dispositivo CPE [25], así como una terminación de circuito directa en un *router* IP en el lado del proveedor del servicio. Los protocolos de la capa enlace como PPP[26] o HDLC[27], son utilizados para señalizar y transferir tramas a través de la conexión.

Acceso con *Frame Relay* y ATM

Dado que los proveedores de servicio pueden según las estadísticas, multiplexar los datos de múltiples suscriptores sobre un único enlace y luego volver a transportar los datos de una red IP, normalmente los precios asociados a los servicios de acceso a Internet con *Frame Relay* y ATM son mucho más bajos que los precios de servicio dedicado, especialmente para empresas que disponen de redes *Frame Relay* y ATM por lo que no se requiere una infraestructura adicional.

Es importante entender la cantidad de agregación ejecutada por la red *Frame Relay* o ATM y además la capacidad y el diseño flexible del *gateway* a Internet. Por ejemplo un *gateway* a Internet sobresuscrito, podría provocar una degradación significativa en el rendimiento en un circuito de acceso a Internet.

Servicio de Abonado Digital

Los servicios de línea de abonado Digital (xDSL) proporcionan acceso a Internet de alta velocidad y bajo costo. Encaja adecuadamente entre el acceso telefónico y los servicios de acceso dedicado en términos de precio y velocidad.

Un beneficio clave de la tecnología xDSL es que puede utilizar los bucles de cables de par trenzado de cobre de la red de telefonía básica, convirtiéndola en una tecnología de acceso popular y pequeños negocios.

La calidad de los cables y la distancia de la oficina central (CO) servidora, puede tener que ver significativamente con el rendimiento y la tasa de transferencia característicos de una conexión xDSL.

[25] CPE: Equipo Terminal de Abonado
[26] PPP: Protocolo Punto a Punto
[27] HDLC: Protocolo de Control de Alto Nivel de Enlace de Datos

En la tabla 2.14 se presentan las características y aplicaciones más frecuentes de las diferentes tecnologías WAN.

SIGLAS	TECNOLOGIA WAN	VELOCIDAD MÁXIMA	APLICACIONES
RDSI	Red Digital de Servicios Integrado	128 Kbps	Usado en pequeñas WAN Provee capacidad adicional a una línea arrendada
X.25	X.25	64Kbps	Validar transacciones en un computador central Transferencia de datos Para un tráfico de ráfaga alto y no susceptible a retardo. Se cuenta con un canal de comunicaciones de calidad no muy alta.
FR	*Frame Relay*	1.544 MBps	Conecta LANs empresariales Interconectividad entre múltiples localidades (más de 3) Tráfico con característica de velocidad variable y con factor de ráfaga muy alto, a demás no debe ser sensible al retardo. Tarifa plana independiente de la distancia pero dependiente de la velocidad de puerto.
ATM	Modo de Transferencia Asíncrona	622 Mbps	*Backbone* de red Interconectividad entre redes LAN de 100 Mbps o más. Interconexión con múltiple servicios tales como *Frame Relay*
T1, T3	T1, T3	1.544 y 44.736 Mbps	Conectividad Central WAN Conectividad LAN - LAN Transporte de voz, datos y eventualmente vídeo.
XDSL	Línea del suscriptor digital	384 Kbps	Conectividad únicamente entre dos localidades Alto tráfico de red. Integración de voz, datos y vídeo en un solo canal. Tráfico a cursarse debe tener una característica de velocidad constante. Su costo es sensible a la distancia.

Tabla 2.14 *Características y aplicaciones de las tecnologías WAN*

X.25 básicamente transporta tráfico de datos, sin embargo actualmente existen múltiples paquetes de software de dominio público que permiten transmitir voz sobre IP en sistemas operativos tales como Windows, UNIX y OS de Macintosh.

Existen también paquetes de software de dominio público para transmitir vídeo sobre IP en sistemas operativos tales como Windows, UNIX y Macintosh. Actualmente las industrias que lideran el mercado, ofrecen las facilidades para integrar tráfico de voz, vídeo y datos sobre IP.

Frame Relay ha sido diseñada para transportar únicamente datos, pero en la práctica se ha demostrado que incluso puede transportar voz y vídeo con una baja calidad. ATM soporta transporte de voz datos y vídeo.

La necesidad de aplicaciones multimedia y de mezclar servicios en una línea de acceso integrada, constituyen las mayores ventajas de ATM. La tendencia actual son las tecnologías que integran múltiples tipos de tráfico (voz, datos y vídeo) y que pueden establecer prioridades entre dichos tipos de tráfico, apareciendo como una simple tecnología de transporte de datos.

Esta capacidad de integración brinda significativos ahorros en los costos, los mismos que pueden ser medidos al compararlos con los costos de adquirir nuevo hardware y software con el fin de "correr" aplicaciones adicionales como voz y vídeo en las redes tradicionales.

Considerando los criterios vertidos anteriormente y conociendo que el costo de ATM aún es elevado se opta para el presente diseño por un acceso dedicado de última milla *clear channel*[28] con tecnología ADSL.

El enlace de última milla puede utilizar diferentes medios, las principales características, se resumen en la tabla 2.15

La selección del medio físico de última milla requiere hallar el balance entre costo y confiabilidad del medio.

[28] *Clear Channel:* es una conexión dedicada que permite enlazar permanentemente dos puntos definidos.

TIPO DE CABLE CARACTERÍSTICA	PAR TRENZADO	COAXIAL	FIBRA ÓPTICA	MEDIOS INALÁMBRICOS
Ancho de Banda	Moderado	Grande	Muy grande	Grande
Atenuación	Alta	Moderada	Muy alta	Alta
Fiabilidad de transferencia	Baja	Alta	Muy alta	Baja
Seguridad	Baja	Moderada	Alta	Baja
Complejidad de instalación	Sencillo	Moderada	Compleja	Moderada
Costo	Bajo	Moderada	Alta	Alto

Tabla 2.15 *Características de los diferentes medios de transmisión*

Para proporcionar un enlace a Internet adecuado, se utilizará un *router* que cumplirá con dos funciones principales:

- Actuar como *gateway* para comunicaciones de voz
- Permitir el acceso de la red a Internet

Un *ruteador* es un dispositivo de propósito general diseñado para segmentar la red, limitar el tráfico de *broadcast* y proporcionar seguridad y control entre dominios de *broadcast*, también puede dar servicio de *firewall* [29]y el acceso a una red WAN (figura 2.15).

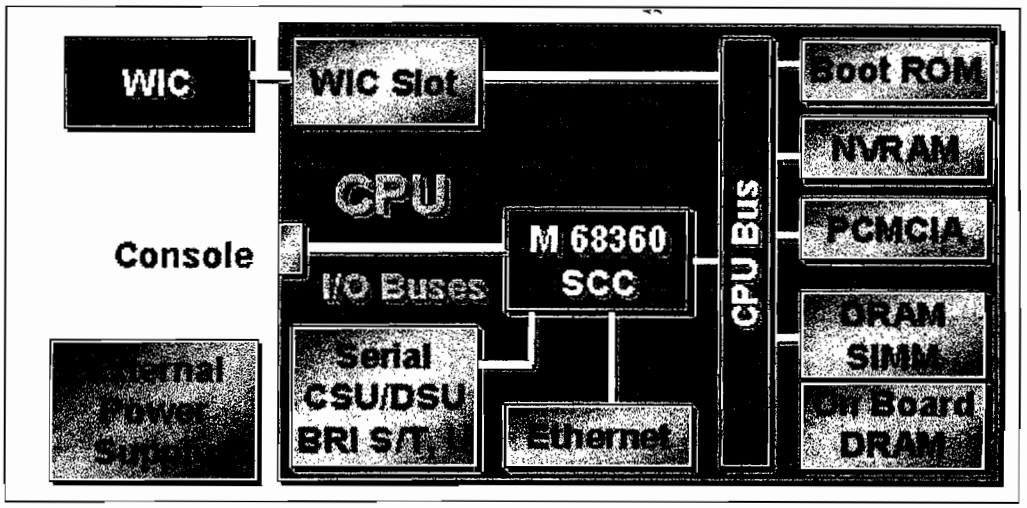


Figura 2.15 *Diagrama de bloques de la estructura interna del router [29]*

[29] *Firewall*: dispositivo físico o software sobre un sistema operativo, que filtra tráfico entre redes

El *router* opera en la capa 3 del modelo OSI y se distingue entre los diferentes protocolos de red, tales como IP, IPX, *AppleTalk*; esto le permite tomar una decisión más inteligente a la del *switch*, al momento de enviar los paquetes.

Las funciones primarias de un *router* son:

- Segmentar la red dentro de dominios individuales de *broadcast*
- Suministrar un envío inteligente de paquetes
- Soportar rutas redundantes en la red

Otros importantes beneficios del *ruteador* son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN
- Integrar diferentes tecnologías de enlace de datos, tales como *Ethernet*, *Fast Ethernet*, *Token Ring*, FDDI y ATM.

El *router* que se utilizará en la Intranet deberá tener las siguientes características:

- Dos puertos *Ethernet* 10/100
- Un puerto serial a 128 Kbps

2.5 PROVEEDORES DE SERVICIOS DE INTERNET (ISPs)

El costo de instalación de una línea especial de alta velocidad para el acceso a Internet (incluso para cortas distancias), resultaría muy costoso. Existen compañías especializadas que pagan la costosa conexión a Internet, hacen grandes inversiones en servidores de alto rendimiento, líneas de datos y *módems*, y después rentan tiempo a otros usuarios interesados en tener acceso al Internet. Estas compañías se denominan Proveedores de Servicios de Internet (ISPs), los cuales ofrecen servicios propios de un controlador de comunicaciones y abren la puerta de acceso a Internet. (figura 2.16).

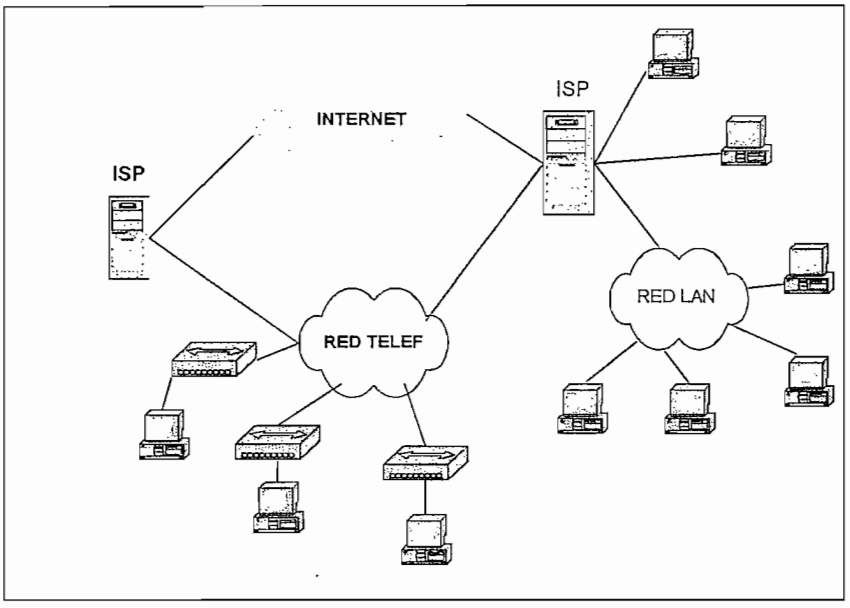


Figura 2.16 *Proveedor de Servicios de Internet (ISP)[46]*

Un elemento importante a tomar en cuenta será, que el ISP sea activo y ofrezca asistencia siempre que se planteen dudas o problemas de utilización.

También será conveniente analizar si el ISP dispone o no de más de una conexión con Internet, con el fin de que un ISP no esté fuera de servicio durante varios días por una simple avería en un cable.

Otro elemento importante de selección es la calidad de servicio. La calidad de servicio (QoS) puede definirse como el rendimiento de los servicios observados por el usuario final. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros. En su conjunto, esas condiciones forman un contrato de tráfico entre el usuario y la red, conocidas como SLA.

2.5.1 ACUERDOS DE NIVEL DE SERVICIO (SLA)

Los SLA especificarán los servicios y las calidades que los clientes recibirán, bien sean estáticos o dinámicos. En los acuerdos estáticos, los usuarios podrán transmitir/recibir información en cualquier momento, mientras que en los SLA dinámicos utilizarán un protocolo de señalización tipo RSVP[30] para solicitar servicios y recursos bajo demanda, antes de la transmisión.

[30] RSVP: *ReSerVation Protocol*

El cumplimiento de los SLAs se garantizan mediante penalizaciones por incumplimiento (o premios por mejora de la calidad). El incumplimiento de un nivel mínimo de calidad, puede suponer la cancelación inmediata del contrato.

Los SLAs:

- Deben garantizar al cliente que el proveedor cumplirá sus responsabilidades
- Deben facilitar al proveedor la regulación de las nuevas necesidades o cambios que el cliente propone
- Deben ser orientados al cliente, medibles y alcanzables.
- Deben ser revisados periódicamente.
- Se deben pactar y deben contener planes de contingencia
- Deben tener estructurado un modelo de penalizaciones ante posibles incumplimientos del proveedor

Los aspectos a considerarse en un SLA son:

- Tipo de servicio.
- Tiempos de Respuesta
- Disponibilidad del Sistema:
  - Número de incidencias negativas en un periodo
- Conectividad:
  - Tipos de equipos que utilizan
- Integridad de los Datos
- Garantías del sistema:
  - Provisiones para seguridad
  - Soporte a clientes y asistencia técnica
  - Planes de Contingencia
- Multas por caída del sistema
- Tareas Preventivas

2.5.2 PARÁMETROS PARA EL ANÁLISIS DE CALIDAD DE SERVICIOS DE LOS ISPs

Un *backbone* de red de un ISP abarca muchas características técnicas importantes, incluyendo las siguientes:

- Topología física de red
- "Cuellos de botella" en la red y tasa de suscripción
- Nivel de redundancia del acceso a Internet de un ISP

Conexiones Físicas

Una topología física adecuada es una que pueda proporcionar un ancho de banda consistente y adecuado para toda la trayectoria del tráfico, incluso en el caso de que una o varias conexiones no estén disponibles.

Los clientes deberían investigar la topología física del proveedor, y el proveedor debería ser capaz de proporcionar un mapa actualizado de la red con todas las conexiones indicadas.

"Cuellos de botella" potenciales de los ISPs y tasa de suscripción

Hay dos "cuellos de botella" potenciales en un ISP: sobre-suscripción de enlaces troncales del *backbone* y circuitos pequeños que llevan a un cliente con flujo de tráfico descendente; un proveedor no debería suscribir peligrosamente sus conexiones sobrecargando sus *routers* en el intento de ganar dinero porque le llevará a perder la credibilidad a largo plazo.

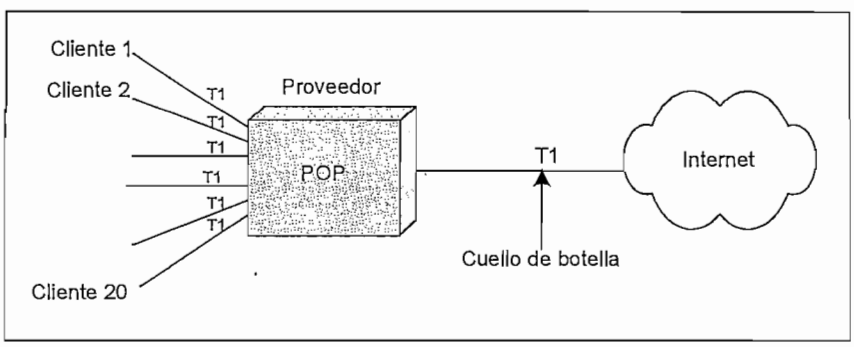


Figura 2.17. Límites de rendimiento del enlace de un ISP [4]

"La sobre-suscripción ocurre cuando la utilización acumulada de múltiples enlaces excedan el ancho de banda del conducto utilizado para transportar el tráfico a su destino. Un proveedor que vende 20 T1 en un POP[31] y se conectan a una NAP[32] mediante un enlace T1 experimentará un "cuello de botella" en la conexión al NAP tal como se ilustra en la figura 2.17. No deberá haber más de cinco enlaces T1 por cada conexión T1 al *backbone*"[4].

Otro ejemplo de "cuello de botella" potencial son los sitios de alta velocidad que intentan acceder a información de sitios de baja velocidad. Un servidor *web* ubicado en un sitio conectado a Internet mediante un enlace de 56 Kbps puede ser accedido a una velocidad máxima de 56 Kbps sin reparar en la velocidad de los enlaces utilizados por las personas que acceden al sitio.

La figura 2.18 ilustra un cliente con acceso T3 a Internet que será limitado a no más de 56 Kbps cuando acceda al servidor *Web*. Obsérvese también que si otro usuario intenta acceder al sitio al mismo tiempo, todos deberán compartir la conexión de 56 Kbps.

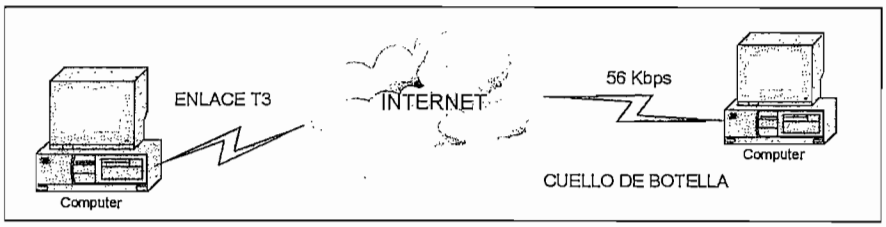


Figura 2.18. *La velocidad de acceso está limitada por el ancho de banda más pequeño [4]*

Es importante que los proveedores controlen y administren la utilización de los enlaces en sus redes. Antes de comprometerse a adquirir los servicios de un ISP, los clientes deberían formular a los proveedores potenciales las siguientes preguntas:

¿Cómo administra la utilización de los enlaces?
¿En que umbral comienza a proporcionar capacidad adicional?

[31] POP: Punto de Presencia
[32] NAP: Punto de Acceso a la Red

¿Cuáles son las tasas de suscripción para este servicio (capacidad disponible, utilizada)?
¿Cuáles son las tasas típicas de suscripción para el *backbone* de la red y los puntos de interconexión?
¿Cuál es el "cuello de botella" teórico para este servicio?

Nivel de redundancia del acceso a Internet de un ISP

Sea por el mal tiempo, por problemas de la portadora o simplemente mala suerte, la conexión de un ISP a un NAP, a otro proveedor o a otro POP no podrá estar disponible en algún punto, lo que dará como resultado la imposibilidad de alcanzar un conjunto de destinos. Una red redundante permite que el tráfico utilice una ruta alternativa para alcanzar dichos destinos mientras se soluciona el problema.

Es importante comprender que la redundancia de interconexión con otras redes son proporcionadas sobre una base global. Si la conexión a un proveedor deja de estar disponible a través del punto de intercambio de tráfico primario se seleccionará el siguiente punto de intercambio más cercano. La idea es asegurarse de que existe la suficiente capacidad de interconexión y *backbone* sobrante para evitar los fallos en uno o más lugares de red. Cuando se habla de redundancia, también debería considerarse un plan de reposición del proveedor.

Algunos proveedores prefieren subcontratar los servicios de repuestos, normalmente a compañías que tienen oficinas geográficamente dispersas, aunque esta actuación incrementa potencialmente el MTR[33] cuando surgen problemas.

2.5.3 ANÁLISIS DE LA CALIDAD DE SERVICIO DE LOS ISPs EN QUITO

Considerando los parámetros mencionados en la sección anterior en lo que respecta a calidad de servicios de los ISPs, se procedió a formular una encuesta que permitió conocer algunos parámetros utilizados por los ISPs.

[33] MTR: Tiempo Medio de Reparación

La encuesta fue realizada tomando una muestra de 8 ISPs que brindan servicio a la ciudad de Quito, medio por el cual se pudieron obtener los datos mostrados en la tabla 2.16.

La mayor parte de los ISPs ofrecen una disponibilidad de enlace de alrededor del 99%, los contratos realizados por algunos ISPs, no especifican multas para los proveedores de servicio en caso de no cumplir con la calidad de servicio ofrecido.

Un 70% de los ISPs encuestados trabajan con conexiones al *backbone* de Internet por medio de fibra óptica, mientras que el 30% restante utiliza enlace satelital para su conexión al *backbone,* el BER fluctúa entre 1exp –8 y 1exp -10.

El 20% de ISPs encuestados no cuenta con una conexión de respaldo para situaciones de caída de enlace o las líneas que ofrecen para éste propósito no son las más adecuada y el 80% dijeron contar con equipos de respaldo para sus *routers* principales; las marcas preferidas en lo que a *routers* se refiere son las series Cisco y en cuanto a servidores trabajan con SUN, DELL, IBM, HPs.

Todos los ISPs encuestados cuentan con planes de contingencia para situaciones de incendio y cortes de energía eléctrica, y realizan mantenimiento a todos sus equipos en un tiempo promedio de dos meses.

En lo que respecta a servicios de valor agregado brindado al cliente incluyen servicios de *Web hosting*, diseño de páginas *Web*, venta de dominios y asesoramiento técnico.

Para la selección del ISP que brindará la conexión a Internet de la Intranet se consideró como parámetros fundamentales:

- Que cuenten con conexión de Fibra óptica debido a que este medio de transmisión provee una conexión confiable y alta capacidad de canal
- Que posea un enlace redundante para situaciones de caída de enlace
- Que ofrezca un buen tiempo de respuesta y gran disponibilidad de enlace
- Una baja tasa de bits errados

	DISPONIB. (%)	T. RESPUESTA (ms)	BER	BACKBONE	ENLACES REDUNDANTES	PLATAFORMA SERVIDORES	SERVICIOS DE VALOR AGREGADO
Access Ram	99	150	1 exp -9	Fibra óptica	SI	Unix	Web Hosting Dominio propio Asesoramiento técnico
ECUTEL	98	-	1 exp -8	Satelital	SI	Linux	Web Hosting Asesoramiento técnico
Interactive	90	200	1 exp -8	Fibra óptica	NO	-	Web Hosting Dominio propio Asesoramiento técnico
Intercom-ECUANEX	99,9	150	1 exp -10	Fibra óptica	SI (dial up)	Linux	Web Hosting Dominio propio Asesoramiento técnico
ONNET	96	-	1 exp - 9	Fibra óptica	SI	Linux, Windows	Web Hosting Asesoramiento técnico
P@nchoNet	98	150	1 exp -10	Fibra óptica	SI	-	Web Hosting Dominio propio Asesoramiento técnico
Quik Internet	96	540	1 exp -9	Satelital	SI	-	Web Hosting Dominio propio Asesoramiento técnico
TELCONET	99,5	150	1 exp -10	Fibra óptica	SI	Linux, Solaris	Web Hosting Dominio propio Asesoramiento técnico

Tabla 2.16 Características de los diferentes ISPs de la Ciudad de Quito

- Costo moderado
- Plataforma de los servidores

Bajo estos criterios se recomienda como posible proveedor de Internet a TELCONET, por cuanto cuenta con:

- Un *backbone* nacional, basado en redes IP con enlaces redundantes satelitales y de fibra óptica. La velocidad de este *backbone* es de hasta 1 Gbps, soportando enlaces sincrónicos de hasta un STM1 (155 Mbps)
- Cuenta con una disponibilidad del 99.5%
- Trabaja con servidores Linux que ofrecen un alto nivel de seguridad al sistema
- Posee múltiples puntos de intercambio de tráfico con grandes proveedores como UUnet y Sprint, además posee interconexión con USA a través un cable submarino de fibra óptica perteneciente a Emergia (Telefónica de España)
- Ofrece una tasa de bits errados de 1 exp-9
- Tiene un costo similar respecto a los otros ISPs

2.6 SISTEMAS OPERATIVOS Y SOFTWARE DE RED

Como se conoce una red se compone de una o más computadoras conectadas entre sí por medio de una o más tecnologías de red como *Ethernet*. Para que una serie de protocolos funcione adecuadamente y transfiera datos entre las computadoras de una red, ésta debe correr un software especial llamado sistema operativo de red.

De la misma forma que un sistema operativo de escritorio, como Windows de Microsoft controla la ejecución de programas y almacenamiento de información en una PC por parte del usuario, un sistema operativo de red controla el funcionamiento conjunto de las diferentes piezas de hardware y software de una red.

Los sistemas operativos de las redes LAN – PC más difundidos en la actualidad son: Windows Server de Microsoft y Linux.

Los sistemas operativos de redes funcionan con el modelo de red cliente – servidor, los cuales dividen una aplicación para redes en dos partes: la parte del cliente y la parte del servidor.

Los sistemas operativos de redes controlan la operación de un servidor de red. Los sistemas operativos de redes hacen uso de una o más protocolos de red para transferir datos de y hacia los clientes, como TCP/IP, o IPX/SPX que definen sencillamente un conjunto de reglas para coordinar la comunicación en red entre los sistemas.

2.6.1 SISTEMAS OPERATIVOS

Una Intranet se compone de una o más computadoras conectadas entre sí. A continuación se realiza un análisis de los diferentes sistemas operativos tanto de red como de cliente, que permitirá elegir la opción más adecuada.

a. Sistema operativo de red

El sistema operativo de red es aquel que mantiene a dos o más computadoras unidas a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder compartir los diferentes recursos y la información del sistema

Las mejores opciones del sistema operativo de red son UNIX y Windows. UNIX es un sistema operativo de eficacia comprobada apto para el modelo de sistemas abiertos de Internet; si el usuario está familiarizado con el sistema operativo UNIX, puede instalar un servidor en forma casi gratuita, pero por desgracia la mayoría de usuarios no están capacitados adecuadamente para el manejo de estos servidores. La mayoría de los programadores prefieren desarrollar aplicaciones con máquinas basadas en Windows, usando lenguajes de programación como Visual Basic de Microsoft.

Muchas compañías optan por Windows en lugar de UNIX a causa de la facilidad de instalación, mantenimiento y administración de la red.

A continuación se describen las ventajas y desventajas de este sistema operativo:

WINDOWS 2003 SERVER

Windows Server 2003 representa una nueva generación tecnológica y un importante avance en la evolución de la plataforma de servidores Windows. Sus mejoras en rendimiento, conectividad, ahorro de costos y la seguridad que ofrece lo han convertido en uno sistemas operativos de red más usados

Ventajas

- Presenta una gran disponibilidad de actualizaciones automáticas del sistema a través del Windows System Resource Manager
- Ofrece mejor conectividad, facilitando al máximo la configuración de enlaces entre delegaciones, acceso inalámbrico seguro y acceso remoto a aplicaciones a través de los Terminal Services, así como en su integración mejorada con dispositivos y aplicaciones
- Permiten disponer de aplicaciones Windows e incluso de los propios escritorios Windows en prácticamente cualquier dispositivo, incluyendo aquellos que ni siquiera funcionan bajo sistemas operativos Windows
- Soporta múltiples procesadores
- Tiene una interfaz de usuario muy amigable

Desventajas

- Cuando se descubre un error en la versión reciente del sistema, Microsoft se espera al lanzamiento de la siguiente versión para solucionarlo
- Presenta costos elevados
- Requiere de gran cantidad de recursos como son memoria, disco duro, etc
- Aún presenta algunos agujeros de seguridad por lo que lo vuelven ocasionalmente inestable.

UNIX

El sistema operativo UNIX ha evolucionado durante los últimos veinte años desde su invención como experimento informático hasta llegar a convertirse en uno de

los sistemas operativos más populares e influyentes del mundo. UNIX es el sistema más usado en investigación científica, pero su aplicación en otros entornos es bastante considerable. UNIX tiene una larga historia y muchas de sus ideas y metodología se encuentran en sistemas como DOS y Windows

Ventajas

- Sistema multiusuario real, puede correr cualquier aplicación en el servidor
- Es escalable, con soporte para arquitectura de 64 bits
- El costo de las diferentes variantes de Unix es muy reducido y algunas son gratis, como FreeBSD y Linux
- Se pueden activar y desactivar *drivers* o dispositivos sin necesidad de reiniciar el sistema
- UNIX puede trabajar con CLI (*Command Line Interface*)
- Los *kernels* de Unix se confeccionan según las necesidades
- Ofrece la capacidad de realizar cómputo remotamente
- Es la mejor solución para enormes bases de datos

Desventajas

- La interfaz de usuario no es muy amistosa en algunas versiones
- Requiere capacitación, ya que debido a su complejidad, no cualquiera puede usarlo
- Padece de la falta de aplicaciones comerciales con nombres importantes.
- La efectividad como servidor de archivos e impresión no es tan eficiente como en otros NOS[34]
- Hay discrepancias entre los distintos diseñadores y vendedores de UNIX.

Para poder hacer una selección adecuada del NOS, es importante tener una opinión objetiva de las personas que trabajan, o están de alguna manera involucradas en el funcionamiento de estos sistemas operativos, brindar una perspectiva un poco más amplia de los pros y contras de cada sistema, teniendo en cuenta los siguientes aspectos:

[34] NOS: *Network Operative System*

- Funcionalidad
- Administración del sistema
- Rendimiento

La tabla 2.11 muestra algunos criterios comparativos que ayudarán a realizar una mejor selección del sistema operativo necesario para la red.

CARACTERÍSTICA	WINDOWS 2003	UNIX
Funcionalidad	alta	alta
Facilidad de uso	alta	moderada
Confiabilidad	moderada	alta
Rendimiento	moderada	alta
Estabilidad	moderada	alta
Costo	alto	moderado
Recursos *freeware*	bajo	alto

Tabla 2.17 *Cuadro comparativo de los sistemas operativos Windows vs UNIX [39]*

Por cuestiones de estabilidad, seguridad y principalmente bajo costo, se selecciona UNIX (Linux Red Hat 9.0) como el sistema operativo más adecuado para el manejo de los servidores de red.

b. Sistema Operativo Cliente

Los sistemas operativos Macintosh trabajan exclusivamente con hardware Macintosh, en contraste con Windows y Linux que son más abiertos a trabajar con cualquier hardware.

Linux no cuenta con una interfaz de usuario amistosa en algunas versiones y requiere capacitación, ya que debido a su complejidad, no cualquiera puede usarlo; por esta razón es aconsejable analizar entre las diversas opciones que ofrece Windows.

La tabla 2.12 presenta la comparación entre las versiones más recientes del sistema operativo Windows.

	Windows 98	Windows ME	Windows 2000	Windows XP
Requerimientos del sistema	486DX/66, 195MB 16MB	P150 320MB 32MB	P133 650MB 64MB	Pentium/300 1.5GB, 128Mb
Lanzado el año	1998	2000	1999	2001
Máxima Memoria soportada	512 MB	512 MB	4 GB	4 GB
Instalación Completa	295 MB	550 MB	650 MB	1.2 GB
AutoActualización por Internet	No	Si	No	si
Gestor de Arranque	No	No	Si	si
Mutiusuario/ Operaciones Multitarea	no/si	no/si	si/si	si/si
Compatibilidad	DOS	DOS	DOS OS/2 Posix	DOS, /NT /2000
Archivo de Sistema	FAT16 ,FAT32	FAT16, FAT32	FAT16, FAT32, NTFS	FAT16, FAT32, NTFS
Sistema de Recuperación	No	Si	System File Protection	si
Archivo/Encriptación de discos	No	No	SSL,PCT,(Pro versión)	SSL, PCT, EFS (Pro versión)
Software cliente/servidor	Si	Si	Si	si
Antivirus/Firewall personal	no/no	No/no	no/no	no/si
Software de video/Grabación	no/no	No/no	no/no	Movie Maker/si
Reproductor/Grabador de DVD	No		No	si

Tabla 2.18 *Características de las versiones Windows [40]*

Windows XP incorpora un nuevo diseño visual para los usuarios con mejoras para proporcionar una imagen más fresca del PC, ofrece una amplia conectividad con otros dispositivos y que a diferencia de otras versiones anteriores de Windows incluye un *firewall* o cortafuegos personal que evita que determinados accesos de gente no deseable se filtren en la PC valiéndose de las nuevas aplicaciones de comunicación instantánea (*Windows Messenger)*, o por reproductores de audio y vídeo (Windows *Media Player);* otra razón para seleccionar este sistema operativo es el editor de vídeo doméstico como es el *Windows Movie Maker* y la versión de Internet Explorer 6.0.

2.6.2 SOFTWARE PARA LOS SERVICIOS DE LA INTRANET

El software para una Intranet, depende de los servicios y aplicaciones brindadas por la Intranet.

Existen varios tipos de programas que se ofrecen bajo licencia "*shareware*" (demostraciones) permitiéndose probarlos durante un plazo de varias semanas y con acceso a un manual de usuario mientras que otras son "*freeware*" (versiones gratuitas), y versiones comerciales.

a. Software para vídeoconferencia y chat

Dentro de la categoría de sistemas personales de vídeoconferencia hay que destacar el grupo denominado "*Web Cam*" que consiste en la utilización de una cámara de vídeo con su programa de instalación y una serie de programas de vídeoconferencia que dejan el tratamiento del sonido a cargo de la tarjeta de sonido, micrófono y altavoces del ordenador donde están instalados. Este tipo de equipos están proliferando debido al reducido costo de una llamada telefónica sobre Internet y a su relativa calidad.

Estos programas permiten las siguientes posibilidades:

- Enviar y recibir audio
- Enviar y recibir vídeo
- Enviar y recibir texto (*chat*)
- Compartir una pizarra
- Transferencia de ficheros

La tabla 2.17 presenta algunas características de los diferentes programas disponibles para vídeoconferencia. De esta tabla se desprende que para la utilización de vídeoconferencia a través de Internet, *Netmeeting* presenta mayores ventajas por ser un software gratuito, transporta simultáneamente audio, video y datos proporcionando los siguientes servicios:

- "Chatear" (en modo texto) hasta con 8 persona, el número de participantes está limitado por el ancho de banda disponible y por la potencia del PC

PRODUCTO	LICENCIA	TAMAÑO (MB)	SISTEMA	AUDIO	VÍDEO	CHAT	PIZARRA	FTP	PUNTUACIÓN
CU-SEEME	*Shareware*	10.7	WIN 95/98/NT 4.0 , MAC	SI	SI	SI	SI	NO	AUDIO **R** VÍDEO **B**
VÍDEO VOXPHONE GOLD	*Shareware* 30 días	0.06	WIN 95/98/NT 4.0	SI	SI	SI	NO	SI	AUDIO **M** VÍDEO **M**
INTERNET PHONE	*Shareware* 30 días	5.2	WIN 95/98/NT 4.0, MAC	SI	SI	SI	SI	SI	AUDIO **R** VÍDEO **MB**
HONEYCOM	*Sareware*	2.85	WIN 95/98/NT 4.0	SI	SI	SI	SI	SI	AUDIO **R** VÍDEO **R**
NETMEETING	*Freware*	2.59	WIN 95/98/NT 4.0	SI	SI	SI	SI	SI	AUDIO **B** VÍDEO **B**

Tabla 2.19 *Programas para vídeoconferencia a través de Internet [41]*

Donde:

M = malo

R = regular

B = bueno

MB = muy bueno

- Intercambiar información gráfica sobre una pizarra electrónica hasta con 8 participantes
- Compartir aplicaciones con otros usuarios
- Enviar ficheros hasta a 8 participantes simultáneamente
- Llamar a otras personas (Telefonía IP), a cualquier parte del mundo
- Hacer vídeoconferencias

La configuración del *Netmeeting*, se lo presenta en forma detallada en el Anexo E.

Para las PCs de los usuarios de la Intranet se requerirá como base el paquete Microsoft Office, que cuenta con procesador de palabra, hojas electrónicas y otros servicios; adicionalmente se instalarán los paquetes que se ajusten a las necesidades del usuario.

2.7 CONFIGURACIÓN DE EQUIPOS

La conexión a Internet abre un extraordinario abanico de servicios, pero es necesario tener claro las limitaciones que imponen los condicionantes de seguridad y economía.

El buen funcionamiento de la red depende en gran medida de una correcta configuración de los equipos, pues de nada serviría contar con equipos de última tecnología si no se aprovechan estas facilidades.

Esta sección describe las configuraciones de todos los equipos de red que forman parte de la Intranet, las mismas que serán planteadas de acuerdo a la aplicación de cada equipo y al sistema operativo utilizado.

Como punto de partida se establece un diseño lógico de la red, que cuenta con tres zonas, que permitirán brindar un buen nivel de seguridad a la Intranet.

Zona de seguridad: La razón para la creación de esta zona es que la mayor parte de ataques a la red provienen desde el exterior, esta zona filtrará el tráfico

entrante y saliente de la red lo cual se verá reflejado en un nivel considerable de seguridad.

Zona desmilitarizada (DMZ): Se plantea esta zona para los servidores *Web* y correo electrónico, debido a que son servicios que están en continuo contacto con el medio externo, lográndose mayor funcionalidad y seguridad para la red interna.

Si bien es cierto que la zona desmilitarizada es de acceso público, esto no implica dejarla sin algún nivel de seguridad.

Para la intranet se considera dividir esta zona en dos niveles:

a. Zona de seguridad para la DMZ.- Está compuesta por dos equipos:

- *Router*.- Permite el tráfico de paquetes IP y mantiene listas de acceso que son reglas que filtran el tráfico en función de direcciones IP, protocolos y números de puertos.

- *Firewall* de los servidores.- Es un software incorporado al Sistema Operativo Linux que utilizarán los equipos servidores, cuyo nivel de seguridad es diferente al *firewall* que protege la red LAN.

b. Zona de seguridad para la red LAN.- Está constituída por una máquina Linux que incluye *firewall*, *proxy* y NAT. Por funcionalidad también se ha incorporado un servidor DNS a nivel interno. Esta equipo utilizará dos tarjetas de red: una que se comunica con el *firewall* de los servidores *Web* y *mail* y una segunda que se comunicará con la red LAN.

Zona Interna: Está compuesta por todas las máquinas que conforman la red LAN de la Intranet, que se halla subdividida en dos grupos de trabajo uno para la administración y control y otro para los usuarios.

En la figura 2.19 se presenta la distribución lógica y los equipos que conforman cada una de las zonas.

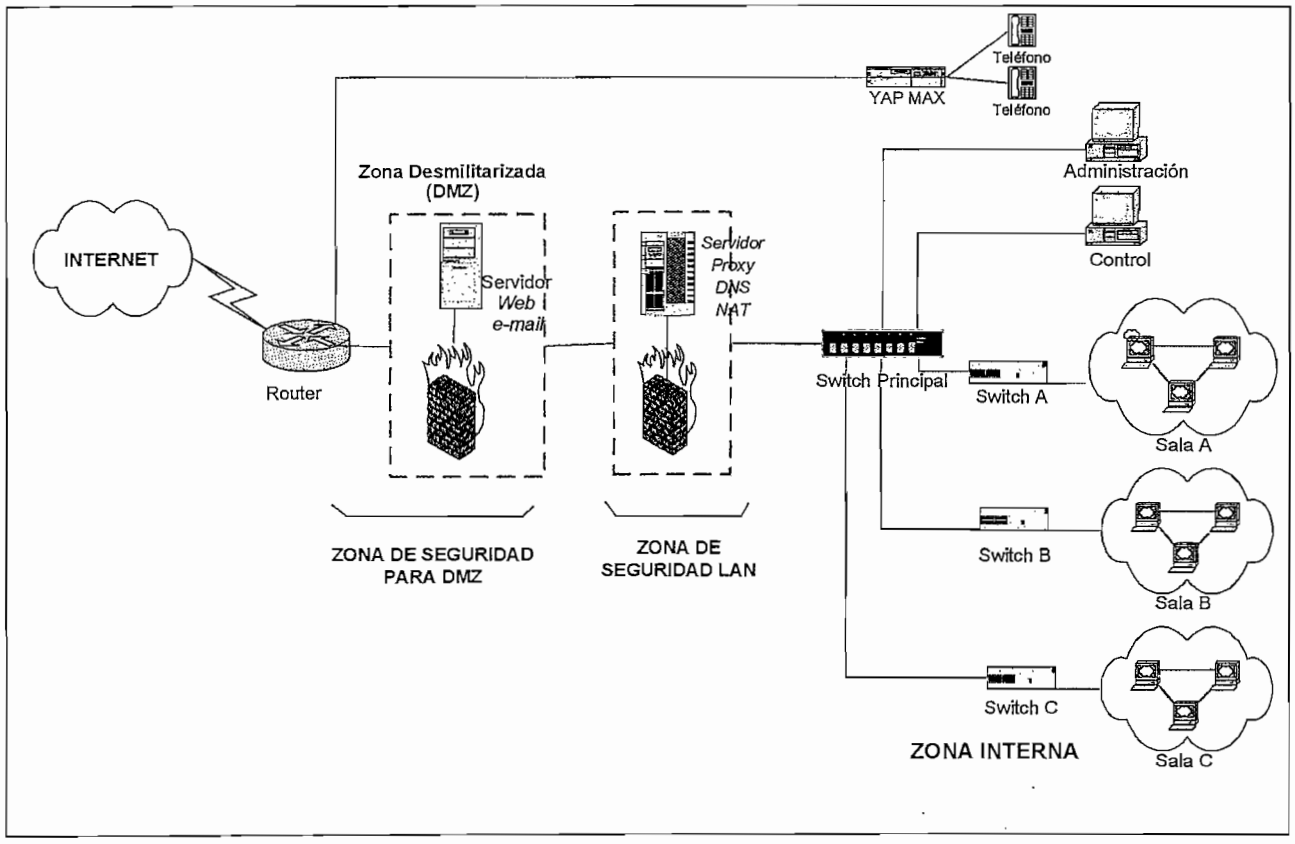


Figura 2.19 *Distribución lógica de la Intranet*

2.7.1 ASIGNACIÓN DE DIRECCIONES IP

El esquema de direccionamiento que se utiliza hoy en día se basa en la versión 4 del Protocolo Internet (IPv4), conocida normalmente como IP, sin embargo se debe tomar en cuenta que a futuro se utilizará el protocolo de direccionamiento IPv6, el cual establece un espacio de direcciones de 128 bits con un mecanismo de opciones que simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6.

Adicionalmente IPv6 aumenta la flexibilidad en el direccionamiento pues incluye el concepto de dirección *anycast* mediante el cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos, además habilita el etiquetado

de los paquetes para identificarlos con flujo de tráfico en particular que permita al emisor solicitar un tratamiento especial para dicha información.

Para este proyecto de titulación se utiliza el esquema de direccionamiento IPv4, debido a que en el país aún no se utiliza IPv6. De acuerdo a las necesidades de conectividad las direcciones IP se las puede dividir en dos categorías:

Direcciones IP públicas
Direcciones IP privadas

a. Direcciones IP públicas

Es una dirección asignada por un Proveedor de Servicios de Internet (ISP), que permite que los equipos sean reconocidos tanto a nivel local como global.

b. Direcciones IP privadas

Son direcciones asignadas por el administrador de la red local y permiten que los equipos sean reconocidos únicamente a nivel interno.

Existen tres bloques de direcciones IP, conocidas como direcciones privadas o reservadas.

Direcciones clase A: 10.0.0.0 hasta 10.255.255.255
Direcciones clase B: 172.16.0.0 hasta 172.31.255.255
Direcciones clase C: 192.168.0.0 hasta 192.168.255.255

Si se utilizan direcciones en los rangos antes mencionados, no se requiere obtener permisos de un registro de direcciones.

Las estaciones de trabajo que tienen direcciones privadas pueden coexistir con las estaciones de trabajo con direcciones públicas como se indica en la figura 2.20, puesto que se puede elegir configurar la mayoría de estaciones de trabajo con direcciones privadas y mantener un pequeño segmento de red con direcciones IP públicas que permitan la salida de la red a Internet.

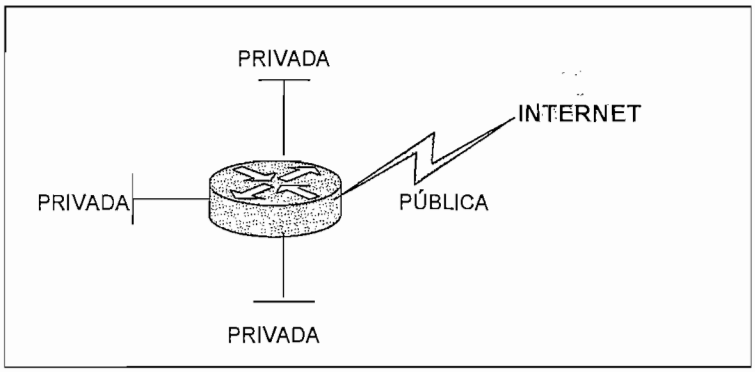


Figura 2.20 Estaciones de trabajo con direcciones privadas accediendo a recursos de Internet [4]

Las redes que tengan la necesidad de migrar de direcciones privadas a direcciones públicas para el acceso a Internet lo pueden hacer con la ayuda de la tecnología de un Traductor de direcciones de red (NAT)[35]. La tecnología NAT permite a las redes privadas conectarse a Internet mediante la traducción de direcciones IP privadas a direcciones IP públicas, cuando las estaciones de trabajo internas requieren conexiones con destinos en Internet (figura 2.21).

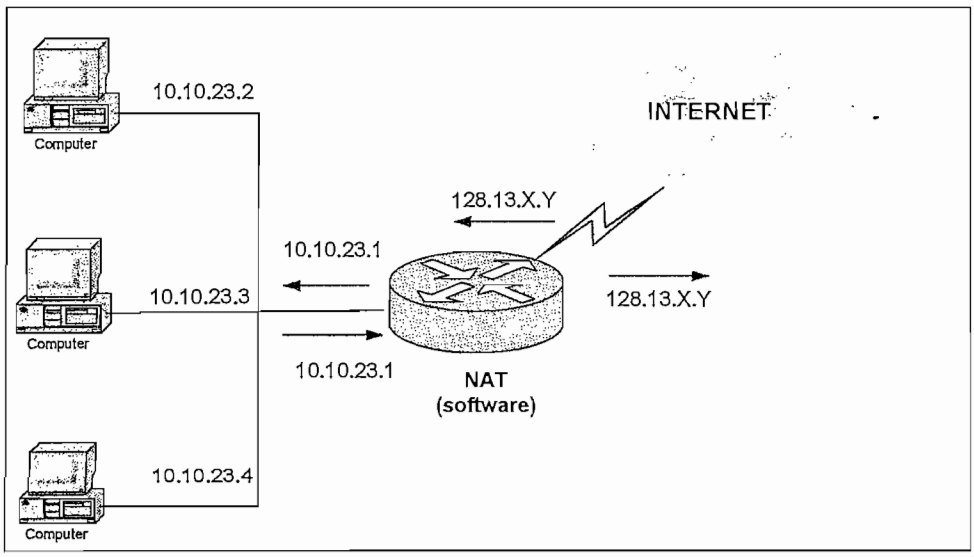


Figura 2.21 Traductor de direcciones de red [33]

Un NAT (*Network Address Translation*), es un mecanismo para la conservación de direcciones IP, ya que permite relacionar múltiples direcciones IP privadas con

[35] NAT: *Network Address Translation*

una única dirección IP pública pero usando diferentes puertos TCP de ésta. Esto es especialmente útil cuando el número de computadoras dentro de la red LAN es mayor que el número de direcciones públicas asignadas por el proveedor de Internet (figura 2.22).

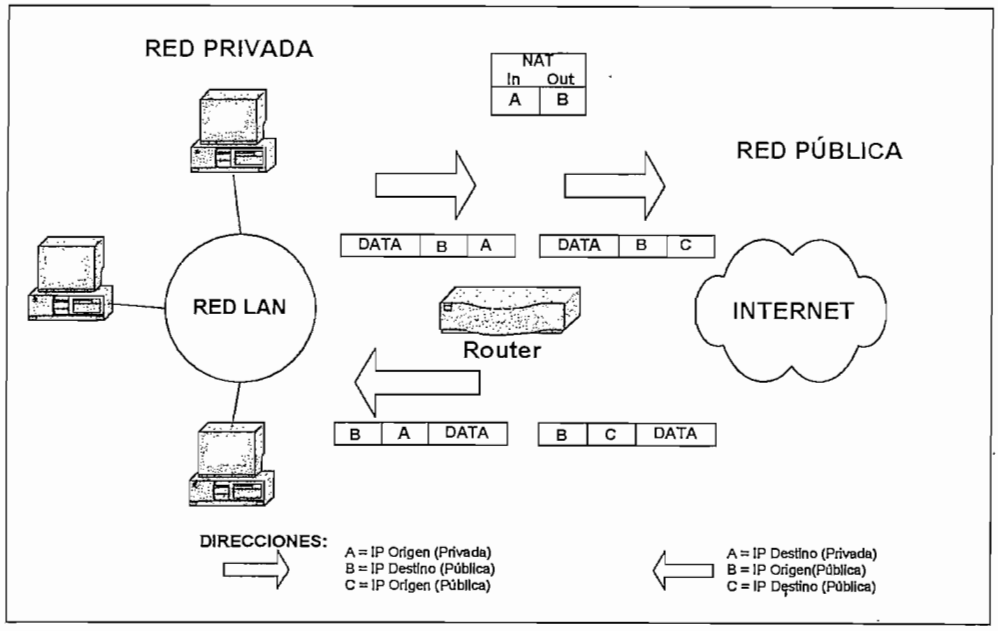


Figura 2.22 *Traslación de direcciones de Red NAT [35]*

El Proveedor del Servicio de Internet, Telconet, deberá asignar al menos seis direcciones IP públicas para el uso de la red, es decir será necesario utilizar direcciones públicas con máscara de 29 bits (255.255.255.248) y que serán distribuidas como se muestra en la figura 2.23 asumiendo que la dirección pública es 212.194.89.24/29, aclarando que las direcciones del enlace WAN pertenecen al ISP.

La dirección asignada al servidor Proxy, permite la salida al Internet de las 44 estaciones de trabajo utilizando una configuración NAT.

La dirección privada clase C (192.168.0.0) será distribuida a las estaciones de la red local, las mismas que de acuerdo a su función en la red estarán divididas en dos grupos:

Grupo A.- Formado por el PC de administración y la máquina de control.

Grupo B.- Formado por las estaciones de trabajo de las diferentes salas.

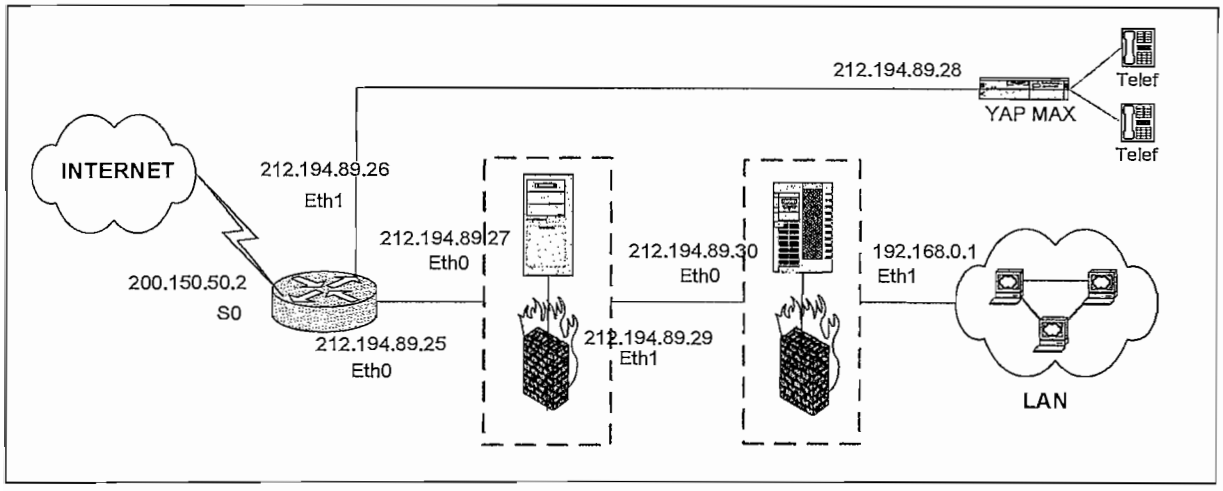


Figura 2.23 *Distribución de direcciones IP públicas*

La figura 2.24 muestra el resumen de la asignación de direcciones IP para la Intranet.

En el Anexo F, se detalla la asignación de direcciones IP para las máquinas de la Intranet.

Las PCs de usuarios utilizarán el sistema operativo Windows XP, cuya configuración de red se describe a continuación:

1.- Menú Inicio, configuración, panel de control y hacer *click* derecho en el icono conexión de área local y escoger la opción propiedades en la que se visualizará la pantalla que se indica en la figura 2.25

2.- Buscar en la lista de elementos el protocolo Internet (TCP/IP). En caso de no encontrarlo entre los elementos instalados, proceder a instalarlo de la siguiente forma: hacer *click* sobre el botón "Instalar...", escoger Protocolo y seleccionar "Agregar...". En la lista de protocolos de red escoja el protocolo Internet (TCP/IP).
3.- Una vez instalado el protocolo TCP/IP se procede a configurar la dirección IP, máscara de subred y *gateway* de las estaciones de trabajo de acuerdo a la distribución preestablecida en el Anexo F (figura 2.26).

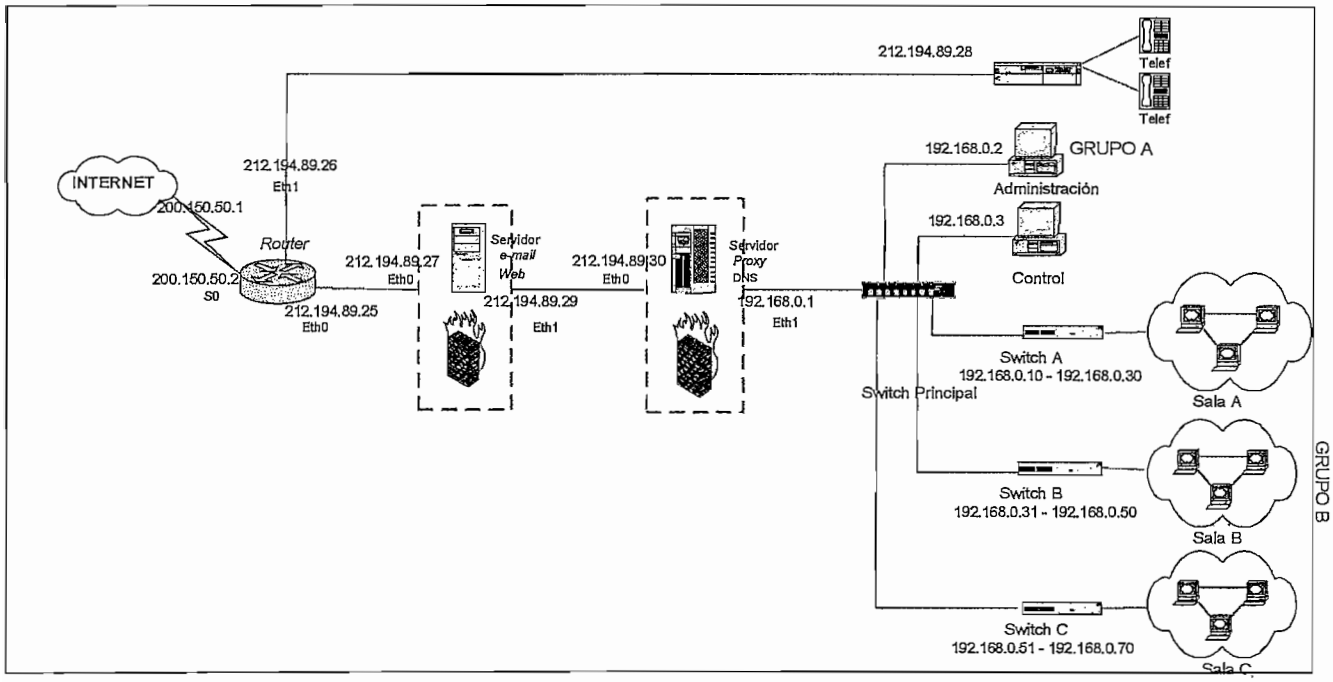


Figura 2.24 Asignación de direcciones IP para la Intranet

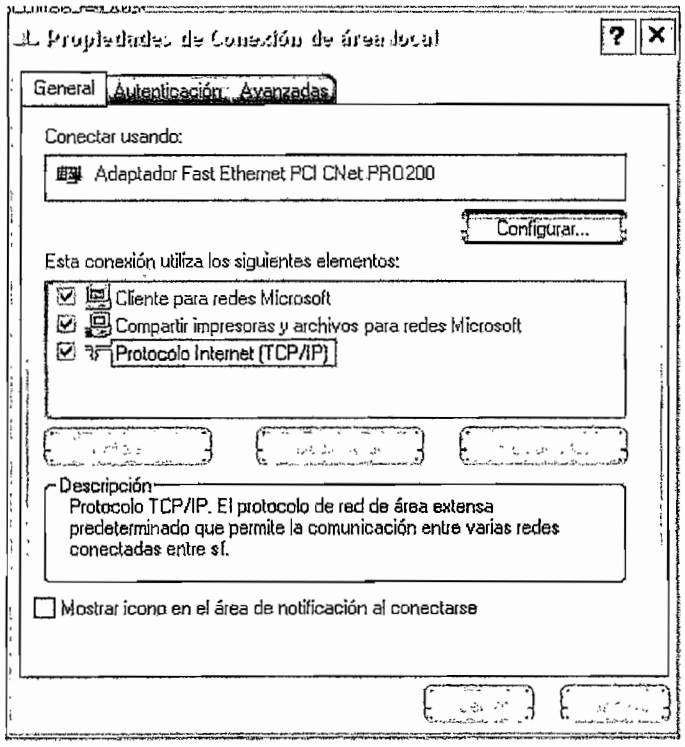


Figura 2.25 Pantalla para configuración de las estaciones de trabajo en Windows XP[43]

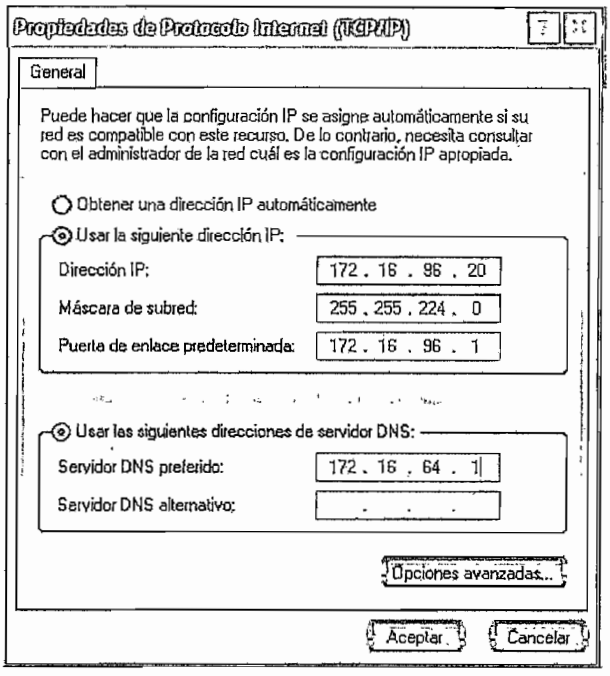


Figura 2.26 *Pantalla de configuración de dirección IP para estaciones de trabajo[43]*

Cada máquina de la Intranet manejará sus propios usuarios, los cuales serán divididos en dos categorías; administrador y usuario PCxx, esto con el objeto de mantener mayor seguridad en la red, puesto que los usuarios PCxx tendrán privilegios restringidos, mientras que el usuario administrador será el único que pueda cargar programas al PC o modificar su configuración. Cabe resaltar que en primer lugar será creada la cuenta del usuario administrador con todos los permisos de configuración y posteriormente la cuenta de usuario PCxx

En la tabla 2.18 se muestran los permisos disponibles para los dos tipos de cuentas de usuario.
Para crear una cuenta de usuario:

1. Hacer *click* en Inicio, Panel de control y, a continuación, en Cuentas de usuario
2. En la ficha "Usuarios", hacer *click* en Agregar
3. Escribir un nombre para la cuenta de usuario, su nombre completo y una descripción de la cuenta
4. Escribir el nombre de dominio y, a continuación, hacer *click* en Siguiente, si el equipo se configura como parte de una red cliente/servidor

5. Escribir una contraseña de usuario y rescribirla para confirmar
6. Reiniciar el computador

Funciones	Administrador	Usuario
Crear cuentas de usuario	SÍ	
Cambiar archivos del sistema	SÍ	
Cambiar la configuración del sistema	SÍ	
Leer archivos de otras cuentas de usuario	SÍ	
Agregar o quitar hardware	SÍ	
Cambiar las contraseñas de otras cuentas de usuario	SÍ	
Cambiar las contraseñas de su propia cuenta de usuario	SÍ	SÍ
Instalar cualquier programa	SÍ	
Instalar la mayoría de los programas	SÍ	
Guardar documentos	SÍ	SÍ
Utilizar los programas instalados	SÍ	SÍ

Tabla 2.20 *Permisos de usuarios en Windows XP [43]*

2.7.2 CONFIGURACIÓN DEL *ROUTER*

La Intranet requiere la utilización de un *router* de tal manera que permita la salida a Internet; para el diseño se utiliza un *router* Cisco pues presenta mayor estabilidad, confiabilidad y actualmente están tomando mayor fuerza en el mercado. [63]

Como se indica en la figura 2.24, para la configuración del *router* se utiliza las siguientes direcciones:

S0 200.150.50.2
Eth0 212.194.89.25
Eth1 212.194.89.26

a. Configuración Básica

Router# configure terminal
Router (config) # hostname INTRANET
INTRANET (config)# enable password (indicar password)
INTRANET (config) # enable secret (indicar clave)
INTRANET (config) # line console 0
INTRANET (config-line) # password (indicar password)
INTRANET (config-line) # login
INTRANET (config-line) # exit
INTRANET (config) # line vty 0 4
INTRANET (config-line) # password (indicar password)
INTRANET(config-line) # login
INTRANET(config-line) # exit
INTRANET(config)# interface serial 0
INTRANET(config-if)# ip address 200.150.50.2 255.255.255.0
INTRANET(config-if)# no shutdown
INTRANET(config-if)# exit
INTRANET(config)# interface ethernet 0
INTRANET(config-if)#ip address 212.194.89.25 255.255.255.248
INTRANET(config-if)# no shutdown
INTRANET(config-if)#exit
INTRANET(config)# interface ethernet 1
INTRANET(config-if)#ip address 212.194.89.26 255.255.255.248
INTRANET(config-if)# no shutdown
INTRANET(config-if)#exit
INTRANET (config)# exit
INTRANET # copy running-config startup-config

b. Configuración del protocolo de enrutamiento

Para la configuración del protocolo de enrutamiento se debe tener en cuenta los servicios de red y el tipo de protocolo a utilizar; se puede optar por configurar los

protocolos RIP, IGRP, OSPF, etc, o en su defecto la utilización de rutas estáticas en caso de tener una única conexión.

Para este caso se procede con la configuración de rutas estáticas por cuanto la red posee una sola salida a Internet mediante enlace dedicado hacia el proveedor. A continuación se presenta la configuración de una ruta estática.

INTRANET(config)# ip route 200.150.50.2/24 200.150.50.1/24

c. Configuración de las listas de acceso

Una lista de control de acceso (ACL) es un conjunto secuencial de reglas de permiso o denegación, aplicadas a una interfaz del *router* que filtran paquetes hacia adentro o fuera del interfaz. Las ACL se pueden utilizar para todo tipo de protocolos enrutados (IP, IPX, *Apple Talk*)

Existen dos tipos de listas de acceso y son:

- ACL estándar
  Sirven para permitir o negar todo el tráfico hacia o desde una red, dependiendo de la dirección origen o destino de la información. A estos filtros se les asigna un valor entre 1 y 99.

- ACL extendida
  Ofrecen mayor flexibilidad porque se puede filtrar tráfico considerando direcciones IP origen o destino, tipo de protocolo y el número de puerto. Se las numera entre 100 y 199.

Toda ACL debe ser configurada siguiendo dos pasos fundamentales:

a. Definir la ACL

   Se ingresa al modo de configuración global con el siguiente comando:

   Router (config) # [protocol] access-list [# de ACL] permit/deny {condición}

Donde :

Protocol	tipo de protocolo a filtrarse
# de ACL	número establecido para la ACL
Condición	dirección origen o destino de la información

b. Aplicarla al interfaz

Se ingresa al modo de configuración global de interfaz con el siguiente comando:

Router (config-if) # [protocol] access group [# ACL] [in / out]

Un concepto muy importante a tomar en cuenta dentro de las ACLs es el de MÁSCARA *WILDCARD*, que es un conjunto de 32 bits repartidos en grupos de 8 bits y separados por un punto. Esta máscara es importante ya que define qué bits de las direcciones IP origen y destino deben tomarse en cuenta para filtrar los paquetes, un valor 0 especifica que el bit debe revisarse, mientras que el valor 1 indica que el bit es ignorado.

Para el presente proyecto se ha decidido utilizar las siguientes ACLs:

- ACLs estándar aplicadas a la interfaz serial y a la interfaz *Ethernet* cuya función es la de no permitir el intercambio de información con dominios que proporcionan material no legal (*hackers*) o inmoral (pornografía). Para el ejemplo se asume una dirección 200.200.0.0 como dirección no permitida.

  Router (config) # ip access-list 1 deny tcp 192.168.0.0 0.0.0.255 200.200.0.0 0.0.0.255
  Router (config-if) # ip access group 1 out

- ACL extendida aplicada a la interfaz serial del *router*, para permitir que un usuario externo a la Intranet pueda acceder a los siguientes servicios (tabla 2.19):

SERVICIO	PUERTO
Web	80
E-mail	25, 110
IRC	6666-6668

Tabla 2.21 *Puertos asignados para los diferentes servicios*

Considerando que se utiliza la política por defecto denegar, es necesario realizar la configuración en los dos sentidos.

Router (config) # ip access-list 100 permit tcp any 212.194.89.27 0.0.0.255 eq 80

Router (config) # ip access-list 100 permit tcp 212.194.89.27 0.0.0.255 any eq 80

Router (config) # ip access-list 100 permit tcp any 212.194.89.27 0 0.0.0.255 eq 25

Router (config) # ip access-list 100 permit tcp 212.194.89.27 0 0.0.0.255 any eq 25

Router (config) # ip access-list 100 permit tcp any 212.194.89.27 0.0.0.255 eq 110

Router (config) # ip access-list 100 permit tcp 212.194.89.27 0.0.0.255 any eq 110

Router (config) # ip access-list 100 permit tcp any 212.194.89.30 0.0.0.255 eq 6666

Router (config) # ip access-list 100 permit tcp 212.194.89.30 0.0.0.255 any eq 6666

Router (config) # ip access-list 100 permit tcp any 212.194.89.30 0.0.0.255 eq 6667

Router (config) # ip access-list 100 permit tcp 212.194.89.30 0.0.0.255 any eq 6667

Router (config) # ip access-list 100 permit tcp any 212.194.89.30 0.0.0.255 eq 6668

Router (config) # ip access-list 100 permit tcp 212.194.89.30 0.0.0.255 any eq 6668

Router (config-if) # ip access group 100 in

- ACL aplicada en la interfaz *Ethernet* 0, que permita enviar tráfico desde el PC del administrador a fin de que el Webmaster pueda verificar y solucionar posibles daños de la red.

  Router (config) # ip access-list 101 permit 192.168.0.2 0.0.0.255
  Router (config-if) # ip access group 101 in

- Cabe indicar que por defecto, la última línea de las listas de acceso es la negación de todo aquello que no se permitió explícitamente.
  Router (config) # ip access-list deny any

2.7.3 CONFIGURACIÓN DE SERVIDORES

Los servidores de red constituyen los puntos estratégicos de la red, pues su funcionamiento determinará el desempeño de la misma, es por ello que se ha elegido utilizar el sistema operativo Linux de la familia Unix, pues es confiable, seguro, estable y adicionalmente es un software *freeware*.

La versión Linux elegida para el levantamiento de servidores de red, es el Red Hat versión 9.0 debido a que presenta grandes mejores de seguridad respecto a versiones anteriores.

El primer paso para lograr un correcto funcionamiento de los servidores es asignar los parámetros de red correspondientes a cada máquina.

a. Asignación de parámetros de red en Linux

La configuración de los parámetros de red es muy importante, puesto que permite localizar posibles fallas.

Los dispositivos de red bajo Linux rompen la tradición de acceder a todos los dispositivos a través de un mismo archivo. Normalmente el dispositivo *Ethernet* se registra como ethx, donde x es el número de dispositivo.

Las direcciones IP con las que deberá configurarse los servidores de red se muestran en la tabla 2.20.

HOSTNAME	DIRECCIÓN IP		*GATEWAY*	*NETMASK*
Servidor *E-mail* *Web*	Eth0 Eth1	212.194.89.27 212.194.89.29	212.194.89.25 212.194.89.25	255.255.255.248 255.255.255.248
Proxy	Eth0	212.194.89.30	212.194.89.29	255.255.255.248
DNS	Eth1	192.168.0.1	212.194.89.29	255.255.255.0

Tabla 2.22 *Direcciones para los interfaces de los servidores de red*

Se considera como parámetros de red aquellos que permiten la comunicación básica entre los equipos de red y son los siguientes:

Hostname

Para la configuración del *hostname* se debe editar el archivo */etc/hosts*, y verificar que esté asociado a una de las direcciones IP, específicamente a la que esté asociado en el servidor de nombres de dominio o DNS.

```
212.194.89.27      servidor.epn.edu              servidor
127.0.0.1          localhost.localdomain         localhost
```

Se debe establecer un nombre para el sistema, éste deberá ser un nombre de dominio completamente resuelto por un servidor de nombre de domino (DNS), de tal modo que el *hostname* del sistema se defina en el fichero /etc/sysconfig/network del siguiente modo:

```
NETWORKING = yes
HOSTNAME = servidor.epn.edu
```

Dirección IP, máscara de sub-red y puerta de enlace

Para la configuración de la dirección IP, subred y puerta de enlace se debe editar el archivo /etc/sysconfig/network-scripts/ifcfg-eth0 en el cual se verifica que los parámetros de red sean los correctos.

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=212.194.89.27
NETMASK=255.255.255.248
GATEWAY=212.194.89.25

Los parámetros anteriores son definidos de acuerdo a la planificación de direccionamiento IP indicado en la tabla 2.16.

Servidor de nombres

La especificación del servidor de nombres se lo realiza editando el archivo /etc/resolv.conf en el que debe establecerse los servidores de resolución de nombres de dominio (DNS), de la siguiente forma:

Nameserver 212.194.89.30

b. Configuración del servidor de Dominio de Nombres (DNS)

El servidor DNS organiza los nombres de máquina (*hostname*) en una jerarquía de dominios. Un dominio es una colección de nodos relacionados entre sí; los dominios pueden ser TLD (*Top Level Domain*) o SLD (*Second Level Domain*), el control administrativo de estos dominios lo realiza la ICANN INTERNIC.

Los servidores DNS se dividen en tres grupos: primarios, secundarios y de *cache*. Los servidores primarios son a los únicos que se los considera autorizados para un dominio particular. Un servidor autorizado es el único en el cual residen los archivos de configuración de dominio. Las actualizaciones de las tablas de dominio de DNS, se almacenan en este servidor.

Los servidores secundarios trabajan como respaldo y como distribuidores de carga de los servidores de nombres primarios. Los servidores primarios conocen la existencia de los secundarios y les envían periódicamente las tablas de actualizaciones.

Los servidores *cache* no contienen archivos de configuración de ningún dominio. En su lugar cuando una máquina cliente realiza una petición a un servidor de *cache* para que se resuelva un nombre este servidor comprueba su propia *cache* local, primero. Si no lo encuentra, buscará en un servidor primario y su respuesta pasará a *cache*.

En el diseño de esta Intranet se configurará un DNS *cache*, debido a su funcionalidad y a que se dispondrá de un DNS primario proporcionado por el ISP.

En vista de que se brindará servicio de *e-mail* y existirá una página *Web* pública es necesario adquirir un dominio que esté disponible. Para la configuración se ha asumido el dominio epn.edu, mismo que puede adquirirse por medio del ISP.

Para el levantamiento del servidor DNS se requiere al menos:

- Un servidor con al menos 128 MB en RAM y la distribución de Red Hat 9.0 instalada.
- Deben estar bien configurados los parámetros de red y es necesario disponer de al menos dos interfaces, una para acceder a la red local y otra para acceder hacia Internet una de éstas puede ser virtual (eth0:0) o una interfaz real (eth1).
- Se necesitará tener instalados los siguientes paquetes: *bind, bind-utils* y *caching-nameserver*. Todos, seguramente, vienen incluidos en alguno de los CDs de instalación. No es conveniente utilizar versiones anteriores a bind-9.1.3, debido a serias fallas de seguridad.

El paquete Red Hat 9.0 cuenta con una herramienta de configuración gráfica, que facilita el levantamiento del servidor DNS. Para acceder a esta herramienta se ingresa al menú de inicio, se escoge la opción configuración del sistema, luego se selecciona configuración de servidores y finalmente servicio de nombre de dominio.

De acuerdo a la configuración lógica de la red se deben crear los siguientes registros:

- Registros tipo A (*Address record*).- Estos registros relacionan un nombre del dominio con una dirección IP.
- Registro MX (*Mail Exchange*).- Estos registros relacionan un nombre de dominio a una IP, pero se utilizan solamente para SMTP y permite separar el servidor de *e-mail* del resto de servidores.
- Registro NS (*Name Server*).- Relaciona un nombre de dominio a una IP e indica cuál es el servidor DNS que posee los registros DNS.
- Registro SOA (*State of Authority*).- Señala cuál es el servidor DNS autoridad sobre una zona.

La configuración de los registros se indica en las figuras 2.27, 2.28, 2.29 y 2.30

Para verificar la configuración de los registros DNS, se digita en consola el siguiente comando:

dig @[dirección IP del DNS] [nombre del dominio] any.
dig @212.194.89.30 epn.edu any

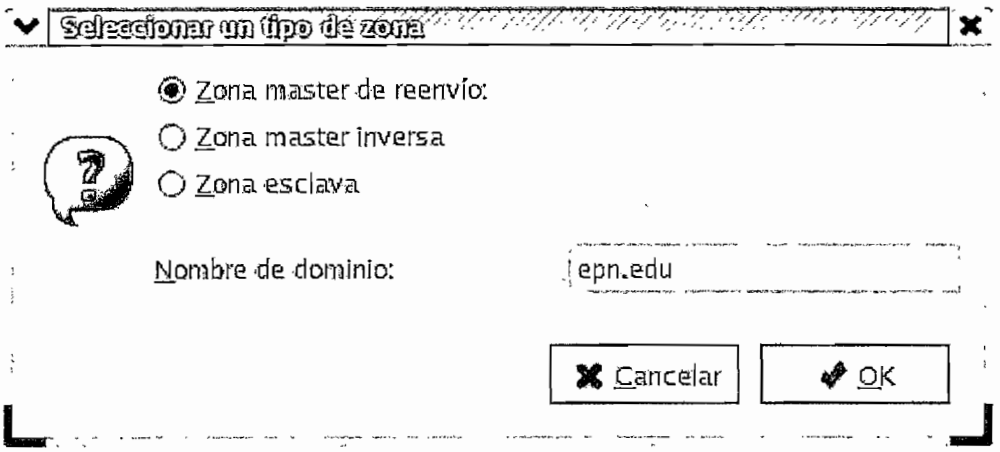


Figura 2.27 *Registro de zona master*

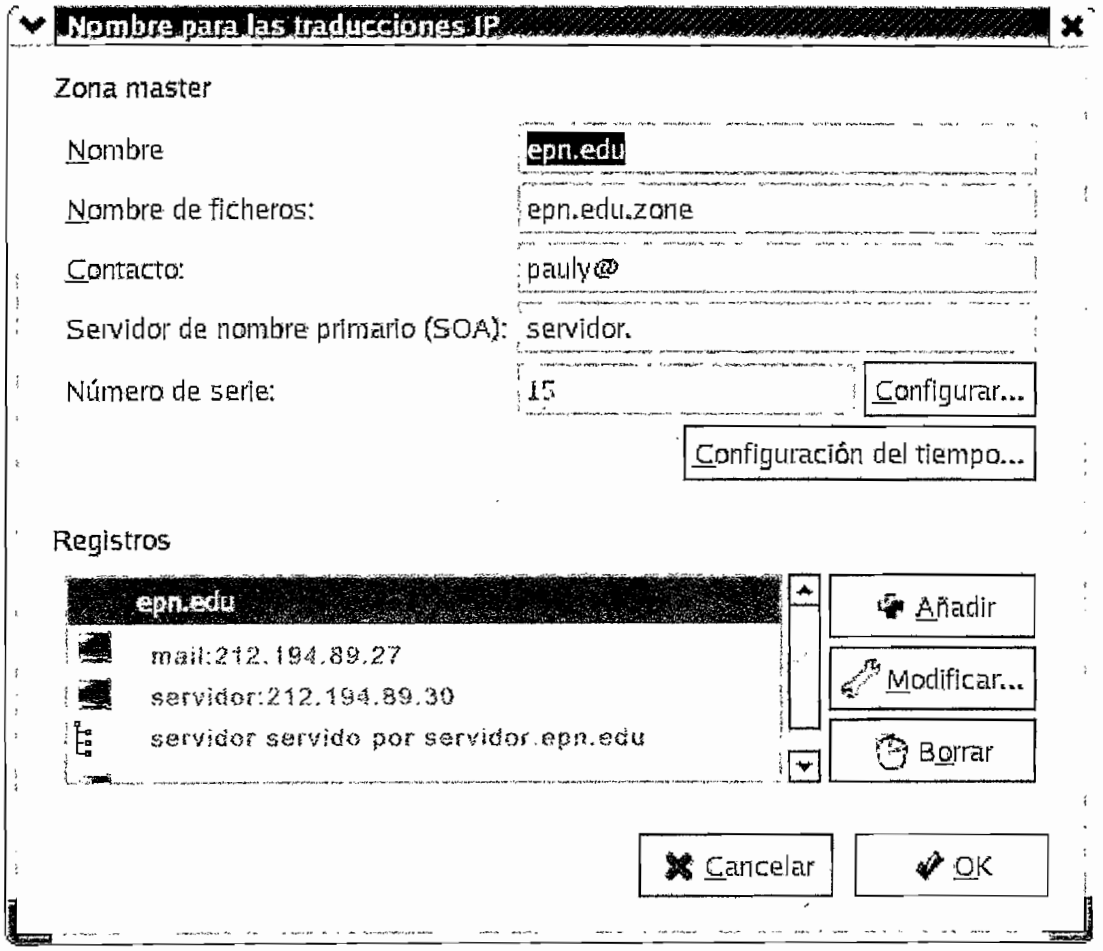


Figura 2.28 Propiedades de zona master

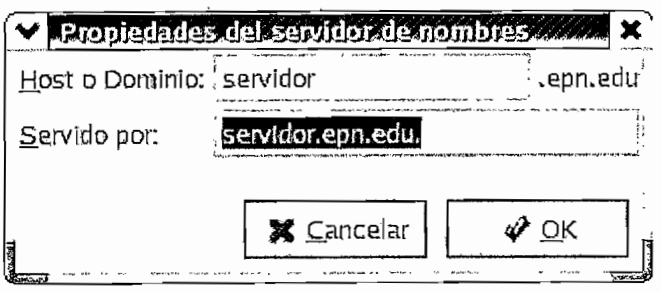


Figura 2.29 Configuración para el Registro DNS

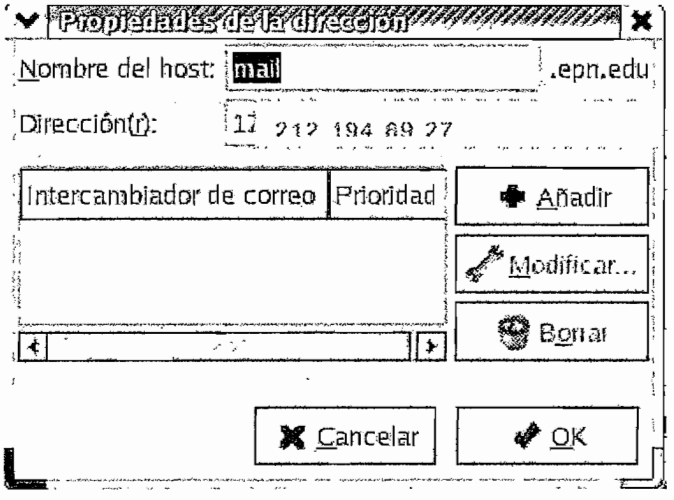


Figura 2.30 *Propiedades para los Registros A*

A continuación se presenta el resultado de este comando:

```
; <<>> DiG 9.2.1 <<>> @212.194.89.30 epn.edu any
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3330
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;epn.edu.                IN      ANY

;; ANSWER SECTION:
epn.edu.        86400 IN      SOA   servidor. pauly. 10 28800 7200 604800
86400
epn.edu.        86400 IN      NS    servidor.epn.edu.
epn.edu.        86400 IN      MX    10 mail.epn.edu.

;; ADDITIONAL SECTION:
servidor.epn.edu. 86400 IN    A     212.194.89.30
mail.epn.edu.   86400 IN      A     212.194.89.27

;; Query time: 0 msec
;; SERVER: 212.194.89.30.1#53(212.194.89.30)
```

;; WHEN: Tue Jul 6 19:51:40 2004

;; MSG SIZE rcvd: 150

El orden de consultas de DNS se especifica en el archivo /etc/nsswitch.conf en la línea de *host.*

Para que el servidor DNS quede añadido entre los servicios de arranque del sistema, se debe ejecutar el siguiente comando a fin de habilitar *named* en los niveles de corrida 3, 4 y 5:

/sbin/chkconfig –level 345 named on

c. Configuración del *Sendmail*

La mayoría de las distribuciones de GNU/Linux incluyen de manera predeterminada *Sendmail*, un poderoso servidor de correo electrónico ampliamente utilizado alrededor del mundo. Éste requiere de una correcta configuración para su mejor aprovechamiento y para poder disponer de un nivel de seguridad aceptable.

Para la configuración de un servidor de *e-mail*, se debe contar con los siguientes elementos:

- Tener un dominio propio
- Tener una IP pública permanente o estática
- Contar con una red local y parámetros de red del servidor perfectamente configurados
- Un servidor con al menos 128 MB RAM y alguna distribución de GNU/Linux instalada
- Estar bien configurado un servidor de nombres *(DNS)*
- Tener instalados los paquetes *sendmail, sendmail-cf, m4, make, xinet e imap*
- Establecer, qué máquinas de la red local, pueden enviar y recibir correo electrónico y cuales NO deben hacerlo

- Determinar cómo recuperar los mensajes de correo electrónico que arriben al servidor POP3 o IMAP.

La configuración del servidor DNS que define bien los servidores de nombres de dominios correspondientes, se debe hacer en el archivo */etc/resolv.conf*, como se indica a continuación:

Search epn.edu

El IP de la máquina que tiene el DNS de la red local
nameserver 212.194.89.30

El DNS del proveedor de servicios
Comprobar que el servidor cuente con los paquetes necesarios para el funcionamiento del *sendmail*, requiere del siguiente comando:

rpm -qa sendmail *

Editar el archivo */etc/mail/sendmail.mc*, con previo respaldo del original, a fin de preparar la configuración del servidor de correo.

Para poder enviar correo desde las máquinas de la red local es necesario comentar la siguiente línea y añadir las interfaces desde las cuales se quiere que escuche peticiones *sendmail.*

dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1,Name=MTA')

Para filtrar *Spam*[36] de manera eficiente, la mejor manera de empezar a hacerlo es rechazando correo proveniente de dominios NO RESUELTOS, es decir dominios que no están registrados en un DNS y que por lo tanto son inválidos. Para tal fin, a menos que se requiera lo contrario, es necesario mantener comentada la siguiente línea:

dnl FEATURE(`accept_unresolvable_domains')dnl

[36] *Spam:* envio de correo masivo no solicitado.

Es necesario establecer que epn.edu corresponde a la máscara que se utilizará para todo el correo emitido desde el servidor. Debe, por tanto, añadirse una línea justo debajo de *MAILER(procmail)dnl* :

MASQUERADE _AS(epn.edu)dnl

Para evitar spam indeseado se añade :
FEATURE(`dnsbl)dnl

Para generar /etc/mail/sendmail.cf se procesa el siguiente comando:

m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

Se abre el archivo /etc/mail/access y se agrega algunas líneas para definir quienes podrán hacer uso de nuestro servidor de correo para poder enviar mensajes:

#Por defecto, solo se permite enviar correo desde el localhost.

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY

#Añadir las direcciones IPs de red permitidas

212.194.89.30/29	RELAY
212.194.89.25/29	RELAY

Especificar también aquellas direcciones de correo que se consideren indeseables o que se deseen bloquear

servidor.indeseable.com	DISCARD
part.com.mx	DISCARD
newlad.com	DISCARD
dmc.com.mx	DISCARD
propnewidea.com	DISCARD
lapromocion.com	DISCARD

hosting.com.mx DISCARD
solopromos.com.mx DISCARD

Al concluir, se debe compilar este archivo para generar otro en formato de base de datos a fin de ser utilizado por *Sendmail* con el siguiente comando:

makemap hash /etc/mail/access.db < /etc/mail/access

Se designa un "alias" a la cuenta de correo de *root* a fin de recibir los mensajes generados por el sistema en una cuenta común de usuario. Se edita el archivo */etc/aliases*, y al final se encontrarán las siguientes líneas:

Person who should get root's mail
root: admin
Esto corresponde a la cuenta de correo local hacia donde se re-direcciona el correo de *root*. Se debe descomentar la última línea y asignar el nombre de la cuenta de usuario que utiliza normalmente.

A fin de que este nuevo alias sea reconocido y pueda ser utilizado por *Sendmail* debe utilizar el comando *newaliases*:

/newaliases

Terminados los detalles de la configuración, se reinicia *sendmail* del siguiente modo:

/etc/init.d/mail/sendmail restart

Generalmente *Sendmail* está incluido entre los servicios que de forma predeterminada se inician con el sistema. Si por alguna razón *Sendmail* no estuviese habilitado, se ejecuta lo siguiente a fin de habilitar *sendmail* en los niveles de corrida 3, 4 y 5:

/sbin/chkconfig --level 345 sendmail on

En el cortafuegos o *firewall*, debe estar abierto el puerto 25, de otro modo el

correo saldría pero no entraría. Verificar que esté presente una línea en el guión de *firewall* similar a la siguiente:

#SMTP
/sbin/iptables -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 25 -j ACCEPT

Finalmente se debe comprobar que en el archivo /etc/resolv.conf se encuentre el registro adecuado de servidores DNS.

Como una medida de seguridad, se debe instalar en el servidor *sendmail* programas como Mcafee o AMAVIS, encargados de la revisión y desinfección de virus.

Servicios POP3 e IMAP

De acuerdo a las capacidades utilizadas por los clientes de correo electrónico, se debe habilitar los servicios ipop3 (POP3 tradicional, autenticación en texto plano), *pop3s* (POP3 seguro, autenticación con criptografía), *imap* (IMAP tradicional, autenticación en texto plano) e *imaps* (IMAP seguro, autenticación con criptografía).

Tomar en cuenta que la autenticación por medio de texto plano es definitivamente un método inseguro, y siempre serán mejor usar los servicios que permitan establecer conexiones seguras.

Los servicios se activan de manera automática ejecutando los siguientes comandos:
/sbin/chkconfig imap on

Se puede habilitar manualmente editando el archivo /etc/xinetd.d/imap, a fin de proporcionar opciones adicionales, como direcciones IP específicas a las cuales se les estaría permitido cierto servicio.

```
service imap
{
    socket_type             = stream
```

```
        wait            = no
        user            = root
        server          = /usr/sbin/imapd
        log_on_success   += USERID
        log_on_failure   += USERID
        disable           = no
}
```

Hecho lo anterior, es necesario reiniciar el *daemon* xinetd con la siguiente línea de comando:

/etc/init.d/xinetd restart

Configuración de los clientes de correo

Los clientes pueden configurar programas de acceso a *e-mail* de acuerdo a los sistemas operativos en uso; por ejemplo Linux cuenta con *Mozilla e-mail*, Eudora, Pegassus, Evolution, Netscape, etc, en Windows el programa más utilizado es el Outlook Express.

Es importante tener en cuenta que el servidor de *e-mail* requiere tener declarados a sus usuarios en el archivo:

/var/spool/mail

El mismo que se crea automáticamente al incluir clientes al sistema. Los clientes deberán ser declarados asignándoles nombre, grupo y *password*, de la siguiente forma:

adduser Nombre-usuario -g grupo_asignado
passwd xxxxxxx

Como se dijo anteriormente la Intranet establece dos grupos de trabajo: administradores y usuarios; los grupos se deben crear con el siguiente comando:

groupadd administradores

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto 8080 para el servicio de *cache* WWW. Para agregar seguridad a la red se debe permitir el acceso desde la red de área local y se especifica que *Squid* escuche peticiones tanto en el puerto 8080 como en el 3128, con la siguiente instrucción:

You may specify multiple socket addresses on multiple lines
#Default: http_port 3128
http_port 212.194.89.30: 3128
http_port 212.194.89.30: 8080

Configuración de *cache*

Parámetros *cache_mem*

El parámetro *cache*_mem establece la cantidad ideal de memoria para:

Objetos en tránsito.
Objetos *Hot*.
Objetos negativamente almacenados en el *cache*.

Los datos de estos objetos se almacenan en bloques de 4 KB. El parámetro *cache_mem* especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos *Hot* y aquellos negativamente almacenados en el *cache* podrán utilizar la memoria disponible hasta que ésta sea requerida. De ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, *Squid* excederá lo que sea necesario para satisfacer la petición.

Por defecto se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo de los hábitos de los usuarios o necesidades establecidas por el administrador; para servidores con al menos 128 MB de RAM, éste parámetro debe establecerse en al menos 16 MB. El

cache_mem permite mejorar el desempeño del *Proxy*, pero dependiendo de la velocidad del disco duro.

cache_mem 16 MB

Parámetro *cache_dir*

Este parámetro se utiliza para establecer el tamaño de *cache* en el disco duro para *Squid*. Por defecto *Squid* utilizará un *cache* de 100 MB, esto implica cuánto de Internet, se almacenará en el disco duro.

Se puede incrementar el tamaño del *cache* hasta donde lo desee el administrador. Mientras más grande el *cache*, más objetos de almacenarán en éste y por lo tanto se utilizará menos ancho de banda. La siguiente línea establece un *cache* de 700 MB.

cache_dir ufs /var/spool/squid 700 16 256

Los números 16 y 256 significan que el directorio del *cache* contendrá 16 subdirectorios con 256 niveles cada uno, mientras que ufs es el tipo de almacenamiento por defecto en el *Proxy*. No es necesario modificar estos valores.

Es muy importante considerar que si se especifica un determinado tamaño de *cache* y éste excede al espacio real disponible en el disco duro, *Squid* se bloqueará inevitablemente.

Adicionalmente se configura los parámetros:

cache_swap_low 90
cache_swap_high 95

Estos parámetros indican que cuando el 95% de la capacidad del *Proxy* ha sido superada, la memoria se vacía automáticamente, hasta llegar al 90% de su capacidad.

maximum_object_size 4096 KB

minimum_object_size 0KB

Señalan que los objetos a guardarse en la memoria *cache* no deberán sobrepasar los 4 MB.

Sección de registro

Esta sección de registro permite el monitoreo de *squid*, manteniendo registros de las actividades del cliente y de los objetos almacenados en *cache*, lo que representa una gran ayuda al administrador de red.

cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log

Para que el registro de fechas sea visualizado en un formato fácilmente entendible se configura:

emulate_httpd_log on

Sección administrativa

Por defecto, si algo ocurre con el *cache*, como por ejemplo que muera el proceso, se enviará un mensaje de aviso a la cuenta *webmaster* del servidor. Puede especificarse una distinta si acaso se considera conveniente.

cache_mgr webmaster@mail.epn.edu

Sección de controles de acceso

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a *Squid*.

Listas de control de acceso

Las listas de control de acceso pueden establecer reglas de acceso de acuerdo a la dirección IP o de dominio, tanto de origen como de destino. Dependiendo del caso se las representará como:

www.sitioporno.com
www.otrositioporno.com
sitioindeseable.com
otrositioindeseable.com
napster
sex
porn
mp3
xxx
adult
warez

Se define una Lista de Control de Acceso que a su vez puntualice al fichero */etc/squid/sitiosdenegados*. Esta lista se la denominará como *"sitiosdenegados"*. De este modo, la línea correspondiente quedaría de la siguiente manera:

acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"

Una vez realizado lo anterior, en la sección de Listas de Control de Acceso se especifica lo siguiente:

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 172.16.96.0/255.255.224.0
acl password proxy_auth REQUIRED
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"

A continuación se modificará una Regla de Control de Acceso existente agregando el símbolo ! que denegará el acceso a la Lista de Control de Acceso denominada *sitiosdenegados*:

http_access allow redlocal !sitiosdenegados

La regla anterior permite el acceso a la Lista de Control de Acceso denominada redlocal, pero niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada *sitiosdenegados*

Las reglas de control de acceso se ejecutan secuencialmente, es por ello que se debe mantener un orden específico, para evitar resultados erróneos. El orden recomendado es:

1.- Reglas de denegación
2.- Directivas de acceso
3.- Denegación total

Sección *httpd acelerator options*

Cache con aceleración

Cuando un usuario hace petición hacia un objeto en Internet, éste es almacenado en el *cache* de *Squid*. Si otro usuario hace petición hacia el mismo objeto y éste no ha sufrido modificación alguna desde que lo accedió el usuario anterior, *Squid* mostrará el objeto que ya se encuentra en el *cache* en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el *cache* de *Squid* y además optimiza enormemente la utilización del ancho de banda.

La sección HTTPD-ACCELERATOR OPTIONS debe habilitarse de la siguiente manera:

```
# Debe especificarse la IP de cualquier servidor Web en la red local

httpd_accel_host 172.16.96.1
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Una vez terminada la configuración, se ejecuta el siguiente comando para iniciar por primera vez *Squid*:

/etc/init.d/squid start

Si se necesita reiniciar para probar cambios hechos en la configuración, ejecutar:

/etc/init.d/squid restart

Para iniciar *Squid* de forma automática cuando se inicie el sistema, se ejecuta:

/sbin/chkconfig squid on

Que habilitará al *Squid* a los niveles de corrida 3,4 y 5

Depuración de errores

Cualquier error al inicio de *Squid* solo significa que hubo errores de sintaxis, o se están citando incorrectamente las rutas hacia los ficheros de las Listas de Control de Acceso.

Para realizar un diagnóstico automático de problemas a *Squid* se debe utilizar el siguiente comando:

/etc/init.d/squid reload

También se puede iniciar *Squid* directamente desde la línea de comando especificando el modo de depuración:

squid -d 5

e. Configuración del *FIREWALL*

Un *firewall* es un dispositivo que filtra el tráfico como mínimo entre dos redes. El *firewall* puede ser un dispositivo basado en hardware o software o un software sobre un sistema operativo. En general se debe verlo como una caja con dos o más interfaces de red en la que se establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no, incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Para que un *firewall* entre redes funcione como tal, debe tener al menos dos tarjetas de red. El *firewall* debe colocarse entre el *router* (con un único cable) y la red local (conectado al *switch* o al *hub* de la LAN) como lo indica la figura 2.31.

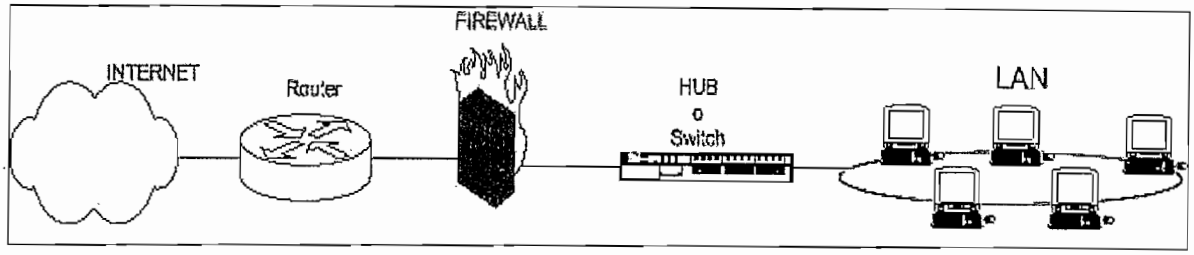


Figura 2.31 *Ubicación del firewall en una red [29]*

Dependiendo de las necesidades de cada red, puede ponerse uno o más *firewalls* para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a Internet (como es el caso de un servidor *Web*, un servidor de correo, etc), y en esos casos obviamente se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es ubicar el servidor en un lugar apartado de la red, denominado DMZ o zona desmilitarizada. El *firewall* tiene entonces tres entradas que se muestran en la figura 2.32.

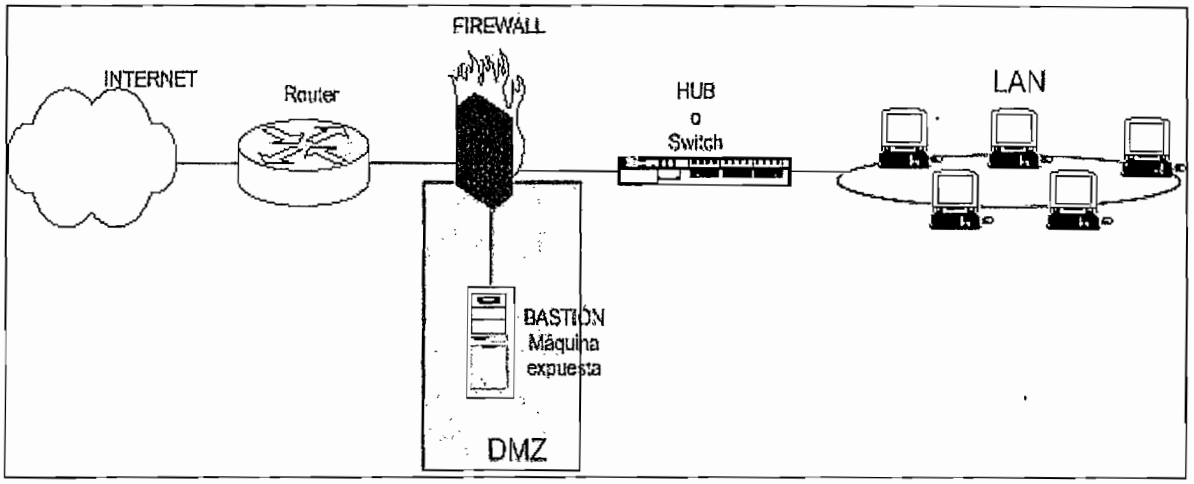


Figura 2.32 *Ubicación del Firewall en una red con DMZ[39]*

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura se permite que el servidor sea accesible desde Internet, de tal forma que si es atacado y se logra acceder a él, la red local sigue protegida por

el *firewall*. Esta estructura de DMZ puede hacerse también con un doble firewall y el esquema sería como el indicado en la figura 2.33

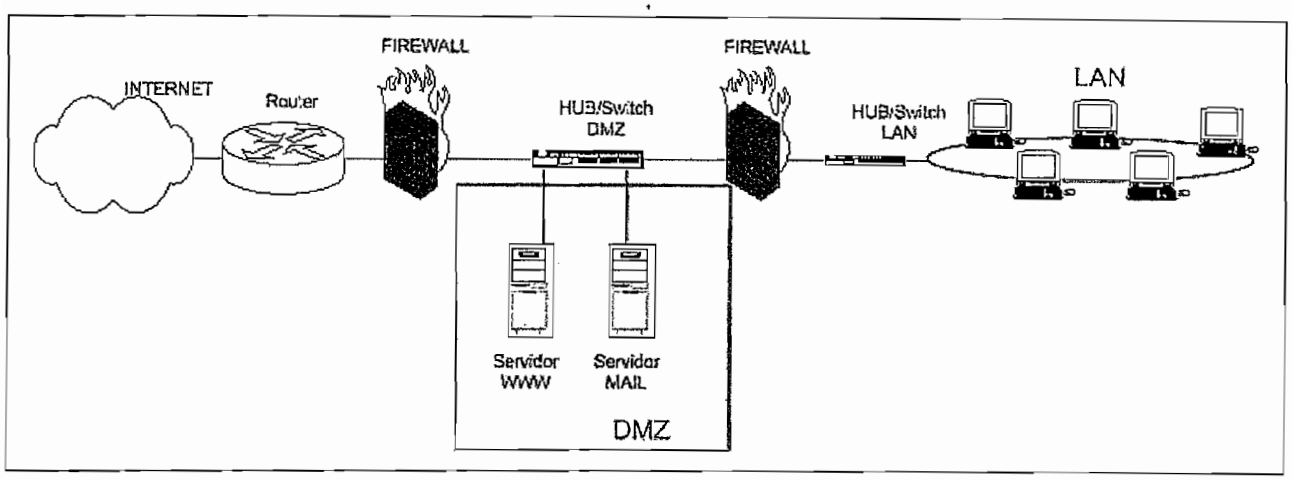


***Figura 2.33** Esquema de red con DMZ y dos firewalls[39]*

Cualquier *firewall* tendrá un conjunto de reglas en las que se examina el origen y destino de los paquetes TCP/IP; también son capaces de filtrar otros protocolos como: UDP, ICMP y otros protocolos vinculados a VPNs.

Hay dos maneras de implementar un *firewall*:

1. Política por defecto ACEPTAR: en principio todo lo que entra y sale por el *firewall* se acepta y solo se denegará lo que se diga explícitamente.
2. Política por defecto DENEGAR: todo está denegado, y solo se permitirá pasar por el *firewall* aquello que se permita explícitamente.

La primera política facilita mucho la gestión del *firewall*, porque solo se preocupa de proteger aquellos puertos o direcciones por las que se interesa; el resto no importa tanto y se deja pasar.

Con la política "aceptar" por defecto, las reglas del *firewall* realizan lo siguiente:

- Habilita el acceso a puertos de administración a determinadas IPs privilegiadas

- Enmascara el tráfico de la red local hacia el exterior (NAT, una petición de un PC de la LAN sale al exterior con la IP pública), para poder salir a Internet
- Deniega el acceso desde el exterior a puertos de administración y a todo lo que esté entre 1 y 1024.

El problema que presenta esta política, es que requiere un gran conocimiento acerca de los posibles ataques, para proteger los puertos vulnerables.

Con la política por defecto "DENEGAR", el *firewall* se convierte en un auténtico "muro" infranqueable. Presenta mayor dificultad de configuración pues requiere el conocimiento de que es lo que se tiene que abrir sin utilizar reglas demasiado permisivas.

Con la política "DENEGAR", el *firewall* tiene las siguientes características:

- Explicitar las conexiones permitidas en los dos sentidos, ya que existe una tercera regla que denegará todo
- Conocer perfectamente qué debe estar abierto y qué no
- Es más difícil de mantener
- Supone un *firewall* mucho más seguro

Para una mayor seguridad la Intranet del presente proyecto utilizará la política "DENEGAR".

Es importante conocer que el orden de las reglas del *firewall* es determinante. Normalmente cuando hay que decidir qué se hace con un paquete se va comparando con cada regla del *firewall* hasta que se encuentra una que le afecta (*match*), y se hace lo que dicte esta regla (aceptar o denegar); después de eso NO SE MIRARÁN MÁS REGLAS para ese paquete. El peligro es poner reglas muy permisivas entre las primeras del *firewall*, puede que las siguientes no se apliquen y no sirvan de nada.

IPTABLES

IPtables es un sistema de *firewall* vinculado al *kernel*[37] de Linux a partir del *kernel* 2.4 de este sistema operativo. Un *firewall* de *Iptables* no es como un servidor que se inicia o detiene, sino que es un simple *script de shell*[38] en el que se van ejecutando las reglas de *firewall*. Este *script* de *shell* puede implementarse en el archivo /etc/rc.d/init.d, de tal forma que se inicia con el sistema.

El *kernel*, dependiendo si el paquete es para la propia máquina o para otra máquina, consulta las reglas de *firewall* y decide qué hacer con el paquete según mande el *firewall*. La figura 2.34 muestra el camino que seguiría un paquete en el *kernel*.

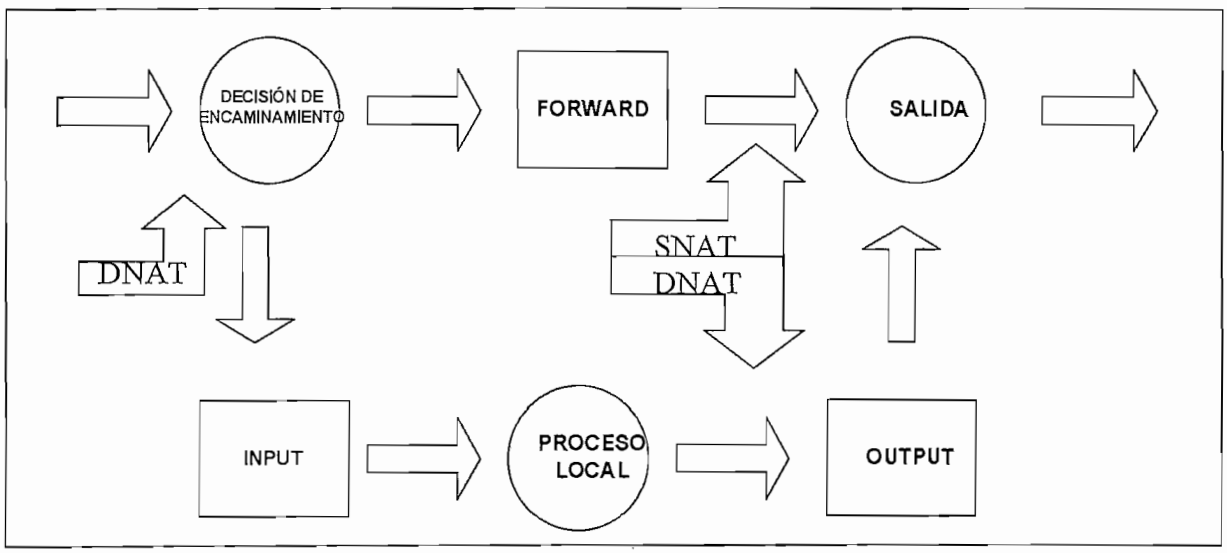


Figura 2.34 *Procesamiento de un paquete en el kernel con Iptables.[39]*

Como se ve en el gráfico, básicamente se mira si el paquete está destinado a la propia máquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia máquina se aplican las reglas *INPUT* y *OUTPUT*, y para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas *FORWARD*.

[37] *Kernel.*- En un sistema operativo, son los programas que residen en memoria y ejecutan las tareas esenciales del sistema como son: funcionamiento, rendimiento y administración de la memoria interna

[38] *Script de shell.*- Conjunto de comandos u órdenes establecidas en un fichero que al ejecutarlo producen una salida concreta

INPUT, OUTPUT y FORWARD, son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT, éstas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino. Antes de las reglas de NAT se pueden tener reglas de tipo *MANGLE*, destinadas a modificar los paquetes.

Por tanto se tienen tres tipos de reglas en *IPtables*:

MANGLE
NAT: reglas PREROUTING, POSTROUTING
FILTER: reglas INPUT, OUTPUT, FORWARD.

De acuerdo a la configuración planteada para la Intranet (figura 2.24), se necesita de dos *firewalls*, el primero protege la zona desmilitarizada y el segundo está destinado a proteger la red LAN.

Tanto los comandos básicos para el manejo de Linux así como los parámetros de especificación para las reglas de *Iptables*, se adjuntan en el Anexo G.

CONFIGURACIÓN DEL *FIREWALL* DE LA ZONA DESMILITARIZADA

Para la zona desmilitarizada se deben realizar las siguientes consideraciones: si las máquinas de la DMZ tienen una IP pública se debe impedir el *FORWARD* por defecto, en este caso no es necesario hacer redirecciones de puerto, basta con enrutar los paquetes para llegar hasta la DMZ, tampoco hace falta enmascarar la salida hacia el exterior de la DMZ, solamente se debe indicar al *router* cómo llegar hasta esa IP pública.

Las reglas usadas para filtrar tráfico entre la DMZ, la red LAN y el exterior son las *FORWARD*, pues se filtran paquetes entre distintas redes y éstos no son destinados al propio *firewall*.

En este *firewall* se debe permitir:

- El acceso del administrador de la red al *firewall* de la DMZ

- Acceso público y de red LAN a los puertos tcp/80/25/110 del servidor de la DMZ
- Acceso del servidor de la DMZ a una base de datos (BBDD) de la LAN a través del puerto 3306
- Bloquear el resto de accesos a la DMZ

A continuación se muestra la configuración del *IPtables* para la DMZ.

```
#!/bin/bash
## SCRIPT de IPTABLES

## FLUSH de reglas ; permiten borrar reglas anteriores en el firewall.
iptables –F
iptables –X
iptables –Z
iptables -t nat -F

## Se establece política por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP

# El localhost se deja abierto (por ejemplo para conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Al firewall DMZ, se tiene acceso desde la PC de administración.
iptables –A INPUT –s 192.168.0.2  -d 212.194.89.29 –j ACCEPT
iptables –A INPUT –d 192.168.0.2  -s 212.194.89.29 –j ACCEPT

# Con esto permite hacer forward de paquetes en el firewall, es decir que otras
#máquinas puedan salir a través del firewall.
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward

## Permitir el acceso desde el exterior al puerto 80 (http), 25 y 110 (e-mail) de la
# DMZ
iptables -A FORWARD -d 212.194.89.27 -p tcp -dport 80 -j ACCEPT
iptables -A FORWARD -d 212.194.89.27 -p tcp -dport 25 -j ACCEPT
iptables -A FORWARD -d 212.194.89.27 -p tcp -dport 110 -j ACCEPT

## En la política por defecto DROP las sentencias del IPtable se las realiza
en # ambos sentidos
iptables -A FORWARD -s 212.194.89.27 -p tcp -sport 80 -j ACCEPT
iptables -A FORWARD -s 212.194.89.27 -p tcp -sport 25 -j ACCEPT
iptables -A FORWARD -s 212.194.89.27 -p tcp -sport 110 -j ACCEPT

## Permitir el acceso desde la red LAN al puerto 80 (http), 25 y 110 (e-mail) de la
# DMZ
iptables -A FORWARD -d 212.194.89.29 -p tcp -dport 80 -j ACCEPT
iptables -A FORWARD -d 212.194.89.29 -p tcp -dport 25 -j ACCEPT
iptables -A FORWARD -d 212.194.89.29 -p tcp -dport 110 -j ACCEPT

## En la política por defecto DROP las sentencias del IPtable se las realiza
en # ambos sentidos
iptables -A FORWARD -s 212.194.89.29 -p tcp -sport 80 -j ACCEPT
iptables -A FORWARD -s 212.194.89.29 -p tcp -sport 25 -j ACCEPT
iptables -A FORWARD -s 212.194.89.29 -p tcp -sport 110 -j ACCEPT

# Se debe permitir que el servidor Web se comuniqué con el firewall de red LAN
con # el fin de aceptar el acceso a una BBDD

iptables - A FORWARD -s 212.194.89.29 -d 212.194.89.30 -p tcp -dport 3306
-j ACCEPT
iptables - A FORWARD -d 212.194.89.29 -s 212.194.89.30 -p tcp -sport 3306
-j ACCEPT
```

Se cierra cualquier otro tipo de acceso
iptables -A FORWARD -d 212.194.89.24/29 -j DROP

CONFIGURACIÓN DEL *FIREWALL* PARA LA RED LAN

La configuración del *firewall* con *IPtables* para una red local que necesita salida a Internet, debe configurarse con reglas NAT que permitan la traducción de direcciones IP privadas a una dirección pública.

En este *firewall* se debe permitir:

- Enmascaramiento de la red LAN para permitir el acceso a Internet
- El acceso del administrador de la red al *firewall* de red LAN
- El acceso del firewall a la base de datos a través del puerto 3306
- Acceso de red LAN a los puertos tcp/80/25/110/53/3128/8080
- Bloquear el resto de accesos al firewall

A continuación se muestra la configuración del *IPtables* para la red LAN:

```
#!/bin/bash
## SCRIPT de IPTABLES
## Script para firewall de red-local

## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat –F

## Se establece politica por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP
```

```
# El localhost se deja abierto
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Al firewall de red local se tiene acceso desde la PC de administración.
iptables –A INPUT –s 192.168.0.2  -d 192.168.0.1–j ACCEPT
iptables –A INPUT –d 192.168.0.2  -s 192.168.0.1 –j ACCEPT

#Se enmascara la red local activando el BIT DE FORWARDING
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# Permitir el forward de paquetes en el firewall, es decir  que otras máquinas
puedan # salir a traves del firewall.
echo 1 > /proc/sys/net/ipv4/ip_forward

# Se debe permitir que el  firewall de red LAN se comunique con la máquina de
administración que tiene la base de datos
iptables - A FORWARD  -s  212.194.89.30  -d 192.168.0.2  -p  tcp  -dport 3306  -j
ACCEPT
iptables - A FORWARD  -d  212.194.89.30  -s 192.168.0.2  -p  tcp  -sport 3306  -j
ACCEPT

## Permitir el acceso desde la red LAN al puerto 80 (http), 25 y 110 (e-mail), 8080
y 3128 (proxy), 53 (DNS)
 iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 80 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 25 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 110 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 8080 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 3128 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -p tcp -dport 53 -j ACCEPT

## En la política por defecto DROP las sentencias del IPtable se las realiza
en # ambos sentidos
```

```
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 80 -j ACCEPT
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 25 -j ACCEPT
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 110 -j ACCEPT
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 3128 -j ACCEPT
iptables -A FORWARD -s 192.168.0.1 -p tcp -sport 53 -j ACCEPT

# Se cierra cualquier otro tipo de acceso
iptables -A FORWARD -d 212.194.89.24/29 -j DROP
iptables -A FORWARD -d 192.168.0.0/24 -j DROP

# Fin del script
```

f. Configuración del Servidor APACHE

El servidor HTTP Apache es el sistema núcleo con funcionalidades básicas que soporta módulos cargables dinámicamente. Estos módulos realizan tareas tales como corrección ortográfica de URL dinámica, reescritura de URL. La configuración por defecto consta de los módulos más comunes. Debido a que Apache está bajo un desarrollo constante, es necesario consultar el archivo *Install* del programa para ver cuál es la configuración por defecto actual y qué módulos opcionales están disponibles.

Red Hat 9.0 cuenta con un interfaz gráfico que facilita en gran medida el levantamiento del servidor *Web*; los pasos a seguir para este fin se indican a continuación:

1.- Menú Inicio, configuración del sistema, configuración de servidores, servidor HTTP a continuación se despliega las pantallas indicadas en las figuras 2.35 y 2.36.

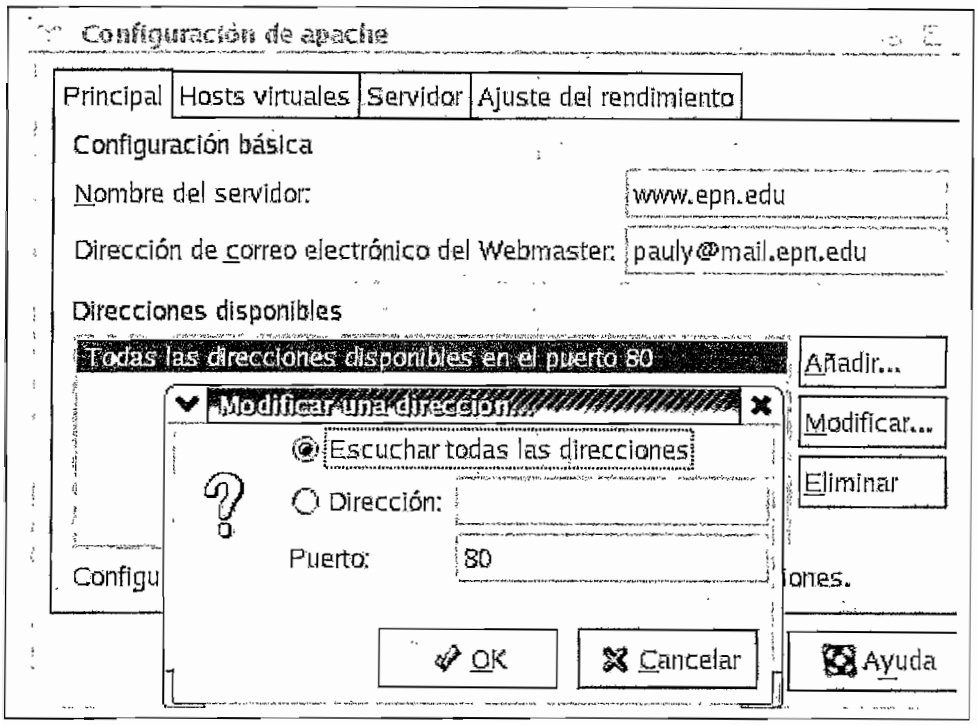


Figura 2.35 Pantalla de las propiedades del servidor Apache

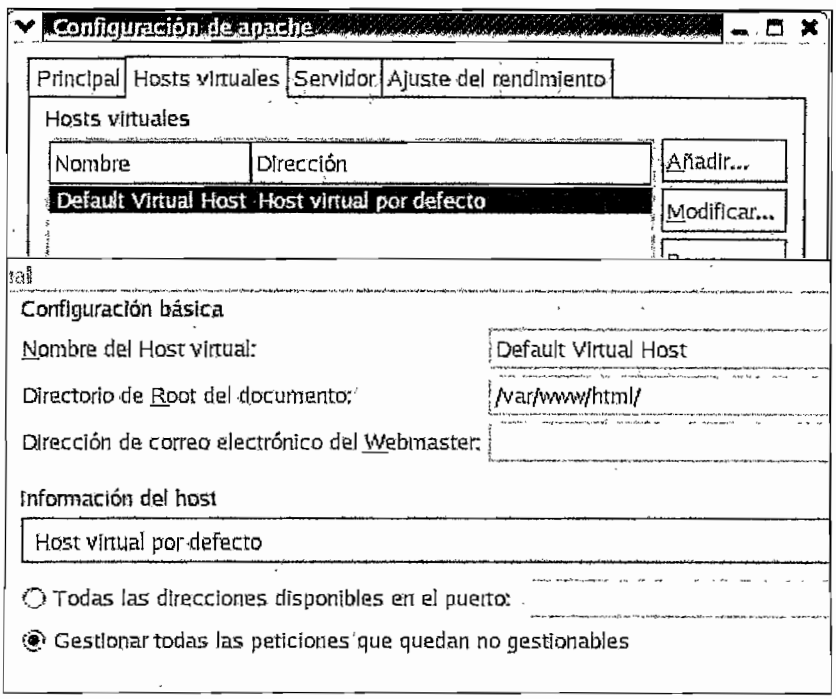


Figura 2.36 Propiedades de host-virtual

Aceptar la configuración y reiniciar los servicios de red con el comando:

/etc/init.d/httpd start.

Para comprobar el funcionamiento del servidor apache, abrir Mozilla e ingresar la dirección del servidor (www.epn.edu) para acceder a la página Web de la Intranet. (figura 2.37).

En un inicio la página *Web* por defecto es la definida por el Apache, la página *Web* de la Intranet debe colocarse en el directorio raiz /var/www/html en un archivo de nombre index.html

El criterio básico de una Intranet es el manejo de TCP/IP en un ambiente *Web*, ofreciendo un acceso remoto a los servicios de la Intranet, que serán diferenciados de acuerdo a los permisos de ingreso de cada usuario.

HTML es un lenguaje de marcación que puede viajar con el propio texto, en principio con cualquier editor de textos se puede crear un documento HTML, pero el proceso de crear una página HTML puede ser tedioso y largo, además de que precisa recordar las diferentes "*tags*" y las normas sintácticas.

Para mejorar el diseño de *Web* surgieron editores que permiten trabajar en un modo visual, más cercano a un entorno WYSWYG (*Whay You See is What You Get*), sin embargo se requiere tener un mínimo conocimiento de HTML pues estas herramientas pueden generar demasiado código basura provocando que las páginas sean muy pesadas y por lo tanto lentas para descargarse.

Para el diseño de la página *Web* de la Intranet se ha utilizado el editor Dreamweaver como herramienta de trabajo.

La página principal de la Intranet (figura 2.37), describe todos los servicios brindados por la Intranet, los cuales se distribuyen en dos ambientes diferentes:

a. Ambiente público

No requiere de autenticación y está abierto al público en general y presenta datos informativos de los servicios ofrecidos y el acceso a la *biblioteca virtual* en la que se pueden realizar consultas sobre la bibliografía existente.

b. Ambiente privado

Requiere de autenticación, está destinado exclusivamente a personal autorizado y permite el acceso a información interna de la Intranet, en lo que a registros de

sistemas de cableado estructurado, software y hardware de la red e información de personal se refiere.

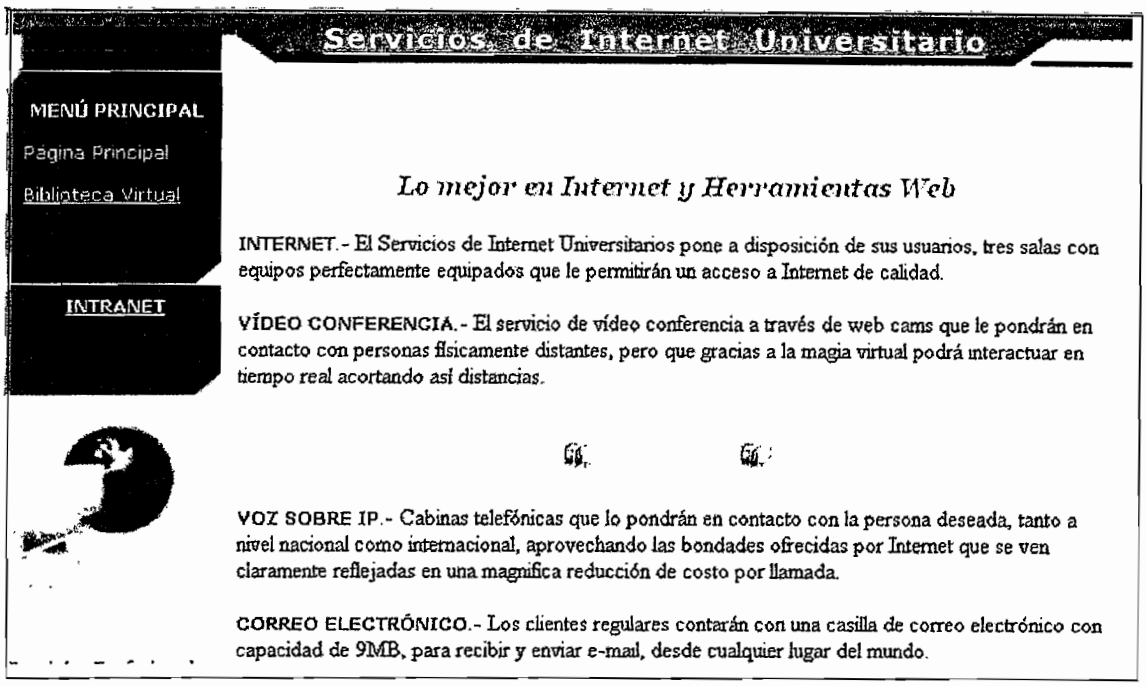


Figura 2.37 Página Web de la Intranet

La figura 2.38 muestra los servicios del ambiente privado de la Intranet.
Las diferentes pantallas que conforman la página Web de la Intranet se muestran en el Anexo H.

Figura 2.38 Página Web para ambiente privado de la Intranet

2.8 ADMINISTRACIÓN Y SEGURIDAD DE LA INTRANET

2.8.1 ADMINISTRACIÓN DE LA INTRANET

La administración de la red incluye áreas distintas, tales como: documentación de la red, seguridad de la red, mantenimiento de la red, administración del servidor, monitoreo del tráfico y mantenimiento del servidor. Cada uno de los temas enumerados es tan importante como el resto, y ninguno se debe pasar por alto. El problema es que muchos administradores consideran que, una vez que la red está funcionando, su tarea ha terminado, pero esto resulta falso ya que después de terminar la configuración de la red es cuando empieza la verdadera tarea del administrador, con el objetivo de asegurar a sus usuarios la correcta utilización de la misma.

En el Anexo I se describe detalladamente el plan de administración diseñado para la Intranet.

2.8.2 SEGURIDAD DE LA INTRANET

Antes de construir una barrera de protección para conectar la red con Internet, es importante que se entienda con exactitud qué recursos de la red y servicios se desea proteger. Una política de red es un documento que describe los asuntos de seguridad de red de una organización. Este análisis se convierte en el primer paso para construir barreras de protección efectivas.

a. Planeación de la seguridad en la red

Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de la Intranet. Esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos de la corporación y edificios de oficinas.

Se debe tener presente que la política de red a usarse no debe disminuir la capacidad de una organización. Una política de red que evita que los usuarios cumplan con sus tareas en forma efectiva puede tener consecuencias

indeseables; los usuarios de red podrían encontrar formas de ignorar la política de red, convirtiéndola en algo inútil.

Una política de seguridad de red efectiva es algo que todos los usuarios de la red y administradores pueden aceptar, y están dispuestos a reforzar.

b. Planteamiento de la política de seguridad

Definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red contra pérdidas y daños. Un planteamiento posible para desarrollar esta política es el análisis de los siguientes puntos:

¿Qué recursos se quieren proteger?

¿Cuáles son las posibles amenazas?

¿Qué tan importante es el recurso?

¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

En la tabla 2.21 se plantean los recursos de la Intranet a ser protegidos cuya importancia es calificada en una escala de 1 a 4, considerándose 1 como de mayor importancia.

En el Anexo K se presenta al detalle el plan de seguridad diseñado para la Intranet.

Se debe examinar con frecuencia la política de seguridad de la red para verificar si los objetivos y circunstancias en la red han cambiado.

Cada vez que se viola la política de seguridad el sistema se abre a amenazas de seguridad, entonces la política de seguridad deberá ser modificada para proteger aquellos elementos que no estén asegurados. Si la política de seguridad es demasiado restrictiva o no está bien explicada es muy posible que sea violada.

Cuando se detecte una violación a la política de seguridad se debe analizar si la violación ocurrió por una negligencia personal, un accidente, error, ignorancia de

la política actual o un desacato voluntario a la política de seguridad. En cada una de estas circunstancias la política de seguridad debe ofrecer guías sobre las medidas a tomar de inmediato.

RECURSO	IMP.	POSIBLES AMENAZAS	MEDIDAS PREVENTIVAS
Servidor	4	Perdida de configuración. Accesos no autorizados. Virus. Corte de energía eléctrica. Robos de hardware. Daño de hardware.	Mantener respaldos actualizados Manejo de claves y *passwords* Chequeo frecuente con antivirus actualizados. Utilización de UPS. Uso de alarmas de seguridad y el ingreso solo a personal autorizado. Redundancia de equipos.
Máquina de administración	3	Pérdida de información Accesos no autorizados Virus Robos de Hardware Daño de hardware	Sacar respaldos periódicos de los archivos de información contable y datos necesarios para la administración del sistema. Manejo de claves y *passwords*. Chequeo frecuente con antivirus actualizados. Uso de alarmas de seguridad y el ingreso solo a personal autorizado Uso de una máquina provisional.
Máquina de control	2	Accesos no autorizados Virus Robos de hardware Daño de hardware	Autenticación Chequeo frecuente con antivirus actualizados. Uso de alarmas de seguridad Uso de una máquina provisional
Máquinas de usuarios	1	Virus Robos de hardware	Chequeo frecuente con antivirus actualizados. Uso de alarmas de seguridad

Tabla 2.23 *Análisis de riesgos de la Intranet*

2.9 DISEÑOS COMPLEMENTARIOS

2.9.1 DISEÑO DE ILUMINACIÓN

La iluminación artificial desempeña un papel tan importante en los hogares, teatros, edificios para oficinas, campos de deportes, etc que sería difícil imaginar las condiciones que existirían sin ella.

Para obtener un buen alumbrado y una iluminación eficaz se necesita no solamente una cantidad suficiente de luz del color apropiado, sino que se tiene que evitar el deslumbramiento y las sombras.

Por mucha luz que se tenga si hay frente a los ojos fuentes de luz deslumbrantes o sombras oscuras proyectadas por objetos en reposo o en movimientos, la iluminación no será buena.

El brillo excesivo de las fuentes luminosas o los objetos alumbrados cansa mucho a la vista.

Se puede definir dos niveles en la iluminación de interiores: local y general. El primero se refiere a las necesidades de luz para tareas específicas que se desarrollan en diferentes puntos del espacio a iluminar. El nivel general corresponde a la iluminación en todas las demás áreas. También puede llamarse alumbrado general por zonas, cuando se deciden niveles de iluminación diferentes para cada zona, lo cual resulta más económico.
Además de definir el nivel de iluminación general se requiere cuidar la colocación de las luminarias de tal forma que se reduzca el deslumbramiento directo o reflejado o las sombras indeseables. También es necesario un completo análisis en los objetos visuales implicados en la tarea visual relativas a: tamaño, reflectancia, velocidad de exposición y contraste en el fondo.

Una vez escogidas las luminarias que se van a utilizar y determinado el nivel de iluminación requerido, podrá calcularse el número de luminarias necesarias para producir tal iluminación. No obstante, para áreas amplias es preferible utilizar el método de los lúmenes porque proporciona una iluminación media uniforme además que su aplicación no es complicada.

a. Cálculo de iluminación

Método del cálculo de lúmenes

Este método se utiliza únicamente para el cálculo de alumbrado en interiores y está basado en la definición de lux, que es igual a un lúmen por un metro

cuadrado. Con la información del fabricante sobre la emisión luminosa inicial de cada lámpara, la cantidad instalada y el área de la zona considerada, puede obtenerse el número de lúmenes por metro cuadrado o luxes.

$$E(lux) = \frac{lúmenes\_emitidos}{Área[m^2]}$$

Este valor difiere de los luxes medidos, debido a que algunos lúmenes son absorbidos por la misma luminaria o por otros factores tales como la suciedad de la luminaria y la disminución gradual de la emisión de luz de las lámparas, entre otras.

En el Anexo L se presentan los niveles de iluminación para diversas tareas recomendadas en el informe No 29 de la "*International Comission Illumination*" constituida por los comités nacionales de iluminación de treinta países. Estas recomendaciones presentan valores mínimos en el lugar mismo de la tarea visual de acuerdo con la práctica actual; una total comodidad visual puede requerir niveles superiores.

Determinación del coeficiente de utilización (CU)

El coeficiente de utilización es el cociente de los lúmenes que llegan al plano de trabajo y los totales generados por la lámpara. Este factor toma en cuenta la eficacia y la distribución de la luminaria, su altura de montaje, las dimensiones del local y la reflectancia de las paredes, techo y suelo. A causa de la múltiples reflexiones que tienen lugar dentro de un local, una parte de la luz pasa hacia abajo del plano imaginario de trabajo más de una vez por lo que en algunas circunstancias el coeficiente de utilización puede sobrepasar la unidad. En general cuanto más alto y estrecho sea el local, mayor será la proporción de la luz absorbida por las paredes y menor el coeficiente de utilización; este efecto se considera mediante la relación de local (RL), que se define como sigue:

Para alumbrado directo, semidirecto y mixto

$$RL = \frac{l * a}{H(l + a)}$$

Para alumbrado semidirecto e indirecto

$$RL = \frac{3(l * a)}{2H(l + a)}$$

Donde:
l = longitud del local
a = ancho del local
H = altura del puesto de trabajo

Los datos técnicos del coeficiente de utilización para las diferentes luminarias están reunidas en el Anexo L.

Cuando se trabaja con luminarias no incluidas en dichas páginas, el coeficiente de utilización deberá tomarse de una luminaria similar.

Para luminarias montadas o empotradas en el techo, la reflectancia del techo es la misma que la del techo real. Para lámparas suspendidas, en cambio es necesario obtener la reflectancia efectiva del techo

Determinación del coeficiente de conservación (CC)

Desde el primer día en que se pone a funcionar el alumbrado, la iluminación va cambiando conforme las lámparas envejecen. Además la suciedad acumulada en las luminarias y otros factores contribuyen a la pérdida de luz. El efecto neto es casi siempre una disminución del nivel de iluminación, aunque ciertos factores pueden producir un incremento.

El coeficiente de conservación es el resultado final por la presencia de todos los factores parciales. Se define como el cociente de iluminación cuando alcanza su nivel más bajo en el plano de trabajo entre el nivel nominal de iluminación de las lámparas.

Para el cálculo del CU se consideran los factores de reflactancia (techo y paredes) indicados en las tablas 2.22 y 2.23.

TIPO DE REFLEXIÓN	MATERIALES	LUZ REFLEJADA (%)
Regular	Vidrio plateado Aluminio abrillantado Aluminio pulido y cromo	80 - 90 75 – 85 60 – 70
Difusa	Encalado con yeso Arce y maderas similares Hormigón Nogal y maderas similares Ladrillo	80 – 90 60 15 – 40 15 – 20 5 – 25
Mixta	Esmalte blanco – aluminio satinado Aluminio cepillado – cromo satinado	70 – 90 55 – 58

Tabla 2.24 *Niveles de luz reflejada en materiales[10]*

Cálculo del número de luminarias

El número de luminarias (unidades de alumbrado) puede calcularse de la siguiente manera:

$$Número\_luminarias = \frac{luxes\_escogidos * área}{lúmenes\_lámpara * CU * CC}$$

TONALIDAD	COLOR DE PAREDES Y TECHOS	LUZ REFLEJADA (%)
Clara	Blanco Crema - claro Amarillo - claro Verde claro y rosa Azul y gris claro	75 – 90 70 – 80 55 – 65 45 – 50 40 – 45
Media	Beige Ocre, marrón claro, verde oliva	25 – 35 20 – 25
Oscura	Verde, azul, rojo, gris (todos oscuros) Negro	10 – 15 4

Tabla 2.25 *Niveles de luz reflejada en paredes y techos [10]*

Determinación de la ubicación de las luminarias

La colocación de las luminarias depende de la arquitectura general, de las dimensiones del edificio, del tipo de luminaria y la ubicación de las tomas de energía existentes.

Para conseguir una distribución uniforme de iluminación sobre una zona, se recomienda colocarlas más próximas a fin de obtener los niveles de iluminación requeridos. Frecuentemente los equipos fluorescentes deben montarse en filas continuas.

Al montar aparatos para alumbrado industrial o comercial, se debe tener en cuenta la distancia que tendrá que recorrer la luz para llegar al plano de trabajo. En una oficina puede ser la parte superior de los escritorios; en una sala de dibujo la superficie de los tableros y en un taller mecánico la altura de la máquina o el banco en el que trabaja el operario.

Como es muy raro que se necesite el máximo de luz en el suelo, sólo se debe planear la instalación para obtener las intensidades apropiadas en el plano de trabajo. El estudio de la maquinaria o del trabajo que se realiza en una habitación o edificio revelará fácilmente a qué altura sobre el suelo se encuentra el plano de trabajo, pero si no pueden tomarse medidas, suele suponerse que éste se encuentra a unos 76 centímetros del suelo.

Altura de montaje o instalación

Es de vital importancia tener en cuenta en la colocación de los aparatos su altura de montaje (figura 2.39). Esta altura es la distancia vertical del foco luminoso al plano de trabajo y por supuesto esta distancia es la que afecta al coeficiente de utilización y a la intensidad de iluminación obtenida en el plano de trabajo.

La distancia desde el piso al techo de una habitación cualquiera se llama altura de techo de la misma.

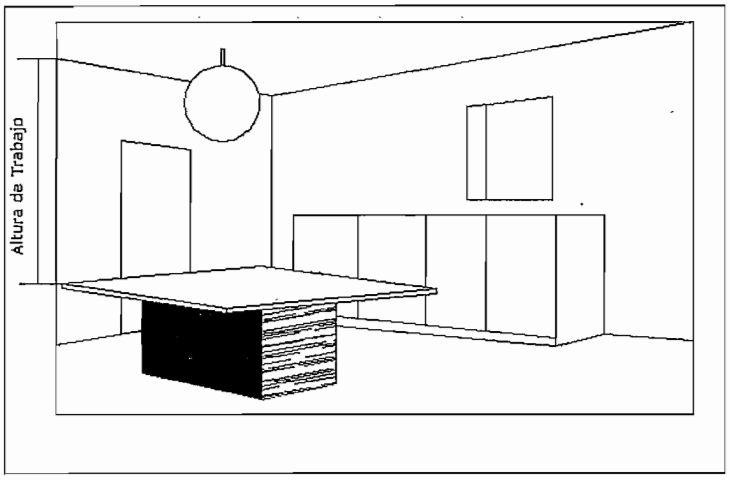


Figura 2.39 *Altura de montaje [10]*

Con alumbrado directo el foco luminoso es la lámpara propiamente dicha y su reflector. En el alumbrado indirecto y semindirecto el foco luminoso se supone que es el techo.

Número y situación de las luces

En general, no se debe tratar nunca de economizar el número de luces o de circuitos de alumbrado cuando se plantea una instalación. Si una buena iluminación representa una economía, es indudable que será una falsa economía tratar de ahorrar algo en los costos de los materiales o aparatos de la instalación, reduciendo el número de salidas para aparatos o esforzándose por separarlos más de lo conveniente.

Teniendo en cuenta la rapidez con que aumentan actualmente los estándares de iluminación en todas las clases de edificios modernos, es preferible planear con vistas al futuro y poner una iluminación adecuada cuando se está instalando.

Pueden obtenerse los mejores resultados si se disponen suficientes salidas, lo bastante próximas unas a otras para dar una distribución e iluminación uniformes.

Distancia de espaciamiento

En las habitaciones pequeñas cerradas por tabiques permanentes y en las cuales es suficiente una lámpara, basta por supuesto situar este aparato en el centro del

techo. En las habitaciones grandes en las que son necesarias varias lámparas, se necesita alguna regla, norma o estándar para fijar el número del espaciamiento de las mesas. La distancia entre las luces o salidas para ellas se denomina distancia de espaciamiento; esta distancia variará algo según la forma y la altura de la habitación, pero puede fijarse fácilmente aplicando la siguiente regla: para obtener la eficiencia máxima, la distancia de espaciamiento debe ser igual a la altura de montaje de las lámparas, en tanto que la distancia máxima de espaciamiento eficiente es de 1.5 veces dicha altura.
En algunos casos, talvez parezca esta distancia innecesariamente pequeña pero si se desea obtener una buena iluminación, las luces pocas veces deben estar espaciadas más de 1.5 veces la altura de montaje.

Puede presentarse algunos casos en los cuales en un edificio no sea necesario dotarlo de iluminación general tan buena, pero si después se destina a algún otro uso, puede ser muy necesario emplear la intensidad estándar de iluminación.

En el diseño se considera que la iluminación será general semidirecta con focos fluorescentes tomando en cuenta su alta luminosidad con un bajo consumo de potencia.

La tabla 2.24 resume el número de luminarias requeridas para la Intranet y a continuación se presenta un ejemplo de cálculo.

Lúmenes_ lámparas = 2300
Luxes_escogidos = 500

a = 4
l = 4.4
h = 2.5
H = 2.5 – 0.60
H = 1.9

$$RL = \frac{3(l*a)}{2H(l+a)}$$

$$RL = \frac{3(4.4*4)}{2*1.9(4.4+4)}$$

$$RL = 1.65$$

Luego de obtener la relación del local se selecciona la letra correspondiente que permitirá escoger el coeficiente CU y CC necesario para el cálculo del número de luminarias.

RL	0.7	0.9	1.12	1.38	1.75	2.25	2.75	3.50	4.50
	J	I	H	G	F	E	D	C	B

Para escoger el coeficiente de utilización y el coeficiente conservación se considera que las paredes serán de encalado con yeso escogiendo el porcentaje promedio del 85%. Como color de paredes y techo se considera serán de color azul el porcentaje de luz reflejada será el 40%, como lo señala las tablas 2.22 y 2.23.

Con la ayuda de las tablas del Anexo L y de acuerdo al tipo de luminaria escogida se determina que los valores para:

CU = 0.49
CC = 0.75

Por lo tanto el número de lámparas necesarias para la sala A es de:

$$\text{Número\_luminarias} = \frac{luxes\_escogidos * área}{lúmenes\_lámparas * CU * CC}$$

$$\text{Número\_luminarias} = \frac{500*(4.4*4)}{2300*0.49*0.75}$$

$$\text{Número\_luminarias} = 10$$

CÁLCULO DE ILUMINACIÓN

LOCAL						Nivel de	LUMINARIAS			CÁLCULOS				Nº Lumin
Nº	DESCRIPCIÓN	DIMENSIONES				Iluminación								
		Ancho (m)	Largo (m)	Altura (m)	Altura Punto_Trabajo	Escogido (Lux)	Tipo	Potencia (w)	Flujo (Lúmenes)	Relación de Local	C.U.	C.C.	Lumn. Calc.	Escog.
1	Sala A	4	4,4	2,5	1,9	500	Fluoresc.	36 (W)	2300	1,65413534	0,49	0,75	8800	10
2	Sala B	4	4,1	2,5	1,9	500	Fluoresc.	36 (W)	2300	1,59844055	0,49	0,75	8200	10
3	Sala C	4	4,3	2,5	1,9	500	Fluoresc.	36 (W)	2300	1,63601776	0,49	0,75	8600	10
4	Cabinas	0,6	0,6	2,5	1,9	50	Ojos de Buey	50(W)	200	0,15789474	0,36	0,8	18	1
5	Administración	3,4	2,6	2,5	1,9	500	Fluoresc.	36 (W)	2300	1,16315789	0,49	0,75	4420	6
6	Bar	1,4	2,6	2,5	1,9	100	F.circular	24 (W)	1700	0,71842105	0,3	0,7	364	1
7	Área de Control	1,9	1,5	2,5	1,9	500	Fluoresc.	36 (W)	2300	0,66176471	0,49	0,75	1425	2
8	Sala de espera	2,6	6,7	2,5	2,5	50	Fluoresc.	36 (W)	2300	1,12387097	0,46	0,7	871	1
9	Corredor	0,7	5,9	2,5	2,5	50	Fluoresc.	36 (W)	2301	0,37545455	0,3	0,7	206,5	1
10	Lavabos Hombres	1,4	2,2	2,5	2,5	50	F.circular	24 (W)	1700	0,51333333	0,3	0,7	154	1
11	Baño Hombres	0,6	1,1	2,5	2,5	50	Incandesc.	60 (W)	500	0,23294118	0,36	0,8	33	1
12	Lavabos Mujeres	1,4	2,2	2,5	2,5	50	F.circular	24 (W)	1700	0,51333333	0,3	0,7	154	1
13	Baño Mujeres	0,6	1,1	2,5	2,5	50	Incandesc.	60 (W)	500	0,23294118	0,36	0,8	33	1
14	Ingreso	1,8	3,3	3	3	100	Fluoresc.	36 (W)	2300	0,58235294	0,3	0,7	594	1

Tabla 2.26 *Cálculo de luminarias*

Distribución de circuitos

Normalmente para áreas habitacionales se usan circuitos de 20 A como máximo; en industrias se pueden usar circuitos con cargas múltiples de hasta 50 A. Las salidas para usos especiales deben tener su propia alimentación y protección. Es posible que aunque algunos circuitos queden con muy poca carga convenga tenerlos alimentados por separado. De este modo se van decidiendo grupos de carga que constituyen los circuitos del tablero.

Para los tableros trifásicos es común dividir la carga total entre tres para conocer el valor exacto de equilibrio. Después se hacen tres grupos cuyos circuitos puedan combinarse para que las sumatorias respectivas sean lo más cercano al valor de equilibrio. El desbalance entre las tres fases debe ser menor al 5 % y se calcula con la siguiente relación

$$\frac{(SM - Sm) * 100}{Sp} < 5\%$$

SM = voltamperes de la fase más cargada
Sm = voltamperes de la fase menos cargada
Sp = voltamperes de la fase promedio (carga total entre 3)

Se puede plantear la carga de alumbrado en forma alternada, para cuando se quiera tener la posibilidad – durante los días no hábiles - de disminuir el nivel de iluminación en forma considerable. Esto se facilita utilizando una numeración consecutiva de las cargas de alumbrado y colocando en un lado del tablero los números impares y en el otro los números pares.

Si se quiere dejar circuitos de reserva para el futuro, deben considerarse como si ya existiesen, sumándolos a la carga total del tablero para especificar el alimentador y su protección. Los interruptores derivados de reserva se pueden colocar sin conectar o sólo dejar los espacios correspondientes.

De acuerdo con los siguientes criterios:

1. Los circuitos de iluminación deben ser independientes de los de tomacorrientes
2. Si se trata de un tablero monofásico se pueden asignar números al azar. Para el caso de tableros bifásicos, se divide la carga en dos, de tal manera que con la combinación de circuitos se obtenga una diferencia mínima entre las cargas conectadas a cada fase.
3. El número máximo de salidas en los circuitos de iluminación y de tomacorrientes no deben superar las 10 salidas.

La distribución de los circuitos de iluminación y de tomacorrientes se presenta en el Anexo M.

2.9.2 INSTALACIONES ELÉCTRICAS

a. Determinación de la demanda de diseño

Como paso previo al dimensionamiento y localización de los elementos de la red, se deben establecer los parámetros que en función de los antecedentes del proyecto y los criterios técnicos y económicos aplicables al caso específico determinan en forma preliminar, valores límites, rangos de capacidades de los equipos, dimensiones mínimas de los componentes, disposiciones a considerar, etc, dentro de los cuales se analizarán alternativas y se desarrollarán los cómputos para justificar en el paso siguiente la selección definitiva de la configuración de la red, localización, dimensiones y capacidades de sus elementos.

Procedimiento para la determinación de la demanda máxima unitaria

En función de factores tales como localización del proyecto en relación a centros urbanos desarrollados, división y uso del suelo, características de las obras de infraestructura previstas, área y características de los edificios a construir, etc. Se establecen, los valores de demanda unitaria a considerar para el diseño.

A continuación se detalla el procedimiento para la determinación de la demanda, aplicable a los casos usuales.

1. Determinación de la carga instalada del consumidor de máximas posibilidades:
   Considerar aquel consumidor que en función de los factores analizados pudiera disponer del máximo número de artefactos de utilización y establecer un listado de los mismos con el número de referencia

2. Carga instalada del consumidor representativo:
   Para cada una de las cargas individuales se establece un factor denominado "factor de frecuencia de uso (FFUn)" expresado en porcentaje, será determinado para cada una de las cargas instaladas en función del número de usuarios que disponen del artefacto correspondiente

3. Determinación de la demanda máxima unitaria (DMU):
   Definida como el valor máximo de la potencia que en un intervalo de tiempo de 15 minutos es suministrado por la red al consumidor individual.

   Se determina a partir de la carga representativa instalada del consumidor (CIR), y la aplicación del factor de simultaneidad (FSn) para cada una de las cargas instaladas, el cual determina la incidencia de la carga considerada en la demanda coincidente durante el periodo de máxima solicitud.

   El factor de simultainedad, expresado en porcentaje será establecido para cada una de las cargas instaladas, en función de la forma de utilización de artefactos y aparatos para una aplicación determinada. En general, los servicios básicos de uso comunitarios, tales como iluminación, calefacción, entretenimiento, etc tendrá un factor cuya magnitud se ubicará en el rango superior.

   El factor de demanda FDM está definido por la relación entre la demanda máxima unitaria DMU y la carga instalada CIR, indica la fracción de la carga instalada que es utilizada simultáneamente en el período de máxima solicitud.

4. Proyección de la demanda:

   La demanda máxima unitaria expresada en vatios, es convertida a kilovatios y kilovoltamperios, mediante la reducción correspondiente y la consideración del factor de potencia.

   El valor obtenido de la demanda máxima unitaria DMU es válido para condiciones iniciales de instalación; para efecto del diseño deben considerarse los incrementos que la misma tendrá lugar durante el período de vida útil de la instalación. Este incremento progresivo de la demanda que tiene una relación geométrica al número de años considerado, se expresa por un valor índice acumulativo anual "Ti" que permite determinar el valor de la demanda máxima unitaria proyectada DMUp para un período de "n" años a partir de las condiciones iniciales de la siguiente expresión:

$$DMUp = DMU\left(1+\frac{Ti}{100}\right)^{n}$$

En la tabla 2.25 se resumen los valores de demanda del diseño.

Los valores de Ti se eligen de acuerdo a la Demanda Unitaria y al tipo de usuario definido por el Ilustre Municipio Metropolitano de Quito. El sector donde se implementará la Intranet es considerado Residencial 1 (usuario tipo A). La tabla 2.26 resume los valores de Ti.

b. Cálculo de conductores

Los principales criterios que se deben considerar para la especificación del conductor son: capacidad de conducción de corriente para las condiciones de instalación, caída de voltaje permitida, capacidad para soportar la corriente de cortocircuito y calibre mínimo permitido para aplicaciones específicas.

El mínimo calibre de conductor usado es el número 14 AWG, aún cuando para fines prácticos se recomienda el número 12 AWG. Por razones constructivas por lo general los calibres superiores al número 1/0 AWG se construyen multifilares, en lugar de ser sólidos, esto debido a que resulta más fácil su manipulación.

APARATOS ELÉCTRICOS Y DE ALUMBRADO				FFU	CIR	FSn	DMU
N°	DESCRIPCIÓN	CANT.	Pn (W)	(%)	(W)	(%)	(W)
1	Computadores	50	12500	100	12500	100	12500
2	Impresoras	2	160	50	80	100	80
3	Fax	1	80	10	8	100	8
4	*Scanner*	1	15	10	1,5	100	1,5
5	Teléfonos	6	30	80	24	50	12
6	Lámpara Fluorescente	46	1840	100	1840	100	1200
7	Lámpara incandescentes	5	250	100	250	100	250
8	Tomacorrientes	25	5000	60	3000	50	1500
9	Microondas	1	750	20	150	100	150
10	Refrigerador	1	300	100	300	100	300
11	Cafetera	1	600	50	300	100	300
12	Radio Grabadora	3	45	75	33,75	100	33,75
13	Televisor	1	250	50	125	100	125
14	Aspiradora	1	400	10	40	100	40
	Totales		**22220**		**18652,25**		**17140,25**

Factor de potencia de la carga FP		Factor de demanda FDM	0,919
DMU (KVA)	16.5	Carga Instalada (KW)	21.58
TI (%)	100	Carga Representativa (KW)	19.831
(1+Ti/100)^10	1024		
DMUp(KVA)	16896		

Tabla 2.27 *Cálculo de la demanda*

USUARIO TIPO	DMU KVA	Ti
A	16 – 8	1,5 – 2,5
B	8 – 4	2,5 – 4
C	4 – 2	4,0 – 5,5
D	2 – 1,2	5,5 – 6,500
E	1,6 – 0.8	6,5

Tabla 2.28 *Valores de Ti*

En la tabla 2.27 se muestran los valores de conductores necesarios para la instalación.

CIRCUITO	POTENCIA (W)	CONSTANTE K	VOLTAJE (V)	FACTOR POTENCIA	CORRIENTE (A)	TIPO DE CONDUCTOR
CI-1	360	1,7	121	1	1,75	TW12AWG
CI-2	360	1,7	121	1	1,75	TW12AWG
CI-3	360	1,7	121	1	1,75	TW12AWG
CI-4	388	1,7	121	1	1,88	TW12AWG
CI-5	204	1,7	121	1	0,99	TW12AWG
TC-1	1700	1,7	121	1	8,26	TW12AWG
TC-2	2000	1,7	121	1	9,72	TW12AWG
TC-3	1700	1,7	121	1	8,26	TW12AWG
TC-4	2250	1,7	121	1	10,9	TW12AWG
TC-5	1700	1,7	121	1	8,26	TW12AWG
TC-6	1750	1,7	121	1	8.50	TW12AWG
TC-7	1400	1,7	121	1	6.8	TW12AWG
TC-8	1800	1,7	121	1	8.70	TW12AWG
TC-9	2000	1,7	121	1	9.72	TW12AWG

Tabla 2.29 *Cálculo de conductores*

c. Cálculo del conductor del tablero de distribución al tablero de medidores

En todas las instalaciones eléctricas, los conductores se deben dimensionar de manera que la caída de voltaje no exceda al 3%, ya sea que se alimente cargas de alumbrado, fuerza, calefacción, aire acondicionado, o cualquier combinación de éstas. En adición la máxima caída de voltaje total en los conductores de alimentadores o circuitos derivados, no debe exceder en ningún caso al 5%.

La caída de voltaje en los circuitos bifásicos, considerando la carga principalmente resistiva y despreciando el efecto inductivo se calcula de la siguiente forma:

$$I = \frac{DMUp}{K * V}$$

$$I = \frac{16896}{1.73 * 210}$$

$$I = 46.5[A]$$

Se considera necesario la utilización de cable TW6AWG.

d. Cálculo de caída de voltaje

$$\Delta V = \frac{\rho L I}{S}$$

$$\Delta V = \frac{1.724^{-2} * 35 * 46.5}{4.11}$$

$$\Delta V = 6.8$$

$$\Delta V(\%) = \left(\frac{6.8}{210}\right) * 100$$

$$\Delta V(\%) = 3.2\%$$

Donde:

ρ = resistividad del cobre (1.724^{-2})

L = longitud del cable entre tablero armario de medidores y *breaker*

I = corriente que llevará el conductor

S = área transversal del conductor

En vista de que la caída de voltaje excede el 3% del voltaje de alimentación (210 V), se decide utilizar el cable THW6AWG

$$\Delta V = \frac{\rho L I}{S}$$

$$\Delta V = \frac{1.724^{-2} * 35 * 46.5}{4.65}$$

$$\Delta V = 6$$

$$\Delta V(\%) = \left(\frac{6}{210}\right) * 100$$

$$\Delta V(\%) = 2.8\%$$

e. Protecciones eléctricas

Aunque no es posible construir una instalación eléctrica totalmente a prueba de fallas, vale la pena dedicar tiempo y esfuerzo al análisis de fallas más probables y a diseñar cuidadosamente el sistema de protecciones.

Se presenta un panorama general de las situaciones que puedan representar peligro para las personas y para los elementos de instalación. Se deben ubicar dispositivos para evitar el peligro dentro de lo posible; aparatos sensores que detecten fallas y tipos de interruptores disponibles para abrir los circuitos en los que aparecen corrientes peligrosas.

La tabla 2.28 resume las protecciones recomendadas para cada circuito, además presenta la distribución de circuitos, considerando el respectivo balance de carga.

La tabla 2.29 muestra los materiales necesarios para la red eléctrica de la Intranet.

Por lo tanto se requieren 42 tubos PVC de una pulgada y 6 rollos de cable TW12AWG y medio rollo de cable THW6AWG.

El plano de la distribución eléctrica se muestra en el Anexo P, y en el Anexo N se muestran las pruebas que se aplican a los sistemas eléctricos.

CIRCUITO	POTENCIA (W)	CORRIENTE (A)	PROTECCIÓN (A)	BALANCEO DE CARGA
CI-1	216	1,05	15	Fase R
CI-2	216	1,05	15	Fase S
CI-3	216	1,05	15	Fase T
CI-4	316	1,53	15	Fase R
CI-5	204	0,99	15	Fase S
TC-1	1700	8,26	15	Fase R
TC-2	2000	9,72	15	Fase T
TC-3	1700	8,26	15	Fase S
TC-4	2250	10,9	15	Fase T
TC-5	1700	8,26	15	Fase S
TC-6	1750	8.50	15	Fase R
TC-7	1400	6.8	15	Fase T
TC-8	1800	8.70	15	Fase R
TC-9	2000	9.72	15	Fase S

Tabla 2.30 *Protecciones para la instalación eléctrica*

ELEMENTO	CANTIDAD
Focos fluorescentes	46
Focos fluorescentes circular	1
Focos ahorradores	4
Cajas	90
Interruptores	15
Tomas	75
Protecciones	14
Codos	7
Cajetines de paso	5
Tuberías una pulgada	125 m
Cable TW12AWG	258 m
Cable THW6AWG	35 m
Tablero De distribución	1

Tabla 2.31 *Resumen de materiales necesarios para la instalación eléctrica*

CAPÍTULO III

ANÁLISIS ECONÓMICO Y DE FACTIBILIDAD DEL PROYECTO

ANÁLISIS ECONÓMICO Y DE FACTIBILIDAD DEL PROYECTO

La puesta en marcha de una Intranet implica gastos como son: equipamiento, instalación, mantenimiento, etc. Los mismos que garantizan el buen funcionamiento de la red.

En este capítulo se analizan los aspectos económicos de la Intranet, que incluyen estudios de mercado, aspectos técnicos (relación costo beneficio), aspectos financieros enmarcados en la determinación de la inversión requerida, formas de financiamiento, punto de equilibrio y evaluación financiera.

El estudio de factibilidad plantea el estudio de variables que inciden en un proyecto.

"Todo proyecto se compone de cuatro partes fundamentales" [19]:

a. Estudio de mercado

Sirve como base para estimar los ingresos generados por el proyecto.

El estudio de mercado aborda la oferta y demanda de bienes o servicios. Intenta determinar la cantidad de producto o servicio que va a ser demandado; es decir, establece cuánto se debe producir, a qué precio, especificando las características del producto o servicio, abordando problemas de comercialización, materiales, etc.

b. Estudio Técnico

Describe las características técnicas que determinan el tamaño requerido de la empresa para atender a la demanda, características de maquinaria, del equipo, así como los costos en que se incurrirá y cuáles serán los ingresos que va a generar. Este aspecto del proyecto se ha tratado en el capítulo 2 con gran detalle.

c. Estudio Financiero

Este estudio señalará las necesidades totales de capital para la inversión, la misma que debe ser desglosada en inversión fija y capital de trabajo.

d. Evaluación Financiera

Determina patrones de comparación financiera. Los indicadores básicos de evaluación financiera que miden la rentabilidad de un proyecto son: Rentabilidad simple, período de recuperación de capital, relación costo beneficio, valor actual neto (VAN) y la tasa interna de retorno (TIR)

3.1 ESTUDIO DE MERCADO

Para lograr un desarrollo sistemático para el estudio de mercado, se deben seguir los siguientes pasos:

- Definición del problema
- Formulación de un diseño de investigación
  - → Análisis de datos secundarios
  - → Método para la recopilación cuantitativa de datos
  - → Definición de la información necesaria
  - → Diseño del cuestionario
  - → Proceso de muestreo y tamaño de la muestra
- Trabajo de campo o recopilación de datos
- Preparación y análisis de datos
- Preparación y presentación de informes

3.1.1 DEFINICIÓN Y ANÁLISIS DEL PROBLEMA

La Institución educativa, para la cual se lleva a cabo el presente proyecto, no cuenta con un servicio adecuado de acceso a Internet, y la mayor parte de potenciales usuarios (estudiantes) hasta ahora, no han podido acceder a muchos de sus beneficios, debido a que no existe dentro de la Institución un lugar adecuado para realizar esta actividad.

Se debe realizar para cualquier proyecto un análisis de la situación tanto interna como externa que definitivamente influirá en la implementación del mismo, ya que

lo que busca una investigación de mercado es minimizar la incertidumbre de decisión.

Debe considerarse un análisis del entorno en el cual se desenvolverá el proyecto, considerando variables macroambientales y microambientales, pues de esta forma se podrá prever los continuos cambios que se dan en el ambiente del mismo.

a. Macroambiente

En este ambiente inciden determinadas variables sobre las cuales la empresa que implementará el proyecto, no tiene influencia alguna por lo que es necesario que la organización se adapte a ella.

Las variables macroambientales que incidirán en el proyecto son:

Variables tecnológicas

El proyecto se desenvuelve en un ambiente en el que las tecnologías de acceso a Internet, hardware y software mantienen un desarrollo acelerado, que conlleva a una actualización continua de equipos, lo que representa inversiones periódicas que permitan satisfacer las crecientes necesidades del usuario.

Estos avances tecnológicos incentivan al usuario a ser partícipe de las facilidades y beneficios de estos sistemas de comunicación, generándose la necesidad de utilizar centros que brinden acceso de calidad a estas facilidades.

Variables políticas

El grado de incidencia de las variables políticas del país y de la Institución en el proyecto, dependerá del nivel de consenso que se pueda alcanzar en los niveles administrativos de la Institución, para la ejecución y administración de este centro.

b. Microambientales

Las variables microambientales pueden generar cambios que influyen en la disponibilidad y el precio del producto o servicio.

Las variables microambientales que incidirán en el proyecto son:

Demanda

"La demanda es la cantidad del producto o servicio que el consumidor está dispuesto a adquirir por un cierto precio y en un tiempo determinado" [17]

El constante desarrollo de la ciencia y la tecnología obliga al sector académico de la Institución a mantenerse actualizado, lográndose una constante demanda del servicio de acceso a Internet en los períodos lectivos de la Institución.

La demanda de los servicios de Internet dentro de la Institución, se ve favorecida por la distribución de horarios de estudio, que impiden al sector académico aprovechar este servicio desde sus hogares o lugares distantes a los predios universitarios.

Oferta

"La oferta es la cantidad del producto o servicio que se ofrece al consumidor por un precio determinado" [17]

Dentro de la Institución educativa sí existe oferta de acceso a Internet, pero los niveles de calidad en lo que respecta a velocidad, no satisfacen las necesidades del usuario; adicionalmente en horas pico el número de centros no es suficiente para abastecer la demanda generada.

En lo que a VoIP y vídeoconferencia se refiere, no existe ningún lugar que solvente esta necesidad.

Existen pocos centros externos a la Institución que brindan servicio de acceso a Internet, pero sólo uno de ellos ofrece VoIP y vídeoconferencia.

Proveedores

La calidad de los servicios brindados por la Intranet, depende de forma directa del cumplimiento de los niveles de calidad de servicio acordados con el ISP.

Usuarios

El proyecto está dirigido para toda la comunidad universitaria, y en alto porcentaje a los estudiantes que debido a su capacidad económica demandan de un servicio eficiente a costos razonables.

Análisis externo

Este análisis contempla la formulación de fortalezas, debilidades, oportunidades y amenazas que probablemente se presenten en el proyecto.

Fortalezas

"Es un atributo interno que debería poseer la empresa y que puede constituirse en una ventaja frente a las empresas de la competencia".

La fortaleza de este proyecto es:

- Personal con buen conocimiento técnico

Oportunidades

"Son los factores que existen en el mercado que podrían ser aprovechados por la empresa en su beneficio".

Las oportunidades son:

- Baja calidad del servicio ofrecido actualmente
- Mercado constante
- Alta demanda insatisfecha

Debilidades

"Falta de atributo interno que se constituye en una desventaja frente a las empresas competidoras". [17]

Las debilidades son:

- Fuerte inversión inicial
- La ubicación del local

Amenazas

"Es cualquier factor externo a la empresa que podrían afectar su normal desarrollo". [17]

Las posibles amenazas son:

- Demasiados requerimientos legales que desanimen la inversión en el proyecto

- Existencia de grupos con intereses específicos que intenten impedir la concreción del proyecto

Es importante ahora, que luego del análisis del contexto que rodea el problema, se definan los servicios que se pretende ofrecer.

3.1.2 DEFINICIÓN DE SERVICIOS

a. Acceso a Internet

El acceso a Internet que se brindará, contará con niveles de calidad aceptables, es decir la red estará disponible de 8h00 a 18h00 y contará con una buena velocidades de acceso.

b. Videoconferencia

Inicialmente se plantea el servicio de vídeoconferencia de escritorio, el cual contará con una PC totalmente equipada que permitirá ofrecer este servicio a precios accesibles.

A mediano plazo se propone mejorar este servicio, usando una cámara especializada para el efecto.

c. Voz sobre IP

Se prestará este servicio a través de dos cabinas telefónicas, aprovechando las ventajas de acceso a Internet que permiten disminuir el costo por llamada.

d. Correo electrónico

Se contará con servidores de correo electrónico que permiten un almacenamiento de 10 MBytes por cuenta de correo.

e. Servicios varios: fax, *scanner*, impresión

Como complemento a los servicios de Internet, se ofrecerán impresiones a blanco y negro con impresora láser y a color con impresoras de inyección a tinta.

El servicio de *scanner* será de alta resolución y finalmente también se dará servicio de fax cuando el usuario así lo requiera.

f. Servicio de bar

Para mejorar el confort de los usuarios se contará con servicio de bar, el cual pondrá a disposición colas, sánduches, cafés, jugos, etc.

El paso que sigue a la definición del problema y los servicios que se pretenden brindar es la investigación de mercado, que como una actividad científica consiste en un proceso sistemático de tareas que conlleven a resultados que se ajusten a la realidad.

3.1.3 INVESTIGACIÓN DE MERCADO

El proceso de investigación de mercado, consiste en los siguientes pasos:

1. Establecer la razón fundamental del estudio
2. Objetivos de la investigación y necesidades de información
   Esta actividad implica la determinación de la información que se requiere para un proyecto en particular.
3. Diseño de la investigación y fuentes de datos
   Es un plan básico que guía las fases de recolección y análisis de datos del proyecto de investigación. Es la estructura que especifica el tipo de información a recolectar, las fuentes de datos y los procedimientos y análisis de recolección de datos.
4. Diseño de la muestra
   Requiere una definición precisa de la población de la que se extraerá la muestra y determinará su tamaño.
5. Procesamiento y análisis de datos recopilados
6. Presentación de resultados

A continuación se desarrollarán estos pasos aplicándolos a la Intranet objeto de este proyecto

a. Objetivo de la investigación

- Determinar la demanda de acceso a los servicios de Internet dentro de la Institución educativa.

b. Necesidades de información

- Determinar la frecuencia con que los estudiantes de la Institución acceden a los servicios de Internet
- Determinar cuáles de los servicios de Internet son los más utilizados.
- Determinar el lugar desde el cual los usuarios generalmente acceden a Internet.
- Determinar la percepción de los usuarios respecto al acceso a Internet con el que se cuenta en la Institución educativa, tanto en calidad como en costo.
- Determinar qué valor estarían dispuestos a pagar los usuarios de este sistema.
- Determinar las sugerencias de los usuarios para el mejoramiento del servicio de acceso a Internet.

c. Diseño de la investigación y fuentes de datos

Existen algunos tipos de investigaciones, en el presente caso se utilizará la investigación concluyente del tipo descriptiva, que en su mayor parte depende principalmente de la formulación de preguntas a los encuestados y de la disponibilidad de datos en fuentes secundarias. Este tipo de investigación permitirá determinar la asociación de las diferentes variables de *marketing* y determinar la frecuencia de ocurrencia, así como realizar predicciones en cuanto a éstas.

En este proyecto, lo que se busca es el estudio dél potencial mercado con el fin de determinar su tamaño, así como los requerimientos de los usuarios. Para este objetivo, se tomará una muestra de los elementos de los posibles usuarios, y se aplicará una encuesta, que permita describir las características de los consumidores y la frecuencia de los fenómenos de *marketing*.

Las fuentes de datos que se pueden utilizar en este tipo de investigación son: 1) encuestas 2) situaciones análogas 3) experimentación y 4) datos secundarios; de ellas se utilizarán tanto la encuesta como los datos secundarios.

La encuesta, es una manera de obtener información por medio de la formulación de preguntas; en este caso esta fuente de datos resulta adecuada ya que la información que se intenta conseguir son datos sobre las percepciones, actitudes y motivaciones que los posibles usuarios tienen respecto a los servicios del Internet prestados al interior de la Institución educativa.

También se utilizarán datos secundarios que es información ya recolectada y publicada para propósitos diferentes a las necesidades específicas de la investigación.

En este estudio, los datos secundarios internos (proporcionados por la misma Institución) utilizados serán las listas de estudiantes matriculados durante los últimos tres años.

La recolección de datos se hará por medio de cuestionarios, que permitirá de algún modo cuantificar las características del mercado. Un cuestionario debe estar correctamente formulado, si se desea encontrar respuestas acordes con la realidad.

Las secciones de una encuesta son:

1. Datos de identificación: se solicitan datos personales de los encuestados como su nombre, dirección, teléfono, ocupación, etc, todo esto según el proyecto en particular.
2. Solicitud de cooperación: es una enunciación abierta diseñada para conseguir la colaboración del encuestado en relación con la entrevista. Generalmente se explica la organización que realiza la entrevista, se indica el propósito del estudio y si existe, un tiempo determinado para la encuesta.

3. Instrucciones: son comentarios para el encuestado sobre cómo usar el cuestionario, instrucciones especiales sobre el uso de preguntas específicas.
4. Información solicitada: son las preguntas planteadas por el investigador.

El diseño del cuestionario es más una habilidad que una tarea científica. No existen pasos, principios o pautas que garanticen un cuestionario eficaz y eficiente. A pesar de esto, se tienen siete pasos que facilitarán el desarrollo de un cuestionario y son:

- Revisar las consideraciones preliminares
- Decidir sobre el contenido de las preguntas
- Decidir sobre el formato de respuestas
- Decidir sobre la redacción de la preguntas
- Decidir sobre la secuencia de la preguntas
- Decidir sobre las características físicas de la encuesta
- Elaborar un borrador, revisarlo y reeditarlo

Se ha decidido para esta encuesta utilizar preguntas de selección múltiple, ya que reducen el tiempo asociado tanto a la recolección de datos, como a su procesamiento.

A continuación se presenta la encuesta formulada para esta investigación de mercado:

OBJETIVO:

Recopilar información sobre el servicio de acceso a Internet y de los requerimientos y expectativas de la comunidad universitaria, respecto al mismo, con el fin de ofrecer una nueva propuesta de servicio.

DATOS PERSONALES:

Carrera en la que estudia _____ Ingeniería ☐

Tecnología ☐

Nivel _____ Edad _____

Sexo: Masculino ( ) Femenino ( )

CUESTIONARIO:

1.- ¿Cuál es el lugar que más utiliza para acceder al Internet?

a) Un cybercafé ☐
b) Mi domicilio ☐
c) Los centros de cómputo de la EPN ☐

2.- Con qué frecuencia visita un centro de cómputo o cybercafé para utilizar Internet?

a) No visito ☐
b) De 1 a 2 veces en la semana ☐
c) De 3 a 4 veces en la semana ☐
d) Menos de 3 veces en la semana ☐

3.-Cuando visita estos lugares qué tiempo aproximado suele navegar por Internet?

a) 0 a 1 hora ☐
b) 1 hora a 2 horas ☐
c) 2 horas a 3 horas ☐
e) Más de 3 horas ☐

4.- La calidad de servicio de Internet en los centros de cómputo o cybercafès que usted ha frecuentado ha sido:

a) Rápida ☐ b) Normal ☐ c) Lenta ☐

5.- Cuál de los siguientes servicios lo motivan a acudir a un lugar que brinde acceso a Internet?

a) Navegación por Internet ☐
b) Correo Electrónico ☐
c) Transferencia de Archivos ☐
d) Uso de computadores ☐
e) Llamadas telefónicas internacionales ☐
f) Otros (especifique) ☐

6.- Cuál considera sería el precio adecuado por una hora de servicio de Internet ?

a) De 0,80 a 1 dólares ☐
b) De 1,01 a 1,20 dólares ☐
c) Más de 1,20 dólares ☐

Sugerencias _____

d. Diseño de la muestra

La muestra utilizada para la encuesta se obtuvo de una población de: 7592 estudiantes de la Institución tal como se muestra en las tablas 3.1, 3.2 y 3.3 , datos proporcionados por la Dirección de Planificación.

El tamaño de la muestra se obtuvo de la siguiente manera:

$$n = \frac{e^2 * p * q * N}{e^2(N-1) + E^2 * p * q}$$

Donde:

n = tamaño de la muestra

e^2 = desviación estándar

N = universo de la muestra

E = estimación de error

p = probabilidad de que el encuestado sea usuario del sistema

q = 1 - p

Se asumen los valores p = 0.5 y q = 0.5 debido a que, el valor de estimación de error es de 0,06 y la desviación estándar se ha considerado 2.

$$n = \frac{4 * 0.5 * 0.5 * N}{0{,}06^2(N-1) + 4 * 0.5 * 0.5}$$

$$n = \frac{N}{0.0036(N-1) + 1}$$

$$n = \frac{7592}{0{,}0036(7592-1) + 1}$$

$$n = 268$$

La muestra escogida para realizar las encuestas para el estudio de mercado corresponde a 268 estudiantes de la Institución.

ESCUELA DE FORMACIÓN EN CIENCIAS		
Fecha	Período	Alumnos
2001-1	1	1137
2001-2	2	1176
2002-1	3	1133
2002-2	4	1371
2003-1	5	1468
2003-2	6	1470
2004-1	7	1555

Tabla 3.1 *Ingreso a la Escuela de Formación de Ciencias en los últimos tres años*[1]

ESCUELA DE FORMACIÓN EN INGENIERÍA		
Fecha	Período	Alumnos
2001-1	1	4409
2001-2	2	4162
2002-1	3	4491
2002-2	4	3971
2003-1	5	4471
2003-2	6	4489
2004-1	7	4483

Tabla 3.2 *Ingreso a la Escuela de Ingeniería en los últimos tres años*[48]

ESCUELA FORMACIÓN TECNOLÓGICA		
Fecha	Período	Alumnos
2001-1	1	1081
2001-2	2	1172
2002-1	3	1172
2002-2	4	1231
2003-1	5	1143
2003-2	6	1157
2004-1	7	1141

Tabla 3.3 *Ingreso a la Escuela de Formación Tecnológica de los últimos tres años* [48]

[1] Información obtenida de la Unidad de Sistemas de Información de la EPN

e. Procesamiento de datos

Las encuestas se han realizado, tomando en cuenta la distribución de los estudiantes a fin de conseguir datos reales de la situación.

Los resultados de las encuestas se tabulan a continuación en las tablas 3.4 a 3.9, mostrando además el porcentaje alcanzada en cada opción:

1. ¿Cuál es el lugar que más utiliza para acceder al Internet?

Un cybercafé	71	26,49 %
Mi domicilio	75	27,98 %
Los centros de cómputo de la EPN	122	45,52 %

Tabla 3.4 *Respuestas a la pregunta 1*

2. ¿Con qué frecuencia visita un centro de cómputo o cybercafé para utilizar Internet?

No visito	42	15.67 %
De 1 a 2 veces en la semana	118	44.02 %
De 3 a 4 veces en la semana	82	30.59 %
Menos de 3 veces en la semana	26	9.70 %

Tabla 3.5 *Respuestas a la pregunta 2*

3. ¿Cuando visita estos lugares que tiempo aproximado suele navegar por Internet?

0 a 1 hora	129	48.13 %
1 hora a 2 horas	130	48.50 %
2 horas a 3 horas	18	6.71 %
más de 3 horas	11	4.10 %

Tabla 3.6 *Respuestas a la pregunta 3*

4. La calidad de servicio de Internet en los centros de cómputo o cybercafès que usted ha frecuentado ha sido:

Rápida	42	15.67 %
Lenta	141	52.61 %
Normal	85	31.71 %

Tabla 3.7 *Respuestas a la pregunta 4*

5. ¿Cuál de los siguientes servicios lo motivan a acudir a un lugar que brinde acceso a Internet?

Navegación por Internet	190	44.7 %
Correo Electrónico	119	28.0 %
Transferencia de Archivos	82	19.3 %
Uso de computadores	27	10.07 %
Llamadas telefónicas internacionales	7	2.61 %
Otros	0	0 %

Tabla 3.8 *Respuestas a la pregunta 5*

6. ¿Cuál considera sería el precio adecuado por una hora de servicio de Internet?

De 0,80 a 1 dólares	226	84.32 %
De 1,01 a 1,20 dólares	11	4.10 %
Más de 1,20 dólares	1	0.37 %
Menos de 0,80 dólares	30	11.19 %

Tabla 3.9 *Respuestas a la pregunta 6*

f. Análisis de datos

En esta sección, se realiza un análisis de los posibles usuarios del servicio, así como la proyección adecuada de la demanda.

1.1.4 USUARIOS DEL SERVICIO

a. Perfil del usuario

Este servicio está dirigido específicamente a toda la comunidad universitaria de la Escuela Politécnica Nacional.

Esta Institución requiere como instrumento de apoyo, el servicio de Internet, correo electrónico, transferencia de archivos, uso de computadores y llamadas telefónicas nacionales e internacionales, para el desarrollo de sus actividades estudiantiles, personales y profesionales.

Se prevé que son los estudiantes quienes en mayor cantidad requieren de los servicios antes mencionados; son jóvenes que la mayor parte del tiempo pasan dentro de la Institución, es por esto que para poder desarrollar sus actividades estudiantiles o extracurriculares necesitan de un excelente servicio tecnológico de acceso a Internet.

b. Segmentación del consumidor

La reunión de consumidores, tomando en consideración que su comportamiento es similar en el acto de la compra se la conoce con el nombre de segmentación.

En este caso el grupo al cual se dirige este proyecto es el estudiantado de la Institución.

3.1.5 ANÁLISIS DE LA DEMANDA

3.1.5.1 Demanda actual e histórica

La demanda se obtiene a través de un proceso de recolección de información, para lo cual se debe tener información completa y veraz acerca del producto o servicio y las necesidades del usuario.

La demanda actual e histórica de este proyecto se obtuvo mediante los registros de la población estudiantil por escuelas, proporcionada por la Dirección de Planificación. Cabe recalcar que en la cuantificación de la demanda no se incluyó

a los alumnos de pre–politécnico y posgrados debido a varias causas las cuales se especifican a continuación:

- Este grupo de alumnos no utiliza el servicio que se propone con tanta periodicidad, como lo hacen los estudiantes de ingeniería y tecnología
- En el grupo de estudiantes de pre-politécnico existe un porcentaje de alumnos que no seguirán perteneciendo a la Institución debido a diversos factores (académicos, laborales, familiares, económicos, etc.) por esto dicho grupo no sería un usuario potencial de este proyecto.
- Los estudiantes de maestrías no utilizarán el servicio brindado por la Intranet, debido a que sus actividades las realizan fuera del horario de servicio propuesto para la red.

La tabla 3.10 presenta en resumen la demanda actual e histórica:

DEMANDA ACTUAL E HISTÓRICA		
Fecha	**Período**	**Total de Alumnos**
2001-1	1	6627
2001-2	2	6510
2002-1	3	6796
2002-2	4	6573
2003-1	5	7082
2003-2	6	7116
2004-1	7	7179

Tabla 3.10 *Demanda actual e histórica de la población estudiantil*

El cuadro anterior muestra el total de alumnos potenciales en el servicio de la Intranet. Se debe considerar en base a la encuesta realizada que cierto porcentaje de estudiantes accede al servicio en lugares externos al Campus Universitario, por lo cual se realizarán ciertos cálculos que reflejen el verdadero número de estudiantes que utilizará la Intranet.

El porcentaje de personas que utiliza los equipos de la EPN es del 45.52%; mientras que las personas que acceden a Internet en los cybercafés alcanzan el 26.49% y el porcentaje de alumnos que utilizan el servicio en sus hogares es de

27.98%. Partiendo de estos valores se obtienen los siguientes resultados (Tabla 3.11)

DEMANDA REAL ACTUAL E HISTÓRICA		
Fecha	Período	Total de Alumnos que acceden a centros cómputo de EPN
2001-1	1	2294
2001-2	2	2290
2002-1	3	3070
2002-2	4	2969
2003-1	5	3199
2003-2	6	3215
2004-1	7	3243

Tabla 3.11 Demanda real a centros de cómputo de la población estudiantil en la EPN

3.1.5.2 Proyección de la demanda

Debido a que existen variaciones heterogéneas en la demanda histórica en cada una de las escuelas de la institución, la proyección de la demanda de estudiantes debe hacerse obligatoriamente de una forma individual, es decir por cada Escuela

Para realizar la proyección de la demanda se pueden utilizar tres métodos diferentes, que se aplicarán según las características particulares de cada caso.

Los métodos son:

- Método del promedio móvil
  Esta técnica asume que la demanda del mercado será con tendencia más o menos constante durante un período de tiempo.

- Método del promedio móvil ponderado
  Esta técnica es una variación del método anterior, y permite aplicar determinada importancia o peso a cada uno de los años, esta asignación hace que las proyecciones sean más sensibles a los cambios recientes conservando las tendencias de estos períodos.
- Método de alisado exponencial simple

Trabaja a partir de una serie de valores históricos, donde las alzas y bajas cíclicas y estacionales pueden "plancharse" en una línea o curva de tendencia mediante el uso de los promedios variables.

- Método de Holt – Winters
  Es una variación compleja del método anterior y sirve para proyecciones de mediano y largo plazo.

Se debe indicar además, que para confirmar la consistencia de los datos obtenidos en la proyección se realiza el análisis de correlación, éste permite determinar que tanto se vinculan entre sí los valores obtenidos. Cabe indicar que este factor puede calcularse utilizando la función del mismo nombre que se halla en Microsoft Excel.

El factor de correlación se halla entre –1 y +1, si el valor es cercano a uno de los extremos del intervalo indica que los puntos obtenidos se encuentran bastante cerca de la recta o están sobre ella, mientras que los valores tendientes a 0 implican una mayor dispersión.

En los párrafos siguientes, se presentarán los resultados de las proyecciones de demanda los cálculos respectivos, se encuentran detallados en el Anexo Q.

La proyección de la demanda se realiza para 8 semestres, pues es un intervalo de tiempo en el que se espera haber recuperado la inversión.

a. Proyección de la demanda para la Escuela de formación en Ciencias

La tabla 3.1 indicó el número de estudiantes ingresados en los últimos períodos lectivos, estos datos servirán como base para realizar los cálculos de proyección para esta escuela de formación.

Para la proyección de la demanda de la Escuela de Ciencias, se utiliza el método de Holt – Winters cuyo factor de correlación es 0.98. Los resultados se muestran en la tabla 3.12

Semestres	PROYECCIÓN DE LA DEMANDA
1	1464.61
2	1522.9
3	1581.19
4	1639.48
5	1697.77
6	1756.06
7	1814.35
8	1872.64

Tabla 3.12 *Proyección de la demanda de la Escuela de Ciencias para un período de cuatro años*

b. Proyección de la Escuela de Ingeniería

La tabla 3.2, muestra el proceso histórico de la población estudiantil de la Escuela de Ingeniería, debido a que estos datos no presentan ninguna secuencia, se decide utilizar el método de los promedios móviles ponderados que arrojan un factor de correlación de 0.97

La tabla 3.13 muestra la demanda proyectada para la Escuela de Ingeniería.

Semestres	PROYECCIÓN DE LA DEMANDA
1	4588
2	4796
3	5004
4	5212
5	5420
6	5628
7	5836
8	6044

Tabla 3.13 *Proyección de la demanda de la Escuela de Ingeniería para un período de cuatro años*

c. Proyección de la Escuela de formación Tecnológica

La tabla 3.3 indicó el número de estudiantes ingresados en los últimos períodos lectivos, para la proyección de la demanda de esta escuela, se utiliza el método de Holt – Winters que arroja un factor de correlación de 0.80 .

Los resultados de la proyección se muestran en la tabla 3.14

Semestres	PROYECCIÓN DE LA DEMANDA
1	1262
2	1272
3	1277
4	1282
5	1286
6	1291
7	1296
8	1301

Tabla 3.14 *Proyección de la demanda de la Escuela de formación Tecnológica para un período de cuatro años*

3.2 ESTUDIO FINANCIERO

El estudio financiero presenta la información relativa a costos de inversión, financiamiento, operación y los ingresos previstos durante el período de vida útil del proyecto.

Se debe hacer una descripción de cada uno de los componentes de inversión: inversiones fijas, y el capital de trabajo para la puesta en marcha del proyecto. Los primeros corresponden a los bienes que el proyecto adquiere orientados a la explotación y otros activos correspondientes a los gastos de capital previos a la producción. El capital de trabajo está referido a los medios requeridos para la

operación del proyecto (gastos de materia prima, sueldos, salarios, etc) cuya recuperación se logra en el momento de percibir ingresos.

Los valores para cada uno de los elementos necesarios para la ejecución del proyecto como son: construcción del local, equipos, mano de obra, etc. se los considera de acuerdo a las proformas obtenidas en el mercado nacional, tomando como criterio el promedio obtenido entre al menos dos cotizaciones.

Se debe indicar que los cálculos financieros, se realizaron utilizando el programa de la Corporación Financiera Nacional (CFN), mismo que se halla en la documentación magnética del presente trabajo.

A continuación, se desglosarán los gastos e inversiones necesarias para la implementación y mantenimiento del presente proyecto.

3.2.1 INVERSIONES

a. Inversiones fijas

Las inversiones fijas se realizan en el período de instalación del proyecto y se utilizan en éste. Estas inversiones comprenden bienes que están sujetos a depreciación, tales como maquinaria, edificios, etc.
En los siguientes párrafos se indican los costos por inversiones fijas, para la implementación de una Intranet en una institución educativa.

Costos de construcción

Este rubro enmarca los gastos correspondientes al diseño, construcción y adecuación del local.

Los costos de construcción se muestran en la tabla 3.15 que resume el presupuesto necesario tanto para la construcción del local como para la adecuación del mismo.

RUBRO	CANTIDAD	UNIDAD	TOTAL ($)
Diseño arquitectónico	1	U	600,00
Estructura	1	U	3015,00
ARENAS			
Arena Negra	16	m^3	790,00
Arena Azul	8	m^3	65,00
CEMENTO			
Cemento Rocafuerte	150	50 Kg	1100,00
BLOQUES			
Bloques	5000	U	1000,00
ENLUCIDOS			
Enlucido de fajas incluye andamios	18	m	70,00
Enlucido vertical incluye andamios. Mortero 1:6, e = 1.5 cm	220	m^2	700,00
Enlucido liso exterior incluye andamios Mortero 1:6 e= 1.5 cm	50	m^2	400,00
Enlucido horizontal incluye andamios	60	m^3	500,00
BALDOSAS			
Baldosas grano gris #2 40x40 fondo gris	48	m^2	457,00
VARIOS			
Puerta plywood 0.70 lacada incluye marcos y tapamarcos	9	U	1080,00
Ventana corrediza de aluminio	44.64	m^2	892,80
ACABADOS			
Sanitarios y grifería			500,00
TOTAL			11169,80

Tabla 3.15 *Costo de construcción y adecuación del local*

Costos de equipos

En las tablas 3.16 y 3.17 se presentan los costos para el equipamiento de la Intranet tanto a nivel de red LAN como los requeridos para el enlace WAN, los datos corresponden a valores promedios del mercado nacional.

Red LAN

El núcleo de la red está constituida por *switches*, como se indicó en el capítulo 2, ya que éstos aseguran la optimización del ancho de banda disponible.

EQUIPO	DESCRIPCIÓN	CANTIDAD	V.UNI($)	TOTAL($)
Switch Cisco Catalyst	24 port, 10/100 Catalyst *Switch*, *Standard Image only*	1	790,00	790,00
Switch 3COM	3Com® *OfficeConnect® Dual Speed Switch* 16 Plus	3	300,00	900,00
UPS	Potencia 1000VA, 120VAC/60Hz	2	235,00	470,00
Computador	Pentium4, procesador 3.06 GHz, mainboard INTEL 800MHz, 560MB en RAM, Disco de 120 GB,monitor 15"	1	1000,00	1000,00
Computador	Pentium4,procesador 2,8 GHz, 256 MB RAM,disco 80 GB *Mainboard* Intel 800MHz	2	850,00	1700,00
Computadores	Pentium4, procesador 2,26GHz,*Mainboard* BIOSTAR, 256MB en RAM,disco 40GHz, monitor 15"	42	500,00	21000,00
Teléfonos	Panasonic	6	20,00	120,00
Visor	Visor para cabinas	2	150,00	300,00
Impresora	Hewlett Packard Laser 1300N	1	380,00	380,00
Impresora	Lexmark	1	110,00	110,00
Scanner	*Scanner* HP	1	100,00	100,00
Fax	Panasonic KX-FHD 351LA	1	180,00	180,00
Webcam	Ultraportatil y conexión a puerto USB	1	50,00	50,00
	SUBTOTAL			27100,00
	12% IVA			3252,00
	TOTAL			30352,00

Tabla 3.16 *Resumen de costos de equipos de la red LAN*

Red WAN

En la tabla 3.17 se presenta una alternativa de inversión en equipos de comunicación para la red WAN y los equipos necesarios para la transmisión de voz sobre IP.

ITEM	EQUIPO	DESCRIPCIÓN	CANT.	V.UNI($)	TOTAL($)
1	*Router* 805	*Router Cisco* 805, 1 *Ethernet*, 1 WAN, 4F/8D	1	790,00	790,00
2	*Yap Max2*	*Yap Max* 2 salidas para teléfono, 1 puerto TCP/IP	1	230,00	230,00
		SUBTOTAL			1020,00
		12% IVA			122,40
		TOTAL			1142,40

Tabla 3.17 *Resumen de costos de equipos para la red WAN*

Costos de instalación

Los gastos de instalación deben incluir todo lo relacionado con la colocación de máquinas y equipo en condiciones de trabajo, es decir, instalaciones eléctricas, iluminación, cableado estructurado, así como mano de obra y otros gastos de montaje.

En la tabla 3.18 se indican los costos para materiales de instalaciones eléctricas y puestas a tierra, necesarios para el diseño y los elementos de iluminación que utilizará el local.

ITEM	DESCRIPCIÓN	CANTIDAD	V.UNI ($)	TOTAL($)
1	Tubo de 1" PVC reforzado	42	2,70	113,40
2	Cajetines de paso	5	0,25	1,25
3	Conectores EMT 1"	15	0,50	7,50
4	Codos PVC 1"	7	0,25	1,75
5	Uniones EMT 1"	30	0,50	15,00
6	Rollos Cable TW12AWG	3	20,00	60,00
7	Rollos Cable THW6AWG	0,5	100,00	50,00
8	Tablero de distribución 8/16	1	25,00	25,00
9	Protecciones Térmicas 6/E	14	3,50	49,00
10	Cajetines rectangulares profundos	90	0,25	22,50
11	Toma doble polar blanco Kit Kora	75	2,00	150,00
12	Interruptor doble blanco Kit Kora	15	3,00	45,00
13	Lámpara fluorescentes 2x32W doble	16	20,00	320,00
14	Lámpara fluorescentes doble	1	12,00	12,00
15	Focos ahorradores 20w	4	2,60	10,40
16	Foco 0/3 color navitar	2	3,00	6,00
17	Varillas *copperweld* (conex. Tierra)	4	6,00	24,00
	SUBTOTAL			912.80
	12% IVA			109.50
	TOTAL			1022.30

Tabla 3.18 *Cuadro de costos de materiales utilizados en instalaciones eléctricas e iluminación*

La tabla 3.19 resume los costos de materiales destinados a la instalación de cableado estructurado, finalmente la tabla 3.20 recopila el costo por mano de obra para los diferentes trabajos de instalación.

CANTIDAD	UNIDAD	DESCRIPCIÓN	V.UNI ($)	TOTAL ($)
46	U	*Patch cord* 1,6 m	0,30	13,80
46	U	*Patch cord* 3,0 m	0,50	23,00
491	m	Cable UTP cat 6 BELDEN	0,20	98,20
49	U	*Plugs* RJ-45 AMP	0,30	14.70
6	U	*Plugs* RJ-8 NEXXT	0,15	0.90
43	m	Cable telefónico	0,12	5,16
55	U	Cajas sobrepuestas 40mm DEXSON	1,50	82,50
55	U	*Face Plates*	0,20	11,00
1	U	*Rack* de piso 2,1 m aluminio negro queso	80,00	80,00
4	U	Organizador horizontal 60*40 tipo canaleta 1UR	12,25	49,00
1	U	Organizador vertical	12,00	12,00
6	U	Bandeja simple 1UR BEAUCOUP	16,25	97,50
4	U	*Patch panel* 24p cat 6 NEXXT	83,75	335,00
7	U	Ductos PVC rígidos 2"	15,00	105,00
13	U	Ductos metálicos	20,00	260,00
		SUBTOTAL		1187,76
		12% IVA		142,53
		TOTAL		1330.29

Tabla 3.19 *Resumen de materiales necesarios para la instalación de cableado estructurado*

ITEM	DESCRIPCIÓN	TOTAL
1	Mano de obra para construcción	1280,00
2	Mano de obra Instalaciones eléctricas	500,00
3	Mano de obra por instalación de cableado estructurado.	1000,00
4	Instalación del enlace para conexión a Internet	450,00
5	Instalación de cabinas telefónicas	85,00
	TOTAL	3315,00

Tabla 3.20 *Resumen de costos de mano de obra*

Costos de mano de obra

Los costos de mano de obra para la construcción del local han sido considerados por el total de la obra, igualmente en lo que respecta a instalaciones eléctricas, conexión a tierra, instalación de cabinas telefónicas y de la línea telefónica.

En lo que respecta a cableado estructurado el costo por mano de obra ha sido cotizado por punto, siendo el valor indicado en la tabla el costo por 50 puntos de cableado estructurado.

Muebles y enseres

Tanto para las salas como para las oficinas de administración y control se requiere de muebles (escritorios, mesas, sillas, etc).

Las tablas 3.21 y 3.22 presentan los muebles necesarios para el normal funcionamiento de la Intranet, los mismos que han sido considerado requerimientos mínimos.

ITEM	DESCRIPCIÓN	CANTIDAD	V.UNI ($)	TOTAL($)
1	Escritorios para computadores	42	20,000	840,00
2	Sillas para usuarios	44	16,00	704,00
3	*Counter* de grafito para control	1	150,00	150,00
4	Estación de trabajo para administración	1	200,00	200,00
5	Sillas ejecutivas	2	60,00	120,00
6	Sillones de espera	1	145,00	145,00
7	Divisiones para Cabinas Telefónicas estructura de hierro	2	250,00	500,00
	SUBTOTAL			2659,00
	12% IVA			319.08
				2978.08

Tabla 3.21 Costos de muebles necesarios para la Intranet

ITEM	DESCRIPCIÓN	CANTIDAD	V. UNI($)	TOTAL ($)
1	Refrigeradora	1	250,00	250,00
2	Licuadora	1	55,00	55,00
3	Cafetera	1	100,00	100,00
4	Microondas	1	80,00	80,00
5	Vajilla	1	30,00	30,00
6	Vitrinas	2	150,00	300,00
	SUBTOTAL			815,00
	12% IVA			97,80
	TOTAL			912,80

Tabla 3.22 Costos de enceres necesarios en bar

Otros equipos

Este rubro incluye aquellos equipos no utilizados directamente en el proceso de administración o producción como son las alarmas, bombas de agua, herramientas, etc. La tabla 3.23 describe estos rubros.

ITEM	DESCRIPCIÓN	CANTIDAD	V.UNI ($)	TOTAL ($)
1	Extinguidor de fuego de C02 12 libras	1	87,00	87,00
2	Alarma	1	1000,00	1000,00
	SUBTOTAL			1087,00
	12% IVA			130.44
	TOTAL			1217.44

Tabla 3.23 Dispositivos complementarios al diseño

b. Gastos de constitución

Se refiere a todos aquellos gastos requeridos por las leyes ecuatoriana para la implementación de una empresa, tales como pagos en notarías, patentes, etc, y el pago de honorarios de abogados.

Los trámites legales para la elaboración de este proyecto dependen directamente de la forma legal que las autoridades de la Institución lo ordenen; el capítulo IV hace mención a todos los asuntos legales que se requiere para efectos de cálculo se establece como gastos de constitución un valor de $ 1000 aclarando que este rubro varía de acuerdo a la figura legal que le otorgue la Institución.

Licencias

El equipo de computación de la Intranet, trabaja bajo el sistema operativo en algunos casos de software libre como es el caso del RED HAT 9.0 que utilizarán los servidores. Windows XP profesional, y Office 2003 de Windows, utilizados por las estaciones de trabajo, son programas que requieren licencias para su utilización cuyos costos de licencia se especifican en la tabla 3.24.

ITEM	DESCRIPCIÓN	CANTIDAD	V.UNIT. ($)	TOTAL ($)
1	Windows XP professional	45	22,00	990,00
2	Office 2003	45	29,70	1336,50
3	SQL	1	500,00	500,00
	TOTAL			2826,50

Tabla 3.24 *Resumen de los costos por licencias para los equipos de la Intranet.*

El costo de licencias propuesto en la tabla 3.24 está bajo la consideración de licencias académicas y que requieren una renovación anual, cabe aclarar que existen otro tipo de licencias cuyo valor es superior al indicado.

c. Imprevistos

Todo estudio financiero, tiene siempre un margen de error debido a fluctuaciones de precios, cambios de las condiciones originales, etc, por lo cual es conveniente incluir un rubro de imprevistos, los cuales se calculan generalmente como un porcentaje de la suma del grupo de inversiones fijas.

Para el caso de estudio se considerará el 1% del monto total.

d. Capital de trabajo

La estimación de las necesidades de capital de trabajo es uno de los aspectos importantes de un proyecto; se llama capital circulante o de trabajo al patrimonio que requieren las organizaciones para atender las operaciones de funcionamiento inicial.

Se debe contar con una reserva de recursos, correspondiente a gastos corrientes y sistemáticos.

Para este proyecto se considera como capital de trabajo los rubros correspondientes a la primera cuota del servicio de acceso a Internet, la adquisición de 3 resmas de papel bond, una caja de CDs y 3 cajas de disquetes, que son suministros necesarios para prestar servicio a los usuarios. La tabla 3.25 presenta un resumen de los costos necesarios para estas adquisiciones.

ITEM	DESCRIPCIÓN	CANTIDAD	V. UNIT [USD]	TOTAL [USD]
1	Acceso a Internet (ancho de banda 128Kbps)	1	896,00	896,00
2	Resmas de papel bond	3	3,00	9,00
3	CDs	1	12,00	12,00
4	Disquetes	3	3,00	9,00
5	Insumos productos para el bar	1	30,00	30,00
	TOTAL			956,00

Tabla 3.25 *Resumen de costos de capital de trabajo sugerido*

Para obtener una clara visión de la inversión necesaria en la implementación de la Intranet, se presenta en la tabla 3.26 un resumen de las inversiones necesarias para la ejecución del proyecto.

Cabe indicar que el proyecto se plantea en fases e inicialmente funcionará con una sala, luego del análisis financiero, se determinará el período de tiempo que deberá transcurrir antes de que se pueda realizar la nueva inversión de equipos para las salas restantes.

Se ha considerado además que el tiempo de vida útil del proyecto es de 10 semestres, que requiere de un período preoperativo de seis meses que es el tiempo que se requiere poner en marcha el proyecto.

PROYECTO INTRANET EPN	
	TOTAL DE INVERSIONES
ACTIVOS FIJOS NETOS	
Terreno	0,00
Construcción del local	11,16
Equipos de LAN	10,11
Equipos WAN	1,14
Sistema eléctrico	1,02
Sistema cableado estructurado	1,32
Muebles	1,82
Enceres	0,91
Alarma y extintores	0,65
Licencias	0,94
SUBTOTAL	29,07
ACTIVOS DIFERIDOS	
Gastos Preoperativos	1,21
Gastos de constitución	1,00
Intereses Preoperativos	0,00
Gastos por instalaciones	3,31
Imprevistos	0,28
SUBTOTAL	5,80
OTROS ACTIVOS	**0,00**
INVERSION TOTAL	**34,87**

Tabla 3.26 *Inversión necesaria para la implementación del proyecto*

Adicionalmente en la tabla 3.27 se indica los costos contemplados para futuras inversiones, en lo que respecta a la ampliación del servicio de vídeoconferencia a una video conferencia grupal y el servicio de *Web Hosting* , servicios que implican un aumento de ancho de banda a un valor mínimo de 256 Kbps, indicando que estos rubros no será incluidos en el presupuesto contemplado para este proyecto, por cuanto, es una inversión proyectada para luego de algunos años.

EQUIPO	DESCRIPCIÓN	CANTIDAD	V.UNI($)	TOTAL($)
FX Quad BRI Module	FX Quad BRI Module for ViewStation FX H.323 or ViewStation H.323	1	690,00	690,00
WiewStation H.323	Polycom ViewSatation H.323, videoconferencing system with up to 768kbps over IP/H323	1	4430,00	4430,00
Televisor	Sony 24 pulgadas	1	500,00	500,00
	SUBTOTAL			5620,00
	12% IVA			674.40
	TOTAL			6294.40

Tabla 3.27 Equipos para videoconferencia grupal

3.2.2 FINANCIAMIENTO DE LAS INVERSIONES

El financiamiento de un proyecto constituye una parte muy importante ya que financiar su inversión, es conceder el crédito necesario para que pueda construirse y funcionar; para ello los socios fundadores deben suscribir una cierta cantidad como capital y en caso de requerirlo solicitar a una entidad financiera otorgue un préstamo, tomando en cuenta que siempre será necesario mantener un equilibrio entre las diferentes fuentes de financiamiento, ya que se debe pagar intereses financieros desde el inicio de las operaciones y puede resultar peligroso para el crecimiento futuro del proyecto.

El financiamiento óptimo del proyecto implica contar con el capital necesario para cubrir el 100% de la inversión, pero si el capital real no suma esta cantidad de dinero se puede plantear como alternativa de financiamiento el acudir a una entidad bancaria o solicitar préstamo a terceros.

Otra alternativa es la de implementar el proyecto por fases, la propuesta para la Intranet es que inicialmente funcione con una sala (15 computadores), luego de recuperada la inversión, se puede invertir en el nuevo equipo y muebles para las 2 salas restantes.

Se considera una inversión del 100% para cálculos de rentabilidad del proyecto.

3.2.3 PRESUPUESTO DE COSTOS Y GASTOS

Los presupuestos del proyecto se fundamentan en la presupuestación de costos, gastos y ventas. Los costos son aquellos pagos realizados por la compra de materiales directos o indirectos y el pago de la nómina de empleados, es decir el pago de todos los recursos que intervienen en la prestación del servicio. Los gastos son aquellos pagos realizados para cancelar actividades que no tienen relación con el servicio, como son gastos administrativos y finalmente, las ventas se refieren a la estimación de ingresos que se obtendrán por el servicio de acuerdo al estudio de mercado.

a. Presupuesto de Costos

En este presupuesto se incluyen todos los costos que implican el prestar el servicio.

Los costos matemáticamente pueden ser expresado mediante la ecuación:

$$C_{Tt} = C_D + C_I$$

Donde:

C_T = Costos totales
C_D = Costos directos
C_I = Costos indirectos

Costos directos

Los costos inherentes en su totalidad a la ejecución del proyecto se los conoce como costos directos, como son sueldos, alquiler del ancho de banda, pago de luz, agua teléfono, etc.

Los costos directos pueden a su vez clasificarse en costos fijos y costos variables. Los primeros son aquellos que permanecen constantes independientemente del nivel de servicio brindado como son: depreciación, mantenimiento, sueldos, etc, y los costos variables son aquellos que cambian de

acuerdo a la demanda de servicio como son: consumo de agua, suministros y consumibles varios.

Costos fijos

Para la Intranet motivo de estudio, se presenta como costos fijos aquellos desembolsos mensuales necesarios para su funcionamiento, los cuales estarán presentes de forma independiente a la demanda, como son: consumo de energía eléctrica, servicio de acceso al Internet, sueldos de los técnicos encargados, el servicio de agua potable y finalmente la depreciación que será considerada para todos los equipos de la red, como son *router*, *switches*, computadores, teléfonos, impresoras, fax, etc.

La depreciación se calcula considerando el valor de la compra del equipo menos un valor residual del 20% del valor inicial a un tiempo de vida útil promedio de 5 años, por ser equipos cuyo desarrollo tecnológico es acelerado; para la depreciación muebles y enceres se toma como tiempo de vida útil 6 años. El valor por depreciación se calcula de acuerdo a la ecuación:

$$D = \frac{V_I - V_R}{V_U}$$

Donde:

V_I = Valor inicial del equipo

V_R = Valor residual del equipo al alcanzar su vida útil

V_U = Vida útil

Para el costo de mantenimiento se deberá destinar un valor entre el 0.5% al 1% del costo total de los equipos.

La tabla 3.28 muestra los costos fijos mensuales necesarios para el normal funcionamiento de la Intranet.

ITEM	CUENTA	COSTO[USD]
1	Tarifa mensual del servicio de Internet	450.00
2	Sueldos de los 1 asistentes técnicos	150.00
3	Sueldo administrativo	270,00
4	Sueldo de limpieza	100,00
5	Consumo de agua potable	20,00
6	Consumo de energía eléctrica	500.00
7	Depreciación	219.00
	TOTAL	1249.00

Tabla 3.28 Costos fijos mensuales de la Intranet

Costos variables

La tabla 3.29 describe los costos variables mensuales de la Intranet cuyos valores son calculados en base a los valores de demanda establecidos en los estudios de mercado. Son considerados como costos variables hojas para el servicio de impresión, disquetes, CDs, etc. cuyo valor es directamente proporcional al nivel de demanda existente.

DESCRIPCIÓN	COSTO	DEMANDA	TOTAL[USD]
Tarjetas Net2phone	0,15	110	16,50
Hojas	0,05	330	16,50
Disquetes	0,30	165	49,50
CDs	0,50	165	82,50
Productos del bar	0,50	330	165,00
TOTAL			330,00

Tabla 3.29 Costos variables mensuales de la Intranet

b. Presupuesto de Gastos

Conocido también como costos indirectos, y hacen mención a los gastos de administración, ventas y financieros que incurrirán en la operación.

En los gastos o costos indirectos para el funcionamiento de la Intranet, se considera los materiales de oficina utilizados y útiles de aseo necesarios.

La tabla 3.30 muestra los gastos o costos indirectos considerados para la Intranet.

ITEM	DESCRIPCIÓN	TOTAL[USD]
1	Materiales de Oficina, esferos, hojas de papel bond, etc.	10,00
2	Suministros de limpieza	20,00
	TOTAL	30,00

Tabla 3.30 Costos indirectos o gastos administrativos

3.2.4 PRESUPUESTO DE VENTAS

Una vez culminada la investigación de mercado, se estima cuál será el volumen de ventas y el precio del producto. Con esta información se puede proyectar el volumen de ingresos.

Para el presupuesto de ventas, se ha considerado únicamente el servicio de Internet porque es el más representativo.

El costo que se ha asignado a la hora de servicio de Internet es de $1,00.

Se ha estimado que se abarcará el 70 % de la demanda insatisfecha, y se asume que la Intranet atenderá todos los días 10 horas de lunes a viernes, en horario de 8h:00 a 18h:00.

En la tabla 3.31 se muestra el porcentaje del mercado al que se espera llegar.

VENTAS DEL PROYECTO Miles de dólares	PRODUCTO Servicio de Internet
% ventas en el mercado local	70,00
% ventas en el mercado local	30,00
% de desperdicios	00,00

Tabla 3.31 Porcentaje de ventas que se espera alcanzar

La tabla 3.32 muestra el número de horas totales que se ofrecerá el servicio de acceso a Internet a partir del segundo período, pues como ya se mencionó el primer período es considerado preoperativo.

INGRESOS PROYECTADOS

Períodos		2	3	4	5	6	7	8
PRODUCTOS								
ACCESO A INTERNET	**UNIDAD**							
Producción neta total	Horas	16800,00	16800,00	16800,00	16800,00	16800,00	16800,00	16800,00
Precios mercado local		1,00	1,00	1,00	1,00	1,00	1,00	1,00
Precios mercado externo		1,00	1,00	1,00	1,00	1,00	1,00	1,00
Ventas mercado local		11,76	11,76	11,76	11,76	11,76	11,76	11,76
Ventas mercado externo		5,04	5,04	5,04	5,04	5,04	5,04	5,04
TOTAL VENTAS	**Miles USD**	16,80	16,80	16,80	16,80	16,80	16,80	16,80
Mercado local		11,80	11,80	11,80	11,80	11,80	11,80	11,80
Mercado externo		5,00	5,00	5,00	5,00	5,00	5,00	5,00
TOTAL ESTIMADO POR VENTAS		**16,80**	**16,80**	**16,80**	**16,80**	**16,80**	**16,80**	**16,80**

Tabla 3.32 Ingresos proyectados[Miles USD]

La producción bruta por período se ha calculado de la siguiente manera:

$$Horas\_semestrales = (No\_máquinas) * (Horas\_diarias) * (días\_mes) * 6meses$$
$$Horas\_semestrales = 14 * 10 * 5 * 4 * 6\_horas$$
$$Horas\_semestrales = 16800\_horas$$

3.2.5 ANÁLISIS DEL PUNTO DE EQUILIBRIO

Examina la relación entre producción, utilidades y costo. También considera cambios en la estructura de precios y costos que pueden contribuir a una mayor rentabilidad.

El punto de equilibrio se interesa principalmente en el análisis de:

1.- Cómo varia el ingreso con cambios en volumen de ventas
2.- Como varían los ingresos con cambios en los costos y precios.

El ingreso neto es igual a los ingresos por ventas menos todos los costos incluyendo depreciación, mano de obra y otros gastos corrientes.

Para obtener el valor del punto de equilibrio es necesario aplicar la siguiente expresión:

$$Pto\_equilibrio = \frac{Costos\_fijos + Gastos\_variales}{Precio\_hora - Costo\_variable - Gastos\_variables\_hora}[horas]$$

La figura 3.1 muestra el gráfico del punto de equilibrio, éste resulta de la intersección entre los costos totales y las ventas, en este caso se consideran que los costos variables no influyen en gran medida por lo tanto el punto de equilibrio se calcula en base a costos fijos.

FLUJO DE CAJA PROYECTADO

	PREOP.	2	3	4	5	6	7	8
A. INGRESOS OPERACIONALES								
Recuperación por ventas	0,00	16,80	16,80	16,80	16,80	16,80	16,80	16,80
Parcial	0,00	16,80	16,80	16,80	16,80	16,80	16,80	16,80
B. EGRESOS OPERACIONALES								
Pago a proveedores	0,00	3,77	3,77	3,77	3,77	3,77	3,77	3,77
Mano de obra directa e imprevistos		1,82	1,82	1,82	1,82	1,82	0,00	0,00
Gastos de administración		2,42	2,42	2,42	2,42	2,42	0,18	0,18
Gastos de fabricación		0,60	0,60	0,60	0,60	0,60	0,60	0,60
ICC (0,8%) y Corpei (1,5/1000)	0,00	0,14	0,14	0,14	0,14	0,14	0,14	0,14
Parcial	0,00	8,75	8,75	8,75	8,75	8,75	4,69	4,69
C. FLUJO OPERACIONAL (A - B)	0,00	8,05	8,05	8,05	8,05	8,05	12,11	12,11
D. INGRESOS NO OPERACIONALES								
Crédito de proveedores de activos fijos	0,00							
Aportes de capital (efectivo subproyecto)	34,87	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Parcial	34,87	0,00	0,00	0,00	0,00	0,00	0,00	0,00
E. EGRESOS NO OPERACIONALES								
Pago de intereses		0,00	0,00	0,00	0,00	0,00	0,00	0,00
Pago de créditos de corto plazo	0,00		0,00	0,00	0,00	0,00	0,00	0,00
Pago participación de trabajadores		0,00	0,77	0,77	0,77	0,77	0,77	1,38
Pago de impuesto a la renta (15%)	0,00	0,00	0,64	0,64	0,64	0,64	0,64	1,16
Reparto de dividendos		0,00	0,00	0,00	0,00	0,00	0,00	0,00
Reposición y nuevas inversiones								
Construcción del local	11,16	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Equipos de LAN	10,11	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Equipos WAN	1,14	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Sistema eléctrico	1,02	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Sistema cableado estructurado	1,32	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Muebles	1,82	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Enceres	0,91	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Alarma y extintores	0,65	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Licencias	0,94	0,00	0,94	0,00	0,94	0,00	0,94	0,00
Activos diferidos	5,80							
Otros activos	0,00							
Parcial	34,87	0,00	2,35	1,41	2,35	1,41	2,35	2,54
F. FLUJO NO OPERACIONAL (D-E)	0,00	0,00	-2,35	-1,41	-2,35	-1,41	-2,35	-2,54
G. FLUJO NETO GENERADO (C+F)	**0,00**	**8,05**	**5,69**	**6,63**	**5,69**	**6,63**	**9,75**	**9,57**
H. SALDO INICIAL DE CAJA	0,00	0,00	8,05	13,74	20,38	26,07	32,70	42,46
I. SALDO FINAL DE CAJA (G+H)	**0,00**	**8,05**	**13,74**	**20,38**	**26,07**	**32,70**	**42,46**	**52,03**

***Tabla** 3.33 Flujo de caja proyectadas para la Intranet [Miles de USD]*

3.2.7 ESTADOS FINACIEROS PROYECTADOS

Con la información de inversiones, ventas, costos y gastos, se puede realizar proyecciones de estados financieros.

COSTOS Y GASTOS PROYECTADOS

PERÍODO:		2	3	4	5	6
COSTOS DIRECTOS DE PRODUCCION						
Mano de obra directa		1,80	1,80	1,80	1,80	1,80
Imprevistos %	1,0%	0,02	0,02	0,02	0,02	0,02
Subtotal		**1,82**	**1,82**	**1,82**	**1,82**	**1,82**
COSTOS INDIRECTOS DE PRODUCCIÓN						
Materiales indirectos		0,00	0,00	0,00	0,00	0,00
Suministros y servicios		6,85	6,85	6,85	6,85	6,85
Mantenimiento y seguros		1,01	1,01	1,01	1,01	1,01
Imprevistos %	1,0%	0,08	0,08	0,08	0,08	0,08
Parcial		7,94	7,94	7,94	7,94	7,94
Depreciaciones		6,59	6,59	6,59	6,59	6,59
Amortizaciones		0,36	0,36	0,36	0,36	0,36
Subtotal		**14,89**	**14,89**	**14,89**	**14,89**	**14,89**
GASTOS DE ADMINISTRACION	% depreciación imputado	80,00	80,00	80,00	80,00	80,00
Gastos que representan desembolso:						
Remuneraciones		2,22	2,22	2,22	2,22	2,22
Materiales de Oficina, esferos, hojas de papel bond, etc.		0,06	0,06	0,06	0,06	0,06
Suministros de limpieza		0,12	0,12	0,12	0,12	0,12
Parcial		2,42	2,42	2,42	2,42	2,42
Gastos que no representan desembolso:						
Amortizaciones		0,22	0,22	0,22	0,22	0,22
Subtotal		**2,65**	**2,65**	**2,65**	**2,65**	**2,65**
GASTOS DE VENTAS	% depreciación imputado	20,00	20,00	20,00	20,00	20,00
Gastos que representan desembolso:						
Comisiones sobre ventas	0,0%	0,00	0,00	0,00	0,00	0,00
Imprevistos	1,0%	0,00	0,00	0,00	0,00	0,00
Parcial		0,00	0,00	0,00	0,00	0,00
Gastos que no representan desembolso:						
Depreciaciones		0,00	0,00	0,00	0,00	0,00
Subtotal		**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
TOTAL		**19,35**	**19,35**	**19,35**	**19,35**	**19,35**

Tabla 3.34 Costos y gastos proyectados [Miles USD]

BALANCE GENERAL E HISTÓRICO PROYECTADO

Miles USD	Saldos iniciales	2	3	4	5	6	7	8	9	10	11
ACTIVO CORRIENTE											
Caja y bancos	0,00	8,05	13,74	20,38	26,07	32,70	42,46	52,03	60,65	70,22	66,00
Inversiones temporales		0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
TOTAL ACTIVOS CORRIENTES	0,00	8,05	13,74	20,38	26,07	32,70	42,46	52,03	60,65	70,22	66,00
ACTIVOS FIJOS											
Construcción del local	11,16	11,16	11,16	11,16	11,16	11,16	11,16	11,16	11,16	11,16	11,16
Equipos de LAN	10,11	10,11	10,11	10,11	10,11	10,11	10,11	10,11	10,11	10,11	10,11
Equipos WAN	1,14	1,14	1,14	1,14	1,14	1,14	1,14	1,14	1,14	1,14	1,14
Sistema eléctrico	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02
Sistema cableado estructurado	1,32	1,32	1,32	1,32	1,32	1,32	1,32	1,32	1,32	1,32	1,32
Muebles	1,82	1,82	1,82	1,82	1,82	1,82	1,82	1,82	1,82	1,82	1,82
Enceres	0,91	0,91	0,91	0,91	0,91	0,91	0,91	0,91	0,91	0,91	0,91
Alarma y extintores	0,65	0,65	0,65	0,65	0,65	0,65	0,65	0,65	0,65	0,65	0,65
Licencias	0,94	0,94	0,94	0,94	0,94	0,94	0,94	0,94	0,94	0,94	0,94
Subtotal activos fijos	29,07	29,07	29,07	29,07	29,07	29,07	29,07	29,07	29,07	29,07	29,07
(-) depreciaciones		2,44	3,94	6,39	7,89	10,33	11,83	14,28	15,78	18,22	19,72
TOTAL ACTIVOS FIJOS NETOS	29,07	26,63	25,13	22,69	21,18	18,74	17,24	14,80	13,29	10,85	9,35

ACTIVO DIFERIDO	5,80	5,80	5,80	5,80	5,80	5,80	5,80	5,80	5,80	5,80	5,80
Amortización acumulada		0,58	1,16	1,74	2,32	2,90	3,48	4,06	4,64	5,22	5,80
TOTAL ACTIVO DIFERIDO NETO	5,80	5,22	4,64	4,06	3,48	2,90	2,32	1,74	1,16	0,58	-0,00
TOTAL DE ACTIVOS	**34,87**	**39,89**	**43,51**	**47,12**	**50,73**	**54,34**	**62,02**	**68,56**	**75,11**	**81,65**	**75,35**
TOTAL DE PASIVOS CORRIENTES	0,00	1,41	1,41	1,41	1,41	1,41	2,54	2,54	2,54	2,54	-0,00
TOTAL DE PASIVOS	**0,00**	**1,41**	**1,41**	**1,41**	**1,41**	**1,41**	**2,54**	**2,54**	**2,54**	**2,54**	**-0,00**
PATRIMONIO											
Capital social pagado	34,87	34,87	34,87	34,87	34,87	34,87	34,87	34,87	34,87	34,87	34,87
Reserva legal	0,00	0,00	0,36	0,72	1,08	1,44	1,81	2,46	3,12	3,77	4,42
TOTAL PATRIMONIO	**34,87**	**38,48**	**42,09**	**45,71**	**49,32**	**52,93**	**59,48**	**66,02**	**72,57**	**79,11**	**75,35**
TOTAL PASIVO Y PATRIMONIO	**34,87**	**39,89**	**43,51**	**47,12**	**50,73**	**54,34**	**62,02**	**68,56**	**75,11**	**81,65**	**75,35**

Tabla 3.35 Balance general proyectado[en MILES DE DÓLARES]

Los dos estados financieros básicos que se deben hacer, se los muestra a continuación y se los ha realizado considerando una inversión del 100% con capital originado por el aporte de los promotores del proyecto, para un período contable de un año.

a. Estado de resultados proyectados

Incluye los ingresos, costos y gastos contables que se prevé tendrá el proyecto, para una año. Esta información se la obtiene del presupuesto de ventas, costos y gastos.

En la tabla 3.34 se muestra el estado proyectado de costos y gastos de la Intranet.

b. Balance general proyectado

Este estado financiero permite observar cómo quedará la empresa al finalizar cada año. Por lo tanto, es aconsejable realizarlo al finalizar la proyección de cada año y debe incluir todos los recursos, obligaciones y patrimonio de la empresa, es decir, el activo, pasivo y patrimonio, para un período contable de un año.

El balance general proyectado, se muestra en la tabla 3.35

3.3 EVALUACIÓN FINANANCIERA DEL PROYECTO

Evaluar el proyecto es medir el grado de rendimiento de los recursos financieros en la implementación de una unidad de servicios.

3.3.1 PERÍODO DE RECUPERACIÓN DE CAPITAL (TR)

Es el método más usado, se lo define como el espacio de tiempo necesario, para que el flujo de efectivo recibido iguale los desembolsos de efectivo realizados en la inversión.

Es la razón de la inversión fija inicial sobre los flujos de ingresos efectivos anuales, como hace referencia la ecuación siguiente:

$$TR = \frac{Io}{R}$$

Donde:

Io = Inversión inicial
R = Flujo de caja anual

Para el presente proyecto, se ha calculado que el tiempo de recuperación de la inversión es de aproximadamente 5 semestres y medio, este dato se muestra en la tabla 3.36

3.3.2 VALOR PRESENTE NETO (VAN)

Implica obtener en valor presente, es decir al año 0 los equivalentes de los flujos producidos por el negocio. Con el método del valor presente, todos los flujos de caja se descuentan del valor presente, utilizando la tasa de rendimiento requerida. Si el valor de estos flujos de efectivo descontados es cero o más, se acepta la propuesta.

$$VAN = -I_O + \sum VA_{(flujos\_efectivos)} * K$$

Donde:

Io = Inversión inicial
VA (flujos de efectivo) = Flujos de caja anual al valor presente
K = Tasa requerida de rendimiento

El valor del VAN para el presente proyecto es de 6550 dólares semestrales y se muestra en la tabla 3.36

ÍNDICES FINANCIEROS

Período	*2*	*3*	*4*	*Promedio*
Composición de activos				
Activo corriente/activos totales	20,2%	31,6%	43,2%	31,7%
Activo fijo/activos totales	66,8%	57,8%	48,1%	57,5%
Activo diferido/activos totales	13,1%	10,7%	8,6%	10,8%
Apalancamiento				
Pasivos totales/activos totales	3,5%	3,2%	3,0%	3,3%
Pasivos corrientes/activos totales	3,5%	3,2%	3,0%	3,3%
Patrimonio/activos totales	96,5%	96,8%	97,0%	96,7%
Composición de costos y gastos				
Costos directos/costos y gastos totales	15,6%	15,6%	15,6%	15,6%
Costos indirectos/costos y gastos totales	61,6%	61,6%	61,6%	61,6%
Gastos administrativos/costos y gastos totales	22,7%	22,7%	22,7%	22,7%
Gastos de ventas/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Gastos financieros/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Costo de ventas/costos y gastos totales	77,3%	77,3%	77,3%	77,3%
Costo materia prima/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Costo materiales indirectos/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Costo suministros y servicios/costos y gastos totales	32,4%	32,4%	32,4%	32,4%
Costo mano obra directa/costos y gastos totales	15,5%	15,5%	15,5%	15,5%
Costo mano obra indirecta/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Gastos personal administ./costos y gastos totales	19,1%	19,1%	19,1%	19,1%
Gastos personal ventas/costos y gastos totales	0,0%	0,0%	0,0%	0,0%
Total remuneraciones/costos y gastos totales	34,6%	34,6%	34,6%	34,6%

Liquidez	Miles USD			
Flujo operacional	8,0	8,0	8,0	8,0
Flujo no operacional	0,0	(2,4)	(1,4)	(1,3)
Flujo neto generado	8,0	5,7	6,6	6,8
Saldo final de caja	8,0	13,7	20,4	14,1
Requerimientos de recursos frescos	0,0	0,0	0,0	0,0
Capital de trabajo	6,6	12,3	19,0	12,6
Indice de liquidez (prueba ácida)	5,7	9,7	14,4	10,0
Indice de solvencia	5,7	9,7	14,4	10,0

Retorno				
Tasa interna de retorno financiera (TIRF)	16,25%	6,5	2,2	
Tasa interna de retorno del inversionista (TIRI)	16,25%			
Valor actual neto (VAN)	6,51	Miles USD		
Período de recuperación	5,22	SEMESTR		
Coeficiente beneficio/costo	2,24			
Utilidad neta/patrimonio (ROE)	9,39%	8,58%	7,90%	8,62%

Utilidad neta/activos totales (ROA)	9,05%	8,30%	7,67%	8,34%
Utilidad neta/ventas	21,50%	21,50%	21,50%	21,50%
Punto de equilibrio	53,93%	53,93%	53,93%	53,93%
Cobertura de intereses	0,0	0,0	0,0	0,0

Sociales				Miles USD
Sueldos y salarios	4,02	4,02	4,02	4,02
Valor agregado	9,19	9,19	9,19	9,19
Generación de divisas	5,04	5,04	5,04	5,04

Costo de oportunidad	6,0%	SEMESTRE

Tabla 3.36 *Reporte de índices financieros*

3.3.3 TASA INTERNA DE RETORNO (TIR)

Llamada también tasa de rendimiento, es la tasa de descuento que hace que el valor actual de los flujos producidos en el tiempo sea igual a los flujos de inversión. El criterio de aceptación que se emplea consiste en comparar la tasa interna de rendimiento con la tasa de rendimiento requerida. Si la primera excede de la tasa requerida, se acepta el proyecto.

$$I_O + 5\sum_{1}\left[\frac{Fi}{(1+TIR)^i}\right] = 0$$

Donde:

Io = Inversión inicial
F = Flujos de efectivo
TIR = Tasa interna de retorno
I = Período en años

El valor del TIR para el presente proyecto es del 16,25% semestrales y se muestra en la tabla 3.36

CAPÍTULO IV

ESTUDIO LEGAL DE LA INTRANET

ESTUDIO LEGAL DE LA INTRANET

Este capítulo hace una recopilación de los diferentes aspectos legales que regirán tanto la implementación como el normal funcionamiento de la Intranet.

La parte legal a la que se sujetará el proyecto enfoca dos aspectos importantes:

- El marco legal establecido por los organismos reguladores de las telecomunicaciones, a los que estará sujeta la Intranet.
- La figura legal establecida por la Institución bajo la cual se llevará a cabo la implementación de la Intranet.

Finalmente se considera para este capítulo, los trámites varios necesarios que deberán realizarse, como son: agua potable y luz eléctrica.

4.1 PERMISOS LEGALES

La Intranet propuesta en este proyecto cuenta con beneficios orientados al servicio de la comunidad universitaria, es por ello que es necesario contar con el registro del SENATEL, en la categoría Centros de información y acceso a la red de Internet.

La Resolución 399-18-CONATEL-2002, dispone el registro de los Centros de información con acceso a la red de Internet, y establece una serie de requisitos a cumplirse los cuales, amparan excepciones y casos adicionales, el registro de estos centros está a cargo de la Secretaría Nacional de Telecomunicaciones, y para la inscripción de los centros, los interesados deben seguir los siguientes pasos:

1. Obtener el formulario de solicitud de Registro del centro
2. Llenar el formulario de solicitud de Registro

3. Adjuntar al formulario todos los documentos indicados como anexos
4. Acercarse personalmente a las oficinas de la SENATEL en las ciudades de Quito, Guayaquil o Cuenca con la documentación completa y cancelar los valores correspondientes.

De acuerdo con el reglamento los documentos a adjuntarse a la solicitud de inscripción son:

- Solicitud dirigida al señor Secretario Nacional de Telecomunicaciones (según formato).
- Copia de la escritura de constitución de la empresa, o de su domiciliación en el país, en caso de empresas extranjeras.
- Copia del nombramiento del Representante Legal, debidamente inscrito en el Registro Mercantil.
- Copia del RUC.
- Copia de la cédula de identidad y papeleta de votación del representante legal.
- Número de terminales o computadoras dedicadas al servicio.
- Copia del contrato con el respectivo proveedor de Internet (ISP).

Una vez presentada la documentación y previo el análisis respectivo, la Secretaría Nacional de Telecomunicaciones procederá al registro de las personas naturales o jurídicas y a la emisión del certificado de registro que será entregado al interesado.

El certificado de registro tiene una duración de un año y podrá ser renovado previo el pago de los derechos correspondientes y la actualización de la información requerida.

Los valores a cancelarse por concepto de derechos para los centros de Información y acceso a la red de Internet con más de dos terminales cancelan

$ 100 por concepto de emisión del certificado y $ 300 por concepto de derechos de registro es decir un total de $ 400 anuales.

Estos centros de información y acceso a Internet, tienen la opción de acogerse al plan Internet para todos, mismo que exonera del pago de los rubros antes mencionados, pero bajo el compromiso de brindar servicio de acceso a Internet gratuito durante cuatro horas del día y en un total del 40% de las máquinas destinadas a este servicio.

El formulario que deberá presentarse para el registro y la resolución 399-18-CONATEL-2002 se adjunta en el Anexo S.

4.2 LICENCIAS DE SOFTWARE

Las estaciones de trabajo de la Intranet, utilizarán diferentes programas y sistemas operativos, en el caso de los servidores, éstos trabajan con software libre bajo el ambiente de Linux con licencia GNU (licencia pública general). En el caso de los terminales de usuario, que se manejan con sistema operativo Windows y el Office de la Microsoft, necesitan contar con las licencias de operación respectivas, los valores de estas licencias se indicaron en el capítulo III.

La licencia pública GNU, especifica explícitamente que el software desarrollado es libre, y nadie puede coartar estas libertades. Es permitido revender este software, incluso con algún beneficio; sin embargo, en esta reventa el vendedor debe proveer el código fuente completo, incluyendo cualquier cambio que haya realizado.

4.3 LEGISLACIÓN PARA VOZ SOBRE IP

Al momento de realizar este proyecto de titulación, el Ecuador aún no cuenta con un reglamento para la regulación de voz sobre IP, sin embargo, el SENATEL encargado de la regulación y normatividad del sector de las telecomunicaciones,

tiene a cargo de la Dirección de Servicios al Público, el proceso de elaboración de la norma regulatoria para la certificación de la Conectividad IP.

Está norma definirá los procedimientos, protocolos de prueba y verificación, instrumentos y perfil de los técnicos certificados que deberían disponer las empresas que pueden ser merecedoras de la acreditación por parte del SENATEL. Esto permitirá certificar a las diferentes compañías a fin de que el usuario pueda oficializar sus reclamos correspondientes de considerar necesario, cuando un servicio de conectividad IP no esté siendo brindado con los parámetros de calidad establecidos en el contrato.

En los días previos a la entrega de este proyecto, la Procuraduría General del Estado, el CONATEL y la SENATEL reconocieron que el servicio de voz sobre IP no está contra la ley.

El CONATEL, la SENATEL y la Procuraduría General reconocieron la legalidad del servicio de voz sobre IP (VoIP) y ahora las dos partes discuten una normativa para regular la calidad de la Internet, que se traduciría en la Ley de Telecomunicaciones e Internet.

Los problemas para los proveedores del VoIP comenzaron cuando las autoridades de telecomunicaciones se opusieron a que existan centros que ofrezcan el servicio de llamadas internacionales por Internet, con el argumento de que sólo las operadoras de servicios finales (Andinatel y Pacifictel) podían hacerlo. Además, querían que los proveedores de Internet aportaran el 1% de sus ganancias al Fondo Nacional de Telecomunicaciones (Fodetel).

Mientras los proveedores de VoIP sostenían que este es un "servicio agregado" de Internet y que en el país no hay una ley que la regule, por lo que pidieron la comparecencia de las autoridades de Telecomunicaciones al Congreso Nacional.

En el Congreso, los representantes del CONATEL y el SENATEL reconocieron que la Internet no es un servicio público, es decir, no es obligación del Estado

proveer el servicio, por lo que el Gobierno no puede dictar reglamentos para regular su uso o distribución, solo puede normar sobre su calidad.

4.4 TRÁMITES LEGALES INSTITUCIONALES

Por tratarse de un monto de inversión que sobrepasa los 40000 dólares, la ejecución del proyecto de acuerdo al estatuto y reglamentos que rigen la universidad, es necesario presentar a Consejo Politécnico la propuesta de proyecto indicando el presupuesto requerido para su construcción, este organismo analizará la viabilidad de su ejecución, bajo dos figuras legales:

1. Intervención directa de la Universidad, lo que implica una inversión al 100% de la Institución, siendo necesario verificar disponibilidad presupuestaria o en su defecto formas de financiamiento para obtener los fondos necesarios, que serán incluidos en el presupuesto del siguiente año, debido a que no se podrían realizar modificaciones de este monto al presupuesto en curso.

De ser éste el caso, Consejo Politécnico delegará una persona o personas responsables de la organización y ejecución del mismo, de acuerdo al alcance establecido y enmarcado en parámetros legales señalados por Consejo Politécnico.

Por cuestiones de agilidad y simplicidad de administración será recomendable se autorice el control y vigilancia a la Dirección de Proyectos de la Institución.

Bajo este marco legal, el personal necesario será contratado directamente por la Universidad y las adquisiciones de equipos, muebles, etc. cumplirán con el respectivo reglamento para el llamado a concurso de ofertas, para lo cual será conveniente hacer el llamado por categorías de acuerdo a las necesidades que vaya presentando el proyecto; estos concursos serán clasificados según sus características, magnitud y costo, con el fin de elaborar bases reales para cada

concurso de ofertas, tendientes a proporcionar una acertada selección de los oferentes.

Dentro de los diferentes concursos que deberán realizarse para la contratación de servicios, adquisición de bienes y la construcción de la infraestructura necesaria para la implementación del proyecto se tienen:

- Concurso para la ejecución de infraestructura del local; el cual deberá contemplar la infraestructura física, los acabados del local e instalaciones eléctricas, el cual será llevado a cabo de acuerdo a los planos presentados en este proyecto.
- Concurso para el diseño de cableado estructurado de la red.
- Concurso para la adquisición de equipos de red, como son *router, switches*, computadores, UPSs, etc. los cuales deberán contener los programas y las respectivas licencias de funcionamiento.
- Concurso la provisión de muebles necesarios para el funcionamiento del proyecto.
- La contratación del servicio a Internet, el cual deberá considerar los diferentes acuerdos de calidad de servicio indicados en el capítulo II. Basado en el análisis realizado por este proyecto en el mismo capítulo, se propone la contratación del servicio de Internet a Telconet, aclarando que es decisión de las autoridades encargada de la ejecución del proyecto el acoger o no está propuesta.

Es necesario mencionar que, para cada caso se deberá nombrar una comisión responsable de llamar al concurso, elaborar las bases, cuyos parámetros técnicos se describieron en el segundo capítulo de este proyecto de titulación, calificar las propuestas concursantes y escoger la propuesta ganadora, que por ser esta una gran responsabilidad se deberá incluir en cada comisión

personas con conocimientos técnicos de acuerdo al caso, de tal manera de establecer sólidos criterios de selección.

Todos los procesos anteriormente anotados, deberán enmarcarse en los reglamentos adoptados por la Institución y la Ley de Contratación Pública del Ecuador.

En caso de autorizarse la administración del proyecto a la Dirección Administrativa de Proyectos de la institución, la construcción de obras, la adquisición de bienes se efectuará de acuerdo al Normativo para el apoyo a la presentación y administración de los proyectos y trabajos de extensión de la Escuela Politécnica Nacional, el cual se lo describe en el Anexo T.

2. El proyecto se podrá realizar, otorgando los derechos a terceros bajo concesión para lo cual se presentará la propuesta a la Dirección Administrativa de la Institución, misma que se encargará de llevar a cabo el concurso de oferentes para la concesión, estableciendo bases, y tiempos para la calificación de ofertas y la elección de la empresa ganadora. Este procedimiento se lo llevará a cabo tomando como base la Ley de contratación pública del Ecuador que establece, las siguientes modalidades para el llamado a concurso de oferentes:

   - Concurso privado
   - Concurso público

Dependiendo del caso la Dirección Administrativa hará el llamado a concurso público o privado de acuerdo al monto, valor que se indican en la tabla 4.1

FECHAS	PRESUPUESTO INICIAL DEL ESTADO (PIE)	CONCURSO	
		PUBLICO	PRIVADO
Enero /2003	6.701.298.620,72	268.051,94	67.012,99
Enero /2004	6.950.837.468,61	278.033,50	69.508,37

Tabla 4.1 *Montos establecidos por la ley de contratación pública del Ecuador para el llamado a concurso de oferentes*

Para el caso del concurso público de ofertas, será necesaria publicar la convocatoria por tres días consecutivos en dos periódicos de mayor circulación nacional, editados en dos ciudades diferentes

Una vez establecida la oferta ganadora la Dirección Administrativa con ayuda del departamento legal, serán los responsables de la elaboración del contrato de concesión el cual contemplará parámetros como: tiempo de concesión, porcentaje de utilidades que se entregará a la Institución, parámetros para la terminación del contrato, etc. Es recomendable especificar si se utilizará los servicios básicos como son agua y luz de la institución y como se cancelará este consumo, o en su defecto si el concesionario requiere hacer la solicitud de estos servicios directamente a las empresas pertinentes.

4.5 TRÁMITES PARA SERVICIOS BÁSICOS

En caso de realizarse el proyecto a través de una concesión como se dijo en la sección anterior, será necesario establecer cómo se deberá resolver el consumo de los servicios básicos, en caso del concesionario requiera hacer estos trámites individualmente, los pasos que deberá seguir son los siguientes:

4.5.1 AGUA POTABLE

El procedimiento a seguir para la solicitud de un medidor de agua potable es:

1. Solicitar el formulario de solicitud de servicio de agua potable y llenar la información solicitada por el EMAAP-Q.
2. Acudir al edificio principal del EMAAP-Q ubicado en la Av. Mariana de Jesús y presentar la solicitud en los módulos diez u once de CATASTROS, para obtener la asignación del código de localización.
3. Dirigirse al módulo 12 de CONTRATOS, para el ingreso y asignación del número de solicitud.
4. Con el número de solicitud, se deberá acercar a la ventanilla 9 del edificio principal a cancelar el respectivo pago por la solicitud y recibir el contrato del servicio solicitado.

Todos estos trámites se los realiza de forma personal o por delegación notariada concedida por el propietario.

Los requisitos que se adjuntarán a la solicitud son:

- Copia de la cédula de identidad o el RUC del propietario y solicitante.
- Presentar papeleta de votación actualizada
- Escritura notariada de la propiedad.

Por tratarse de una escritura de concesión es necesario presentar una solicitud al jefe del departamento de ingeniería del EMAAP-Q, exponiendo las condiciones con las que se realizaron la concesión del inmueble. El departamento de ingeniería analiza estas condiciones y ordena la inspección del lugar asignado, con este documento se deberá seguir el procedimiento mencionado en los párrafos anteriores.

La solicitud que deberá llenarse para la presentación de la solicitud del servicio de agua potable se adjunta en el Anexo S.

4.5.2 SERVICIO DE ENERGÍA ELÉCTRICA (EMPRESA ELÉCTRICA QUITO)

Los pasos a seguir para adquirir un medidor de energía eléctrica son los que se describen a continuación:

1. Acudir al edificio de la EEQ ubicado en la Av. 10 de Agosto y Mariana de Jesús o a la agencia de esta institución más cercana.

   Se debe llevar:

   - Cédula de Identidad
   - Las escrituras del inmueble en caso de ser propietario, caso contrario se debe acudir con una autorización otorgada por el dueño del lugar, haciendo referencia a que se permite la colocación del contador de energía

2. Llevar un estudio de carga y demanda avalizado con la firma de un Ing. Eléctrico o Electrónico colegiado

3. Esperar la inspección que determinará:
    - Si existe lugar para otro contador en el tablero de medidores
    - Si es posible otorgar el servicio requerido, desde un transformador existente cercano (ubicado como público o de la cámara de transformación)

4. En el mejor de los casos, es decir, que aún exista capacidad en el transformador, el inspector dará las instrucciones respectivas, aprobada la solicitud se procederá a pagar a la EEQ los derechos y garantías para la colocación del medidor.

4.6 CONSTITUCIÓN DE UNA COMPAÑÍA

Para la constitución de una compañía existen cinco especies de compañías reconocidas por el estado ecuatoriano que son:

- Compañía de nombre colectivo
- Compañía en comandita simple y divida por acciones
- Compañía de responsabilidad limitada
- Compañía anónima
- Compañía de economía mixta

a. Compañía de nombre colectivo

"Se contrae entre dos o más persona que hacen el comercio bajo una razón social". [20]

En esta compañía sólo los nombres de los socios pueden formar parte de la razón social. El capital de la compañía en nombre colectivo se compone de los aportes que cada uno de los socios entrega.

Para la constitución de la compañía será necesario el pago de no menos del cincuenta por ciento del capital suscrito.

b. Compañía en comandita simple y dividida por acciones

Existe bajo una razón social y se contrae entre uno o varios socios solidarios e ilimitadamente responsables y otros que son simples suministradores de fondos, llamados socios comanditarios, cuya responsabilidad se limita al monto de sus aportes.

La razón social será necesariamente el nombre de uno o varios de los socios solidariamente responsables, al que se agrega siempre las palabras "compañía en comandita", escrita con todas sus letras o la abreviatura que comúnmente suele usarse.

El socio comanditario no podrá ceder ni traspasar a otras personas sus derechos en la compañía ni sus aportaciones, sin el consentimiento de los demás, en cuyo caso se procederá a la suscripción de una nueva escritura social.

c. Compañía de responsabilidad limitada

Es la que se contrae entre tres o más personas que solamente responde por las obligaciones sociales hasta el monto de sus aportaciones individuales y hacen el comercio bajo una razón social o denominación objetiva, a la que se añadirá en todo caso las palabras "Compañía Limitada", o su correspondiente abreviatura.

El capital de esta compañía estará formado por las aportaciones de los socios y no será inferior al monto fijado por la Superintendente de Compañías. Estará dividido en participaciones expresadas en la forma que señale el Superintendente de Compañías.

Al constituirse la compañía, el capital estará íntegramente suscrito y pagado por lo menos en el cincuenta por ciento de cada participación. Las aportaciones pueden ser en especies y pueden consistir en bienes muebles o inmuebles que correspondan a la actividad de la compañía. El saldo del capital deberá integrarse en un plazo no mayor de doce meses a contarse desde la fecha de constitución de la compañía.

d. Compañía anónima

Es una sociedad cuyo capital es dividido en acciones negociables, está formada por el aporte de sus accionistas que responden únicamente por el monto de sus acciones.

La compañía podrá establecerse con el capital autorizado que determine la escritura de constitución. La compañía podrá aceptar suscripciones y emitir acciones hasta el monto de ese capital. Al momento de constituirse la compañía, el capital suscrito y pagado mínimo será el establecido por resolución de carácter general que expida la Superintendencia de Compañías.

Todo aumento de capital será autorizado por la junta general de accionistas y luego de cumplidas las formalidades pertinentes, se inscribirá en el registro mercantil correspondiente

e. Compañía de economía mixta

Corresponde a las empresas dedicadas al desarrollo y fomento de la agricultura y de las industrias convenientes a la economía nacional y a la satisfacción de necesidades de orden colectivo, a la prestación de nuevos servicios públicos o al mejoramiento de los ya establecidos.

De acuerdo al servicio que brindará la Intranet, se puede optar por una compañía en comandita por acciones, de responsabilidad limitada o anónima, debido a que las compañías de nombre colectivo ya no están en vigencia y las de economía mixta son empresas que forman parte del Estado Ecuatoriano.

4.6.1 REQUISITOS PARA EL REGISTRO DE LA COMPAÑÍA EN LA SUPERINTENDENCIA DE COMPAÑÍAS

a. Nombre

Las compañías deben coexistir en una razón social, una denominación objetiva o de fantasía, la cual deberá ser aprobado por la Secretaría General de la Oficina Matriz de la Superintendencia de Compañías.

b. Solicitud de aprobación

Presentar al Superintendente de Compañías tres copias certificadas de la escritura de constitución de la compañía, a las que se adjuntará la solicitud suscrita por el abogado, con la que se pide la aprobación del contrato constitutivo.

c. Número mínimo y máximo de socios o accionistas

De acuerdo a la razón social de la compañía deberá establecerse el número de accionistas o socios para la compañía (tabla 4.2).

COMPAÑÍA	NÚMERO MÍNIMO DE SOCIOS O ACCIONISTAS	NÚMERO MÁXIMO DE SOCIOS O ACCIONISTAS
En comandita simple por acciones	2 accionistas	-------
Responsabilidad limitada	3 socios	15 socios
Sociedad anónima	2 accionistas	--------

Tabla 4.2 *Número de socios o accionistas para la constitución de las compañías*

d. Capital mínimo

El capital mínimo suscrito por la compañía deberá ser de acuerdo a la razón social de la compañía cuyos valores mínimos se especifican en la tabla 4.3 El capital deberá subscribirse y deberá pagarse con al menos el porcentaje mínimo de acuerdo a la compañía (tabla 4.3) del valor nominal de cada participación. Las aportaciones pueden consistir en dinero o especies, bienes muebles o inmuebles.

COMPAÑÍA	CAPITAL MÍNIMO	% MÍNIMO DE CAPITAL A PAGARSE
En comandita simple por acciones	800 dólares de los Estados Unidos de América	25%
Compañía limitada	400 dólares de los Estados Unidos de América	50%
Sociedad anónima	800 dólares de los Estados Unidos de América	25%

Tabla 4.3 *Valores mínimos a cancelarse para la constitución de las compañías*

Una vez elegida la razón social con la que se va a constituir la compañía, se requiere realizar los siguientes trámites:

1. Depositar en una entidad bancaria al menos la cuarta parte del capital social de la compañía.
2. Designar el administrador que tenga la representación legal de la empresa e inscribir su nombramiento con la razón de su aceptación, en el Registro Mercantil dentro de los 30 días posteriores de su aceptación.
3. Con la ayuda de un abogado redactar la escritura de constitución de la compañía, en la que se especificarán: el domicilio, nombre y razón social de la misma, nombres y porcentaje de aportación de los accionista, especificando si ésta es en numerario o especies y finalmente los estatutos que la regirán. Este documento debe ser notariado.
4. Solicitar el registro de la compañía mediante un escrito dirigido al Superintendente de Compañías.
5. La Superintendencia de Compañías revisa la razón social de la compañía y verifica la no existencia de algún registro con el mismo nombre.
6. Una vez registrada se procederá a la afiliación en la cámara de producción correspondiente, previa cancelación de los valores correspondientes (tabla 4.3).
7. Con el documento de afiliación a la cámara, se cancelan los impuestos correspondientes al SRI[1] a fin de obtener el número de RUC[2] y la patente otorgada por el Municipio de Quito.
8. Inscribir la escritura de constitución de la compañía en el Registro Mercantil.
9. Finalmente, una vez aprobada e inscrita la compañía en el Registro Mercantil, se debe publicar el extracto de la escritura de constitución en uno de los periódicos de mayor circulación del país, por tres días consecutivos.

[1] SRI: Servicio de Rentas Internas
[2] RUC: Registro Único de Contribuyentes

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

- Un correcto dimensionamiento de los equipos y del enlace WAN de la red, debe basarse en estudios de tráfico cuyos resultados deben ser lo más cercanos a la realidad.

- Se debe concentrar los equipos importantes de la red en un solo espacio físico, pues esto ayuda a una mejor administración y contribuye a la seguridad física de dichos dispositivos.

- La velocidad de acceso a Internet no solo depende del tiempo de respuesta del enlace de última milla, sino también, y de forma directa de las características de servicio ofrecidas por el ISP, que a su vez depende de la capacidad y redundancia de sus enlaces de *backbone*, a la troncal de Internet.

- Existen ISPs, que no cuentan con personal técnico en el departamento de atención al cliente, por esta razón no están en la posibilidad de orientar al cliente para elegir una alternativa de servicio que satisfaga sus requerimientos.

- El servicio ofertado por la mayor parte de los ISPs, no brindan suficientes garantías para el cliente, en vista de esta situación la SENATEL, se halla en la fase preliminar del estudio técnico, que permitirá establecer el reglamento tendiente a normar la calidad de servicio ofrecido por los ISPs.

- Las licencias GNU son licencias abiertas, lo que implica que el usuario tiene acceso al código fuente y puede modificarlo de acuerdo a su necesidad; sin embargo, no necesariamente este tipo de licencias son gratuitas.

- Linux es un sistema operativo estable y seguro pues se conoce que Windows ha sido atacado por alrededor de 2000 tipos de virus, mientras que Linux ha sido atacado por alrededor de 40 virus.

- La complejidad de la configuración en Linux es relativa, pues se puede realizar de dos maneras diferentes; utilizando las herramientas gráficas del sistema en cuyo caso el ambiente de configuración es similar al de Windows Server, y a través de consola, situación en la que se requiere de absoluto cuidado ya que un error mecanográfico puede echar a perder el sistema.

- A nivel de usuario Linux ofrece también una interfaz gráfica que brinda la posibilidad de manejar este sistema mediante ventanas muy similares a las de Windows, sin embargo, la equivocada concepción que la gente tiene de este sistema ha llevado a la gran mayoría a considerarlo sumamente complicado de utilizar.

- Una de las grandes ventajas de Linux, es el ahorro económico que puede brindar en redes pequeñas, por cuanto puede cumplir con las funciones de *router* que en muchas ocasiones es el equipo más costoso de la red.

- Es una realidad que Linux puede ser instalado en cualquier computador en modo texto, sin embargo si se quiere contar con las facilidades del interfaz gráfico de forma eficiente, será necesario utilizar un equipo con al menos 256 MB en memoria RAM y un procesador de 900 MHz.

- Linux brinda las facilidades de interactuar en redes mixtas, redes con sistemas operativos distintos, a través de SAMBA, el cual permite el acceso y compartir archivos de Windows a Linux o de Linux a Windows.

- Linux considera que la visualización de la topología de red es un hueco para la seguridad, por cuanto cualquier persona sabría la configuración de la misma y esta situación podría ocasionar un ataque a la red; es por ello que este sistema operativo no trae configuración por *default* para este servicio, en caso de ser necesario se puede instalar la herramienta LANBROWSER.

- Linux brinda la posibilidad de establecer seguridad a dos niveles:
  - A nivel de capa aplicación mediante el servidor *proxy* de Linux que da la facilidad de realizar un control, usando reglas de acceso, las cuales pueden filtrar el tráfico mediante dominios o direcciones IP, o también da la posibilidad de redireccionar paquetes.
  - A nivel de capa red, mediante un *script* de *shell*, configurado con IPTABLES.

- Se consideró que para la configuración de IPTABLES, es más seguro utilizar la política de todo negado para luego permitir sólo los servicios necesarios para la red, puesto que con la política contraria fácilmente se puede pasar por alto el cierre de algunos puertos que podrían permitir ataques a la red.

- Para la máquina que actúa como *firewall* en la red, es mejor utilizar tarjetas *Ethernet* independientes, pues al configurar interfaces virtuales, el rendimiento de la tarjeta se ve reducido en un 50%.

- En el *firewall*, se debe especificar el puerto de destino de cualquier petición, puesto que un *hacker* puede lograr acceder a la máquina de la DMZ, lo que le permitiría abrir cualquier puerto de la LAN siempre que pueda establecer como su puerto de origen el puerto TCP que fue abierto.

- Las conexiones "legales" no usan como puerto origen nada por debajo de los puertos 1024; cuando alguien se conecta a otro puerto en su extremo abre un puerto por encima del 1024, es por ello que el *firewall* debe proteger los puertos bajos.

- La tecnología *fast-ethernet* conmutada utilizada para el diseño garantiza una capacidad suficiente para satisfacer las necesidades de la red, pues ofrece una reducción de los dominios de colisión, lo que permite mejorar el rendimiento de la red.

- El estudio de seguridad de una red debe lograr el balance entre seguridad y economía, para esto es necesario identificar los puntos críticos de la red, debido a que se puede estar invirtiendo grandes sumas de dinero en datos que podrían recuperarse o no son cruciales para el desenvolvimiento de la red.

- En los últimos tiempos se han presentado varias discrepancia acerca de la legalidad de Voz sobre IP, que luego de varios debates, la SENATEL, el CONATEL y la Procuraduría General del Estado concluyeron que este servicio, no es telefonía y que por tanto no es ilegal.

- Para que los resultados obtenidos del estudio de mercado sean lo más cercanos a la realidad, es importante realizar las encuestas sin dejar de lado a ningún sector de los potenciales usuarios, aclarando que el número de encuestas aplicado a cada sector debe ser proporcional a su tamaño.

- De los datos obtenidos del programa ofrecido por la CFN el proyecto es factible y rentable y promete un periodo de recuperación de la inversión inicial de dos años y medio.

5.2 RECOMENDACIONES

- Se recomienda utilizar una máquina para realizar los *backups* de los archivos de configuración y respaldo a los servidores de la red, el requerimiento para este computador es que tenga gran capacidad de almacenamiento, y se lo deberá ubicar en un lugar seguro.

- Antes de iniciar las configuraciones de los servidores es recomendable sacar respaldos de los archivos de configuración existentes por *default*, de tal manera si algo falla se pueda recuperar la configuración inicial.

- Para los computadores de usuarios, se recomienda que la velocidad en bus de datos sea de al menos 133 MHz, muchas veces el mercado ofrece grandes velocidades de procesamiento y gran capacidad de memoria RAM, sin embargo la eficiencia del equipo está directamente relacionada con la velocidad de transmisión de los datos.

- Es necesario tener claro que el diseño de una Intranet abarca una parte lógica, una parte física y un estudio profundo de su seguridad. En el presente proyecto se analizó todos los campos de seguridad de la Intranet, sin embargo se podría profundizar aún más en lo que respecta a seguridad en *Web* y bases de datos.

- Se recomienda que los servidores *Web* y *mail* sean configurados en dos máquinas separadas, por cuanto mejoraría notablemente su rendimiento.

- Se recomienda que el administrador de la red, lleve un registro de los diferentes problemas que susciten en la red con la respectiva solución, de tal manera que en caso de reincidir en una situación similar, pueda contar con una documentación real para agilizar la solución de problemas.

- Se recomienda realizar anualmente el análisis para la actualización del sistema operativo de la Intranet, mientras que los programas de antivirus deben ser revisados por lo menos una vez al mes.

- Las versiones de hardware deberían actualizadas de acuerdo a los avances tecnológicos, pero debería realizarse al menos cada cinco años.

- El proyecto de la Intranet es factible y rentable, sin embargo, se debe tomar en cuenta que la inversión inicial es bastante elevada y se recomienda el inicio de su funcionamiento con 14 máquinas.

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

Ancho de banda

Rango de frecuencia ocupado por una señal que transporta información que difiera de su valor máximo más allá de lo especificado. Banda de frecuencias que puede ser reproducida por un amplificador, y que representa la diferencia entre dos frecuencias dadas.[7]

ANSI (*American National Standards Institute*)

Instituto Nacional Americano de Estandarización. Organismo no gubernamental que agrupa a 300 comités de estandarización y se encarga de emitir recomendaciones y normas para los sistemas de telecomunicaciones e informática en los Estados Unidos. [7]

Backbone

Medio de conexión de alta velocidad entre computadoras encargadas de circular grandes volúmenes de información. Los *backbones* conectan ciudades o países, y forman la estructura fundamental de las redes de comunicación. Tiene una banda ancha. [7]

Browser

Software cliente diseñado para navegar por la WWW, FTP, WAIS, Usenet, http, https, etc. Es el programa navegador. [35]

Bus Mastering

La tecnología *Bus Mastering* reduce el tiempo de espera y acelera el rendimiento del sistema.[6]

Cableado

Conjunto de cables destinados a la distribución de señales o energía eléctrica. Reunión y atado de conductores mediante cuerda o por otro método, con el fin de facilitar el manejo de los conductores y dar al conjunto de ellos mejor aspecto, mayor rigidez mecánica y un código de identificación [17]

Cache

Pequeña memoria de alta velocidad utilizada en computadoras para aumentar la velocidad de ejecución de código en línea. Está situada entre el procesador central y la memoria prin*cipal.* [47]

Carrier

Infraestructura física por la cual se transportan los datos, voz e imagen. También se refiere a la empresa que ofrece el servicio de transmisión o conducción de señales; se le traduce como portador o portadora. [40]

Correo electrónico

Servicio de almacenamiento y envío de mensajes de un computador a otro. Los textos se guardan en espera de que el destinatario se conecte al sistema para recibirlos. [32]

Chat

Conversación realizada entre distintos usuarios a través de la computadora. La versión avanzada de esta forma de comunicación es la videoconferencia que permite la conversación directa a través de voz e imagen de los usuarios.[32]

CGI (*Common Gateway Interface*)

Es un programa que se ejecuta en tiempo real en un Web Server en respuesta a una solicitud de un *Browser*. Cuando esto sucede el Web Server ejecuta un proceso hijo que recibirá los datos que envía el usuario (en caso de que los haya), pone a disposición del mismo algunos datos en forma de variables de ambiente y captura la salida del programa para enviarlo como respuesta al Browser. [5]

Encriptación

Método para convertir los caracteres de un texto de modo que no sea posible entenderlo si no se la lee con la clave correspondiente, tanto en el envío como en la recepción. Hay claves públicas(PKI) y privadas [3]

Ethernet

Red de área local. Las redes Ethernet operan a velocidades de 10 Mbps, usando técnicas CSMA/CD. Ethernet es una conexión del tipo de banda base.[6]

Firewall

Conjunto de programas de protección que impiden el acceso desde el exterior a una red privada. Muy usado en Intranets. [5]

Gateway

Dispositivo de interfase entre redes, capaz de convertir distintos protocolos para poder comunicarse. Es la puerta de acceso a la red. [40]

Hipertexto

Información organizada en forma de conceptos unidos por las relaciones que tengan entre ellos. Son los textos subrayados que guardan un link. [40]

ISP (Proveedor de Servicios de Internet)

Empresa que actúa de intermediaria entre un usuario de Internet y la Internet en sí y que permite la conexión a los nodos de Internet. [4]

IEEE *(Institute of Electric and Electronic Engineers*)

Instituto de Ingenieros Eléctricos y Electrónicos. Organismo norteamericano, parte del ANSI, que mediante estudios propios promueve normas de estandarización. El IEEE es una organización profesional y una de sus principales actividades es el desarrollo de normas no obligatorias pero generalmente aceptadas, en el área de comunicaciones y electrónica, con énfasis en técnicas de medición y definición de términos.[11]

Intensidad de tráfico

Intensidad del tráfico cursado es igual al volumen del tráfico dividido entre la duración de la observación, siempre que el periodo de observación, siempre que el periodo de observación y los tiempos de ocupación se expresen en las mismas unidades. La intensidad media de tráfico así calculada se expresa en *erlangs*. [5]

Interfaz de conexión

Concepto que especifica la interconexión entre dos equipos conectados a funciones distintas. Esta especificación se refiere al tipo, número y papel de los circuitos de interconexión; así como al tipo y forma de las señales intercambiadas por esos circuitos. [4]

IP (Internet Protocol)

Ruta de acceso de un equipo, proporcionada por un servidor para lograr conexión a la red o Internet. **[6]**

Jitter

Variaciones pequeñas y rápidas en la forma de una onda debidas a fluctuaciones en la tensión de alimentación, inestabilidades y otras causas. [7]

Patch panel

Paneles organizados, normalmente identificados y etiquetados que sirven para realizar conexiones de diferentes cableados horizontales, dispositivos, y servidores. Incluso son muy utilizados en telefonía, sobre todo la digital [17]

Protocolo

Conjunto de reglas que se utilizan en el intercambio de información entre sistemas o dispositivos. Juegan un papel muy importante en redes de computadoras, y en general en las comunicaciones. [11]

PPP (*Point to Point Protocol*)

Protocolo punto a punto. Protocolo para comunicaciones entre ordenadores mediante una interfaz de serie. Utiliza el protocolo Internet. [11]

Puerto

Dispositivo que tiene un canal de salida y uno o más canales de entrada, de tal modo que el estado del canal de salida está completamente determinado por los estados del canal de entrada excepto durante los transitorios de conmutación. Son puertos lógicos: *and, or, not, nand y nor.[11]*

Rack

Es una estructura metálica rígida auto soportada, utilizada para soportar dispositivos y paneles de parcheo, afirmadas al techo o al piso. Sus medidas normalmente son: alto 48 cm(19") y ancho 2.10 mtas.(7").[17]

RSVP

Es un protocolo de señalización que reserva recursos a lo largo de un camino entre nodo origen y nodo destino para un flujo específico lo que nos permite garantizar la Calidad de Servicio. Se han especificado tres tipos de servicio en RSVP. El servicio garantizado, el cual realiza una reserva de ancho de banda para el tráfico del flujo de información y asegura unos valores máximos de retardo. El siguiente servicio es el de carga controlada, el cual reserva ancho de banda, pero no establece un servicio garantizado a nivel de retardo. Por último se encuentra el de mejor esfuerzo, el cual es un servicio sin manejo de reserva de recursos y por lo tanto no puede asegurar la calidad de la transmisión.[11]

Script

Conjunto de comandos u órdenes en un fichero que ordenados producen una salida concreta. Los *Scripts* no requieren ser compilados, ya que quien los ejecuta (interpreta) en la misma *shell* a través de los comandos que dispone.[15]

Shell

La *shell*, es una capa que protege al usuario de la máquina pura y dura y él mismo, gracias a la *shell* puedes introducir comandos, y te podrá hacer la vida más o menos fácil, dependiendo de la *shell* que uses. Generalmente en Linux, la *shell* suele ser la *'bash',* que se caracteriza por no tener necesidad de teclear todos los comandos, o nombres de ficheros ya que cuando pulsas tabulador, terminará de escribir el resto.[17]

Seguridad de transmisión

Componente de seguridad de comunicaciones que resulta de todas las medidas destinadas a proteger la transmisión contra intercepción no autorizada, análisis de tráfico y falsificación. [16]

Sistema operativo

Programa que administra los ambientes de *hardware y software* de un sistema de computación. Es un conjunto de programas escritos en lenguaje máquina y que apoyados en elementos de hardware permiten un control de todas las operaciones que un equipo de cómputo puede realizar. [14]

Software shareware

El software *shareware* se caracteriza porque es de libre distribución o copia, de tal forma que se puede usar, contando con el permiso del autor, durante un periodo limitado de tiempo, después de esto se debe pagar para continuar utilizándolo, aunque la obligación es únicamente de tipo moral ya que los autores entregan los programas confiando en la honestidad de los usuarios. [14]

Software freeware

Por licencias de uso FREEWARE se entienden todas aquellas que permiten el uso libre de la aplicación, comúnmente estas están restringidas a fines no comerciales. En caso de pertenecer a una entidad comercial y desear utilizar una aplicación bajo esta licencia debe consultar primero con los desarrolladores de la misma. [14]

SPAM

Se llama spam a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas web [15]

Tasa de bits errados

Fracción de una secuencia de bits de mensajes que se reciben con error en promedio por cada millón de bits transmitidos, en condiciones normales las transmisiones por satélites tienen una menor tasa de bits errados que las transmisiones terrestres, ya que típicamente sólo se realiza un reflejo o repetición de señal, con lo que la introducción de ruido, y por consiguiente la degradación, es menor.

Sin embargo está sujeto a mayores errores en condiciones climatológicas adversas. Porcentaje de datos transmitidos incorrectamente sobre el total de datos, expresados como una fracción del número total de bits transmitidos. Sus siglas en inglés son BER. [6]

Tarjeta de interfaz

Tarjetas de circuito impreso que componen el hardware de una interfaz tal como un puerto de comunicaciones serial o paralelo, tarjeta de vídeo.[40]

Tiempo de acceso

Tiempo invertido en la búsqueda de una información situada en memoria y su transferencia a la unidad central de proceso del ordenador[37]

Topología

Término que describe la configuración, conexión, clase y forma de operación de los elementos que componen una red de comunicaciones de datos, red de área local o red digital de servicios integrados. Estudio de aquellas propiedades de los espacios que generalizan la noción del "límite" y "función continua" del análisis.[7]

Tráfico

Conjunto de telegramas transmitidos y/o recibidos, así como los pendientes de transmitir, conversaciones o comunicaciones telefónicas en curso, número de circuitos telefónicos en uso durante determinado tiempo, conjunto de las peticiones de comunicación emanadas de un grupo de circuitos o de enlaces considerados, tomando en cuenta tanto el número de las comunicaciones como sus duraciones. Técnica de dar curso a los mensajes que ingresan a un sistema de conmutación[19]

URL

El URL de un recurso de información es su dirección en Internet, la que permite que el navegador la encuentre y la muestre de forma adecuada. Por ello el URL combina el nombre del ordenador que proporciona la información, el directorio donde se encuentra, el nombre del fichero y el protocolo a usar para recuperar los datos. [40]

Vida útil

En determinadas condiciones, intervalo que comienza en un instante dado y termina cuándo la intensidad de fallas se hace inaceptable o cuando el elemento se considera irreparable tras una avería[18]

REFERENCIA BIBLIOGRÁFICA

9	Guía para el diseño de instalaciones eléctricas Editorial Alfaomega Mexico 1995	HARPER, Enriquez
10	Instalaciones Eléctricas conceptos básicos y diseño Editorial Alfaomega México 1992	CAMPERO LITTLEWOD, Eduardo NEAGU BRATU, Servan
11	Guía completa de Protocolos de Telecomunicaciones Ed:MC Graw Hill 2002	RAD COM
12	Linux , manual de referencia Madrid - España MC- Graw Hill 2001	PETERSEN, Richard
13	Administración de Red Hat Linux al descubierto Ed:Pretice Hall Madrid - España 1999	SANENK, Thomas
14	Manual de administración de Linux Ed: Prentice Hall Hispanoamericana México 1997	SHAH, Steve
15	Guía rápida de Linux Ed: Limusa Colombia 1996	CASADO ESTRADA, José
16	Programa de certificación CCNA 2001	CISCO
17	Apuntes de Sistemas de Cableado Estructurado	FLORES, Fernando
18	500 Ideas para generar negocios ED: Milanesat Barcelona – España 1995	MARIÑO, Wilson
19	Planificación Financiera Asociación de Facultades Ecuatorianas de Filosofía y Ciencia de la Educación	CALDAS M, Marco Antonio

2001

20 Fundamentos de Marketing
Edición 2000
Ed:MC-Graw Hill
1998
PANTON, Etzel

21 Ley de compañías
Ed:Talleres de la corporación de Estudios y Publicaciones
Marzo 1999

TESIS

22 Estudio de Factores técnicos y operativos que intervienen en la infraestructura de calidad de servicio
LOOR FONSECA, Diego

23 Análisis del desempeño del protocolo para la transmisión de voz de una red WAN
OLIVO FERNÁNDEZ, Fabián 001.64404/OL49

24 Diseño del sistema de red para la transmisión de voz y datos para el Municipio de Santo Domingo de los Colorados, criterios para su administración
SALAZAR ARMIJOS, Diego Ricardo

25 Diseño de un sistema de comunicaciones para la transmisión de voz, datos y videoconferencia
QUILLAGANA CHAMBA, Nely Angélica

26 Marco teórico para aplicar voz sobre IP.
GUAYAQUIL PROAÑO, Patricio

27 Planificación de la red de computadores de área local de la Compañía Petrolera Occidental de exploración y producción
GRANIZO CEDEÑO, Luis Fernando

28 Diseño de la red para la integración de los sistemas de voz, datos y vídeoconferencia en la empresa proveedor de servicios — VÉLEZ ACOSA, Juan Carlos

29 Puesta a Tierra de Instalaciones Eléctricas — GARCÍA, Rogelio

PÁGINAS WEB

30 http//www.onside.net/faq/intranet.html

31 http://static.howstaffworks.com/gif

32 http://www.network_plumbig.com/html

33 http//www.cyckades.com.pr/soporte.html

34 http//web.net2phone.com/yapmax.html

35 http://www.comunicaciones.unitronics.es/tecnologia/voip.htm

36 http://exa.unne.edu.ar/depar/areas/informatica/Sistemas Operativos/MonogSO/SISMUL02.html

37 http://www.openbsd.org/faq/pf/es/nat.html

38 http://ludwig.dgsca.unam.mx/solicitud/tecnolo.html

39 http:/es.tldp.org/tutoriales/tutorial linux/linux_files.html

40 http://static.howstuffworks.com/gif airbone_internet.html

41 www.computerworld.ec.com/español/saccy.html

42 www.dlacuadra.com/videoconferencia.html

43 http://www.osmosislatina.com/diversos/mas_facil.htm

44 http://www.microsoft.com/latam/windowsxp/evaluacion/compare/default.asp

45 http://www.ibiblio.org/sinner/video/index_es.html

46 http://www.intel.com/proshare/conferencing/products/index.htm

47 http://www.sun.com/products-n-solutions/sw/ShowMe/index.html

48 http:www.kn.pacbell.com/wired/vidconf/multipoint.html

49 http:www.busn.ucok.edu/tips/info_int/pktswt.htm

50 http://www.busn.ucok.edu/tips/info_hrd/lan.htm

51 http://www.busn.ucok.edu/tips/info_hrd/lan.htm

52 http://www.erols.com/mcdowels/standard.html.

53 http://www.canaldinamic.es/PCMANIA/PC056/PO/pc056poporto8000.html

54 http:www.kn.pacbell.com/wired/vidconf/multipoint.html

55 http://uvision.com/idx/index.html

56 http://www.ausnetinfo.com.au/vcdefinition.html

57 http://www.faqs.org/faqs/jpeg-faq/part1/preamble.html

58 http://www.visc.vt.edu/succeed/videoconf.html

59 http://www.kn.pacbell.com/wired/vidconf/intro.html

60 http://www.visc.vt.edu/succeed/videoconf.html

61 http://www.man.ac.uk/MVC//SIMA/video1/toc.htm

62 http://www.svetlian.com/Webmaster/dream_tutor1.htm

63 http://www.programacion.com/html/tutorial/dreamweaver/2/#introdream