UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

ESTUDIO DE FACTIBILIDAD PARA LA IMPLANTACIÓN DE VPN'S A TRAVÉS DE INTERNET EN LA OPERADORA DE TURISMO "QUIMBAYA TOURS INTERNATIONAL HOLDING"

AUTORES:

CECILIA DEL PILAR DÍAZ JARRÍN

MÓNICA KRUSPKAYA GARCÍA SÁNCHEZ

TUTOR:

ING. DAVID GUEVARA

ASESOR:

ING. M.Sc. EDISON ÁLVAREZ

TESIS DE GRADO, PREVIO A LA OBTENCIÓN
DEL TÍTULO DE INGENIERO EN SISTEMAS

AMBATO – ECUADOR

JUNIO - 2005

El presente trabajo se llevó

a efecto en la Facultad de

Ingeniería en Sistemas con la

Dirección de los señores profesores

Ing. David Guevara (Director) e

Ing. M.Sc. Edison Álvarez (Asesor)

AGRADECIMIENTO

Al haber culminado una etapa de nuestras vidas en la Facultad de Ingeniería en Sistemas, miles de sentimientos llenan nuestro espíritu; la alegría del deber cumplido, la satisfacción de saber que el esfuerzo tiene su recompensa y haber aprendido que el camino al triunfo debemos recorrerlo día a día y que en este trayecto necesitamos del amor, comprensión y dedicación de muchas personas a nuestro alrededor.

Agradecer primeramente a Dios, que es el dador de todo bien, y quien al nacer nos entrega dones a cada uno para que seamos únicos, especiales, y para que sepamos acrecentarlos; gracias a Él por regalarnos la vida, protegernos y darnos la oportunidad de compartir nuestra existencia con nuestras familias y amigos.

A nuestros padres por su apoyo moral y económico, por ser nuestros amigos incondicionales, guías y consejeros; quienes nos han hecho comprender que nuestra existencia no tiene dificultades sino retos, siempre junto a nosotras para compartir nuestros triunfos y ayudarnos a aprender de nuestros errores.

A nuestros hermanos por esa voz de aliento en los momentos que pensábamos desistir y abandonar este sueño.

A nuestro director de tesis Ing. David Guevara y a nuestro asesor Ing. Edison Álvarez, quienes orientaron el presente trabajo, para que este anhelo se convierta en una realidad.

Al personal Docente y Administrativo, de quienes no solo hemos recibido conocimientos, sino amistad sincera, comprensión y buenos consejos.

A la Operadora de Turismo "Quimbaya Tours International Holding" que nos brindó el apoyo necesario para la realización de este trabajo investigativo, y en forma especial al Ing. Danilo Villacrés, Gerente de Sistemas.

A todos nuestros familiares y amigos quienes han estado junto a nosotras dándonos su apoyo total, ya sea con el hombro amigo, creyendo en nuestra capacidad o compartiendo sus conocimientos de forma desinteresada.

Cecilia y Mónica

A mi hijo, Carlos Andrés, que es mi fortaleza, por quien todo sacrificio y superación nunca serán suficientes para retribuir la paciencia y comprensión que se necesita en esta carrera. Gracias por ser la alegría de mi vida, la razón de mi existencia y mi sueño hecho realidad.

Mónica

DEDICATORIA

A mis padres, Alberto y Charito; a mis hermanos Patty, Carlos y David, porque este logro no sólo representa mi dedicación, sino el esfuerzo y sacrificio de todos. Porque han sido mi soporte, mi ejemplo y el incentivo diario para seguir adelante, he aprendido junto a ellos que la vida no es solo trabajo y esfuerzo sino también es compartir llanto y alegrías, especialmente porque han hecho que mi vida se llene de ilusiones y anhelos, que hoy, con la ayuda de Dios se convierten en realidad.

Cecilia

DEDICATORIA

A mi hijo, Carlos Andrés; por el tiempo que no pude estar a su lado, por su salud que no siempre pude cuidar, por los besos de buenas noches que no le pude dar, por su colaboración y dedicación en las tareas escolares, que muchas veces tuvo que hacer solo, ya que ser madre y estudiante a la vez requirió el sacrificio de los dos. Pero sobretodo porque su existencia, vitalidad y ocurrencias han sido el estímulo necesario para salir adelante y buscar mi superación.

Mónica

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Nosotras, CECILIA DEL PILAR DÍAZ JARRÍN, portadora de la cédula de identidad 020147976-3 y MÓNICA KRUSPKAYA GARCÍA SÁNCHEZ, portadora de la cédula 180245234-0, declaramos que la investigación enmarcada en el desarrollo de la Tesis es absolutamente original, auténtica y personal; en tal virtud, el contenido, efectos legales y académicos que se desprendan del trabajo de Tesis son y serán de nuestra exclusiva responsabilidad legal y académica.

_____ _____

Cecilia Díaz J. Mónica García S.

PRÓLOGO

Quimbaya Tours International Holding es una empresa dedicada al turismo, y por tener agencias en diferentes países, sus necesidades de comunicación se han incrementado notablemente con el transcurso de los años; por ello se pretende que las nuevas tecnologías de información puedan brindarle la posibilidad de realizar diversas tareas que hace apenas unos años no eran posibles.

El presente estudio busca realizar una investigación acerca de la tecnología *VPN (Virtual Private Network, Redes Privadas Virtuales)* y los diversos puntos que se involucran, como lo es la seguridad, formas de encriptación más utilizadas y los diversos métodos que las aplican.

Conjuntamente a la investigación de la tecnología, se efectúa la búsqueda del mejor proveedor de equipos y enlace que se necesitan en la implantación de una VPN, para lo cual se hace un análisis de Factibilidad Económica, Técnica y Operativa.

Se abarcará todo un proceso de investigación, planeación y elección para una posible implantación de esta tecnología en beneficio de la Empresa.

ÍNDICE

CAPÍTULO III FUNDAMENTO TEÓRICO

CAPÍTULO IV TECNOLOGÍA VPN

CAPÍTULO V SEGURIDAD

ÍNDICE DE FIGURAS

Figura CONTENIDO Pág.

CAPÍTULO II SITUACIÓN ACTUAL DE LA TRANSMISIÓN DE DATOS DE "QUIMBAYA TOURS"

CAPÍTULO III FUNDAMENTO TEÓRICO

CAPÍTULO IV TECNOLOGÍA VPN

CAPÍTULO V SEGURIDAD

CAPÍTULO VI VPN SOBRE WINDOWS 2000 ADVANCED SERVER

CAPÍTULO VII PROVEEDORES DE EQUIPO Y ENLACE

CAPÍTULO VIII RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

Tabla **CONTENIDO** **Pág.**

CAPÍTULO II SITUACIÓN ACTUAL DE LA TRANSMISIÓN DE DATOS EN "QUIMBAYA TOURS"

CAPÍTULO VII PROVEEDORES DE EQUIPO Y ENLACE

CAPÍTULO VIII RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE ANEXOS

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y cualquier problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

Además las redes están cambiando las formas de comercio y las formas de vida en general. Las decisiones comerciales se toman cada vez más rápidamente y los que las toman requieren acceso inmediato a información exacta.

Pero antes de preguntar lo rápido que se puede conectar, es necesario saber cómo funcionan las redes, qué tipo de tecnología está disponible y qué diseño se ajusta mejor a cada conjunto de necesidades.

Cuando una empresa añade una nueva división, la tecnología debe ser lo suficientemente flexible para reflejar los cambios de configuración. Conocer las posibilidades de las redes y cuándo usar cada tipo de tecnología, es

esencial, para establecer el sistema correcto en los entornos de información actuales que cambian dinámicamente.

Los avances tecnológicos están haciendo posible que los enlaces de comunicaciones puedan transmitir señales más rápidamente y con más capacidad. Teniendo en cuenta que es muy fácil implementar tecnología de punta, pero, que aún no está totalmente establecida, y es muchas veces incompatible, lo cual puede traer dificultades futuras.

1.2 JUSTIFICACIÓN

Por estas razones hace algunos meses, se presentó como alternativa el uso de VPN's (***Virtual Private Networks, Redes Privadas Virtuales***) a través del Internet, pero al no existir un Estudio de Factibilidad para esta empresa, los ejecutivos piensan que estas redes no brindan las ventajas de seguridad y calidad que ofrece un enlace dedicado, enfrentándose al dilema de Calidad vs. Precio.

Es así como "Quimbaya Tours International Holding" decidió auspiciar un estudio sobre el tema de comunicación y la forma de hacerla lo más óptima

posible, sobre la base del cual podrá o no, tomarse la decisión final de su implantación.

El presente estudio se enfocará en la tecnología VPN a través del Internet como la alternativa para solucionar los inconvenientes que actualmente tienen las Agencias en el campo de la comunicación.

1.3 OBJETIVOS

1.3.1 GENERAL

Elaborar un Estudio de Factibilidad, Seguridad y Beneficios que brindarían la posible implantación de VPN's a través del Internet para mejorar el problema de comunicación y transmisión de información en la Operadora de Turismo "Quimbaya Tours International Holding".

1.3.2 ESPECÍFICOS

- Realizar una investigación sobre la tecnología VPN.
- Investigar acerca de las seguridades, encriptación y autenticación que se aplica en VPN's.

- Determinar las formas de comunicación que tiene la Empresa y optimizarlas con la implantación de la tecnología VPN.
- Recomendar el mejor proveedor de equipos y enlace, tomando en cuenta la calidad y servicios que ofrecen.

1.4 ALCANCES Y LIMITACIONES

Se pretende que este estudio se convierta en un precedente, en el campo de la transmisión de datos así como fuente de consulta para estudiantes y personas involucradas en ésta área.

Además que se constituya en una herramienta útil para la optimización de las comunicaciones en la Operadora de Turismo “Quimbaya Tours International Holding”.

A pesar de que el presente estudio ha sido auspiciado directamente por el Gerente Regional de Sistemas de la Empresa, la prioridad que se le dé a la implantación o no de esta tecnología no depende de él, la decisión final la toman conjuntamente el Presidente, y el Comité de Dirección de la misma.

En este estudio se presenta una simulación de cómo funciona una VPN con una topología que emula la conexión vía Internet mediante la utilización de software, debido a que las Agencias más cercanas a Quimbaya Quito son las de Lima y Bogotá, razón por la que resulta más difícil el realizar una práctica concreta dentro de la Empresa.

Otra de las limitantes para poder realizar una práctica mediante la conexión de equipos diseñados para una VPN es su costo elevado ya que mientras no se autorice su implantación la Empresa no puede adquirirlos.

1.5 METODOLOGÍA

Se ha usado la Investigación Bibliográfica o Documental para la recolección, procesamiento y análisis de la información, tomada de fuentes indirectas como: libros, folletos, manuales y documentos relacionados con la Tecnología VPN.

Se hará uso del Método Científico para la recolección de datos empleando para esto como técnica bibliográfica la Lectura Científica, también se utilizará información encontrada en Internet, y no se descarta el uso de cuestionarios.

Se trabajará directamente con el Gerente Regional de Sistemas cuya residencia es la ciudad de Lima y además con sus Asistentes en cada Agencia de América Latina, vía Internet, pues son ellos, quienes están involucrados directamente en el manejo de la red de la Empresa.

CAPÍTULO II

SITUACIÓN ACTUAL DE LA TRANSMISIÓN DE DATOS EN "QUIMBAYA TOURS INTERNATIONAL HOLDING"

2.1 RESEÑA HISTÓRICA

Quimbaya es el nombre de una antigua tribu precolombina, dotada de una organización excepcional, cuyos miembros eran orfebres maravillosos, les gustaba crear y poseían una gran imaginación.

Así treinta siglos más tarde los dueños de esta Empresa han revivido el nombre de esta valerosa y trabajadora tribu para poner en práctica todas sus características que los hicieron perdurar en el tiempo.

Quimbaya Tours Internacional Holding, ingresa a este mercado tan competitivo dedicado al Turismo, y en su afán de eficiencia y calidad en el servicio, fueron creando poco a poco sus oficinas, en América del Sur hace 18 años, empezando en 1987, en Bogotá – Colombia, paulatinamente crecieron a los países vecinos como Ecuador, Perú, Bolivia, Chile, Argentina, Brasil, luego por Centro América en México, Guatemala, Costa

Rica y Panamá, además Europa en Gran Bretaña, Francia, España, Italia y ahora en Oriente Medio en Tel Aviv.

2.2 ÁMBITO DE ACCIÓN

Hoy en día es una empresa dedicada al Turismo, con más de cien personas que forman equipos de gente dinámica e interesados en los viajes de sus clientes.

Para ello Quimbaya no sólo se preocupa de las necesidades, motivos o tipos de viaje, sino que tiene también relaciones privilegiadas con muchos establecimientos en los países que tiene ingerencia.

De hecho la satisfacción más grande de Quimbaya es el excelente conocimiento de los países gracias a sus 11 oficinas locales.

La Empresa vende paquetes turísticos a agencias europeas y trabajan por satisfacer todas las necesidades de sus clientes invitándolos a descubrir los extraordinarios paisajes de nuestros países, utilizando todos los medios actuales disponibles.

Con Quimbaya los turistas tienen itinerarios completos, prestaciones de calidad, tours con total seguridad, elección de hoteles de calidad y negociación con tarifas preferenciales.

2.3 SITUACIÓN ACTUAL Y UBICACIÓN EN EL MERCADO

La Empresa se ha consolidado en el área del Turismo a nivel de América Latina y esto se lo puede deducir de los resultados obtenidos.

En el 2004, el número de clientes de Quimbaya llegó a 24.636 en relación a los 17.112 en el 2003, significando un alza del 44%. El detalle por países es el siguiente:

País	*Clientes*
Argentina	4.713
Bolivia	1.048
Brasil	5.362
Chile	212
Ecuador	1.879
Guatemala	652
México	4.691
Perú	6.109

Tabla 2.1 Países y número de clientes en el 2004

2.4 PROYECCIÓN

En el campo comercial la Empresa en el año 2004 creó sus nuevas agencias en Inglaterra y Tel Aviv con el afán de mantener y superar en el 2005, el crecimiento de clientes, obtenido en el año anterior.

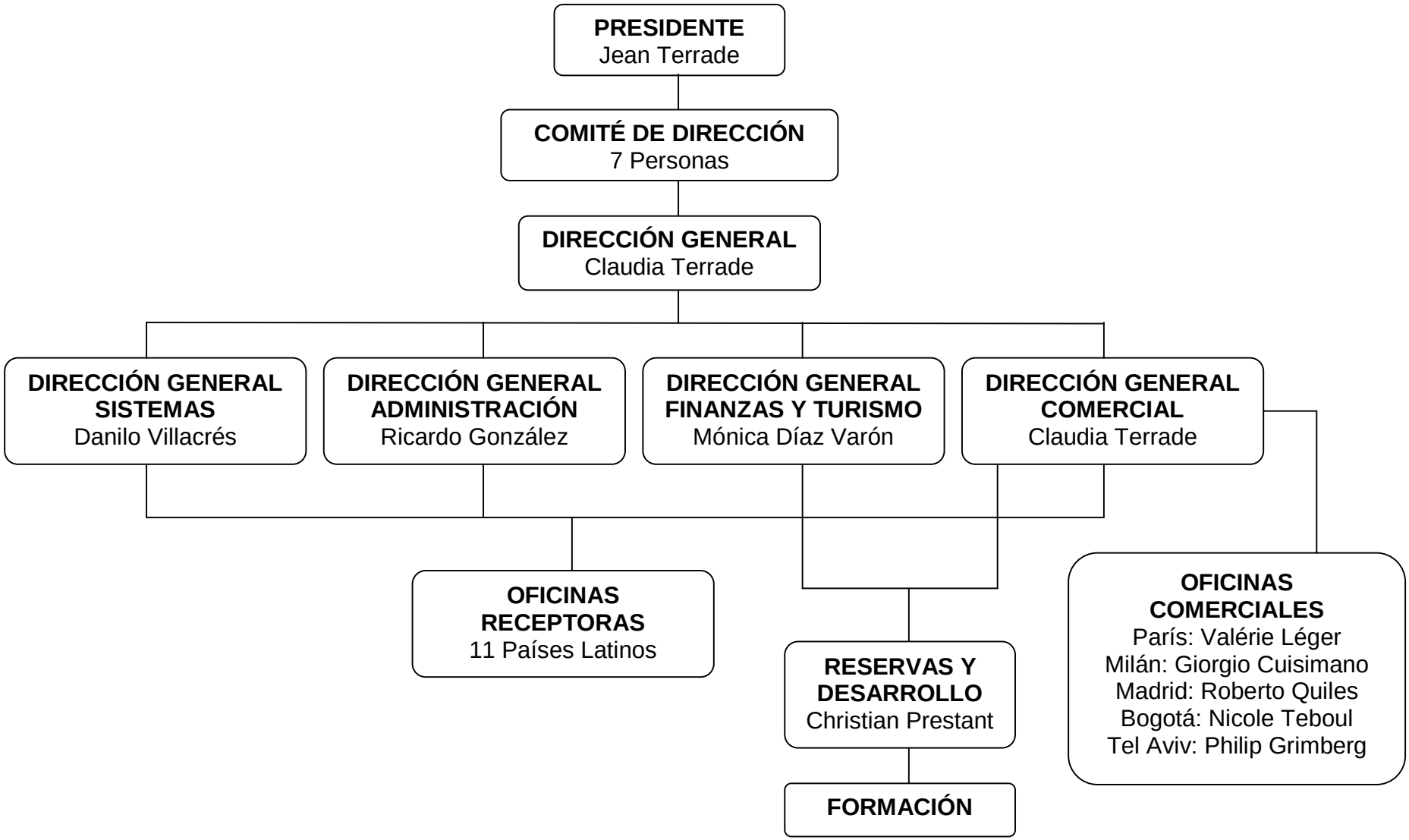
En cuanto al campo informático el Departamento de Sistemas continúa desarrollando su propio software orientado al campo del turismo, siendo el único en su género, por lo cual se lo ha patentado con el propósito de una futura comercialización y presentación en ferias internacionales en el área del turismo.

Para el año 2005 se quiere optimizar el aspecto de las comunicaciones, pues es un tema que se lo ha pospuesto por el desarrollo del Sistema Integrado, por ello se ha auspiciado el tema de las VPN's como la opción requerida.

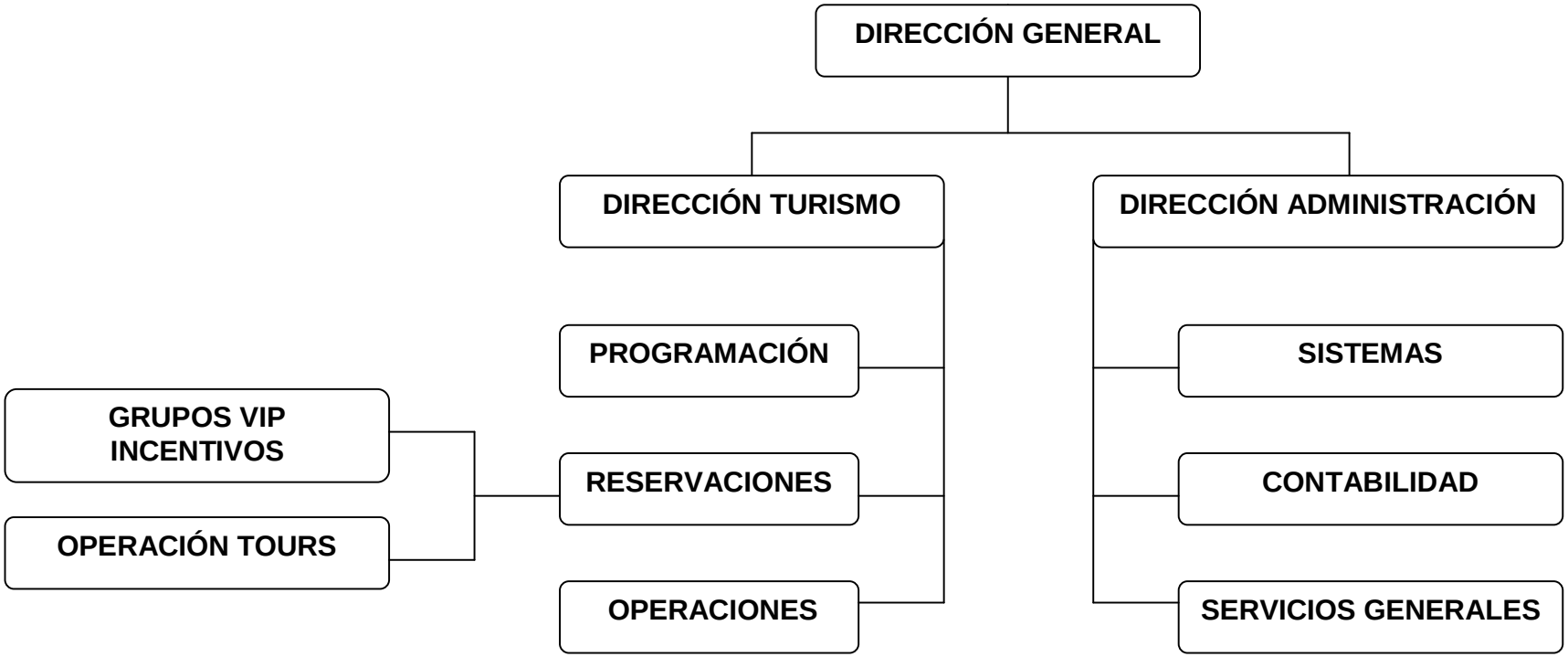
2.5 ORGANIZACIÓN

Quimbaya Tours es una estructura eficaz; la Holding supervisa las 4 oficinas comerciales y las 11 oficinas receptoras en América Latina.

ESTRUCTURA GENERAL DE QUIMBAYA TOURS INTERNATIONAL HOLDING



ESTRUCTURA DE LAS OFICINAS RECEPTORAS



2.6 FORMA DE INTERCAMBIO DE INFORMACIÓN ENTRE LAS AGENCIAS

Debido a que todas las Agencias se encuentran geográficamente dispersas, el intercambio de información se realiza mediante e-mails, cd's enviados por correo alterno, fax, o vía telefónica y tienen solamente una determinada hora en la tarde para transmitirla a través de Internet.

Dándose en muchas ocasiones el problema de que al ser muy extensa, exceden el tiempo asignado a cada una de ellas, produciéndose una congestión en la red y retardo en la llegada de información que en ocasiones es urgente.

Además se tienen costos excesivos en telefonía internacional debido a que es la única forma que tienen de acceder a información importante y en tiempo real.

Si surgen complicaciones con el mal manejo del Software Sisturi por parte de los empleados fuera del área de sistemas alterando las bases de datos por mal ingreso de los mismos, los Asistentes del Gerente de este departamento pueden dar soluciones temporales pero siempre es necesario la presencia de él para solucionar dichos inconvenientes en

forma definitiva, razón por lo que además de los viajes planificados a cada país surgen viajes no previstos en el presupuesto de la Empresa.

2.7 VOLUMEN DE INFORMACIÓN QUE TRANSFIERE

El volumen de información aproximada que se transfiere diariamente es de 20 Mb por oficina, ya que por las causas anteriormente citadas no se puede extender más para cada agencia; por ello también mucha información que se necesita en otros departamentos se deja de transferir dando prioridad exclusivamente al Departamento de Reservas.

Dependiendo de la temporada y la Agencia muchas de las veces los 20Mb resultan insuficientes para transferir solo la información importante y fundamental de cada una de ellas, así como para recibir oportunamente datos confiables y actualizados.

Uno de los grandes inconvenientes que se tiene actualmente es que al no contar con una forma de interconexión remota todo lo referente al área de sistemas está centralizado exclusivamente en una sola persona y el momento en que ésta falte, sería muy notaria la acefalía del departamento

precisamente por la ausencia de una forma efectiva de comunicación entre las Agencias.

2.8. SEGURIDAD INFORMÁTICA EN LAS DIFERENTES OFICINAS COMERCIALES

Para saber el tipo de acceso a Internet y las seguridades con que cuenta cada una de las oficinas comerciales se realizó un formulario de preguntas el cual fue contestado por los encargados del Departamento de Sistemas de los distintos países. (***Ver Anexo 1***)

A continuación se presenta de forma tabulada las respuestas de las preguntas del cuestionario para tener una mejor apreciación de la situación actual en cuanto a enlaces y seguridad de la Empresa.

1. Sobre el tipo de acceso a Internet Primario.

Tipo	Porcentaje	Velocidad Up	Velocidad Down
Fibra Óptica	11 %	128 Kbps	64 Kbps
ADSL	78 %	316 Kbps	458 Kbp
Otros	11 %	32 Kbps	64 Kbps

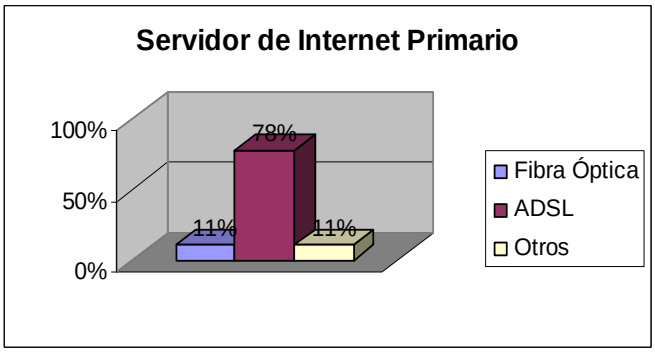


Fig. 2.1 Tipo de Servidor de Internet Primario

La Empresa tiene contratados en 7 de sus oficinas el servicio ADSL como enlace de última milla para el Servicio de Internet.

2. Internet Secundario (Dial -Up)

Dial - Up	Porcentaje
Si	56 %
No	44 %

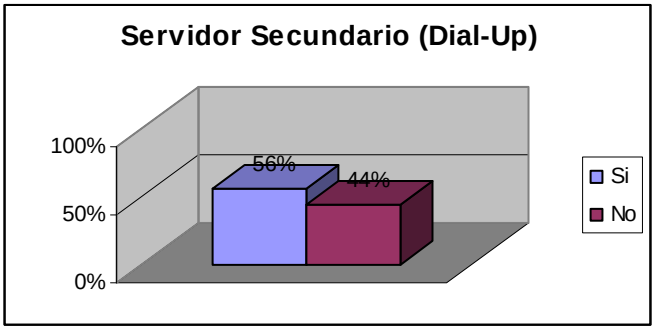


Fig. 2.2 Servidor de Internet Secundario

Solamente las Agencias más grandes poseen un Servicio de Internet Secundario en este caso por conexión telefónica (Dial-Up).

3. Servidor de Internet

Posee	Porcentaje
Si	100 %
No	0%
Software	Linux Kipux Server 100 %

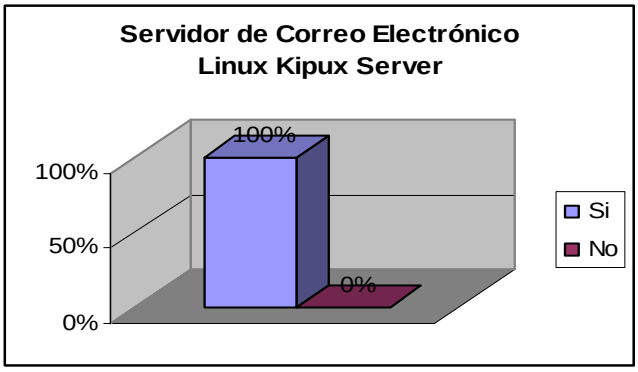


Fig. 2.3 Servidor de Correo Electrónico

Como todas las Agencias tienen acceso al Internet, la totalidad de las mismas poseen un Servidor de Correo Electrónico que funciona bajo Linux Kipux Server.

4. Servidor de Datos

Sistema Operativo	Porcentaje
Windows 2003 Server	11 %
Windows XP Profesional	56%
Windows NT Server	22 %
Windows 2000 Server	11%

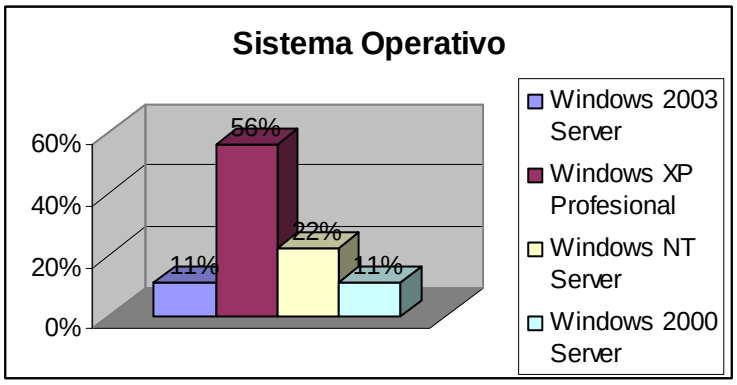


Fig. 2.4 Sistema Operativo del Servidor de Datos

La Empresa tiene licencias de Windows en diferentes versiones como Sistema Operativo ya sea del Servidor de Datos o el equipo que cumple estas funciones, siendo el Windows XP Profesional el que se encuentra instalado en la mayoría de las Agencias.

Generación de claves para el ingreso al Sistema	Porcentaje
Automático	78 %
Manual	22 %

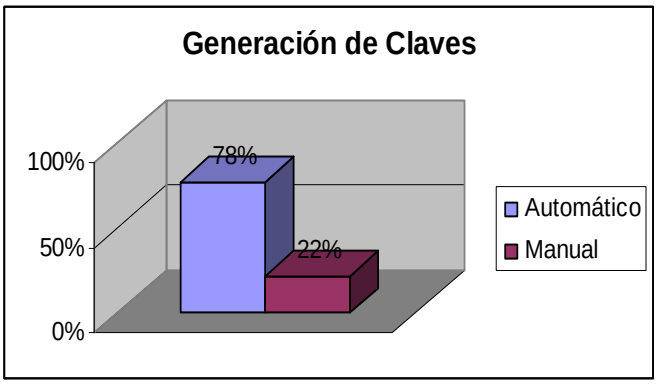


Fig. 2.5 Generación de Claves de Acceso

La mayoría de las Agencias utiliza procesos automáticos para la generación de claves de acceso al Sistema.

5. Seguridad de la Información

Programa para Respaldos	Porcentaje
Backup Windows	44 %
Mandy Backup	11%
Winzip	11 %
Quemadores de Cd	34 %

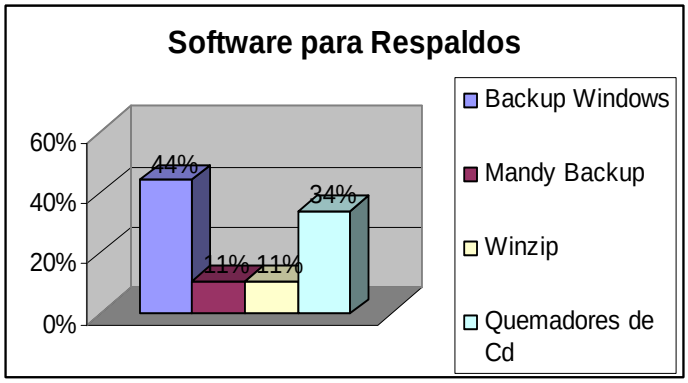


Fig. 2.6 Software utilizado para Respaldos

Los programas utilizados para respaldar la información son las que ofrece Windows, para guardarlos de forma comprimida el Winzip y para masterizar la información en Cd's diferentes quemadores.

Archivos que se Respaldan	Porcentaje
Sisturi	100 %
Sistemas de Contabilidad	55%
Archivos de mails	44 %
Archivos de datos	67 %

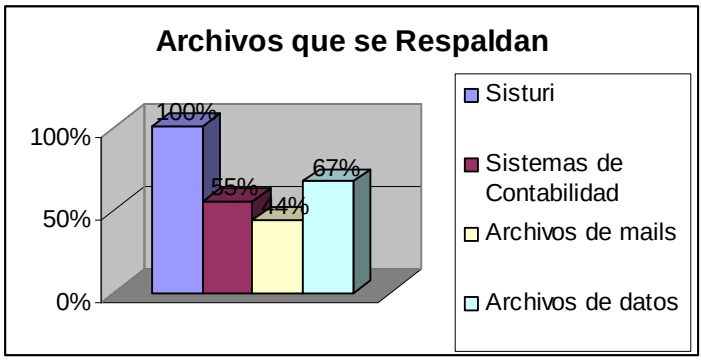


Fig. 2.7 Archivos que se respaldan

El Sistema denominado Sisturi, es el software que el Departamento de Sistemas desarrolló exclusivamente para esta Empresa, es por ello que se respalda el 100% de la información que procesa en todas las Agencias.

Frecuencia de Respaldos	Porcentaje
2 veces al día	22 %
Diario	45 %
1 vez por semana	11 %
1 vez cada 15 días	11 %
1 vez por mes	11 %

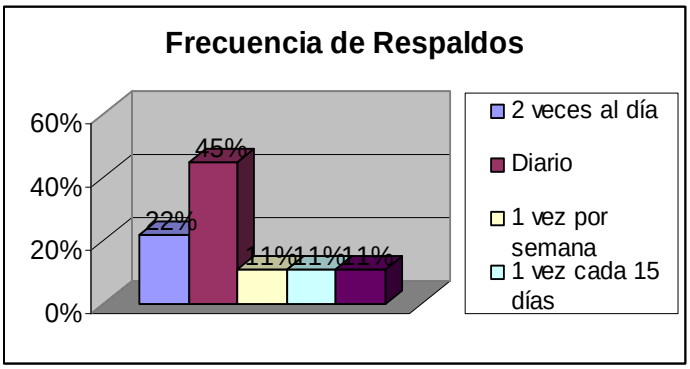


Fig. 2.8 Frecuencia de respaldos

Solamente las 2 Agencias más grandes que tiene Quimbaya respaldan la información 2 veces al día, mientras que las que están con un crecimiento progresivo la respaldan diariamente, pero las pequeñas lo hacen esporádicamente.

Dispositivo de Respaldo	Porcentaje
Tape Backup	11 %
Cd's	67%
Discos Duros	22 %
Casillas de Seguridad	55 %

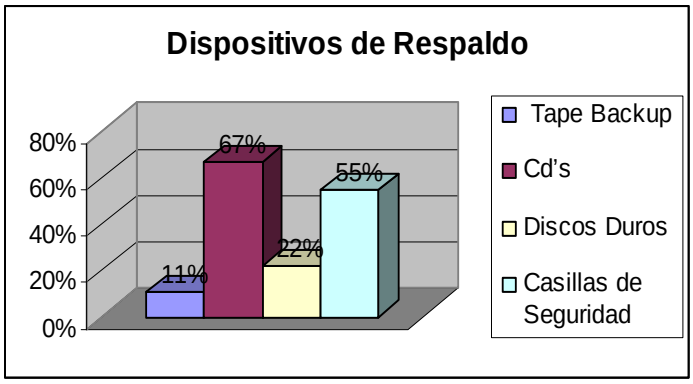


Fig. 2.9 Dispositivos de Respaldo

El dispositivo de respaldo de información más utilizado es el CD y Discos Duros los cuales son guardados solo por la mitad de las Agencias en Casillas de Seguridad.

Antivirus	Porcentaje
MacAfee	67 %
Norton	33%

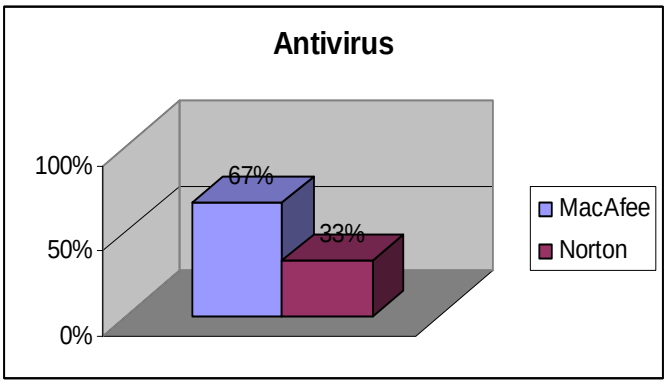


Fig. 2.10 Antivirus

En la actualidad el antivirus más utilizado por la Empresa es el McAfee.

Frecuencia de Antivirus	Porcentaje
Diario	56 %
1 vez por semana	33 %
2 veces por semana	11 %

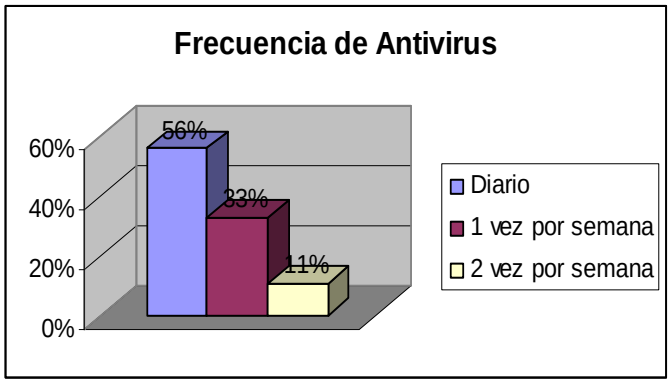


Fig. 2.11 Frecuencia del Uso de Antivirus

La frecuencia del uso del antivirus depende del criterio del encargado del Departamento de Sistemas pero en general más de la mitad ha optado por una revisión diaria.

Planes de Contingencia	Porcentaje
Ataques de Virus	78 %
Pérdida de Información	67 %
Daño de equipos	78 %

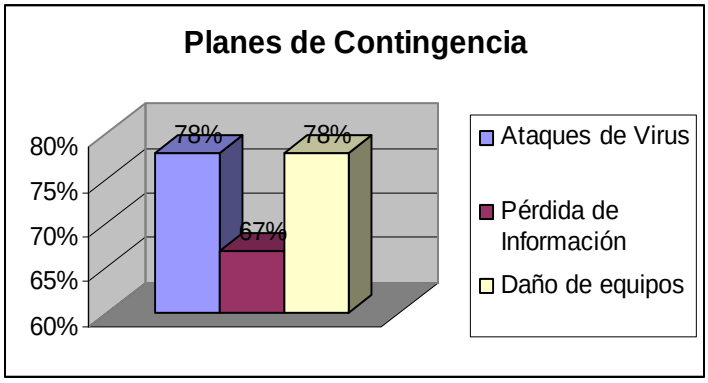


Fig. 2.12 Planes de Contingencia

Todas las Agencias tienen Planes de Contingencia diferentes, nada estandarizado. Pero la mayoría ha dado prioridad a planes en contra de Ataques de Virus y Daños de Equipos.

Seguridad del Departamento de Sistemas	Porcentaje
Oficina Propia	56 %
Acceso de Usuarios Externos	11 %
Mantenimiento externo a Servidores y Pc's	56 %

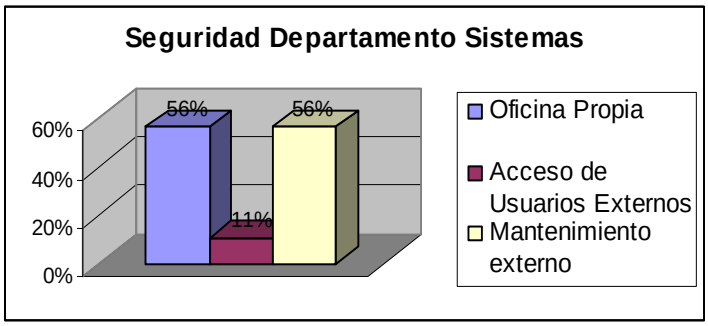


Fig. 2.13 Seguridad en el Departamento de Sistemas

Solamente las Agencias grandes cuentan con oficina propia siendo en éstas más fácil el control de la seguridad; así mismo la mitad de las Agencias contratan mantenimiento externo tanto para Servidores como para los demás equipos.

De acuerdo a las tabulaciones anteriores se concluye que:

B En la mayoría de las Agencias se tiene contratado el servicio de ADSL como enlace de última milla, además los ISP proveen en promedio una velocidad Up de 316 Kbps y velocidad Down de 458 Kbps. La conexión secundaria a Internet (Dial-Up) la tienen la mitad de las Agencias. Todas poseen además un Servidor de Internet el cual trabaja bajo Linux Kipux Server.

B Todas las Agencias tienen ya sea un Servidor de Datos dedicado o un equipo con tecnología de punta que realiza tales funciones, los mismos que trabajan sobre diferentes versiones de Windows y tienen buena velocidad de procesamiento y gran capacidad de almacenamiento.

B Las formas de seguridad que se brindan, tanto al Departamento de Sistemas como a la información que se maneja, de posibles ataques de virus, pérdida o robo de información, desastres o daños de equipos son diferentes de acuerdo al criterio de cada encargado y no se cuenta con un Plan de Seguridad Estandarizado para todas las Agencias.

2.9 SISTEMAS OPERATIVOS Y EQUIPOS DE LAS OFICINAS COMERCIALES

Cada una de las oficinas comerciales de América Latina, tienen su respectiva red LAN para enlazar los diversos departamentos que conforman las mismas.

Trabajan con Linux Kipux Server para lo que es el Servidor de Correo Electrónico y diferentes versiones de Windows como sistema operativo para los Servidores de Datos y las estaciones de trabajo.

SISTEMAS OPERATIVOS Y NÚMERO DE EQUIPOS

País	*Win'98*	*Win'XP Profesional*	*Win'XP Home Ed*	*Win' NT Server*	*Win'NT Workstat*	*Win'2000 Server*	*Linux Kipux Server*	*Total*
Argentina	6	8	0	1	0	0	1	***16***
Bolivia	4	1	0	0	0	1	1	***7***
Brasil	6	8	0	0	0	1	1	***16***
Colombia	2	1	0	0	0	0	1	***4***
Chile	2	1	0	0	0	1	1	***5***
Ecuador	6	5	0	0	0	1	1	***13***
Guatemala	2	2	0	0	0	1	1	***6***
México	6	8	1	0	0	1	1	***17***
Perú	4	10	0	2	9	0	1	***26***

Tabla. 2.2 Sistemas Operativos y Número de Equipos de cada Agencia

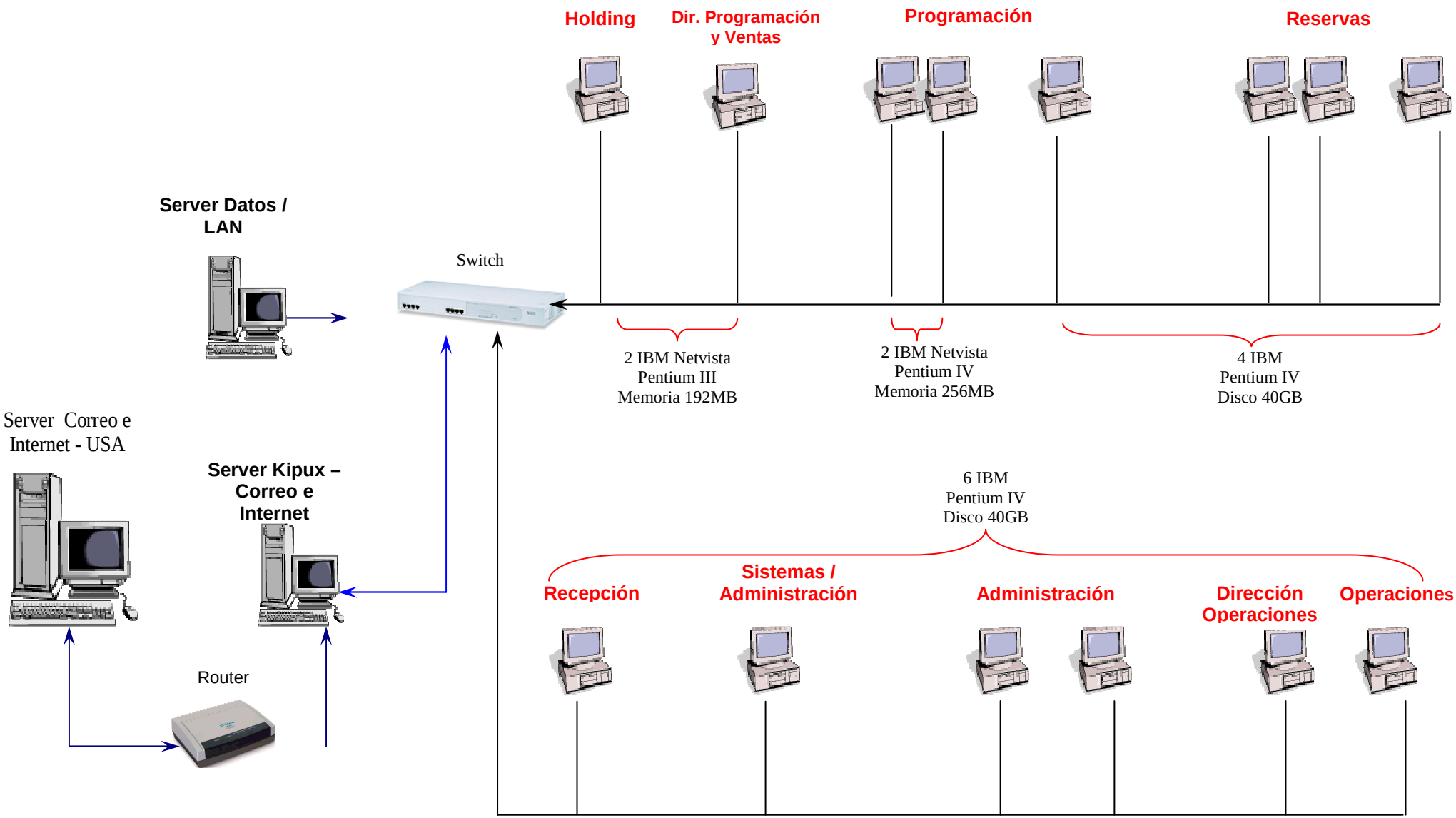
2.10 ESQUEMAS DE RED

Aquí se presenta de forma gráfica la distribución e interconexión de los diversos departamentos que conforman cada una de las oficinas comerciales de América Latina.

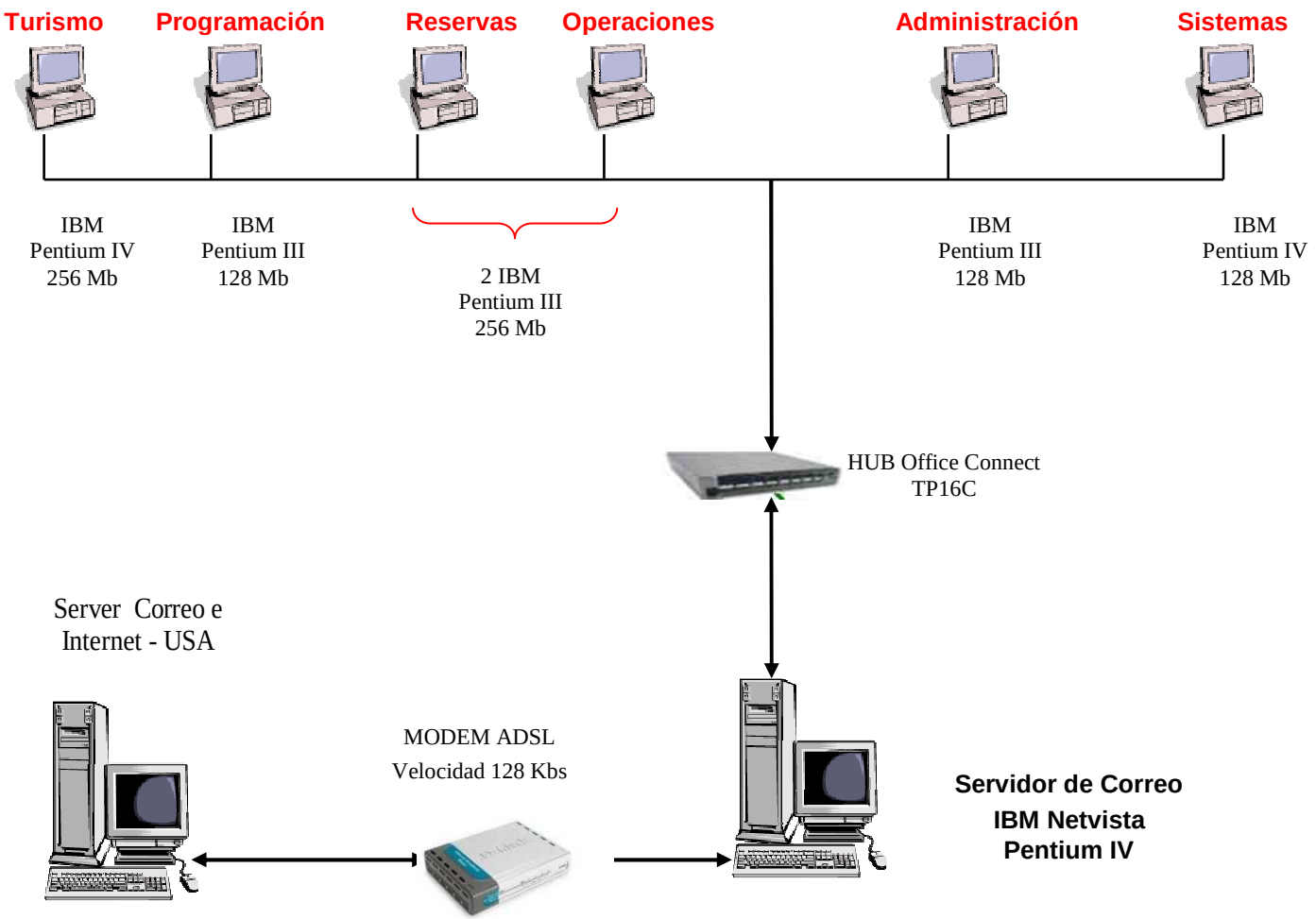
Todas las Agencias cuentan con una red LAN completamente operativa, pues internamente no existe pérdida o retraso de información; el problema de comunicación surge al no haber tratado de enlazar remotamente todas las Agencias que conforman la Holding tanto en América como en Europa, para la transferencia de información en tiempo real de forma transparente y fácil para el usuario.

Los equipos que se utilizan para la configuración de cada una de las redes LAN son de marca, relativamente nuevos y se los renueva de forma que estén acorde a los avances tecnológicos en cuanto a Hardware y Software.

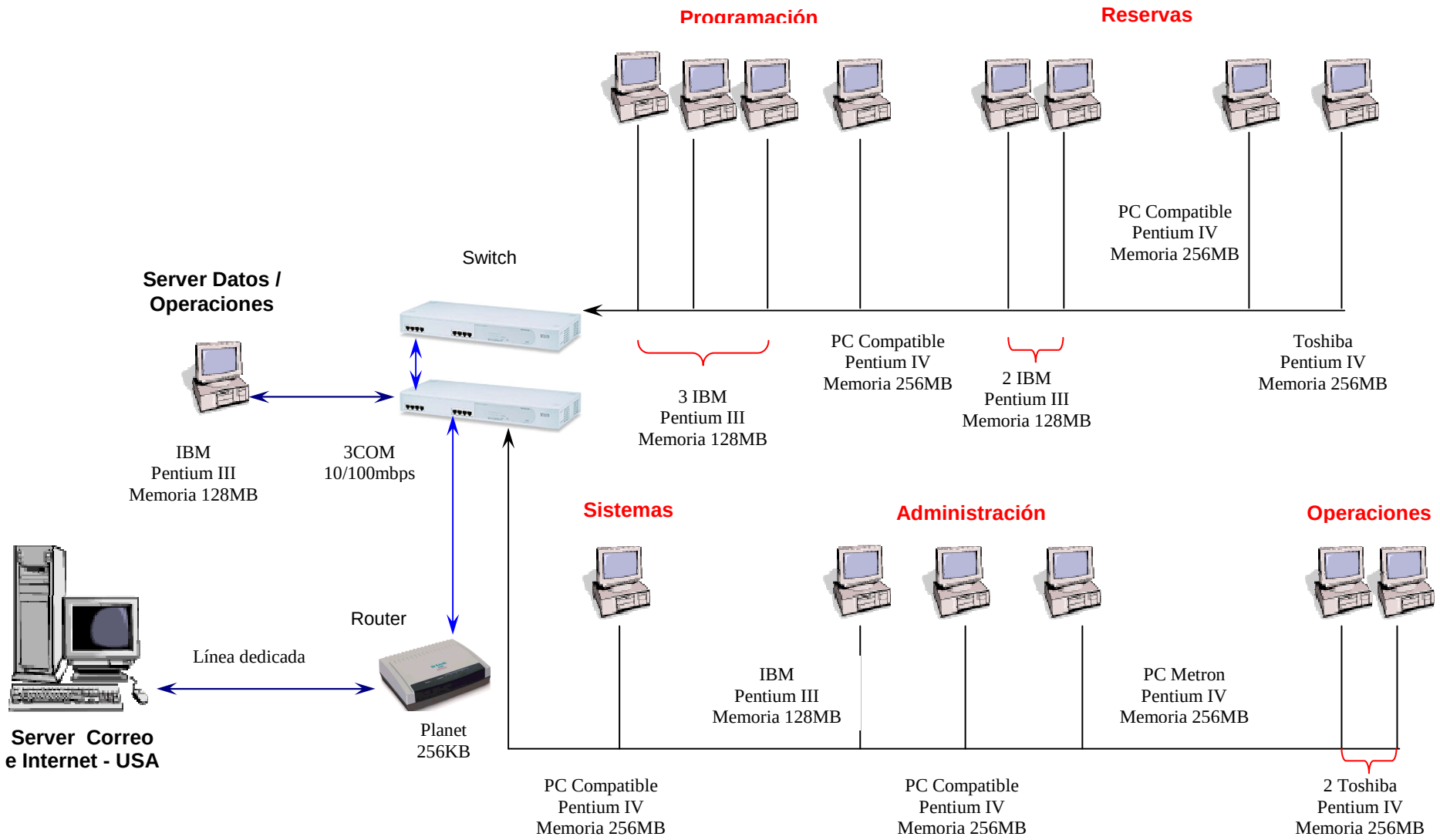
ESQUEMA DE RED QUIMBAYA TOURS "*ARGENTINA*"



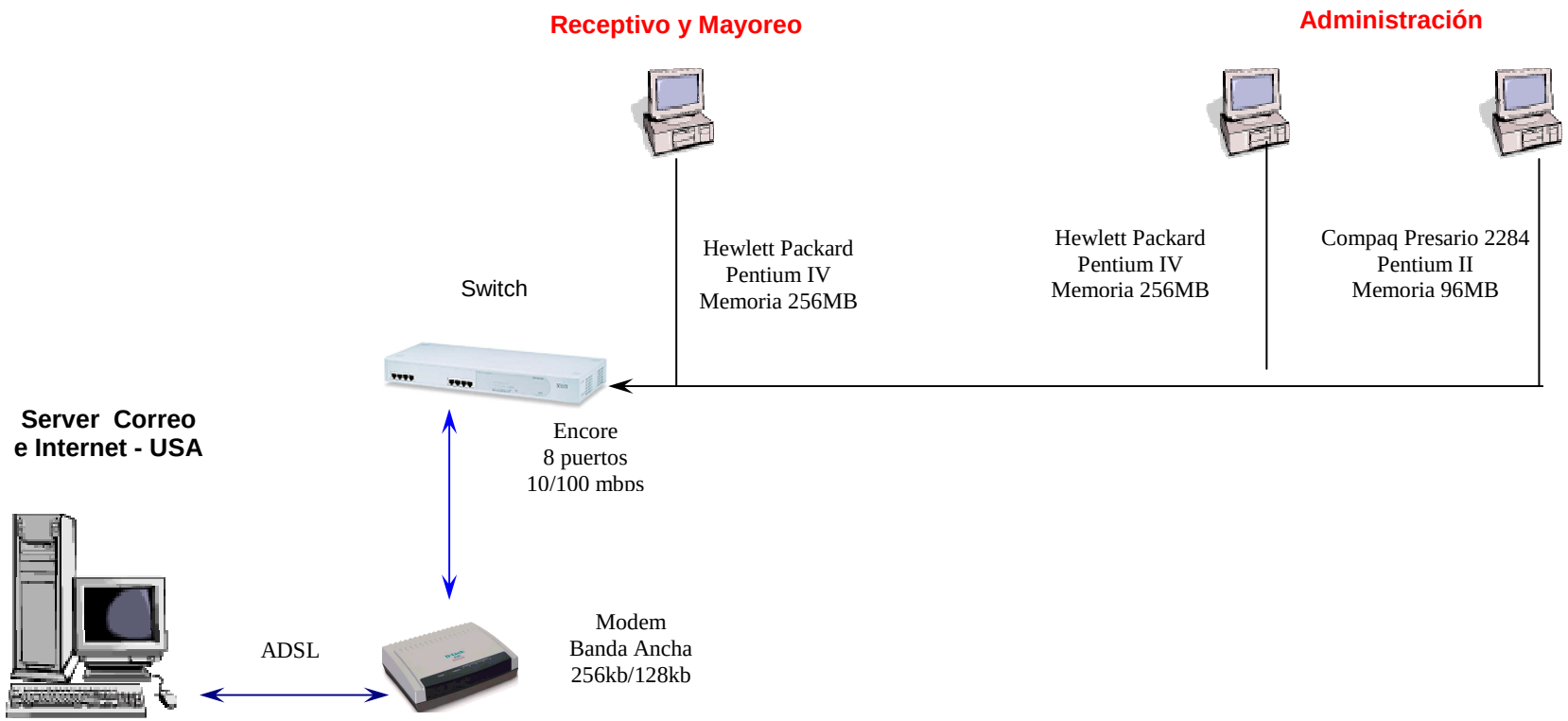
ESQUEMA DE RED QUIMBAYA TOURS "*BOLIVIA*"



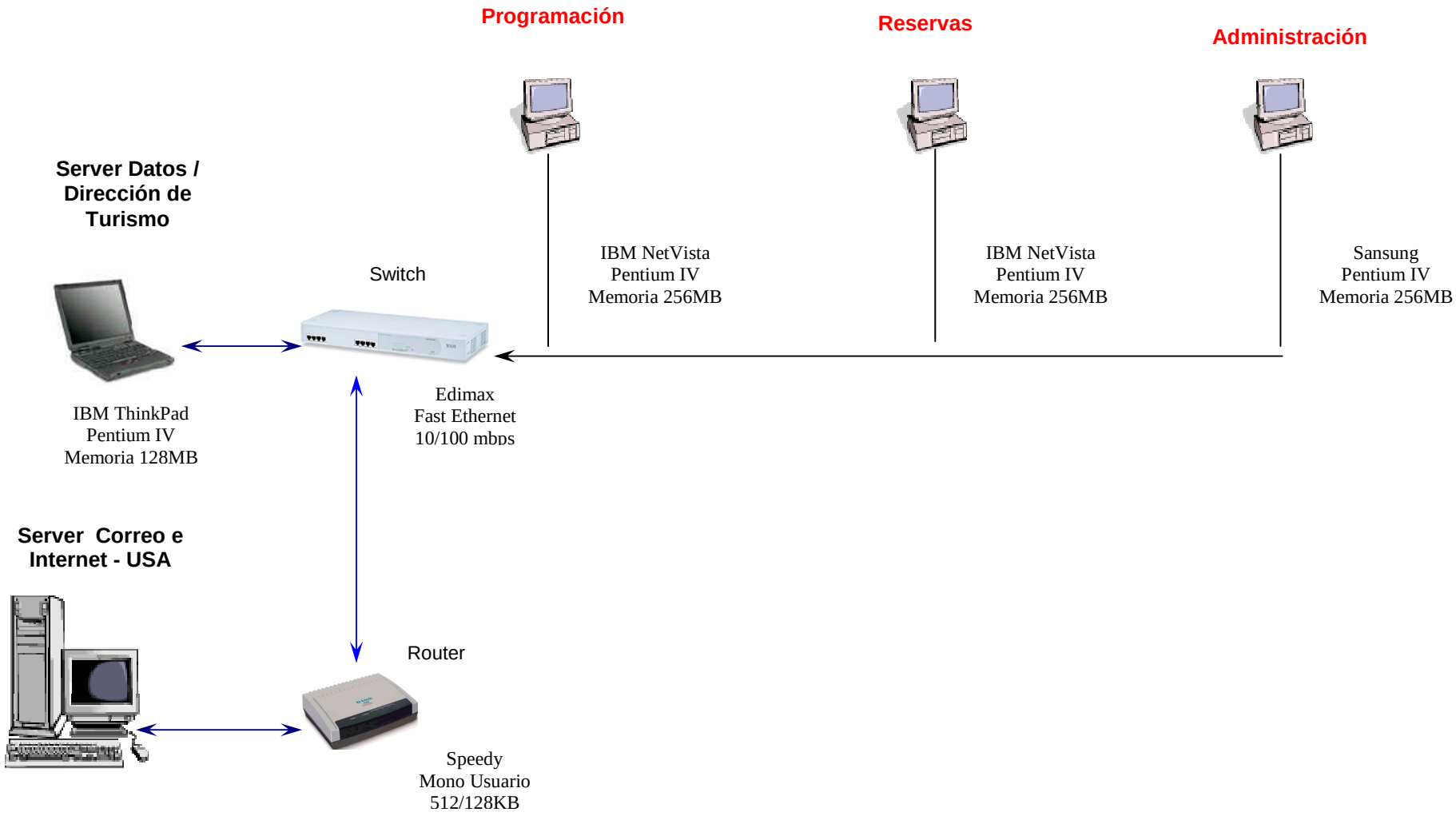
ESQUEMA DE RED QUIMBAYA TOURS "*BRASIL*"



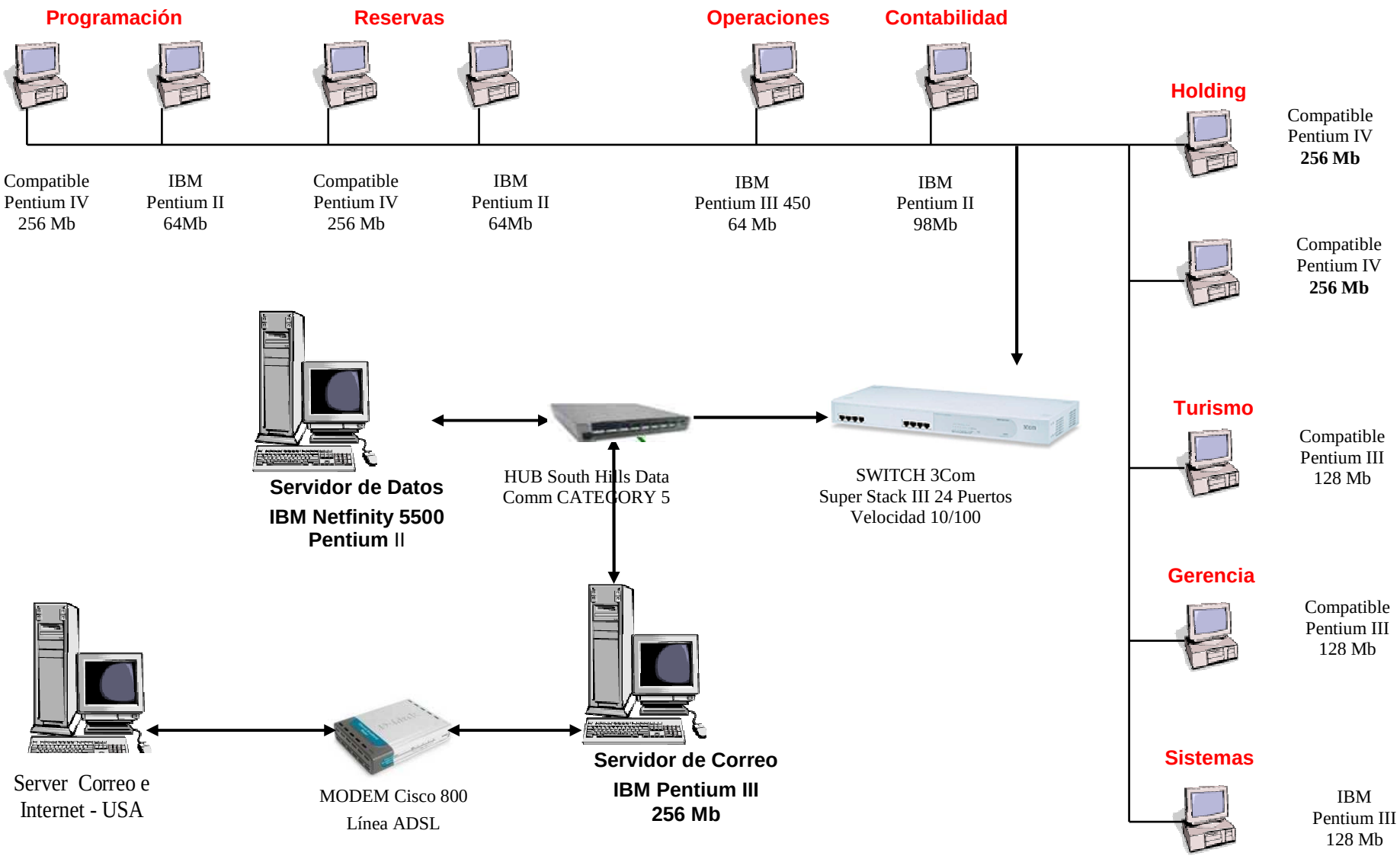
ESQUEMA DE RED QUIMBAYA TOURS "*COLOMBIA*"



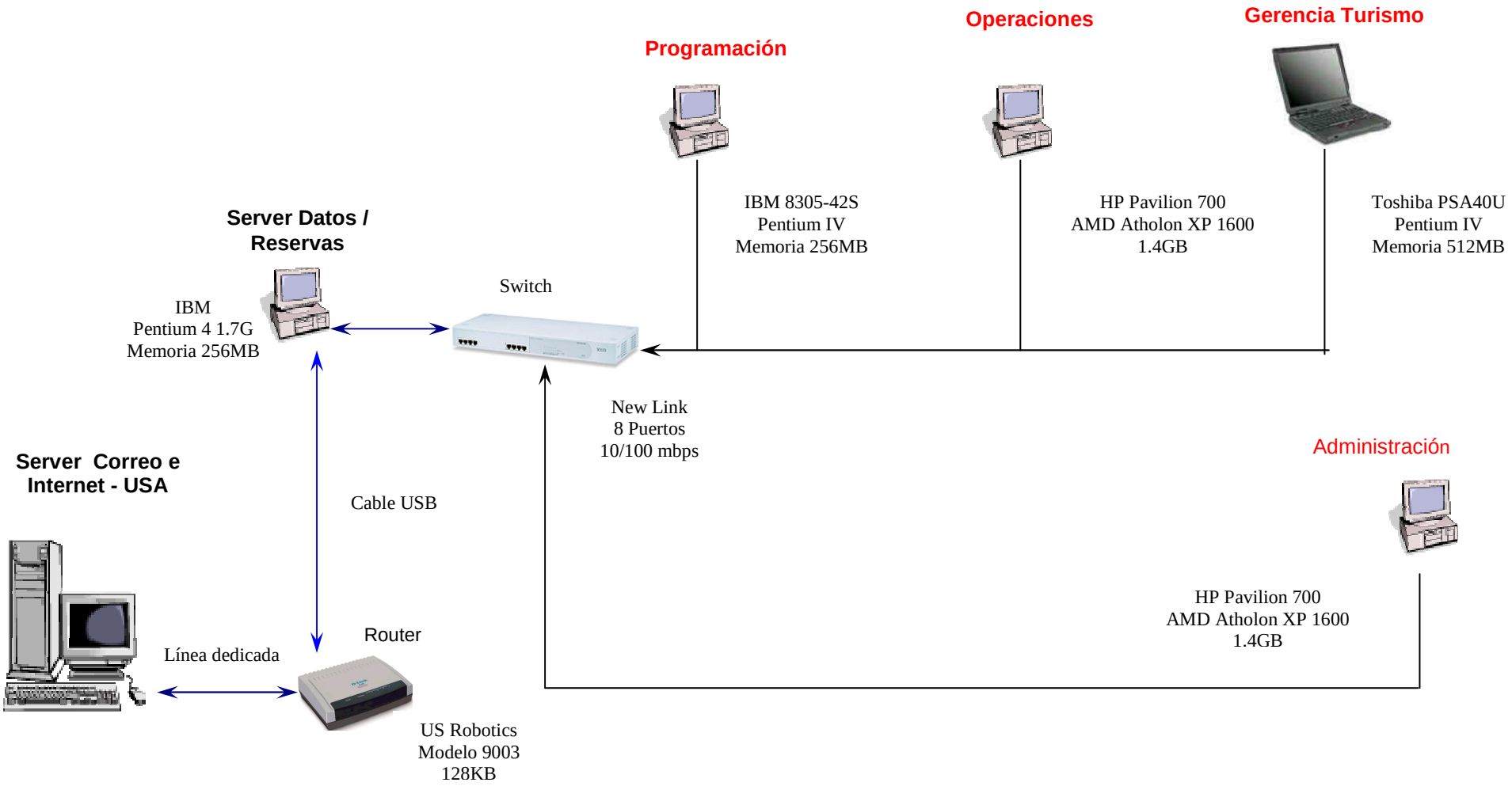
ESQUEMA DE RED QUIMBAYA TOURS "*CHILE*"



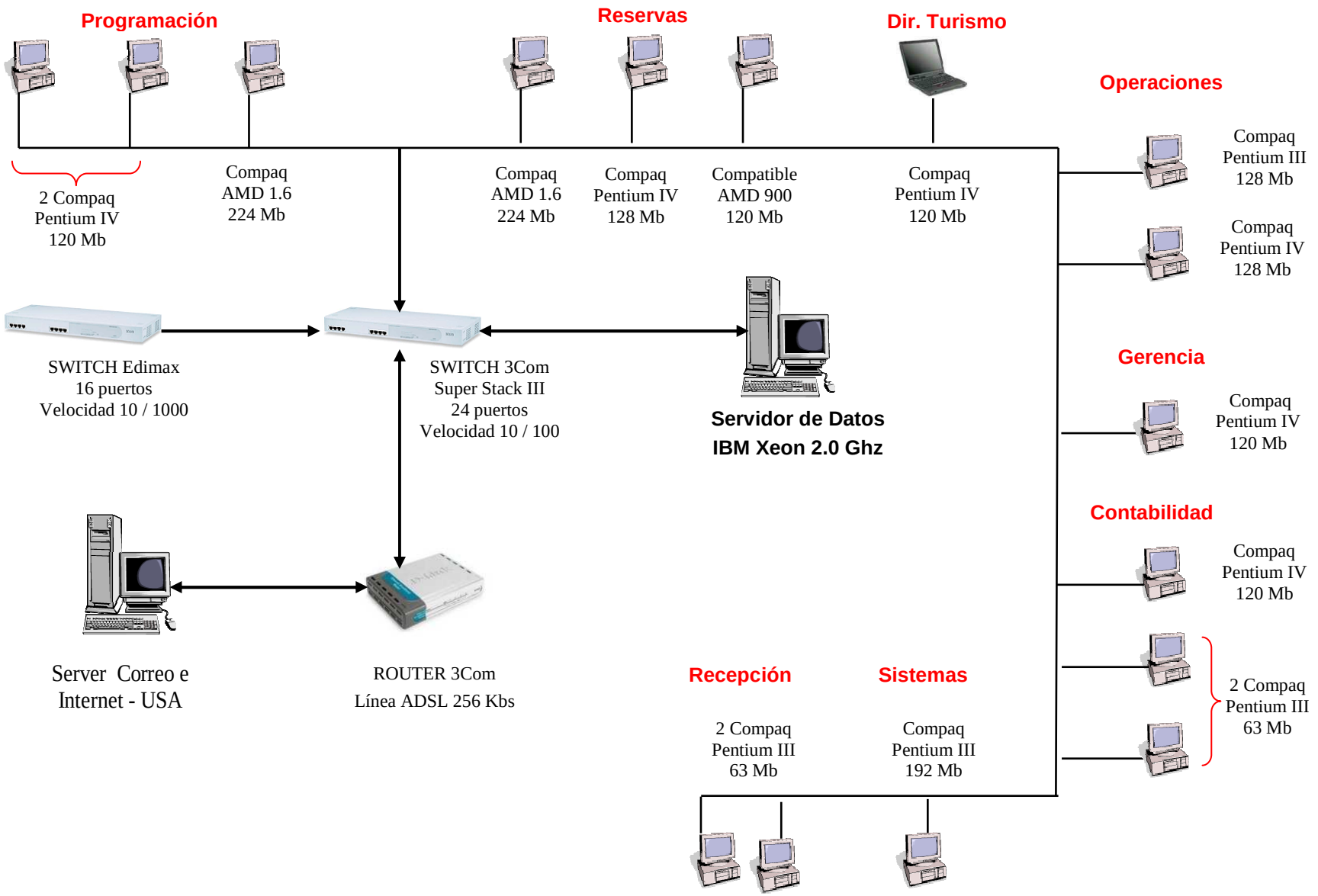
ESQUEMA DE RED QUIMBAYA TOURS "*ECUADOR*"



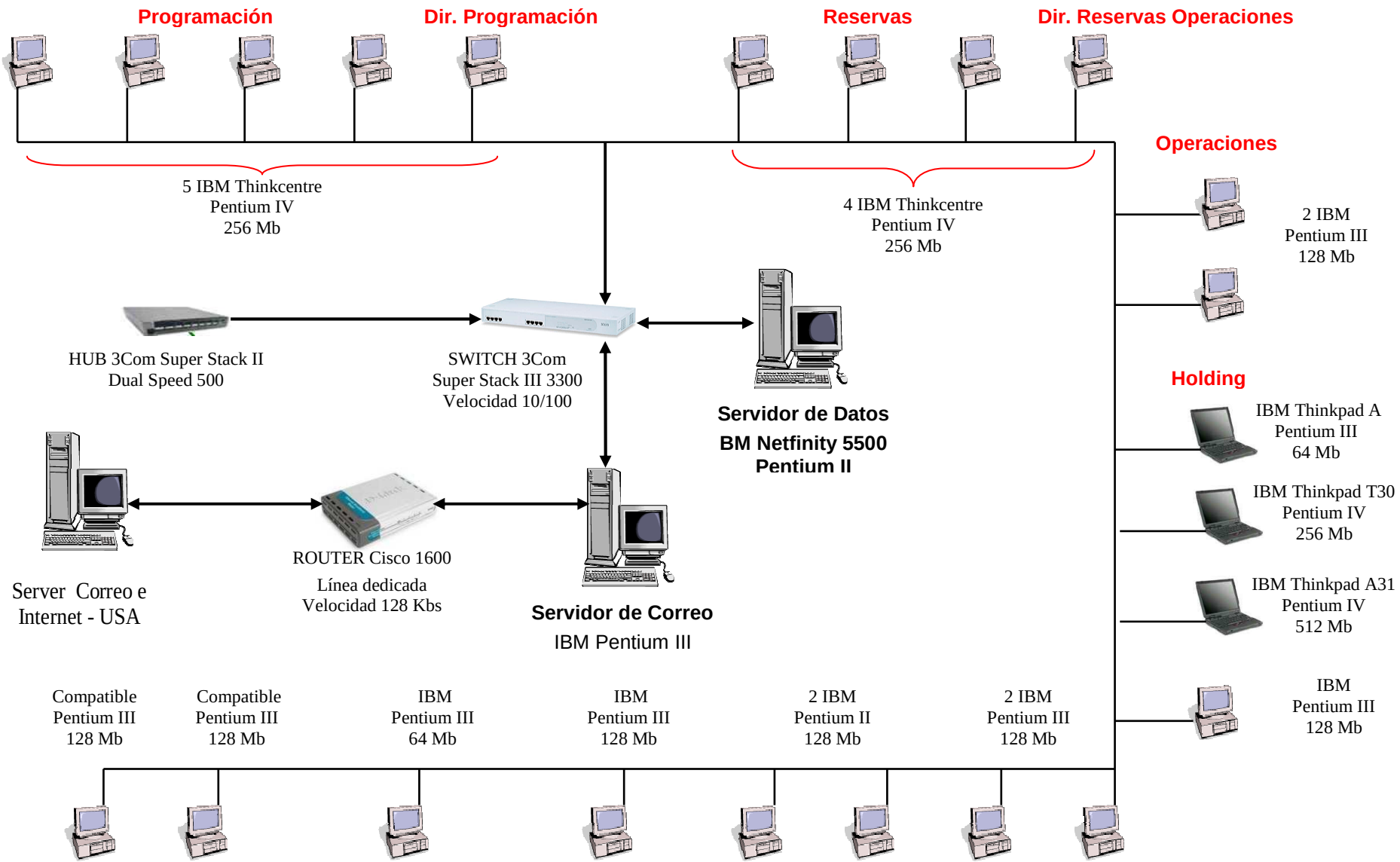
ESQUEMA DE RED QUIMBAYA TOURS "*GUATEMALA*"



ESQUEMA DE RED QUIMBAYA TOURS "*MÉXICO*"



ESQUEMA DE RED QUIMBAYA TOURS "*PERÚ*"



CAPÍTULO III

FUNDAMENTO TEÓRICO

3.1. TRANSMISIÓN DE DATOS

Cuando se establece una comunicación se está compartiendo información, ésta puede ser local o remota.

La ***transmisión de datos*** es el intercambio de información entre dos dispositivos a través de algún medio de comunicación como un cable.
La transmisión de datos es local si los dispositivos de comunicación están en el mismo edificio o en un área geográfica restringida y se considera remota si están separados por una distancia considerable.

3.1.1 CARACTERÍSTICAS

La efectividad del sistema de comunicaciones depende de tres características fundamentales:

a. ***Entrega:*** entregar los datos en el destino correcto, estos deben ser recibidos por el dispositivo o usuario adecuado y solamente por éste.

b. ***Exactitud*****:** los datos no deben ser alterados en la transmisión, si esto ocurre, son incorrectos y no se pueden utilizar.

c. ***Puntualidad*****:** los datos entregados tarde son inútiles. En el caso del vídeo, el audio y la voz, la entrega puntual significa entregar los datos a medida que se producen, en el mismo orden y sin un retraso significativo. Este tipo de entregas se llaman transmisión en tiempo real.

3.1.2 COMPONENTES

Un sistema de transmisión de datos está formado por cinco componentes:

a. ***Mensaje:*** es la información (datos) a comunicar. Puede estar formado por texto, gráficos, sonido, vídeo o cualquier combinación de los anteriores.

b. ***Emisor:*** es el dispositivo que envía los datos del mensaje. Puede ser una computadora, una estación de trabajo, una videocámara y otros muchos.

c. ***Receptor:*** es el dispositivo que recibe el mensaje. Puede ser una computadora, estación de trabajo, teléfono, televisión y otros.

d. ***Medio:*** camino físico por el cual viaja el mensaje. Puede estar formado por un cable de par trenzado, coaxial, de fibra óptica, un láser u ondas de radio (terrestres o microondas de satélite).

e. ***Protocolo:*** conjunto de reglas que gobiernan la transmisión de datos. Representa un acuerdo entre los dispositivos que se comunican. Sin un protocolo dos dispositivos pueden estar conectados pero no comunicados, igual que una persona que habla español no puede ser comprendida por una que sólo hable japonés.

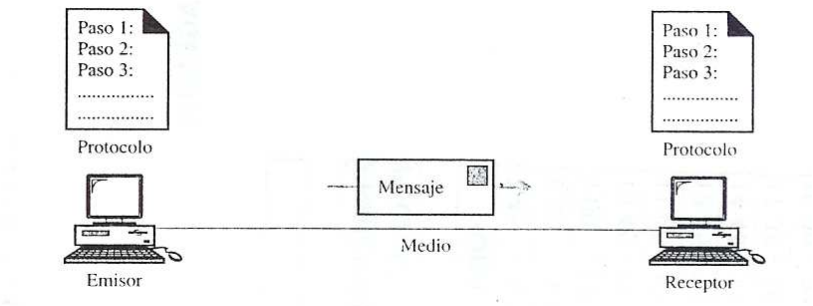


Fig. 3.1 Componentes de un Sistema de Transmisión de Datos

3.1.3 IMPORTANCIA DE LA TRANSMISIÓN DE DATOS

Las actividades a las que se ven sometidas cada vez más las redes de las empresas, involucran la necesidad de contar con grandes anchos de banda, para la transmisión de datos.

Actualmente la rentabilidad de un negocio se define por su planeación para reducir costos de operación al máximo para tener márgenes de utilidad extraordinarios.

La reducción de costos no se aplica solamente a redes locales, sino a redes corporativas con oficinas en diversas regiones, pues el costo de los enlaces dedicados que sirven para conectar sus redes WAN[1], tienen una renta muy elevada.

Para reducir estos costos se aprovechan las ventajas de los enlaces compartidos como Frame Relay[2], y/o Internet, mediante las llamadas Redes Virtuales Privadas (VPN's) minimizando costos por interconexión.

[1] WAN, Wide Area Network, Redes de Área Amplia
[2] Frame Relay, Red troncal de área amplia que conecta redes de área local.

Para evitarse esos costos, se trata de integrar voz y datos sobre una sola red, migrando hacia sistemas de Voz IP[3], y aprovechando el enlace con el que se cuente, PDH[4] Frame Relay, o Internet para estas aplicaciones.

3.2. REDES

Una Red de computadoras es una colección de estándares, basadas en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio y recursos, sin sacrificar velocidad, costo o maniobrabilidad.

Se puede decir también que una red es un conjunto de dispositivos (a menudo llamado nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo canales de comunicación.

[3]Voz IP, transmisión de voz en tiempo real sobre protocolo IP
[4] PDH, Jerarquía digital plesíncrona es una técnica de transferencia de datos para redes de cable de cobre.

3.2.1 CRITERIOS PARA EL DISEÑO DE REDES

Para que sea considerada efectiva y eficiente, una red debe satisfacer:

a. ***Prestaciones:*** se pueden medir de muchas formas incluyendo el tiempo de tránsito y el tiempo de respuesta. El tiempo de tránsito es el necesario para que un mensaje viaje de un dispositivo a otro y el de respuesta es el tiempo transcurrido entre una petición y una respuesta. Las prestaciones de una red dependen de factores como:

- ***Número de usuarios:*** la existencia de un gran número de usuarios concurrentes puede retrasar el tiempo de respuesta en una red no diseñada para coordinar gran volumen de tráfico. El diseño de una red se basa en una estimación del número medio de usuarios que estarán comunicados al mismo tiempo. Sin embargo, en los periodos pico de carga, el número real de usuarios puede exceder con mucho la media y por tanto causar una disminución de las prestaciones. La forma en que una red responde a la carga es una medida de su rendimiento.
- ***Tipo de medio de transmisión:*** el medio define la velocidad a la cual se pueden enviar los datos a través de una conexión (tasa de datos).
- ***Hardware:*** el tipo de hardware incluido en la red afecta tanto a la velocidad como a la capacidad de transmisión de la misma. Una

computadora de alta velocidad con una gran capacidad de almacenamiento da lugar a mejores prestaciones.

- ***Software:*** el software utilizado para procesar los datos en el emisor, el receptor y los nodos intermedios afecta también a las prestaciones de la red. Un software bien diseñado puede acelerar el proceso de transmisión y hacer que ésta sea más efectiva y más eficiente.

b. ***Fiabilidad:*** además de tener en cuenta la exactitud de la entrega, la fiabilidad de la red se mide por:

- ***Frecuencia del fallo:*** todas las redes fallan ocasionalmente. Sin embargo, una red que falla a menudo es muy poco útil.
- ***Tiempo de recuperación de una red después de un fallo:*** una red que se recupera rápidamente es más útil que una que no lo hace, pues representa un ahorro considerable en tiempo y dinero al restaurar el servicio rápidamente.
- ***Catástrofe:*** las redes deben estar protegidas de eventos catastróficos tales como fuego, terremotos y robos. Una protección adecuada contra un daño imprevisto, es tener copias de respaldo de software de la red.

c. ***Seguridad:*** los aspectos de seguridad de la red incluyen proteger los datos contra:

- ***Accesos no autorizados:*** los datos sensibles deben estar protegidos frente a accesos no autorizados. La protección incluye los códigos y contraseñas de identificación de los usuarios y las técnicas de cifrado.
- ***Virus:*** debido a que la red es accesible desde muchos puntos, puede ser susceptible de sufrir ataques de virus de computadoras. Una buena red está protegida ante estos ataques mediante mecanismos de software y hardware diseñados específicamente para este propósito.

3.2.2. CLASES DE RED

3.2.2.1 Redes de Área Local (LAN, *Local Area Network*)

La importancia de las LAN reside en que en un principio se pueda conectar un número pequeño de computadoras que puede ser ampliado a medida que crecen las necesidades del cliente o de la empresa. Las redes locales se caracterizan por:

- Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo.
- Ser un medio de comunicación común a través del cual se pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo.
- En la mayoría de los casos, las LAN's están contenidas dentro de una reducida área física, que puede ser un edificio de oficinas, una oficina

concreta de ese edificio, una empresa, una universidad, etc. mediante cables de conexión normales.

B Una distancia entre estaciones de trabajo relativamente corta, entre unos metros y varios kilómetros, aunque la distancia puede ser mucho mayor utilizando dispositivos de transmisión especiales.

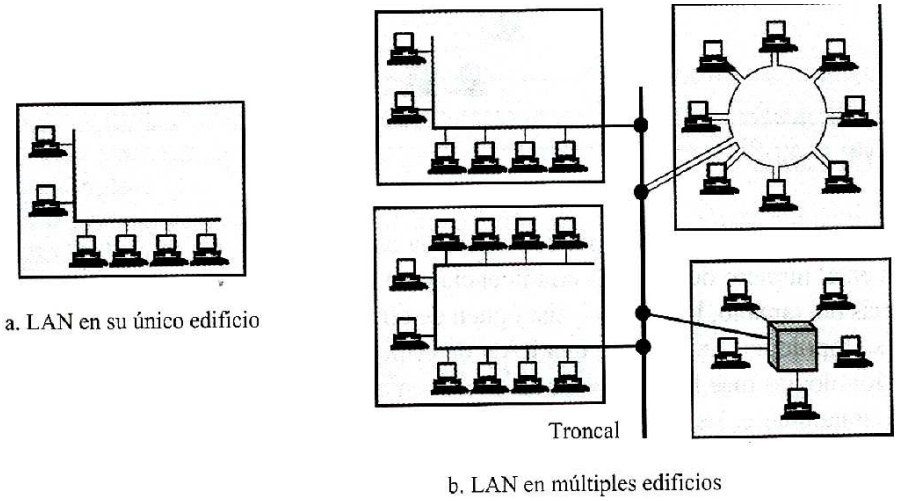


Fig. 3.2 Red de Área Local (LAN)

3.2.2.2 Redes de Área Metropolitana (MAN, *Metropolitan Area Network*)

Este tipo de red ha sido diseñada para que se pueda extender la conexión a lo largo de una ciudad entera. Puede ser una red única, como una red de televisión por cable, o puede ser una forma de conectar un cierto número de LAN en una red mayor, de forma que los recursos puedan ser compartidos de LAN a LAN y de dispositivo a dispositivo.

Para intercambiar datos, se pueden conectar de forma privada utilizando cables, encaminadores [5] o pasarelas [6]. Sin embargo, si necesitan conectarse en un área geográfica más grande, la conexión a través de una infraestructura privada, es impracticable.

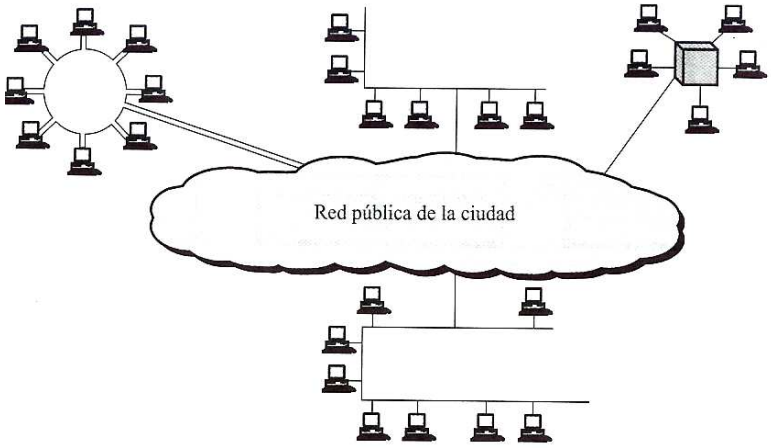


Fig. 3.3 Red de Área Metropolitana (MAN)

3.2.2.3 Redes de Área Amplia (WAN*, Wide Area Network*)

Proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de vídeo sobre grandes áreas geográficas que pueden extenderse a un país, un continente, o incluso el mundo entero.

[5] Encaminador, dispositivo de interconexión que conecta dos o más redes y reenvía paquetes de una red a otra.
[6] Pasarela, dispositivo que conecta dos redes diferentes que utilizan protocolos de comunicación diferentes.

Las WAN pueden utilizar dispositivos de comunicación públicos, alquilados o privados, habitualmente en combinaciones, y además pueden extenderse a lo largo de un número de kilómetros ilimitado.

Entre las formas más comunes de interconectar redes WAN se encuentran los enlaces privados como lo son: Frame Relay, ATM[7] y VPN's. Cada una de estas formas de interconexión requiere de un tercero, que es el proveedor del enlace, el cual cobra una renta por su uso y mantenimiento. Pero también se puede interconectar mediante redes públicas compartidas, como es el caso del Internet.

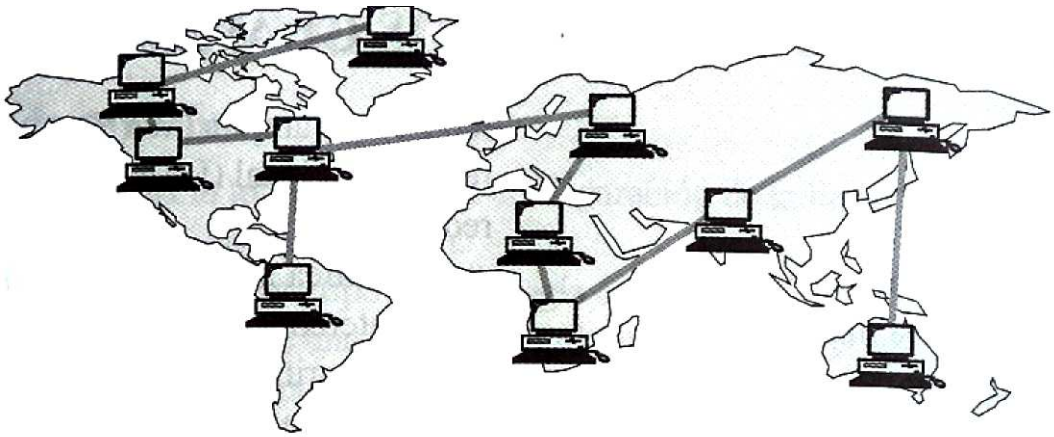


Fig. 3.4 Red de Área Amplia (WAN)

3.2.2.4 Redes Inalámbricas (WIRELESS)

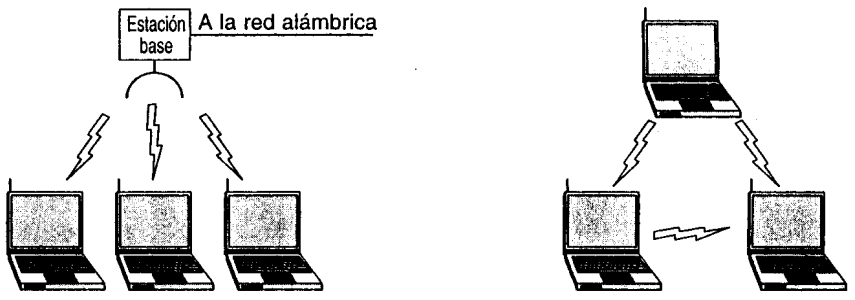
[7] ATM, tecnología Cell Relay para conmutación y transporte de diferentes tipos de información como voz, video y datos.

Estas redes son útiles en lugares en donde por alguna razón no se pueda tender cableado, operan generalmente en el rango de frecuencia de 2.4 GHz, que se encuentra disponible para uso industrial, científico y médico.

Una de sus limitantes, es la distancia máxima a la que se puede encontrar el equipo del *Access Point*[8] (91 m), para poder tener un buen servicio.

La velocidad de acceso es de 11 Mbps, la cual disminuye dependiendo del número de usuarios y la distancia hasta el access point. .Sin embargo, esto se soluciona colocando varios access points estratégicamente distribuidos,

de manera que la señal no se pierda al estar en movimiento y pueda pasar de un punto de acceso a otro cuando el equipo se desplace.



(a) Con una estación base **(b) De equipo a equipo**

Fig. 3.5 Redes Inalámbricas (WIRELESS)

[8] Access Point, dispositivo que brinda direcciones que identifican al usuario de un protocolo.

3.2.2.5 Frame Relay (Retransmisión de Tramas)

Frame Relay se puede utilizar como red troncal de área amplia de bajo costo para conectar redes de área local que no necesitan comunicaciones en tiempo real pero que pueden enviar datos a ráfagas.

La tecnología de Frame Relay transfiere la información en unidades de longitud variable conocidas como ***"frames"*** y suele emplearse como tecnología de acceso en los extremos o periferia de la red.

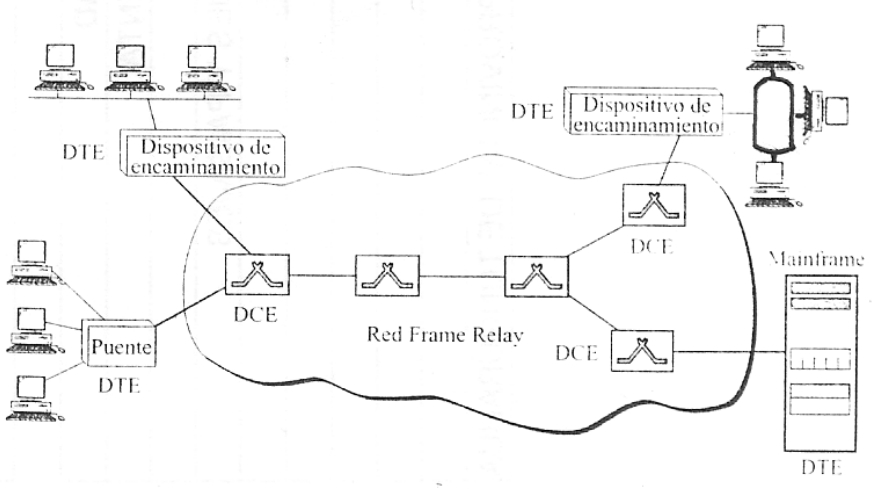


Fig. 3.6 Red Frame Relay

Frame Relay se ha mostrado muy útil en la interconexión de redes LAN (una aplicación con un volumen de negocios muy importante) porque la mayor parte de éstas redes emplean unidades de transmisión de datos de

tamaño variable al igual que el frame de Frame Relay, lo que simplifica la transferencia de datos.

a. Ventajas:

- Ofrece mayores velocidades (1,524 Mbps y más recientemente 44,476 Mbps).
- Opera sólo en el nivel físico y de enlace de datos. Esto significa que puede utilizarse fácilmente como red troncal para ofrecer servicios a protocolos que ya tienen un nivel de red.
- Permite datos a ráfagas. Los usuarios no necesitan adherirse a una velocidad fija.
- Es menos cara que otras WAN tradicionales.

b. *Desventajas*:

- Aunque algunas Frame Relay operan a 44,376 Mbps, ésta velocidad no es suficientemente alta para protocolos que requieren mayor velocidad.
- Permite tramas de longitud variable pero esto puede crear retardos variables a diferentes usuarios.
- Debido a los retardos variables que no están bajo el control del usuario, Frame Relay no es adecuada para enviar datos sensibles a los retardos, como vídeo o audio de tiempo real.

3.2.2.6 ATM (Retransmisión de Celdas) y sus Celdas de 53 bytes

La tecnología de *Cell Relay*[9], cuya representación más importante es la tecnología ATM (*Asynchronous Transfer Mode*) transfiere la información en unidades de longitud fija denominadas celdas ("*cells*") y suele emplearse como una tecnología común para la conmutación y transporte de una variedad de tipos de información.

ATM ofrece una mayor velocidad al emplear una unidad de tamaño fijo denominada celda (53 bytes), lo que simplifica el procesamiento a nivel de los nodos, haciéndolo predecible y eficiente.

ATM es más adecuada para aplicaciones y sistemas con altos volúmenes de transmisión de datos de medios combinados, en particular: datos, voz y audio.

Ofrece velocidades de acceso en el rango de 155 Mbps hasta 2,4 Gbps., esto nos indica que ATM es capaz de trabajar con anchos de banda más grandes que Frame Relay.

[9] Cell Relay, tecnología que transfiere la información en unidades de longitud fija llamadas celdas.

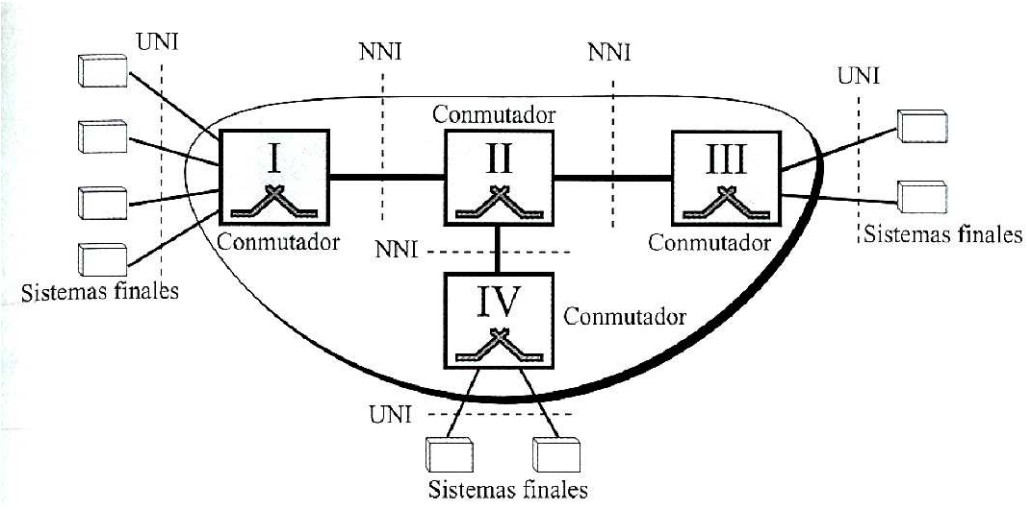


Fig. 3.7 Arquitectura de una Red ATM

3.2.2.7. DSL (Línea de Abonado Digital)

La ***línea de abonado digital*** (**DSL,** *Digital Subscription Line*) es una tecnología nueva que usa las redes de telecomunicaciones existentes, como la línea telefónica de bucle local, para conseguir entrega de datos, voz, vídeo y multimedia con alta velocidad.

3.2.2.7.1 ADSL (Línea de Abonado Digital Asimétrica)

La ***línea de abonado digital asimétrica*** (**ADSL**, *Asymmetric Digital Subscriber Line*) proporciona tasas de bits mayores en la dirección de entrada (desde la central telefónica a la casa del abonado), que en la dirección de salida (desde la casa del abonado a la central telefónica).

ADSL divide el ancho de banda de un cable de par trenzado (1 MHz) en tres bandas. La *primera*, para el servicio telefónico regular (POTS). La *segunda*, para la comunicación de salida. Y la *tercera*, para comunicación de entrada.

Algunas implementaciones ocultan la banda de entrada y salida para proporcionar más ancho de banda en la dirección de entrada.

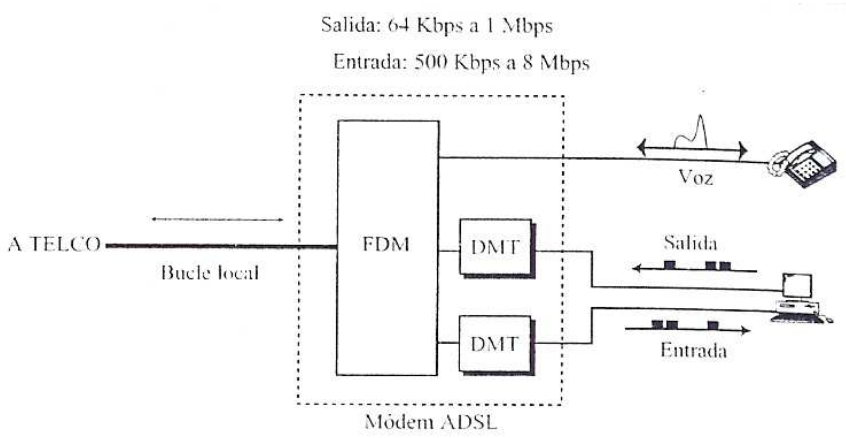


Fig. 3.8 Módem ADSL

3.2.2.8 RDSI (*Red Digital de Servicios Integrados*)

La red de servicios integrados (RDSI, ó ISDN *Integrated Services Digital Network*) es un conjunto de protocolos que combinan los servicios de transporte de datos y la telefonía digital, la idea principal es digitalizar la red telefónica para permitir la transmisión de audio, video y texto a través de las líneas telefónicas existentes.

RDSI proporciona conectividad digital de extremo a extremo entre un equipo local y un equipo o red remotos mediante una línea telefónica local para la conexión a la red.

Brinda a los usuarios servicios digitales completamente integrados, los que se pueden agrupar en tres categorías:

- ***Servicios Portadores:*** ofrecen un medio para transferir información (voz, datos y video) entre usuarios, sin que la red manipule el contenido de la misma.
- ***Teleservicios:*** la red puede cambiar o procesar el contenido de la información. Dependen de las facilidades de los servicios portadores y se han diseñado para acomodar las necesidades de usuarios sin que éstos tengan que preocuparse de los detalles del proceso.
- ***Servicios Suplementarios:*** son aquellos que proporcionan funciones adicionales a los servicios portadores o teleservicios.

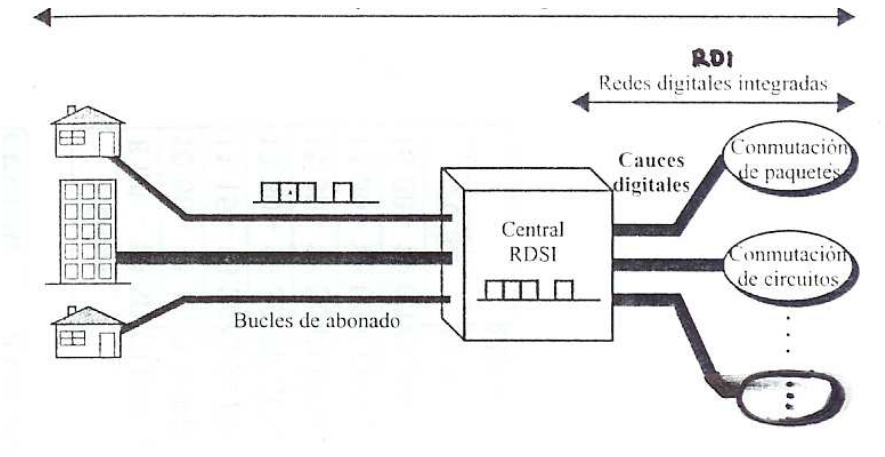


Fig. 3.9 (Red Digital de Servicios Integrados (RDSI)

3.2.2.9. Internet

Internet no es del todo una red, sino un inmenso conjunto de redes diferentes que usan ciertos protocolos comunes y proporcionan ciertos servicios comunes.

En la actualidad el número de usuarios de Internet es desconocido, pero es cierto que son cientos de millones en todo el mundo.

Una máquina está en Internet si ejecuta la pila de protocolos de TCP/IP[10], tiene una dirección IP[11] y puede enviar paquetes IP[12] a todas las demás máquinas en Internet.

[10] Protocolo TCP/IP, conjunto de protocolos de cinco niveles que define el intercambio de transmisiones en Internet.
[11] Dirección IP, direcciones utilizadas en el nivel de red para definir de forma única una estación en Internet que utiliza el protocolo TCP/IP.

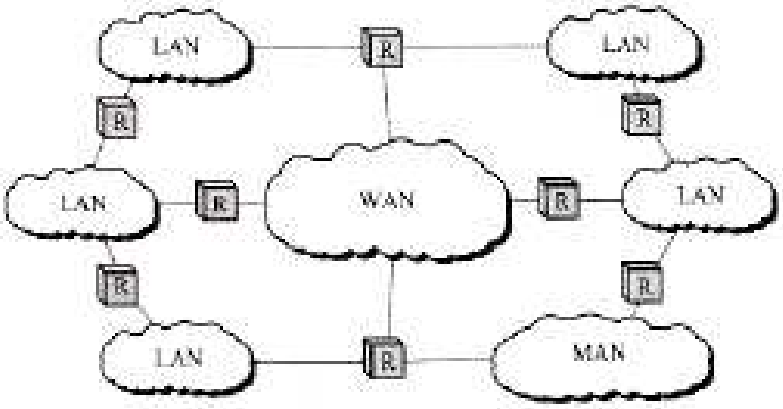


Fig. 3.10 Internet

[12] Paquetes IP, unidad de datos que tiene una dirección IP.

CAPÍTULO IV

TECNOLOGÍA VPN

4.1. REDES PRIVADAS VIRTUALES (VPN'S)

4.1.1 RESEÑA HISTÓRICA

La tecnología en nuestros días avanza muy rápidamente y en los últimos años las redes se han convertido en un factor crítico para cualquier organización.

Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial.

Surge entonces el término Red Privada Virtual (**VPN**, del inglés ***Virtual Private Network***) y ya forma parte del lenguaje común de la industria de las telecomunicaciones y redes de servicios, aunque su significado puede variar según cómo se lo utilice.

4.1.2 CONEXIONES REMOTAS

Cuando se desea enlazar oficinas centrales con alguna sucursal y oficinas remotas se tienen tres opciones:

a. ***Módem:*** su desventaja es el costo de la llamada, que es por minuto conectado, además puede ser una llamada de larga distancia, a parte no cuenta con la calidad y velocidad adecuadas.

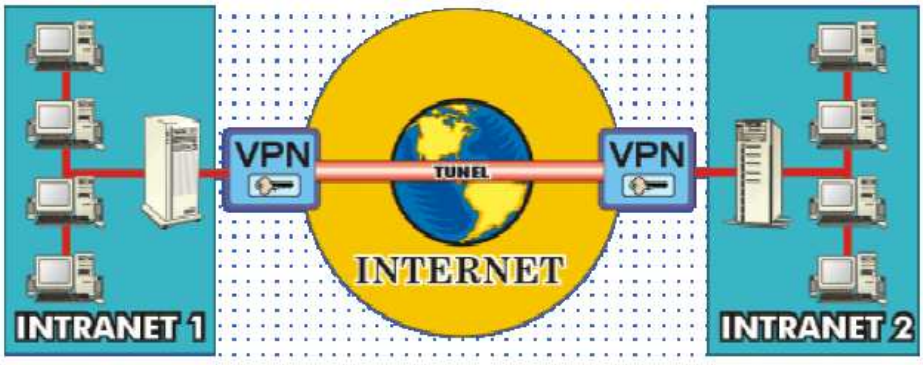
b. ***Línea Privada:*** se tiene que tender el cable para la empresa ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado.

c. ***VPN:*** los costos son bajos porque sólo se realizan llamadas locales, además de tener la posibilidad de que los datos viajen encriptados y seguros, con buena calidad y velocidad.

4.1.3 DEFINICIÓN DE VPN

Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública. Para el usuario una VPN se ve como cualquier otra red privada, es por eso que se la denomina virtual, sin embargo ésta comparte su tráfico con otros cientos o miles de usuarios al mismo tiempo.

a)



b)

Fig. 4.1 Ejemplos de Red Privada Virtual

A pesar de ser compartida, tiene todas las características de una red privada, como lo es el acceso limitado a usuarios autorizados.

La tecnología VPN permite que una compañía se conecte a las sucursales o a otras compañías (extranets) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras. Está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas y operaciones con una alta interdependencia de socios, donde los trabajadores deben conectarse a recursos centrales y entre sí.

De esta manera, las empresas se pueden enfocar a su negocio principal con la garantía de que nunca se comprometerá su accesibilidad y que se instalen las soluciones más económicas.

Las VPN pueden enlazar las oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos de Internet como IP[1], IPSec[2], Frame Relay, ATM.

[1] Protocolo IP, protocolo entre redes de nivel de red que gobierna la transmisión sin conexión a través de redes IP.
[2] IPSec, protocolo de nivel de red que permite la transferencia de información segura sobre una red IP.

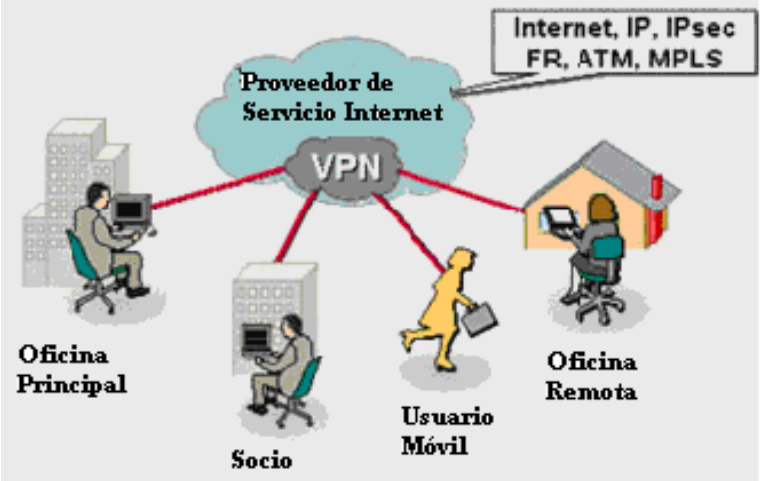


Fig. 4.2 VPN de oficina corporativa

En base a esta definición, se puede decir que las redes públicas de X.25[3], ATM o Frame Relay son VPN's de Nivel 2[4].

Sin embargo, la tecnología emergente de Redes Privadas Virtuales se basa en los protocolos de Nivel 3 (*Nivel de Red del modelo OSI*[5]), más específicamente en IP. Esta tecnología busca implementar redes de servicios privadas particionando redes públicas o compartidas de IP, donde la red pública IP más conocida y difundida mundialmente es Internet.

Una VPN permite además, que la comunicación se realice por un canal seguro que cumpla estos requisitos:

[3] X.25, primera red de datos pública orientada a la conexión.
[4] VPN de nivel 2, VPN que trabajan en el nivel de enlace de datos del modelo OSI.
[5] Modelo OSI, modelo de Interconexión de Sistemas Abiertos, es una arquitectura por niveles para el diseño de sistemas de red que permite la comunicación.

- ***Confidencialidad:*** los datos que circulan por el canal sólo pueden ser leídos por emisor y receptor. La manera de conseguir esto es mediante técnicas de encriptación.
- ***Autenticación:*** emisor y receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Esto puede conseguirse mediante firmas digitales o aplicando mecanismos desafío−respuesta[6].
- ***Integridad:*** Debe garantizarse la integridad de los datos, esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se puede utilizar firmas digitales.
- ***No repudio (Firma Digital):*** Cuando un mensaje va firmado, el que lo firma no puede negar que el mensaje lo emitió él.

4.1.4 FUNCIONAMIENTO BÁSICO DE UNA VPN

[6] Mecanismo desafío-respuesta, mecanismo de preguntas y respuestas que permiten verificar a un usuario

Los datos generalmente encriptados parten del servidor dedicado, hasta llegar a un firewall[7], que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan a nube de Internet donde se genera un túnel[8] dedicado únicamente para que los datos, con mayor velocidad y ancho de banda, lleguen a su vez al firewall remoto y terminen en el servidor remoto.

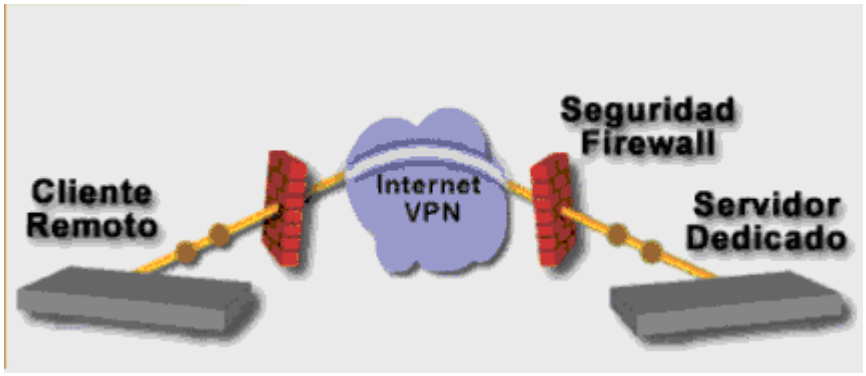


Fig. 4.3 Funcionamiento de una VPN

4.1.5. ESCENARIOS TÍPICOS DONDE SE USAN VPNS

Hay algunos modelos de empresa en los que la tecnología VPN proporciona notables beneficios.

4.1.5.1 Branch offices o Agencias

[7] Firewall, cortafuegos, es una combinación de hardware y software que provee seguridad al sistema.
[8] Túnel, camino lógico a través del cual se encapsulan paquetes que viajan en una red intermedia.

Se trata de localizaciones de una misma empresa separadas geográficamente y que necesitan intercambiar datos entre ellas, acceder a una misma base de datos, aplicación, etc. La VPN permite conexiones confidenciales de una red a otra.

4.1.5.2 Extranets

Empresas diferentes, pero que trabajan conjuntamente, pueden compartir información de manera eficiente y segura entre sus respectivos negocios sin que terceras personas tengan acceso a los datos compartidos. En este caso también se interconectan las redes corporativas, aunque sólo se da acceso a un segmento de cada red.

4.1.5.3 Usuarios móviles

Aquí se habla de trabajadores que pasan gran parte del tiempo fuera de la empresa, como *teletrabajadores* o los llamados "*road warriors*", personas que necesitan acceder a la red de la empresa pero que están constantemente cambiando de ubicación. Se permite a un ordenador personal o portátil el acceso a la red corporativa, manteniendo la privacidad.

4.1.6 OBJETIVOS DE UNA VPN

Los objetivos básicos que persigue una empresa cuando decide instalar un servidor de VPN en una o varias de sus sedes son los siguientes:

- Proporcionar movilidad a los empleados.
- Acceso a la base de datos central sin utilización de operadores telefónicos.
- Interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública.
- Intercambio de información en tiempo real.
- Correo electrónico corporativo.
- Acceso remoto a la información corporativa.
- Teletrabajo.
- Flexibilidad y facilidad de uso.
- Obtención de la máxima velocidad de transferencia de datos usando con eficiencia los recursos empleados.
- Fácil adaptación a las nuevas tecnologías.

4.1.7 REQUERIMIENTOS BÁSICOS DE LAS VPN

Al implantar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma que

deberá permitir la libertad para que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la LAN así como las oficinas remotas se conecten entre sí para compartir recursos e información.

Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet, por lo tanto, debe proporcionar lo siguiente:

a. ***Autenticación de usuario:*** verifica la identidad de un usuario y restringe el acceso de la VPN a usuarios autorizados. Además proporciona registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.

b. ***Administración de dirección:*** asigna una dirección al cliente en la red privada, y se asegura de que las direcciones privadas se mantengan así.

c. ***Encriptación de datos:*** los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

d. ***Administración de llaves:*** genera y renueva las llaves de encriptación para el cliente y para el servidor.

e. ***Soporte de protocolo múltiple:*** maneja protocolos comunes utilizados en las redes públicas; estos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (*PPTP*[9]) o un Protocolo de túnel de nivel 2 (*L2TP*[10]) cumple con todos estos requerimientos básicos y, aprovecha la amplia disponibilidad de Internet a nivel mundial.

4.1.8. TIPOS DE REDES PRIVADAS VIRTUALES

4.1.8.1. De acuerdo con el Servicio de Conectividad

4.1.8.1.1 VPN de Acceso Remoto (*Remote Access VPN's*).

Provee acceso remoto a la intranet o extranet corporativas a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado ISDN[11], DSL[12], cable, o IP para la conexión segura de usuarios móviles o sucursales remotas a los recursos corporativos.

[9] PPTP, Point to Point Tunneling Protocol, protocolo de túneles que utiliza una conexión TCP.
[10] L2TP, Layer 2 Tunneling Protocol,protocolo de túneles sobre Internet.
[11] ISDN, conjunto de protocolos que combinan los servicios de transporte de datos y la telefonía digital

Características:

- Llamadas locales o gratuitas
- Propagación del acceso
- Instalación y soporte del PS (Proveedor del Servicio)
- Acceso único al nodo central (elimina la competencia por puertos)
- Tecnologías de acceso ISDN y DSL
- Movilidad IP
- Seguridad reforzada por el cliente

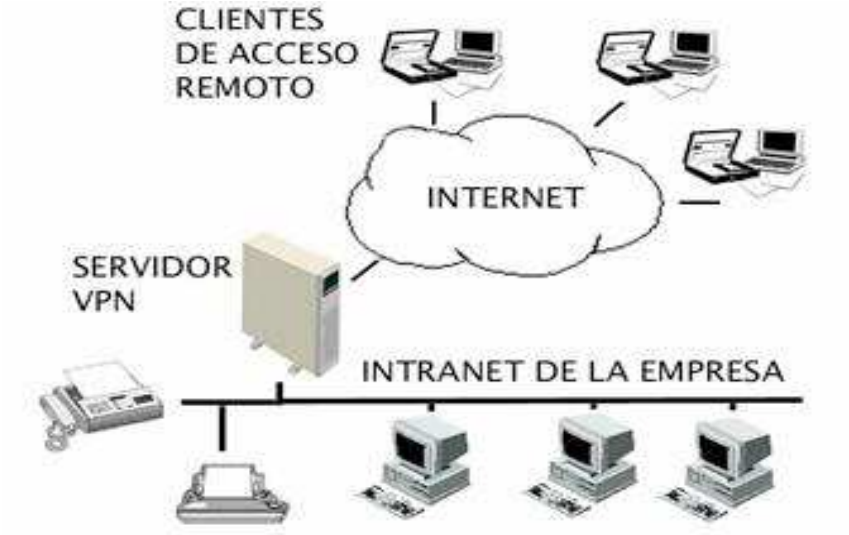


Fig. 4.4 VPN de Acceso Remoto

4.1.8.1.2 VPN de Intranet

[12] DSL, usa las redes de telecomunicaciones como la línea telefónica para conseguir entrega de datos, voz, vídeo y multimedia con alta velocidad

Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad.

Como característica se puede decir que extiende el modelo IP a través de la WAN compartida.

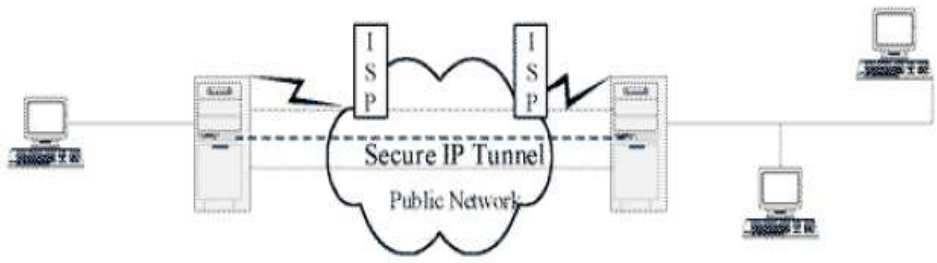


Fig. 4.5 VPN de Intranet

4.1.8.1.3 VPN de Extranet

Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública.

Extiende la conectividad a proveedores y clientes sobre una infraestructura compartida usando conexiones virtuales dedicadas.

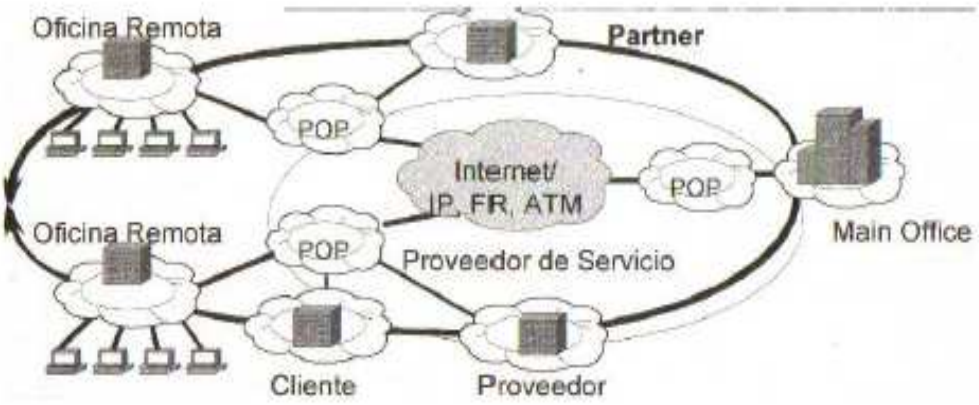


Fig. 4.6 VPN de Extranet

4.1.8.1.4 VPN Dinámica

Permite la posibilidad de intercambio de información en diversos formatos, gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc. Proporciona una seguridad importante para la empresa.

Se ajusta dinámicamente a un grupo heterógeneo de usuarios. Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado.

Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

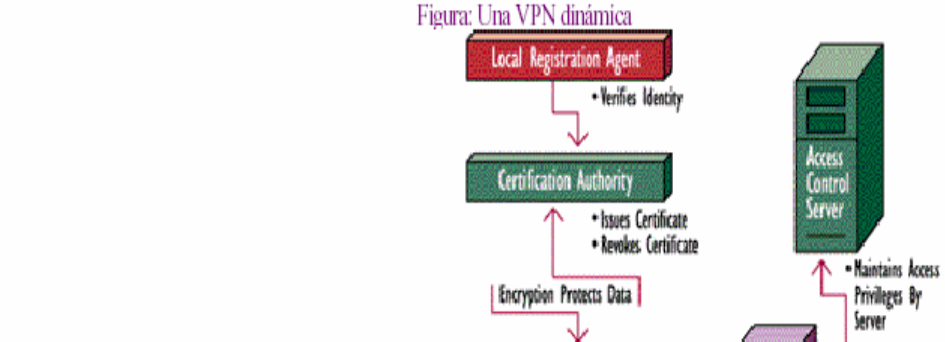


Fig. 4.7 VPN Dinámica

4.1.8.2. De acuerdo con el Medio de Conectividad

4.1.8.2.1 Sistemas basados en Hardware

Los sistemas basados en hardware, son routers[13] que encriptan. Son seguros y fáciles de usar. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación.

4.1.8.2.2 Sistemas basados en Cortafuegos

Estos se implementan con software de cortafuegos (*firewall*). Tienen las ventajas de los mecanismos de seguridad que utilizan estos dispositivos, incluyendo el acceso restringido a la red interna. Satisfacen los requerimientos de autenticación segura, aumentan la protección y les

provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN.

El rendimiento decrece, ya que no se tiene hardware especializado de encriptación.

4.1.8.2.3 Sistemas basados en Software

Son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados, o los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN's ofrecen el método más flexible en cuanto al manejo de tráfico, este puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en las VPN por hardware, todo el tráfico es enrutado por el túnel.

4.1.9. INTERNET COMO MEDIO DE INTERCONEXIÓN

Hay una gran variedad de redes públicas que pueden ser empleadas para hacer conexiones de VPN's, pero la más interesante es por supuesto el

[13] Router, dispositivo que se conecta a dos o más redes y reenvía los paquetes de una red a otra.

Internet, debido a que esta red pública global se encuentra en todos lados, y es aquí donde se encuentran desarrollándose más las VPN's actualmente.

Las razones principales que han impulsado el desarrollo de VPN's en Internet son que:

- Las compañías han empezado a apreciar el valor del Internet como medio de promoción y venta de servicios y productos.
- Muchas organizaciones ven al Internet como un medio alterno de comunicación.
- La implantación de una VPN por este medio implica ventajas y desventajas en comparación con otros medios de interconexión, es por ello que antes de realizar cualquier cosa es recomendable hacer un estudio a fondo.

4.1.9.1 Ventajas

- Reducción de los gastos de enlaces RAS[14] de larga distancia.
- Reducción de las llamadas de larga distancia de los usuarios móviles.
- Disminución en la inversión del equipo de comunicaciones.
- Disminución en los costos de administración de la infraestructura.
- Seguridad en la conexión (alta redundancia[15]).

[14] RAS, Servidor de Acceso Remoto donde se ejecuta el servicio de enrutamiento y acceso remoto.
[15] Redundancia, bits añadidos a un mensaje para el control de errores.

4.1.9.2 Desventajas

- Necesidad de una implantación robusta en el aspecto de seguridad.
- No hay soporte técnico en la totalidad de enlace.
- Incertidumbre en la ruta que siguen los paquetes de información.
- Necesidad de compatibilidad de la red privada con TCP/IP.

4.1.9.3 Puntos de oportunidad

- Acceso remoto a la red local de la oficina y utilización de los recursos computacionales.
- Grupos de trabajo (Cliente - Proveedor - Distribuidor).
- Comunicación de nuevas oficinas con la red corporativa.
- Mayor redundancia que los enlaces dedicados.
- Educación y capacitación a distancia (Multicast IP[16]).
- Comercio electrónico.

Un aspecto importante que soporta la decisión de implantar o no una VPN utilizando Internet es la Calidad de Servicio (*QoS*[17]) que involucra la capacidad de la infraestructura para ofrecer un determinado nivel de servicio medido en términos de un máximo de latencia[18], de un ancho de banda[19] garantizado o de una combinación de ambos.

[16] Multicast IP, permiteque varias copias de un mismo paquete sean enviadas a un grupo de receptores IP.
[17] QoS, Qualite of Service, en ATM un conjunto de atributos relacionados con las prestaciones de una conexión.
[18] Latencia, hace referencia a un retardo en la propagación.
[19] Ancho de banda, capacidad de transmisión de información de una línea o una red.

En este aspecto, Internet presenta su principal desventaja ya que por ser una red global, de alta redundancia no se tiene control alguno sobre la trayectoria que puedan seguir los paquetes que viajan a través de ésta.

4.1.10. FUNCIONAMIENTO BÁSICO DE UNA VPN DE INTERNET

a. El usuario remoto marca a su ISP[20] local y se conecta a la red del ISP de forma usual.

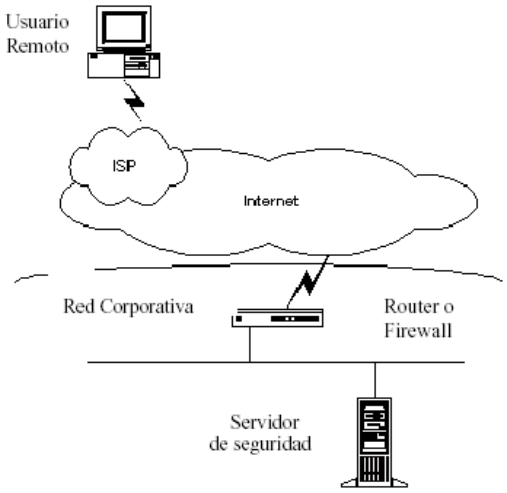


Fig. 4.8 Conexión Usuario – ISP

b. Cuando se desea conectarse a la red corporativa, el usuario inicia el túnel mandando una petición al servidor de seguridad destino de la red

[20] ISP, Internet Service Provinder, Proveedor de Servicio de Internet.

corporativa. Este servidor autentica al usuario y crea el otro extremo del túnel.

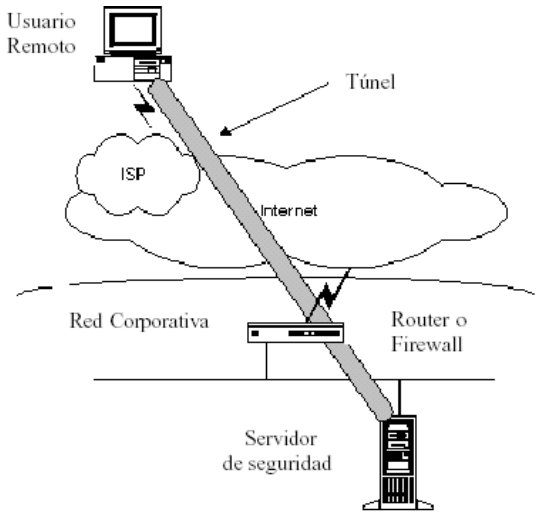


Fig. 4.9 Creación del túnel

c. El usuario comienza a mandar datos a través del túnel, los cuales son encriptados[21] por el software de la VPN antes de ser enviados sobre la conexión del ISP.

[21] Encriptados, datos codificados.

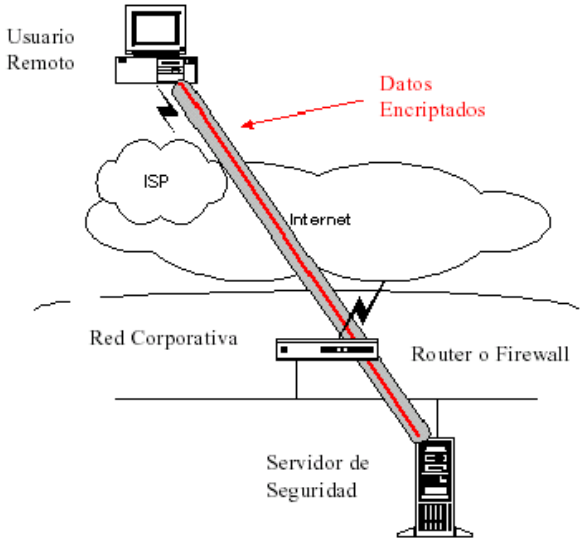


Fig. 4.10 Envío de datos encriptados

d. El servidor de seguridad en el destino recibe los datos y los desencripta, posteriormente envía estos paquetes a la red corporativa. Cualquier información que sea mandada de regreso al usuario remoto es también encriptada antes de ser enviada sobre Internet.

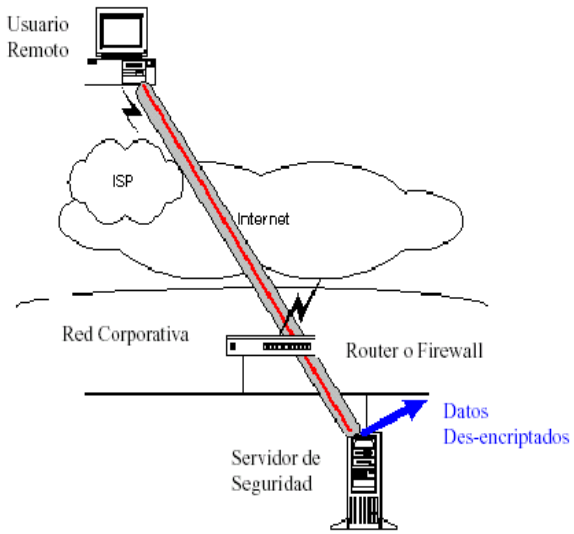


Fig. 4.11 Desencriptación de datos

La siguiente figura ilustra como se puede utilizar el software de VPN desde cualquier lugar por medio de cualquier servicio dial-in[22] del ISP que exista.

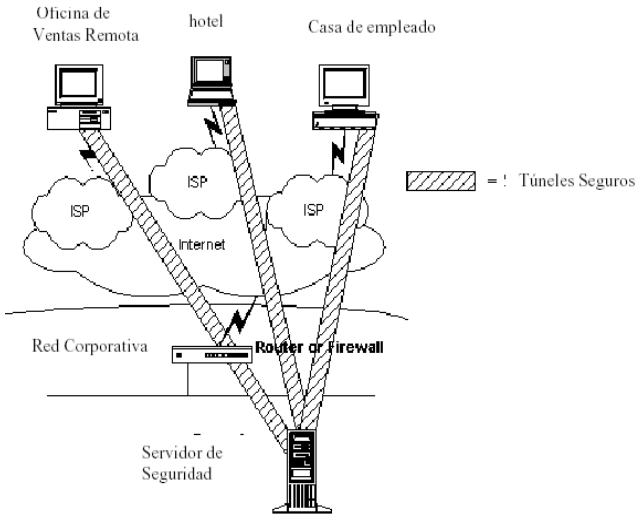


Fig. 4.12 VPN a través del Internet

4.2. TECNOLOGÍA DE TÚNEL

4.2.1 DEFINICIÓN DE TÚNEL

La técnica usada para envolver las datos de carga encriptados, con cabeceras que pueden ser leídas es lo que se llama túnel; en otras palabras es un camino lógico a través del cual se encapsulan paquetes que viajan en una red intermedia.

4.2.2 TUNNELING

Es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo.

Tunneling incluye todo el proceso de encapsulado[23], desencapsulado y transmisión de las tramas[24].

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos, a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños. El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

---

[22] Dial-in, inicio de una conexión telefónica.
[23] Encapsulado, técnica en la que la unidad de datos de un protocolo se sitúa dentro de la porción del campo de datos de otro protocolo.
[24] Trama, grupo de bits que representan un bloque de datos.

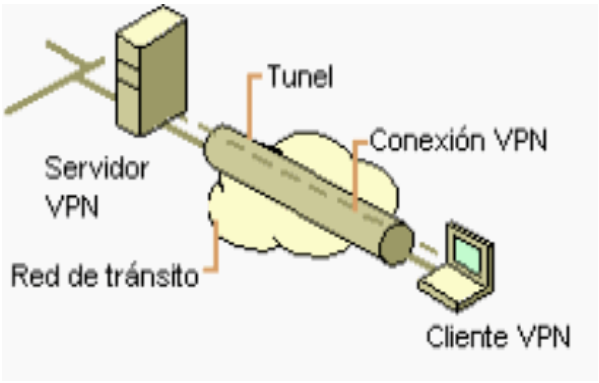


Fig. 4.13 Tunneling

4.2.3 ASPECTOS BÁSICOS DE TÚNELES

Trabajar en un sistema de túnel es una forma de utilizar una infraestructura de la red para transferir datos de una sobre otra; los datos que serán transferidos (o *carga útil*) pueden ser los *frames*[25] (o *paquetes*) de otro protocolo.

En lugar de enviar un frame a medida que es producido por el nodo de origen, el protocolo de túnel lo encapsula en un encabezado adicional. Éste proporciona información de entubamiento de manera que la carga útil encapsulada pueda viajar a través de la red intermedia. De esta manera, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red. Cuando los frames encapsulados llegan a su destino sobre la red se desencapsulan y se envían a su destino final.

Las tecnologías de túnel existen desde hace tiempo. Algunos ejemplos incluyen:

- ***Túneles SNA sobre intranets IP***: cuando se envía tráfico de la Arquitectura de la Red del Sistema (*SNA, Simple Network Architecture*) a través de una intranet IP corporativa, el frame SNA se encapsula en un encabezado UPN[26] e IP.
- ***Túneles IPX para Novell NetWare, sobre intranets IP:*** cuando un paquete IPX[27] se envía a un servidor NetWare[28] o ruteador IPX, el servidor o ruteador añaden al paquete un encabezado UDP[29] e IP y luego lo envía a través de una intranet IP. El ruteador destino quita este encabezado UPD e IP, y dirige el paquete al destino de IPX.

En los últimos años, sin embargo se han desarrollado nuevas tecnologías como son:

- ***Protocolo de Túnel de Punto a Punto (PPTP):*** permite que se encripte el tráfico IP, IPX o NetBEUI[30], y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.

---

[25] Frame, paquete de datos de longitud variable.
[26] Encabezado UPN, encabezado en el nombre de cuenta del usuario.
[27] IPX, Internet Packet Exchange, protocolo de NetWare encargado de enrutar y dirigir dentro de las LANs.
[28] Servidor NetWare,
[29] UDP, protocolo de nivel de transporte de TCP/IP no orientado a conexión.

- ***Protocolo de Túnel de Nivel 2 (L2TP):*** permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas[31] punto a punto, como IP, X.25, Frame Relay o ATM[32].
- ***Modo de Túnel de Seguridad IP (IPSec):*** deja que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP, para enviarse a través de una red corporativa IP o una red pública IP como Internet.

4.2.4 FUNCIONAMIENTO DE LOS TÚNELES

Para las tecnologías de túnel de Nivel 2[33] como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales deben estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión.

Las tecnologías del túnel de Nivel 3[34] asumen que todos los aspectos relacionados con la configuración, han sido manejados por procesos manuales; por lo que para estos protocolos no existe una fase de mantenimiento de túnel.

---

[30] NetBeui, Protocolo de red de Conexiones de red de Microsoft, utiliza enrutamiento de origen Token Ring.
[31] Datagrama, en conmutación de paquetes, una unidad de datos independiente.
[32] X.25, Frame Relay y ATM, redes orientadas a la conexión.
[33] Nivel 2, nivel de datos del Modelo OSI.

Para los protocolos de Nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir un túnel.

Cuando se establece el túnel, es posible enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

4.2.5. REQUERIMIENTOS BÁSICOS DEL TÚNEL

4.2.5.1 Autenticación de usuario

Los protocolos de túnel Nivel 2 heredan los esquemas de autenticación del usuario de PPP. Mientras que los esquemas de Nivel 3 suponen que los puntos finales son bien conocidos (y autenticados) antes de que se estableciera el túnel.

La mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios; como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de

[34] Nivel 3, nivel de red del Modelo OSI.

seguridad cuando se combina el IPSec con un protocolo de Nivel 2, como el L2TP.

4.2.5.2 Soporte de Token[35]

Al utilizar el protocolo de autenticación extendible (**EAP**[36], *Extensible Autentication Protocol*), los protocolos de túnel Nivel 2 pueden ofrecer soporte a una amplia variedad de métodos de autenticación, incluidas contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares, por ejemplo, IPSec define la autenticación de los certificados de llaves públicas[37].

4.2.5.3 Asignación dinámica de direcciones

El túnel de Nivel 2 da soporte, a la asignación dinámica de direcciones de clientes, basadas en un mecanismo de negociación de protocolos de control de la red; en general los esquemas del túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel.

4.2.5.4 Compresión de datos

[35] Token, medio compartido en donde se transfiere mensajes especiales reservados.
[36] EAP, es una extensión del PPP que admite métodos de autenticación arbitrarios.
[37] Llaves públicas, en cifrado, llave o clave conocida por todos.

Los protocolos de túnel Nivel 2 proporcionan soporte a esquemas de compresión basados en PPP. En el Nivel 3 no existen formas de compresión, sin embargo se están investigando mecanismos similares para su uso.

4.2.5.5 Encriptación de datos

Los protocolos de Nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio.

La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.

4.2.5.6 Administración de llaves

Un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la autenticación del usuario y luego las renueva en forma periódica. IPSec negocia explícitamente una llave común durante el intercambio y también las renueva de manera periódica.

4.2.5.7. Soporte de protocolo múltiple

El sistema de túnel de Nivel 2 da soporte a protocolos múltiples de carga útil, lo que facilita a los clientes tener acceso a sus redes corporativas utilizando IP, IPX, NetBeui, etc.

En contraste, los protocolos de túnel Nivel 3, como el IPSec, por lo común dan soporte sólo a redes objetivo que utilizan el protocolo IP.

4.2.6. PROTOCOLOS DE TÚNEL

Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel.

La tecnología de túnel se puede basar en el protocolo de Nivel 2 o Nivel 3; estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI).

Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes.

4.2.6.1 Point to Point Protocol (PPP)

De este protocolo dependen en gran medida los protocolos de tunneling del nivel 2. PPP fue diseñado para el envío de datos a través de conexiones

punto a punto. Encapsula los paquetes IP, IPX y NetBeui en frames PPP y luego los transmite a través de un link punto a punto.

Existen cuatro fases de negociación en una sesión PPP. Cada una de éstas debe completarse satisfactoriamente antes que la conexión PPP esté lista para transferir datos. Estas fases son:

- Establecimiento de link PPP.
- Autenticación de usuario.
- Control de remarcado.
- Llamado de protocolos.

4.2.6.2 Point to Point Tunneling Protocol (PPTP)

Encapsula los frames de PPP en datagramas de IP para la transmisión sobre redes IP como Internet. Utiliza una conexión TCP para el mantenimiento del túnel y una encapsulación de ruteo genérica. Los datos de los frames de PPP pueden ser encriptados y/o comprimidos.

4.2.6.3 Layer 2 Tunneling Protocol (L2TP)

Este protocolo es una combinación de PPTP y L2F. Es un protocolo de red que encapsula frames de PPP para ser enviados sobre redes IP, X.25, Frame Relay o ATM. Cuando se configura para usar IP como su datagrama de transporte, L2TP puede ser utilizado como un protocolo de

túneles sobre Internet. L2TP. También puede ser utilizado directamente sobre varios medios de uso en WAN como Frame Relay, sin la necesidad de una capa de transporte IP.

4.2.6.4 Layer 2 Forwarding (L2F)

Consiste en un protocolo de transmisión que permite que los servidores de acceso dial-up[38] conjunten la información en frames de PPP y lo transmitan sobre los puntos de la WAN. El servidor L2F luego abre los paquetes y los coloca en la red. En contraste con PPTP y L2TP, L2F no tiene un cliente definido.

4.2.6.5 Internet Protocol Security (IPSec)

Es un protocolo del nivel 3 que permite la transferencia de información segura sobre una red IP.

Un aspecto importante de este protocolo es el hecho que define el formato de paquete para una red IP sobre el modo de túnel IPSec, el cual consiste en un túnel cliente y servidor los cuales están ambos configurados para utilizar IPSec y un mecanismo de encriptación negociado.

[38] Acceso dial-up, acceso vía telefónica.

IPSec tiene las siguientes características y limitantes:

- Soporta solamente tráfico IP
- Es controlado por una póliza de seguridad, una serie de reglas de filtrado.

4.2.7. MODO DEL TÚNEL DE SEGURIDAD DE PROTOCOLOS PARA INTERNET

El IPSec es un estándar de protocolo de Nivel 3 que da soporte a la transferencia protegida de información a través de una red IP.

IPSec además de su definición de mecanismos de encriptación para tráfico IP, define el formato de paquete para un modo de túnel IP sobre IP, generalmente referido como un modo de túnel IPSec.

Un túnel IPSec consiste en un cliente y un servidor, ambos configurados para utilizar los túneles IPSec y un mecanismo negociado de encriptación. Utiliza el método de seguridad negociada para encapsular y encriptar todos los paquetes IP, para una transferencia segura a través de una red privada o pública IP.

Así, se vuelven a encapsular la carga útil encriptada con un encabezado IP de texto. Y se envía en la red para su entrega a un servidor de túnel. Al

recibir este datagrama, el servidor del túnel procesa y descarta el encabezado IP de texto y luego desencripta su contenido, a fin de recuperar el paquete original IP de carga útil. Enseguida, se procesa el paquete IP de carga útil de manera normal y se enruta su destino en la red objetivo.

4.2.7.1 Funciones y limitaciones del modo de túnel IP

- Sólo da soporte a tráfico IP ·
- Funciona en el fondo de la pila IP por tanto, las aplicaciones y los protocolos de niveles más altos heredan su comportamiento.
- Está controlado por una *política de seguridad* (un conjunto de reglas que se cumplen a través de filtros). Esta política de seguridad establece los mecanismos de encriptación, de túnel y los métodos de autenticación disponibles, en orden de preferencia. Tan pronto como existe tráfico, ambos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán.
- Posteriormente, se encripta todo el tráfico y luego se envuelve en un encabezado de túnel.

4.2.8. TIPOS DE TÚNEL

4.2.8.1 Túneles Voluntarios

Un túnel voluntario ocurre cuando, una estación de trabajo o un servidor de entubamiento utilizan el ***software del cliente del túnel***, a fin de crear una conexión virtual al servidor del túnel objetivo; para lograr esto se debe instalar el protocolo apropiado de túnel en la computa*dora* ***cliente.***

En determinadas situaciones, el cliente debe establecer una conexión de marcación con el objeto de conectarse a la red antes de que el cliente pueda establecer un túnel (éste es el caso más común). Un buen ejemplo es el usuario de Internet por marcación, que debe marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un entubamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este es el caso para un cliente en una LAN corporativa, que inicia, un túnel para alcanzar una subred privada u oculta en la misma LAN

4.2.8.2 Túneles Obligatorios

Diversos proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel

para la computadora del cliente es conocida como Procesador Frontal (**FEP**[39]).

Para realizar esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y ser capaz de establecer el túnel cuando se conecte la computadora cliente. En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS[40] activado por los túneles en el ISP.

Esta configuración se conoce como "***túnel obligatorio***" debido a que el cliente está obligado a utilizar el túnel creado por FEP cuando se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel.

En los túneles obligatorios, la computadora cliente realiza una conexión única PPP, y cuando un cliente marca en el NAS se crea un túnel y todo el tráfico se enruta de manera automática a través de éste. Es posible configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel.

[39] FEP, procesador cliente que se dedica por completo al control de la información transmitida.
[40] NAS ,Netware Access Server, Servidor de Acceso a la Red.

De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) a fin de alcanzar un destino no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel.

CAPÍTULO V

SEGURIDAD

5.1 RESEÑA HISTÓRICA

Las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. El número de atacantes va en aumento y están más organizados, ya que día a día van adquiriendo habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La rápida expansión y popularización de Internet, que es un entorno abierto en su sentido más amplio, ha convertido a la seguridad en redes en uno de los tópicos más importantes dentro de la Informática Moderna. Con tal nivel

de interconexión, los virus y los hackers[1] se instalan a sus anchas, aprovechando las deficientes medidas de seguridad tomadas por administradores y usuarios a los que esta nueva revolución ha cogido por sorpresa.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

5.2. CAUSAS QUE COMPROMETEN LA SEGURIDAD

Existen varias causas por medio de las cuales se ve comprometida la seguridad de la información:

[1] Hacker, vándalo informático.

- ***La deficiencia en los equipos respectivos de soporte*** como UPS[2], plantas eléctricas de respaldo, unidades de copias de seguridad, reguladores de corriente y estrategias óptimas para su aplicación, son indispensables a la hora de evaluar la seguridad de la información en una empresa.
- ***La ingeniería social*****,** consiste en conseguir las claves de los usuarios haciéndose pasar por el administrador de la red o un simple operador de su proveedor de servicio a Internet.
- ***El espionaje industrial***, las diferentes técnicas como entrar de manera ilegal a un servidor del DoD (*Department of Defense from USA*) o a la misma NASA, hasta hace unos años eran simplemente libretos de ciencia ficción ya han dejado de serlo para ser completamente posibles.
- ***Aprovechar la deficiente administración de una red***, ningún sistema operativo esta eximido de fallos de seguridad, por lo tanto los administradores deben estar atentos ante las noticias actualizadas de fallos de seguridad en cada uno de los programas que tienen en sus servidores, para instalar las actualizaciones de los mismos o en su defecto los parches que controlan los fallos de seguridad a esos programas.
- ***Los virus*** en muchas ocasiones acompañan a programas vistosos y útiles, pero poco confiables en Internet.

[2] UPS, sistema de alimentación ininterrumpida.

- ***Fallos de seguridad en programas***, cuando el fallo no es intencional se les llama bug[3] y cuando es intencional se les llama puertas traseras o troyanos[4], dependiendo del servicio que preste dicho fallo.
- ***Los vándalos informáticos***, como los cracker, son los más peligrosos y directamente responsables de la seguridad computacional.

5.2.1 DEFINICIÓN DE HACKER Y CRACKER

Se tienen varias definiciones del término "***hacker***", la mayoría de las cuales trata con la afición a lo técnico y la capacidad de deleitarse con la solución de problemas y a sobrepasar los límites. Los hackers construyeron Internet, hicieron del sistema operativo UNIX lo que es en la actualidad, hacen que funcione la WWW, etc.

El término "***cracker***" está asociado a personas que se divierten ingresando ilegalmente en computadoras y estafando al sistema de telefonía.

La diferencia básica está en que los hackers construyen cosas, los crackers las destruyen.

[3] Bug, virus informático.
[4] Puertas traseras o troyanos, programas que se enmascaran como otros para intentar dañar información o equipos.

5.3. TENDENCIAS DE SEGURIDAD

5.3.1 PROTECCIÓN DE LOS SISTEMAS DE TRANSFERENCIA O TRANSPORTE.

El administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible.

5.3.2 APLICACIONES SEGURAS EXTREMO A EXTREMO

La información a ser enviada por la red se la debe asegurar mediante un procedimiento de encapsulado previo al envío. De esta forma, la información puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Esta operación, puede usarse para abordar el problema de la seguridad en aplicaciones como correo electrónico, videoconferencia, acceso a bases de datos, etc.

En ambos casos, un problema de capital importancia es la gestión de ***passwords*** (contraseñas). Este problema es inherente al uso de la

Criptografía [5] y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. Otro no menos importante es el nivel de implicación de los usuarios con respecto a la seguridad de los datos que están manejando, que en la mayoría de los casos suele ser nulo.

5.4. SISTEMAS DE SEGURIDAD

5.4.1 SEGURIDAD FÍSICA

Tiene que ver con la protección física, y por ello, de la ubicación del sistema y de los datos. Se puede distinguir entre:

- ***Pasiva***, que protege de eventos como puedan ser variaciones ambientales de temperatura, humedad, caídas en el suministro eléctrico, desastres naturales, choques, inundaciones, explosiones, etc.
- ***Activa***, que pueden ser ataques terroristas, robos de información o del propio sistema, accesos no autorizados.

5.4.2 SEGURIDAD EN EL ACCESO AL SERVICIO

[5] Criptografía, forma de codificación de datos.

- ***Activa***, para no permitir el acceso a usuarios que no estén identificados e incluso prohibir el acceso a usuarios identificados que lo hagan desde direcciones de red no autorizadas.
- ***Pasiva,*** para emplear sistemas cortafuegos, proxys[6] y enmascaradores[7] de red, que son barreras más o menos sofisticadas de tipo software o hardware que se interponen entre la red y el sistema.

5.4.3 SEGURIDAD EN LAS COMUNICACIONES

Evita las escuchas de información no autorizadas, que tienen ver con el espionaje, cuya contramedida suele ser la protección, cifrado y/o Criptografía. En el caso de las comunicaciones es especialmente importante comprobar la seguridad en tres puntos vitales:

- ***La autenticación***, para comprobar que tanto el usuario y el proveedor del servicio son realmente quienes dicen ser.
- ***La confidencialidad*****,** para garantizar que los datos que se envían sólo serán conocidos por usuario y servidor; que nadie, en un paso intermedio pueda tener acceso a dicha información.

[6] Proxy, maneja el tráfico entre la red y los servidores de Internet.
[7] Enmascarador, dispositivo que extrae la dirección de red física a partir de una dirección IP.
[8] RAID, arreglo de discos.

- ***La integridad de los datos enviados*,** el servidor ha de estar seguro de que los datos recibidos son idénticos a los enviados, es decir, que no han sido modificados por el camino.

5.4.4 SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

En servicios críticos que implica la duplicidad de máquinas, software y naturalmente todo lo comentado hasta ahora. Este tipo de circunstancias se previene con las técnicas de alta disponibilidad.

5.4.5 SEGURIDAD Y PROTECCIÓN DE LOS DATOS

Engloba básicamente la salvaguarda y custodia de éstos. Para ello se emplean los muy conocidos sistemas redundantes o RAID[8], copias de seguridad y técnicas similares. Ésta es una parte importante y especialmente sensible, en temas de seguridad, como es el ataque por virus a los sistemas. Tampoco se puede olvidar de los bugs, de los sistemas operativos, las aplicaciones comerciales o los errores en el desarrollo de los sistemas.

[8] RAID, areglo de discos

5.5. PLAN DE SEGURIDAD

Un sistema de seguridad completo debe contar con la selección y diseño previo de las herramientas adecuadas, que sea capaz de responder favorablemente ante posibles negligencias de los usuarios, ataques malintencionados, y posibles catástrofes naturales.

Para esta labor es necesario que la organización que desee implantar un sistema de seguridad siga una metodología y cuente con un grupo de trabajo formado tanto por personal interno de la organización, como externo, si así fuese requerido o si la empresa no cuenta con personal calificado.

La metodología para implantar el plan de seguridad debería desarrollar en profundidad los siguientes puntos:

5.5.1 COMITÉ DE SEGURIDAD Y GESTIÓN DE RED

Formar un equipo que se encargue de definir los objetivos, establecer tareas, actividades y responsabilidades. Debería incluir representantes de cada área funcional de la organización.

5.5.2 EVALUACIÓN DE LA RED. ARQUITECTURA

Es el proceso de identificar y documentar toda la red, su topología[9], elementos y recursos. Este proceso generará las herramientas necesarias para establecer una política de seguridad efectiva.

5.5.3 ADMINISTRACIÓN DE LA RED Y MÉTODOS DE CONTROL DE ACCESO

Con esto, se pretende verificar como son tratadas las cuentas de usuarios y sus permisos. Esto revelará no sólo como están configurados los permisos de acceso, sino también saber si hay uno o varios administradores para cada tarea en particular.

También es necesario conocer como trabajan los controles de acceso desde los sistemas del usuario, incluyendo qué servicios se han activado después de identificarse en la red.

[9] Topología, manera en que los nodos están conectados unos con otros.

5.5.4 SISTEMAS DE CONTROL DE ACCESO

Una vez introducidos en la red firewalls, dispositivos de control de acceso, sistemas de detección de intrusos, etc., es necesario validar su configuración y funcionalidad.

Las diferentes configuraciones y mecanismos de los sistemas de control de acceso forman la base de la seguridad de la red.

5.5.5 SEGURIDAD EN LAS APLICACIONES INFORMÁTICAS

Se debe saber exactamente cuáles son las aplicaciones informáticas utilizadas en la organización y las vulnerabilidades de cada una de ellas.

5.5.6 ANÁLISIS DEL TRÁFICO DE LA RED

Un analizador de redes revelará qué tipo de tráfico hay en la red. Esto puede indicar, no sólo si las contraseñas pueden ser fácilmente robadas, sino que también ayudará a conocer el rendimiento y comportamiento de la red.

5.5.7 AUDITORÍA DE SEGURIDAD Y DETECCIÓN DE INTRUSIONES

Una auditoría de seguridad junto con los sistemas de detección de intrusos permitirá identificar vulnerabilidades en estos. Así se puede encontrar diversas maneras en las que los datos confidenciales podrían ser sustraídos.

También se pueden detectar posibles errores de diseño de la red. Para esto se deben usar las últimas herramientas de análisis de vulnerabilidades, cuyos resultados deberán tenerse en cuenta a la hora de reestructurar la red.

5.5.8 POLÍTICA DE SEGURIDAD DE RED

La política de seguridad ayudará a saber que tan preocupada e interesada está la organización acerca de la seguridad e integridad de sus datos. También puede clarificar objetivos organizacionales. Deberá ser la base para implementar los controles de seguridad que reduzcan las vulnerabilidades y riesgos.

5.5.9 POLÍTICA DE CONTROL DE VIRUS

Una política antivirus ayudará a prevenir pérdida de datos como consecuencia de infecciones de virus informáticos.

5.5.10 PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE CATÁSTROFES

Bien redactados y con los pasos y actuaciones bien claros, un Plan de Recuperación de datos minimizará el tiempo de malfuncionamiento de la red en caso de caída de los servidores, caída de la pasarela a Internet u otros dispositivos críticos.

5.6. RECOMENDACIONES PARA LOS USUARIOS DE LA RED

Cualquier usuario o administrador de una red computacional que siga las siguientes recomendaciones está procurando un nivel de seguridad alto, tanto para su información, como para la de sus compañeros de trabajo.

a. ***La contraseña es personal, no debe ser prestada*** bajo ninguna circunstancia. Hay que recordar que las contraseñas deben cambiarse periódicamente. No es recomendable utilizar contraseñas cortas, mínimo 8 caracteres y mucho menos palabras que se puedan encontrar

en algún diccionario o que tengan alguna relación con el dueño de la misma. Se sugiere que sean palabras sin sentido usando los caracteres especiales.

b. ***La utilización de los antivirus es importante***, se debe ejecutar por lo menos una vez al día a todo el disco duro del equipo, se pueden configurar para que se ejecuten al iniciar el equipo, además se debe vacunar todo diskette que se utilice, aunque sea de origen confiable. Sí ya se ha sido vacunado y se lo reutiliza en otro equipo se debe vacunarlo nuevamente. Hay que vacunar todos los archivos adjuntos a los correos y aquellos que se descarguen de la red.

c. ***Colocar el protector de pantalla protegido por contraseña***, ésta no debe ser igual a las anteriormente utilizadas, debido a que existen programas que logran descifrar la contraseña de los protectores de pantalla y de acceso a la red. No sobra colocar una contraseña en el boot de arranque[10], esto restringirá el acceso aunque se apague. No está de más que el equipo tenga una *llave física o hardkey*, la cual impedirá que cualquier persona pueda destaparlo, quitar la pila del

[10] Boot de arranque, archivo de inicio del Sistema.

CMOS[11] o el *jumper de la BIOS*[12] (*Basic Input utput System*) y modificar la contraseña.

d. Sí se comparte información en la red, se debe ***asegurar el dar los permisos estrictamente necesarios a los usuarios adecuados y por el mínimo tiempo posible***. Ya que al compartir la información con todos los permisos habilitados se corre el riesgo de perderla. Además existen programas especializados en descifrar las claves de directorios compartidos por contraseñas para luego colocar programas que se auto ejecuten desde allí y realizar alguna labor específica.

e. ***No se debe instalar programas no autorizados*** por el administrador de la red. Estos programas pueden ser ***troyanos*** (programas que prometen ser algo y realmente realizan otra cosa que compromete la seguridad del usuario) o ***puertas traseras*** (programas que permiten entrar al sistema ya vulnerado de manera más sencilla y reiterativa) que le dan acceso a los vándalos informáticos para realizar alguna labor concreta en la red.

[11] CMOS, RAM de configuración del computador.
[12] BIOS, informacise almacena en la memoria de sólo lectura de forma que se pueda ejecutar al encender el equipo

f. ***Si se maneja información secreta para la empresa, lo mejor es mantenerla encriptada*****,** en el disco duro local con una copia respectiva en el servidor. Lo mismo se aplica para el correo electrónico. No hay que olvidar asegurar la llave privada, si ésta se pierde es probable que la información sea descifrada.

g. ***Procurar que el equipo se encuentre en óptimas condiciones***, es decir que tenga buena ventilación, mantenimiento de hardware y software por personal autorizado de la empresa. No se debe desinstalar ni instalar ningún tipo de hardware sin autorización del administrador, ya que esto provocará cambios en la configuración del equipo corriendo el riesgo de perder la información.

h. Además de mantener copia de la información encriptada en el servidor. Se deben ***realizar copias de respaldo actualizadas*** de la información vital, que maneje en el disco duro y colocarla en un lugar seguro bajo llave y encriptada. En el caso que la información se guarde en un lugar fuera de la empresa bajo medidas extremas de seguridad, el administrador de la información de los usuarios debe ser el encargado de esta labor.

i. ***Mantener la información de la empresa en la misma y no transportarla a otro sitio diferente*** de ésta. Ya que se corre el riesgo de no tener las mismas precauciones de seguridad en otro sitio y por ende se estará atentando contra la seguridad de la información y de la empresa.

5.7 RECOMENDACIONES PARA EL ADMINISTRADOR DE LA RED

a. ***Establecer políticas de seguridad*** apropiadas para la red computacional de la empresa, creación de usuarios, manejo de contraseñas, instalación de hardware y software, perfiles de usuario estándar y minimizar la cantidad de cuentas de administradores de la red. Estrategias de contingencia en caso de pérdida de información de los usuarios o suspensión de los servidores de la empresa por alguna razón.

b. ***Implementar sistemas de seguridad para la red*** en cada uno de los servidores de la empresa utilizando firewalls, proxy, o filtros. Mantener un servidor de prueba en donde se pueda instalar y desinstalar los programas que se tiene, para realizar pruebas de seguridad a los programas que se usa. Identificar qué servidores deben pertenecer a la

red militarizada y cuáles no, esto se debe realizar para identificar los anillos de seguridad de la red.

c. ***Responder inmediatamente ante cualquier sugerencia o queja*** de un usuario con respecto a la seguridad de la información. Probablemente él haya detectado un fallo de seguridad importante ahorrándole tiempo y dinero a la empresa en solucionarlo.

d. Tratar de ***no sobrecargar los servidores*** asignándoles muchos servicios, esto baja el rendimiento y atenta contra la seguridad y la constancia de los servicios en los mismos. Ante cualquier tipo de falla de hardware o software se debe acudir inmediatamente al proveedor de servicio o al servidor BDC[13] (*Backup Domain Control*) de la empresa.

e. ***Implementar estrategias para la creación de las copias de respaldo*****,** mantener copias diarias, semanales, mensuales y anuales; además estas deben ser encriptadas y guardadas en lugares seguros como bancos o cajas de seguridad contra incendios en lugares fuera de la empresa y de extrema seguridad.

[13] Servidor BDC, Servidor de Dominios de Reserva, contiene toda la información de cuentas y directivas de seguridad del dominio.

f. ***Leer diariamente los logs***[14] que arroja el servidor, éstos muchas veces informan de accesos no permitidos en horas no acostumbradas. Es importante restringir el acceso al máximo de los usuarios de la red, eso incluye días a la semana, horas, directorios y sitios de trabajo.

g. La mejor auditoría de seguridad para la red de la empresa es el intento de violación de la seguridad de la misma, por lo que el administrador se debe ***convertir en el cracker de la empresa***, manteniéndose al día en nuevas estrategias de violación a las redes y aprendiendo más de los crackers.

h. Se ***debe tener la menor cantidad de puertos abiertos*** en los servidores. Estos pueden ser en cualquier momento puertas de acceso a los vándalos de la red. Existen programas que avisan en línea si algún puerto ha sido abierto de forma anormal o si alguien está conectado a alguno de ellos de forma fraudulenta. Hay que tener en cuenta que si se tiene instalado algún programa que ofrece un servicio innecesario se está dejando un puerto abierto el cual puede ser violentado.

i. ***El acceso al centro de cómputo*** donde se encuentran los servidores de la empresa, ***debe ser completamente restringido y auditado*** cada

[14] Logs archivos de texto que muestran el funcionamiento y la utilización del equipo en momentos específicos

instante. Se recomienda utilizar sistemas electrónicos para verificar el acceso al centro de cómputo.

5.8 SEGURIDAD EN VPN'S

Uno de los aspectos de mayor importancia a considerar al implantar una VPN es la seguridad. Por su naturaleza el contar con una VPN significa que los datos que una compañía intercambia se encuentran en una red pública, por lo tanto se encuentran expuestos y vulnerables a algún ataque. Si una red LAN no se encuentra conectada a Internet, al implementar una VPN se requerirá que se esté en Internet, lo cual abrirá la red a los posibles peligros que se encuentran presentes en esta red pública.

En Internet se encuentran algunos hackers que pueden tratar de penetrar a las redes solo porque les representa un reto u otros porque les pagan por hacerlo, también se encuentra la inconveniencia del correo basura (*spam email*) o los ataques de DoS (*Denial of Service*) en los cuales el intruso arroja ataques masivos de mensajes que logran tirar los servidores de una red. Y no hablar de los virus en archivos adjuntos de e-mail y en sitios de ftp[15] sospechosos.

[15] ftp, uno de los protocolos TCP/IP que se utiliza para copiar archivos entre dos equipos en Internet.

A estos problemas se está expuesto tan solo con el hecho de contar con salida a Internet para una red local, ahora pues, el hecho de realizar transferencia de información privada entre dos redes remotas utilizando como medio al Internet nos genera algunos otros problemas, entre los cuales destacan los siguientes:

- ***Snooping o Sniffing***: el primero monitorea el tráfico de la red, el segundo lee este tráfico, con lo cual queda expuesta toda información privada.
- ***Captura de direcciones***: un paquete transmitido contiene bastante información en los encabezados y demás que pueden ser utilizada con fines malignos. Esta información contiene direcciones de servidores, de DNS[16], proxys, ruteadores y demás de la red privada. Por lo cual le puede ser de gran ayuda a un hacker que planea realizar un ataque.
- ***Hijacking*:** la comunicación de una VPN se realiza mediante un intercambio de mensajes o sesión. Y si no se toman las precauciones adecuadas es posible que una persona ajena tome el control de la sesión (a esto se le llama *Hijacking*).
- ***Falseo de datos:*** si los datos que se envían pueden ser leídos por una persona ajena, entonces también pueden ser modificados, lo cual puede tener consecuencias muy serias, que ponen en duda la seguridad de todo el sistema.

Existen métodos sin embargo para evitar estos serios problemas de seguridad en una VPN. Entre los más importantes se encuentran los siguientes:

- Criptografía o Encriptación
- Autenticación

5.9. CRIPTOGRAFIA

La palabra Criptografía proviene del griego ***kryptos***, que significa esconder y ***gráphein,*** escribir, es decir, escritura escondida. La Criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "*esconder*" el mensaje (cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado lee el mensaje "*escondido*" (descifrar o desencriptar)

---

[16] DNS, Domain Names Service, Servidor de Nombres de Dominio.

Fig. 5.1 Proceso Encriptación - Desencriptación

En las VPN's este proceso es realizado automáticamente y es totalmente transparente a los usuarios, tal como se realiza en una transacción segura utilizando un browser como el Internet Explorer o Netscape.

Los principales problemas de seguridad que resuelve la Criptografía son:

- ***La privacidad***: la información enviada sólo puede ser leída por personas autorizadas.
- ***La integridad*****:** la información no puede ser alterada en el transcurso de ser enviada.
- ***La autenticidad*****:** se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mandó o que el mensaje recibido es el que se esperaba.

- *El no rechazo (firma digital)*: se refiere a que no se pueda negar la autoría de un mensaje enviado.

Cuando se diseña un sistema de seguridad una gran cantidad de problemas pueden ser evitados si se ponen en función de comprobar autenticidad, de garantizar privacidad, de asegurar integridad y evitar el no-rechazo.

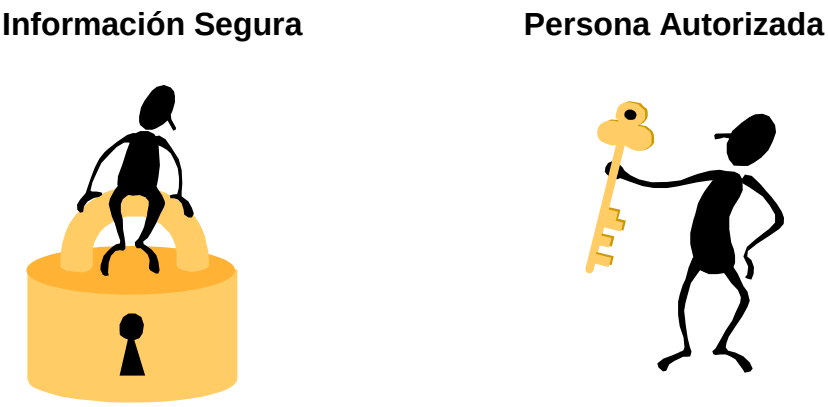


Fig. 5.2 Sistema de Seguridad

5.9.1. LA CRIPTOGRAFÍA CLÁSICA

La Criptografía no surge con la era informática, sino que ya viene desde los principios de la historia. Algunos de los algoritmos que han sido utilizados son los siguientes:

5.9.1.1 Rellenos de una sola vez

- ***Cifrado*:** se escoge una cadena de bits al azar como clave, y se va aplicando sobre el texto normal con una XOR[17] bit a bit
- ***Descifrado*:** Se vuelve a aplicar XOR con la misma cadena de cifrado. Inconvenientes: Manejo de la clave entre emisor y receptor y su sincronización.

5.9.1.2 Sustitución

Consiste en la sustitución de parte del texto original, mediante el desplazamiento (rígido o progresivo) o bien utilizando coordenadas de tablas.

La forma de descifrar es invirtiendo el cifrado, mantiene los mismos problemas que el de relleno.

5.9.1.3 Transposición

[17] XOR, compuerta que realiza procesos de disyunción lógica.

Se basa en la reordenación aplicada al texto original mediante una clave establecida. Al igual que en la sustitución, el descifrado se realiza mediante la clave y de nuevo la reordenación, presenta los mismos inconvenientes.

En los algoritmos explicados anteriormente la dificultad en el cifrado y el descifrado no es muy complejo, si se tiene en cuenta las posibilidades que ofrecen hoy en día los ordenadores, la capacidad de cómputo es muy elevada.

Por otra parte se los debe tener en cuenta pues sientan las bases de la Criptografía e indican lo importante que ha sido la información.

5.9.2 LA CRIPTOGRAFÍA MODERNA

La Criptografía moderna se basa en las mismas ideas básicas que la Criptografía tradicional, la transposición y la sustitución, pero con distinta orientación. En la Criptografía moderna el objetivo es hacer algoritmos de cifrado complicados y rebuscados.

Los Criptosistemas no son otra cosa que una representación del sistema de Criptografía, que se utiliza en un determinado sistema de seguridad.

Los algoritmos de Criptografía moderna se dividen según el tratamiento del mensaje en:

a. Cifrado en bloque

B **DES**

El texto original se codifica en bloques de 64 bits, clave de 56 bits y 19 etapas diferentes.

El descifrado se realiza con la misma clave y los pasos inversos. El inconveniente es que puede ser descifrado probando todas las combinaciones posibles, cosa que queda solucionada con Doble DES (ejecuta el DES 2 veces con 3 claves distintas) y el Triple Des (2 claves y 3 etapas).

B **RSA**

Se basa en la dificultad de factorizar número grandes por parte de los ordenadores. El principal inconveniente como es de suponer es la lentitud.

B **IDEA**

Tenemos una clave de 128 bits con 8 iteraciones. El descifrado se realiza aplicando el mismo algoritmo pero con subclaves diferentes.

Hay que destacar que el RSA pertenece a los algoritmos con clave pública mientras que el DES y el IDEA son algoritmos de clave secreta.

b. Cifrado en flujo o cifrado bit a bit

B *A5,* es el algoritmo de cifrado de voz. Gracias a él, la conversación va encriptada. Se trata de un algoritmo de flujo (*stream cipher*[18]) con una clave de 64 bits. Hay dos versiones, denominadas A5/1 y A5/2; esta última es la versión autorizada para la exportación, y en consecuencia resulta más fácil de atacar.

c. Sistemas CEE de curvas elípticas

B CCE es otro tipo de Criptografía de clave pública es el que usa curvas elípticas definidas en un campo finito. La diferencia que existe entre este sistema y RSA es el problema matemático en el cual basan su seguridad.

Son idóneos para ser implementados en donde el poder de cómputo y el espacio del circuito es reducido, donde se requiere una alta velocidad de procesamiento o grandes volúmenes de transacciones, donde el espacio de almacenamiento, la memoria o el ancho de banda es limitado. Lo que permite su uso en Smart Cards[19], Celulares, Fax, Palms, PC's, etc.

Son el mejor candidato para reemplazar a las aplicaciones que tienen implementado RSA, estas definen también esquemas de firma digital, Intercambio de claves simétricas y otros.

[18] Stream Cipher, flujos binarios.
[19] Smart Cards, tarjetas inteligentes.

5.9.3. DIVISIÓN DE LA CRIPTOGRAFÍA

La Criptografía se divide en dos grandes ramas, la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica.

5.9.3.1 Cifrado con Clave Privada o Criptosistemas Simétricos

Existe una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside sólo en mantener dicha clave en secreto.

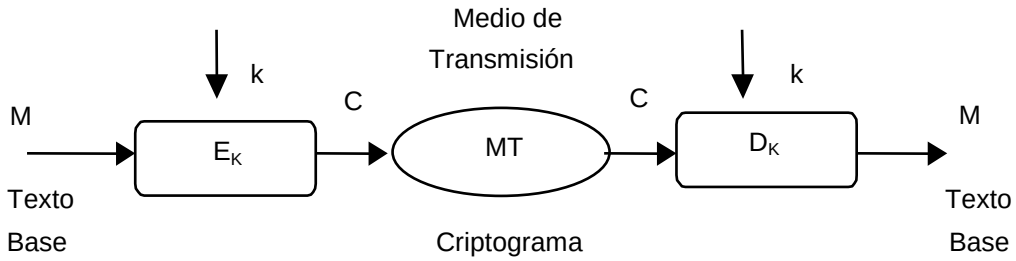


Fig. 5.3 Cifrado con Clave Privada

Con Ek[20] se cifra el mensaje original aplicándole la clave k y con Dk[21] se lo descifra, aplicándole de la misma forma la clave k.

[20] Ek, codificación aplicando la clave privada k.
[21] Dk, decodificación aplicando la misma clave privada k.

La confidencialidad y la integridad se logran si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen simultáneamente si se protege la clave privada.

5.9.3.2 Cifrado con Clave Pública o Criptosistemas Asimétricos

Cada usuario crea un par de claves, una privada para descifrar y otra pública para cifrar, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa.

La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello, usan funciones matemáticas de un solo sentido con trampa

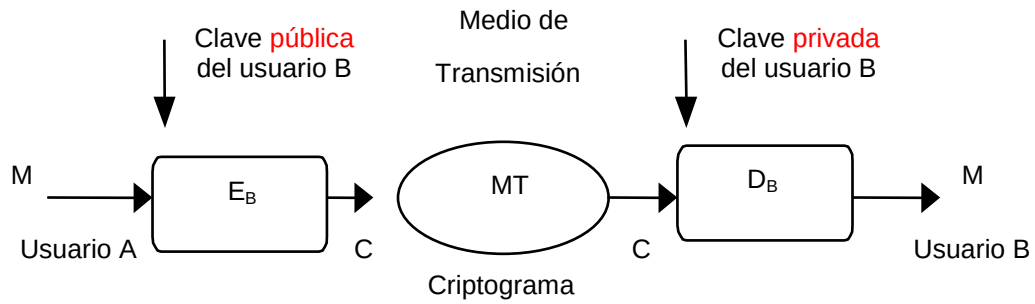


Fig. 5.4 Encriptación con clave pública y privada del Emisor

Hay que tener en cuenta que Eb[22] y Db[23] son inversas dentro de un cuerpo, y se cifra con la clave pública del destinatario, de forma que solo él, al tener su clave privada pueda acceder al mensaje original.

[22] Eb, codificación con la clave pública del usuario B
[23] Db, decodificación con la clave privada del destinatario B.

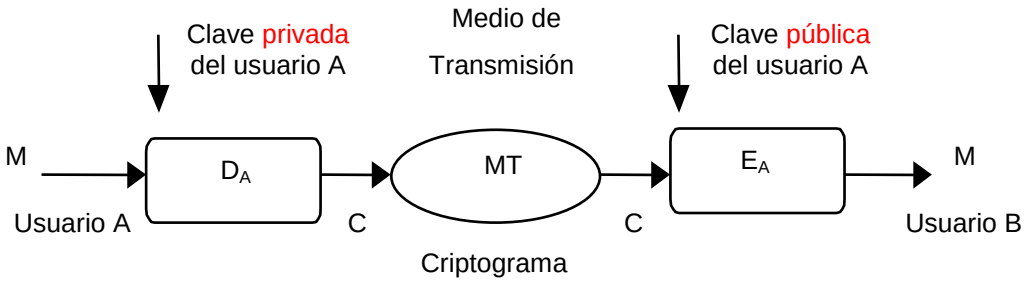


Fig. 5.5 Encriptación con clave pública y privada del Receptor

En este segundo caso se observa como está basado el cifrado con la clave privada del emisor y al igual que antes hay que tener en cuenta que Ea[24] y Da[25] son inversas dentro de un cuerpo.

5.9.3.3 Diferencias

Los sistemas de clave pública son más rápidos, aunque es posible que no sean tan seguros. Hay algunos tipos de ataques que les pueden afectar.

Los sistemas de clave privada son más lentos, aunque son más seguros, los algoritmos son más complejos y es más difícil su traducción por otros sujetos.

5.9.4. EL CONTROL DE INTEGRIDAD

Además en la Criptografía de Clave Pública se ejerce también un ***control de la integridad*** (se asegura de que el mensaje recibido fue el enviado por

[24] Ea, codificación con la clave pública del emisor A.

la otra parte y no uno manipulado), para cumplir con este objetivo se utilizan funciones de dispersión unidireccional (o *hash*[26]).

La función de dispersión llamada compendio de mensaje, tiene 3 propiedades importantes:

- Dado un mensaje P, es fácil calcular el compendio del mensaje MD (P).
- Dado un compendio MD (P), es computacionalmente imposible encontrar P, es decir no tiene inversa.
- No se pueden generar dos mensajes que tengan el mismo compendio, a menos que sean el mismo mensaje.

Los algoritmos más utilizados son el MD5 y el SHA.

- **MD5**

  Opera con los bits, de forma que cada bit de salida es afectado por cada bit de entrada.

  Coge el mensaje original y lo rellena hasta conseguir una longitud de 448 módulos de 512 bits

  Añade al mensaje la longitud original del mismo como un entero de 46 bits.

  Inicializa un buffer de 128 bits de tamaño a un valor fijo.

---

[25] Da, decodificación con la calve privada del usuario A.
[26] Hash, resultado de tamaño fijo obtenido al aplicar una función matemática unívoca

En cada iteración coge un boque de 512 bits de entrada y lo mezcla por completo con el buffer y los valores de una tabla construida a partir de los valores de una tabla de la función seno.

Una vez terminado el cálculo, el buffer contiene el valor del compendio del mensaje.

B **SHA**

Genera un compendio de mensaje de 160 bits, funciona igual que el MD5, pero con un buffer de 160 bits.

Es más seguro que el MD5, debido sobretodo a que utiliza un mayor número de bits que el MD5, pero como es normal también será más lento.

5.9.5. LA FIRMA DIGITAL

Consiste en que el receptor puede saber a ciencia cierta de quien es el mensaje y esto se lo consigue mediante la firma digital, al ser esta única, como si fuera una firma normal en un papel, se tiene como un acuse o un recibo, que demuestra quién ha enviado el mensaje.

La firma digital puede ser utilizada al igual que el hash tanto en los sistemas de clave pública como en los de clave privada. Por este motivo es muy utilizada en documentos legales y financieros.

5.9.5.1 Requisitos:

- Debe ser fácil de generar.
- Será irrevocable, no rechazable por su propietario.
- Será única, sólo posible de generar por su propietario.
- Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
- Debe depender del mensaje y del autor

5.9.5.2 Ventajas:

- La principal ventaja de la firma digital en comparación de la firma autógrafa, es que el procedimiento de verificación es exacto y que es imposible en la práctica su falsificación.
- La firma digital es portable, es decir, puede ser realizada en diferentes puntos del mundo, de forma simultánea y sin necesidad de testigos.

5.9.5.3 Desventajas:

- Quizá la más notable desventaja actual de la firma digital en contra de la firma autógrafa, es que la primera no es valida legalmente aún en muchos países. Parece ser que esto obedece a una transición natural de esta nueva tecnología, que por lo tanto existe un rechazo en su aceptación a pesar de los grandes beneficios que proporciona.
- Su seguridad depende de la clave privada, es decir, que si la clave privada se compromete por alguna causa, entonces, se compromete la seguridad de la firma digital, esto quiere decir que puede ser usada por individuos y eventos no autorizados.

5.10 AUTENTICACIÓN

Otro aspecto muy importante es el saber si un usuario es quien dice ser y si sólo él tiene las llaves para la decodificación del mensaje.

Si un intruso entra a un sistema lo demás resulta mucho más fácil, ya que aún entrando como usuario de bajo nivel [27], puede tener acceso a información valiosa para acceder a niveles superiores.

[27] Usuario de bajo nivel, usuarios con acceso restringido a la información.

Es por ello que mantener la puerta de entrada[28] lo suficientemente segura para que no entren intrusos pero lo suficientemente accesible para que los usuarios legítimos no tengan problemas de acceso se vuelve una encrucijada para los administradores de la red.

Si se trata de implementar una VPN pequeña corriendo en Windows es fácil utilizar el PPTP (*Point to Point Tunneling Protocol*) para autenticar el acceso en el servidor. Este protocolo se utiliza entre el Servidor de Acceso y el ISP que provee acceso a Internet a los usuarios, y funciona de la misma forma que el Servidor de Acceso Remoto (*RAS*) al cual los usuarios marcan directamente.

Sin embargo surgen problemas cuando se trata de VPN's más grandes, debido a que es difícil que el administrador pueda decidir hasta donde confiar en los usuarios que entran a la VPN desde entidades sobre las cuales no se tiene control. Para esto también se han desarrollado ciertos medios utilizados también por los ISP's como son: **RADIUS** (*Remote Authentication Dial-In User Service*) y **TACACS** (*Terminal Access Controller Access Control System*).

B **RADIUS**

Este es un sistema de autenticación de cuentas utilizado por muchos ISP's para verificar la identidad de sus usuarios, y como su nombre lo indica fue desarrollado para servir a usuarios de Dial-up.

Cuando un usuario trata de acceder al servidor de la red que es un Cliente Radius, la información de usuario y clave es enviada a un servidor Radius, el cual verifica que la información sea correcta y autoriza el acceso al sistema.

La petición al servidor Radius contiene de manera encriptada el nombre y clave del usuario, así como también el número de identificación del cliente y el puerto al que se dirige, y éste es autenticado mediante el uso de una llave compartida.

Una vez que el servidor Radius valida la solicitud del cliente, pasa la información a otros métodos de autenticación como son PPP, PAP[29], CHAP[30], etc. Los cuales dan acceso o rechazan al usuario.

B **TACACS**

Es más viejo que Radius, trabaja muy parecido a éste. Las contraseñas de los usuarios son administradas en una Base de Datos Centralizada. No

---

[28] Puerta de entrada, medio de ingreso a la información.
[29] PAP, protocolo de autenticación por contraseña, sin formato para la autenticación de conexiones PPP
[30] CHAP, protocolo de autenticación por desafío en tres fases, sin formato para la autenticación de conexiones PPP

permite el cambio de contraseñas, ni la utilización de los factores. Su código es de dominio público.

Radius utiliza el UDP (*User Datagram Protocol*) entre el cliente y el servidor, y TACACS utiliza TCP.

CAPÍTULO VI

VPN SOBRE WINDOWS 2000 ADVANCED SERVER

La práctica que a continuación se detalla es una simulación de cómo funciona una VPN con una topología que emula la conexión vía Internet mediante la utilización del Windows 2000 Advanced Server.

El siguiente gráfico muestra la topología que se ha utilizado para la práctica.

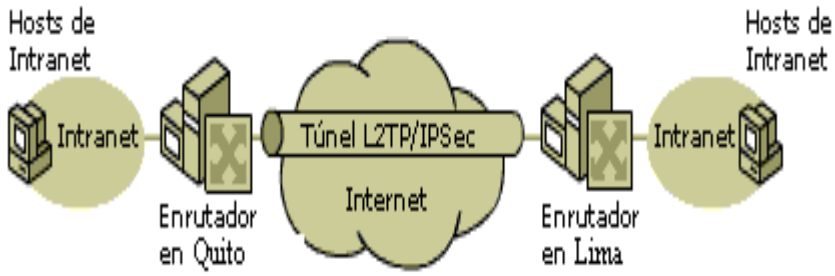


Fig. 6.1 Esquema de una VPN

Una vez realizada esta práctica se tendrán conocimientos de:

- Instalación del Ruteo y Acceso Remoto.
- Configuración del Ruteo y Acceso Remoto para permitir conexiones VPN.

- Configuración y prueba de las conexiones VPN usando el Asistente para Conexión de Red.

Para completar esta práctica es necesario:

- Una computadora con Windows 2000 Advanced Server que esté configurado como un Controlador de Dominio.
- Una dirección IP estática y máscara de subred.
- Otra computadora con configuraciones similares a la anterior.

6.1 CONFIGURACIÓN DEL SERVIDOR DE RUTEO Y ACCESO REMOTO

El Acceso Remoto permite a los usuarios conectarse a la red desde una ubicación lejana para poder crear conexiones de acceso remoto apropiadas en clientes remotos y configurar los derechos de acceso de usuarios hacia el Servidor de Acceso Remoto.

Para configurar este servicio se deben seguir los siguientes pasos:

a. Inicie su sesión como ***Administrador*** del Dominio.

b. En el menú de ***Herramientas Administrativas*** seleccione ***Ruteo y Acceso Remoto.***

c. En el árbol de la Consola, clic derecho en el nombre del servidor, clic en ***Configuración y Activación de Ruteo de Acceso Remoto***.

d. Clic en ***Siguiente***.

e. Aparecerá la ventana del ***Asistente para la instalación del Servidor de Enrutamiento y Acceso Remoto***

f. Clic en ***Siguiente***

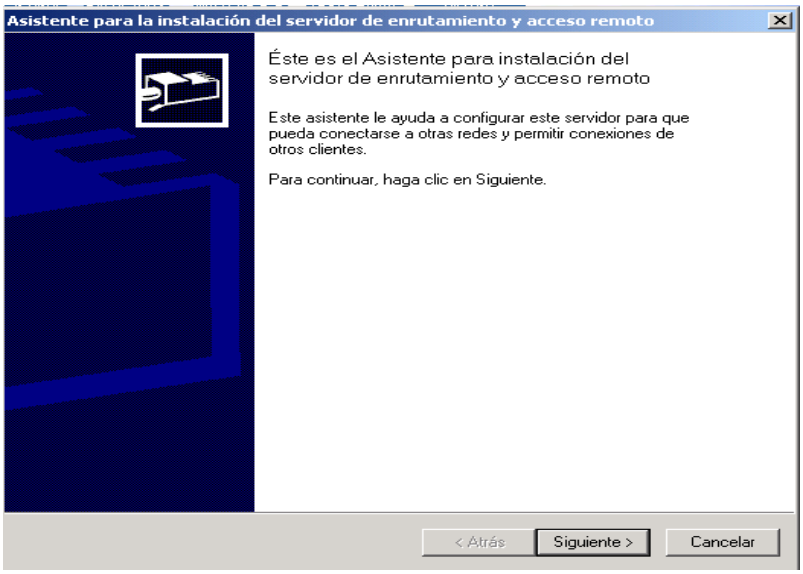


Fig. 6.2 Asistente del Servidor de Enrutamiento y Acceso Remoto

g. En la ventana de Configuraciones comunes seleccione la opción ***Servidor de Acceso Remoto***.

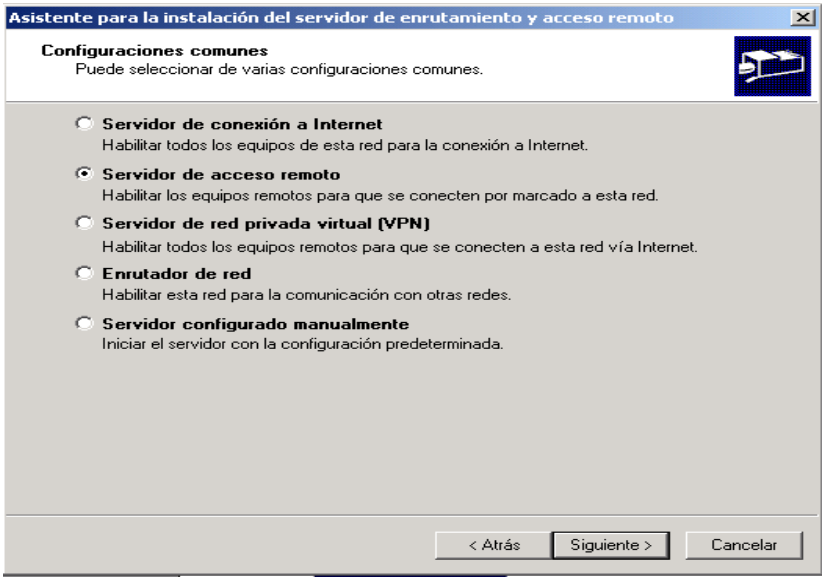


Fig. 6.3 Ventana de Configuraciones Comunes

h. Clic en ***Siguiente***.

i. En la ventana de Protocolos de cliente remoto, clic en ***Siguiente***.

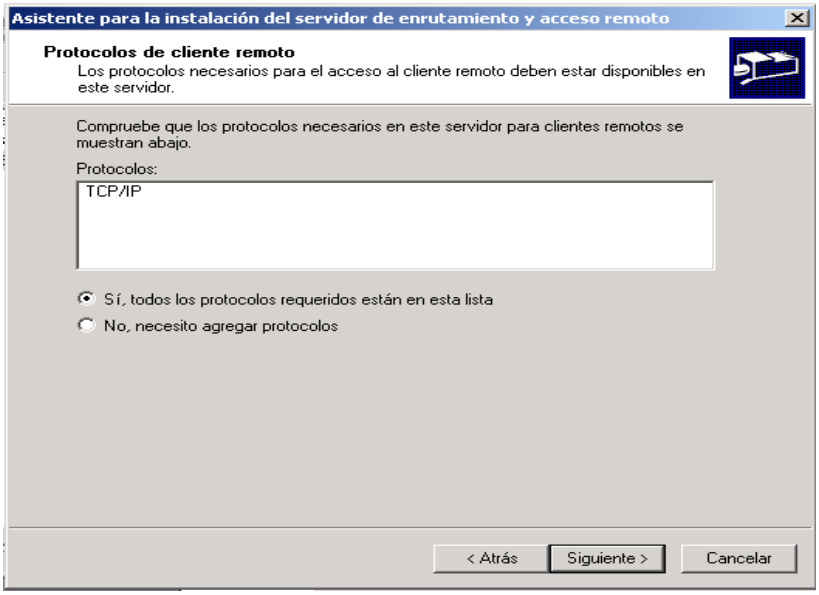


Fig. 6.4 Ventana Protocolos de Cliente Remoto

j. En la ventana de Selección de red, bajo nombre verifique que su servidor este seleccionado. Clic en ***Siguiente***.

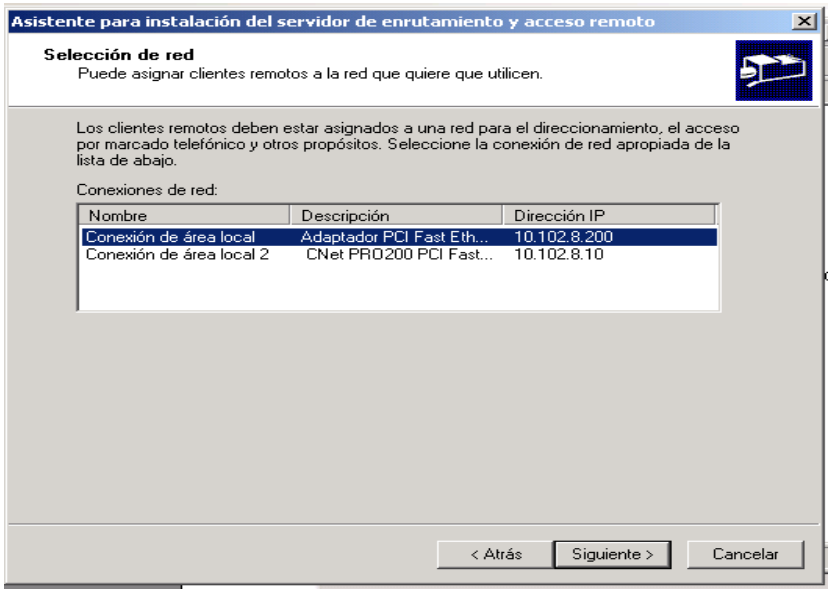


Fig. 6.5 Ventana Selección de Red

k. En la ventana de Asignación de direcciones IP, clic en ***Desde un intervalo de direcciones especificado***.

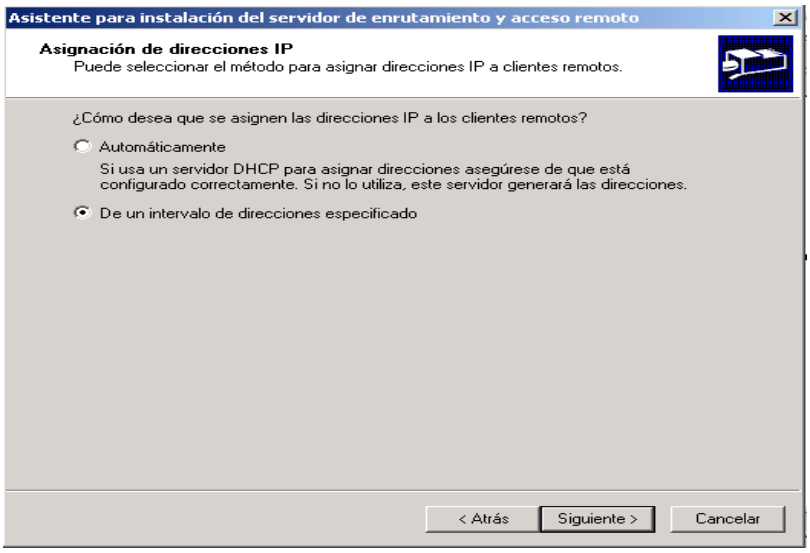


Fig. 6.6 Ventana de Asignación de Direcciones IP

l. Clic en ***Siguiente***.

m. En la Ventana de Asignación de rangos de direcciones, clic en ***Nueva.***

n. Aparecerá la ventana de Intervalo de dirección nueva.

o. Añadir las direcciones IP del intervalo.

p. Clic en ***Siguiente*** para regresar a la ventana anterior.

q. Clic en ***Siguiente***.

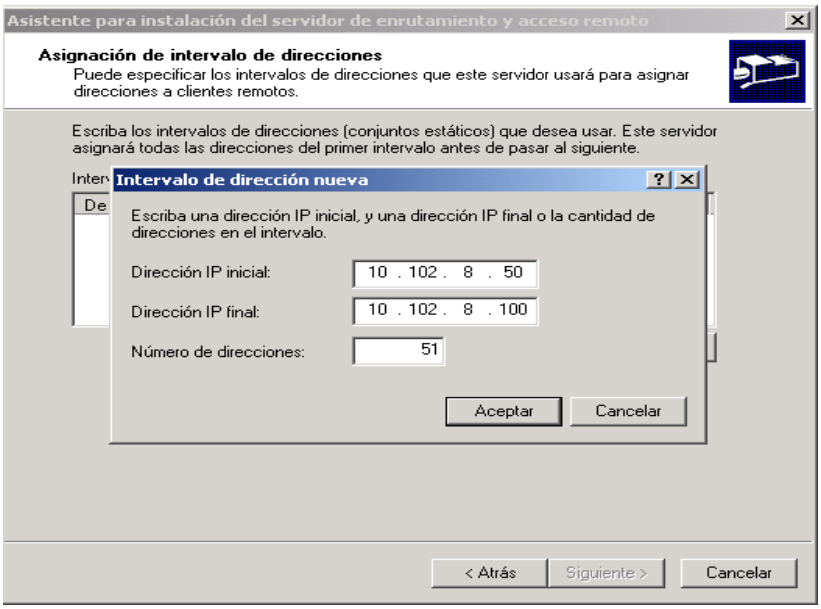


Fig. 6.7 Ventana de Asignación de Intervalo de Direcciones

r. En la ventana de Administrar servidores de acceso remoto múltiples verificar que este seleccionado ***No, no quiero configurar este servidor para usar RADIUS ahora***. Clic en ***Siguiente***

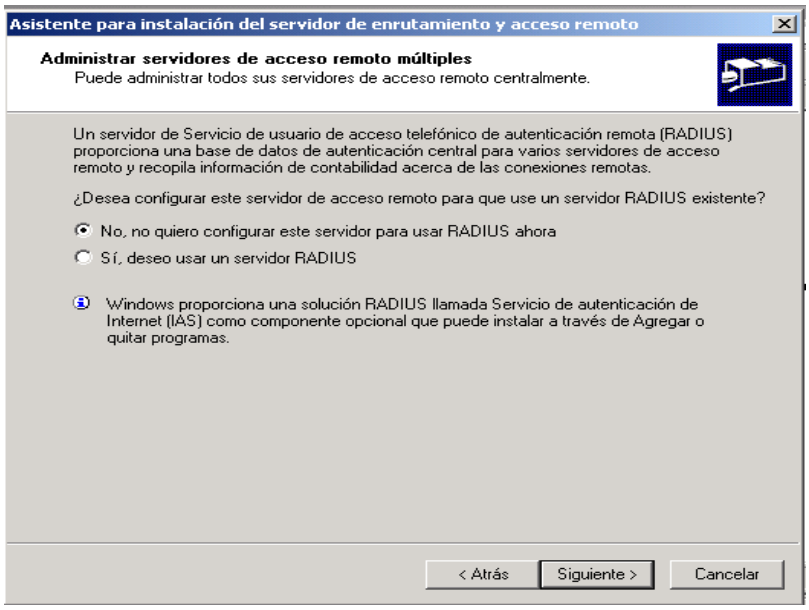


Fig. 6.8 Ventana Administrar Servidores de Acceso Remoto Múltiples

s. Clic en ***Finalizar*** para cerrar el Asistente.

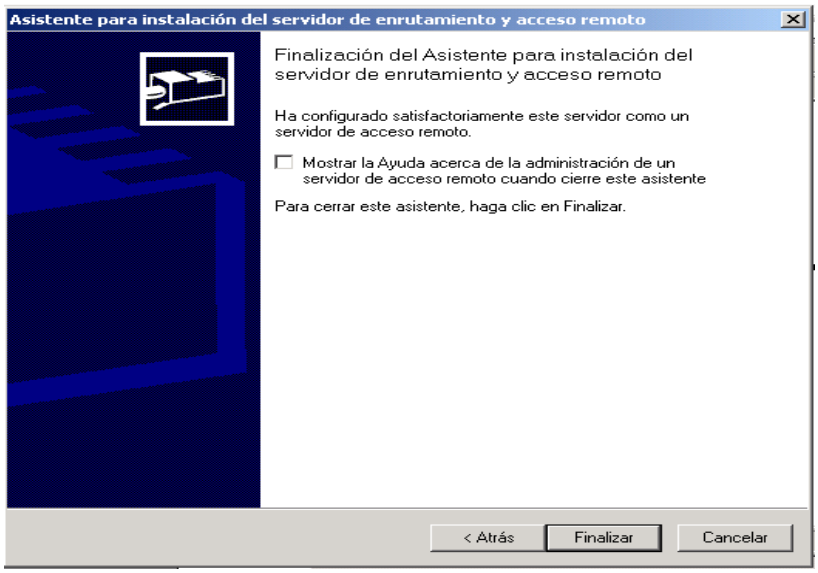


Fig. 6.9 Ventana de Finalización del Asistente de Ruteo

Una vez configurado el Servidor de Ruteo y Acceso Remoto aparecerá en la consola los puertos, clientes, enrutamiento IP, etc. del Servidor

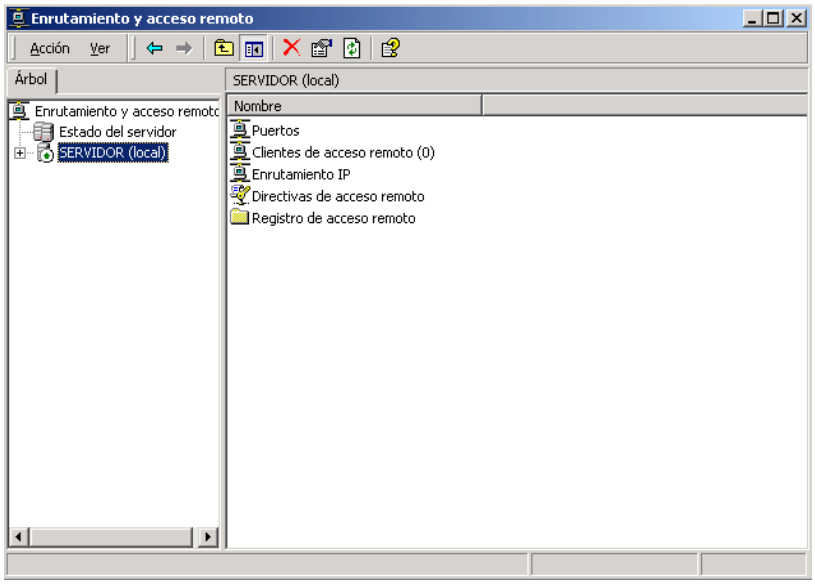


Fig. 6.10 Consola de Enrutamiento y Acceso Remoto

Terminada la instalación y configuración del primer servidor se debe realizar el mismo proceso en el segundo servidor, la única diferencia es el intervalo de las direcciones de enrutamiento que el Servidor asignará a sus clientes remotos.

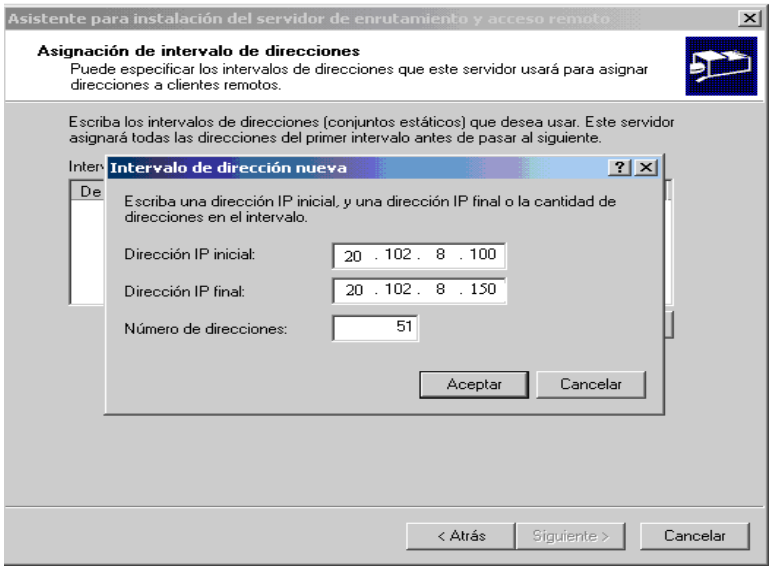


Fig. 6.11 Asignación de Direcciones del Segundo Servidor

6.2 CONFIGURACIÓN DE UNA VPN

Una vez configurado el Acceso Remoto se puede realizar la configuración de una VPN ya que Windows 2000 Advanced Server automáticamente habilita los protocolos PPTP o L2TP para establecer conexiones remotas cuando se crean puertos VPN durante la instalación del Ruteo y Acceso Remoto.

Para configurar una VPN en el Servidor de Acceso Remoto se deben seguir los siguientes pasos:

a. Clic derecho en ***Mis Sitios de Red***.

b. Clic en ***Propiedades***.

c. En ***Conexiones de Red y Dial up,*** doble clic en ***Nueva conexión***.

d. En la ventana de Información de localidad escriba un código de área.

e. Clic en ***Siguiente.***

f. Clic para cerrar opciones de Teléfono y Módem.

g. Ejecutar el ***Asistente para Conexión de Red.***

Fig. 6.12 Asistente para Conexión de Red

h. Clic en ***Siguiente***.

i. En la ventana de tipo de conexión de red seleccionar ***Conectar a una red privada a través del Internet.***

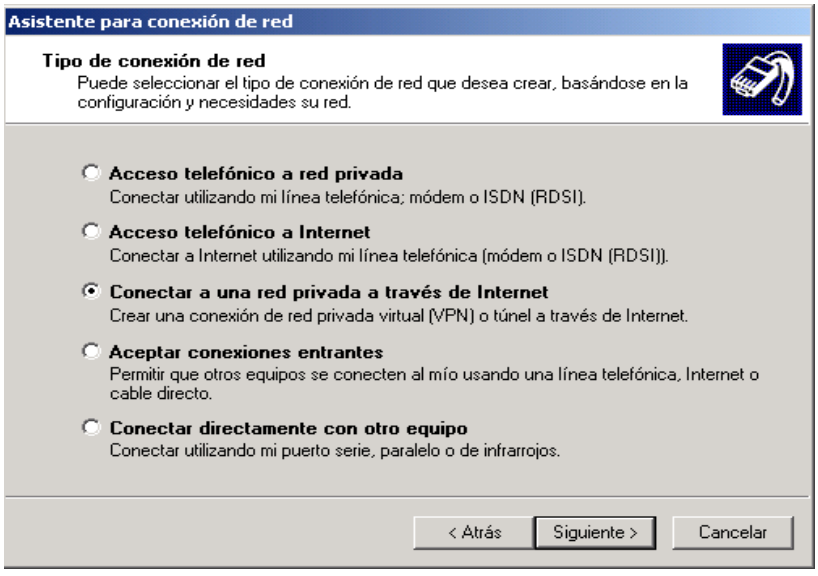


Fig. 6.13 Ventana Tipo de Conexión de Red

j. Clic en ***Siguiente***.

k. En la ventana de Dirección de destino escribir la *dirección IP de destino. o el nombre del Host Remoto* que dará acceso mediante el túnel a la Red Privada.

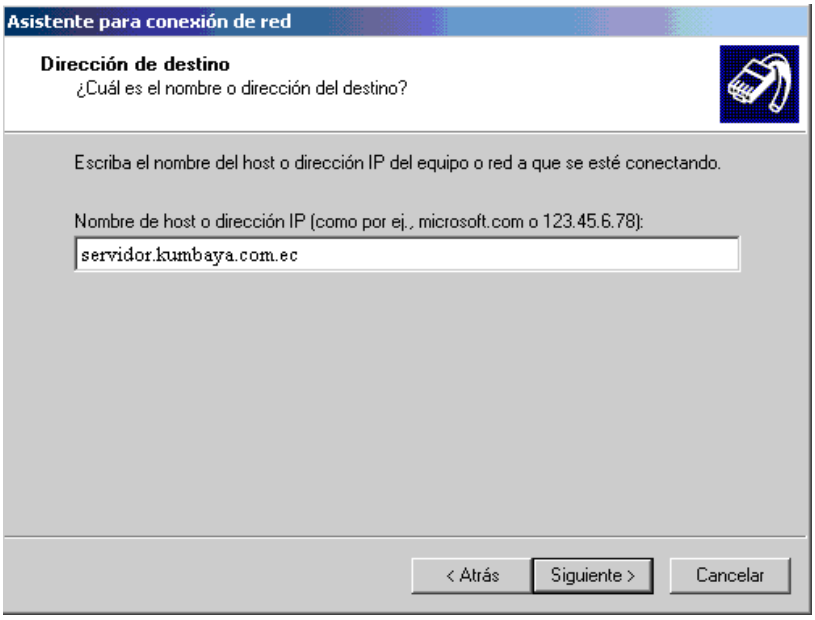


Fig. 6.14 Ventana de Dirección de Destino

l. Clic en ***Siguiente***.

m. En la ventana de disponibilidad de conexión se puede mantener esta conexión para todos los usuarios o para uso exclusivo.

n. Seleccionar ***"Solo para mi"*.**

o. Clic en ***Siguiente***.

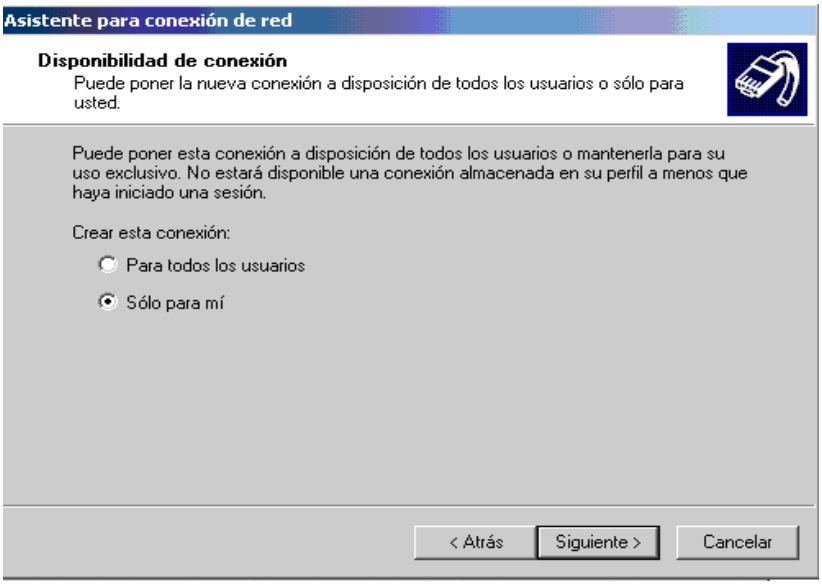


Fig. 6.15 Ventana de Disponibilidad de Conexión

p. Aparecerá la ventana de finalización del asistente, donde se da un nombre a la conexión además da posibilidad de crear un acceso directo en el escritorio para una localización mas rápida.

q. Clic en ***Finalizar***.

Fig. 6.16 Ventana Finalización del Asistente para Conexión de Red

r. Una vez creada la conexión aparecerá la ventana principal de la Conexión VPN donde se pide el nombre y contraseña del usuario, también permite modificar las propiedades de la conexión que en este caso no será necesario.

s. Clic en ***Conectar***.

Fig. 6.17 Ventana Principal de la Conexión VPN

t. Aparecerá la ventana de progreso de la conexión, también mostrará los posibles errores que puedan ocurrir.

Fig. 6.18 Ventana de Estado de la Conexión VPN

u. Con este mensaje se confirma que la conexión se ha realizado con éxito, tras cerrar esta ventana se debería poder acceder a las máquinas de la red remota sin problemas.

Concluida la instalación y configuración de la VPN en el primer servidor se debe realizar el mismo proceso en el segundo servidor, este proceso se diferencia del anterior en la Dirección o Nombre del Host de Destino para la nueva conexión.

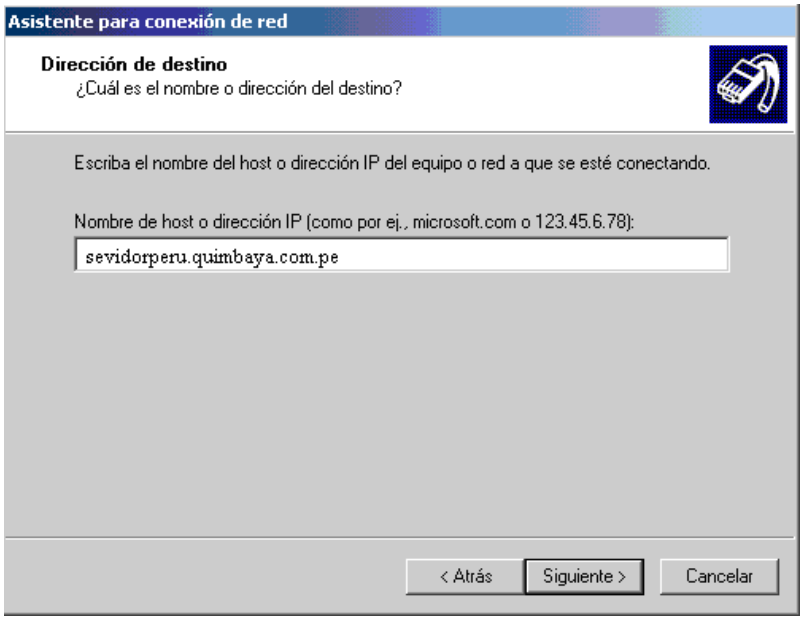


Fig. 6.19 Host de destino de la Conexión VPN del segundo servidor

6.3 COMPROBACIÓN DEL TÚNEL DE LA VPN

Para comprobar que los paquetes están viajando por un túnel seguro dentro de una VPN se pueden utilizar los siguientes comandos:

- **TRACERT,** determina la ruta tomada hacia un destino, mediante el envío de mensajes de petición de eco del Protocolo de Mensajes de Control de Internet (ICMP) al destino con valores de campo de tiempo de vida (TTL) que crecen de forma incremental.

  La ruta mostrada es la lista de interfaces del enrutador entre el host de origen y el de destino.

  tracert [**-d**] [**-h** *Saltos Máximos*] [**-j** *Lista de Hosts*] [**-w** *Tiempo de espera*] [***nombre de destino***]

  Parámetros:

  -d: impide que *tracert* convierta direcciones IP en nombres de Host. Esto puede acelerar la presentación de resultados de *tracert.*

  -h *Saltos Máximos*: especifica el número máximo de saltos en la ruta para buscar el destino. El valor predeterminado es 30 saltos.

-j *Lista de Hosts*: enrutamiento relajado de origen a lo largo de la lista de host. La *Lista de Hosts* es una serie de direcciones IP (en notación decimal con puntos) separadas por espacios, máximo 9.

-w T*iempo de Espera*: especifica la cantidad de tiempo, en milisegundos, entre intentos Si no se recibe dentro del período de tiempo de espera, se muestra un asterisco (*). El tiempo de espera predeterminado es 4000 (4 segundos).

***Nombre de Destino*:** especifica el destino, identificado por la dirección IP o el nombre de host.

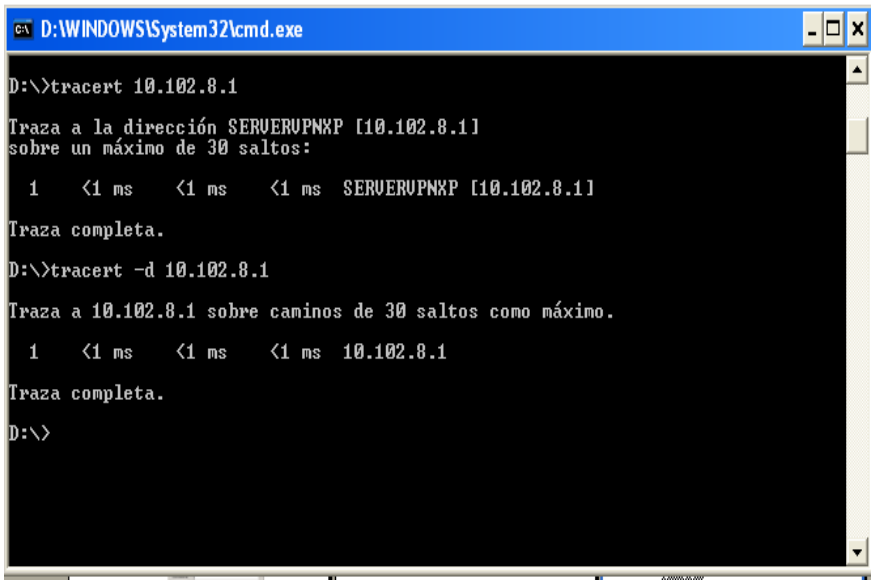


Fig.6.20 Ejecución del Comando Tracert

B **WINDUMP,** programa cuya utilidad principal es analizar el tráfico que circula por la red. Se apoya en la librería de captura pcap, la cual presenta una interfaz uniforme y que esconde las peculiaridades de cada sistema operativo a la hora de capturar tramas de red.

Parámetros:

–i: si el host tiene más de una interfase de red.

–**D:** para determinar el número de interfases.

C:\>windump –D

–n*:* para agilizar el proceso de visualización evitando la resolución de nombres.

Host*:* para filtrar por host (nombre o IP).

port*:* para filtrar por puerto (nombre o número).

C:\>windump -i 2 -n host www.quimbaya.com.pe and port 80

src*:* para filtrar por origen (host/puerto) como prefijo al comando ***host*** o ***port.***

dst*:* para filtrar por destino (host/puerto) como prefijo al comando ***host*** o ***port***.

ip protocol*:* para filtrar por tipo de protocolo o los comandos ***icmp***, ***igrp***, ***udp***, ***nd***, o ***tcp***.

–w*:* para grabar la captura y para abrirlos el comando ***-r***.

C:\>windump -r evidencia not dst host intruso and not icmp

and u **or*:*** para realizar concatenaciones lógicas

not: para negar algún elemento (puerto/host/protocolo) mediante un filtro, se lo usa como prefijo al filtro que se crea.

C:\>windump -i 2 host servidor and not port 80

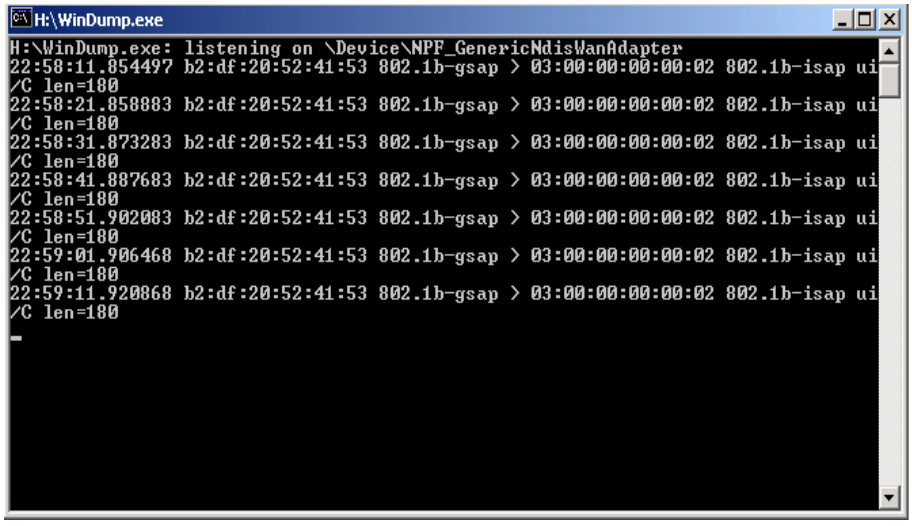


Fig. 6.21 Ejecución del Comando Windump

B **VISUALROUTE,** es un ping visual, rápido e integrado, es un programa que hace el seguimiento de la ruta de paquetes y automáticamente

analiza problemas de conectividad; despliega los resultados en el mapa mundial de la pantalla.

Requerimientos para el programa en Windows:

- Windows 95/98/Me/NT/2000/XP.
- Monitor a color con resolución 800x600 256 (o superior).
- Un stack Microsoft's TCP/IP.
- Una conexión a Internet.

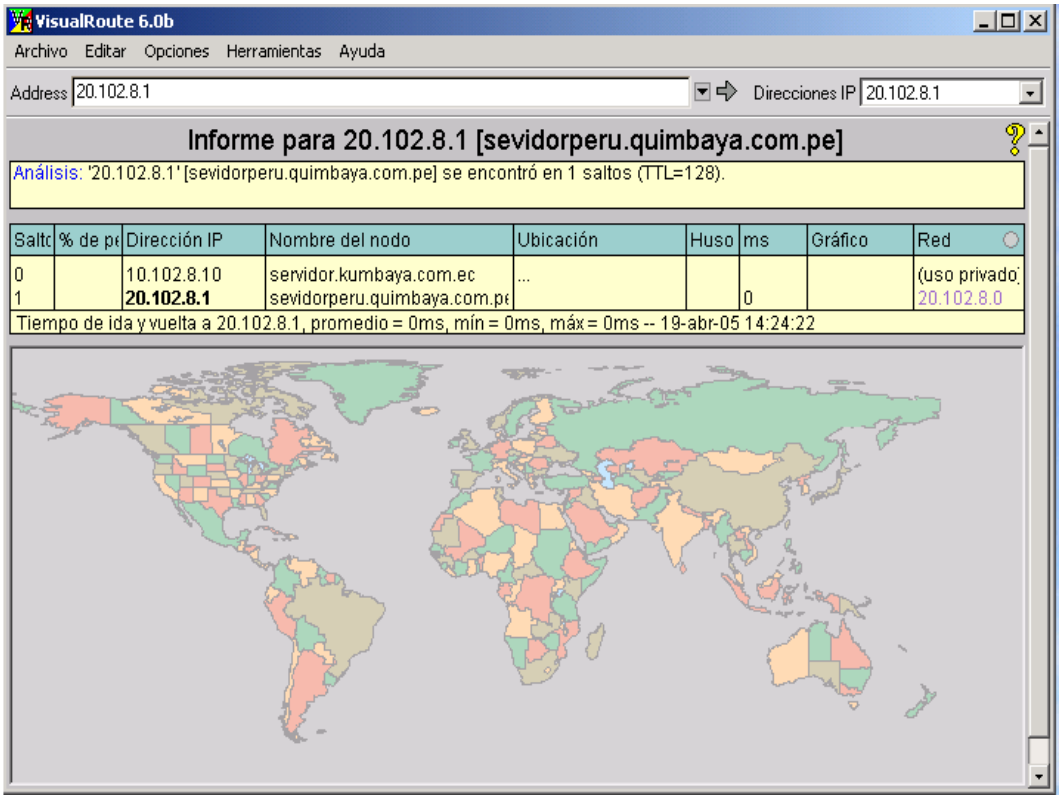


Fig. 6.22 Pantalla de VisualRoute

B **IP-TOOLS,** ofrece varios utilitarios TCP/IP en un solo programa, puede trabajar bajo Windows 95/98/ME/NT 4.0/2000 y Windows XP, y resulta una herramienta muy útil para quien que utiliza Internet o Intranet.

Permite operación multitareas. Puede ejecutar todos los utilitarios simultáneamente y obtener información de un host individual, de todos los hosts en rango de las direcciones IP (ej. 10.102.8.1 – 10.102.8.200) o trabajar con una lista de hosts y direcciones IP.

Puede guardar toda la información en archivos de texto (o HTML).

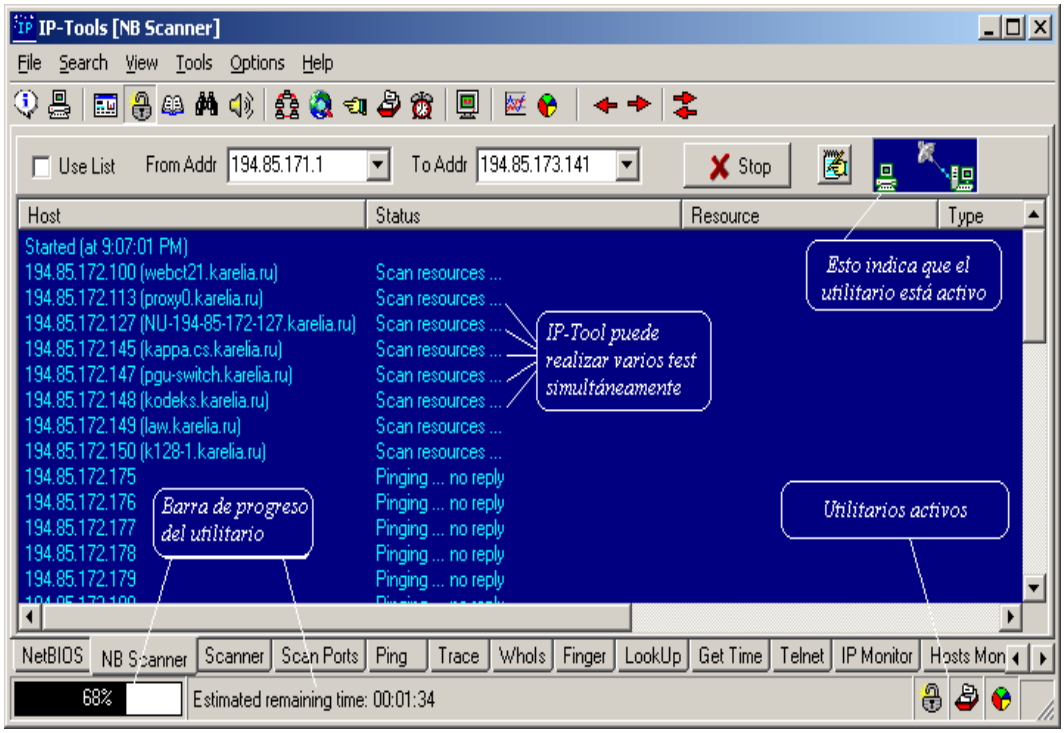


Fig. 6.23 Pantalla de IP-Tools

IP-Tools incluye 15 utilitarios:

- ***Local Info***, examina al host local y muestra información del procesador, memoria, datos del Winsock, etc.
- ***Connection Monitor***, despliega información de las actuales conexiones de red TCP,UDP.
- ***NetBIOS Info***, obtiene información NetBIOS acerca de las interfases de red (local y PC remotos).
- ***NB Scanner***, escáner de recursos compartidos.
- ***Name Scanner***, explora los nombres de los hosts bajo el rango de las direcciones IP.
- ***Port Scanner***, explora los servicios de host (soporta rango de direcciones, como 10.102.8.1 -10.102.8.200).
- ***Ping Scanner***, realiza un ping en un host remoto en la red (soporta rango de direcciones).
- ***Trace,*** rastrea la ruta a un host remoto a través de la red.
- ***WhoIs***, obtiene información sobre nombres desde el Network Information Center.
- ***Finger***, señala uno o más usuarios en un host remoto.
- ***LookUp***, busca nombre de dominios de acuerdo a su dirección IP o una dirección IP desde el nombre del dominio.

- ***GetTime***, obtiene la hora desde los servidores de horarios (y configura la hora correcta en el sistema local)
- ***Telnet***, cliente telnet.
- ***IP-Monitor***, muestra gráficas en tiempo real para TCP,UDP,ICMP In,Out,Error packets.
- ***Host Monitor***, monitorea el estatus arriba/abajo de los hosts seleccionados.

CAPÍTULO VII

PROVEEDORES DE EQUIPO Y ENLACE

7.1. EQUIPOS

7.1.1 PROPUESTA TECNOLÓGICA DE CISCO

Cisco como proveedor de tecnología ofrece una variedad de productos para la implantación de VPN's empresariales.

En cuanto a seguridad, el equipo de Cisco maneja en el Nivel 3 el protocolo IPSec, y para el Nivel 2 puede utilizar L2TP que es el estándar para aplicaciones de tunneling. Además de esto puede utilizar PPTP, L2F, GRE[1], entre otros. También en cuanto a formas de encriptación, se puede utilizar DES[2], 3DES[3] y RC4[4] de 40 a 128 bit para utilización en MPPE (*Microsoft Point to Point Encryption*)[5].

[1] GRE, Generic Routing Encapsulation, Encapsulación Genérica de Ruteo.
[2] DES, Estándar de cifrado de datos aplica un cifrado por bloques con una clave de 56 bits.
[3] 3DES, procesa cada bloque tres veces, utilizando una clave única de 56 bits cada vez:
[4] RC4, Algoritmo de cifrado de claves de 128 bits o claves de 40 bits.
[5] MPPE, garantiza la confidencialidad de los paquetes entre el cliente de acceso remoto y el servidor de acceso remoto o del túnel.

Una ventaja de Cisco es que ofrece soluciones que se pueden aplicar en equipo de esta misma marca con una simple actualización del IOS[6], como es el caso de firewalls que se pueden instalar en ruteadores, o también ofrece la aplicación pero de manera separada por medio de otro equipo.

Esto puede ayudar a salvar costos en caso de que se cuente ya con cierta infraestructura de esta misma marca, además que presenta una mayor flexibilidad y posibilidad de crecimiento futuro.

En cuanto a detección de intrusos ofrece el sistema ***Cisco NetRanger***, el cual opera en conjunto con los firewalls instalados y tiene la capacidad de analizar el contenido y el contexto individual de cada paquete para determinar si el tráfico está autorizado, y en caso de no serlo puede aplicar la política de seguridad correspondiente.

Ofrece estándares para asegurar la Calidad del Servicio (QoS) los cuales pueden ser aplicados al proveedor del servicio de red para poder administrar un ancho de banda punto a punto a través de la VPN, y esta QoS puede ser medida y monitoreada mediante otra característica del IOS instalado en el ruteador.

[6] IOS, software de Sistema Operativo propio de Cisco.

También es importante destacar que en cuanto a formas de autentificación, los productos de Cisco pueden trabajar con *RADIUS y TACACS*[7].

Este proveedor nos ofrece soluciones de seguridad para VPN's, con los productos:

- ***Concentrador Cisco VPN 3000*:** permite el acceso remoto a las VPN, la plataforma y software del cliente incorporan alta disponibilidad y escalabilidad con las más avanzadas técnicas de encriptación y autentificación.

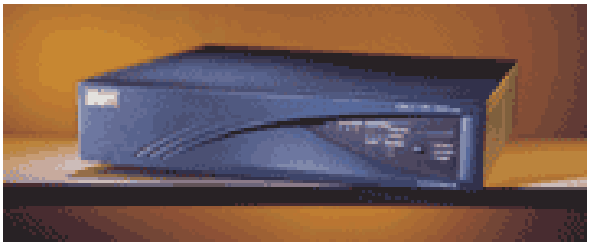


Fig. 7.1 Concentrador Cisco VPN 3000

- ***Cisco Pix Firewall*:** maneja protocolos IPSec y posee capacidad VPN de altos niveles de seguridad y desempeño.

[7] RADIUS Y TACACS, protocolos de autenticación de seguridad sobre Internet.

Los aliados de seguridad Cisco Pix son una familia de aparatos especializados para proveer poderosos servicios de seguridad a redes integradas incluyendo un estado de inspección para Firewalls, VPNs y protección de intrusos en línea.

Los rangos de la familia Cisco Pix van desde los compactos “Plug and Play” que son Firewalls de escritorio para pequeñas oficinas hasta los poderosos Firewalls Gibabits para empresas y proveedores de servicio.

Los aparatos para seguridad Cisco Pix son la solución ideal para clientes que buscan Firewalls de calidad garantizada con aplicaciones innovadoras, inspección de protocolos, servicios completos de multimedia y soporte de voz.

Es una excelente opción para organizaciones cuyas directivas de seguridad son dadas por jerarquía de la infraestructura de seguridad y dan una clara diferencia entre seguridad y operación de la red.

Estos dispositivos integran en un solo aparato Firewalls, Protección de Intrusos y Tecnologías VPN haciendo que los clientes se beneficien de seguridad reforzada, costos más bajos de propiedad y bajos costos operacionales, ya que son el resultado de compartir servicios integrados

en una sola plataforma; permitiendo tomar ventaja de los múltiples beneficios de la convergencia de datos, voz y vídeo.

La siguiente tabla proporciona pautas generales sobre la familia Cisco Pix para una elección óptima del dispositivo que se ajuste mejor a los requerimientos de las empresas.

NOMBRE	*VELOCIDAD*	*APLICACIÓN*	*USUARIOS*
Cisco Pix 501	60 Mbps	Pequeñas Oficinas	1-20
Cisco Pix 506E	100 Mbps	Pequeñas Agencias	20-99
Cisco Pix 515E	188 Mbps	Medianas Agencias	100-999
Cisco Pix 525	330 Mbps	Pequeñas Empresas	100-999
Cisco Pix 525E	400 Mbps	Grandes Empresas	1000-4999
Cisco Pix 535	1.6 Gbps	Corporaciones	+ de 500.000

Tabla 7.1 Familia Cisco Pix

Fig. 7.2 Cisco Pix 501

Fig. 7.3 Cisco Pix 506E

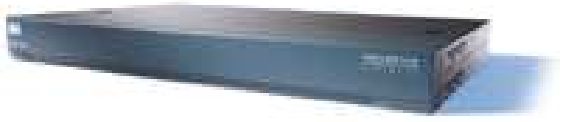


Fig. 7.4 Cisco Pix 515E

Fig. 7.5 Cisco Pix 525

Fig. 7.6 Cisco Pix 525E

Fig. 7.7 Cisco Pix 535

- ***Cisco Secure Integrated Software:*** disponible para un gran número de Ruteadores y Switches[8] que corren el IOS Cisco. Aumenta las capacidades existentes de seguridad con un firewall robusto, así como detección de intrusos, Encriptación DES, y capacidades de administración segura.

Fig. 7.8 Ruteadores Cisco Series 7600

[8] Switch, conmutador, dispositivo que conecta varias líneas de comunicación.

- ***Cisco Secure Integrated VPN Software:*** combina IPSec con firewalls robustos, detección de intrusos y capacidades de administración segura. Encriptación 3DES y autentificación por certificados digitales, claves de un sólo intento y llaves pre-compartidas. Soporta además acceso remoto, Intranet y Extranet.

- ***Cliente para VPN Cisco Secure:*** permite conectividad segura para acceso remoto, estándares IPSec, DES y 3DES.

- ***Sistema de detección de intrusos:*** provee de detección de intrusos en tiempo real. Brinda protección a LAN y Extranets, además cuenta con sensores de análisis de paquetes individuales.

A continuación se presenta una tabla que enumera las funciones y beneficios de los productos ofrecidos por Cisco

CARACTERÍSTICA	*FUNCIÓN*	*BENEFICIO*
IOS de Cisco	Las características de VPN corren en el software de Cisco.	Asegura el funcionamiento con todos los productos de Cisco.Permite la utilización de estructura ya existente.
Solución Integral	Une todos los aspectos de la red de datos, Intranet, Extranet y Dial Access.	Reduce la complejidad de la red creando una plataforma común.
Arquitectura abierta	Utiliza las facilidades de las capas 2 y 3.	Permite escoger una forma de transporte que mejor se ajuste a las necesidades.
Seguridad robusta en cuanto a autentificación de usuarios, tunneling y encriptación paquetes.	Permite la utilización segura del Internet para la interconexión de WAN.	Reduce costos por ancho de banda y administración.
Administración de ancho de banda	Administra el tráfico de la red basado en patrones de tráfico y prioridad.	Administra de mejor manera el ancho de banda a través de redes compartidas.
Integración de aplicaciones de propósito simple	Integra la administración del ancho de banda y el firrewall en el ruteador	Reduce la complejidad de la red.
Solución basada en estándares.	Uso del IPSec, L2TP, GRE, DES y 3DES	Se integra de forma transparente a la infraestructura existente.
Relación de servidor con el proveedor	Cisco provee el equipo de red utilizado en el 80% del Internet.	Alto nivel de integración a través de los proveedores de infraestructura WAN

Tabla 7.2 Funciones y Beneficios de Cisco

7.1.2 PROPUESTA TECNOLÓGICA DE 3COM

Una característica importante de los modelos de 3Com es que cuentan con la característica de firewall integrado.

Las conexiones remotas pueden ser establecidas por PPTP, IPSec y L2TP. Además se cuenta con un cliente de IPSec para los usuarios móviles que utilizan plataformas Win95, 98, NT y 2000.

En cuanto a formas de encriptación, puede manejar MPPE de 40 y 128 bits además de IPSec, DES y 3DES de 56, 112 y hasta 168 bits de longitud en llaves.

La creación de túneles seguros puede ser realizada mediante ruteadores con capacidades de VPN, o con la ayuda de software como Windows 2000.

Todos los productos corren sobre el Sistema Operativo Empresarial EOS[9]. Dependiendo del ancho de banda que se requiera, 3Com cuenta con productos como:

[9] EOS, Sistema Operativo para servidores.

- ***Office Connect NB:*** ofrece una extensa gama de servicios y protocolos WAN con el mínimo costo de propiedad, el máximo ancho de banda y máxima disponibilidad de la red.

Fig. 7.9 Officce Connect NetBuilder

- ***PathBuilder S500:*** conmutador de Nivel3, soporta encriptación 3DES y hasta 2048 túneles simultáneos, ofrece conexiones seguras a usuarios móviles, oficinas remotas y partners[10]. Está diseñado como una oficina central de una red privada virtual (VPN) de 3Com

Fig. 7.10 Conmutador PathBuilder S500

- ***Routers Multiprotocolo NetBuilder*:** incorporan compresión de datos (sobre PPP, Frame Relay y X.25), gestión inteligente del ancho de

banda, priorización de datos, filtros inteligentes, dial-on-demand[11] y tunneling de NetBIOS[12] sobre IP, tunneling con VPN y soporte NAT[13].

Fig. 7.11 Router Multiprotocolo SuperStack NetBuilder

7.1.3 PROPUESTA TECNOLÓGICA DE NORTEL NETWORKS

- ***Switch Contivity 4500***: es una solución completa para la implantación de VPN's, la cual provee un gran desempeño, además de infraestructura segura y escalable.

[10] Partners, socios
[11] Dial on demand, marcado bajo demanda.
[12] NetBIOS, interfaz de programación de aplicaciones (API) que pueden utilizar los programas en una (LAN).

Fig. 7.12 Switch Contivity 4500

Brinda a los usuarios los beneficios de ruteo, encriptación y compresión de datos, además de un control de seguridad y ancho de banda.

Los switches Contivity 4500 soportan hasta 5000 túneles simultáneos sin sacrificar el desempeño de la red.

En cuanto a seguridad todas las conexiones pueden ser encriptadas para asegurar privacidad, además que se puede obtener seguridad adicional mediante técnicas de filtrado para cada usuario o grupo de trabajo.

El encapsulado maneja los protocolos PPTP, L2F, L2TP e IPSec, con la capacidad para mantener túneles de múltiples tipos activos simultáneamente.

La autentificación puede ser realizada en una variedad de servidores externos que incluyen LDAP[14] (*Lightweight Directory Access Protocol*), RADIUS (*Remote Authentication Dial-In User Services*), Windows NT, Security Dynamics[15].

[13] NAT, Network Adresses Translation, Traductor de Direcciones de Red.

7.1.4 PROPUESTA TECNOLÓGICA DE LUCENT TECHNOLOGIES

Lucent Technologies ofrece equipos para la implantación de VPN's corporativas, como:

- ***Firewall Brick 80:*** ofrece ancho de banda protegido de 80 Mpbs, 10 Mbps con encriptación 3DES y una capacidad de manejar hasta 400 túneles simultáneos. Ideal para oficinas pequeñas y medianas, así como para clientes remotos.

Fig. 7.13 Firewall Brick 80

[14] LDAP, Protocolo compacto de acceso principal de Active Directory
[15] Security Dynamics, Seguridad Dinámica

- ***Firewall Brick 2001*:** ofrece un ancho de banda protegido de 125 Mbps o 75 Mbps con encriptación 3DES y una capacidad de manejar hasta 3000 túneles simultáneos. Ideal para empresas medianas y grandes.

Fig. 7.14 Firewall Brick 2001

- ***VPN Firewall Brick 350:*** ofrece el tamaño correcto para la ejecución y capacidad de distribución de los servicios de los niveles de seguridad, IP VPN, VLAN[16] y optimización de los servicios de banda ancha para los usuarios finales para pequeñas y medianas empresas. Puede soportar más de 300 firewalls virtuales y hasta 4.092 VLANs.

Fig. 7.15 VPN Firewall Brick 350 Empresarial

[16] VLAN, LAN Virtual, que permite la comunicación entre hosts como si estuvieran en la misma LAN física

- ***Switches y Ruteadores Foundry Networks*:** desempeño de hasta 178 Mbps y capacidad de switching total de 480 Gbps. Tipos: FastIron, BigIron, NetIron y ServerIron.

Fig. 7.16 Switches y Ruteadores Foundry Networks

Además de estos modelos de hardware, Lucent también ofrece un cliente de acceso remoto bajo el esquema de seguridad IPSec, el cual posee una seguridad robusta.

En cuanto a software para servidores de VPN's ofrece LSMS (*Lucent Security Management Server*) el cual permite una administración sencilla y centralizada, con la capacidad de administrar hasta 20000 clientes de IPSec y hasta 1000 firewalls y ruteadores.

El software del cliente para IPSec provee una solución completa de acceso remoto para usuarios individuales de computadoras PC’s desktops y laptops bajo una plataforma de Windows 95, Windows 98, Windows 2000 y Windows NT.

Además que sus características ofrecen una fácil instalación y uso, con una protección integral, ya sea que se encuentre conectado a un módem ordinario, a un ruteador WAN, a una línea digital, con cableado o de forma inalámbrica.

Estos sistemas trabajando en conjunto ofrecen una solución completa en cuanto a protección de recursos, privacidad de la información y prueba de identidad.

CARACTERÍSTICAS ESPECIALES

Opciones soportadas	NAT, revisión antivirus en el gateway, filtros extensivos, firewall integrado.
Protocolo de Encriptación	IPSec
Número de funciones soportadas simultáneamente.	3000
Características de seguridad.	Entrust, Verisign, IKE, llaves precompartidas, RADIUS, SecurID, Tockens.
Compresión	Sí (Site to Site)
SNMP Genérico soportado.	Las alarmas pueden ser enviadas como trampas SNMP de LSMS al administrador SNMP.
Software Cliente para PC.	Lucent IP Sec Client V3.0 incluido.
Aplicación de administración.	Lucent Security Manager Server V5.0, Java GUI, CLI residente en plataformas de windows NT, y Sun Solaris.
Redundancia	Túneles primarios y secundarios.

Tabla 7.3 Características Especiales de Lucent Technologies

7.2. PROVEEDORES DE EQUIPOS

7.2.1 ADEXUS

Es una empresa a nivel internacional con probada capacidad y experiencia, que posee oficinas en Estados Unidos, Chile, Perú y Ecuador. Es uno de los principales proveedores de soluciones en el área informática a nivel empresarial, corporativo e incluso gubernamental.

En Ecuador es una empresa dedicada a la provisión de soluciones y servicios especializados con contenido tecnológico de sistemas de información y de comunicaciones, integrando recursos humanos, equipos, programas y servicios varios; para ello cuenta con dos oficinas una en Quito y otra en Guayaquil.

Los servicios que brinda en Ecuador son un importante valor agregado a la gestión técnica y comercial de sus clientes. Para esto, posee un equipo permanente de especialistas en las áreas de: análisis y diseño de bases de datos, seguridad computacional, administración y operación de sistemas, ingeniería de sistemas, comunicaciones y redes, diseño y desarrollo de aplicaciones, entre otros.

Paralelamente proporciona un completo servicio post-venta que incluye consultoría, soporte, mantenimiento, capacitación, levantamiento de requerimientos y recomendaciones para próximas etapas.

Posee alianzas comerciales con los siguientes proveedores de equipos, por lo cual sus precios son los más competitivos del mercado:

- ***Agilent*:** soluciones de Comunicaciones
- ***Cisco Systems*:** soluciones para Networking de datos
- ***Extreme Networks*:** redes Gigabit Ethernet
- ***Marconi:*** Switches ATM
- ***Rad:*** productos de Conectividad, Telecomunicaciones y Redes
- ***RSA Security*:** seguridad para acceso a redes basadas en Token

Además, al ser Internet actualmente un área de gran desarrollo en todo el mundo, cuyas tecnologías evolucionan a diario. Adexus en Ecuador dispone en este sentido de una completa gama de productos y servicios orientados a éste ámbito, entre los que se cuentan: soluciones de comercio electrónico; diseño, desarrollo y hosting de sitios Web; desarrollo de aplicaciones Java; seguridad de accesos; desarrollo de contenido Web e Intranet; entre otros.

En nuestro país uno de los proyectos exitosos de Adexus fue iniciar a Andinanet en sus operaciones como ISP, otorgando acceso a Internet, gracias al aporte tecnológico de la agencia en Ecuador.

En la ejecución del proyecto se utilizaron las más avanzadas tecnologías provistas por diversos fabricantes, entre los que destacan Compaq Computers, Sun Microsystems, Cisco Systems, Lucent Technologies y Paradyne, líderes en sus respectivos mercados, lo que garantizó la solidez técnica de la solución.

7.3. PROVEEDORES DE ENLACE

Al ser las VPNs a través del Internet una tecnología en desarrollo para comunicaciones MAN y WAN, en Ecuador no existen proveedores que las oferten como un servicio, por lo cual son las mismas empresas las que tienen que configurar sus equipos y contratar un proveedor de enlace que se ajuste a las necesidades de las mismas.

En nuestro país el organismo que se encarga de la regulación de las telecomunicaciones es la Superintendencia de Telecomunicaciones, que ha

concesionado la licencia para ofrecer servicios de transmisión de datos a las empresas:

- Andinatel
- Conecel (Porta)
- Etapa Telecom
- Grupo Bravco
- Impsatel del Ecuador
- Megadatos
- Nedetel
- Otecel (Movistar)
- Pacifictel
- Suratel
- Telconet
- Transelectric
- Transnexa

El mercado de transmisión de datos se encuentra repartido de la siguiente manera:

EMPRESA	*CIRCUITOS*
Suratel	11814
Andinatel	3952

Impsat	1245
Megadatos	915
Pacifictel	671
Telconet	227
Etapa	203
Conecel	166
Otecel	77
Transelectric	56
Transnexa	52
Nedetel	33
Bravco	12

Tabla 7.4 Distribución Mercado de Transmisión de Datos

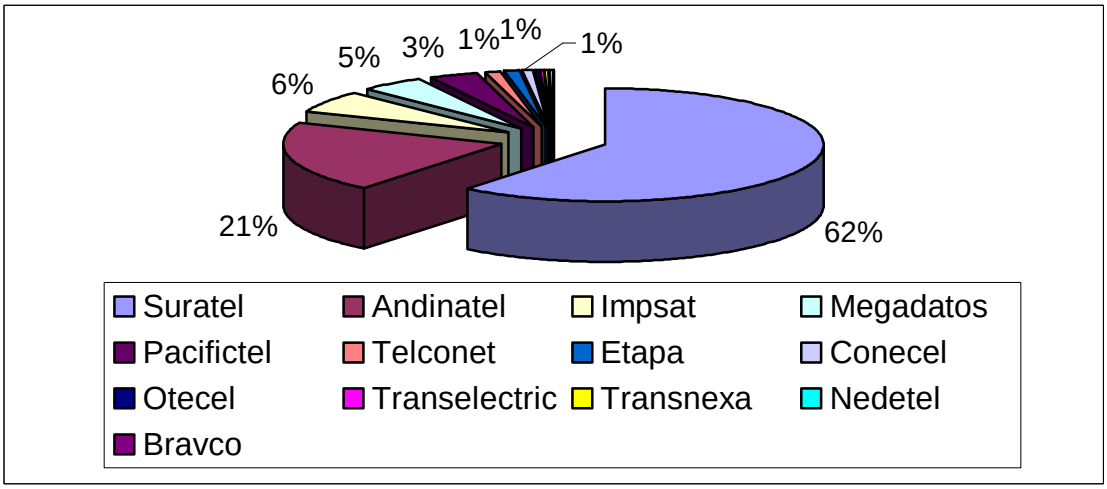


Fig. 7.17 Distribución Mercado Transmisión de Datos

7.3.1 SURATEL

Es un grupo empresarial sólido, formado por: Webmaster, Grupo TVCable, TVCable, Satnet y Suratel con tecnología de vanguardia para ofrecer soluciones en telecomunicaciones, entretenimiento y servicios afines.

Con su tecnología e infraestructura propia, puede enlazar redes en modalidad punto a punto y punto multipunto: Interconexión de redes LAN, Intranet, Extranet, Mainframes, emulación de terminales, pudiendo soportar todo tipo de aplicaciones que requieren un acceso dedicado.

Dos de los servicios que ofrece para el enlace vía Internet son:

- ***Clear Channel***: servicio dirigido a aquellos clientes que tienen la necesidad de un canal extremo a extremo dedicado, con una disponibilidad total garantizada de su ancho de Banda, el cual podrá ser usado en cualquier momento.

  Es recomendable para aquellos clientes que intercambian grandes flujos de información por periodos largos de tiempo.

  De acuerdo al equipamiento del que se dispone los canales pueden ser desde 64 Kbps hasta 4096 Kbps, incrementándose en pasos de nx64 Kbps.

El cliente puede usar su canal conforme a sus necesidades y aplicaciones, sin ningún tipo de restricción en cuanto a protocolos.

- *Clear Channel IP Connect:* un servicio de LAN sobre WAN bajo canales dedicados y/o concentrados en un solo origen. Permite que redes de área local geográficamente dispersas aparezcan como una sola red lógica. Se orienta a empresas pequeñas. Provee una velocidad de enlace de n x 64 Kbps

7.3.2 ANDINANET

Es una división de ANDINATEL S.A. que satisface las necesidades de conexión al Internet de clientes, empresas, proveedores de servicios de Internet y compañías de telecomunicaciones, brindando soluciones integrales de red y asesoría personalizada de acuerdo a las necesidades de las mismas.

Las ventajas que esta empresa ofrece son:

- Enlaces que van desde 64k, 128k hasta ISDN y ADSL.

- Tecnología de última generación.
- Tráfico de Internet vía Cable Panamericano de Fibra Óptica.
- Redundancia Satelital.
- Acceso ilimitado para el servicio de Internet.
- Cobertura Nacional.
- Infraestructura de telecomunicaciones propia.
- Personal altamente capacitado.
- Ancho de banda Ilimitado.
- Servicio Técnico las 24 horas.
- Planes tarifarios a la medida de la empresa.

Andinanet en su sitio web ofrece el servicio VPN pero no lo implementan verdaderamente, además del servicio de Clear Channel, Frame Relay, ISDN, ADSL y Dial up Networking.

Para la implementación de una VPN se necesita del Clear Channel que actúa como una conexión permanente al Internet sin la necesidad de establecerla vía telefónica, dicha conexión se da desde la empresa a un ISP o a una sucursal de la misma.

Los canales dedicados se miden por el tamaño de su capacidad y están disponibles en los siguientes anchos de banda: 64K, 128K, 256K, 512K,

1536K (T1), 2048K (E1), a mayor ancho de banda mayor capacidad de transmisión.

Desde su creación Andinanet ha procurado captar el mercado ofreciendo un excelente servicio para ganar y retener clientes por lo cual ha tenido un crecimiento progresivo importante.

CAPÍTULO VIII

RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

8.1 RESULTADOS

La Empresa tiene una gran fortaleza sobre otras que están en su mismo campo de acción, pues el sistema que se encuentra desarrollado e implementado cumple a cabalidad las necesidades de ésta en cuanto al procesamiento de información.

Desde la creación de la Empresa hasta la presente fecha los dueños de la misma han dado preferencia en el Departamento de Sistemas al desarrollo de software especializado en el área del Turismo descuidando el área de las comunicaciones, sin tomar en cuenta el incremento paulatino de las agencias dispersas geográficamente, así como el volumen de información que necesitan transferir entre ellas; aspecto vital en la actualidad.

Quimbaya Tours es una empresa con un rápido crecimiento, con buena administración y tecnología de punta en el área de Sistemas, por ello no es conveniente seguir manteniendo las actuales formas de comunicación entre agencias, ya que esto causa pérdida de tiempo y dinero.

A continuación se precisan los aspectos en los cuales el presente Estudio puede colaborar en la optimización de las comunicaciones, seguridad de las redes LAN de cada agencia, conexiones remotas, además de la factibilidad técnica, operativa y económica.

Las encuestas realizadas a los Asistentes del Gerente de Sistemas en cada agencia tuvieron como objetivo obtener información acerca del tipo de acceso a Internet, características de los Servidores, seguridad de la información y del Departamento de Sistemas.

En el aspecto de seguridad una vez tabulada y analizada la información se concluyó que las formas de aplicarla son muy elementales debido a que en cada Agencia prevalece el criterio del Asistente del Gerente de Sistemas por lo cual no existen Planes de Contingencia en función de empresa y esto quedó expuesto con un suceso ocurrido a finales del año anterior que por cuestiones ajenas a la Holding se cayó el enlace a Internet por unas horas lo cual demostró lo frágil que resulta la configuración de la red así como el no contar con enlaces de respaldo que cubran este tipo de eventualidades.

Razón por lo que se recomienda elaborar un Plan de Seguridad Estandarizado el mismo que deberá ser puesto en práctica en cada una de las Agencias.

Se deberá conformar un comité de seguridad para establecer tareas, actividades y responsabilidades, el que se encargará de documentar y evaluar la red, designar un administrador para la misma y los métodos de control de acceso mediante software o hardware.

Paralelamente se debe realizar una auditoría de seguridad y detección de intrusos para descubrir las vulnerabilidades de la red y así poder hacer un consenso entre las Agencias sobre las Políticas de Seguridad, Políticas de Control de Virus, Planes de Contingencia y Recuperación ante catástrofes que cada una requiere y lograr finalmente un estándar para la Empresa.

El siguiente aspecto analizado es la optimización de la transferencia de información con la implantación de la Tecnología VPN a través de un Clear Channel como enlace a Internet, siendo la mejor opción para Quimbaya Tours tomando en cuenta la relación Costo/Beneficio, sobre otras formas de conexiones remotas.

Si se tiene en cuenta el servicio Dial-Up la desventaja es el costo de la llamada que es por minuto conectado, es larga distancia, además no cuenta con la calidad y velocidad adecuadas.

Al tener una línea privada el servicio contratado es caro si se toma en cuenta que dependiendo del proveedor está compartida en relaciones de 4 a 1, 8 a 1 o más, es decir 4 o más usuarios acceden al Internet a través de la misma línea, disminuyendo notablemente calidad y velocidad de transmisión.

Los servicios anteriores son formas de enlace a Internet mientras que la VPN es una red de comunicaciones privada implementada sobre una infraestructura pública, donde los datos viajan exclusivamente por el túnel que ésta crea, garantizando privacidad e integridad, se tiene acceso limitado de usuarios autorizados por ello a pesar de ser compartida, tiene todas las características de una red privada.

En consideración a que las Agencias se encuentran en diferentes países de América Latina, la transferencia de información se la requiere en el menor tiempo posible por lo que se necesitaría de un Clear Channel 1 a 1 que garantice el ancho de banda contratado e incremente la velocidad de transmisión.

Se contempla como óptima la implantación de esta tecnología mediante equipos ya que ofrecen versatilidad para trabajar con diferentes Sistemas Operativos, lo cual es una gran ventaja sobre la implantación vía software ya que si se decide cambiarla es necesario saber cómo funciona la VPN en cada plataforma y volver a configurar los computadores, lo que no sucede con los equipos que una vez configurados se adaptan a la red.

Por ello se realizó un análisis de calificación en base a criterios de evaluación que otorgó el Gerente de Sistemas de acuerdo a prioridades empresariales para sugerir equipos, sumando en total un 100% los cuales se ordenaron como se indica a continuación:

CRITERIO	*PORCENTAJE (%)*
Seguridad	40
Precio	30
Soporte de protocolos	15
Capacidad	15
TOTAL	**100**

Tabla 8.1 Criterios a ser tomados en cuenta para la Evaluación

Como se puede ver en la tabla anterior, el aspecto que mayor peso tiene es la seguridad, ya que esto es realmente lo que se considera más importante al momento de implantar una VPN, sobretodo en la Empresa ya que por su

actividad, la seguridad de la red es un aspecto de vital importancia, sobre la cual cualquier cambio debe ser realizado de forma muy cuidadosa.

El siguiente aspecto de mayor peso que se consideró fue el precio, esto es debido a que en los aspectos restantes, como capacidad y soporte de protocolos se vio que todos los equipos garantizan estos servicios. Por ejemplo en el caso de capacidad, hay equipos que ofrecen 2000 conexiones simultáneas lo cual resulta excesivo para el uso que se le daría a la VPN ahora y en el futuro, y en cuanto al aspecto de soporte a protocolos todos ofrecen los más comunes como IPSec, PPTP y las formas más frecuentes de encriptación sobre las cuales se ha pensado diseñar la VPN.

Para tener un mejor criterio de selección se ha realizado un resumen de las principales características que ofrecen los equipos de las diferentes marcas.

PROVEEDOR	ENCAPSULACIÓN	ENCRIPTACIÓN	SEGURIDAD	AUTENTICACIÓN	EXTRAS
CISCO	IPSec (capa 3), L2TP, PPTP, L2F, GRE	DES, 3DES, RC4, MPPE	Verisign, Entrust	RADIUS, TACACS	Detección de intrusos, QoS, actualización de IOS.
3COM	PPTP, IPSec, L2TP	MPPE, DES, 3DES	N/A*	N/A*	Hardware de encriptación, soporta hasta 2048 túneles.
NORTEL NETWORKS	PPTP, L2F, L2TP, IPSec	RC4/RSA, DES, 3DES	N/A*	LDAP, RADIUS, Windows NT, Security Dynamics, Axent	Soporta hasta 5000 túneles.
LUCENT TECHNOLOGIES	IPSec	3DES	Verisign, Entrust	RADIUS, SecurID Tokens	Cliente IPSec, soporta hasta 3000 túneles, ancho de banda de 75 Mbps, 3DES.

Tabla 8.2 Tabla Comparativa de las características de Equipos

** N/A No Aplica*

Tomando en cuenta las características anteriores de las diferentes marcas de equipos se les dio una calificación sobre 5 para lo que es Seguridad, Soporte de Protocolos, Capacidad y Precio:

PROVEEDOR	*SEGURIDAD*	*SOPORTE DE PROTOCOLO*	*CAPACIDAD*	*MENOR PRECIO*	*TOTAL*
CISCO	3	4	1	4	**12**
3COM	1	2	2	3	**8**
LUCENT TECHNOLOGIES	4	1	3	1	**9**
NORTEL NETWORKS	2	3	4	2	**11**

Tabla 8.3 Tabla Comparativa en Base a Criterios de Evaluación

Criterios de Evaluación:

1 Deficiente
2 Malo
3 Bueno
4 Muy Bueno
5 Excelente

A continuación se muestran los resultados de la evaluación anterior:

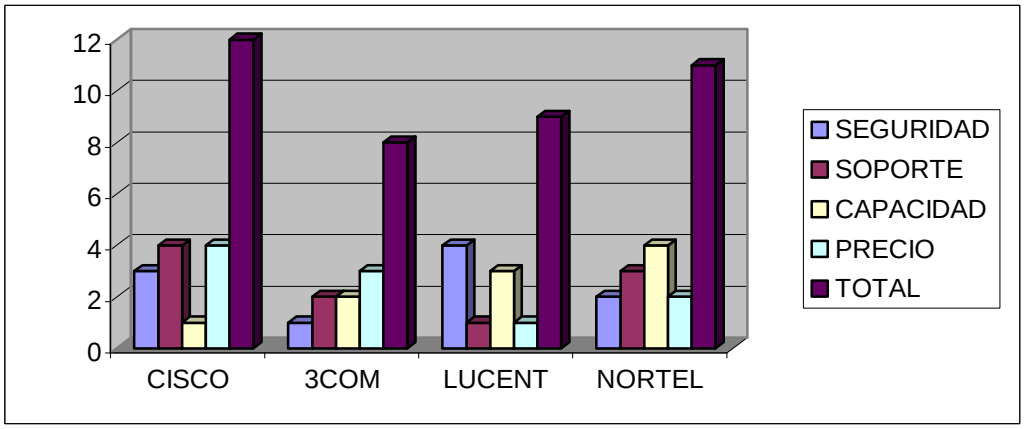


Fig. 8.1 Cuadro Comparativo por Marcas de Equipos

Como se puede observar en la gráfica en el análisis de los equipos para implementar la VPN, Cisco es la mejor opción aunque con una diferencia mínima con respecto a Nortel Networks.

La principal ventaja que ofrece Cisco como infraestructura base para implementar VPNs radica en el precio, pues tiene una familia de equipos especializados que concentran en un solo dispositivo ruteadores, firewalls, encriptadores y pueden establecer múltiples túneles virtuales simultáneos (Cisco Firewall Pix).

Cisco tiene otra ventaja en cuanto a protocolos manejados para el encapsulado de paquetes y el establecimiento de los llamados túneles virtuales, ya que además del IPSec soporta L2TP, L2F, GRE y PPTP

En el tema de seguridad, todas las marcas analizadas ofrecen encriptación de tipo 3DES que es el estándar utilizado por ser uno de los más seguros. Sin embargo como se puede ver en la tabla 7.2 algunos de los equipos manejan además otros tipos dando un valor agregado al producto. Tal es el caso de Cisco que además de 3DES ofrece encriptación DES, MPPE, y RC4.

En cuanto a lo que son proveedores de equipos y enlace se ha tomado en consideración las empresas que brindan precios competitivos en el mercado además de soluciones específicas en telecomunicaciones sin olvidar la Calidad del Servicio, asesoría permanente y su probada experiencia en desarrollo de proyectos con instituciones de renombre.

Una vez analizadas las formas de enlaces, equipos y proveedores se presentan las siguientes tablas con la información que ayudará a la toma de decisiones.

1. Velocidad de Enlace

ENLACE	*VELOCIDAD UP (Mbps)*	*VELOCIDAD DOWN (Mbps)*
Dial Up (Incluida llamada telefónica)	0.32	0.32
Línea Dedicada Compartida	128	128
Clear Channel PPP	520	520

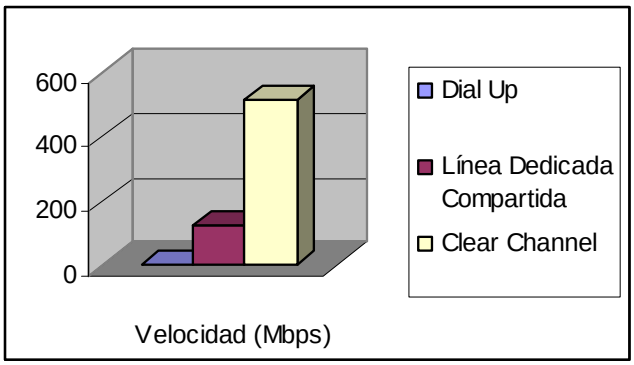


Fig. 8.2 Velocidad de Enlace

El servicio Clear Channel ofrece una mayor velocidad y garantiza el ancho de banda contratado pues no se comparte con otros usuarios.

2. Precios por mes de acuerdo al Proveedor de Enlace.

PROVEEDOR	*DIAL UP (incluye llamada telefónica)*	*LINEA DEDICADA COMPARTIDA*	*CLEAR CHANNEL*
Andinanet	166*	336*	952*
Ecuanet	250*	392*	980*
Otecel	720*	422*	1080*

**** Valores incluyen IVA***

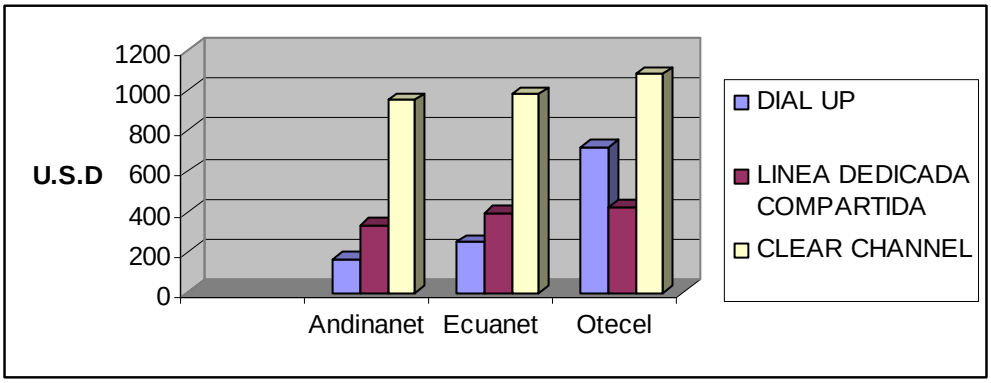


Fig. 8.3 Precios de acuerdo al Proveedor de Enlace

Andinanet tiene un precio más competitivo porque la tecnología y equipos son propios y ocupa su división de carrier que es Andinadatos la cual maneja su propia base tecnológica a diferencia de los demás ISP's.

3. Precios de los equipos necesarios para implantar una VPN.

Equipo	*Cisco*	*Nortel*	*Lucent Technologies*	*3COM*
Switch (24puertos)	620*	0	260*	225*
Router	0	0	910*	850*
Firewall	0	0	730*	680*
Equipo Integrado	950*	1820*		
Total	1570*	1820*	1900*	1755*

**** Valores no incluyen IVA***

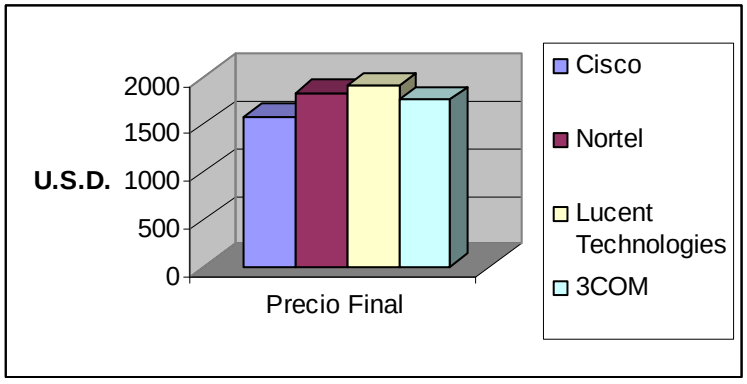


Fig. 8.4 Precios de Equipos para implantar una VPN

Cisco al tener un equipo integrado para la implementación de VPNs reduce considerablemente los costos de inversión.

4. Proveedor de Equipos.

PROVEEDOR	PRECIO OFERTADO	ASISTENCIA TÉCNICA	PROYECTOS IMPLANTADOS	TOTAL
ADEXUS	5	4	5	14
SONDA	3	2	1	6
DOS	3	1	1	5

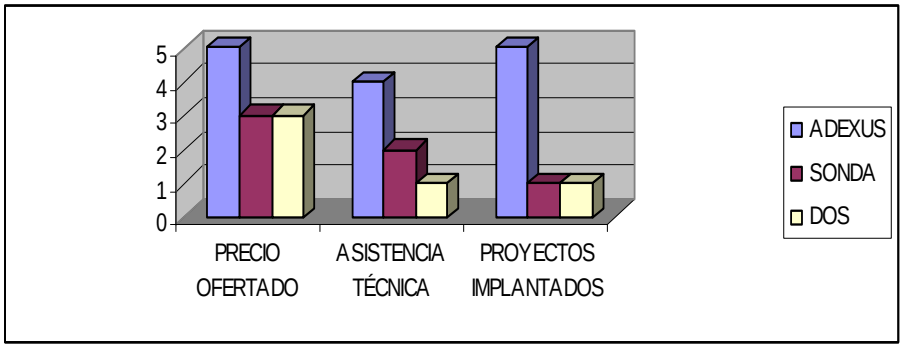


Fig. 8.5 Proveedores de Equipo

Criterios de Evaluación:

1. Deficiente
2. Malo
3. Bueno
4. Muy Bueno
5. Excelente

Siendo Adexus el broker de Cisco para Ecuador ofrece precios más competitivos en el mercado y garantiza el servicio post-venta.

Al tener todas las Agencias conectadas en red mediante una VPN se obtienen beneficios como:

- Reducción en costos de llamadas telefónicas internacionales.
- Eliminación de viajes imprevistos que realiza el Gerente de Sistemas y viáticos para sus gastos.
- Optimización de la Administración de toda la red.
- Acceso remoto a información corporativa.
- Control de usuarios.
- Mejoramiento de la Calidad de Servicio.
- Intercambio de Información en tiempo real.
- Monitoreo de las tramas dentro de la red.
- Facilidad de uso.

La implantación de la VPN le significará a la Empresa solamente una inversión de 1050 USD por Agencia, que es lo que cuesta el Cisco Firewall Pix, ya que se utilizará la infraestructura existente y el servicio ADSL que todas las Agencias tienen contratado sobre el cual se configurará esta tecnología.

Si se considera que la Holding está conformada por 11 Agencias Receptoras y 4 Oficinas Comerciales la inversión total sería de 15750 USD y se reducirían los egresos anuales que se producen en América Latina, los mismos que se detallan en la siguiente tabla:

EGRESOS AMÉRICA LATINA	***SIN VPN USD / AÑO***	***CON VPN USD / AÑO***
20 Viajes Programados	14000	7000
2 Viajes Imprevistos	1400	0
Viáticos	8000	3500
Llamadas Internacionales	24000	10000
TOTAL	***47400***	***20500***

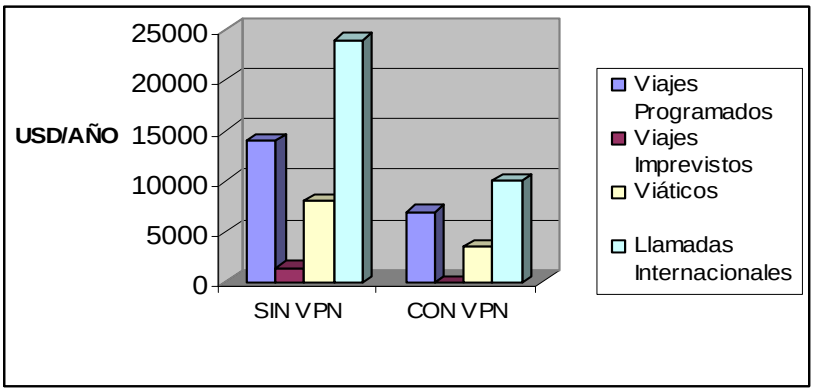


Fig.8.6 Egresos Operativos Anuales Agencias América Latina

Del análisis anterior se deduce que económicamente es factible para la Empresa realizar un egreso de esta magnitud, pues en un año se gastan 47400 USD en mantenimiento del Sistema al no contar con una red de acceso remoto; mientras que con la implantación de la VPN los gastos se reducirían a partir del segundo año en un 57%.

Ya que se debe tener en cuenta que el primer año a los egresos ya reducidos se debe añadir el valor de la inversión lo que representaría un egreso total de 36250 USD que da un ahorro neto del 24% comparados con los egresos actuales por año que realiza la Empresa.

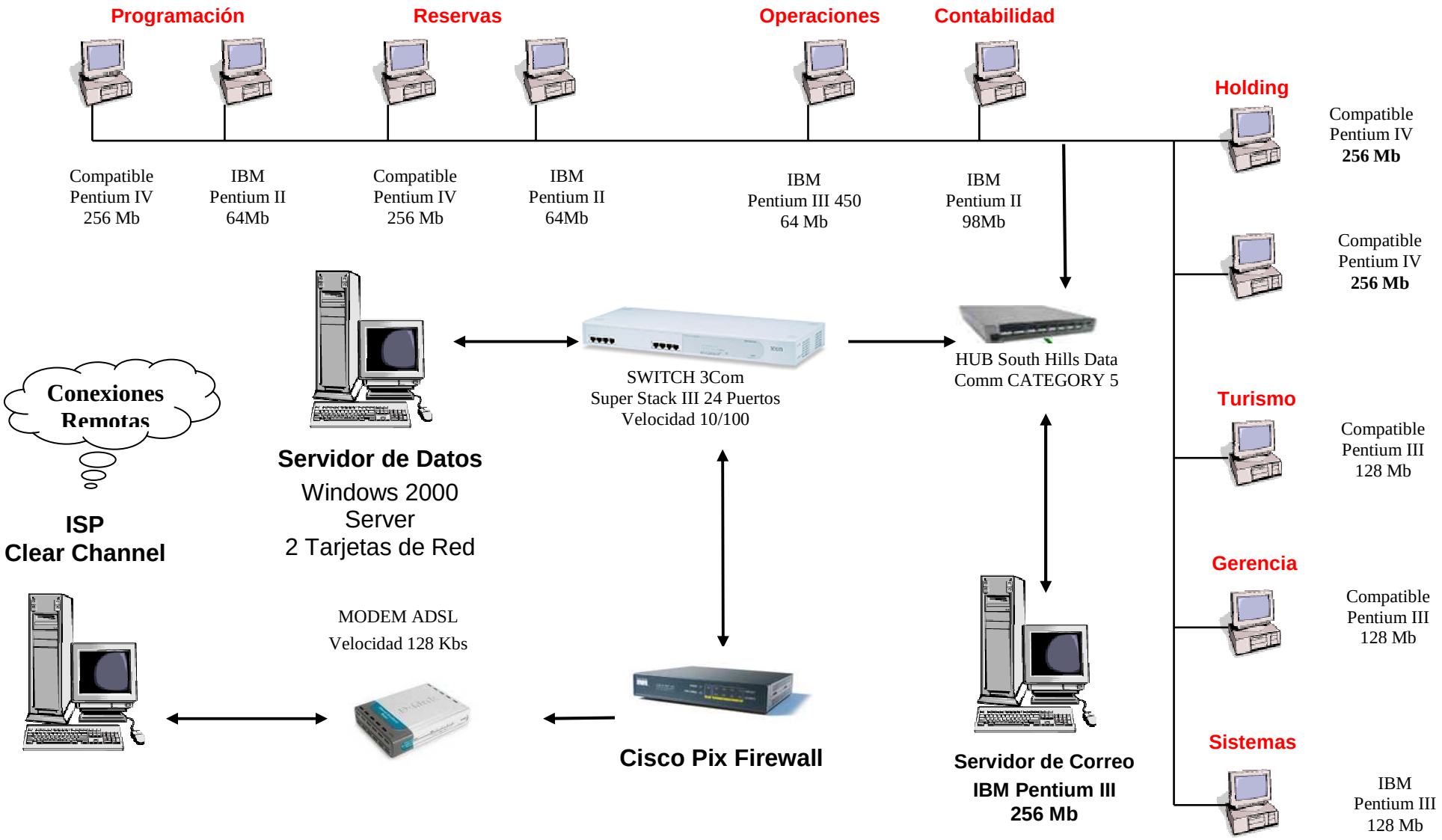
No se requiere contratar más profesionales para la configuración de los equipos y la administración de la red porque tanto el Gerente Regional de Sistemas como cada uno de sus Asistentes tienen experiencia previa así

como cursos de capacitación en estas áreas, además contarían con el respaldo del proveedor de los equipos, el cual brinda asesoría permanente; por ello operativamente es factible la implantación de la VPN.

Técnicamente es factible implantar la VPN pues al poseer cada una de las Agencias la infraestructura y el enlace necesarios, se requieren cambios mínimos en las arquitecturas de las redes LAN para adaptarse a la nueva tecnología, además de que se pueden optimizar al máximo recursos mal utilizados.

Como un ejemplo de la nueva arquitectura, utilizando el Cisco Firewall Pix, se presenta el diseño de la LAN en Ecuador.

ESQUEMA DE RED QUIMBAYA TOURS "*ECUADOR*"



8.2 CONCLUSIONES

- Una VPN a través del Internet es un medio de transmisión de datos segura y una solución en el área de las comunicaciones para una empresa que tenga agencias dispersas geográficamente.
- Puede ser comparada con un sistema de líneas dedicadas usadas por una sola empresa, la idea de esta tecnología es brindar las mismas capacidades del sistema anterior a un costo mucho menor utilizando la infraestructura pública compartida.
- La tecnología VPN en este momento se encuentra en desarrollo y tiene grandes proyecciones de crecimiento e implantación debido a que reduce costos, brinda mayor seguridad y no es necesario un proveedor de servicio, sino solamente un proveedor de enlace.
- Si surgen problemas en las VPNs, no es porque estas redes sean deficientes, normalmente surgen complicaciones por el QoS entregado por el proveedor de enlace, mala configuración de los equipos o problemas de hardware.
- La optimización del túnel de datos de una VPN depende del ancho de banda real que es entregado por el proveedor de enlace así como la velocidad de transmisión de los datos dentro del túnel.
- Si el canal de enlace es compartido se pueden tener problemas al momento de transmitir datos, especialmente en lo que es velocidad, ya

que dependiendo de como el proveedor divida el canal para múltiples usuarios se tiene un ancho de banda real entregado, por ejemplo en una relación de 4 a 1 (4 usuarios para 1 canal), 8 a 1, etc., en comparación al ancho de banda contratado.

- A mayor ancho de banda tenemos mayor velocidad de transmisión dependiendo del peso de datos que se maneje.
- Debido a que la pérdida de la información puede comprometer el éxito de una empresa se hace indispensable el contar con métodos de seguridad en la red para proteger lo que es información sensible como datos de productos, reportes financieros y planes de marketing; por ello el protocolo IPSec fue creado para brindar seguridad en comunicaciones privadas de red sobre protocolos IP usando procesos criptográficos.
- Los procesos de encriptación ofrecen una gran protección en contra de ataques o intrusiones a la red tanto internas como externas, constituyéndose en uno de los métodos más confiables para proteger datos privados en un ambiente público.
- El protocolo IPSec puede reforzar su función implementando directivas de seguridad, las cuales son propiedades o reglas que definen el nivel de seguridad que se desea en una empresa.
- El método más seguro para encriptación de datos sobre VPNs es el 3DES, usa tres claves de 56 bits, es decir procesa cada paquete tres

veces usando una clave única cada vez; lo que le da un factor de ventaja de 2.5 respecto a la seguridad aunque reduce la velocidad de procesamiento en comparación a otros métodos de encriptación.

8.3 RECOMENDACIONES

- Se recomienda a la Empresa que para mejorar sus comunicaciones considere la implantación de redes VPN a través del Internet, para tener una transmisión de información más eficiente, en el momento que se requiera sin sufrir retrasos.
- La implantación de una VPN abaratará costos de operatividad, en un primer momento se requiere hacer inversión para la compra de los equipos pero se obtiene un beneficio a corto plazo además que se optimiza el uso del Internet.
- Es mejor que la Empresa compre y configure los equipos para implantar esta tecnología.
- Para que la Empresa tenga un mejor manejo de transmisión de datos a través de una VPN se recomienda contratar servicios de Internet de banda ancha en cada una de sus Agencias.

- Las VPNs a través del Internet para su funcionamiento necesitan de IPs públicas para cada Servidor de red VPN, por ello la Empresa necesitaría mínimo una IP pública por Agencia.
- En el caso que la Empresa decida no comprar hardware adicional y desee utilizar sus Servidores de Intranet como Servidores VPN se recomienda que estos tengan dos tarjetas de red, una para la red interna y otra para el acceso remoto, pues el momento en que se lo habilita para el acceso remoto, si cuenta con una sola tarjeta, la Intranet se quedará sin Servidor ya que estará siendo ocupada por la conexión VPN.
- Si se opta por implementar la VPN mediante software se debe configurar el IPSec para brindar seguridad a la conexión VPN, además se deben añadir directivas de seguridad acorde a las necesidades de los usuarios, pudiendo fijarse tiempos de conexión, acceso a equipos, acceso a información entre otros.
- En cuanto a los equipos basándose en los resultados descritos anteriormente se recomienda la adquisición de equipos Cisco en este caso para la implantación de la VPN el Cisco Firewall Pix, ya que al ser un dispositivo integrado abarata costos al no ser necesario comprar individualmente routers, firewalls y encriptadores.
- Además se recomiendan los equipos Cisco porque la mayor parte del Internet está basado en su infraestructura, adicionalmente al tener un software propio para sus equipos denominado IOS Cisco permiten

ofrecer soluciones que se pueden aplicar en equipos de la misma marca con una simple actualización del IOS.

- En cuanto a proveedores de equipo se recomienda a la empresa Adexus por ser el broker de Cisco para Ecuador, por ello sus precios son comercialmente competitivos además que son los únicos que entregan directamente servicios post-venta, como mantenimiento y asesoría personalizada.
- Respecto al proveedor de enlace se recomienda contratar el servicio de Andinanet por su ventaja en costos, mejor ancho de banda, servicio al cliente, tasa de error por enlace menor a las otras empresas, experiencia y calidad de servicio.

RESUMEN

La carrera de Ingeniería en Sistemas, al estar sometida a un cambio vertiginoso y constante, con nuevas tecnologías que aparecen día a día, ha llevado a realizar un estudio de factibilidad aplicable a una empresa real, en el campo del intercambio de la información.

Es así como Quimbaya Tours International Holding ha decidido auspiciar un estudio sobre *VPN's* (*Virtual Private Network, Redes Privadas Virtuales*) a través del Internet y la forma de hacerla lo más óptima posible, sobre la base del cual podrá o no, tomarse la decisión final de su implantación.

Por esta razón se realizará una investigación acerca de las VPN's y los diversos puntos que se involucran, como lo es la seguridad, la tecnología existente, los proveedores del servicio y equipo para la implantación de una VPN, analizándose los factores a favor y en contra que lleven a elegir la mejor alternativa.

El presente estudio investigativo está distribuido en ocho capítulos, en los cuales se desarrollan los siguientes temas.

El primer capítulo (INTRODUCCIÓN) hace referencia a los antecedentes, justificación, objetivos general y específicos, del tema a tratar; se aclara el alcance y las limitaciones de la investigación, así como la metodología a emplearse.

El segundo capítulo (SITUACIÓN ACTUAL DE LA TRANSMISIÓN DE DATOS EN "QUIMBAYA TOURS INTERNATIONAL HOLDING") es una descripción formal de la Empresa, campo de acción, posicionamiento en el mercado y un análisis de la situación actual en el tema de transmisión de datos.

El tercer capítulo (FUNDAMENTO TEÓRICO) contiene una breve investigación de lo que es transmisión de datos, tipos de redes, y las formas de interconexión entre éstas, que actualmente utilizan las empresas a nivel mundial.

El cuarto capítulo (TECNOLOGÍA VPN) hace referencia a lo que es esta tecnología, requerimientos básicos, tipos, ventajas y desventajas, además el Internet como medio de comunicación y la tecnología Tunneling.

El quinto capítulo (SEGURIDAD) trata un tema tan complejo como es la seguridad computacional, riesgos informáticos, políticas de seguridad, medios de protección, criptografía y autenticación.

En el sexto capítulo (VPN SOBRE WINDOWS 2000 ADVANCED SERVER) se realiza una práctica de la configuración de una VPN sobre este sistema operativo, además se prueba la transmisión de datos dentro de la red utilizando algunas herramientas para el monitoreo de paquetes.

El séptimo capítulo (PROVEEDORES DE EQUIPO Y ENLACE) realiza el análisis de los proveedores para la implantación de una VPN; factores a favor y en contra para elegir a uno de ellos en base a las características y tecnología que ofrece.

El octavo capítulo incluye los RESULTADOS, CONCLUSIONES Y RECOMENDACIONES que el presente estudio ha generado, para de acuerdo a ello cubrir las necesidades que tiene la Empresa, ya sea adoptando cambios tecnológicos o modificando la tecnología existente.

Finalmente se adjuntan Anexos, Glosario de Términos y Bibliografía.

ANEXO 1

Seguridad Informática en las Diferentes Oficinas Comerciales

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**ARGENTINA**
Nombre:	**MARIANO OLIVEIRA**
Cargo:	**ENCARGADO DE SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL			
Otros	**256 kbps**	**512 kbps**	
Nombre del ISP:	**DATAMARKETS A TRAVÉS DEL SERVICIO FIBERTEL (CABLEMODEM)**		
Contacto:	**GISELLE TAMAROFF**	Teléfono:	**0810-333-3282**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen? **No es dial up, es el adsl anterior que no se dio de baja todavía**			
Nombre del ISP:			
Cuenta de Acceso:		Contraseña:	
Contacto:		Teléfono:	
Usuario en que está configurada la cuenta:			
Departamento al que pertenece:			

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:			
Marca:	**IBM**	Modelo:	**NETVISTA**
Serie:		Procesador:	**P IV 2.4**
Memoria:	**128 Mb**	Disco:	**20 Gb IDE**
Software que utilizan:	**IMPLEMENTACION EN KIPUX**		

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**IBM**	Modelo:	**Xcentre x205**
Serie:		Procesador:	**P IV**
Memoria:	**512 Mb**	Disco:	**36 Gb SCSI**
Sistema Operativo:	**Windows 2003 Server**		
¿Tienen algún patrón para generar las claves?	**Si por el momento.**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Backup de Windows 2003**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Sistema de Turismo Sistur 5.5** **Sistemas de Contabilidad Bejerman** **Archivos de mails PST de los usuarios** **Archivos de Datos de los Usuarios** **Archivos de Datos de uso común**
¿Con qué frecuencia sacan los respaldos?	**Hasta hoy una vez por semana. A partir de la próxima semana se automatizará para que se haga diariamente**
¿Qué dispositivo utilizan para los respaldos?	**Tape BackUp**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**No**
¿Qué software antivirus utiliza?	**McAfee Scan Antivirus**
¿Con qué frecuencia actualiza su antivirus?	**Diariamente en forma automática**
¿Tienen plan de contingencias en caso de Contagio de virus?	**SI**

¿Tienen plan de contingencias en caso de pérdida de información?	**SI**
¿Tienen plan de contingencias en caso de daños de equipos?	**NO, pero se encuentra en reparación un equipo IBM que quedará libre y se podrá utilizar en dichos casos**

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:		No, Porqué:	**Se comparte con el Gerente Administrativo en forma Part Time**
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué. **NO. El departamento de sistemas se esta armando de a poco, por lo tanto todavía no se ha decidido si alguien más en la oficina tendrá acceso a los servidores, y hasta que punto podrá trabajar en ellos**			
¿Con qué seguridades cuenta el Departamento de Sistemas: **Ninguna**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:		Contacto	
Teléfono:		Frecuencia:	
¿Qué equipos reciben este mantenimiento?			

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**BOLIVIA**
Nombre:	**NATALY MIRANDA ALVAREZ**
Cargo:	**ENCARGADA DE SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica	**Si**		
ADSL		**Si**	
Otros			
Nombre del ISP:	**ENTEL**		
Contacto:	**DEPARTAMENTO DE INTERNET**	Teléfono:	**800103638**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:			
Cuenta de Acceso:		Contraseña:	
Contacto:		Teléfono:	
Usuario en que está configurada la cuenta:			
Departamento al que pertenece:			

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	
Marca:	**IBM**	Modelo:	**8305-24S**
Serie:	**PC300 GL4S**	Procesador:	**PENTIUM 4**
Memoria:	**256 MB de RAM**	Disco:	**40 Gb**
Software que utilizan:	**KIPUX SERVER**		

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Sistema Operativo:			
¿Tienen algún patrón para generar las claves?			

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**La información de respaldo se realIza sacando Backups**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Saco respaldo del Sistema de Turismo (Sisturi) y de archivos importantes de los diferentes departamentos**
¿Con qué frecuencia sacan los respaldos?	**Los respaldos se sacan diariamente**
¿Qué dispositivo utilizan para los respaldos?	**CD's**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**SI**
¿Qué software antivirus utiliza?	**McAfee Antivirus**
¿Con qué frecuencia actualiza su antivirus?	**Diariamente**
¿Tienen plan de contingencias en caso de contagio de virus?	**Se realiza la eliminación inmediata de éste y la limpieza respectiva, esto es factible debido a la actualización diaria del antivirus**
¿Tienen plan de contingencias en caso de pérdida de información?	**SI, realizo copias de seguridad de los documentos**

¿Tienen plan de contingencias en caso de daños de equipos?	**SI, tenemos técnicos especialistas encargados de esto**

Seguridad del Departamento de Sistemas			
El Departamento de Sistemas cuenta con Oficina Propia?			
Si:		No, Porqué:	**No, debido a la falta de espacio en las oficinas de Quimbaya Bolivia**
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué. **No, por seguridad**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **Con Passwords, y llaves de los sitios donde se guardan copias de seguridad y dispositivos importantes para el mantenimiento de equipos**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			

Empresa:	**Interredes**	Contacto	**Juan Carlos Arteaga**
Teléfono:	**2352894**	Frecuencia:	**No es muy frecuente, cerca de una vez en tres meses**
¿Qué equipos reciben este mantenimiento?	**Impresoras, Cableado y Pc**		

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**BRASIL**
Nombre:	**WALACE PEÇANHA CAVALCANTE**
Cargo:	**ANALISTA DE SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL	**256 Kbps**	**512 Kbps**	
Otros			
Nombre del ISP:	**TELEMAR**		
Contacto:	**Soporte Técnico**	Teléfono:	**0800-565658**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**Terra**		
Cuenta de Acceso:	**Quimbaya@terra.com.br**	Contraseña:	**203040**
Contacto:	**Soporte Técnico**	Teléfono:	**0800-707777**
Usuario en que está configurada la cuenta:	**Luiz Sampaio**		
Departamento al que pertenece:	**Directoria Administrativa**		

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	**X**
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Software que utilizan:			

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**Montada**	Modelo:	
Serie:		Procesador:	**Pentium 4 / 2.2 GHZ**
Memoria:	**256 RAM**	Disco:	**80 GB**
Sistema Operativo:	**Windows XP Professional SP 1**		
¿Tienen algún patrón para generar las claves?	**SI - Ausencia de un Dominio.**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Handy Backup**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Outlook, Word, Excel, Sistema Informático, Lotus, Favoritos IE, Sistema Contabilidade.**
¿Con qué frecuencia sacan los respaldos?	**1 vez por semana**
¿Qué dispositivo utilizan para los respaldos?	**HD 80 GB**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**HD 80 GB**
¿Qué software antivirus utiliza?	**Norton Anti Vírus**
¿Con qué frecuencia actualiza su antivirus?	**2 veces en la semana**
¿Tienen plan de contingencias en caso de contagio de virus?	**SI**
¿Tienen plan de contingencias en caso de pérdida de información?	**SI**
¿Tienen plan de contingencias en caso de daños de equipos?	**SI**

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:	**X**	No, Porqué:	
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué: **NO. Debido a que políticas de seguridad y metodología de rutina de trabajo.**			
¿Con qué seguridades cuenta el Departamento de Sistemas:			

¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:		Contacto	
Teléfono:		Frecuencia:	
¿Qué equipos reciben este mantenimiento?			

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**CHILE**
Nombre:	**HELGA FRECH**
Cargo:	**DIRECTORA DE TURISMO**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL	**612 / Mono / IP Dinámica**		
Otros			
Nombre del ISP:			
Contacto:		Teléfono:	

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:			
Cuenta de Acceso:		Contraseña:	
Contacto:		Teléfono:	
Usuario en que está configurada la cuenta:			
Departamento al que pertenece:			

Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	**No contamos con servidor Internet aparte**
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Software que utilizan:			

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**IBM**	Modelo:	**LAPTOP**
Serie:		Procesador:	**PENTIUM IV – 2.4**
Memoria:		Disco:	**40 GB**
Sistema Operativo:	**XP**		
¿Tienen algún patrón para generar las claves?	**NO**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Ninguno / Backup en CD**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Carpetas word / Sisturi**
¿Con qué frecuencia sacan los respaldos?	**1 vez c/15 días**
¿Qué dispositivo utilizan para los respaldos?	**CD**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**escritorio**
¿Qué software antivirus utiliza?	**Norton**
¿Con qué frecuencia actualiza su antivirus?	
¿Tienen plan de contingencias en caso de contagio de virus?	
¿Tienen plan de contingencias en caso de pérdida de información?	
¿Tienen plan de contingencias en caso de daños de equipos?	

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:		No, Porqué:	**Inicio de actividades Octubre 2003 / El volumen no lo justifica**
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué.			
¿Con qué seguridades cuenta el Departamento de Sistemas?			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:		Contacto	
Teléfono:		Frecuencia:	
¿Qué equipos reciben este mantenimiento?	**Cuando es necesario, la empresa SM Comercial limitada quien viene a darnos soporte técnico.**		

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**COLOMBIA**
Nombre:	**OSCAR MANUEL SÁNCHEZ L.**
Cargo:	**TECNÓLOGO DE SOPORTE HARDWARE Y SOFTWARE**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL	**100 Mbps**	**100 Mbps**	
Otros			
Nombre del ISP:	**ETB**		
Contacto:	**ETB BOGOTA**	Teléfono:	**018000112170**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**No se tiene acceso a Internet secundario**		
Cuenta de Acceso:		Contraseña:	
Contacto:		Teléfono:	
Usuario en que está configurada la cuenta:			
Departamento al que pertenece:			

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	**X**
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Software que utilizan:			

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**Hp Compaq**	Modelo:	**D 220 Mt**
Serie:	**MXD4060BZM**	Procesador:	**PENTIUM 4**
Memoria:	**256 DDR**	Disco:	**40 Gb**
Sistema Operativo:	**Windows Xp Professional**		
¿Tienen algún patrón para generar las claves?	**No**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la Información?	**Se hacen Backups en CD**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Excel, Word, y correo electrónico.**
¿Con qué frecuencia sacan los respaldos?	**Mensualmente**
¿Qué dispositivo utilizan para los respaldos?	**Grabado de Cds**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**Si**
¿Qué software antivirus utiliza?	**Norton**
¿Con qué frecuencia actualiza su antivirus?	**Diariamente**
¿Tienen plan de contingencias en caso de contagio de virus?	**No**
¿Tienen plan de contingencias en caso de pérdida de información?	**No**
¿Tienen plan de contingencias en caso de daños de equipos?	**No**

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:		No, Porqué:	**Se da soporte técnico a través de una entidad externa**
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué. **No solo el Ingeniero de soporte en caso de algún fallo en los equipos o el sistema.**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **Se realizan mensualmente revisiones a los equipos (Hardware), al sistema operativo antivirus y backups de Información.**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:	**Intel&Comp**	Contacto	**OSCAR MANUEL SÁNCHEZ L**
Teléfono:	**2267761**	Frecuencia:	**Mensualmente**
¿Qué equipos reciben este mantenimiento?	**3 Pcs, 2 Impresoras**		

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**ECUADOR**
Nombre:	**LUCY AGUILAR**
Cargo:	**ASISTENTE DE SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL	**32 UP**	**128 DOWN**	
Otros			
Nombre del ISP:	**Andinanet**		
Contacto:	**Carlos Andrés Flores**	Teléfono:	**2941 949**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**Interactive**		
Cuenta de Acceso:	**Quimbaya**	Contraseña:	**lalla99**
Contacto:	**Departamento Técnico**	Teléfono:	**2986 450**
Usuario en que está configurada la cuenta:	**Lucy Aguilar**		
Departamento al que pertenece:	**Departamento de Sistemas**		

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI: X		**NO:**	
Marca:	**IBM**	Modelo:	**Pentium III**
Serie:	**78-T1255**	Procesador:	**Pentium III**
Memoria:	**256 Mb.**	Disco:	**20 Gb.**
Software que utilizan:	**Kipux Server**		

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**IBM**	Modelo:	**Netfinity 550**
Serie:	**NC23HKYV4**	Procesador:	**Pentium II.**
Memoria:	**1 Gb.**	Disco:	**28 Gb.**
Sistema Operativo:	**Windows NT Server**		
¿Tienen algún patrón para generar las claves?	**Las claves se debe cambiar cada 15 días, pero este cambio lo realizan cada usuario.**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Copia de Seguridad de Microsoft**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Sistemas de Turismo, Contables y Cartera**
¿Con qué frecuencia sacan los respaldos?	**Diariamente**
¿Qué dispositivo utilizan para los respaldos?	**Disco Duro y luego CDs**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**Si, un cajón con seguridad en el Dpto. de Sistemas**
¿Qué software antivirus utiliza?	**Mcaffee**
¿Con qué frecuencia actualiza su antivirus?	**1 vez por semana**
¿Tienen plan de contingencias en caso de contagio de virus?	**Si, el antivirus actualizado, en cuanto se presenta algún problema corremos el antivirus.**
¿Tienen plan de contingencias en caso de pérdida de información?	**Se respalda la información más importante diariamente**

¿Tienen plan de contingencias en caso de daños de equipos?	**Siempre tenemos una PC de repuesto mientras se repara la que esté con problemas**

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:	**X**	No, Porqué:	
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué: **No, porque la Asistente de Sistemas es la única autorizada para acceder a estos equipos.**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **Cuenta con oficina propia, es totalmente independiente de otros departamentos, con las debidas seguridades, esta oficina la abre y la cierra la persona encargada del Dpto. de Sistemas.**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:	**Tecmoware**	Contacto	**Ing. Galo Beltrán**
Teléfono:	**2562052**	Frecuencia:	**4 veces al año**
¿Qué equipos reciben este mantenimiento?	**El Servidor de Datos**		

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**GUATEMALA**
Nombre:	**COMSISA –JOSÉ ANGEL GALVEZ (EMPRESA PARTICULAR)**
Cargo:	**GERENTE – VENTAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Optica	**No**	**No**	
ADSL	**Aprox. 450 K**	**512 K**	
Otros			
Nombre del ISP:	**Telgua - Turbonet**		
Contacto:	**Samuel Lopez**	Teléfono:	**(502) 2899001**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**Telgua – Tele Red**		
Cuenta de Acceso:	**Telgua**	Contraseña:	**ES-06-VALR**
Contacto:	**Personal Telgua**	Teléfono:	**(502) 3230100**
Usuario en que está configurada la cuenta:	**Adriana Díaz Varón**		
Departamento al que pertenece:	**Gerente Quimbaya Guat. (Dirección de Turismo**)		

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	**No hay Servidor**
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Software que utilizan:			

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones: SE UTILIZA UN ROUTTER Y LÍNEA DEDICADA			
Marca:	**US Robotics**	Modelo:	**9003**
Serie:		Procesador:	
Memoria:	**128 KB**	Disco:	
Sistema Operativo:	**Windows XP Professional**		
¿Tienen algún patrón para generar las claves?	**No; las Claves se obtienen desde el Centro de Cómputo en Perú**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Explorer (Archivos Winzip)**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Sisturi 5.5**
¿Con qué frecuencia sacan los respaldos?	**Diaria**
¿Qué dispositivo utilizan para los respaldos?	**Quemadores de CD. (Últimos 5 días de cada mes)**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**No**
¿Qué software antivirus utiliza?	**McAfee**
¿Con qué frecuencia actualiza su antivirus?	**Actualización Automática, Semanal**
¿Tienen plan de contingencias en caso de contagio de virus?	**Sí, Soporte Técnico de Comsisa**
¿Tienen plan de contingencias en caso de pérdida de información?	**No hay**
¿Tienen plan de contingencias en caso de daños de equipos?	**Equipo Asegurado (Comsisa da a préstamo unidades mientras puedan durar estos.**

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:	**Si**	No, Porqué.	
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué. **Si (Gerencia general a cargo del administrador del sistema) Por la naturaleza del cargo.**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **No se ubicó el criterio**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas: **No**			
Empresa:		Contacto	
Teléfono:		Frecuencia:	
¿Qué equipos reciben este mantenimiento?			

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**MÉXICO**
Nombre:	**EDUARDO FIGUEROA RODRÍGUEZ**
Cargo:	**SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica			
ADSL	**512 kbps**	**318 kbps**	
Otros			
Nombre del ISP:	**Prodigy Infinitum**		
Contacto:		Teléfono:	**01800 123 22 22**

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**Avantel**		
Cuenta de Acceso:	**quimbamx**	Contraseña:	**qt0201**
Contacto:		Teléfono:	**53453900**
Usuario en que está configurada la cuenta:	**Servidor**		
Departamento al que pertenece:	**Sistemas**		

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	**no**
Marca:		Modelo:	
Serie:		Procesador:	
Memoria:		Disco:	
Software que utilizan:			

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**IMB**	Modelo:	**Xeon**
Serie:	**78-DH758**	Procesador:	**Intel 2.00 Ghz.**
Memoria:	**260 Mb.**	Disco:	**34 Gb.**
Sistema Operativo:	**Windows Server 2000**		
¿Tienen algún patrón para generar las claves?	**no**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**Easy CD Creator**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Todo el sistemas Sisturi5.5**
¿Con qué frecuencia sacan los respaldos?	**Dos veces al día**
¿Qué dispositivo utilizan para los respaldos?	**CD-RW Creative**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**En unidad D del servidor y el equipo de Sistemas**
¿Qué software antivirus utiliza?	**McAfee VirusScan**
¿Con qué frecuencia actualiza su antivirus?	**Diariamente**
¿Tienen plan de contingencias en caso de contagio de virus?	**Desconectar Switch, todos los equipos de la red, revisión general equipo por equipo, vacunar, respaldar información, formatear en caso necesario, cargar programas.**
¿Tienen plan de contingencias en caso de pérdida de información?	**Precisamente por eso se hacen dos respaldos diariamente**

¿Tienen plan de contingencias en caso de daños de equipos?	**Se tiene el equipo de sistemas, disponible en sesión de usuario en caso de daños a equipos**.

Seguridad del Departamento de Sistemas			
¿El Departamento de Sistemas cuenta con Oficina Propia?			
Si:	**Si**	No, Porqué:	
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué: **Nadie más tiene acceso al Servidor, ni equipo de sistemas, para preservar la confidencialidad de la información, e integridad de la misma y del sistema.**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **Nadie tiene acceso al servidor ni el equipo de sistemas, protección con contraseñas.**			
¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:		Contacto	
Teléfono:		Frecuencia:	
¿Qué equipos reciben este mantenimiento?			

Gracias por su colaboración.

DEPARTAMENTO REGIONAL DE SISTEMAS

FORMULARIO PARA EL DEPARTAMENTO DE SISTEMAS

RESPONDER A LAS SIGUIENTES PREGUNTAS:

Persona encargada del Departamento de Sistemas:	
País:	**PERÚ**
Nombre:	**ISIDRO ALARCÓN**
Cargo:	**ASISTENTE DE SISTEMAS**

¿Qué tipo de Acceso a Internet Primario tienen?			
Tipo	**Velocidad Up**	**Velocidad Down**	
Fibra Óptica	**128**	**64**	
ADSL			
Otros			
Nombre del ISP:	**TelMex**		
Contacto:		Teléfono:	

¿Qué tipo de Acceso a Internet Secundario (Dial Up) tienen?			
Nombre del ISP:	**Terra**		
Cuenta de Acceso:	**quimbaya@terra.com.pe**	Contraseña:	**Quimbaya**
Contacto:	**Terra Network**	Teléfono:	
Usuario en que está configurada la cuenta:	**Maritza Martínez (Está configurada en el Server Kipux, ya no por línea telefónica)**		
Departamento al que pertenece:	**Recepción**		

¿Cuenta con un servidor de Internet?, de ser afirmativa la respuesta indique sus características:			
SI:		**NO:**	
Marca:	**IBM**	Modelo:	**6563/43S**
Serie:	**78-FCHGB**	Procesador:	**Pentium III**
Memoria:	**128**	Disco:	**40 GB**
Software que utilizan:	**Kipux**		

Características del Servidor de datos, si no cuenta con un servidor dedicado, indicar las características del equipo que realiza tales funciones:			
Marca:	**IBM NetFinity 5500**	Modelo:	**8660-72U**
Serie:	**23KY027**	Procesador	**Pentium III**
Memoria:	**128**	Disco:	**8 GB**
Sistema Operativo:	**Windows NT**		
¿Tienen algún patrón para generar las claves?	**No entiendo que claves???**		

Seguridad de la Información:	
¿Qué programa utiliza para respaldar la información?	**CD Writer en discos CD-RW**
¿Cuáles son los archivos de los cuales sacan el respaldo?	**Sisturi 5.5 , Base de datos del Telecrédito, SIGO(Sistema de Contabilidad), hojas excel de Libro Bancos**
¿Con qué frecuencia sacan los respaldos?	**Mañana y Tarde**
¿Qué dispositivo utilizan para los respaldos?	**CD Writer**
¿Tienen una casilla de seguridad para almacenar los respaldos?	**No**
¿Qué software antivirus utiliza?	**McAfee**
¿Con qué frecuencia actualiza su antivirus?	**Cada semana**
¿Tienen plan de contingencias en caso de contagio de virus?	**Si, tenemos asistencia inmediata con nuestro proveedor BAFING, contrato que nos liga por dos años.**
¿Tienen plan de contingencias en caso de pérdida de información?	**Sólo los respaldos de seguridad.**

¿Tienen plan de contingencias en caso de daños de equipos?	**Tenemos dos equipos de respaldo, algunas partes y suministros.**

Seguridad del Departamento de Sistemas			
El Departamento de Sistemas cuenta con Oficina Propia?			
Si:	**Si**	No, Porqué:	
¿A excepción de la persona encargada de Sistemas hay otros usuarios que tienen acceso a los servidores y equipos del Dpto. de Sistemas? Si, No, Porqué. **Nadie, solo usuarios de sistemas**			
¿Con qué seguridades cuenta el Departamento de Sistemas? **Puerta con llave para la hora de salida y entrada**			

¿Existen otras entidades que se encargan del mantenimiento de los servidores y PCs?, en caso de ser así: responda las siguientes preguntas:			
Empresa:	**System Support**	Contacto	**Pablo Romero**
Teléfono:		Frecuencia:	**Tres veces**
¿Qué equipos reciben este mantenimiento?	**Server de Datos** **Servidor de Correo** **Equipos de Oficina cuando se requiere** **Impresoras HP Láser** **Fotocopiadora**		

Gracias por su colaboración.

BIBLIOGRAFÍA

LIBROS

TANENBAUM, Andrew S.: (2003) **Redes de Computadoras,** Edit. Prentice Hall, Cuarta Edición, Ámsterdam - Holanda.

FOROUZAN, Behrouz: (2002), **Transmisión de Datos y Redes de Comunicaciones,** Edit. McGraw Hill/ Interamericana de España S.A.U., Segunda Edición, Cofás – España.

SIGON, Karanjit: (2000), **Edición Especial Microsoft Windows 2000 TCP/IP,** Edit. Prentice Hall, Edición Especial, España.

RAYA CABRERA, José Luis, RAYA GONZÁLEZ, Laura: (2000) **Como construir una Intranet con Windows 2000 Server,** Edit. Alfomega S.A., Bogotá –Colombia.

MADROM, Thomas: (1992), **Redes de Área Local,** Edit. Grupo Noriega Editores, Primera Edición, México D.F. – México.

2000 Microsoft Corporation: (2002), **Microsoft Training and Certification,** Edit. Cargraphics S.A., Colombia.

FOLLETOS Y REVISTAS

ALVEAR Gardenia y otros: (2004), **Reparaciones de Circuitos de Datos en Provincias**, Edit. Andinatel S.A., Quito - Ecuador.

2000 Microsoft Corporation, White Paper: (2003), **Windows2000 Virtual Private Networking Scenario**, Redmond – USA.

NIÑO, Miguel Angel y otros,(2001), **Seguridad Computacional, Libro de consulta para administradores y Usuario,** Universidad de Cauca, Primera Edición, Colombia.

LUCENA, José Manuel: (2003), **Criptografía y Seguridad en Computadores**, Tercera Edición, España

DIRECCIONES DE INTERNET

Redes Privadas Virtuales

http://www.enterasys.com/la/pr/releases/2001/mar/3-2.html ENTERASYS

http://www.sica.gov.ec/agronegocios/Biblioteca/Ing%20Rizzo/agricultura/factibilidad_camaron.htm

http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdf

http://www.redaccionvirtual.com/redaccion/multimedia/descargar.asp

http://www.telefonica-data.com.pe/pdf/tarifasoficialesipvpnabv2k310.pdf

http://www.protel.net.mx/protel/datos/protelvpn.php

http://www.monografias.com/trabajos12/monvpn/monvpn.shtml

http://www.redes-linux.com/manuales.php?catId=VPN

http://www.redes-linux.com/manuales/vpn/introduccion_vpns.pdf

http://www.redes-linux.com/manuales/vpn/trabajo.pdf

http://www.oronetes.net/webs/doc/pptp/pptp.pdf

http://sites.inka.de/sites/bigred/devel/cipe.html

http://www.arsenet.com/conexadsl.html

http://www.portalmundos.com/mundoinformatica/redes/vpn.htm

http://www.microsoft.com/windows2000 and the Windows2000/NT Forum at

http://computingcentral.msn.com/topics/windowsnt.

Seguridad

http://www.uv.es/ciuv/cat/vpn/

http://cag.lcs.mit.edu/~cananian/Projects/PPTP/

http://highland.dit.upm.es:8000/UNIX/index.html

http://members.nbci.com/arturovaldes/linuxcur.htm

http://www.elhacker.net

http://www.it.kth.se/docs/rfc/rfcs/rfc1750.txt

http://wwwdi.ujaen.es/~mlucena

http://www.rsasecurity.com

http://www.certicom.com

http://www.cryptography.com/

http://csrc.nist.gov/encryption/aes/aes_home.htm

Productos y Proveedores

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00801daa53.html

http://www.cisco.com/global/ES/solutions/ent/avvid_solutions/vpn_home.shtml

http://www.cisco.com/en/US/products/hw/routers/prod_models_home.html

http://www.mtmnet.com/3com_switches.htm

http://www.mtmnet.com/vpn.htm

http://lat.3com.com/lat/technology/index.html

http://www.cisco.com/go/pix

http://nortelnetwoks.com/products/library/collateral/contivity.htm

http://www.yankeegroup.com/custom/research/report_overview.jsp?ID=9568

http://www.dooyoo.es/switches-routres/nortel-contivity-100/#sd

http://www.dooyoo.es/equipos-de-red/lucent-vpn-firewall-brick-80

http://www.dooyoo.es/equipos-de-red/lucent-vpn-firewall-brick-500

http://www.dooyoo.es/equipos-de-red/lucent-products

http://adfarm.mediaplex.com/ad/ck/2404-9561-8070-20?mpro=http://landingstrip.dell.com/landingstripemea/ls.asp

http://www.lucent.com/products/solution/0,,CTID+2017-STID+10080-SOID+1223-LOCL+1,00.html

http://www.adexus.com

http://corporativo.andinanet.net/new/pages/prod.html

http://www.suratel.com/contenido.php

Herramientas para Monitoreo de Redes

http://www.visualware.com.

http://www.visualware.com/visualroute/index.html

http://www.ks-soft.net

http://www.ks-soft.net/hostmon.esp/index.htm

http://www.ks-soft.net/ip-tools.esp/downpage.htm

http://www.notepager.net/software.htm