AUTORIA

Latacunga 2003.

Los Autores.

CERTIFICADO

En cumplimiento a lo estipulado en el artículo 9 literal f) del Reglamento del curso Preprofesional de la Universidad Técnica de Cotopaxi, en calidad de director de tesis del tema "**PROPUESTA DE UN SISTEMA DE SEGURIDAD INFORMÁTICO PARA LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**", propuesto por los Egdos. Marcelo Panchi y Samuel Sinche debo confirmar que el presente trabajo de investigación fue desarrollado de acuerdo a los planeamientos formulados por la denuncia y construcción teórica del objeto de estudio.

La claridad y veracidad de su contenido a más del desempeño y dedicación puesto por los autores de cada etapa de su realización merecen especial atención y su consideración como trabajo de calidad.

En virtud de lo antes expuesto considero que los autores de la presente tesis se encuentran en habilitados para presentarse al acto de defensa de tesis.

Ing. Fernando Defáz

DIRECTOR DE TEIS

AGRADECIMIENTO

Al culminar una etapa mas de la vida estudiantil, Primeramente agradecemos a Dios y a nuestros Padres, a nuestros Maestros nuestra eterna gratitud porque ellos fueron, quienes nos forjaron día a día, de los cuales llevamos las mejores enseñanzas y concejos.

Además un reconocimiento a la Universidad Técnica de Cotopaxi, quien brindo su colaboración en la presente tesis. Y en especial gratitud al Ing. Fernando Defáz, Director, Dr. Pedro Bedón y Ing. Adrián Mena Asesores de Tesis por su guía y compresión.

DEDICATORIA

A nuestros Padres, quienes con su nobleza y entusiasmo depositaron en nosotros su apoyo y confianza, para ser útiles a la sociedad y a la Patria.

Ellos hicieron posible la culminación de una etapa muy importante en nuestra vida estudiantil.

Índice General

CAPITULO II

CAPITULO IV

Índice de Figuras

Índice de Tablas

RESUMEN

La Universidad Técnica de Cotopaxi no ha podido quedarse al margen de la tecnología actual; por lo que cuenta con el servicio de Internet con IMPSAT como "Proveedor de Internet ", el cual suministra 256 kbps de ancho de banda las 24 horas del día y los 7 días de la semana. Para la administración del servicio de la red e Internet consta con dos servidores cada uno con el sistema operativo Linux red hat 7.3, utilizados para navegar en Internet, recibir y enviar correo electrónico respectivamente.

Es notorio que la seguridad que poseen los servidores es ínfima puesto que en la actualidad existen en Internet los piratas informáticos o Hacker los cuales son personas sin escrúpulos que destruyen los datos e ingresan virus en las computadoras y eliminan información sin dejar rastro alguno. Cualquier departamento de la Universidad puede ser infectado con virus, puesto que la mayoría de computadoras no poseen antivirus actualizado.

Se dice que el mayor porcentaje de vulnerabilidad de la información es por parte de personas propias de la red y no de personas extrañas a la red; por lo que se tiene que proteger más de los ataques directos por los usuarios que de ataques indirectos.

El presente estudio envuelve la necesidad de presentar una propuesta de seguridad informática para la Universidad Técnica de Cotopaxi, partiendo por buscar las necesidades de seguridad informática que requiere la Universidad, posteriormente determinar las políticas de seguridad para la red informática, e iniciar con el estudio de factibilidad operativa, técnica, económica de los Firewalls a nivel de Hardware y Software logrando la selección del mejor Firewall para los sistemas operativos Linux Red hat 7.3 y Windows 2000 Server y con esta información se procedió al diseño de la arquitectura de seguridad de red para la Universidad Técnica de Cotopaxi. Y por ultimo se realizó la demostración del sistema de seguridad informática a través de herramientas hackers, para lo cual es necesario instalar y configurar los sistemas operativos Linux red hat 7.3 y Windows 2000 Server con su respectivo Firewall software IpTable y Outpost.

ABSTRACT

The Technical University of Cotopaxi has not been able to stay to the margin of the current technology; because it has the Internet service with IMPSAT like Supplier of Internet", which it gives 256 kbps of band wide the 24 hours of the day and the 7 days of the week. For the administration of the service of the net and Internet, It consists with two servers each one with the operating system Linux net hat 7.3,it is used to navigate in Internet, It receives and send electronic mail respectively.

It is evident that the security that the servers possess it is owner because at the present time exist the computer pirates or Hacker. It exists in Internet which are people without scruples that destroy the data and they enter virus in the computers and they eliminate the information without leaving any rake. Any department of the University can be infected with virus, because the most of computers don't possess modernized antivirus.

It is said that the biggest percentage in vulnerability of the information is by the people owner and not of strange people to the net; for that it has to protect more than the direct attacks for the users that of indirect attacks.

The present researching work has the necessity to present a proposal of computer security for the Technical University of Cotopaxi, It is leaving to look for the necessities of computer security that it requires the University, then to determine the politicians of security for the computer net, and to begin with the study of operative feasibility, technique, economic of the Firewall to level of Hardware and Software getting the selection of the best Firewall for the operative systems Linux Net hat 7.3 and Windows 2000 Server and with this information we proceeded to design of the architecture of net security for the Technical University of Cotopaxi. For the last we make the demonstration of the system of computer security through the hackers tools, for that is necessary to install and to configure the operative systems Linux net hat 7.3 and Windows 2000 Server with theirrespectively Firewall software IpTable and Outpost.

INTRODUCCIÓN

Las redes de área local han progresado en las ultimas décadas, perfeccionándose cada vez más hasta poder almacenar enormes cantidades de información. Pero desde luego el problema de robo de datos, corrupción y escuchas se incrementó. La situación empeoro cuando las empresas instalaron redes de área local (LAN) para conectar todo y en éste proceso aumentaron las oportunidades de aparición de brechas de seguridad.

En una red desde cualquier estación de trabajo es probable eliminar archivos de sistema en el servidor, dejando sin funcionamiento a los usuarios que acceden a cada instante a los recursos compartidos, este es uno de los múltiples problemas que puede presentarse. Por este motivo la seguridad juega un papel muy importante dentro del uso de una red y mayormente cuando se trata de la red mundial de computadoras que es Internet.

Existe gente allá afuera que desean introducirse en las redes de otras personas vía Internet, las razones varían desde la inocente curiosidad hasta la maliciosa interferencia y el espionaje internacional. Al mismo tiempo el valor de Internet en las empresas y negocios es tan grande que es necesario encontrar mecanismos de seguridad mediante Firewall. Un Firewall es una seguridad que se encuentra entre la red interna y el Internet. Su propósito es filtrar el acceso a la red en base a las políticas de acceso de su compañía.

CAPITULO I

Las redes de computadoras

1.1 Introducción a Redes

La lucha por comunicación ha llevado al hombre a tratar de comunicarse a larga distancia, sea a nivel local, regional, nacional, internacional e inclusive en el espacio exterior. Se ha pasado desde los teléfonos con línea análoga, hasta la actual "red de redes" como se le conoce a Internet.

En la actualidad, a través del Internet se puede hacer desde las tareas más simples como consultar información, desarrollo compartido en grupo de ideas y proyectos, hasta llegar a los negocios virtuales o e-business.

Las redes pueden ser de diferentes: tecnologías, sistemas operativos, medios de transmisión y protocolos de comunicación.

Para ello utilizan dispositivos de interconexión de diferente complejidad de acuerdo a la solución requerida.

1.2 Tipos de redes de computadoras

Las redes se clasifican en base a una escala de distancias entre nodos y su área de cobertura son las siguientes:

- Red de área local LAN.
- Red de área de campus CAN.
- Red de área metropolitana MAN.
- Red de área extendida WAN.

- Inter-Redes (LAN-LAN, LAN-CAN-LAN, LAN-CAN-MAN-CAN-LAN, LAN-WAN-LAN, WAN-WAN, etc).

1.2.1 Tecnologías de redes LAN[1]

Las tecnologías de redes son un conjunto de normas que rigen la comunicación entre computadoras de una red.

Los estándares más populares son:

- Ethernet IEEE 802.3.
- Fast Ethernet IEEE 802.3 u.
- Gigabit Ethernet IEEE 802.3 z.
- 100VG-AnyLAN.
- Token Bus IEEE 802.4.
- Token Ring IEEE 802.5.
- FDDI.

1.2.1.1 Tecnologías Ethernet

Ethernet es hoy en día el standard para las redes de área local. Ethernet se define como un modo de acceso múltiple y de detección de colisiones (CSMA/CD, carrier sense multiple access/collision detection). Cuando una estación quiere acceder a la red, primero escucha si hay alguna transmisión en curso, y si no es así transmite. Es el caso de

[1] Redes y telecomunicación, Codesis, 1998. www.codesis.com.co

que dos redes detecten probabilidad de transmitir al mismo tiempo, se producirá una colisión; pero esto queda resuelto con los sensores de colisión que detectan esto y forzan una retransmisión de la información.

1.2.1.1.1 Ethernet IEEE 802.3

Una red Ethernet IEEE 802.3 tiene las siguientes características:

- Trabaja a una velocidad de 10 Mbps.
- ***Canal único***. Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento.
- Es de ***difusión*** debido a que todas las transmisiones llegan a todas las estaciones (aunque sólo su destinatario aceptará el mensaje, el resto lo descartarán).
- En Ethernet cualquier estación puede transmitir.
- En Ethernet ninguna estación tiene mayor autoridad que otra.

1.2.1.1.2 Fast Ethernet IEEE 802.3 u

También conocido como 100 BaseT, es la evolución de 10 BaseT pero aumentando la velocidad de transmisión de datos a 100 Mbps. Conserva el método de acceso CSMA/CD y puede utilizar cable UTP niveles 3, 4 y 5.

Los datos pueden ser transmitidos en incrementos de velocidad de 10 Mbps a 100 Mbps sin ningún protocolo de traslación o cambios en el software de aplicaciones y de interfuncionamientos, por lo que Fast Ethernet mantiene las funciones de control de error al igual que la longitud y formato de las tramas de 100 Base T.

1.2.1.1.3 Gigabit Ethernet IEEE 802.3 z

Los Beneficios que brinda Gigabit Ethernet:

- El estándar de Gigabit Ethernet transmitan los datos en 1,000 megabits por segundo (Mbps), que corre diez veces más rápido que las conexiones de Ethernet 10/100BASE-T convencionales.
- Es una inversión sencilla y rentable que puede aliviar rápidamente y fácilmente los embotellamientos de conexiones de red.

- Gigabit Ethernet sobre conectividad de cobre gasta menos para mantener que los cables ópticos de fibra. Usted puede aumentar la función de la red con Gigabit sobre su infraestructura con categoría 5.
- Un estándar para UTP en proceso

Tecnologías / Características	Ethernet	Fast Ethernet	Gigabit Ethernet
Solución Ethernet	10BASE-T	100BASE-T	1000BASE-T
Protocolo Ethernet	802.3	802.3u	802.3z
Velocidad de transferencia	10Mbps	100Mbps	1000Mbps
Distancia Máxima	100Metros	100Metros	100Metros
Media	UTP (Untwisted Pair) CAT. 3/4/5	UTP CAT. 3/4/5	UTP CAT.5/4
Topología	Estrella	Estrella	Estrella

Tabla1.1Comparación de tecnologías Ethernet.

1.2.1.2 100VG-AnyLAN

Definida por el estándar IEEE 802.12 para soportar tanto a topología Ethernet y Token Ring también es una tecnología para alta velocidad (100 Mbps). Introduce un nuevo concepto en cuanto al método de acceso llamado Método de Acceso Prioritario por Demanda (DPAM, Demand Priority Access Method).

Las ventajas que ofrece 100VG sobre el 100BaseT:

- 100VG-AnyLan puede soportar tanto aplicaciones de Ethernet como de token ring, aunque no en la

misma red. Se utiliza un ruteador para poder ir de un 100VG Ethernet a un 100VG token ring y viceversa.

- 100VG elimina las colisiones de paquetes y permite un uso más eficiente del ancho de banda de la red. Esto es realizado utilizando un esquema de acceso por prioridades de demanda en lugar de el CSMA/CD, esquema utilizado en 10Base-T Ethernet y fast Ethernet.
- La demanda permite establecer prioridades rudimentarias del tráfico sensitivo al tiempo, así como la voz y el video en tiempo real, haciendo que 100VG esté bien surtido para las aplicaciones multimedia.
- Los precios para el equipo requerido para una 100VG se pueden comparar con los de 100BaseT y son considerablemente menores a los del equipo para una red ATM.

1.2.1.3 Token Ring

En coordinación con el estándar IEEE 802.5 utiliza una topología lógica de anillo pero físicamente utiliza topología estrella. La velocidad de transmisión de datos es de 4 Mbps ó 16 Mbps y método de acceso Token Passing.

1.2.1.4 Token Bus

Es similar a token ring que utiliza el método de acceso de Token Passing, con única diferencia que trabaja con una topología en bus.

Una red TOKEN Ring tiene las siguientes características:

- Cada estación tiene que esperar su turno.
- Utiliza enlaces punto a punto entre cada estación y la siguiente.
- Tiene siempre una estación que supervisa el buen funcionamiento de la red.
- Token ring se comportará mejor en entornos de alta carga.

1.2.1.5 FDDI

La Interface de Datos por fibra Óptica (FDDI, Fiber Distribution Data Interface), es una tecnología más de MAN que de LAN, utiliza topología lógica de anillo y método de acceso Token Passing pero permite transmisión de datos a 100 Mbps y su medio de transmisión es la fibra óptica, por lo que accede a mayores distancias de operación. No está estandarizado por la IEEE sino por el Instituto Nacional de Estándares Americanos (ANSI) como X3T9.5.Se utiliza principalmente

para implantar un backbone de alta velocidad entre redes LAN en un ambiente de Campus. FDDI define el uso de 2 tipos de fibra: monomodo y multimodo. En la monomodo da una mayor distancia debido a que maneja en su transmisor de luz un rayo láser, y en la fibra multimodo el generador de luz es un diodo emisor de luz (LED), lo que proporciona una distancia mucho menor.

A continuación se presenta una tabla de comparaciones entre las tecnologías:

	IEEE 802.3	IEEE 802.3u	IEEE 802.3.z	IEEE 802.12	IEEE 802.5	IEEE 802.4	FDDI
Nombre Comercial	Ethernet	Fast Ethernet	Gigabit Ethernet	100VG-AnyLAN	Token Ring	Token Bus	FDDI
Topologia (Fisica)	Bus, Estrella árbol	Estrella	Estrella	Estrella	Anillo (MSAU - Estrella)	Bus	Estrella
Funcionamiento Lógico	bus	Estrella		Bus	Anillo	Anillo	Estrella
Velocidad de TX	10 Mbps	100 Mbps	1000 Mbps	16Mbps	4 Mbps- 16 Mbps	1,5 Mbps- 10 Mbps	100 Mbps
Señal Analógica /digital	Digital	Digital	Digital	Digital	Digital	Analógica	Analógica
Protocolo MAC	CSMA/CD	CSMA/CD	CSMA/CD	100VG-AnyLAN	Token Passing (Paso de testigo)	Token Passing (Paso de testigo)	PMD Protocolo dependiente del medio físico (Token passing modificado)
Medios de Transmisión	UTP,Coaxial, Fibra optica	UTP,Fibra optica	- Ffibra óptica multimodo - fibra óptica monomodo -Coaxial -UTP Categoría 5.	UTP,STP, Fibra Optica	UTP	Coaxial Banda Ancha de 75 Ω	Fibra óptica multimodo

Longitud del Cable	500 metros (coaxial grueso). UTP (100 m) UTP Blindado (300 m) Fibra optica 2000 m	UTP (100 m) UTP Blindado (300 m) Fibra optica 2000 m	-500 metros con fibra óptica multimodo -2000 metros con fibra óptica monomodo -25 metros con Coaxial -100 con UTP Categoría 5.	100m (UTP categoria 3) 150m (UTP categoria 5)	UTP (100 m) UTP Blindado (300 m)	500 m	100m

Tabla 1.2 Relación entre Tecnologías de red.

1.3 Dispositivos de Interconexión [2]

Para la interconexión de redes se utilizan los siguientes tipos de dispositivos:

1.3.1 Repetidores

Funcionan a nivel de capa 1, copian y reexpiden los bits individuales entre segmentos de cables. Son dispositivos de bajo nivel que solo amplifican las señales eléctricas. Se utilizan para extender una red LAN 802.3 uniendo los segmentos que la conforman hasta un máximo de 2.5 Km (4 repetidores y cinco segmentos de 500 m).

1.3.2 Puentes (Bridges)

Trabajan a nivel de capa 2, almacenan y reexpiden tramas entre redes tipo LAN (similares o diferentes). Los puentes son repetidores selectivos, puesto que discriminan el paso de las tramas de acuerdo a

sus direcciones de destino. Utilizan las direcciones MAC (físicas) para el encaminamiento, por tanto son independientes de los protocolos de capas superiores. Las LAN interconectadas se miran como una sola LAN lógica, el puente reenvia el broadcast de LAN. También, introducen algunas modificaciones a las tramas, antes de que se reexpidan, como por ejemplo, agregar o eliminar algunos campos de la cabecera de la trama. Fáciles de implementar, con poca o ninguna configuración.

Los tipos de puentes: transparente (Ethernet), de encaminamiento fuente (token ring), de encaminamiento fuente transparente (token ring + ethernet), traductor (protocolos MAC diferentes), remotos (LANs distantes), son los más utilizados.

1.3.3 Switch capa 2

Básicamente es un dispositivo capa 2, rápido, multipuerto. Algunas de sus característica importantes:

- Similar en función y capacidad a un puente (transparente).
- Rápido, debido a que sus funciones son realizadas por hardware.
- Baja latencia, con un rápido tiempo de respuesta.
- Utilizan las direcciones MAC (físicas) para el reenvío de las tramas.

[2] http://www.itlp.edu.mx/publica/tutoriales/redes/index.htm

- Fácil de implementar, bajo costo.

1.3.4 Switch capa 3

El switch de capa 3 básicamente representa lo siguiente:

- Similar en función a un router rápido, multipuerto.
- Rápido, debido a que sus funciones son realizadas por hardware.
- Baja latencia, con un rápido tiempo de respuesta.
- Para el encaminamiento de los paquetes utiliza las direcciones lógicas proporcionadas por los protocolos ruteables.
- Menor costo que el tener un arreglo de routers.
- Pueden conectarse a Hubs o a otros switches.
- Puede convertirse en un backbone (colapsado) de red.

Los switches se utilizan al interior de una red de campus, mientras que los routers se utilizan para conectar la red a enlaces WAN

1.3.5 Encaminadores (Routers)

Trabajan a nivel de capa 3, almacenan y reexpiden paquetes entre redes diferentes (heterogéneas), permitiendo conexiones de redes LAN-WAN, MAN-WAN, WAN-WAN. Conceptualmente son similares a los puentes; al funcionar en la capa de red poseen una gran flexibilidad y pueden conectar redes con formatos de direccionamiento incompatibles, lo cual las hace más lentas que los puentes. Realizan decisiones de encaminamiento basadas en costos (anchos de banda),

balanceo de la carga y en base a la información de control que se envía entre los sistemas integrantes de una red.

Los routers se configuran con las direcciones lógicas de la capa de red, las mismas que son proporcionadas por los protocolos ruteables, entre estos pueden mencionarse:

- Internet Protocol IP
- Internet Packet Exchange IPX
- Internetwork Datagram Protocol IDP

Los protocolos ruteables permiten al router entender la topología de la red. Las tablas de encaminamiento son actualizadas en cada router de la red. La configuración de la red puede ser estática o dinámica.

1.3.6 Pasarelas (Gateways)

Son dispositivos que traducen a los diferentes tipos de protocolos. Por tanto, pueden operar en cualquiera o en todas las capas del modelo OSI (preferentemente de la capa de transporte para arriba). Al proveer mayor funcionalidad que un repetidor, puente, o encaminador, generalmente procesa la información a una velocidad más lenta que los anteriores. Tienen la capacidad de comunicar redes con protocolos muy diferentes mediante la conversión de protocolos.

1.3.7 Relación entre dispositivos de interconexión

Las definiciones de repetidores, puentes, enrutadores y gateways son entrelazadas con los conceptos de capas de la arquitectura de red y el manejo de los paquetes de datos, como se indica en la tabla 1.3. Algunas veces el hardware desarrolla las funciones definidas en el modelo de referencia OSI y es controlado por los programas de firmware interno contenidos en la memoria, para desarrollar las funciones descritas en el modelo.

CAPA	FUNCIONES	DISPOSITIVO DE ENLACE
7 Aplicación	Funciones especializadas tales como transferencia de archivos, terminal virtual, correo electrónico	Gateway
6 Presentación	Programas de formateo de datos y conversión de caracteres	Gateway
5 Sesión	Programas de negociación y establecimiento de conexión con el otro nodo	Gateway
4 Transporte	Programas para asegurar la transmisión de los datos de extremo a extremo	Gateway
3 Red	Programas para encaminar paquetes a través de múltiples redes	Encaminador
2 Enlace	El firmware hace la transferencia de unidades de información, tramas y chequeo de errores	Puente
1 Física	El firmware hace la transmisión de datos sobre el canal de comunicaciones	Repetidor

Tabla 1.3 Dispositivos de Interconexión en las capas del modelo OSI.

La tabla 1.4 muestra las ventajas y desventajas relevantes de los dispositivos de interconexión mencionados.

DISPOSITIVO	VENTAJAS	DESVENTAJAS
REPETIDORES	• Pueden interconectar diferentes tipos de medios físicos, tales como par trenzado y coaxial • Proveen una forma barata de extender el cable de la red hasta el máximo permitido por el control de acceso al medio • No requieren mucha configuración para su uso	• Al permitir una carga de tráfico pesada, pueden degradar la operación de los segmentos de LAN • Un problema en un segmento de la LAN puede interrumpir la comunicación entre el resto de segmentos
PUENTES	• División de la LAN para simplificar la administración de la red • Pueden aislar segmentos de LAN de modo que el tráfico no pase innecesariamente entre ellos, lo que deriva en un incremento del ancho de banda disponible en cada segmento • Aislamiento de problemas y localización de fallas • Interconectan diferentes tipos de redes LAN	• El hardware es relativamente caro • El enlace de comunicación con un puente remoto es por lo general más lento que con un puente local en un cable de red LAN
ENRUTADORES	• Actúan como una pared entre segmentos de LAN, previniendo que problemas en un segmento no dañen a otros • No requieren cuidado en cuanto a los protocolos de capa MAC usados en cada segmento LAN • Pueden mover datos entre redes con diferentes tipos de control de acceso al medio y señalización • Usan eficientemente el medio Inter-LAN	• Pueden manejar varios métodos de acceso, pero necesitan un protocolo de comunicación común, tales como TCP/IP, SPX/IPX, DECNet, y otros • Son más caros que los puentes • Tienen un relativo nivel de esfuerzo para la instalación, configuración y operación • Consumen tiempo trabajando en cada paquete o trama, lo que los hace lentos, con una baja velocidad del circuito Inter-LAN
GATEWAYS	• No ponen una carga alta en los circuitos de comunicación Inter-LAN • Desarrollan trabajos específicos eficientemente, como el intercambio de correo o archivos, por lo que no es necesario un adiestramiento o software especial	• Realizan tareas específicas y no son eficientes para cualquier tipo de aplicaciones • Son dependientes del protocolo

Tabla 1.4 Ventajas y Desventajas de los Dispositivos de Interconexión

En el siguiente cuadro se presenta las características mas importantes de hub, Switch, Hub Switch.

	IEEE 802.3 HUB	IEEE 802.3 Switch	IEEE 802.3 u HUB Switch
Nombre Comercial	Ethernet 10Base-T	Ethernet 10Base-T conmutado Ethernet 100Base-T conmutado	Ethernet rápido ó Fast Ethernet • 100Base-T4 • 100Base-Tx • 100 Base-F
Topología (Fisica)	Estrella	Estrella	
Velocidad de TX	10 Mbps	10 Mbps 100 Mbps	100 Mbps
Señal Analógica /digital	Digital	Digital	Digital
Protocolo MAC	CSMA/CD	CSMA/CD	CSMA/CD
Colisión de Datos S/N	SI	SI	SI
Determinístico S/N (No tiempo real)	NO	NO	NO
Prioridades S/N (QoS)	NO	NO	NO
Medios de Transmisión	UTP Cat 3/5	**UTP Categoría 5**	**- 4 pares UTP Niveles 3,4 ó 5** -2 pares STP, UTP nivel 5 - 2 Fibras ópticas
Longitud del Cable	100, máx 500 m	100 m	-100, máx 200 m -100, máx 200 m -400 m

Tabla 1.5 características mas importantes de hub, Switch, Hub Switch

1.4 Grupo de protocolos TCP/IP[3]

TCP/IP, cuyo significado es ***Transmission Control Protocol and the Internet Protocol,*** es un conjunto de protocolos (software) que definen un tipo de red, su manejo y su administración; este conjunto de protocolos está dominando actualmente el mundo de la comunicación de datos tanto de los sistemas UNIX así como de otros sistemas con plataformas de software diferentes.

En las redes TCP/IP existen también las denominadas Intranet y Extranet:

- Intranet es una red TCP/IP interna de una organización.
- Extranet es una red formada usando Internet para conectar las Intranets.

1.4.1 Arquitectura del protocolo TCP/IP

La arquitectura del protocolo TCP/IP es en base al modelo OSI[4]; presenta en la siguiente tabla.

TCP/IP	OSI
Aplicación	7. Nivel de aplicación
	6. Nivel de presentación
	5. Nivel de sesión
Transporte	4. Nivel de transporte
Internet	3. Nivel de red
Interfaz de red	2. Nivel de datos
	1 Nivel físico

Tabla1.6 *Comparación de los niveles TCP/IP con los OSI.*

[3] REDES DE COMPUTADORES TCP/IP INTERNET , Ing. Gustavo Samaniego B.(2002), Pg 1-20

1.4.2 Caracteristicas de TCP/IP

- Es un protocolo estándar, abierto, amigable, útil para el desarrollo de aplicaciones distribuidas o que utilizan un entorno de red, en forma independiente del computador o su sistema operativo.
- Es independiente del hardware de la red, lo que permite integrar varios tipos de redes. TCP/IP puede correr sobre una red Ethernet, token ring, X.25, FDDI, en redes sobre líneas telefónicas, y sobre redes que utilicen cualquier medio de transmisión de datos.
- Posee un esquema de direcciones que permite asignar una dirección única a cada dispositivo de la red.
- Posee un conjunto de protocolos estandarizados, que permiten la amplia disponibilidad de servicios en red para el usuario.

1.4.3 Las direcciones IP

Una dirección IP contiene una "parte de red" y una "parte de host", pero el formato de estas partes es diferente para cada tipo de dirección IP. El número de bits de dirección usado para identificar la red, y el número de bits usado para identificar al host, varía de acuerdo a la **clase de dirección**.

Las tres principales **clases** de red son **clase A, clase B,** y **clase C**, cuyas estructuras se observan en el siguiente cuadro:

[4] Redes de área local, Jorge E. Rodriguez G.(1996), Pg 91-92

Equivalencias: R = red

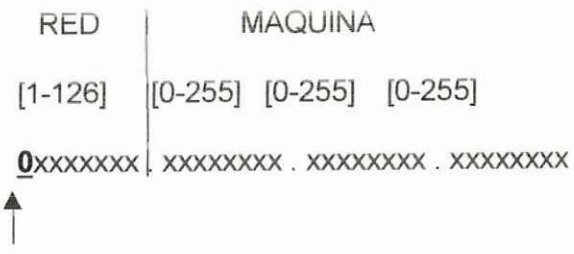
N = nodos

Clase de red	bits del 1er Byte	Rango del 1er. Byte	Formato de la dirección	Número de redes	Número de hosts por red
A	0XXXXXXX	1 – 126 * (0 y 127 son de uso especial)	R.N.N.N	$2^7 - 2$	$2^{24} - 2$
B	10XXXXXX	128 – 191	R.R.N.N	2^{14}	$2^{16} - 2$
C	110XXXXX	192 – 223	R.R.R.N	2^{21}	$2^8 - 2$
D	1110XXXX	224 - 239			
E	11110XXX	240 - 247			

Tabla 1.7 Clases de redes

Examinando los primeros bits de una dirección IP, el software IP puede rápidamente determinar la clase de dirección y su estructura. Las siguientes reglas IP determinan la clase de dirección, tomando en cuenta los bits dentro de los bytes de la dirección:

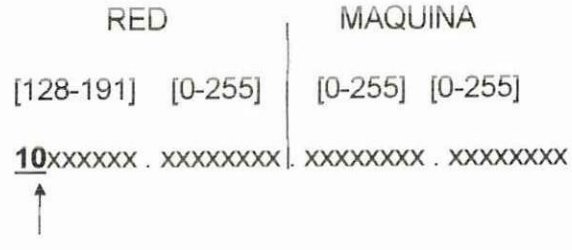
- Si el primer bit de una dirección IP es **0**, esta dirección pertenece a una red de **clase A**. El primer bit de una dirección de clase A identifica la clase de dirección. Los siguientes 7 bits identifican la red, y los últimos 24 bits identifican al host. Existe aproximadamente 126 números de red de clase A, pero cada red de clase A puede estar compuesta de millones de hosts (en el rango de 2^{24}).



Clase A

Los valores **0** y **127** del primer byte se reservan para usos especiales.

- Si los dos primeros bits de una dirección son **1 0**, esta es una dirección de una red de **clase B**. Los primeros dos bits identifican la clase; los siguientes 14 bits identifican la red, y los últimos 16 bits identifican el host. Existen miles de números de redes de clase B (2^{14}) y cada red de clase B puede contener miles de hosts ($2^{16} - 2$).



Clase B

- Si los tres primeros bits de una dirección IP son **1 1 0**, esta es una dirección de red de **clase C**. En una dirección de red de clase C, los tres primeros bits identifican la clase de dirección; los siguientes 21

bits son la dirección de la red, y los últimos 8 bits identifican el host. Hay millones de números de redes de clase C (2^{21}), pero cada red de clase C está compuesta por cerca de 254 hosts.

RED			MAQUINA
[192-223]	[0-255]	[0-255]	[0-255]
110xxxxx .	xxxxxxxx .	xxxxxxxx	. xxxxxxxx

Clase C

- Si los cuatro primeros bits de una dirección son **1 1 1 0**, esta pertenece a una dirección reservada especial. El primer byte toma valores mayores a 223. Estas direcciones son llamadas direcciones de **clase D**, pero realmente no se refieren a redes específicas. Los números asignados dentro de este rango son direcciones de **multicast**. Las direcciones de Multicast son usadas para direccionar grupos de computadores, todos al mismo tiempo. Las direcciones multicast identifican a un grupo de computadores que utilizan un protocolo común.

Las direcciones IP son usualmente escritas como cuatro números decimales separados por puntos, en donde cada uno de los de ellos está dentro del rango de 0-255. Puesto que los bits que identifican la clase son contiguos a los bits de dirección de la red

se analizarán los valores de bytes completos dentro de las direcciones de red y de máquina.

Considérese la dirección 27.104.0.19. El primer bit de esta dirección es 0, por lo tanto se está hablando de una red de clase A, en la que la máquina host 104.0.19 está en la red 27. Un byte especifica la red y tres bytes identifican el host.

00011011 . 01101000 . 0000000 . 00010011 **clase A**

27 104 0 19

8 bits de red 24 bits de máquina

En la dirección 130.66.12.12, los dos primeros bits de alto orden son 1 0 por lo tanto se está hablando de una dirección de clase B, en la que el host 12.12 está en la red 130.66. Dos bytes identifican la red y dos el host.

10000010 . 01000010 . 00001100 . 00001100 **clase B**

130 66 12 12

16 bits de red 16 bits de máquina

Finalmente en el ejemplo de la dirección de red de clase C, 192.188.48.7 los tres primeros bits son 1 1 0, por lo tanto se habla de una máquina 7 en una red 192.188.48; tres bytes identifican a la red y un byte al host.

11000000 . 10111100 . 00110000 . 00000111 **clase C**

192 188 48 7

24 bits de red 8 bits de máquina

No todos los números de red ni todos los números de host están disponibles para su uso. Se debe considerar que si el primer byte es superior a 223 esta es una dirección reservada. Los valores 0 y 127 del primer byte son reservados para usos especiales. La dirección 0.0.0.0 designa la "ruta por defecto" y la dirección 127.0.0.0 es la "dirección loopback". La ruta por defecto es usada para simplificar la información de encaminamiento que es manejada por el protocolo IP. La dirección loopback se utiliza para pruebas del TCP/IP y para la comunicación de procesos internos en la máquina; simplifica las aplicaciones de redes permitiendo al host local ser direccionado de la misma manera que a un host remoto, es decir, realizar en un host local las mismas operaciones y poner en función los mismos servicios que se los pondría en un host remoto.

Existen también algunas direcciones de host que tienen usos especiales. En todas las clases de redes, las direcciones de host 0 y 255

son reservadas. Una dirección IP con todos los bits de la parte de host puestos a cero (0) representan a la red en si misma. Por ejemplo 26.0.0.0 se refiere a la red 26, y 128.66.0.0 se refiere a la red 128.66. Direcciones de esta forma son usadas en tablas de encaminamiento para referirse a redes completas.

1.4.4 Dirección de broadcast:

Una dirección IP con todos los bits de la parte de máquina puestos a uno (1) es una "dirección de broadcast". Una dirección de broadcast es usada para direccionar simultáneamente a todas las máquinas dentro de una red. La dirección de broadcast para la red 128.66 es 128.66.255.255. Un datagrama enviado a esta dirección es entregado a todas y cada una de las máquinas individuales dentro de la red 128.66.

IP utiliza la parte de red de la dirección para encaminar el datagrama entre redes. La dirección completa, incluyendo la información del host, es usada para hacer la entrega final cuando el datagrama alcanza la red de destino.

1.4.5 Máscara

Existe el término "máscara", muy utilizado en redes TCP/IP; para obtener la máscara se debe poner unos (1s) en todos los bits de la parte de red, y ceros (0s) en todos los bits de la parte de máquina. La

máscara permite determinar el número de subredes que contiene una red.

La máscara para una red de clase A es 255.0.0.0 , para una red de clase B es 255.255.0.0 y para una red de clase C es 255.255.255.0; éstas máscaras se refieren a redes que no contienen subredes.

1.4.6 Subredes (Subneting)

La estructura estándar de una dirección IP puede modificarse localmente para usar bits de la dirección del host como bits de direcciones de redes adicionales. Esencialmente, la "línea de división" entre los bits de dirección de red y los bits de dirección del host es movida con la creación de subredes, esto se logra reduciendo el número de hosts que pueden pertenecer a una red. Esta definición de redes dentro de una red más grande es conocida como **subred**.

Para conocer como definir una dirección de subred, debe tomarse en cuenta el número de subredes que se desea obtener y de acuerdo a esto, tomar un número exponencial de base **2** elevado a la **n,** tal que el resultado del cálculo anterior cubra el número de subredes requeridas. Este número **n** servirá posteriormente para realizar un desplazamiento de la línea de división entre los bits de la parte de red y los bits de la parte de host.

ejemplo: Dividir una red en 3 subredes

Para dividir una red en tres subredes, es necesario que el número 2 se eleve a la 2 (**n** igual a 2) cuyo resultado es 4 con lo cual se estaría cubriendo el 3 que es el número de subredes deseado.

Una subred está definida por la aplicación de un bit de **máscara**, la "máscara de subred", a la dirección IP. Si un bit está dentro de la máscara, el bit equivalente en la dirección es interpretado como un bit de red. Si un bit está fuera de la máscara, el bit se considerará como parte de la dirección del host. La subred es conocida solamente de forma local. Para el resto de Internet, la dirección es interpretada como una dirección IP.

Una manera más clara de ver lo anterior sería colocar una línea de división entre la parte de red y la de máquina, a continuación mover esta línea hacia la derecha (parte de máquina) tantos bits como se haya calculado el número **n**.

Por ejemplo, si se toma la red de clase C 192.188.48.0 y se la divide en 4 subredes, el número **n** sería 2, porque 2 elevado a la 2 es 4. Por lo tanto es necesario apoderarse de los 2 bits más significativos del primer byte de la parte de máquina para realizar la definición de las subredes.

Para cada subred, a más de calcular su número IP es necesario calcular su dirección de Broadcast.

La máscara es única para todas las subredes, y permite determinar cuantas subredes existen en una red.

Sin subredes:

192 . 188 . 48 . 0

11000000 . 10111100 . 00110000 . 00000000 clase C

RED MAQUINA

Con 4 subredes:

11000000 . 10111100 . 00110000 . 00 000000 clase C

RED MAQUINA

Este momento, la parte de red a pasado de 24 bits a 26 bits, con lo cual, y siguiendo la definición de dirección de red, se coloca 0s en la parte de máquina y los 2 bits adicionales en la parte de red, nos sirven para realizar las combinaciones necesarias y obtener las 4 subredes requeridas.

Coherentemente con las definiciones de broadcast y de máscara, se puede proceder a calcular estos valores para las 4 subredes:

1) 192.188.48.0 primera subred

11000000 . 10111100 . 00110000 . **00** 000000

192.188.48.63 broadcast 1era subred

11000000 . 10111100 . 00110000 . 00 111111

255.255.255.192 máscara 1era subred

11111111 . 11111111 . 11111111 . 11 000000

2) 192.188.48.64 segunda subred

11000000 . 10111100 . 00110000 . **01** 000000

192.188.48.127 broadcast 2da subred

11000000 . 10111100 . 00110000 . 01 111111

255.255.255.192 máscara 2da subred

11111111 . 11111111 . 11111111 . 11 000000

3) 192.188.48.128 tercera subred

11000000 . 10111100 . 00110000 . **10** 000000

192.188.48.191 broadcast 3era subred

11000000 . 10111100 . 00110000 . 10 111111

255.255.255.192 máscara 3era subred

11111111 . 11111111 . 11111111 . 11 000000

4) 192.188.48.192 cuarta subred

11000000 . 10111100 . 00110000 . **11** 000000

192.188.48.255 broadcast 4ta subred

11000000 . 10111100 . 00110000 . 11 111111

255.255.255.192 máscara 4ta subred
11111111 . 11111111 . 11111111 . 11 000000

Las máscaras de subred son orientadas al bit y pueden ser aplicadas a cualquier clase de dirección. Si se administra una red, debe evaluarse correctamente si se necesita o no utilizar subredes para solucionar algún problema organizacional o topológico.

1.4.7 Familia de Protocolos TCP/IP

Hay una serie de protocolos implementados dentro de TCP/IP, los más importantes se detallan a continuación:

- Protocolo sencillo de transferencia de correo (SMTP puerto 23): es un protocolo de servicio de correo electrónico , listas de correo , etc...y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP .
- Protocolo de transferencia de ficheros (FTP puerto 21) : FTP es otra forma de moverse por Internet. Hacer FTP consiste en la conexión a un servidor FTP para obtener un fichero, también es posible a veces dejar ficheros.
- TELNET (puerto 23): es un protocolo para que dos computadores lejanos se puedan conectar y trabajar uno en el otro como si estuviera conectado directamente . Uno de ellos es

el usuario y el otro el servidor. TCP se encarga del intercambio de información .

1.5 Seguridad en una Red[5]

1.5.1 Definición de seguridad

Pueden existir varios modos para definir la seguridad. En términos simples la seguridad en computadoras personales trata de permitir que sigan haciendo su trabajo sin interrupciones debidas al extravío de la información; es decir tener la libertad de disfrutar las ventajas de las computadoras personales sin consecuencias negativas.

1.5.2 Seguridades en Internet

1.5.2.1 Firewall en Internet

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Para que un Firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

El firewall debe estar entre la red Internet y la red interna de la institución, como se ilustra en el siguiente gráfico:

[5] Manual de Seguridad para PC y redes locales, *STEPHEN cobb (1998)*, Pg 3,510-55

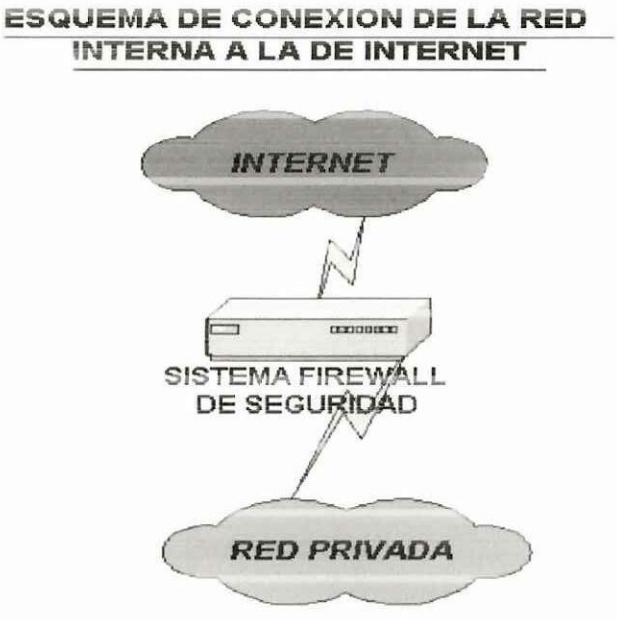


Figura 1.1 Esquema de conexión de la red interna a la Internet

1.5.2.2 Funciones de un Firewall

Las funciones más importantes a continuación:

- Concentra la seguridad.
- Centraliza los accesos.
- Genera alarmas de seguridad.
- Traduce direcciones (NAT).
- Monitorea y registra el uso de Servicios de WWW y FTP.

1.5.2.3 Topologías de Firewall

Aunque el propósito de todos los firewalls es el mismo, existen diferencias en sus topologías y prestaciones. Se pueden distinguir los siguientes tipos:

- Screening Router

- Bastion Host
- Dual Homed Gateway
- Screened Host Gateway
- Screened Subnet
- Gateway Híbrido

1.5.2.3.1 Screening Router

Es un componente básico de la mayoría de los Firewalls. Puede ser un router comercial o uno basado en una estación con capacidad para filtrar paquetes. Muchos tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP/IP. Algunos firewalls sólo consisten en un screening router entre la red privada e Internet.

En general, permite la comunicación entre los múltiples nodos de la red protegida con Internet. La zona de riesgo es proporcional al número de nodos de la red protegida y el número y tipo de servicios para los que se permite el tráfico. Es difícil controlar los daños que pueden producirse dado que el administrador de la red debe examinar regularmente cada host para buscar trazas de ataques.

1.5.2.3.2 Bastión Host

Son sistemas identificados por el administrador de la red como puntos claves en la seguridad de la red. En general, tienen un cierto grado de atención extra por parte del administrador en cuanto a su seguridad. Son auditados regularmente y pueden tener software modificatorio para determinar/modificar las comunicaciones y reparar fallos de seguridad del sistema.

1.5.2.3.3 Dual Homed Gateway

Algunos firewalls son implementados sin necesidad de un screening router. Para ello se conecta un bastion host entre la red que se quiere proteger y la Internet, desactivando las funciones de reenvio TCP/IP. Los hosts de la red privada pueden comunicarse con el gateway, al igual que los nodos de Internet, pero el tráfico directo entre ambas redes está bloqueado.

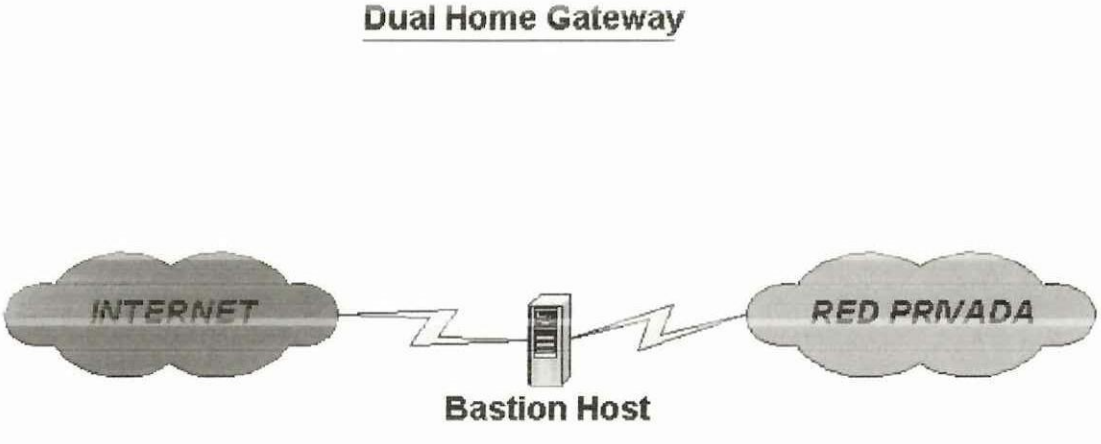


Figura 1.2 Dual Home gateway

Esta estructura de firewalls es empleada habitualmente debido a que es fácil de implementar. Al no reenviar el tráfico TCP/IP, bloquea completamente la comunicación entre ambas redes. Su facilidad de uso depende de la forma en la que el administrador proporciona el acceso a los usuarios:

- Proporcionando pasarelas para las aplicaciones.
- Proporcionando cuentas a los usuarios en el bastion host.

El principal inconveniente es que un hacker minimamente preparado puede borrar sus huellas fácilmente, lo que hace muy difícil descubrir el ataque. Si el único usuario es el administrador, la detección del intruso es mucho más fácil, porque el simple hecho de que alguien haya entrado en el sistema es un indicativo de que sucede algo raro.

1.5.2.3.4 Screened Host Gateway

Es la configuración de firewalls más común. Está implementada usando un bastion host y un screening router. Habitualmente el bastion host está en la red privada y el screening router está configurado de modo que el bastion host es el único nodo de dicha red que es accesible desde Internet para un pequeño número de servicios.

Screened Host Gateway

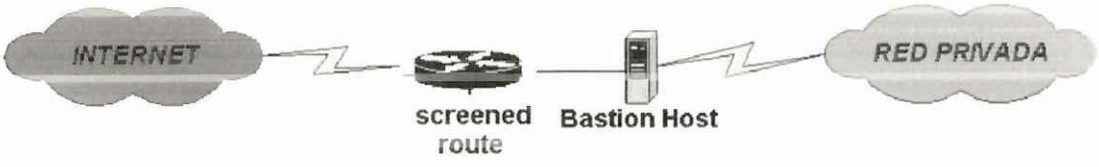


Figura 1.3 Screened Host Gateway.

Como el bastion host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas.

La zona de riesgo se circunscribe al bastion host y el screening router. La seguridad de éste último depende del software que ejecute. Para el bastion host, las consideraciones sobre seguridad y protección son similares a las hechas para un sistema del tipo *dual homed gateway*.

1.5.2.3.5 Screened Subnets

En algunas configuraciones de firewalls se crea una subred aislada, situada entre la red privada e Internet. La forma habitual de usar esta red consisten en emplear screening routers configurados de forma que los nodos de dicha subred son

alcanzables desde Internet y desde la red privada. Sin embargo, el tráfico desde Internet hacia la red privada es bloqueado.

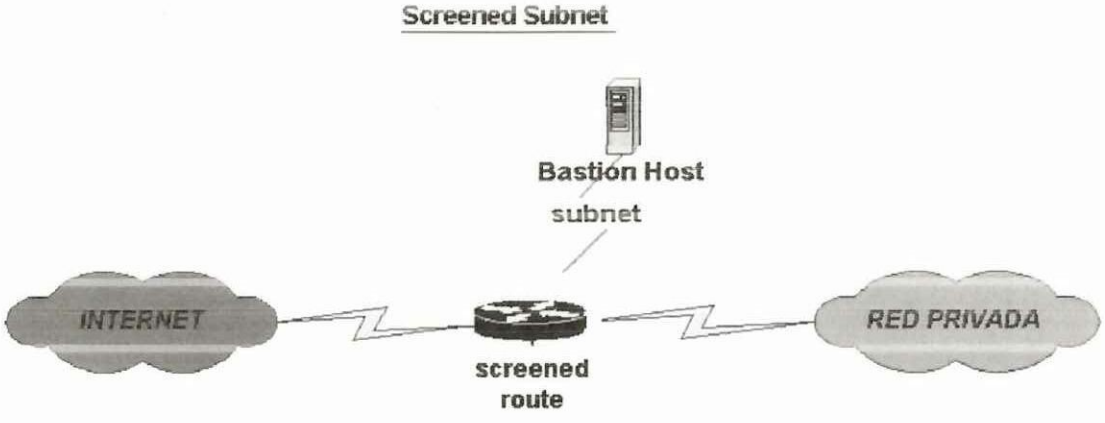


Figura 1.4 Screened Subnet

En la subred suele haber un bastion host como único punto de acceso a la misma. La zona de riesgo es pequeña y está formada por el propio bastion host. Los screening routers filtran el tráfico y proporcionan las conexiones entre Internet, la sudred y la red privada. La facilidad de uso y las prestaciones de la subred varían, pero en general sus servicios se basan en un bastion host que ofrece los servicios a través de *gateways para las aplicaciones*, haciendo hincapié en que lo que no está explícitamente permitido está prohibido.

1.5.2.3.6 Gateway Híbrido

Es cualquier estructura diferente de las anteriores. Este tipo de configuraciones pueden beneficiarse del uso de múltiples protocolos, el encapsulamiento de unos protocolos sobre otros. Sin embargo, el ocultar la estructura del Firewall no es un medio de aumentar la seguridad en si mismo, sino una forma de dificultar el ataque. Conviene tener en cuenta que un hacker no se va a desanimar por la existencia de este tipo de dificultades.

1.5.3 Piratería de Software y sus problemas

Si se hace una copia ilegal de un Software, existe la posibilidad de ser perseguidos por ello. Ni que decir de las empresas que permiten o alimentan la copia ilegal de Software, están tirando piedras contra su propio tejado.

1.5.3.1 Qué es piratería

Es una copia de Software realizada violando los términos bajos los que reciben la licencia para usarla. Dentro de los amplios márgenes definidos por la ley y la jurisprudencia estos términos son dictados por el propietario de Software y pueden variar considerablemente.

1.5.3.2 Acuerdos de licencia

Los acuerdos de licencia son realmente una declaración formalizada de derechos similar a la correspondiente cuando se adquiere un libro. Los editores de Software sostienen la necesidad de formalizar la relación en términos de unos acuerdos de licencia por varias razones, siendo quizá la mas obvia es la facilidad con que se puede realizar una copia.

1.5.3.3 Hackers, Crackers y Piratas

Junto a los avances de la informática y las comunicaciones en los últimos años, ha surgido una hueste de apasionados de estas tecnologías, que armados con sus ordenadores y conexiones a redes como Internet, ha logrado humillar a instituciones tan potencialmente seguras como el Pentágono y la NASA.

Se puede encontrar con diferentes términos para definir a estos personajes: *hackers*, *crackers*, piratas, etc., estando normalmente condicionado el calificativo a los objetivos y a los efectos de sus ataques a los sistemas. El término ***hacker***, por ejemplo, se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños. Los ***crackers***, en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los ***piratas***, su

actividad se centra en la obtención de información confidencial y *software* de manera ilícita.

1.5.4 Seguridad de Redes y Comunicación

La compartición de recursos en una red es muy ventajosa. Sin embargo, estas ventajas conllevan un incremento de los riesgos, según el principio natural de que cuando más se puede ganar más se puede perder. La conexión de dos computadoras abre un nuevo frente para el ataque, que puede usarla para obtener los datos que se transfieren o para penetrar en uno o más de los sistemas interconectados.

1.5.4.1 Controles de Acceso

Son restricciones que previenen que usuarios no autorizados e intrusos tengan libre acceso a sistemas de información. Algunos son controles de inicio de sesión para prevenir qué usuarios puedan acceder en determinados momentos o en computadoras específicas. También hay permisos de nivel que determinan exactamente qué directorios y archivos puede ver un usuario. Los controles de acceso deberían establecerse mediante comités que incluyan a los administradores de los grupos de trabajo, los jefes de departamento, los jefes de división, los administradores del sistema y los oficiales de seguridad. Una vez que se establece el plan de control, se deben

garantizar el acceso a las cuentas de usuarios individuales o de grupos.

1.5.4.2 Cuentas de Usuarios

Los administradores crean una cuenta de usuario para cada persona que necesite acceder a la red. Las cuentas de usuarios tienen un nombre y una contraseña que los usuarios escriben para acceder al sistema o a la red en general. Una cuenta especial de invitado está disponible para empleados temporales o visitantes que no necesiten una cuenta especial, pero necesitan un acceso limitado al sistema.

1.5.4.3 Inicios de sesión y contraseñas

El suceso de inicio de sesión tiene el potencial más grande de comprometer la seguridad en sus sistemas. Los usuarios deberían asegurarse de que nadie vea cómo escribe sus contraseñas. Obviamente, cualquiera que consiga la contraseña de una cuenta puede acceder a los sistemas de computadoras con todos los derechos y privilegios de esa cuenta.

1.5.4.4 Gestión de claves o contraseñas

Abarca la generación, distribución, almacenamiento, tiempo de vida, destrucción y aplicación de las claves de acuerdo con una política de seguridad.

1.5.4.4 Generación de claves

La seguridad de un algoritmo descansa en la clave. Un criptosistema que haga uso de claves criptográficamente débiles será él mismo débil. Algunos aspectos a considerar que se presentan a la hora de la elección de las claves son:

Espacio de claves reducido .- Cuando existen restricciones en el número de bits de la clave, o bien en la clase de bytes permitidos (caracteres ASCII, caracteres alfanuméricos, imprimibles, etc.), los ataques de fuerza bruta con hardware especializado o proceso en paralelo pueden desbaratar en un tiempo razonable estos sistemas.

Elección pobre de la clave.- Cuando los usuarios eligen sus claves, la elección suele ser muy pobre en general (por ejemplo, el propio nombre o el de la mujer), haciéndolas muy débiles para un ataque de fuerza bruta que primero pruebe las claves más obvias (ataque de diccionario).

Claves aleatorias.- Claves buenas son las cadenas de bits aleatorios generadas por medio de algún proceso automático (como una fuente aleatoria fiable o un generador pseudo-aleatorio criptográficamente seguro), de forma que si la clave

consta de 64 bits, las 264 claves posibles sean igualmente probables. En el caso de los criptosistemas de clave pública, el proceso se complica, porque a menudo las claves deben verificar ciertas propiedades matemáticas (ser primos dos veces seguros, residuos cuadráticos, etc.).

Distribución de claves.- Las claves criptográficas temporales usadas durante la comunicación, llamadas claves de sesión, deben ser generadas de forma aleatoria. Para protegerlas será necesaria seguridad física o cifrado mediante claves maestras, mientras que para evitar que sean modificadas deberá utilizarse seguridad física o autenticación. La autenticación hace uso de parámetros como time-stamps y contadores para protegerse también contra la reactuación con antiguas claves.

Almacenamiento de claves .- En sistemas con un solo usuario, la solución más sencilla pasa por ser su retención en la memoria del usuario. Una solución más sofisticada y que desde luego funcionará mejor para claves largas, consiste en almacenarlas en una tarjeta de banda magnética, en una llave de plástico con un chip ROM (ROM key) o en una tarjeta inteligente, de manera que el usuario no tenga más que insertar el dispositivo empleado en alguna ranura a tal efecto para introducir su clave.

Otra manera de almacenar claves difíciles de recordar es en forma encriptada mediante una clave fácil de recordar, como por ejemplo almacenar en disco la clave privada RSA cifrada mediante una clave DES.

Tiempo de vida de claves.- Una clave nunca debería usarse por tiempo indefinido. Debe tener una fecha de caducidad, por las siguientes razones:

- Cuanto más tiempo se usa una clave, aumenta la probabilidad de que se comprometa (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).
- Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, por lo que toda la información protegida con esa clave queda al descubierto.
- Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar desbaratarla.
- En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

Destrucción de claves.- Las claves caducadas deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de un adversario, puesto que con ellas podría leer los

mensajes antiguos. En el caso de haber sido escritas en papel, éste deberá ser debidamente destruido; si habían sido grabadas en una EEPROM, deberá sobrescribirse múltiples veces, y si se encontraba en EPROM, PROM o tarjeta de banda magnética, deberán ser hechas añicos. En función del dispositivo empleado, deberá buscarse la forma de que se vuelvan irrecuperables.

1.5.5 Medidas protectoras [6]

Los Mecanismos de seguridad más importantes son los siguientes:

- **Intercambio de autenticación**: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, porque existen ataques para desbaratarlos.
- **Cifrado**: garantiza que la información no sea legible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.
- **Integridad de datos**: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada

generalmente valor de comprobación de integridad (Integrity Check Value o ICV).

- **Firma digital**: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad.
- **Control de acceso**: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

- **Tráfico de relleno**: consiste en enviar tráfico junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- **Control de encaminamiento**: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

[6] Manual de Seguridad para Windows NT, *sheldon, Tom* (1999), Pg 37-38. 45-46

CAPITULO II

Análisis del dominio a estudio

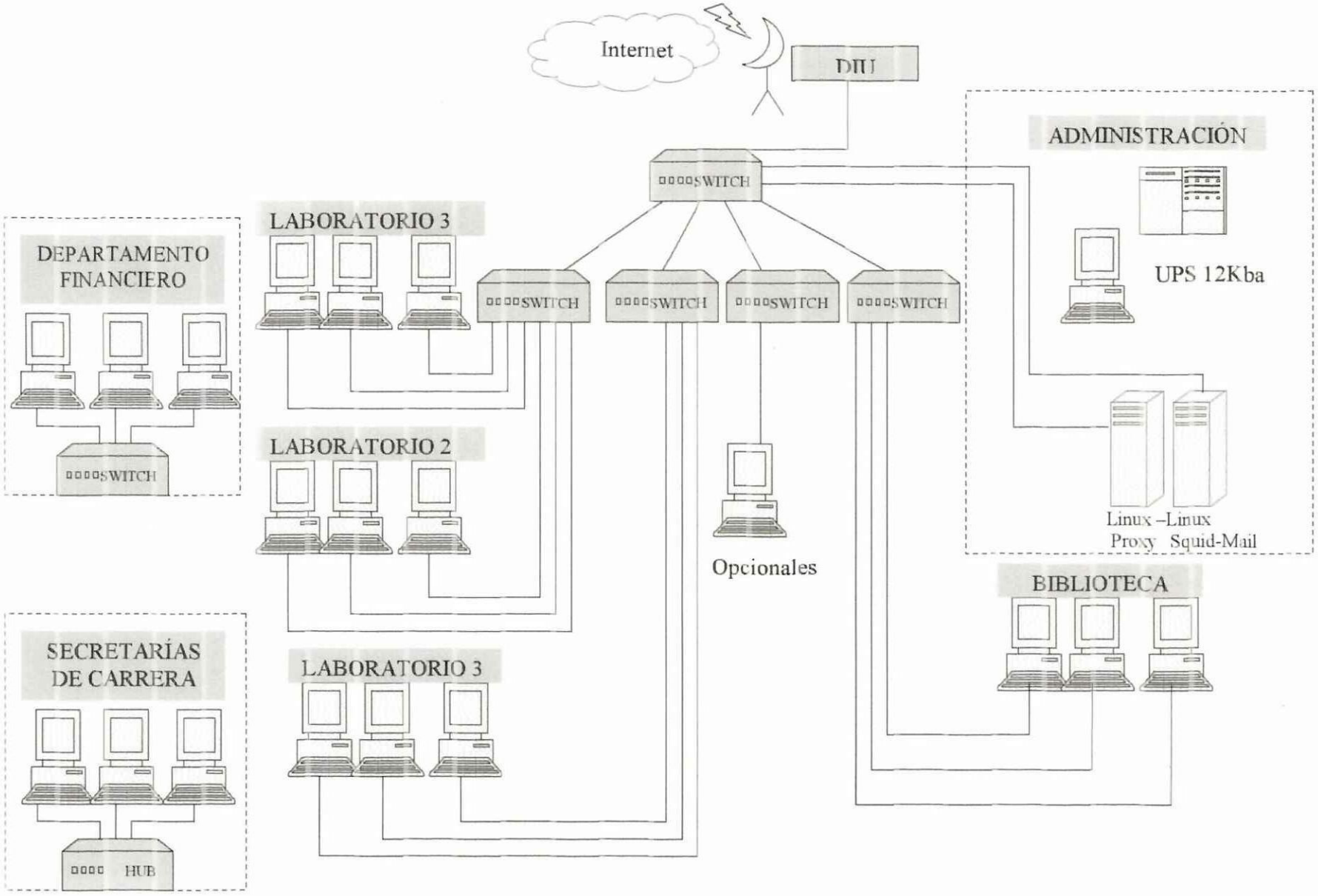
2.1 Estudio de la situación actual de la red de datos de la Universidad Técnica de Cotopaxi (UTC)

Con el propósito de una mejor organización para analizar la situación actual de la red de la Universidad Técnica de Cotopaxi se han dividido en las siguientes áreas: Laboratorios de computación, Biblioteca, Departamento Financiero, Secretaría de Carreras, Usuarios Independientes y opcionales,

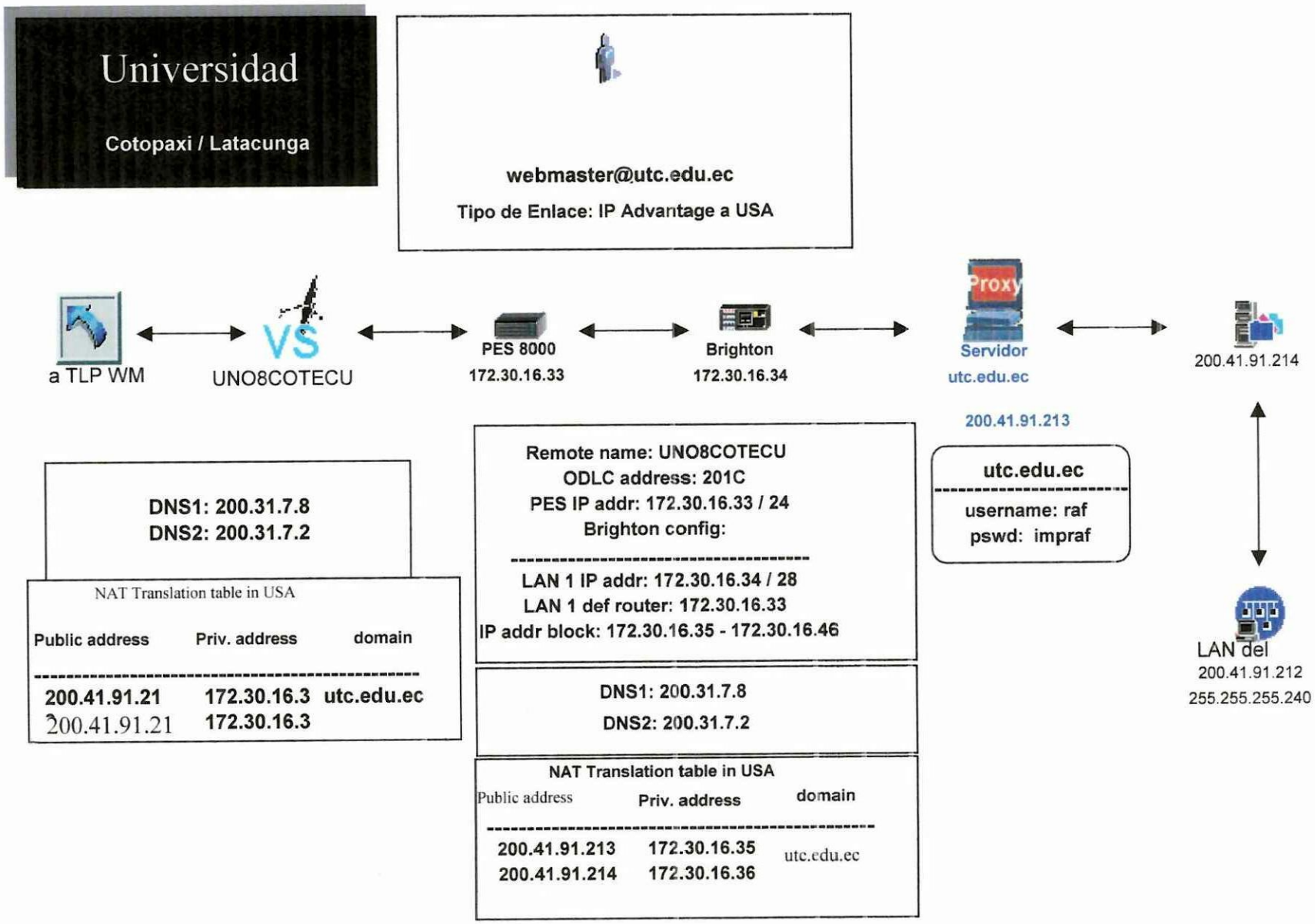
Para la recopilación de la información es necesario emplear técnicas como son la observación y encuestas que serán aplicadas al personal encargado de cada oficina con el fin de conocer el estado actual de software y hardware de cada computador. Permitiendo de está manera la tabulación de las encuestas y al personal técnico en la rama informática de la institución.

El estudio se lo realiza tomando en cuenta las tres redes LAN existentes, como son de los Laboratorios de Computación, Departamento Financiero y secretaria de Carreras, mediante la representación de diagramas se indicara donde se encuentran situados los equipos informáticos, tipo de conexión y detalle del software y del hardware existente.

2.1 DIAGRAMA DE LA RED DE DATOS DE LA UTC



2.2 DIAGRAMA DE INTERCONEXIÓN SATELITAL



2.2 Descripción de la red LAN de la UTC

A continuación se describe en forma general la red LAN de la UTC comenzando por los laboratorios de Computación, Biblioteca, usuarios opcionales e independientes, y los Departamentos de Secretaria de Carreras y Financiero.

2.2.1 Análisis de los Laboratorios de Computación

A continuación se explica en forma técnica referente a los laboratorios de computación.

- ✓ Descripción del ámbito informático y de red
  - La Universidad Técnica de Cotopaxi cuenta con tres laboratorios de computación los cuales se encuentran conectados mediante una red Ethernet y Fast Ethernet con una velocidad de transmisión es de 10Mbps y 100Mbps respectivamente, además consta con equipos informáticos moderados los cuales se encuentran en su mayor parte concentrado en el centro de computo de la Universidad.
  - Los Laboratorios 1 y 2 poseen 11 y 11 computadoras respectivamente. Son Marca Compaq Pentium II los cuales se encuentran conectados en red y disponen de servicio de Internet. El Laboratorio 3 posee 8 computadores Pentium III de 866 Mhz. y presta servicio exclusivo de Internet.

- Por el excesivo número de estudiantes que quieren acceder a Internet, el Laboratorio de computación utiliza un sector de la Biblioteca en el cual se encuentran cuatro computadoras, las cuales facilitan el acceso a Internet a la comunidad Universitaria.
- La Biblioteca posee dos computadoras en red, en la principal está instalado el programa Siabug que es un sistema automatizado de Biblioteca, en el cual contiene la base de datos de los libros y en el terminal esta configurado Siabug de consulta para facilitar la búsqueda de libros.
- Los operadores de computadoras son los encargados de controlar los dispositivos de interconexión para la red de datos de la Universidad mencionados.

✓ Topología utilizada

La red se encuentra instalada con una topología tipo Estrella

✓ Cableado

El cable utilizado en esta red interna, es el UTP categoría 5.

✓ Equipos de conexión

- La red de la Universidad utiliza una tecnología Ethernet y Fast Ethernet empleando un Switch 10 /100 3Com Súper Stack 2, de 12 puertos y a un Switch 3Com 16 plus de 16 puertos.

- ✓ Estado actual de las conexiones
    - Cableado UTP esta instalado en el laboratorio mediante conexiones internas (por la pared) las cuales dan a cajetines con conectores RJ45.
    - Los componentes de red y los sistemas de comunicación en todas la áreas de la red (tarjetas de interfase de red, cables y conectores), están en buen estado de funcionamiento.
- ✓ El Servidor de Red
    - La computadora que esta trabajando como servidor de la red es un IBM PC SERVER 350, este servidor se emplea como Proxy que permite complementar la seguridad para la salida a Internet, además tiene instalado el paquete Apache para el servidor Web. Actualmente es el que controla toda la red, y esta funcionando como un servidor dedicado.
    - El dominio de la red es: utc.edu.ec. La red esta operando con una plataforma de ambiente Linux Red Hat 7.3, existe otro servidor secundario Compaq Proline en el cual se encuentra configurado para correo electrónico el mismo que utiliza Squid mail para esta función.

- ✓ Estaciones de Trabajo

  En las estaciones de trabajo esta instalado y configurado Windows Milenium o XP para trabajar en red, las mismas que poseen software básico. Los más utilizados son los siguientes:

  - Office 97, graficadotes, Mónica, paquetes visuales como: Visual Studio, y otros.
  - A continuación se describen las licencias que posee la Universidad Técnica de Cotopaxi, no obstante existen en las computadoras software instalado sin su respectiva licencia.

Software	Número de Licencias	Empresa Proveedora
AutoDesk AutoCad R14+R2000 SP AE	2	Argos
BackOffice CAL 4.5 English	16	Argos
BackOffice SBS 4.5 Español AE	1	Ingelsi
Corel Draw V8.0 AE	1	Argos
Corel Draw V8.0 AE	1	Ingelsi
Delphi Developer	1	
Exchange CAL 5.5 English	21	Argos
Ingles Your Way 2.0	1	Ingelsi
Monica Cal - Software Contable	10	Argos
Monica Software Contable	1	Argos
Norton Utilities V. 3.0	1	Ingelsi
Office 95	1	
Office 97 (paquete)	1	Ingelsi
Office para windows 95 version 7	1	
Office Pro 2000 Win32 English	21	Argos
Office Pro 2000 Win32 English (paquete)	1	Argos
Office Pro 97 Win32 English	20	Ingelsi
Power Translator Pro - Traductor	1	Ingelsi
Proxy Server 2,0 Español	1	Ingelsi
TVD Suite 1-Yr Subscription License v4.0	55	Argos
TVD Suite Subscription License v4.0 (Paquete)	1	Argos
Visual C++ V1.52	1	

VStudio .NET Pro 6.0 Win32 (paquete)	1	Argos
VStudio .NET Pro 6.0 Win32 English	15	Argos
Windows NT Svr 4.0 English	1	
WinNT CAL 4.0 English	29	Argos
WinNT Wrkstn 4.0 English	1	Argos
WinNT Wrkstn 4.0 English	20	Argos

Tabla 2.1 Licencias de software

- ✓ Protocolos de comunicación utilizados.

  El protocolo de comunicaciones utilizado es el TCP/IP.

- ✓ Recursos Humanos

  - Existen dos operadores de computadoras quienes son los encargados de controlar los dispositivos de interconexión de la red de datos de la Universidad, mencionado equipos de red se encuentran ubicados en la misma oficina.
  - Hay cuatro ayudantes de laboratorio los cuales son escogidos basándose en sus calificaciones estudiantiles y de acuerdo a un análisis emitido por el departamento de Bienestar Social, el tiempo que presenta este servicio es por el lapso de 6 meses, que realizan turnos rotatorios dependiendo de sus horarios de estudio de la UTC.

✓ Las direcciones IP utilizadas

- En los servidores la IP son:

Grupo	Nombre Pc	IP	Mascara
Servidores	IBM Server	10.10.1.1	255.255.255.0
		172.30.16.35	255.255.255.240
Servidores	Compaq Server	10.10.1.2	255.255.255.0
	Router - DIU	172.30.16.33	
	DierecPc	172.30.16.34	

Tabla 2.2 Direccionamiento IP de servidores

- Las direcciones IP de los Laboratorios son:

Grupo	Nombre Pc	IP	Mascara
LAB1	Compaq10 hasta Compaq21	10.10.1.10 hasta 10.10.1.21	255.255.255.0
LAB2	Compaq22 hasta Compaq31	10.10.1.22 hasta 10.10.1.31	255.255.255.0
Administrativo	RelacPublic	10.10.1.80	255.255.255.0
Administrativo	DirecSistem	10.10.1.81	255.255.255.0
Administrativo	Rectorado	10.10.1.82	255.255.255.0
LAB3	PC_56	10.10.1.56	255.255.255.0
LAB3	PC_69	10.10.1.69	255.255.255.0
Administrativo	DirecAdministra	10.10.1.83	255.255.255.0
Administrativo	DirecSistem	10.10.1.84	255.255.255.0
Administrativo	Rectorado	10.10.1.85	255.255.255.0
Internet	Biblioteca	10.10.1.100	255.255.255.0
Internet	Internet101	10.10.1.101	255.255.255.0
Internet	Internet102	10.10.1.102	255.255.255.0
Internet	Internet103	10.10.1.103	255.255.255.0
Internet	Internet104	10.10.1.104	255.255.255.0

Tabla 2.3 Direccionamiento IP de terminales

✓ Salida satelital a Internet

- El servicio de Internet que dispone la Universidad Técnica de Cotopaxi, es proporcionado por la Empresa Impsat, el cual es un servicio de tipo VISAT de alta velocidad, con una

portadora de 2 Mb compartida, de 256 kbps de bajada y 128 kbps de subida.

- Se dispone de un servidor el cual se encuentra ubicado en el campus central de la Universidad Técnica de Cotopaxi, posee un Proxy y FireWall basado en el sistemas operativo Linux Red Hat 7.3.El cual se conecta a un Brigthon el cual tiene la función de mejorar la velocidad de la portadora también es conocido con el nombre de DirectPC.
- Luego se conecta a un Pes8000 o conocido también como DIU, el cual cumple la función de codificar y decodificar la información tanto entrante como saliente (analógico <-> digital), se encarga de establecer la conexión entre estaciones mediante antenas.
- Finalmente tenemos la antena la cual es una UNO8COTECU, es una antena de fibra de vidrio de 1.8 metros de diámetro, la cual se encuentra apuntando al satélite que se encuentra en la orbita ecuatorial, y se comunica con el TLP WM tele puerto en Miami Estados Unidos, mejorando la velocidad de conexión ya que el enlace entre la Universidad Técnica de Cotopaxi es en forma directa con Miami.

Ventajas

- Velocidad de 2 Mb con una portadora compartida
- Conexión Directa a Estados Unidos – Miami
- Estabilidad en el Enlace.
- El DNS se encuentra en Estados Unidos.
- Conexión permanente 24 horas.

Desventajas

- Costo Elevado.
- Retardo satelital (Implícito – se compensa con una portadora de alta capacidad).
- Cortes de señal anticipado de acuerdo a un calendario planificado (SONOUTAGER).

✓ Varios

- El costo de los ticket es de acuerdo a las resoluciones tomas por las autoridades de la UTC; cuyos costos son los siguientes:

Servicio de Usuario	0,08
Servicio de Internet	0,40
Servicio de Internet a personas particulares	0,80
Grabación de CD	1,00
Impresión color	0,20
Impresión Blanco y Negro	0.08
Scanner	0,12

Tabla 2.4 Costos de Ticket

- El estudiante que no tenga comprado su ticket también esta pagando directamente a los encargados del laboratorio el valor del uso de los equipos.

- No existe un software de monitoreo en los terminales.
- No existe un software de auditoria en los terminales.
- Los Usuarios opcionales son computadoras conectadas a Internet mediante Switch que posee el Laboratorio de Computación entre las cuales se encuentran las siguientes:
    - Rectorado.
    - Vicerrectorado.
    - Dirección de CIYA.
    - Relaciones Públicas.
    - Dirección Administrativa
    - Dirección Financiera
    - Pagaduría

2.2.2 Análisis de la red del Departamento Financiero

Existe una red LAN entre computadoras, las cuales pertenecen a cada una de las oficinas de la dirección mencionada:

- Director Financiero
- Contador
- Auxiliar uno de Contabilidad
- Auxiliar dos de Contabilidad
- Secretaría de Dirección Financiera
- Sub Dirección Financiera

- ✓ Topología utilizada

  La mencionada red se encuentra instalada con una topología tipo Estrella.

- ✓ Cableado

  El cable utilizado en esta red interna es el UTP categoría 5, el cual se encuentra instalado mediante canaletas a la pared.

- ✓ Equipos de Conexión

  Por la topología con la que trabaja esta red está utilizando un Switch 3com Super Stack 3, el mismo que posee 24 puertos para la conexión en red.

- ✓ Estado actual de las conexiones

  El switch que se esta utilizando en esta red actualmente, tiene algunos puertos disponibles en caso de proyecciones futuras.

- ✓ El servidor de red

  - El servidor de red es un Pemtium IV de marca COMPAQ Proliant, con Windows 2000 Server; el cual permite identificar a cada una de las oficinas del departamento, este servidor se encuentra ubicado en la Dirección Financiera. El control del servidor de red esta a cargo del personal que labora en la oficina de contabilidad en caso de surgir algún contratiempo con el servidor solicitan ayuda al personal encargado del laboratorio de computación.
  - Las seguridades que se encuentran en el servidor son:
    - Tiene una llave para su encendido
    - Contraseña de Windows 2000

- ✓ Estaciones de trabajo

  En las terminales de trabajo esta instalado y configurado Windows Milenium para trabajar en red. Para la seguridad en la red estas computadoras tienen cuentas en el servidor con sus respectivos nombre de usuario y contraseña, las mismas que poseen software básico. Los más utilizados son los siguientes:

  - Office 97, antivirus.

- ✓ Software de aplicación

  En el servidor se encuentra instalado un software llamado OLYMPO, el cual contiene todas las funciones de un ciclo contable, cuyo empresa proveedora es PROTELCOTELSA – Quito. Para garantizar la utilización de este software la empresa proveedora ha dotado de nombre de usuario y contraseñas para el acceso a las funciones contables del sistema y además se realizan respaldos cada tres meses para mantener la información fidedigna.

- ✓ Protocolos de Comunicación utilizados

  El protocolo de comunicación usado es el TCP/IP

- ✓ Varios

  Las oficinas de este departamento comparten una impresora Epson LQ 2170 y Láser HP Color.

2.2.3 Análisis de la red LAN existente en la Secretarias de Carreras

Son cuatro computadoras que integran esta red LAN, las cuales están organizadas respectivamente en su área de trabajo en donde se analizaron las siguientes: Secretarias Ciencias Agropecuarias Ambientales y Veterinarias (CAAV), Secretaría de Carrera administrativas humanísticas y del Hombre (CC.AA.HH.H), Secretaría de Carrera de Ciencias de la Ingeniería y Aplicadas(CIYA), Centro de Educación a Distancia, Centro de Investigación y Postgrado.

Esta red interna es absolutamente independiente de la LAN interna de las demás redes existentes en la Universidad.

- ✓ Topología utilizada

  La mencionada red se encuentra instalada con una topología tipo Estrella.

- ✓ Cableado

  El cable utilizado en esta red interna es el UTP categoría 5, el cual no brinda las garantías suficientes puesto que existen tramos que están sin protección.

- ✓ Equipos de Conexión

  Por la topología con la que trabaja esta red está utilizando un HUB el mismo que posee 8 puertos para la conexión en red.

- ✓ Estado actual de las conexiones

  El HUB que se esta utilizando en esta red actualmente, tiene algunos puertos disponibles en caso de proyecciones futuras.

- ✓ Servicio de impresión en la Red

  La característica primordial al momento es para compartir el servicio de impresión para las oficinas de secretaría.

  El control de Impresión en red esta a cargo de la secretaria del Ciencias Humanísticas y del Hombre, en caso de surgir algún contratiempo en la red solicitan ayuda a los operadores del centro de computo.

  El software instalado en los terminales es Windows 98, además poseen software básico como es Office 97, antivirus.

- ✓ Software de Aplicación
  - En Secretarías de Carrera no existe ningún software que permita la Automatización de la información que permita brindar un mejor servicio a quienes lo soliciten.

- ✓ Protocolos de Comunicación utilizados

  El protocolo de comunicación usado es el TCP/IP

- ✓ Otros Usuarios

  Para los usuarios independientes se han considerado a los siguientes:

  - Dirección de Planeamiento
  - Procuraduría
  - Secretaria General
  - Bienestar Universitario
  - Dirección de Proyección Social

- Administración CEYPSA
- Sala de Profesores
- Laboratorio de Suelos
- Fue-C
- Recepción

ESTUDIO

DE

LA SITUACIÓN ACTUAL DE LA RED

EN LOS

LABORATORIOS DE COMPUTACIÓN.

CONTENIDO

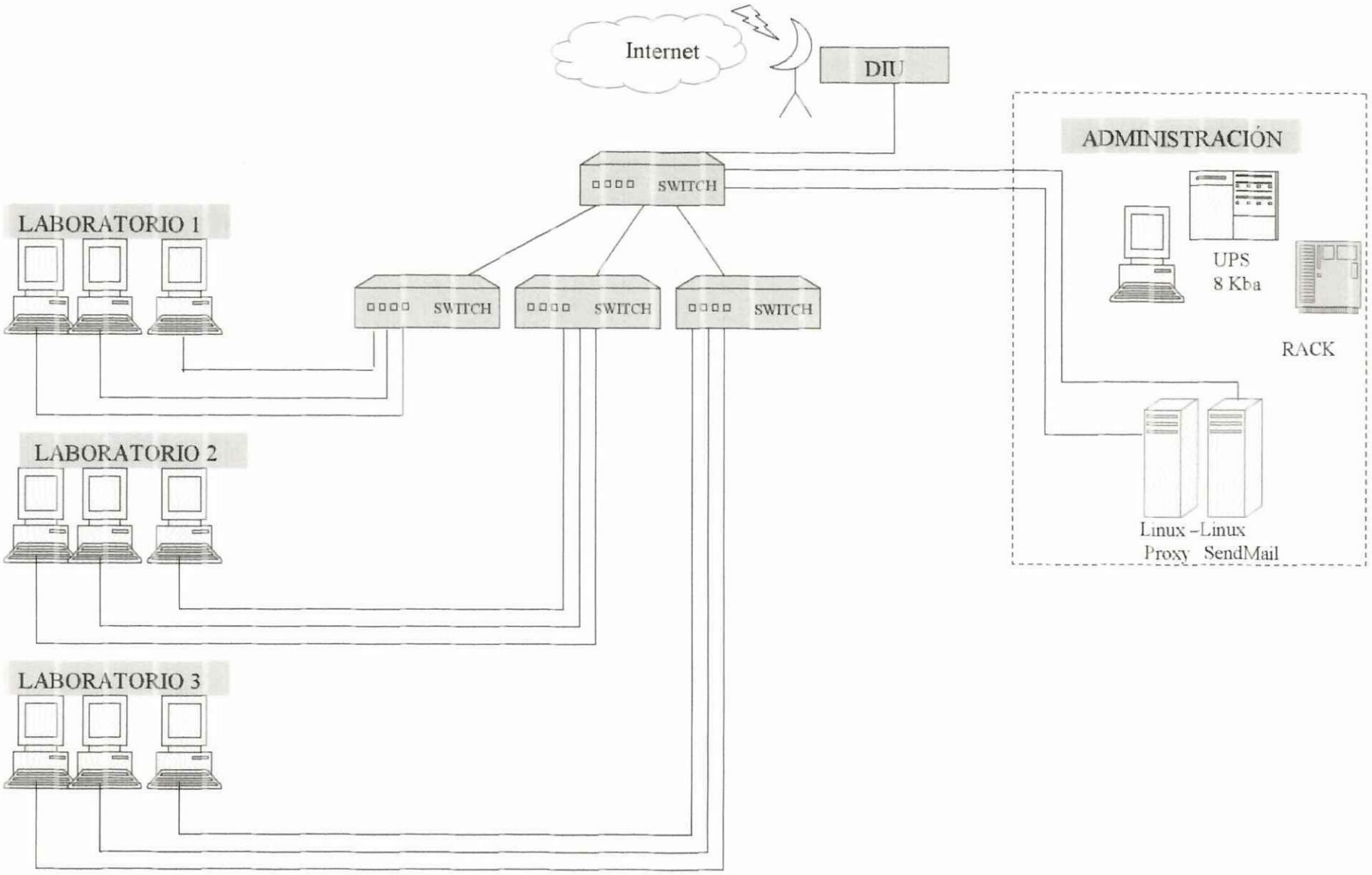
2.3.1 DIAGRAMA DE LA RED DE DATOS.

2.3.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED.

2.3.3 ANÁLISIS DE LAS ENCUESTAS REALIZADAS A LOS LABORATORIOS DE COMPUTACIÓN (Ver Anexo 1).

2.3.4 INTERPRETACIÓN DE RESULTADOS DE LOS LABORATORIOS DE COMPUTACIÓN (Ver Anexo 1).

2.3.1 DIAGRAMA DE LA RED DE DATOS DE LOS LABORATORIOS DE COMPUTACIÓN



2.3.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED DE LOS LABORATORIOS DE COMPUTACIÓN.

Tabla 2.5 Computadoras del área de administración

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	IBM	SERVER 35O	80	256	✓	✓	✓	Ethernet 10/100	Linux Red Hat 7.3	Proxy		TCP/IP
1	Compaq	SERVER	80	256	✓	✓	✓	Ethernet 10/100	Linux Red Hat 7.3	SendMail		TCP/IP
1	Compaq	Pentium IV	80	256	✓	✓	✓	Ethernet 10/100	Windows Me		- Office, - Mónica - Flash - Autocad - Antivirus	TCP/IP

Tabla 2.6 Computadoras del Laboratorio 1

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
9	Compaq	Pentium Pro	1.95	64	✓	✓	✓	Ethernet 10/100 Mbps	Windows Me		Office, Mónica Compiladores (C, Borland C++, Visual studio, Delphi) -Flash - Antivirus	TCP/ IP

Tabla 2.7 Computadoras del Laboratorio 2

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
13	Compaq	Pentium Pro	1.95	64	✓	✓	✓	Ethernet 10/100 Mbps	Windows Me		Office, Mónica Compiladores (C, Borland C++, Visual studio, Delphi) -Flash - Antivirus	TCP/ IP

Tabla 2.8 Computadoras delLaboratorio 3

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
14	Clon	GenuIneInte l 3	10	256	✓	✓	✓	Ethernet link 10/100	Windows XP		Office, Mónica Compiladores (C, Borland C++, Visual studio, Delphi) -Flash - Antivirus	TCP/ IP

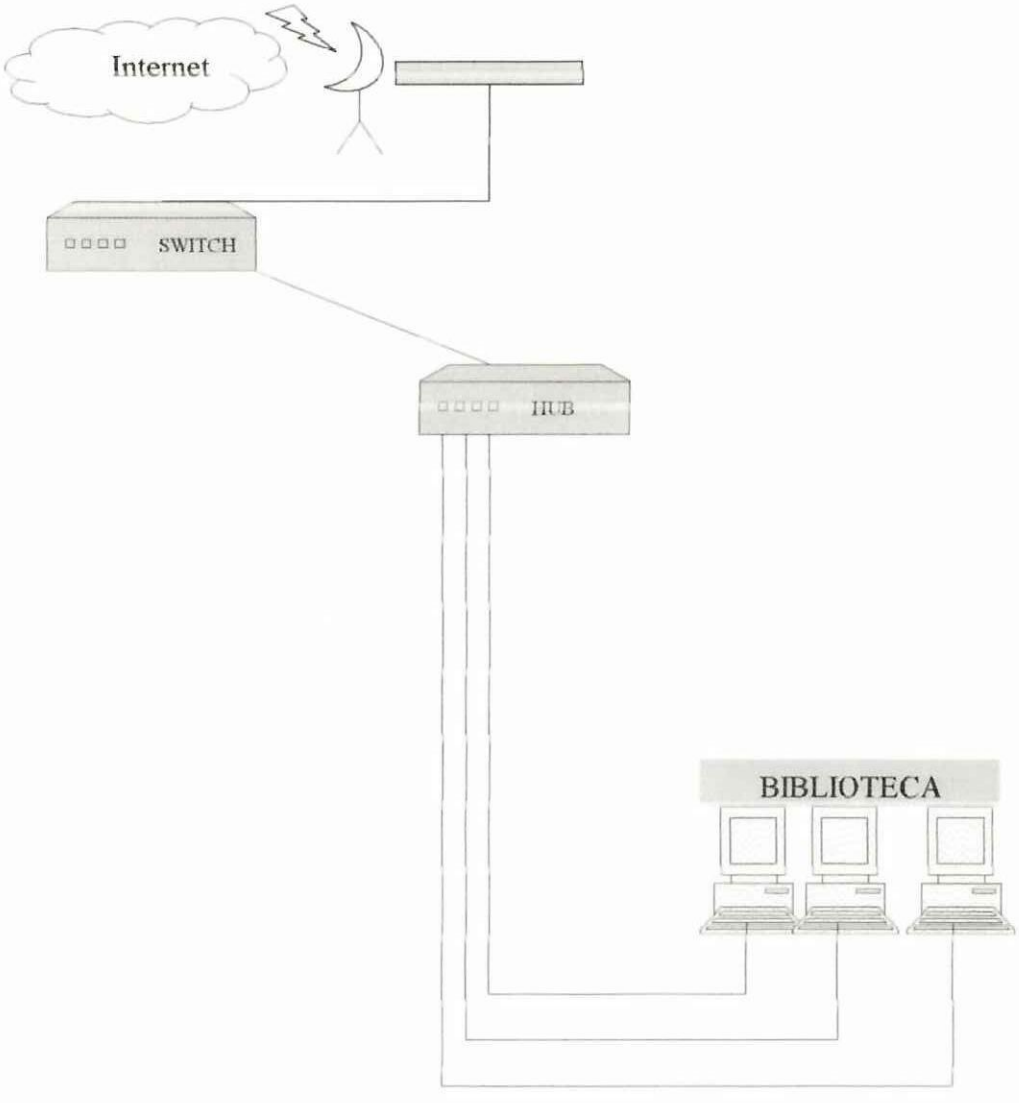
ESTUDIO
DE
LA SITUACIÓN ACTUAL DE LA RED
EN DE
LA BIBLIOTECA

CONTENIDO

2.4.1 DIAGRAMA DE LA RED DE DATOS.

2.4.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN.

2.4.1 DIAGRAMA DE LA RED DE DATOS DE LA BIBLIOTECA.



2.4.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN EN LA BIBLIOTECA.

Tabla 2.9 Computadoras de la Biblioteca área Internet

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
5	Compaq	Intel Pentium Pro	1.95	64	✓	✓	✓	Ethernet 10/100	Windows 95		- Office -Explorador de Internet - Antivirus	TCP/ IP

Tabla 2.10 Computadoras de la Biblioteca

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium III	30	128	✓	✓		Fast Ethernet	Windows 98	Siabug (Sistema Bibliotecario)	- Office - Antivirus	TCP/IP
1	DTK	Intel 486	0.80	16	✓			Fast Ethernet	Windows 95	Siabug		TCP/IP

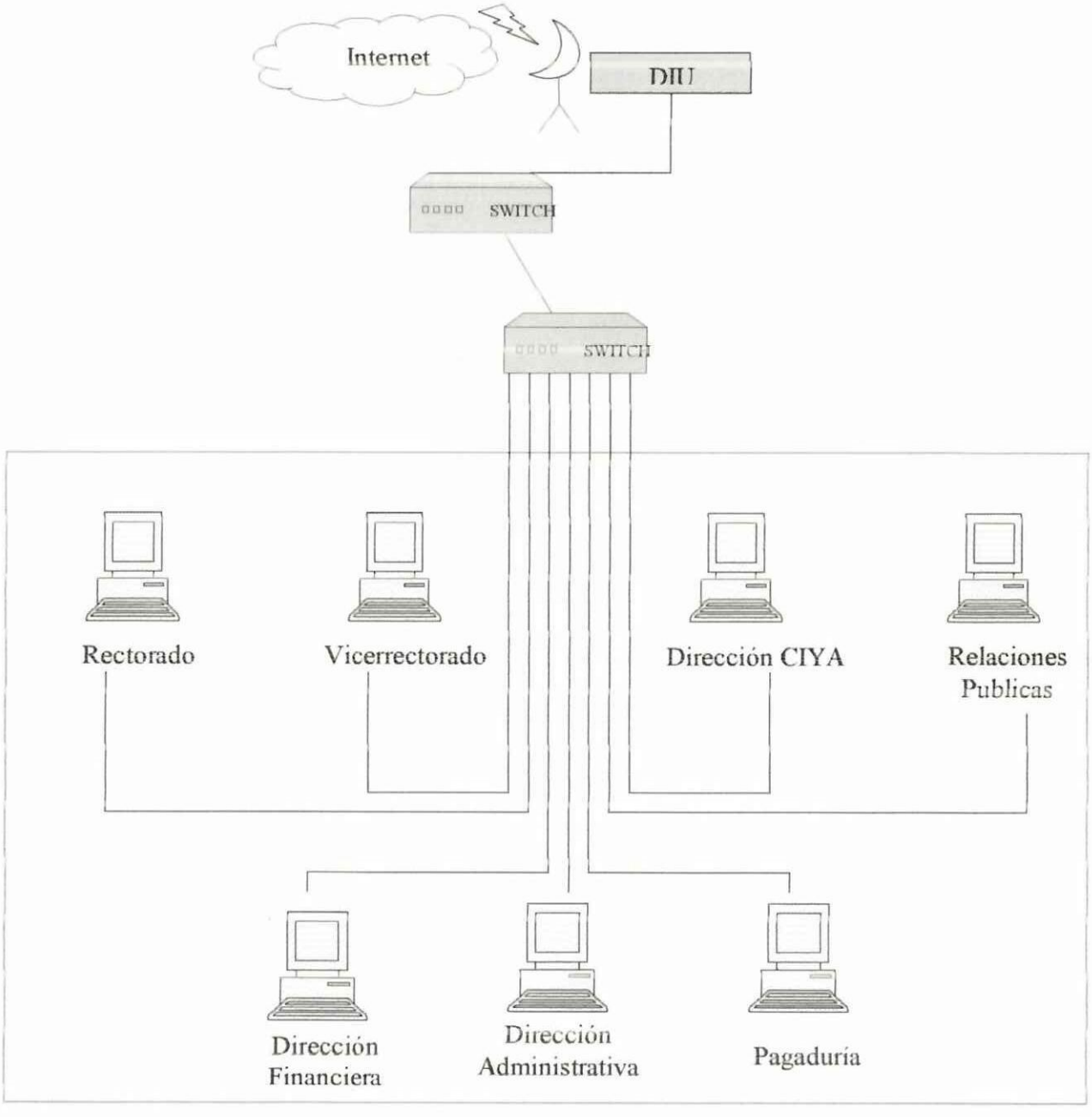
Tabla 2.11 Constatación física de otro hardware en la biblioteca

Ubicación	Cantidad	Descripción	Marca	Modelo	Tipo	Estado
Biblioteca	1	Impresora	Epson	Q870	Matricial	Bueno

ESTUDIO
DE
LA SITUACIÓN ACTUAL DE LA RED
EN LOS
USUARIOS OPCIONALES.

CONTENIDO

2.5.1 DIAGRAMA DE RED DE USUARIOS OPCIONALES



2.5.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED DE USUARIOS OPCIONALES.

Tabla 2.12 Computadora del Rectorado

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium II	30	256	✓	✓			Windows XP		- Office - Antivirus	TCP/IP

Tabla 2.13 Computadoras del Vicerrectorado

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro(Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓		Fast Ethernet	Windows Me		- Office - Antivirus	TCP/IP
1	DTK	Cirix Instead 486	1.2	32	✓	✓		Fast Ether link	Windows 95		- Office - Antivirus	TCP/IP
1	Toshiva Portatil	Intel Pentium III	18.66	256	✓	✓			Windows XP		- Office - Antivirus	TCP/IP

Tabla 2.14 computadora de Relaciones Publicas

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium II	30	256	✓	✓			Windows XP200		- Office - Antivirus	TCP/IP

Tabla 2.15 Computadora de Dirección de Carreras CIYA

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium IV	30	256	✓	✓		Color	Windows 98		- Office - Antivirus	TCP/IP

Tabla 2.16 Computadora de la Oficina Dirección Administrativa

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium Pro	8	64	✓	✓			Windows 98		- Office - Antivirus	

Tabla 2.17 Constatación física de otro hardware de Secretarías de Carrera

Ubicación	Cantidad	Descripción	Marca	Modelo	Tipo	Estado
Vicerrectorado	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno

ESTUDIO
DE
LA SITUACIÓN ACTUAL
DE LA RED
DEL DEPARTAMENTO FINANCIERO.

CONTENIDO

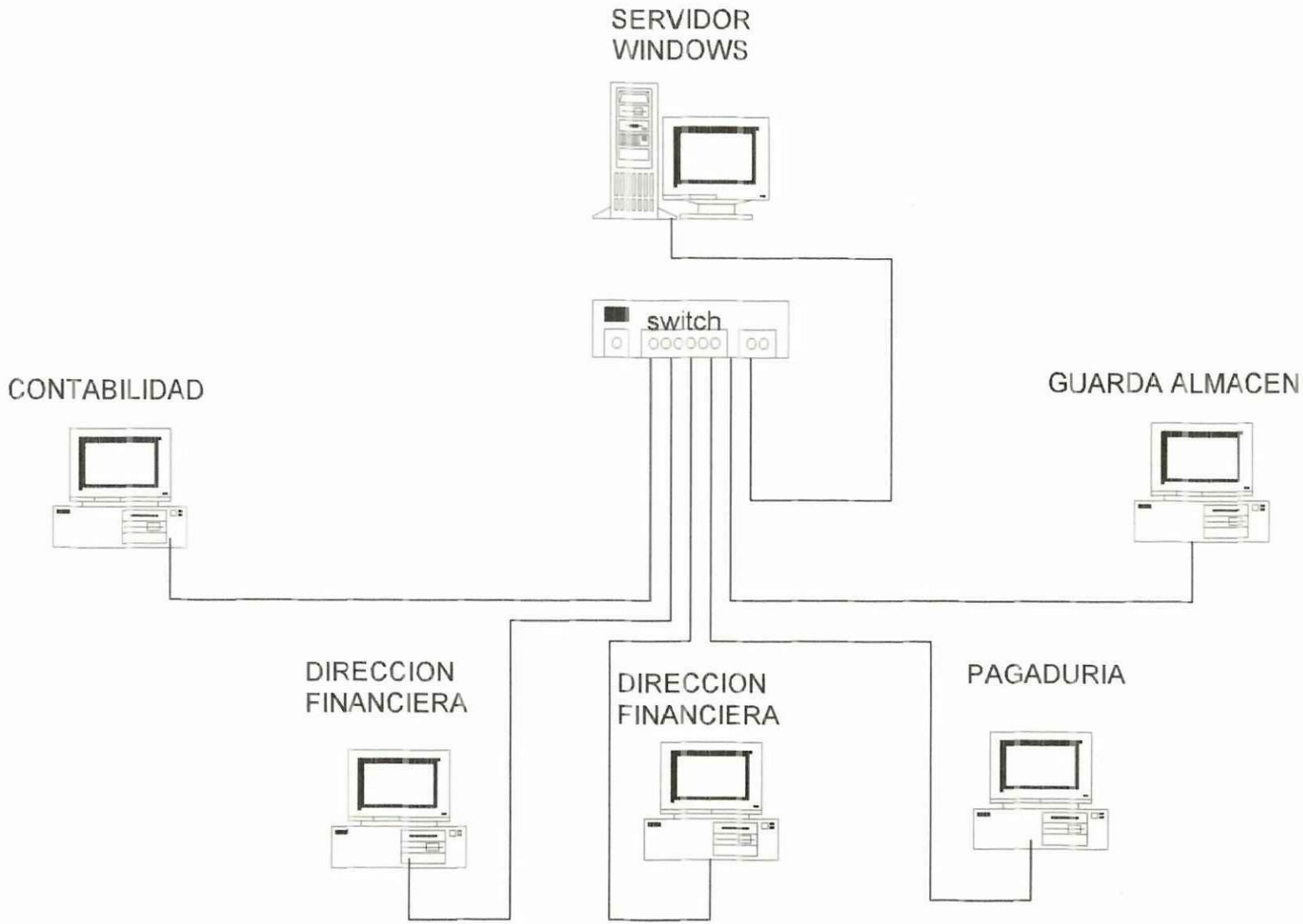
2.6.1 DIAGRAMA DE LA RED DE DATOS.

2.6.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED.

2.6.3 ANÁLISIS DE LAS ENCUESTAS AL DEPARTAMENTO FINACIERO (Ver Anexo 3).

2.6.4 INTERPRETACIÓN DE RESULTADOS DEPARTAMENTO FINACIERO(Ver Anexo3).

2.6.1 DIAGRAMA DE LA RED LAN DEL DEPARTAMENTO FINANCIERO



2.6.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED DEL DEPARTAMENTO FINACIERO.

Tabla 2.18 Computadoras de Dirección Financiera

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium II	8	32	✓	✓		Ethernet 10/100	Windows NT	OLYMPO(Sistema contable)	- Office - Antivirus	TCP/IP
1	Premio	Intel Pentuim I Pro	2	16	✓	✓		Ethernet 10/100	Windows 95		- Office - Antivirus	TCP/IP
1	Compaq	Intel Pentium II	8	64	✓	✓		Ethernet 10/100	Windows 95	OLYMPO(Programa Contable)	- Office - Antivirus	TCP/IP

Tabla 2.19 Computadoras de Contabilidad

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓		Ethernet 10/100	Windows Me		- Office - Antivirus	TCP/IP
1	Compaq	Intel Pentuim II P	30	256	✓	✓		Ethernet 10/100	Windows 98	Olympo	- Office - Antivirus	TCP/IP
1	Compaq	Intel Pentium II	8	64	✓	✓		Ethernet 10/100	Windows 95	Olympo	- Office - Antivirus	TCP/IP

Tabla 2.20 Computadora de Tesorería

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
2	Compaq	Pentuim Genuine Intel	20	64	✓	✓		Ethernet 10/100	Windows 98	Tesorería Conex	- Office - Antivirus	TCP/IP

Tabla 2.21 Computadoras de Guarda Almacén

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓		Ethernet 10/100	Windows Me		- Office - Antivirus	TCP/IP
2	Premio	Intel Pentuim I	1.58	32	✓	✓		Ethernet 10/100	Windows 95		- Office - Antivirus	TCP/IP

Tabla 2.22 Constatación física de otro hardware en el Departamento Financiero

Ubicación	Cantidad	Descripción	Marca	Modelo	Tipo	Estado
Dep.Financiero	1	Impresora	HP	670C	Inyección a tinta	Bueno
Contabilidad	2	Impresora	Epson	Fx2180	Matricial	Bueno
Contabilidad Auxiliar	1	Impresora	HP	Deskyet 840 C	Inyección a tinta	Bueno
Tesoreria	1	Impresora	Epson	Lx300	Matricial	Bueno
Guarda/almacen	1	Impresora	Epson	LQL70	Matricial	Bueno
Auxiliar Guarda/almacen	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno

ESTUDIO

DE

LA SITUACIÓN ACTUAL DE LA RED

DE LAS SECRETARÍAS DE CARRERA

CONTENIDO

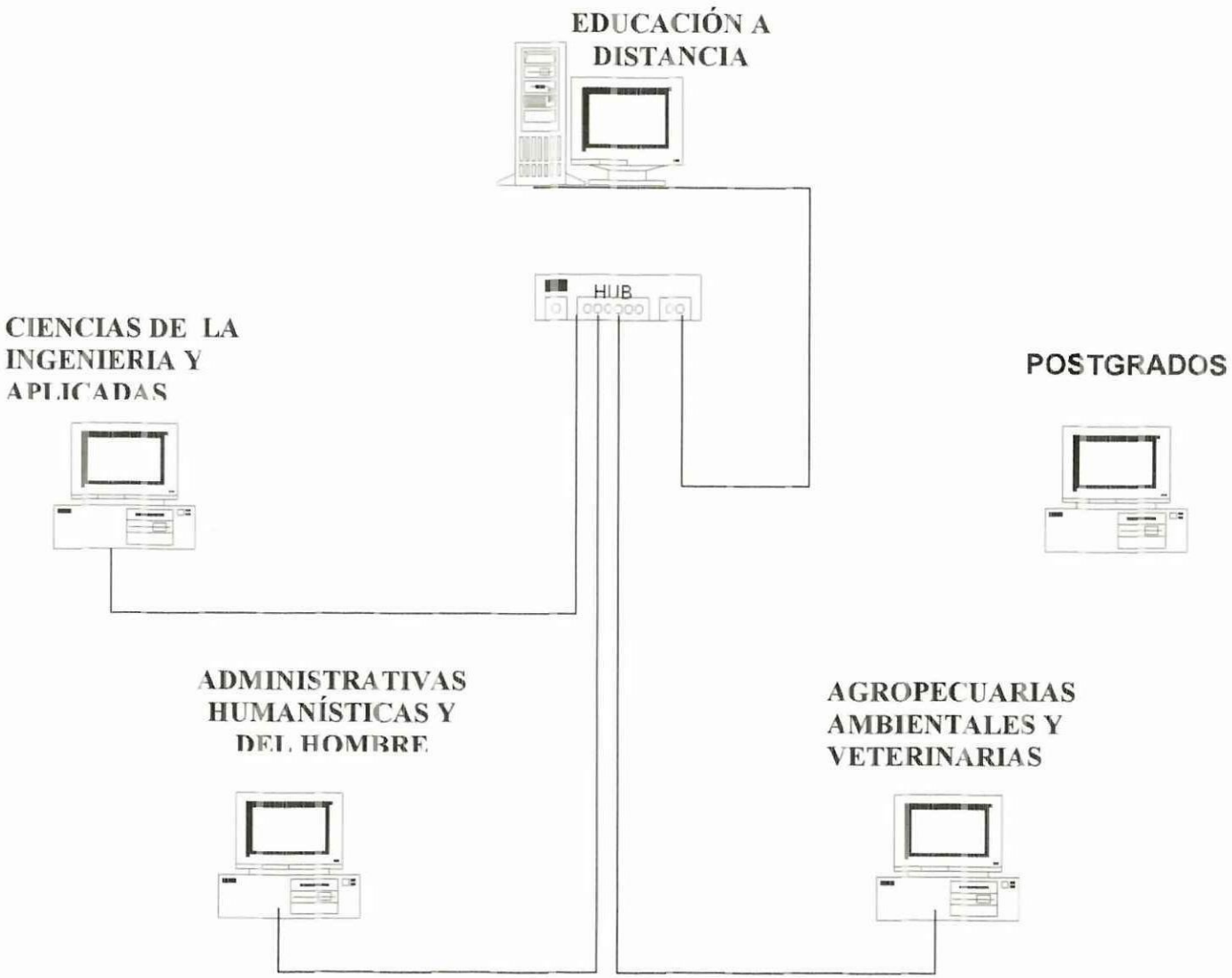
2.7.1 DIAGRAMA DE LA RED DATOS.

2.7.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED.

2.7.3 ANÁLISIS DE LAS ENCUESTAS A LAS SECRETARÍAS DE CARRERA (Ver Anexo3).

2.7.4 INTERPRETACIÓN DE RESULTADOS DE LAS SECRETARÍAS DE CARRERA (Ver Anexo).

2.7.1 DIAGRAMA DE LA RED DE SECRETARÍAS DE CARRERA.



2.7.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE RED DE SECRETARÍAS DE CARRERA.

Tabla 2.23 Computadora de Secretaria de Distancia

Cant	HARDWARE								SOFTWARE			
	Marca	Procesador	Disco Duro (Gb)	Ram (Mb)	Dispositivos			Tarjeta de red	Sistema Operativo	Sistema de Aplicación	Utilitarios	Protocolo
					Floppy	CD	Multi media					
1	Compaq	Intel Pentium IV	80	256	✓	✓	✓	Ethernet 10/100	Windows XP 2002		- Office - Antivirus	TCP/IP

Tabla 2.24 Computadora de Secretarias de Carrera Administrativas Humanísticas y del Hombre

Cant	HARDWARE								SOFTWARE			
	Marca	Procesador	Disco Duro (Gb)	Ram (Mb)	Dispositivos			Tarjeta de red	Sistema Operativo	Sistema de Aplicación	Utilitarios	Protocolo
					Floppy	CD	Multi media					
1	Premio	Intel Pentium Pro	1.57	32	✓	✓		Ethernet 10/100	Windows 98		- Office - Antivirus	TCP/IP

Tabla 2.25 Computadora de Carrera de ciencias de la ingeniería y aplicadas

Cant	HARDWARE								SOFTWARE			
	Marca	Procesador	Disco Duro (Gb)	Ram (Mb)	Dispositivos			Tarjeta de red	Sistema Operativo	Sistema de Aplicación	Utilitarios	Protocolo
					Floppy	CD	Multi media					
1	Premio	Intel Pentium Pro	1.57	32	✓	✓		Ethernet 10/100	Windows 98		- Office - Antivirus	TCP/IP

Tabla 2.26 Computadora de Secretarias Ciencias Agropecuarias Ambientales y Veterinarias

Cant	HARDWARE								SOFTWARE			
	Marca	Procesador	Disco Duro (Gb)	Ram (Mb)	Dispositivos			Tarjeta de red	Sistema Operativo	Sistema de Aplicación	Utilitarios	Protocolo
					Floppy	CD	Multi media					
1	Premio	Intel Pentium Pro	1.57	32	✓	✓		Ethernet 10/100	Windows 98		Office	TCP/IP

Tabla 2.27 Computadora de Secretarías de Postgrados

Cant	HARDWARE								SOFTWARE			
	Marca	Procesador	Disco Duro (Gb)	Ram (Mb)	Dispositivos			Tarjeta de red	Sistema Operativo	Sistema de Aplicación	Utilitarios	Protocolo
					Floppy	CD	Multi media					
1	Clon	Intel Pentium III	30	256	✓	✓		Ethernet 10/100	Windows 98		- Office - Antivirus	TCP/IP
1	Clon	Intel Pentium I Pro	30	256	✓	✓		Ethernet 10/100	Windows 95		- Office - Antivirus	TCP/IP

Tabla 2.28 Computadora de constatación física de otro hardware en Secretarías de Carrera

Ubicación	Cantidad	Descripción	Marca	Modelo	Tipo	Estado	Observaciones
Secretaria	1	Impresora	HP	670C	Láser	Bueno	

ESTUDIO

DE

LA SITUACIÓN ACTUAL DE LA RED

DE USUARIOS INDEPENDIENTES.

CONTENIDO

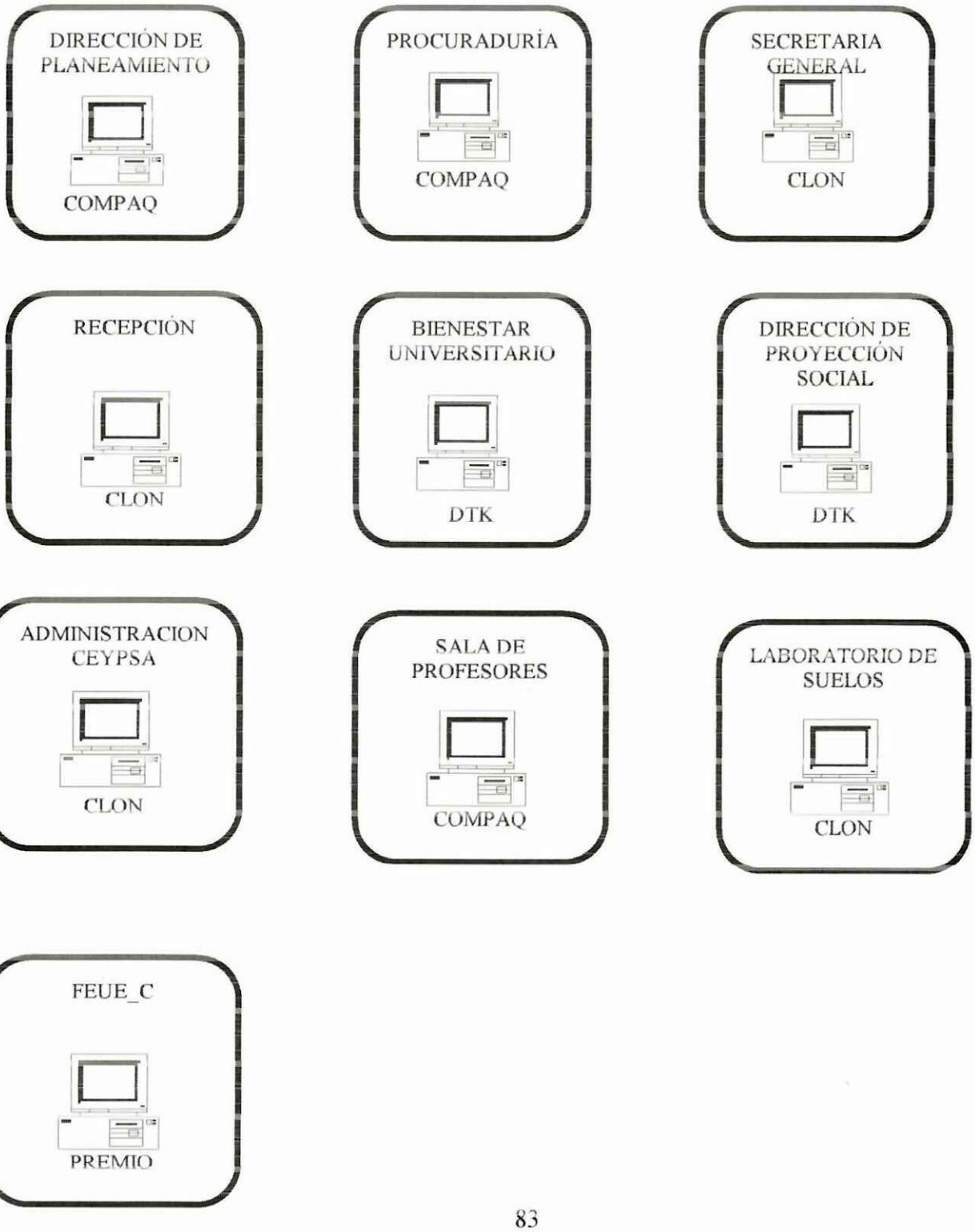
2.8.1 DIAGRAMA DE LA RED DE DATOS.

2.8.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN

2.8.3 ANÁLISIS DE LAS ENCUENSTAS REALIZADAS A LOS USUARIOS INDEPENDIENTES (Ver Anexo 4).

2.8.4 INTERPRETACIÓN DE RESULTADOS DE LOS USUARIOS INDEPENDIENTES (Ver Anexo 4).

2.8.1 DIAGRAMA DE USUARIOS INDEPENDIENTES.



2.8.2 CARACTERÍSTICAS DE HARDWARE, SOFTWARE E INTERCONEXIÓN DE USUARIOS INDEPENDIENTES.

Tabla 2.29 Computadora de Secretaria General

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓		Fast Ethernet	Windows Me		- Office - Antivirus	TCP/IP

Tabla 2.30 Computadoras de Proyección Social

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	DTK	Intel Pentium 486	1.2	23	✓	✓		Fast Ethernet	Windows 95		- Office - Antivirus	TCP/IP

Tabla 2.31 Computadora de la Oficina de Planeamiento y Planificación

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
2	Compaq	Intel Pentium Pro	8	4.15	✓	✓		Ethernet	Windows 95		- Office - Antivirus - AutoCad	TCP/IP

Tabla 2.32 Computadora de la oficina de administración Ceypsa

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓		Ethernet	Windows Me		- Office - Antivirus - Diccionarios	TCP/IP

Tabla 2.33 Computadora de la Oficina de Procuraduría

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium II	4	64	✓				Windows 98		- Office - Antivirus	TCP/IP

Tabla 2.34 Computadora de la sala de profesores

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Compaq	Intel Pentium Pro	4.15	64	✓	✓			Windows 95		- Office - Antivirus	TCP/IP

Tabla 2.35 Computadora de Laboratorios de Suelos

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓			Windows Me		- Office -Antivirus - AutoCad	

Tabla 2.36 Computadora de FEUE

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Premio	Intel Pentium Pro	30	256	✓	✓		Fast Ether link	Windows 98		- Office - Antivirus	TCP/IP

Tabla 2.37 Computadora de la Oficina de Bienestar Universitario

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	DTK	CirixInstel	1.96	15	✓	✓		Ethernet	Windows 95		- Office - Antivirus	TCP/IP

Tabla 2.38 Computadora de la Oficina de Recepción

Cant	HARDWARE								SOFTWARE			
	Marca	*Procesador*	*Disco Duro (Gb)*	*Ram (Mb)*	*Dispositivos*			*Tarjeta de red*	*Sistema Operativo*	*Sistema de Aplicación*	*Utilitarios*	*Protocolo*
					Floppy	*CD*	*Multi media*					
1	Clon	Intel Pentium III	30	256	✓	✓			Windows 98		- Office - Antivirus	

Tabla 2.39 constatación de física de impresoras usuarios Independientes

Ubicación	Cantidad	Descripción	Marca	Modelo	Tipo	Estado
Secretaria de postgrado	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno
Recepción	1	Impresora copiadora	Xerox	214/212 DPC/E	Laser	Bueno
Dirección administrativa	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno
Direc.administrativa Secretaria	1	Impresora	HP	Deskyet 670c	Inyección a tinta	Regular
Proyección Social	1	Impresora	HP	Deskyet 670c	Inyección a tinta	Bueno
Bienestar universitario	1	Impresora	HP	C5884a	Inyección a tinta	Bueno
FEUE	1	Impresora	Epson	LQ810	Matricial	Dañada
Laboratorio de Suelos	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno
Secretaria	1	Impresora	HP	Laseryet450 Pcl6	Laser	Bueno
Secretaria General	1	Impresora	HP	Laseryet5l	Inyección a tinta	Bueno
Planeamiento	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno
Planeamiento	1	Impresora	Epson stylus	1520	Matricial	Bueno
Proyectos productivos	1	Impresora	Lexmark	Z32	Inyección a tinta	Bueno
Procuraduría	1	Impresora	HP	Deskyet845	Inyección a tinta	Bueno
Secretaria distancia	1	Impresora	Epson	Fx2180	Matricial	Bueno

2.9 Modelo de referencia OSI que utiliza la Universidad Técnica de Cotopaxi.

Con el fin de complementar el estudio de la red de la Universidad, es necesario analizar el modelo OSI[1] que utiliza la Universidad, para poder conocer con más detalle de las vulnerabilidades que pueden suscitarse en esta capas de red.

Funciones de las capas

7	Aplicación	Procesos de red a aplicaciones
6	Presentación	Representación de datos
5	Sesión	Comunicación entre hosts
4	Transporte	Conexiones de extremo a extremo
3	Red	Direccionamiento y mejor Ruta
2	Enlace	Accesos a otros medios
1	Física	Transmisión

Capa 7: La capa de aplicación: La capa de aplicación es la capa del modelo OSI mas cercana al usuario, y está relacionada con las funciones de mas alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales. Es el medio por el cual los procesos de aplicación de usuario acceden al entorno OSI.

[1] Lan times "Guía de Interoperatibilidad para redes", Tom Sheldom, 1997, Pg 76-79, 226-227

Su función principal en la red de datos de la Universidad es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.

Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, estando éstas controladas por protocolos de aplicación, y utilizando los servicios del nivel de presentación.

Las aplicaciones que se usan en la Universidad son:

- Programa contable Olympo
- Programas de hojas de cálculo.
- Programas de procesamiento de texto.
- Correo electrónico (mail - smtp).
- Páginas web (http).

En lo que se refiere a la capa de aplicación la Universidad cuenta con un software de aplicación para la red LAN del departamento Financiero llamado Olympo en el cual se maneja todo lo concerniente a un sistema contable.

El software Olympo esta protegido con contraseñas de usuario general propia del software, y las pertenecientes al servidor de bases de Datos de este departamento. Ninguna otra protección se ha encontrado dentro de este software contable. La seguridad en el nivel de aplicación es muy pobre, puesto que el programa contable Olimpo es el único tiene seguridad, y los demás programas usados en esta capa tienen poca o ninguna seguridad.

Capa 6: La capa de presentación: La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo. La tarea principal que cumple en la red de la Universidad es de aislar a las capas inferiores del formato de los datos de la aplicación, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red.

Es también la responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

En este ámbito la Universidad realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizados un formato común, estableciendo la síntesis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local estándar y red viceversa.
- Definir la estructura de los datos a transmitir. En el caso de la Base de datos se define el orden de transmisión y la estructura de los registros.
- Definir el código a usar para represente una cadena de caracteres(ASCII, EBCDIC, etc).
- Servir para dar el formato de la información que va a visualizar o imprimirla.
- Comprimir los datos si es necesario.

La seguridad en esta capa es media, por lo que un virus o un ataque cualquiera daña los formatos de datos reconocidos por el computador en otro incomprensible,

lo cual se traduce en un caos. Antes de imprimir los datos o encriptarlos, existen procesos que reconocen la clave de compresión o encriptación, con la cual pueden descifrar los datos, justo antes de protegerlos en la capa de aplicación.

Capa 5: La capa de sesión: La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos.

Las principales funciones que cumple en la red de la Universidad son:

- Establecer, administrar y finalizar las sesiones entre dos hosts que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, esta capa restaura la sesión a partir de un punto seguro y sin perdida de datos o si esto no es posible termina la sesión de una manera ordenada chequeando y recuperando todas sus funciones, evitando problemas en sistemas transaccionales.
- Sincronizar el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre maquinas y así poder regular quien habla y por cuanto tiempo o si hablan en forma alterna, es decir, las reglas del dialogo que son acordadas.

- Ofrecer disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar *tokens*. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación.
- Hacer *checkpoints*, que son puntos de recuerdo en la transferencia de datos.

La seguridad en esta capa, se haya que en las sesiones entre host, donde puede suceder que exista la intrusión de un pirata informático de el cual no se ha determinado el host que se ha comunicado y la conexión quede infinita buscando quien se esta comunicándose sin identificarse.

Si la sincronización de los Host no se ha establecido o existe dificultades en mantenerla, porque los host no son de la misma generación y la velocidad es muy rápida en los computadores de ultima generación, por lo que la velocidad de la red en este punto disminuye considerablemente si existen computadores antiguos.

Si la sesión se pierde por alguna falla, esta no siempre la restaura y puede suceder perdida en la transmisión de datos entre la comunicación de los Host, o mucho retrazo en la trasmisión.

Capa 4: La capa de transporte: La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. Para ello segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor.

La funciones principales en la red de la universidad son:

- Controlar la interacción entre procesos usuarios.
- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y direccionamiento de máquinas a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas, llamadas segmentos, en caso necesario y los pasa al nivel de red.
- Realizar funciones de control y numeración de unidades de información, fragmentación y reensamblaje de mensajes.
- Se encarga de garantizar la transferencia de información a través de la sub-red.

La seguridad en esta capa es para garantizar que se reciban todos los datos que son transportados de un Host a otro con un orden adecuado, realizando un control de extremo a extremo esto evita el congestionamiento o el cuello de botella de la información transmitida, en caso de la transportación del flujo de información fallara, los segmentos que pasan a nivel de red, se perderían en caso de situaciones extremas.

Capa 3: La capa de red: La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. También se ocupa de aspectos de contabilidad de paquetes.

La red de datos de la Universidad en la capa de red posee siguientes puntos:

- Dividir los mensajes de la capa de transporte en unidades más complejas, denominadas paquetes, y los ensambla al final.
- Debe conocer la topología de la subred y manejar el caso en que las fuente y el destino están en redes distintas.
- Para ello, se encarga de encaminar la información a través de la sub-red, mirando las direcciones del paquete para determinar los métodos de conmutación y enrutamiento, y rutea los paquetes de la fuente al destino a través de ruteadores intermedios.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Debe controlar la congestión de la subred.
- En esta capa es donde trabajan los routers.

En esta capa de red la seguridad se basa en que los encaminadores y la conmutación debe ser adecuada para concatenar redes geográficamente distintas, en el caso de fallar un paquete, por parte de algún pirata informático, su envío de

nodo a nodo se debe buscar la ruta más adecuada para el envío del paquete usando ya sea un circuito virtual o como datagramas.

Capa 2: La capa de enlace de datos: La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, formación y entrega ordenada de tramas y control de flujo. Por lo tanto, su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo.

En la red de la Universidad sus principales funciones son:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agregar una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato predefinido llamado trama o marco. Suelen ser de unos cientos de bytes.
- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.

- Enviar los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Controla la congestión de la red.
- Regula la velocidad de tráfico de datos.
- Controla el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Se encarga de la de secuencia, de enlace lógico y de acceso al medio (soportes físicos de la red).

La seguridad en la capa de enlace de datos puede ser vulnerada por falsa articulación de datos con virus o con caballos de troya, que puede ser agregados en esta capa.

Capa 1: La capa física: La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

En la red de la Universidad sus principales funciones se puede resumir en:

- Definir las características físicas (componentes y conectores mecánicos) y eléctricas (niveles de tensión).
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio. No existe estructura alguna.
- Manejar voltajes y pulsos eléctricos.

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión, pero no la fiabilidad de ésta.

Los elementos que forman la capa física en lo concerniente a la red de la universidad están funcionando en optimo rendimiento en 60%, las dificultades se encuentra en el laboratorio 3, en el cual las instalaciones físicas están en la interperie, aunque en este sitio existen canaletas, los cables no están bien cubiertos. Por el mismo hecho de tener reducido el espacio físico para la distribución de las computadoras debería estar mejor organizada.

Para tener una mejor seguridad de los Equipos informáticos se debería tratar de distribuir mejor a estos equipos y dar un mantenimiento adecuado.

- En los laboratorios 1 y 2 la organización es buena, solo existen algunos puntos de red que no se usan por estar muy cerca de la puerta de la Administración del mismo.
- En el Departamento Financiero, el aspecto de la capa física es bueno para desempeñar las funciones asignadas, y su distribución es excelente por su amplio espacio físico.
- Las secretarias de carrera en el aspecto de organización y distribución de equipos informáticos es buena, lo que hay que mejorar con respecto a seguridad física de equipos, es el **HUB** por estar mal ubicado en el suelo con las conexiones pertenecientes a esta red independiente de secretarias.

Los estándares con respecto al cableado en el T568 A, T568B, y en algunos sitios no se usa ningún estandar.

2.10 Amenazas, Vulnerabilidades que en la actualidad presenta la red informatica de la UTC.

No.	Amenazas y vulnerabilidades	Soluciones
1	En el ciberespacio existen hackers o piratas informáticos que pueden ingresar a los servidores y causar daños a los mismos	Establecer una mecanismo de seguridad para evitar el ingreso de los hackers a los servidores
2	Cuando se trabaja con Internet la información puede venir infectada con virus informático que puede ingresar al servidor ocasionando daños en el sistema operativo y por ende dejando fuera de servicio.	Instalando un antivirus actual en el servidor se evitara que se integre virus informático.
3	La pagina Web de U.T.C. puede ser alterada por los Hackers	Instalar un firewall para proteger de ataques externos.
4	No existe un firewall tipo Hardware y software que evite el ataque de virus y hackers a los servidores.	Instalar un firewall tipo hardware y software para evitar que Virus informático y a los hackers.
5	En caso de instalar un software sin su respectiva licencia la compañía de Microsoft puede realizar auditorias y los equipos que no cumplan con su respectivas licencias serán retirados del centro de computo.	Usar un control mensual de los programas que se encuentran instalados con su respectiva licencia. (Software de Auditoria)
6	No existe un mecanismo de seguridad para proteger a los servidores de ataques internos	Establecer un reglamento interno de seguridad para los operadores y ayudantes del centro de computo
7	Se puede introducir virus informático a través de disquetes	Instalar antivirus actuales en cada una de la computadoras del centro de computo (Crear políticas de actualización)
8	Sin poseer un sistema de seguridad informático apropiado ninguna institución deseara invertir en proyectos informáticos por los riesgos que esta presenta.	Diseñar una propuesta de seguridad para la institución
9	El personal que cumplen con la función de operadores del centro de computo no reciben capacitación relacionada con la seguridad informática por parte de institución	La institución debe preocuparse por capacitar a los operadores en técnicas que tenga que ver con la seguridad informática
10	No existe un manual de funciones para los operadores	Establecer un manual de funciones por parte de las autoridades
11	Las autoridades no reservan un presupuesto para la seguridad informática	La institución debe asignar un presupuesto para la adquisición de equipos relacionados con la seguridad informática.
12	La UTC no cuenta con un cuarto de equipos donde se concentren todos los equipos para una correcta administración y funcionamiento.	Crear un cuarto de equipos a los cuales se ingrese solo el personal de asignado para controlar los elementos activos de la red.
13	Los diferentes departamentos no se encuentran Interconectados entres si por	Concentran las diferentes departamentos para que todos formen una sola red Informática

	una red datos.	utilizando un servidor.
14	Existe un dispositivos "switch" que protege en parte a los servidores	Adquirir un firewall que proteja al 100% a los servidores en forma externa e interna
15	El servidor de Linux posee un Proxy el mismo que funciona como firewall pero no cubre en su totalidad la seguridad externa	Existen los IPTables propios de Linux que activando y desactiva direcciones IP podemos controlar el envió y recepción de información.
16	La necesidad de ampliar la red informática a la hacienda	Por la distancia se debe utilizar una red inalámbrica para controlar el envió y recepción de la información a través del centro de computo.
17	En Internet existe millones de ficheros distribuidos en miles de ordenadores que pueden ser copiados libremente usando Ftp.	Configurar el servidor Ftp para autentificar al usuario, para así pueda a ser uso de servicio.
18	Con Ftp tenemos que traer lo archivos desde el lugar al que estamos conectados hasta nuestro ordenador y después verlos	Con Telnet podemos ver lo ficheros en la pantalla de nuestro ordenador
19	FTP utiliza el puerto 21 que se encuentra abierto cuando utiliza Internet	Lo recomendado sería cerrar todos los puertos y habilitar los necesarios.
20	(Puerto 25) La información de los "mails" que viajan por el Internet no es tan confiable desde el origen hacia el destino.	Con la criptografía se protegen los datos, para que de esta manera no puedan ser descifrada por los hackers.
21	La falta de contraseñas, o el uso de esta con pocos caracteres, es un problema de seguridad	Debe evitarse las contraseñas con pocos caracteres y predefinidas

Tabla 2.40 Amenazas ,vulnerabilidades y soluciones.

CAPITULO III

Propuesta de un sistema de seguridad para la red de datos de la Universidad Técnica de Cotopaxi.

3.1 Necesidades de una seguridad informática de la Universidad Técnica de Cotopaxi.

Las necesidades que a continuación se detallan se obtuvo del análisis de las entrevistas realizadas a las diferentes dependencias de la UTC.

- Establecer un sistema de seguridad en los servidores, para proteger de forma externa e interna del pirateo de información por parte de los famosos Hackers.
- Crear una política de seguridad en el servidor para impedir el uso indebido de juegos, pornografía, chateo.
- Instalar en el servidor principal un Antivirus con tecnología actual, para que en caso de ingresar un virus informático no deje de funcionar el servidor y la red de datos.
- Implantar una política de seguridad para las contraseñas y claves del usuario .
- Controlar el uso de instalación de programas con sus respectivas licencias que posee cada computadora de la Universidad para que en caso de presentarse auditorias externas por parte del empresa Microsoft se lo ejecute sin ninguna dificultad.

- Integrar las computadoras de los diferentes departamentos a la Red de Datos de la Universidad Técnica de Cotopaxi, para brindar los diferentes servicios que presenta la misma.
- Habilitar los puertos de comunicación de la Red únicamente los necesarios .
- Crear un cuarto de equipos para una mejor funcionalidad y administración de la Red .
- Establecer un acta de compromiso para los usuarios de la Red de datos de la Universidad Técnica de Cotopaxi.
- Capacitar frecuentemente el personal encargado de los laboratorios con temas relacionados con la seguridad informática.
- Las autoridades de la Institución deben asignar un presupuesto para equipos tipo Hardware y Software en la seguridad informática.

3.2 Objetivos

Objetivo General

- Proveer información segura y permitida para la red de datos interna y externa de la Universidad Técnica de Cotopaxi.

Objetivos Específicos

- Buscar mecanismos de seguridad que proporcionen protección a la red informática de la Universidad Técnica de Cotopaxi.
- Determinar las políticas de seguridad que se consideren necesarias para los usuarios de la red informática.

- Instalar un sistema de seguridad informático en los servidores.

3.3 Justificación del sistema de seguridad.

El presente trabajo investigativo está basado en la necesidad de un sistema de seguridad informático que beneficiará a la Universidad Técnica de Cotopaxi, la misma que se centrará en los servidores, de la red interna y en el Internet respectivamente, con la implantación de la seguridad se evitará que los hackers o piratas ingresen virus informáticos y datos de dudosa procedencia; además exploren, experimenten y dificulten el buen funcionamiento de los sistemas tecnológicos que existen en la Universidad, de esta manera se conseguirá que la información no sea manipulada y que mantenga alejados a los mismos. La principal vulnerabilidad de los sistemas de la Universidad Técnica de Cotopaxi, es de carecer de mecanismos de control que eviten el uso no autorizado de los recursos informáticos de la red . Con un sistema de seguridad eficiente en la red informática de la Universidad Técnica de Cotopaxi, se logrará que gente no autorizada ingrese a la red de computadoras y causen daños a la misma.

3.4 Políticas de seguridad para los usuarios de la red de datos de la Universidad Técnica de Cotopaxi.

El estudio desarrollado en el capítulo II, nos induce a buscar alternativas de seguridad; para lo cual se debe establecer políticas, acordes a las necesidades de la Institución.

3.4.1 Autorizaciones

3.4.1.1 Autorización de acceso

La autorización para el acceso a los servidores de datos debe ser gestionada ante la Administración de Sistemas y deberá contar con la autorización expresa de la misma, después que la autorización es otorgada, la Administración pondrá los recursos a disposición del usuario o investigador.

3.4.1.2 Identificaciones de usuarios

Todos los usuarios que acceden a recursos informáticos de la Red UTC requieren de una única e intransferible identidad, normalmente un username para una persona, y un nombre de máquina para una computadora personal. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la Red UTC.
La Administración proporcionará este identificador como parte del proceso de autorización. Los identificadores concedidos expiran cuando el usuario solicita expresamente a la Administración la cancelación de acceso para dicho identificador, o cuando se compruebe un uso indebido. Será obligación de cada Jefe/Director informar la baja de los usuarios de su área que cesen en su función para que sea dado de baja el permiso de acceso existente.

La desconexión de un dispositivo de su puerto autorizado y conexión a otro puerto de la red es una violación de este código. Los dispositivos y computadoras móviles deben ser autorizadas para usar cualquier puerto de la red.

Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de la Red UTC están sujetas a sanciones disciplinarias.

3.4.1.3 Las contraseñas

Los usuarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos de Red UTC con las contraseñas confidenciales que les fueron asignadas. Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios, deben expirar periódicamente y poseer una longitud mínima.

Todas las acciones realizadas bajo el auspicio de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular.

Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a la Administración.

3.4.2 Administración y control

3.4.2.1 Administración de Recursos Informáticos

Las funciones de administración incluyen la administración de los Servidores de Internet, Bases de Datos implementadas o que se implementaran, supervisión del tráfico de la red, la seguridad de accesos a la red y servicios como Dominios NT, los firewalls, proxys y/o la instalación de nuevos enlaces, hardware de conectividad tales como hubs, routers, sniffers, o analizadores de protocolos; la presencia de tal software o hardware no autorizado por la Administración en la red UTC es una seria violación de esta política. La Administración puede quitar de la red y confiscar sin advertencia cualquier dispositivo sospechoso de violación de esta política.

Ninguno de los Departamentos podrá conectarse a Internet, sin el consentimiento y supervisión previos de la Administración, a fin de no alterar o interferir con dispositivos ya instalados propios de la Red y/o ajenos a ella.

Será responsabilidad de los encargados orientar, coordinar y proponer contenidos para el website de la red UTC, en el marco de las propuestas de la red universitaria, y de las necesidades e inquietudes propias de la Universidad.

3.4.2.2 La propiedad de los Datos

De acuerdo a las Políticas de Seguridad informática se define que los roles de ***Propietarios de los Datos*** recaen en los Jefes/Directores de cada Departamento de la Universidad, quienes son los responsables máximos de la información en cada una de las dependencias. Las tareas operativas relacionadas con este rol pueden ser delegadas, previa notificación fehaciente a la Administración.

Ningún Departamento podrá incluir en sus páginas web, información que no sea de producción genuina de ese sector (en el caso que lo hubiera). Quienes necesiten difundir datos generados en otras dependencias, podrán incluir vínculos (links) hacia las pantallas de origen de los mismos. En cada página será obligatorio incluir el nombre de los responsables de las mismas (operador y/o responsable académico, en este último caso, principalmente el responsable del área) y la fecha de la última actualización.

Los datos de la Red Administrativa serán resguardados de acuerdo a las exigencias de confidencialidad exigidas al empleado por las normas legales de la Administración Pública.

3.4.2.3 El website oficial

El website http://www.utc.edu.ec/ es el sitio oficial de la Universidad. Ninguna página de áreas/dependencias/instituciones que guarden relación de dependencia institucional y/o académica con ésta podrá ser considerada con el título de "página oficial" si está en otro dominio electrónico que sea distinto a utc.edu.ec.

Tampoco se podrá usar el "nombre y/o logo de la Universidad " fuera de este ámbito, o de aquellos que la institución determine oficialmente.

3.4.2.4 Desarrollos de proyectos informáticos de investigación.

Toda actividad desarrollarse en el futuro y que involucre el uso de Recursos Informáticos (Hardware o software) de la UTC; que sirvan como proyectos investigativos que sean de beneficios a la misma, los cuales deberán estar aprobados por el consejo Universitario en un plazo máximo de 15 días, el producto de la investigación, será de propiedad de la Universidad quienes autorizarán el uso del mismo.

3.4.3 Dispositivos de red

3.4.3.1 Autorización

Todo dispositivo que se desee conectar a la red debe ser autorizado por la administración. No pueden conectarse computadoras servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

3.4.3.2 Los Protocolos autorizados

La Red UTC utiliza la conexión de protocolos TCP/IP para permitir la conectividad de la red al servicio de Internet. Se prohíbe la utilización de protocolos alternativos de red como IPX o NetBEUI sin la autorización expresa de la Administración.

3.4.3.3 Servicios de la red

La autorización para ofrecer servicios de red debe obtenerse de la Administración de la Red UTC antes de que tales servicios se ofrezcan. Ejemplo de servicios prohibidos son los servidores FTP, servidores de e-mail, servidores de noticias, servidores WEB, servidores de archivos, etc.

3.4.3.4 Conexiones de computadoras a la red

En caso de que se obtenga la autorización apropiada, la Administración permitirá a una computadora personal la conexión a la red. Esta autorización sólo es para la computadora y para ser usada como un cliente normal en la red.

El uso de la computadoras como gateways o routers a otra red o como servidor de acceso remoto por módem esta prohibido sin la autorización expresa de la Administración.

3.4.4 Utilización de computadoras personales

El usuario es responsable del cuidado del hardware suministrado. La Administración es responsable por la coordinación de reparación de las computadoras de los usuarios que han sido adquiridas a través de la Universidad y/o mediante donaciones a dependencias centralizadas. Las reparaciones y/o ampliaciones de estos equipos no pueden ser hechas o contratadas por el usuario. El mantenimiento y reparación del equipamiento adquirido de cualquier otro modo, queda a cargo del responsable de la compra.

Aquellos equipos o sistemas que proponen un riesgo al funcionamiento razonable de la red u otro recurso informático de la Red UTC serán desconectados sin aviso previo por la Administración.

3.4.4.1 El software

El usuario no instalará ningún tipo de software (estandarizado o no, shareware, freeware, demo, de dominio público, etc.) en los equipos servidores sin la aprobación expresa de la Administración. Toda instalación será considerada como falta plausible de sanción disciplinaria. Dicha aprobación se solicitará por escrito.

3.4.4.2 El acceso

La Administración puede acceder e inspeccionar todos los dispositivos informáticos conectados o no a la red, para los propósitos de resolución de problemas o para investigar violaciones a las políticas de la Red UTC, toda vez que lo necesite y sin previo trámite. Dicho libre acceso debe preverse especialmente en períodos de receso parcial de la actividad académica, por razones de mantenimiento correctivo y o preventivo.

3.4.4.3 El Correo electrónico

Todas los Departamentos que guarden relación académico-institucional con la Universidad deberán poseer una cuenta de correo electrónico, para incorporarse a las listas de correo pertinentes, a fin de facilitar la comunicación y conectividad

institucional. Quienes no posean una, podrán solicitarla a la Administración. La consulta de esta cuenta será de obligación diaria.

3.4.4.4 Las Licencias de Software

Los dispositivos y sistemas conectados a la Red UTC deben, en todo momento, estar por completo en conformidad con las licencias de software y hardware que fueron adquiridos. Al ingresar a la Red UTC, el usuario acepta cualquier responsabilidad legal que surja de una violación a estas políticas.

3.4.4.5 El Hacking

Toda tarea de utilización de técnicas y/o herramientas de hacking desde y hacia la Institución son consideradas como faltas graves y se tomarán las medidas consecuentes con cada caso. Entre las técnicas de Hacking mencionamos:

1. La ingeniería inversa, cracking o desencripción de contraseñas.
2. El escaneo de puertos de TCP/IP.
3. La sustitución de usuarios o Hacking.
4. La sustitución de paquetes IP, también conocida como IP spoofing

5.La utilización de analizadores de protocolos o scanners de tráfico de red.

6.Grabadoras de teclas o Key Loggers

7.Hardware para ataques de Tempesting.

8.Herramientas de denegación de servicio.

9.La ingeniería social.

3.4.4.6 Los Antivirus

Todas las computadoras, y en especial aquellas en donde se instalaron cuentas de correo electrónico, deberán tener instalados antivirus activos, y correrlos periódicamente para controlar todo el equipo. En caso de detectar alguna infección, será obligatorio informar de inmediato a la Administración, para evitar y controlar su posible diseminación.

3.4.4.7 El Resguardo de la información

Cada responsable de área deberá instrumentar políticas permanentes de resguardo de la información de su sector, estipulando mecanismos y tiempos para la realización del backup correspondiente, y controlando el cumplimiento de este procedimiento.

3.4.4.8 El uso de recursos públicos

Las computadoras de uso masivo instaladas en las cátedras, gabinetes, etc. son elementos de uso y responsabilidad compartida. Será considerada falta grave el acceso a los programas y archivos instalados en ellas, el cambio de configuraciones del equipo, la instalación de otros utilitarios de uso personal, el uso de diskettes que no hayan sido autorizados por el Responsable del Sector donde se encuentre el equipo, o que no hayan sido verificados para impedir la trasmisión de virus, y el acceso a casillas de correo y/o archivos personales.

Será obligación de los usuarios el denunciar de inmediato cualquier anomalía que detecten, a fin de preservar estos recursos comunitarios.

3.4.5 Los usos prohibidos

La Red UTC considera el abuso en la utilización de recursos informáticos como una falta grave. A continuación detallamos una lista pequeña de algunos usos de recursos informáticos que se prohíben en la Universidad.

1. Utilización de cualquier recurso informático de la Red UTC para los propósitos comerciales personales o para ganancia personal.

2.La inclusión de patrocinantes en las páginas web de la Red UTC está sujeta a disposiciones oficiales en el ámbito de la Universidad, y a las regulaciones jurídico-contables de la Institucion para convenios, tanto sea a cambio de dinero, materiales y/o servicios. La Administración podrán excluir o no incluir aquellas páginas que no se adecuen a la presente Normativa.

3.Utilización de cualquier recurso informático de la Red UTC para guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general., ni para ninguna actividad no académica, de acuerdo a lo que se estipula para la red Red UTC.

4. Conexiones desautorizadas a la Red UTC.

5.Instalación de hardware y/o software sin la autorización apropiada de la Administración en los equipos que requieren esta autorización.

6.Permitir a personal externo acceder a recursos informáticos de la Red UTC sin la autorización de la Administración.

7.Privar o intentar privar a otros usuarios la utilización y/o acceso a recursos informáticos de la Red UTC.

8. Intentar penetrar la seguridad de cualquier comunicación de la red de computadoras o sistema de la computadoras.
9. El uso desautorizado de cuentas de la computadora u otras formas de acceso a Recursos informáticos de la Red UTC.
10. Utilización de identificadores de usuarios ajenos.
11. Inspeccionar, modificar, o copiar programas o datos sin la autorización de su dueño o que atenten contra las leyes vigentes de legalidad del software y/o propiedad intelectual.
12. Utilizar cualquier correo electrónico o sistema del mensajería, ajenos a la Red UTC o no, para enviar contenido abusivo, ofensivo, obsceno, o saturar los canales de comunicaciones, o el envío "cadenas de cartas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos.
13. Alterar el software o la configuración del hardware de cualquier computadora o agregar cualquier dispositivo o sistema a la red sin el permiso de la Administración.
14. La utilización de software comercial ilegalmente copiado, ya sea texto, imágenes gráficas, o grabaciones de audio o video.
15. Utilización de la Red UTC para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.
16. Posesión o utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la Red UTC.

17. Las computadoras instaladas en una red institucional, y el uso que de ellas se haga, podrán ser monitoreados, tanto a nivel nacional como internacional, pudiendo ser identificadas fehacientemente.

3.4.6 Consideraciones generales de seguridad

La Administración se reserva el derecho de quitar usuarios o dispositivos de la red de computadoras de la Universidad sin notificación previa si se descubre o se sospecha cualquier vulnerabilidad en la seguridad.

Los usuarios son responsables de ayudar a mantener la seguridad de la Red UTC siguiendo los procedimientos de seguridad establecidos.

La presente política es solo un marco de referencia para los usuarios y en virtud de la imposibilidad de enumerar toda prohibición existente, dejamos aquí constancia de que todo aquello que no se encuentra expresamente permitido se encuentra prohibido.

Todas las disposiciones incluidas en este documento son aplicables por igual a las instalaciones y usos de la toda la Red de la Universidad.

El uso incorrecto del equipamiento informático de la Red UTC compromete directamente a la Administración y al área y/o responsable del lugar en que se encuentre instalado, por lo que cada área y/o titular será responsable por los daños y perjuicios técnicos y/o legales que se generen por esta causa, aún cuando se hayan utilizado servicios de uso público irrestricto, como Yahoo, Hotmail, Uolmail, etc..., tanto en sus

servicios de correo, como de foros, chat y otros. La detección de este uso indebido podrá ocasionar la inhabilitación temporal o definitiva del sistema para el usuario responsable, a criterio de la Universidad, en relación directa con la gravedad del perjuicio ocasionado, y en el marco de las Regulaciones Universitarias.

Todo lo referido a sanciones por la trasgresión de estas normativas, se enmarca en las Reglamentaciones y Procedimientos ético-legales vigentes en el ámbito de la Red UTC, y que rigen tanto para docentes, investigadores, no docentes y alumnos, según corresponda.

3.4.7 Acta de compromiso para los usuarios de la red UTC

Toda Institución debe tener en cuenta que no únicamente la seguridad se realiza incorporando cada vez más y más equipos informáticos relacionados a la seguridad. Sino se debe hacer conciencia, promocionando las políticas de seguridad, que no solamente el Administrador es el único responsable de la seguridad de la red de la Universidad. Sino todos y cada uno de los que conforman el grupo de personas que manejan la red, para un mejor desempeño y atención a los usuarios de la red, lo que conlleva a establecer normas para los usuarios de la red y a la vez documentar en lo que se haya plasmado en un Acta de compromiso para tener mayor fuerza. El Acta de compromiso que los usuarios de la red deberán leer y luego firmar para constancia.

Los siguientes items aseveran la integridad de los recursos Informáticos de la Red UTC.

1. El responsable se compromete a guardar su clave secreta, y no divulgarla a otras personas extrañas a la labor desempeñada
2. Es responsabilidad de Usuario la utilización adecuada de cualquier recurso informático de la Red UTC para los propósitos educativos o/y académicos únicamente.
3. Esta prohibida la utilización de cualquier recurso informático de la Red UTC para guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general., ni para ninguna actividad no académica, de acuerdo a lo que se estipula para la Red UTC.
4. No se debe manipular las conexiones de la Red UTC.
5. Esta prohibido la Instalación de hardware y/o software sin la autorización apropiada de la Administración en los equipos que requieren esta autorización.
6. Será una falta permitir a personal externo acceder a recursos informáticos de la Red UTC sin la autorización de la Administración.
7. Es ilegal privar o intentar privar a otros usuarios la utilización y/o acceso a recursos informáticos de la Red UTC.

8. Intentar penetrar la seguridad de cualquier comunicación de la red de computadoras o sistema de la computadoras llevara a sanciones por parte del Administrador.
9. No esta permitido crear cuentas sin previa autorización al Administrador de la Red u otras formas de acceso a Recursos informáticos de la Red UTC.
10. Esta prohibida la utilización de identificadores de usuarios ajenos.
11. Crear, utilizar o distribuir los programas que puedan dañar los datos, archivos, aplicaciones, funcionamientos del sistema, o funcionamientos de la red como: virus, troyanos, key loggers etc, no esta permitido.
12. El Capturar / desencriptar, contraseñas y/o protocolos de comunicaciones es sancionado por la Administración.
13. No es permitido inspeccionar, modificar, o copiar programas o datos sin la autorización de su dueño o que atenten contra las leyes vigentes de legalidad del software y/o propiedad intelectual.
14. Utilizar cualquier correo electrónico o sistema del mensajería, ajenos a la Red UTC o no, para enviar contenido abusivo, ofensivo, obsceno, o saturar los canales de comunicaciones, o el envío "cadenas de cartas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos, es una falta.

15. Alterar el software o la configuración del hardware de cualquier computadora o agregar cualquier dispositivo o sistema a la red sin el permiso de la Administración.
16. La utilización de software comercial ilegalmente copiado, ya sea texto, imágenes gráficas, o grabaciones de audio o video.
17. Esta prohibido la posesión o utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la Red UTC.
18. Las computadoras instaladas en una red institucional, y el uso que de ellas se haga, podrán ser monitoreados, tanto a nivel nacional como internacional, pudiendo ser identificadas fehacientemente. Está prohibido su uso para ingresar a páginas de contenido erótico, pornográfico, de violencia, y cualquier otro tipo de información no académica que sea lesiva a la finalidad de la red.

ACTA DE COMPROMISO

Responsable:.....

Departamento:.....

_____

Firma Responsable

3.5 Estudio de factibilidad para el sistema de seguridad

El análisis del dominio a estudio desarrollado en el capitulo anterior, y las necesidades de seguridad Informática de la Universidad, que se traducen en políticas descritas en el literal 3.1del capítulo III, nos induce a buscar las alternativas de seguridad; tanto para nivel de software como de hardware, los mismos que ayudarán a mejorar la seguridad en la red de la Universidad.

Es imprescindible la búsqueda de un sistema de seguridad para el servidor de Internet de la red de datos de la Universidad Técnica de Cotopaxi (Linux Red Hat), y el servidor del departamento financiero (Windows 2000 Server) para un mejor estudio de factibilidad, se han realizado las siguientes consideraciones.

- Firewall para Linux Red Hat
- Firewall para Windows
- Firewall Hardware

3.5.1 Firewall para Linux Red Hat

3.5.1.1 Factibilidad Operativa para los Firewalls de Linux

El objetivo de la factibilidad operativa es de definir los parámetros básicos como ventajas y beneficios con respecto a la seguridad de los Firewall Linux. A continuación se describen Firewalls para servidor Linux:

3.5.1.1.1 ITS Linux Firewall (software)

ITS es una Infraestructura de Telecomunicaciones seguras. Las enormes oportunidades y el potencial puede fácilmente distraer de los peligros y riesgos que resultan del uso de las nuevas tecnologías. Los "hackers" avanzados penetran en las intranets debido a varios motivos: para robar o manipular información, bloquear recursos compartidos, cometer actos ilegales con la identidad de sus víctimas o simplemente causar una situación de confusión masiva.

Estos escenarios pueden y deben ser evitados con una sencilla medida. El ITS Linux Firewall prevee una protección eficaz para su Red.

El ITS Linux Firewall es un servicio de seguridad, fiable y eficaz, para su empresa. Siendo un componente central en la seguridad global, el ITS Linux Firewall controla, analiza y registra en archivos toda transferencia de datos, por consiguiente provee un nivel de seguridad máxima y protege contra ataques antes de que causen daños irreparables.

El ITS Linux Firewall combina los altos estándares de seguridad de soluciones Hardware con la flexibilidad de un software-Firewall.

Siendo un CD-ROM de sólo lectura, el Firewall no se instala en el disco duro, sino que se arranca directamente del CD-ROM.

Las ventajas principales:

- El software (del Firewall) no puede ser manipulado, un factor muy importante para una seguridad adicional.
- El disco de Configuración está creado con el Sistema de Administración "Firewall". Esta interfaz "User-friendly" hace posible una administración y configuración cómoda de un número ilimitado de ITS Linux Firewall. Es verdaderamente un concepto que incorpora todas las ventajas.
- El ITS Linux Firewall combina funcionalidades de fácil comprensión, con un esfuerzo mínimo para su implementación y administración.
- Red de seguridad interna y externa: Dependiendo de sus registros, El ITS Linux Firewall protege su Red contra el acceso externo o define los límites para el propio personal de la empresa. Esto incluye una implementación, configuración y administración muy sencilla. El Sistema de Administración "Firewall" minimiza el tiempo empleado en estos trabajos y facilita de forma más rápida la disponibilidad de su seguridad.

- El Filtro de Contenido protege contra contenidos no deseados: El ITS Linux Firewall ofrece la posibilidad adicional de filtrar los contenidos de páginas HTML de forma eficaz. Los contenidos no deseados son identificados y bloqueados y sólo los elementos de lenguaje son transferidos.
- Proxy y Protección: El Proxy le ayuda a agilizar sus operaciones en la WWW. El Proxy salva las páginas que se han visto previamente y las recarga de forma más rápida cuando éstas son nuevamente solicitadas. Además, el Proxy bloquea el acceso a páginas que no son apropiadas y/o autorizadas.
- El Sistema de Registro hace que la transferencia de datos sea transparente: Su Red empresarial no sólo está expuesta a peligros externos. Muchos ataques a su información vienen de fuentes internas. El ITS Linux Firewall registra continuamente la transferencia de datos internos y externos y, por consiguiente, facilita la búsqueda de pistas que indiquen su mal uso.
- La tecnología "código abierto" genera soluciones individuales: Su creatividad no se ve limitada. Las ventajas de una solución "código abierto" no están limitadas

solamente a un ahorro económico. El código fuente, el cuál se provee junto con la solución, le permite llevar a cabo una completa adaptación a sus herramientas.

- Mantenimiento - Mejoramiento Sistemático: El mantenimiento activo en concepto de seguridad garantiza un máximo grado de seguridad. El mantenimiento ITS es del tipo activo que cumple con todos los requerimientos IT y está adaptado para el uso de soluciones de Linux a nivel empresarial. Esto incluye un mantenimiento garantizado y otros servicios que aseguran permanente y convenientemente su uso. Recibirá regularmente todas las actualizaciones. La asistencia y documentación detallada es básica para asegurar la calidad en la instalación de todas las actualizaciones.

3.5.1.1.2 Firewall Iptables de Red Hat (Software)

El cortafuego que posee Ret Hat, para interactuar con la red es iptables, que se incorpora a la familia Linux desde la versión 7.3.

Los Iptables son básicamente comandos del sistema operativo Linux, con una interfase de texto para interactuar con el usuario. Por consiguiente la reglas que se establecen dan el nivel de seguridad que el Administrador ejecuta.

Los iptables usan métodos de filtrado de paquetes usando cadenas o reglas que operan con el kernel de Linux para decidir no sólo qué paquetes se permite entrar o salir, sino también qué hacer con los paquetes que cumplen determinadas reglas, donde *iptables* ofrece un método mucho más extensible de filtrado de paquetes, proporcionando al administrador un nivel de control mucho más refinado sin tener que aumentar la complejidad del sistema entero.

- Bajo *iptables*, cada paquete filtrado se procesa únicamente usando las reglas de una cadena, en lugar de hacerse con múltiples. Es decir, un paquete FORWARD.
- Cuando especificamos las interfaces de red que vamos a usar en una regla, deberemos utilizar sólo interfaces de entrada (opción -i) con cadenas INPUT o FORWARD y las de salida (opción -o) con cadenas FORWARD o OUTPUT. Esto es necesario debido al hecho de que las cadenas OUTPUT no se utilizan más con las interfaces de entrada, y las cadenas INPUT no son vistas por los paquetes que se mueven hacia las interfaces de salida.

3.5.1.1.3 Firewall SecurePoint (Software)

Securepoint Firewall es una solución de firewall para Linux muy segura para proteger su pasarela a Internet. Securepoint se

puede usar también en instalaciones con otros firewalls, y para proteger redes locales interconectadas. Securepoint es un software completo de alto rendimiento con un sistema operacional basado en el núcleo seguro de Linux.

La última versión de Securepoint trae renovado el control del interface de red, nuevas posibilidades de configuración mediante el programa config.fw que incluye copia de seguridad de la configuración, reestablecimiento de antiguas configuraciones, aplicación de parches, y envío de configuración al sistema de mail on-line del departamento de soporte del producto.

Para cada una de sus funciones entre algunas contamos con las siguientes:

- Existe soporte gratuito en línea
- La interface es gráfica y amigable
- Existen paquetes adicionales que se pueden cargar únicamente configurando opciones de usuario como son:
    - Firewall
    - VirusWall (http, ftp, smpt, virus scanner)

- Dentro del sistema de archivos que maneja son:
  - Ext2
  - Ext3 (journaling file system)
  - Reiserfs (journaling file system)
- El Securepoint Security Manager es el programa de configuración del Securepoint del Firewall & VPN en el servidor. La versión de WindowsTM del Securepoint Security Manager contiene en el directorio del cliente en el CDROM.
- En la consola del cortafuego, los usuarios de Linux experimentados pueden hacer las escenas de la configuración más allá de la consola de Securepoint o integra los servicios adicionales. Se puede establecer contraseñas para las consolas.
- Las reglas del cortafuego: Todos los usuarios que comunican por el cortafuego deben adherir automáticamente a su política de seguridad. Si ellos no hacen, Securepoint lo bloquea. Para configurar las reglas, seleccione Modifique-> las Reglas. Usted determina la dirección a través de la cual quiere una comunicación.

- La topología: Se puede conseguir una apreciación global corta de su red, en un forma grafica.

3.5.1.2 Factibilidad Técnica para los Firewalls de Linux

La factibilidad técnica es el método para precisar las características técnicas que son necesarios para la selección del Firewall software de Linux, para lo cual presentamos las comparaciones de los Firewalls software Linux en la Tabla 3.1.

COMPARACIONES DE SOFWARE FIREWALL LINUX			
Firewall / Características	SecurePoint[1]	ITS[2]	Iptables[3]
Sistema Operativo	Linux	Unix/Linux	Linux
Interface	GUI	GUI	GUI
Escalabilidad	✓	✓	✓
Facilidad en configuraciones	✓	✓	✓
Restricciones de Bloqueo	✓	✓	✓
Enmascaramiento de conexiones	✓	✓	
Puertos	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3
Creación de reglas de restricción	✓		
Especificación de IP	✓		
Licencia	Libre	$ 99.00	Libre
Mínimo Requerimiento	64 MB RAM, 10MB espacio en disco	64MB RAM, 10MB espacio en disco	32MB RAM, 10MB espacio en disco
Protocolo	TCP/IP, NetBeui	TCP/IP	TCP/IP
Herramientas de monitoreo	Supervisa el trafico contando las entradas		
Experiencia	Media	Media	Baja
Conocimiento	Fácil		
Documentación	Alta	Media	Media
VPN	✓	✓	
Capas del modelo Osi y TCP/IP	- Capa de transporte - Capa de red	- Capa de transporte - Capa de red	- Capa de transporte - Capa de red

Tabla 3.1 Comparaciones de software Firewall Linux

3.5.1.3 Factibilidad Económica para los Firewalls de Linux

La factibilidad económica es un factor importante para tomar decisiones de cualquier Institución. Para esto se necesita realizar

[1] www.secuerepoint.cc/products
[2] http://www.its-intl.com/es/services/conectividad/seguridad/firewall.html
[3] http://www.linuxguruz.org/iptables/.

comparaciones de los beneficios de los Firewall Linux, pues la mayor parte de software de Linux son de código abierto, pero si se requiere con aplicaciones comerciales más avanzadas tienen un costo, porque algunas organizaciones añaden código a las aplicaciones. Los valores asignados en cada beneficio en la tabla 3.2 son producto del estudio anterior en todas sus etapas, los cuales contienen una calificación con un rango de 1-10:

Firewall / Beneficios	SecurePoint	ITS	Iptables
Seguridad	8	9	9
Fiabilidad	10	10	10
Escalabilidad	8	8	9
Facilidad de configuración	8	10	9
Soporte en linea	7	9	9
Conocimiento	6	9	9
Funcionabilidad	9	8	10
Documentación	7	6	9
Requerimiento adicional	1	2	0

Tabla 3.2 Beneficios de los Firewalls software para Linux

Los valores de la tabla 3.2 entrega una curva característica para los firewall con respecto a los beneficios.

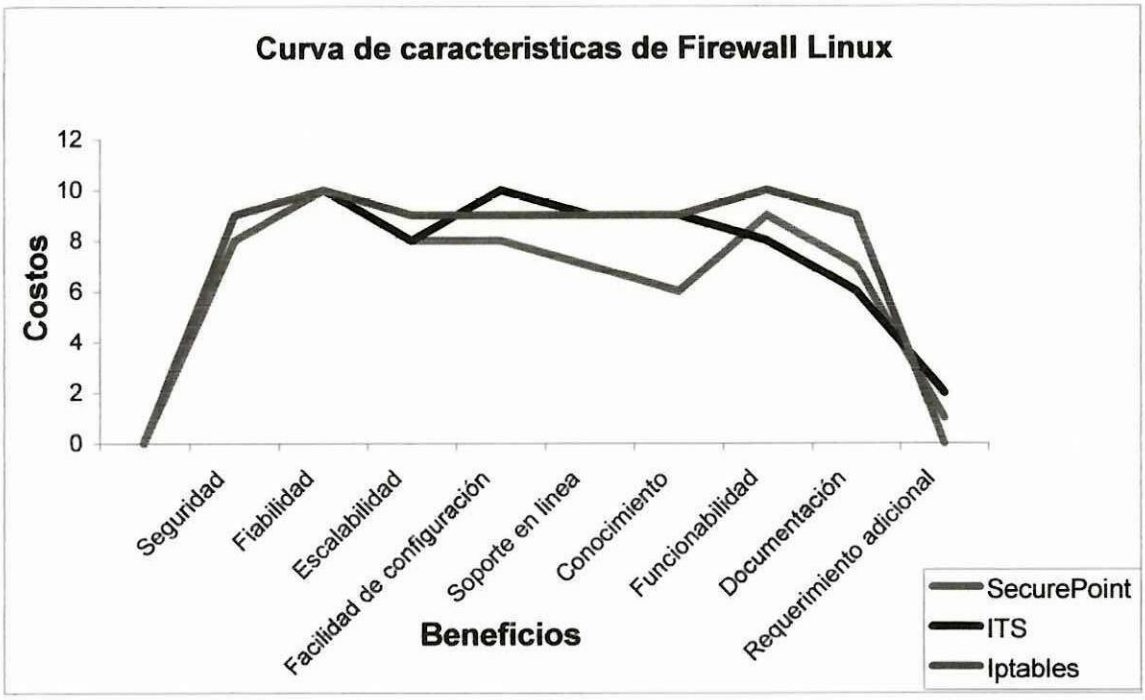


Gráfico 3.1 Curva característica de Firewalls Linux

El gráfico 3.1 demuestra que los Firewalls son eficientes. En donde el Firewall IpTables de propio de Red Hat es el más regular en la relación costo beneficio, porque posee ventaja respecto a los demás Firewall.

3.5.1.4 Selección de una alternativa de seguridad informática para los firewall Linux.

Un estudio de factibilidad representa gráficamente los beneficios que acarreará la puesta en marcha del sistema, por tal efecto se llega a la conclusión de que el firewall Linux Iptables es la mejor opción para las necesidades encontradas en la Universidad. Por los siguientes aspectos:

- Seguridad: con una mejor seguridad para los puertos(ftp, telnet, http, smtp).
- Fiabilidad: los recursos que la Institución posee, son fiables con la seguridad que brinda el Iptables.
- Escalabilidad: los productos de Iptables poseen versiones en escala.
- Facilidad de configuración: su interfase gráfica facilita la configuración e instalación.
- Soporte en línea: lo realiza muy eficazmente, proporcionado por Red Hat en www.redhat.es/
- Conocimiento: Los Iptables consta con comandos en ingles que se tornan fáciles para la asimilación.
- Funcionabilidad: el funcionamiento y puesta en marcha es muy eficaz para las necesidades de la Universidad.
- Documentación: existen manuales del software fáciles de entender en la dirección: http://www.redhat.es/soport.
- Requerimiento adicional: no necesita adicionar a la red ningún software pues tan solo el Iptables que viene incorporado en el mismo sistema operativo.

3.5.1.4.1 Conclusiones

Del análisis de los Firewall Linux SecurePiont, ITS e Iptables. Se ha obtenido que Iptables proporciona mayores ventajas con relación con los demás. Por lo siguiente:

- En la factibilidad operativa sobresale el software Iptables por tener mejores beneficios y ventajas.
- En la factibilidad técnica se realizo comparaciones de los tres diferentes firewall, resultando mas viable el Firewall Iptables por tener mejores características técnicas.
- Iptables ofrece un método mucho más extensible de filtrado de paquetes, proporcionando al administrador un nivel de control mucho más refinado sin tener que aumentar la complejidad del sistema.
- Posee una flexibilidad al crear reglas que proporcionan una estabilidad al nivel seguridad (baja, media, alta) que el administrador desee.
- Iptables viene incorporado dentro de los instaladores del Red Hat lo cual lo hace imprescindible, puesto que los Firewall gráficos utilizan Iptables en su interior.
- El costo-beneficio de los Firewall se analizó en la factibilidad económica, en donde, Iptables es el que posee una mejor relación

costo-beneficio. Según la valoración que se asignó a cada beneficio acorde al análisis de sus características.

- Por consiguiente, el software Iptables es el mejor en seguridad y beneficios que se ajusta a las necesidades de la Universidad.

3.5.1.4.2 Recomendaciones

Se debe tomar en consideración lo siguiente:

- Para aumentar las facilidades de Firewall Iptables, se debe adquirir un software gráfico cuyo costo adicional de la empresa proveedora de $100,00, el cual solamente evita escribir tanto código. Sin embargo el Iptables es libre es acorde a las necesidades de la Universidad.
- Posee una interfase de texto, para su elaboración se debe crear o editar el código y demás conocer algunos comandos para poder implementarse.
- La ejecución de los comando Iptables incluidos en un scrips (archivo de texto), se debe hacerse mediante instrucciones propias de Linux para activar este servicio, los cuales evitan volver a escribir los comandos cada vez que se inicia el servidor.
- Los sistemas de seguridad son útiles para mantener fiables los datos a través de la red. Pero no es útil para actuar con personas

que permanentemente intentan vulnerar la seguridad. Para lo cual solo debe haber una buena actitud.

3.5.2 Firewall Windows 2000 Server

3.5.2.1 Factibilidad Operativa para los Firewalls Windows 2000 Server

Este estudio supone analizar tres alternativas Firewall con las limitantes que se presentarían para ello. Tienen singular importancia por una parte, evaluar la real disponibilidad de recursos software, para llevar adelante el proyecto.

A continuación se mencionan los Firewalls para Windows 2000 Server:

3.5.2.1.1 Firewall Outpost.

Outpost el Firewall personal es el software más avanzado del mundo con un notable prestigio en la seguridad. El diseño de la interfase permite que el administrador de red pueda interactuar con las diferentes pantallas que presenta el Firewall. Para usar Outpost no es necesario tener conocimientos sobre el funcionamiento interno de Windows 2000 Server, lo que se debe conocer es las ventajas que posee el Firewall que a continuación se describen.

- El sistema es compatible con todas las versiones de Windows 95/98/2000/ME/NT y XP.
- La interfase para la instalación y configuración se presenta de modo gráfico lo que facilita la instalación del Firewall, puesto que se presenta en el idioma Español, además el servidor no es interrumpido durante este proceso.

- Pueden usarse muchas configuraciones para restringir el acceso de la red, a su computadora y a sus aplicaciones. puede especificar los protocolos aceptables, puertos y direcciones de acceso (entrante o saliente) para cada uno de estas aplicaciones.
- Bloquea o restringe información que se envía a su computadora.
- Advierte de un ataque a su computadora de cualquier otra computadora y al instante previene el acceso.
- Puede impedirles a sus niños acceder los sitios no deseados del Internet (el sexo, los juegos, y otras).
- Pueda proteger sus información mediante una contraseña.
- Por ejemplo, aparece un mensaje de advertencia cuando alguien se conecta a su PC o cuando algún spyware en su computadora intenta enviar su información personal encima de la Internet.
- También puede crear reglas para la red basándose en las direcciones IP particulares.
- Puede conseguir un informe de la historia de la actividad de cada aplicación o cada conexión a su computadora, si permitió y bloqueó.

3.5.2.1.2 Firewall Kerio

Kerio es un Firewall Personal de fácil instalación y configuración es un sistema diseñado por proteger a una computadora personal. La interfase se presenta para el administrador en el idioma Inglés.

El Firewall KERIO presenta varias ventajas entre ellas tenemos:

- El sistema es compatible con todas las versiones de Windows 98 / NT 4.0 / 2000 / XP.
- El usuario / administrador especifica las reglas que se filtran, permitiendo o impidiendo el acceso de un grupo de direcciones de IP (en varias computadoras dentro de una red local). Un grupo puede contener cualquier número de direcciones de IP, las cuales dirigen rangos o subnets.
- El grupo de dirección personalizado puede definirse en la ventana de Configuración del Firewall.
- Si una computadora intenta comunicarse o alguien quiere establecer una conexión externa, el Firewall Personal detiene la demanda y despliega una ventana de diálogo que pregunta si usted quiere permitir o negar tal comunicación.
- Toda la comunicación se niega explícitamente por las reglas de filtración existentes.
- Una regla de filtración se crea automáticamente permitido o negando el acceso. Esto puede usarse en la configuración inicial de Cortafuego Personal.

- El Firewall Personal KERIO puede cambiarse a un modo especial para las entradas de Internet. Esto puede hacerse en la ventana de Configuración de Cortafuego (después de apretar el botón Avanzado).

3.5.2.1.3 Firewall Tiny (Sandbox)

Tiny (Sandbox) Firewall personal es un sistema diseñado para proteger su información de los hackers o piratas informáticos. Después de su fase de configuración permite la interacción con el administrador en el idioma Inglés.

El Firewall Tiny (Sandbox) posee varias ventajas entre ellas tenemos:

- La Sandbox es la tecnología del seguridad que protege los puestos de trabajo y redes contra los ataques de cualquier tipo (ActiveX, Java, VBS el y otro código ejecutable) de la Internet, correo electrónico o por cualquier otros medios.
- Con la tecnología del sandboxing usted puede crear un ambiente cerrado a los recursos de su computadora. Todas las acciones de acceso y de recursos, se bloquean sólo cuando existen acciones sospechosas.
- Si el Agente de Sandbox no protege su computadora, los procesos hostiles podrían acceder a todos los archivos y recursos que están disponible en su computadora.

- Mediante un proceso se puede acceder a los datos y archivos de su computadora o red los mismos que son enviados a cualquier computadora vía Internet. Un proceso podría filtrarse, manipular, falsificar la información enviada o recibida. Sandbox evita que su información sea tergiversada.
- Un usuario en la Internet puede ingresar a su red del área local y efectuar acciones malévolas, destructivas. Sandbox evita el acceso a su ordenador.

3.5.2.2 Factibilidad Técnica para el firewall Windows 2000 Server

La Universidad cuenta con una gran tecnología, ya sea en software o hardware, además cuenta con un servidor que funciona todo el año las 24 horas del día por lo cual es absolutamente apropiado para realizar la factibilidad técnica.

COMPARACION ENTRE LOS FIREWALL WINDOWS			
Firewall / Características	OUTPOST[4]	KERIO[5]	TINY(Sandbox)[6]
Sistema Operativo	Windows 2000 server	Windows 2000 server	Windows 2000 server
Instalación	Modo Gráfico	Modo Gráfico	Modo Gráfico
Escalabilidad	✓	✓	✓
Facilidad en configuraciones	✓	✓	✓
Restricciones De bloqueo	Alta	Media	Media
Puertos	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3	23 telnet 80 Http 21 Ftp	23 telnet 80 Http 21 Ftp
Interface	Amigable	Poco Amigable	Poco Amigable
Especificación de IP	✓		
Licencia para el Servidor	$950	$600	$400
Mínimo Requerimiento	64Mb RAM. 10 MB espacio en Disco	32MB RAM, 10 MB espacio en Disco	32MB RAM, 10 MB espacio en Disco
Protocolo	TCP/IP, NetBeui	TCP/IP	TCP/IP
Seguridad	Alta	Media	Baja
Documentación	Media	Media	Media
VPN	No	No	No
Capas del Modelo OSI y TCP/IP	- Capa de Transporte - Capa de Red	- Capa de Transporte - Capa de Red	- Capa de Transporte - Capa de Red

Tabla 3.3 Comparación entre los Firewalls software para Windows

[4] www.agnitum.com
[5] www.kerio.com
[6] www.tinysoftware.com

A efectos de diseñar la seguridad de la red es necesario, establecer las respectivas comparaciones entre los tres diferentes Firewalls, y de esta manera obtener resultados que permitirán continuar con la selección de Firewall.

3.5.2.3 Factibilidad Económica para los Firewalls Windows 2000 Server.

Los costos reales tratados en la tabla *3.3*, demuestra el valor de cada Firewall. Para que exista una relación entre costos beneficios, es conveniente asignar valores con el fin de entregar una curva característica la cual sirve para la elección del Firewall más viable. Los valores asignados en cada beneficio en la tabla 3.4 son producto del estudio anterior en todas sus etapas, los cuales contienen una calificación con un rango de 1-10: Para el estudio de la factibilidad económica.

Firewall / Beneficios	Outpost	Kerio	Tiny (Sandbox)
Seguridad	10	9	8
Fiabilidad	9	8	7
Escalabilidad	9	9	9
Facilidad de configuración	10	9	9
Soporte en linea	10	9	9
Conocimiento	8	7	6
Funcionabilidad	9	8	7
Documentación	9	9	9
Requerimiento adicional	0	0	0
Costo	10	7	6

Tabla 3.4 Beneficios de los Firewalls para Windows

Los valores de la tabla 3.4 entrega una curva característica para los Firewalls con respecto a los beneficios.

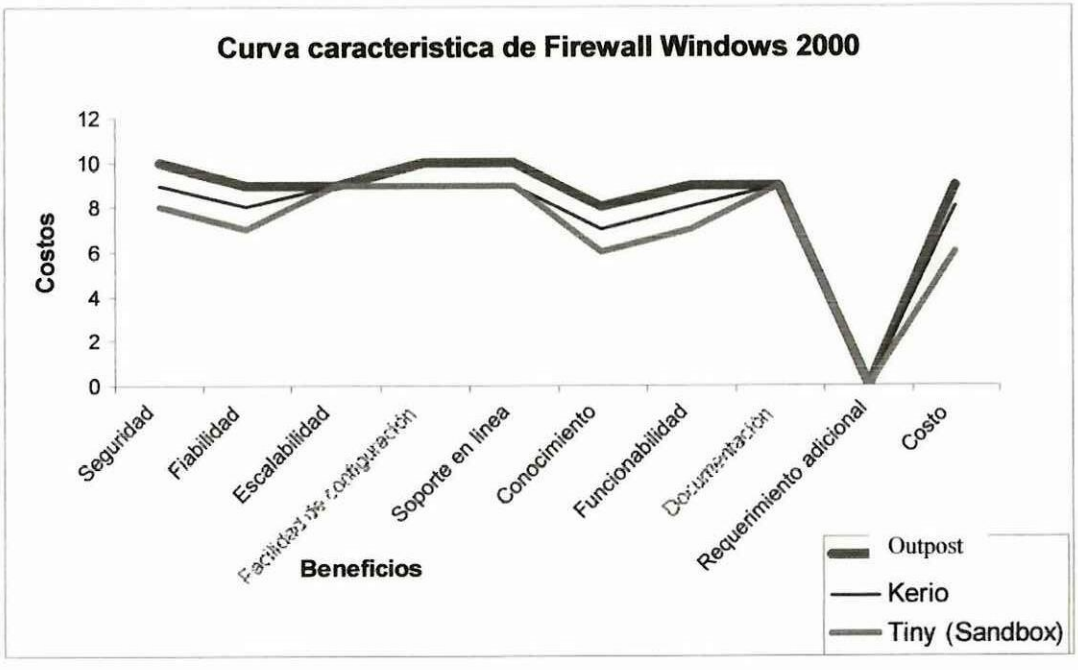


Gráfico 3.2 Curva característica de Firewall Windows 2000 Server

El gráfico 3.2 demuestra que el Firewall Outpost sobresale en las diferentes características técnicas con relación a Kerio y Tiny(Sandbox) sin embargo es necesario mencionar que el costo es alto.

3.5.2.4 Selección de una alternativa de seguridad informática para los Firewalls Windows 2000 Server.

Después del estudio de factibilidad Operativo, Técnico, y Económico sobre los Firewalls se ha a puesto de manifiesto el Firewall OUTPOST por resaltar en las siguientes características.

- Uno de los aspectos más útiles e importantes del Firewall son sus políticas, una política es una táctica que permite vigilar el acceso de su computadora hacia el Internet.
- Se puede crear una regla para limitar el acceso a la red, a los puertos y protocolos.
- Configuraciones múltiples.

  - Puede impedirles a sus niños acceder los sitios no deseados (el sexo, los juegos y otros)
  - Usted puede crear una regla que permitirá o bloqueará la actividad de la red, especificando la dirección IP.
- Protección de contraseñas.

  - Pueda proteger su información por medio de la contraseña y no puede cambiarse sin su permiso.

- Los intervalos de tiempo especificados.

  - Permite o bloquea aplicaciones que dependen del tiempo de un día y día de la semana.
  - Puede bloquear el tráfico no deseado en cierto modo eso está completamente oculto de los usuarios.

- Informado de la actividad.

  - Se presenta un icono del Firewall Outpost en la barra de tareas cuando una regla se activa. Por ejemplo, un mensaje de la advertencia aparece siempre que alguien se conecta a su PC.
  - Puede conseguir un informe de las actividades realizadas o de cada conexión a su computadora, si permitió y bloqueó.

3.5.2.4.1 Conclusiones

- En el estudio de factibilidad operativa se analizó las ventajas que presentan los tres Firewalls (Kerio, Tiny, Outpost), descubriendo que Outpost prosee mejores ventajas que los otros dos mencionados. El Firewall Outpost es compatible con el sistema operativo Windows 2000 Server, su instalación y configuración es fácil y rápida sin presentarse interrupciones en el servidor. Con la configuración correspondiente se restringe o acepta el ingreso de direcciones IP y también a páginas web.
- En la factibilidad técnica Outpost presenta la configuración en modo gráfico lo que permite la interacción con el administrador , el bloqueo de restricciones permite obtener un nivel alto de seguridad, los puertos que controla son: 23 telnet, 80 http, 21 Ftp, 25 Smtp, 110 Pop3, la interfase es amigable para el administrador,

la licencia se debe adquirir para el servidor, el protocolo en que trabaja es TCP/IP y NetBEUI.

- La factibilidad económica cumple con la función de costo-beneficio de los tres firewalls, Outpost posee un costo elevado en comparación con los otros Firewalls, sin embargo por el análisis realizado en la seguridad, fiabilidad, escalabilidad, facilidad de configuración y soporte en línea.

3.5.2.4.2 Recomendaciones

- Las autoridades universitarias deben asignar un presupuesto para la seguridad informática.
- Adquirir en lo posible el Firewall Outpost para Windows 2000 Server para proteger la seguridad en el servidor del Departamento Financiero.

3.5.3 Firewall Hardware

3.5.3.1 Factibilidad operativa para los Firewall de Hardware

Esta factibilidad permite determinar las diferentes facultades que puedan tener los Firewall hardware, además características como ventajas, beneficios y particularidades de los mismos por lo consiguiente se hace necesario enunciar cada uno de ellos como sigue.

3.5.3.1.1 Cisco Secure PIX 525 Firewall

El modelo PIX 525 permite realizar comunicaciones privadas seguras a través de Internet o de cualquier red IP. Integra características clave de las VPN(conexión en túnel, cifrado de datos, seguridad y firewall) para proporcionar plataformas seguras y con capacidad de ampliación a fin de aceptar mejor y con mayor rentabilidad la conexión de acceso remoto y extranet utilizando servicios públicos de datos.

Gráfico 3.3 Cisco Secure Pix 525 Firewall

Características y ventajas principales:

- Componente de una excelente solución en red para los Firewall cisco: Permite a las empresas ampliar las sucursales en una infraestructura mejor.
- Menor costo de propiedad: sencillo de instalar y configurar.
- Sistema integrado seguro y en tiempo real: elimina los riesgos asociados con los sistemas operativos de propósito general.
- VNP basada en estándares : Permite a los administradores reducir los costos de conexión de los usuarios móviles y de sitios remotos.

- Algoritmo de seguridad adaptable: proporciona una seguridad completa para todas las secciones TCP/IP en la protección de recursos privados.
- Espera en actividad y control de errores: proporciona una alta fiabilidad de la red.
- Conversión de las direcciones de la red (NAT): ahora el alto costo de la renumeración IP; amplía el espacio de direcciones IP al mundo exterior.
- Conmutación de corte Proxy: ofrece la mejor autenticación del sector; reduce los costos de operación mediante la reutilización de la base de autenticación ya existente.
- Varias tarjetas de interfaz de red:
- Permite hasta 280.000 conexiones simultaneas
- Evita los ataques de denegación de servicios: protege el Firewall y los clientes y servidores que están detrás de él de hackers intrusos o destructivos.
- El Firewall Hardware Cisco evita el ingreso de virus informáticos que viajan por Internet causando peligros eminentes para una red de computadoras.
- Gran número de aplicaciones compatibles: reduce el impacto de un firewall en los usuarios de la red.

- Filtro Applet Java: permite que el firewall pueda detener las aplicaciones Java potencialmente peligrosas, tomando como base el cliente o una dirección IP.
- Admite aplicaciones multimedia: reduce el tiempo y costo de administración necesarios para dar soporte a estos protocolos; no requiere ninguna configuración especial de los clientes.
- Facilidad de configuración : permite aplicar una normativa de seguridad general con tan solo seis comandos.
- Diseño compacto: sólo requiere dos unidades de bastidor.
- Filtro de dirección URL: proporciona la posibilidad de controlar que tipos de sitios web visitan los usuarios y mantienen un registro de auditoria con fines contables; si se combina con el software Websense Enterprise, tiene un impacto mínimo sobre el rendimiento del PIX Firewall.
- Mail Guard: elimina la necesidad de un retransmisor externo de correo en el perímetro de la red y los ataque de denegación de servicio sobre los retransmisores externos de correo.

3.5.3.1.2 El FortiGate 200 (Firewall hardware)

El firewall FortiGate 200 proporciona servicios de protecciones a la red en tiempo real como: contra virus, gusanos, y otras amenazas.

Gráfico 3.4 Fortigate 200 Firewall

Fortigate protege en los siguientes aspectos:

- Protección antivirus: Descubre y elimina 100% de los virus y gusanos que infectan las redes, en tiempo-real. Examina las entradas y salidas de e-mail (SMTP, POP3) y todo el tráfico de http.
- Elimina virus y gusanos de los túneles de VPN, la infección por parte de usuarios remotos y amigos.
- Permite un plan Intuitivo que facilita la configuración y las políticas del firewall.
- Autenticación del usuario: Banco de datos interior para la autenticación del usuario.
- Horarios de la política: Permite creación de horarios definiendo las fechas (semanas, o mes).
- Cartografía de IP virtual: Contiene mapas a los IP públicos que se dirigen a servidores en la intranet. Es usado para conectar una red de computadoras para afianzar el acceso público.
- Encuadernación de IP/MAC: Automáticamente se realizan lazos en un organizador la dirección de IP con su única dirección de MAC para prevenir spoofing de IP.
- Tráfico : Les permite a los administradores definir el ancho de banda, mismo tiempo limita y asigna prioridades específicas de acuerdo a las políticas del Firewall.

- Descubrimiento de ataques: Descubre los ataques mediante el conocimiento de los ataques más populares que operan en los sistemas y protocolos de la aplicación.
- Email Alarmas: Envía alarmas a mas de 3 direcciones e-mail. Cuando se descubre un ataque.

3.5.3.1.3 Firewall Hardware de 3com

Gráfico 3.5 Firewall 3com

Esta innovadora solución de Firewall empaquetado, ofrece un nivel de seguridad de redes avanzado, usando una exclusiva combinación de hardware y software resistente a manipulaciones.

Las características y ventajas principales:

- La solución 3Com® Firewall empaquetado, le permite controlar la seguridad de la LAN, incluyendo los puntos terminales remotos de la red.
- Combina seguridad distribuida, basada en hardware, con aplicación gestionable de políticas, extendiendo las capacidades del Firewall más allá del perímetro de la red.
- Las tarjetas 3Com Firewall PCI y PC Card, son resistentes a manipulaciones y ayudan a proteger las redes contra códigos

maliciosos, vulnerabilidades de sistemas operativos, y ataques por puerta trasera.

- El 3Com Firewall Policy Server proporciona control centralizado de servidores, ordenadores de sobremesa y portátiles, tanto si están conectados dentro como fuera de la LAN corporativa.
- Los niveles de seguridad de red pueden ajustarse con precisión según las necesidades, simplemente configurando políticas de seguridad apropiadas y trasladando estas políticas a través de la red.

3.5.3.2 Factibilidad Técnica para los Firewall de Hardware

Para determinar los parámetros que sean necesario para la selección del mejor Firewall Hardware, es conveniente analizar los parámetros técnicos. Los cuales se reflejan en las comparaciones de Firewall hardware expuestos en la Tabla 3.5, en donde se presentan los recursos necesarios como herramientas, conocimientos, habilidades, experiencia, etc., que son necesarios para efectuar la selección del Hardware de seguridad del proyecto.

COMPARACIÓN ENTRE LOS FIREWALL HARDWARE[7]			
Firewall / Características	Cisco[8]	Fortigate[9]	3com[10]
Sistema Operativo	Cualquier Posee su propio S.O.	Windows Linux	Empaquetado Propio S.O.
Escalabilidad	✓	✓	✓
Facilidad en configuraciones	✓	✓	✓
Restricciones De bloqueo	Alta	Media	Media
Puertos	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3	23 telnet 80 Http 21 Ftp 25 Smtp 110 POP3
Especificación de IP	✓	✓	✓
Licencia	$1015	$2000	$1500
Mínimo Requerimiento	64Mb RAM. 10 Mb espacio en Disco	32MB RAM, 10 Mb espacio en Disco	32MB RAM, 10 Mb espacio en Disco
Capas del modelo OSI y TCP/IP	-Capa1 -Capa de Transporte -Capa de Red	-Capa1 -Capa de Transporte -Capa de Red	-Capa1 -Capa de Transporte -Capa de Red

Tabla 3.5. Comparación entre los Firewalls hardware

3.5.3.3 Factibilidad Económica para el Firewall Hardware

El factor económico es uno de los elementos necesarios para la toma de decisiones de cualquier Institución, lo cual se describe en las líneas siguientes con el único fin de seleccionar el mejor Firewall hardware. Para que exista una relación entre costos beneficios, es conveniente asignar valores con el fin de entregar una curva

[7] http://monografias.preciomania.com/search_attrib.php/page_id=403/start=25/ut=c8295bd5a7ba3584
[8] http://www.cisco.com/en/US/products/hw/vpndevc/pc2030/index.html
http://www.tribecaexpress.com/Cisco_PIX_501.htm
[9] http://www.tribecaexpress.com/Fortinet_Fortigate.htm
[10] http://www.linuxguruz.org/iptables/.

característica la cual sirve para la elección del Firewall más viable. Los valores asignados en cada beneficio en la tabla 3.6 son producto del estudio de la factibilidad operativa, técnica, los cuales contienen una calificación de 1-10 según la calidad de sus beneficios.

Firewall / Beneficios	Cisco	FortiGate	3com
Seguridad	10	9	8
Fiabilidad	10	10	10
Escalabilidad	9	8	8
Facilidad de configuración	9	10	6
Soporte en línea	10	9	4
Conocimiento	8	9	6
Funcionabilidad	10	8	7
Documentación	6	2	4
Requerimiento adicional	5	4	4
Costo	2	5	6

Tabla 3.6 Beneficios de los diferentes Firewalls Hardware

Los valores de la tabla 3.6 entrega una curva característica para los Firewall con respecto a los beneficios

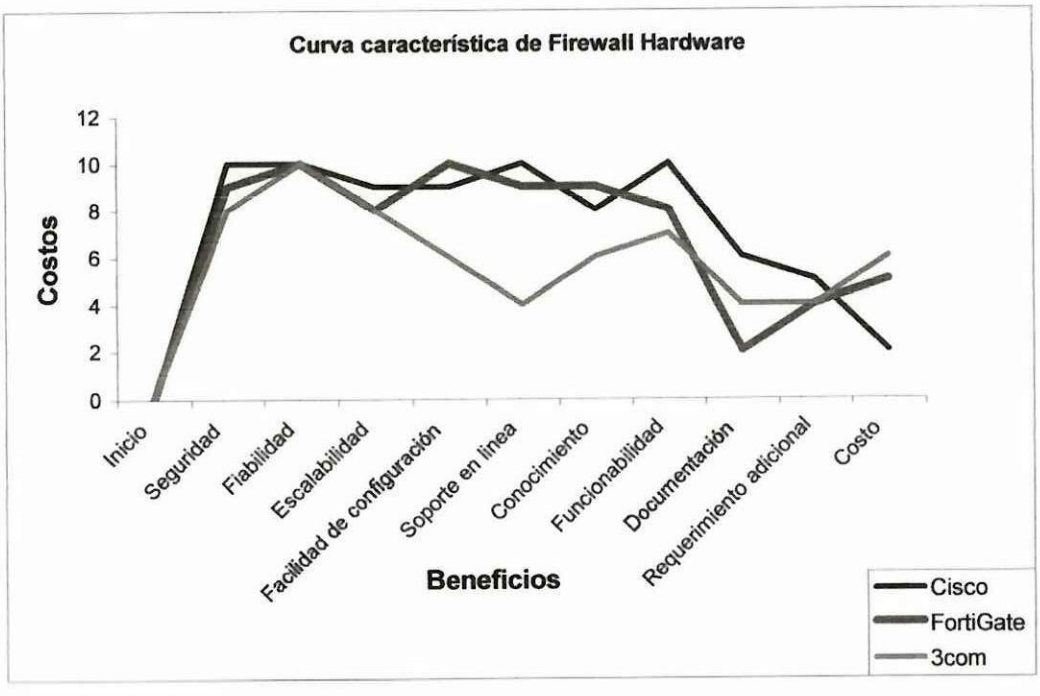


Gráfico 3.6 Curva de benéficos Firewall hardware

Los valores de la tabla 3.6 entregan una curva característica para los Firewall con respecto a los beneficios representados en el gráfico 3.2, en el que sobresale Cisco por poseer una regularidad en los aspectos citados.

3.5.3.4 Selección de una alternativa de seguridad informática para los Firewall Hardware.

Con las características descritas de cada uno de los Firewall hardware, se llega a la conclusión que el Firewall hardware de **Cisco Secure PIX 525** es el mas conveniente porque se acopla mucho mejor a la arquitectura de la red de la Universidad en los siguientes aspecto a continuación:

- Seguridad: la seguridad es para restringir usuarios no autorizados.
- Fiabilidad: con la presente alternativa de solución se puede dar mucha más seguridad a los datos de la Universidad.
- Escalabilidad: la empresa Cisco es un proveedor que tiene muchos anos de experiencia en seguridades de redes y por ende su producto consta de muchas versiones de escalabilidad.
- Facilidad de configuración: Permite una configuración relativamente fácil.
- Soporte en línea: Contiene muchos productos en línea y su soporte lo realiza en su página oficial: www.cisco.com.
- Conocimiento: es de entorno gráfico para una fácil asimilación.
- Funcionabilidad: el funcionamiento y puesta en marcha es muy eficaz para las necesidades de la Universidad.
- Documentación: Se reciben manuales de hardware y software en el momento de la adquisición del dispositivo.
- Requerimiento adicional: Según las características de la implementación de seguridad de red se necesita incorporar algunos elementos de red para la concatenación física de la misma.

  Por lo consiguiente es el más apto para su uso en la Universidad y para proyecciones futuras de la red.

3.5.3.4.1 Conclusiones

Producto de analizar los Firewall Cisco, Fortigate, 3com. Se llegó a la conclusión que el Firewall hardware Cisco es el que posee mejores servicios en seguridad, fiabilidad, rendimiento; por lo cual es la elección más satisfactoria para las necesidades de la Universidad, porque entrega beneficios excelentes. Por lo siguiente:

- En la factibilidad operativa el funcionamiento del Firewall Cisco es eficiente por el hecho de tener mejores ventajas y beneficios que los demás Firewall comparados.
- En la factibilidad técnica se realizaron comparaciones de tres diferentes Firewall, resultando mas aceptable el Firewall Cisco por tener mejores beneficios de seguridad para la red.
- El Firewall Cisco Secure PIX 525 es muy sencillo de instalar y configurar.
- Posee su propio sistema integrado y de esta forma elimina utilizar sistemas operativos específicos.
- Se pueden procesar gran número de aplicaciones compatibles reduciendo el impacto de un Firewall en los usuarios de la red.
- Proporciona una seguridad completa para todas las sesiones TCP/IP en la protección de recursos privados.
- El costo-beneficio de los Firewall se analizó en la factibilidad económica, en donde, Cisco es el que posee una mejor relación

costo-beneficio. Sin embargo su costo es elevado y su rendimiento es óptimo.

Por consiguiente, el software Cisco es el mejor en seguridad y beneficios que se ajusta a las necesidades de la Universidad.

3.5.3.4.2 Recomendaciones

Se debe tomar en cuenta lo siguiente:

- Al instalar el Firewall Cisco Pix o cualquier firewall hardware se debe incurrir necesariamente en gastos (cables, conectores, hubs, etc) adicionales, según la arquitectura de red a incorporar para establecer la seguridad de Red.
- Requiere un espacio adicional en el Rack, lo que induce a crear espacio dentro del mismo, para que el Firewall entre en funcionamiento e interactúe con los dispositivos de conexión relativos a su propósito.
- Los costos mencionados en la tabla 3.5, para la factibilidad técnica del Firewall Hardware solo representa los valores de las tiendas virtuales en Internet, a lo cual se debe añadir el costo de entrega del producto.

3.6 Antivirus[11]

Actualmente en el mercado se encuentran muchos programas de protección contra virus. Muchos de ellos están accesibles en forma de Shareware (software ilimitado) listos para bajar de sitios como Tucows[12] o Download[13].

3.6.1 Factibilidad Operativa

3.6.1.1 Mcafee Viruscan[14]

El antivirus Mcafee tiene las siguientes ventajas:

- Puede revisar equipos en red, con ello se obtiene el control desde un solo equipo, y además las actualizaciones son constantes (15 días o menos).

Las desventajas

- Si se baja el shareware, el programa muy pronto mencionará que su versión expiró, y a veces causa problemas al desinstalarlo.

3.6.1.2 Norton Antivirus[15]

Este Antivirus tiene las siguientes características:

- Exigir pocos recursos al sistema.

[11] http://www.lacompu.com/
[12] http://www.tucous.com/
[13] http://www.download.com/
[14] http://www.mcfee.com/
[15] http://www.norton.com/

- Se puede actualizar bajando el archivo que pesa alrededor de 2.4 Megabytes.
- Para los equipos con Windows 98, todavía se puede acceder a una actualización.

Desventajas:

- Norton Antivirus crea una copia de seguridad de los sectores más importantes de nuestro Disco Duro (vacuna). Si nota algún cambio, procede a reparar dichos sectores, con la copia que ya había guardado, en caso de una instalación nueva o sobre el sistema operativo (a veces se hace para reparar algunos archivos), el Antivirus ocupa la vacuna para reparar, malogrando el disco y dejando el equipo sin sistema.

3.6.1.3 Panda Antivirus[16]

Panda Software en una empresa poco conocida española que lleva bastantes años fabricando antivirus. La particularidad es la cobertura de virus (mas de 50.000) superior a los de la competencia. El Shareware pesa alrededor de 13 Mb.

Las ventajas

- Al instalarse hace una revisión del equipo, sacando la mayor parte de los virus presentes (Ni Norton AV ni Mcafee VS lo hacen y muchas veces se infectan a sí mismos al instalarse).

[16] http://www.panda.com/

- El funcionamiento es bastante simple, y puede incorporarse a Outlook para revisar los e-mails.
- Es fácil de instalar y de desinstalar.

Las desventajas

- No puede actualizarse el shareware, pero funciona bien mucho tiempo.
- Consume más recursos de sistema que otros antivirus, con lo que no es la mejor elección en equipos mas lentos.

3.6.2 Factibilidad Técnica

Programa / Características	**McAfee VirusScan 2003**	**Panda Antivirus Platinum 2003**	**Symantec Norton Antivirus 2003**
Precio en USA	$29	$60	$40
Virus ignorados en prueba de muestreo total	1/1	0/0	1/1
Virus desconocidos.	2	0	3
Tiempo de ejecución (min:sec)	7:30	5:06	3:47
Duración de actualización y pago anual después del primer año	1 año $4.95	1 año $30	1 año $3.95
Actualización automática	Sí	Sí	Sí
PROs y CONTRAs	PROs: Muchos opciones de muestreo, utilitarios de respaldo. CONTRAs: No actualización automática, interfaz confusa	PROs: Ejecución perfecta, rápido, interfaz clara. CONTRAs: El registro y actualización pudieran ser más simples.	PROs: Rápido tiempo de muestreo; excelente actualización. CONTRAs: Difícil de instalar y desinstalar.

Tabla 3.7 Comparación entre los antivirus McAfee, Panda y Norton

3.6.3 Factibilidad Económica

Con el fin de una mejor elección en el software de antivirus, se procede a realizar la curva costo beneficio en función de las características que se presentan en la tabla 3.8:

Antivirus / Características	McAfee 2003	Panda 2003	Norton 2003
Precio en USA	10	5	7
Virus ignorados	5	10	2
Virus desconocidos	6	10	5
Control de virus de red	10	0	0
Tiempo	7	5	3
Actualización	9	9	9

Tabla 3.8 Características de los antivirus

Con los datos expuestos en la tabla 3.8, se representa la curva característica siguiente:

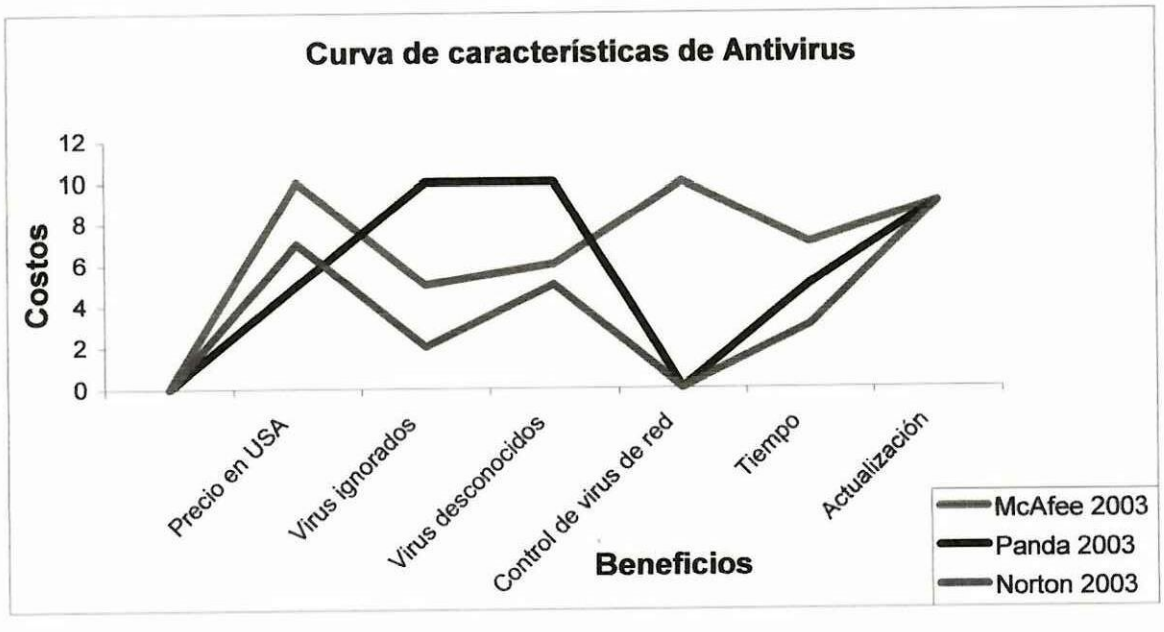


Gráfico 3.7 Curva característica de los antivirus McAfee, Panda, Norton

3.6.4 Selección de una alternativa de antivirus

La curva característica del Gráfico 3.7 muestra claramente, que el antivirus McAfee es más apropiado para la mejor elección por tener las siguientes características:

- Las actualizaciones se realizan cada 15 días, esto es muy importante puesto que los virus nuevos parecen con mucha frecuencia.
- Con una velocidad impresionante es la mejor elección para revisar grandes cantidades de información.
- La inspección de virus en la red McAfee lo realiza con mucha eficacia, para controlar cualquier tipo de virus que pueden acceder de parte de los equipos a la red interna.
- El precio es moderado para la obtención del producto.

Con una eficiencia en su capacidad de reconocer virus nuevos, y una velocidad impresionante es el rastreo de virus, McAfee es la mejor opción para la Universidad, puesto que cuenta con todo los requerimiento que lo harán un antivirus ideal para las funciones en el ámbito informático que se realizan en la Institución.

3.7 Diseño del sistema de seguridad

El estudio anterior proporciona las soluciones de hardware y de software acordes a los requerimientos de seguridad actual de la Universidad, según los sistemas operativos instalados en los servidores los cuales se presentan en el siguiente cuadro:

Sistema Operativo	**Solución Firewall**
Linux Red Hat	Iptables
Windows 2000 Server	Outpuots
Linux Red hat /Windws 2000 Server Hardware	Cisco Secure PIX 525

Tabla3.9 Soluciones de Firewall

Con las soluciones obtenidas en función de su respectivo estudio, es necesario complementar la solución con una arquitectura de seguridad de red tomando en cuenta los recursos óptimos.

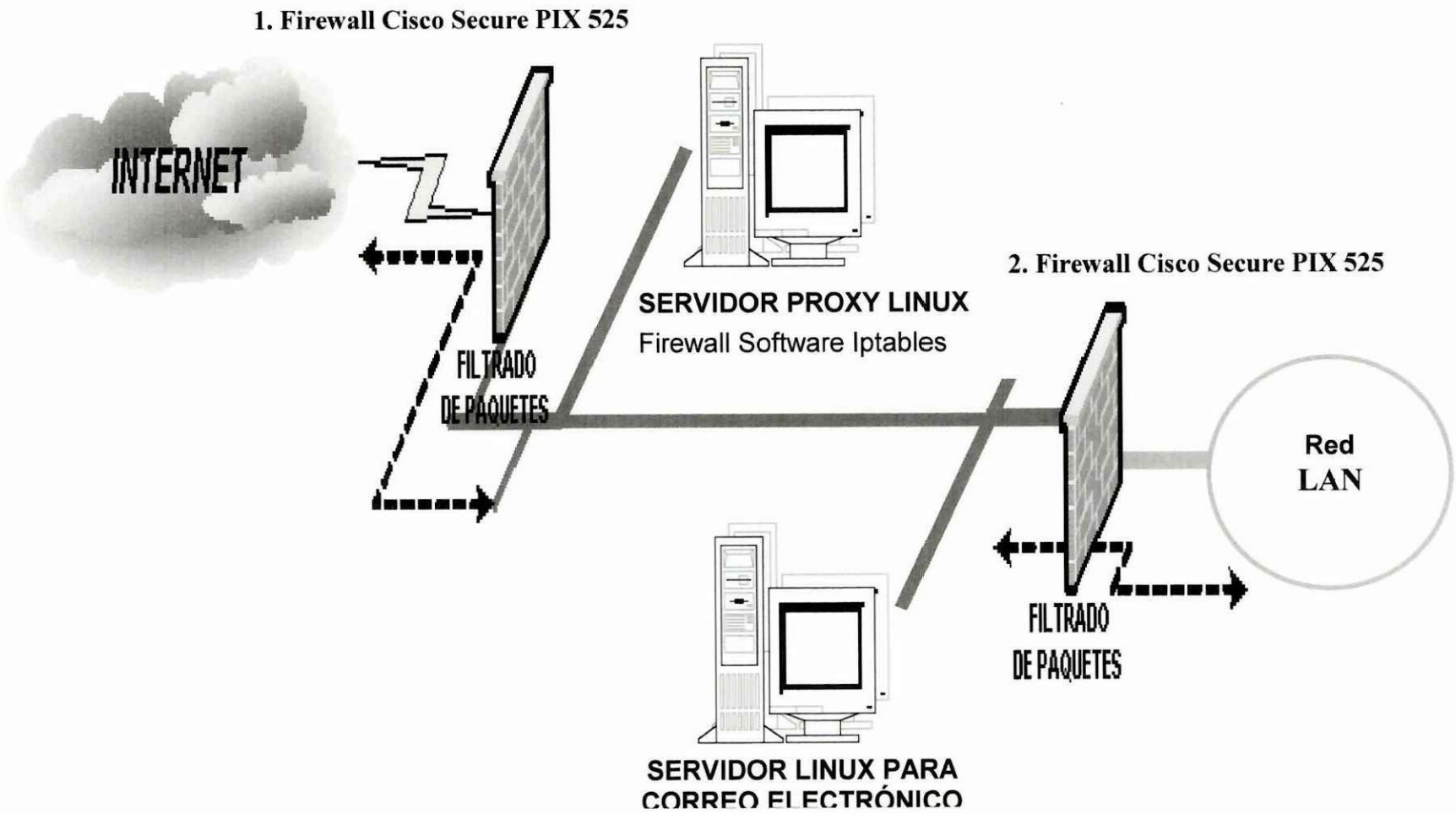


Gráfico 3.8 Diseño de la arquitectura de seguridad de red

3.7.1 Descripción de la Arquitectura de seguridad

La Arquitectura de seguridad propuesta es producto de una investigación minuciosa, entrevistas a personas calificadas sobre el tema, y encuestas realizadas a diferentes Instituciones entre las cuales constan la Universidad Católica y la Universidad Técnica de Ambato. El diseño de seguridad se presenta en la figura 3.8 que a continuación se detalla.

- El servicio de Internet provisto a la Universidad Técnica de Cotopaxi por parte de la empresa IMPSAT, llega a un primer Firewall Hardware (Cisco Secure Pix 525). Este Firewall tiene la función principal de filtrar paquetes a los usuarios externos que requieran información del Servidor Proxy de la Universidad, mediante las restricciones de direcciones IP de usuarios no confiables, otras reglas creadas según las políticas de seguridad informática de la Institución. El Firewall (Cisco Secure Pix 525) evita que los virus informáticos que viajan por Internet ingresan al servidor Proxy y a la red informática de la Universidad Técnica de Cotopaxi, en caso de vulnerar al Firewall en mención los virus informáticos podrían ocasionar que el servidor detenga sus actividades normales; con lo cual las computadoras que están en la red se contaminan y con ello

colapsar por el virus informático, este percance ocurre porque el servidor es la columna vertebral en la red informática.

- En caso extremo de vulnerar al primer Firewall hardware (Cisco secure Pix 525) se presenta el Firewall Software para el Servidor Proxy llamado Iptables que es un programa que posee el sistema operativo Linux Ret hat 7.3 el mismo que proporciona la integridad en la información por sus características de configuración descritas en el capítulo III numeral 3.5.1.1.2, complementando así la seguridad de usuarios externos que intenten ingresar al servidor por medio de Internet.
- Una medida de protección para el servidor de correo electrónico es instalar un segundo Firewall Hardware (Cisco secure Pix 525) el mismo que posee características importantes para restringir usuarios no autorizados, de acuerdo a reglas incorporadas dentro del mismo, las cuales pueden variar según crea conveniente el Administrador de la red. Este Firewall instalado y configurado según diseño es con el fin de impedir el acceso a estudiantes o personas de la red Lan Interna que no tengan el permiso correspondiente al servidor de correo Electrónico, de esta manera se protege de los intrusos internos. Esto permite una mayor confiabilidad en la información tanto externa como interna, para poder trabajar con

mayor seguridad en la red sin que haya interferencias de ninguna clase y más aun robo de información.

Los permisos que se deban establecerse, son de acuerdo a las políticas de seguridad tratadas en el capítulo III numeral 3.1, que el administrador aplique al sistema de seguridad.

CAPITULO IV

Demostración de la seguridad para la red de datos de la Universidad Técnica de Cotopaxi.

4.1 Diseño

El diseño de la demostración es con el fin de presentar la funcionalidad de un sistema de seguridad. La solución óptima que fue desarrollada al final del capitulo III en donde incluye muchos costos, por lo cual la representación gráfica es la mínima en un sistema de seguridad.

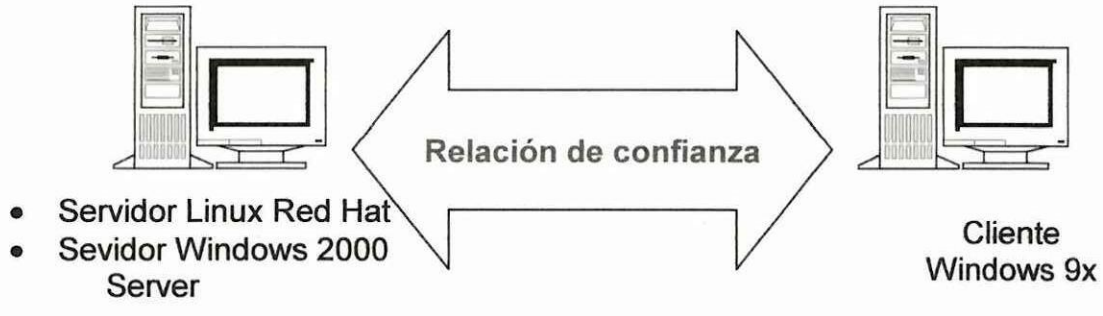


Figura 4.1 Diseño de demostración

En el diseño de demostración de la figura 4.1, se encuentra incluido en su lado izquierdo un servidor, en el cual se encuentran instalados dos sistemas operativos; Servidor Linux Red Hat, y Servidor Windows 2000 Server.

La conexión física entre las computadoras, se realiza con un cable cruzado con sus respectivos conectores, a través de la tarjeta de red.

4.2 Instalación y configuración del sistema de seguridad

Los Firewall software seleccionados en el capítulo anterior, para Windows Outpost e Iptables de Linux Red Hat, por ser las mejores alternativas los mismos que implementados en la Universidad incrementarán la seguridad, mediante los cuales se aplicarán para la demostración desarrollada en los ítem anteriores. A continuación se explicara detalladamente las características y configuraciones de los software elegidos.

4.2.1 Sistema operativo Windows 2000 Server

Microsoft Windows 2000 constituye un gran avance en las áreas de administración de redes, soporte de hardware, acceso a Internet y demás. Sin embargo, los cambios positivos son varios. Windows 2000 Server es con certeza, más fiable, más sencillo de administrar (una vez que nos hemos habituado a los cambios) y más rápido que Microsoft Windows NT. Microsoft Windows 2000 Server, es el sucesor de Microsoft Windows NT 4.

4.2.1.1 Instalación y configuración del sistema Operativo Windows 2000 Server

- Requisitos mínimos para obtener un rendimiento adecuado:

  - **Intel Pentium 133 a 32 bits:** Uno o más procesadores Intel Pentium II 300 Mhz ó más rápidos.
  - **64 Mb de RAM:** 128 Mb de RAM mínimo, 256 Mb o más recomendado.

- **Monitor VGA:** Monitor Súper VGA con resolución de al menos 800 x 600.
- **Teclado y ratón u otro dispositivo señalador**: Cualquier tipo de teclado y ratón u otro dispositivo señalador. (Si el teclado es del tipo PS/2, el ratón debe ser también PS/2 o USB).
- **Partición de 850 Mb con 650 Mb de espacio libre:** 2 Gb de espacio libre en un disco duro Ultra IDE o (preferiblemente) Ultra Wide SCSI con 7200 rpm o más.
- **CD-ROM de inicio 12x**: No se necesita más velocidad para la instalación, aunque tiene que ser compatible con el sistema de inicio.
- **Uno o más adaptadores de red:** Si se va a realizar la instalación a través de la Red.

➢ Instalación desde Windows

Si tenemos instalado Windows 95/98 ó Windows NT, la instalación recopila información y copia los archivos que necesita el equipo para iniciar en el modo de texto de Windows 2000 y después reinicia en modo texto. Se puede entonces (opcionalmente) seleccionar la partición apropiada, después de lo cual se instala Windows 2000 en el disco duro y se pasa al Asistente para instalación de Windows 2000 en modo gráfico, que recopila más información, configura los

dispositivos y termina de copiar los archivos. Después de esto, la instalación está completa y el equipo se reinicia en Windows 2000.

1. Insertar el CD-ROM de Windows 2000 y pulsar en Instalar Windows 2000, si está activa la Reproducción automática del CD-ROM (Notificación automática de inserción).
2. Dependiendo del Sistema Operativo que tengamos y de la Licencia que hayamos adquirido, el sistema activará o desactivará las siguientes opciones, ofreciendo todas las posibilidades de instalación posibles:
    - Actualizar a Windows 2000.
    - Instalar una nueva copia de Windows 2000.

Figura 4.2 Asistente de Instalación de Windows

3. Después de elegir la opción deseada pulsamos **Siguiente**.
4. Contrato de Licencia: Se debe leer el contrato de licencia, seguidamente hay que elegir el botón de opción Acepto este contrato y pulsar con el ratón en Siguiente.

5. **Clave del Producto:** Introducir el CD-KEY del producto que se está instalando.

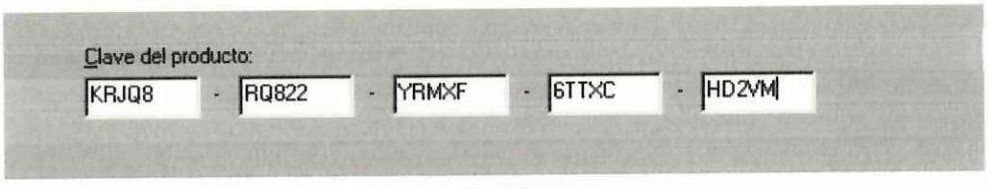


Figura 4.3 Clave de Instalación de Windows

6. La instalación muestra la ventana Seleccionar opciones especiales, y que se utiliza para personalizar las opciones de idioma, el uso de utilidades de accesibilidad durante la instalación para usuarios con problemas de visión.
7. Se debe pulsar en **Siguiente** para copiar los archivos de instalación al equipo. Después de que la instalación termine de copiar archivos, se reinicia el equipo y se pasa al modo de texto de Windows 2000 para la parte de la instalación basada en texto.

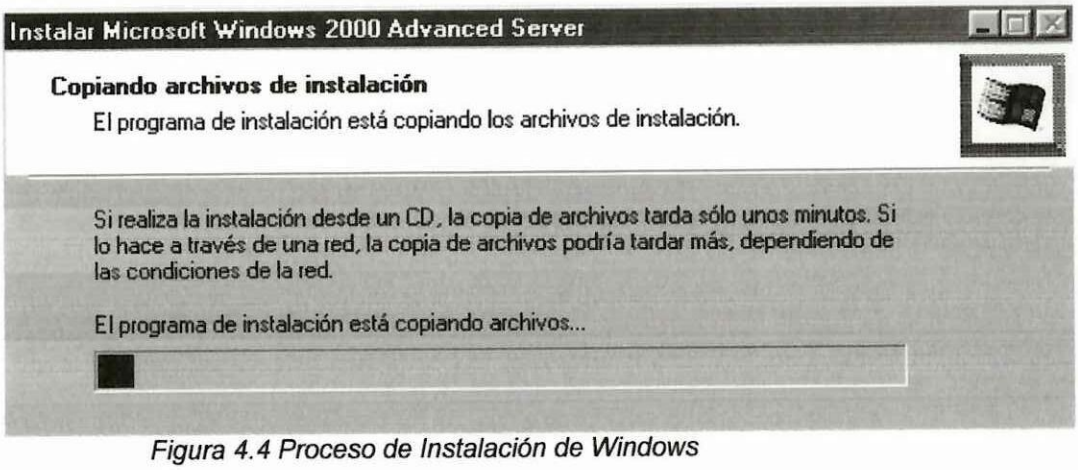


Figura 4.4 Proceso de Instalación de Windows

4.2.1.1.1 Fase del asistente para la instalación de Windows 2000

Cuando la fase basada en texto de la instalación concluya, el equipo reiniciará y Windows 2000 se iniciará por primera vez, cargando el Asistente para la instalación de Windows 2000. Para utilizar el Asistente para la instalación hay que seguir los pasos que se indican a continuación. Al final de cada paso hay que pulsar con el ratón el botón Siguiente o el botón Aceptar para continuar.

1. **Pantalla Instalando Dispositivos:** el Asistente para la instalación detecta y configura los dispositivos instalados en el equipo. Si la instalación no puede detectar de forma apropiada un dispositivo, mostrará un cuadro de diálogo de configuración de dispositivo para la configuración manual del dispositivo.
2. **Configuración regional:** Después de detectar el hardware, se solicitan los parámetros regionales. Estos parámetros afectan a factores tales como la disposición del teclado y cómo se muestran las fechas y la moneda.
3. **Personalización del Software:** Se debe introducir el nombre de la persona bajo la que se registrará el equipo además de la empresa.
4. **Modos de licencia:** Hay que escoger el modo de licencia en la siguiente ventana, como Por servidor o Por puesto. Por defecto aparecerán las licencias para las que tiene el producto. Si se

escoge Por servidor, hay que especificar cuántas Licencias de acceso de cliente se han adquirido.

5. **Nombre del equipo y contraseña del administrador:** Hay que introducir el nombre del equipo en el cuadro de texto Nombre de equipo. Y la contraseña de la cuenta del administrador de hasta 14 caracteres de longitud. En el cuadro de texto Contraseña de administrador, y escribirla de nuevo en el cuadro de texto Confirmar contraseña. Hay que pulsar Siguiente.
6. **Valores de fecha y hora:** Hay que revisar la fecha, hora e información de la zona horaria, realizar cualquier corrección necesaria y pulsar **Siguiente** para configurar los parámetros de red.
7. **Configuración de Red:** Nos da dos posibilidades de configuración, una personalizada o típica.

    - **Configuración típica:** se instalan los siguientes protocolos y servicios de red usados comúnmente: Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y TCP/IP configurado para utilizar DHCP (o Direcciones IP privadas automáticas (APIPA, Automatic Private IP Adressing) si no hay ningún servidor DHCP disponible.)
8. **Grupo de Trabajo y Dominio:** Para unirse a un grupo de trabajo, hay que elegir la primera opción de la ventana Grupo de trabajo o dominio del equipo y escribir el nombre del grupo de trabajo en el

cuadro de texto Dominio o grupo de trabajo del equipo. Para unirse a un dominio existente, hay que pulsar la segunda opción e introducir el nombre del dominio al que se desea unirse en el cuadro de texto Dominio o grupo de trabajo del equipo.

9. **Realizando las tareas finales:** El programa de instalación debe completar el último grupo de tareas para instalar Windows 2000 en su equipo.
10. Cuando la instalación finaliza se reinicia el equipo, se verá la ventana de inicio de sesión estándar de Windows 2000.

4.2.1.1.2 Instalación y configuración del Firewall (OUTPOST) para Sistema Operativo Windows 2000 Server.

1. En la primera pantalla se presenta el mensaje de Bienvenido a la Instalación, en el cual existen dos sugerencias.

   La primera Outpost Firewall FREE.- fácil de usar para la protección en el cual no están todos los beneficios.

   Es por eso que escogemos la segunda opción Outpost Firewall PRO.- en el cual posee casi todos los beneficios, sin embargo existe un tiempo de 30 días, pues es una versión Beta.

Figura 4.5 Instalación de Outpost

2. Pulsamos en botón siguiente y aparecerá el uso de licencia para Outpost Firewall, al cual aceptamos.

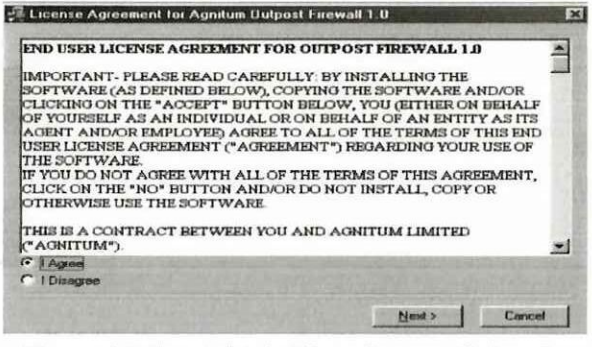


Figura 4.6 Acuerdo de Licencia para Outpost

3. A continuación nos pedirá la ubicación en donde se instalara el Firewall en nuestro caso es en la unidad C.

Figura 4.7 Directorio en el cual se copian los archivos de Outpost

4. El siguiente paso es seleccionar el idioma en el cual se ejecutara el firewall Outpost, seleccione español.

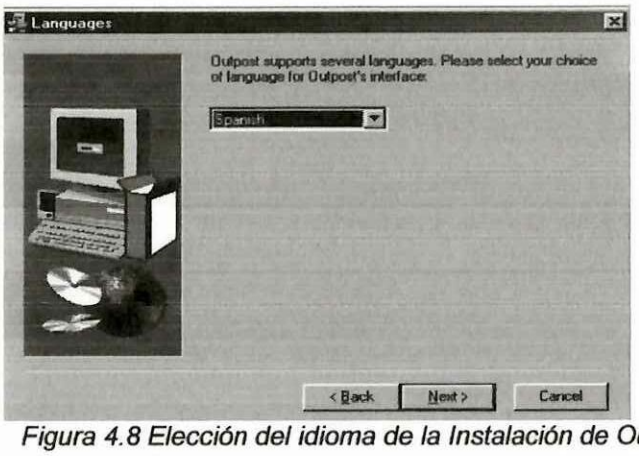


Figura 4.8 Elección del idioma de la Instalación de Outpost

5. La siguiente pantalla nos presenta la instalación de Outpost en la unidad C.

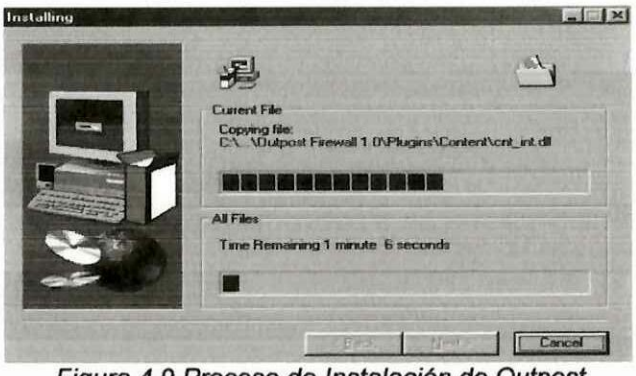


Figura 4.9 Proceso de Instalación de Outpost

6. Por último aparece que la instalación ha sido completada satisfactoriamente

Figura 4.10 Finalización de la Instalación de Outpost

4.2.1.2 Configuración del Firewall aplicando las políticas de seguridad.

La configuración se realiza cuando esta instalado el firewall con las siguientes políticas:

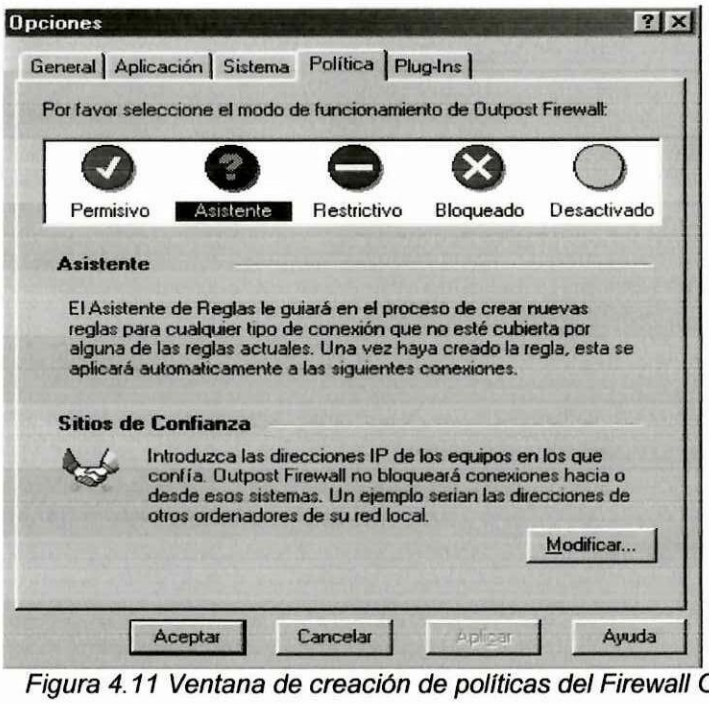


Figura 4.11 Ventana de creación de políticas del Firewall Outpost

- **Permisivo.-** permite todas las comunicaciones que no hayan sido específicamente bloqueadas mediante reglas.
- **Asistente.-** el asistente de reglas le guiará en el proceso de crear nuevas reglas para cualquier tipo de conexión que no este cubierta por alguna de las reglas actuales. Una vez que haya creado la regla, esta se aplicara automáticamente a las siguientes conexiones.
- **Restrictivo**.- Bloquea todas las comunicaciones que no hayan sido específicamente permitidas mediante reglas. Debe crear reglas para cada una de las aplicaciones que desee que tenga acceso a Internet.

- **Bloqueado**.- Bloquea todas las comunicaciones, tanto de Entrada como de salida.
- **Desactivado.-** Desactiva Outpost Firewall y permite todas las conexiones sin ninguna restricción.
- **Contraseña de Protección.-** permite utilizar una contraseña para proteger la configuración de tal manera que si desean ingresar personas ajenas queden restringido el acceso.

4.2.1.3 Pruebas de estabilidad y fiabilidad

Para demostración de la seguridad se procedió a conectar dos computadoras la primera con el Sistema Operativo Windows 2000 Server, que funciona como Servidor. Y la segunda computadora que interviene como cliente, con el sistema operativo Windows XP.

En el firewall Outpost se establecen las política de permisivo que permite el ingreso a la dirección IP 198.162.1.6, de la computadora cliente pues posee el permiso correspondiente.

En la computadora cliente que posee la dirección IP 198.162.1.6, por medio del entorno de red se procedió a ingresar al servidor lo que fue posible por que el firewall se encuentra en modo permisivo.

En el firewall Outpost establecemos la política de modo restrictivo negando el ingreso a la dirección IP 198.162.1.6, de la computadora cliente.

Por medio de la Computadora cliente y utilizando el entorno de red se pretender ingresar al servidor lo que fue imposible pues el servidor lo que tiene el Firewall lo rehúsa por el establecimiento de la política de restrictivo.

Para complementar las pruebas de seguridad se presentan las siguientes herramientas:

WINDOWS	
Amenaza	**Seguridad**
SuperScan.-Es una utilidad que analiza los elementos activos de la red.[1]	*Genios 3.0.* Es un sistema de detección de intrusos (IDS), este escucha las solicitudes de apertura de puerto dentro de un período de tiempo determinado, informa mostrando un cuadro de dialogo cuando detecte una exploración de puertos. Proporcionando el nombre DNS y la dirección IP del infractor.[2]
DumSec.- Es una herramienta para enumerar recursos compartidos en Windows NT y 2000 Server.[3]	Firewall.- Usar el Firewall propuesto para negar el acceso a TCP/UDP a los puertos 135 a 139 y también para Windows 2000 cerrar TCP/UDP 445, porque proporciona información valiosa para los hackers.
Telnet.- Es un servicio que se dispone para conectar computadoras remotas.	Cerrar mediante Firewall el puerto 23.
Ftp.- Es un servicio para interactuar la transferencia de archivos por parte de computadoras remotas.	Cerrar mediante Firewall el puerto 21.
http.- Servicio de navegación por Internet mediante hipertexto.	Cerrar mediante Firewall el puerto 80.
Virus.- Son programas que destruyen archivos de la computadora.	Instalar un antivirus.

Tabla 4.1 Pruebas de estabilidad para Windows

[1] http://www.foundstone.com
[2] http://www.indiesoft.com
[3] http://www.somarsoft.com

4.2.1.4 Análisis de Resultados del sistema de seguridad.

El Firewall Outpost según los resultados de las pruebas obtenidas permite evaluar la funcionalidad de este software, con lo cual se observa la capacidad y el alcance muy amplio en el campo de Seguridad Informática. El Firewall Outpost presenta una interfaz gráfica de fácil manejo, e interacción para el administrador de red.

Uno de los aspectos más útiles e importantes del Cortafuego son sus políticas. En las que se autoriza o niega el ingreso a las direcciones IP. Permite bloquear paginas web no deseadas

Puede proteger la configuración del Firewall Outpost por medio de la contraseña y no puede cambiarse sin su permiso.

Se presenta un icono del Firewall Outpost en la barra de tareas cuando una regla se activa. Por ejemplo, un mensaje de la advertencia aparece siempre que alguien se conecta a su PC.

Puede conseguir un informe de las actividades realizadas o de cada conexión a su computadora, si permitió y bloqueó.

En la actualidad, la seguridad cumple un papel muy importante en el convivir de miles de empresas en el mundo; tal es el punto de importancia de esta tecnología, que en a mayoría de los casos se invierte cuantiosas sumas de dinero para protegerse contra intrusos

con Outpost se protege la información de intrusos que deseen obtener su información.

4.2.2 Sistema operativo Linux red Hat 7.3

Linux es un sistema operativo que tiene código abierto, para que cualquier empresa lo personalice y de esta forma adaptarse a varias empresas. Con el fin de brindar mayor seguridad, porque en un sistema cerrado desconocemos como esta operando, y si esta siendo vulnerado.

4.2.2.1 Instalación y configuración del sistema Operativo Linux

Para el funcionamiento de este sistema operativo solo se necesita un computador con microprocesador Pentium I, pero es aconsejable al menos un Pentium II ó similar con 64 Mb y un disco duro mínimo de 10 Gb para poder trabajar con cierta comodidad.

El CD tiene copiados los archivos de arranque de Linux de manera que permite iniciar el sistema directamente desde la unidad de CD-ROM, como si se tratara de un disco de inicio. Si la BIOS de su equipo soporta esta característica, no tendrá más que activarla de forma que arranque desde la unidad de CD y reiniciar el equipo con el CD dentro de la Unidad.

Una vez creado el disco de inicio y reiniciado el ordenador con este introducido dentro de la disquetera, aparece una pantalla de presentación, proporcionando algunas opciones. En este caso, es necesario pulsar <intro> para continuar.

Tras numerosos mensajes de información sobre el arranque del sistema y el hardware encontrado, da comienzo al programa de instalación. En primer lugar se debe elegir el origen de datos, CDROM Local, y el teclado a utilizar durante la instalación, "es" para el teclado en español. El resto de pasos limitan a configurar el hardware, elegir el paquete que se desea instalar y finalmente copiar los archivos al disco duro y preparar el sistema para poder arrancar Linux (u otro sistema operativo instalado, como Windows 9x). El nivel de seguridad del Firewall es bajo puesto que se debe instalar en forma separada.

La única parte a la que se debe prestar atención es el particionamiento de la unidad de disco duro. Aunque en la práctica es posible, Linux no se puede instalar sobre una partición DOS(FAT16 o la nueva FAT32). Es necesario, por tanto contar con una partición dedicada a Linux, denominada nativa (Linux native). En el caso de contar con poca memoria real instalada en el equipo, se recomienda crear además otra partición de pequeño tamaño, destinada al

intercambio de datos entre la memoria y el disco duro, denominada Swap partición

4.2.2.1.1 Particionamiento del sistema

La herramienta de particionamiento usada en Red Hat Linux 7.3 será el **Disk Druid**. Con la excepción de ciertas situaciones "esotéricas", el **Disk Druid** normalmente mantiene los requisitos de particionamiento de una instalación normal de Red Hat Linux.

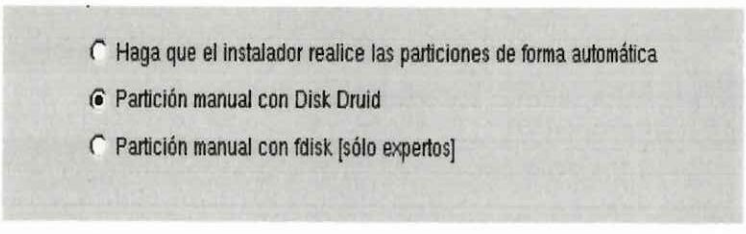


Figura 4.12 Elección del tipo de partición para la instalación de Linux

4.2.2.1.2 Botones de Disk Druid

Estos botones controlan las acciones de **Disk Druid**. Se utilizan para cambiar los atributos de una partición (por ejemplo, el tipo de sistema de ficheros y el punto de montaje) y también para crear dispositivos RAID. Los botones de esta pantalla se utilizan también para aceptar los cambios que hemos realizado, o para salir de **Disk Druid**.

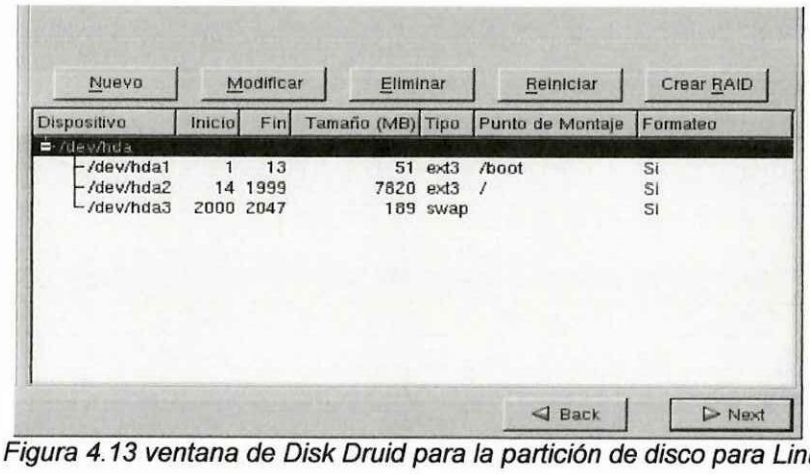


Figura 4.13 ventana de Disk Druid para la partición de disco para Linux

- **Nuevo**: Se usa para pedir una nueva partición. Cuando se selecciona, aparece un cuadro de diálogo que contiene los campos (como por ejemplo punto de montaje y tamaño) que deben ser rellenados.
- **Modificar**: Se usa para modificar los atributos de la partición que tenemos seleccionada en la sección **Particiones**. Si pulsa el botón **Modificar**, se abrirá un cuadro de diálogo. Se puede modificar cualquiera de los campos, en función de si la información ya ha sido escrita o no en el disco.

También puede modificar el espacio libre, tal y como se muestra en la representación gráfica para crear una nueva partición dentro de aquel espacio. Resalte el espacio libre y seleccione el botón **Modificar** o haga doble click en el espacio libre para modificarlo.

- **Borrar**: Se utiliza para borrar la partición que tenemos seleccionada en el momento de pulsar el botón en la sección **Particiones presentes en el disco**. Se le pedirá confirmación en el caso de que quiera borrar cualquier partición.
- **Reiniciar**: Se utiliza para restaurar **Disk Druid** a su estado original. Todos los cambios efectuados se perderán si selecciona **Reiniciar** las particiones.
- **Creación del dispositivo RAID**: La **Creación del dispositivo RAID** puede ser utilizada si quiere proporcionar redundancia a cualquier partición del disco.*Debería utilizarla tan sólo si tiene experiencia con RAID.*

4.2.2.1.3 Campos de la partición

La diferentes etiquetas de cada partición presentan información sobre las particiones que está creando. Las etiquetas son las que siguen a continuación:

- **Dispositivo**: Este campo muestra el nombre del dispositivo de la partición.

- **Inicio**: Este campo muestra el sector de su disco duro en el que empieza la partición.
- **Fin**: Este campo muestra el sector en su disco duro en el que finaliza la partición.
- **Tamaño**: Este campo muestra el tamaño de la partición (en MB).
- **Tipo**: Este campo muestra el tipo de partición (por ejemplo, ext2, ext3, o vfat).
- **Punto de montaje**: Un punto de montaje es el lugar en la jerarquía de directorios a partir del cual un volumen existe; el volumen se "monta" en este lugar. Este campo indica dónde se montará la partición. Si la partición existe pero no se ha definido un punto de montaje, necesitará definir uno. Haga doble click sobre la partición o en el botón **Modificar** para cambiar los parámetros de la partición.
- **Formato**: Este campo muestra si la partición que se está creando se formateará.

4.2.2.1.4 Esquema de particionamiento

Las particiones que se realizaron fueron las siguientes:

- Una partición swap sirve para ampliar la memoria virtual que se usa para ejecutar los paquetes con mayor velocidad y es un aspecto fundamental en el sistema operativo. El tamaño de la partición swap es igual al doble de la cantidad de memoria RAM

que tiene el sistema. La computadora que se usó para prueba es de 128 entonces el swap será de 256.

- Una partición /boot (mínimo 50 MB) — la partición montada sobre /boot contiene el kernel del sistema operativo (que permitirá al sistema arrancar Red Hat Linux), junto a otros ficheros utilizados para el proceso de arranque. Debido a las limitaciones de la mayoría de las BIOS de los ordenadores, se aconseja crear una partición pequeña para guardar estos ficheros. Para la mayoría de los usuarios, una partición de arranque de 50 MB es suficiente.
- Una partición root (1,5-3,7 GB) — aquí es donde se ubica "/" (el directorio raíz). En esta instalación, tiene los ficheros (excepto los almacenados en /boot) se encuentran en la partición raíz. La partición de root para la computadora de prueba es de 7GB.

4.2.2.2 Instalación de servicios Linux

4.2.2.2.1 Compartir archivos Linux en Windows

Para interactuar con archivos Windows se debe instalar el paquete Samba, el mismo que se encuentra incluido en los discos de instalación de Linux.

Para instalar este paquete se siguen los siguientes pasos:

1. Verificar si esta instalado este paquete con la instrucción desde el shell:

rpm –qa samba*

- Debe existir instalados mínimo tres paquetes Samba:

  a) Samba

  b) Samba Client

  c) Samba -common

2. Si no esta instalado se debe proceder de la siguiente manera:

   - Montar el ficheros para la instalación

     # mount /dev/CDROM/RedHat/RPM /mnt/CDROM

   - Instalar mediante la instrucción

     # rpm –ihv Samba*

3. Configurar el fichero smb.conf ubicado en el directorio /etc/samba/

   - Editar el fichero smb.conf con MC o cualquier editor de comandos. Se debe modificar lo siguiente:

     Workgroup =TSUTC

     Server String = Servidor Linux

     Security= share

     [Public]

     comment= documentos compartidos

     path=/home/doc

4. Conceder permisos para el fichero compartido /home/doc

   #chmod 777 /home/doc

   # ls all

5. Activar samba escribiendo en la shell:

```
# ntsysv
```

Activando con la barra espaciadora el servicio: smb(*)

4.2.2.2.2 Compartir archivos Windows en Linux

Los archivos Windows contienen el protocolo típico NetBeui y el tipo de archivo que administra es el FAT, este para comunicarse con los ficheros ext2 ó ext3 lo hacen a través del protocolo smbfs que se añade al instalar Samba. Para lo cual se debe montar los archivos Windows de la siguiente forma:

```
#mount –t smbfs –o username=SMSM,password=SMSM
//maquina1/Dos /Home/doc
```

4.2.2.2.3 Conexión con Internet

Para la habilitación del la conexión a Internet se tiene que crear un archivo en donde se encuentren las reglas del Firewall para permitir la navegación por Internet con los pasos siguientes:

- Crear un archivo con el nombre de Firewall, colocando en la shell lo siguiente:

```
#vi Firewall
: wa !
```

- En el cual se necesita agregar el siguiente código

iptables –F

iptables –t nat –F

iptables –t nat A POSTROUTING –o ppp0 –j MASQUERADE

iptables –A FORWARD –I eth0 –j ACCEPT

- Grabarlo el archivo en el directorio /usr/local/bin
- Colocar el getway la dirección IP a rutear 10.10.1.20. Con el fin de verificarsi está bien instalado se procede a escribir:

route

- Sino se visualiza la dirección Ip del getway se procede a cambiar la "dirección de puerta de enlace predeterminada" en la configuración de red.
- Para ejecutar el fichero Firewall se procede como sigue:
  a) Establecer permisos: # chmod 777 firewall
  b) Ejecutar : # ./ Firewall
  c) Para verificar, listar las reglas IP activas : # iptables –L
- Para que esta configuración se active al reiniciar la computadora se debe editar el fichero /etc/rc.local y colocar el path del fichero al final del texto: /usr/local/bin/Firewall.

4.2.2.2.6 Servidor WEB

Para tener este servicio se debe instalar el paquete **Apache** de la siguiente forma:

- Montar el fichero de instalación.

- Si esta el fichero comprimido, solo se presiona <Intro> para descomprimirlo
- Copiar el fichero descomprimido en /usr/local/src en el cual se encuentran todos los códigos fuentes.
- Instalar siguiendo escribiendo en el shell los siguiente paso:
    1. # ./ configure –prefix=/usr/local/apache –activate –module=src/modules/php4/libphp4a
    2. # make
    3. #make install

- Al final de la instalación se necesita levantar el servidor Web, ubicado en: /usr/local/apache/bin/apachectl start

  Ejecutar: # ./apachectl start
- Para verificar si esta funcionando Apache:

  # ps -aux | grep apache

  # ps - aux | grep http

4.2.2.2.7 Configuración de e-mail (Send mail)

Para la configuración del e-mail en Linux se necesita crear el DNS con el nombre de Dominio tesis.com, con los pasos siguientes:

1. Editar los ficheros:

   /etc/named.conf

   /etc/named/named x

/etc/named/named.forward

2. Activar el servicio Named mediante la siguiente instrucción en la shell:

   # ntsysv

3. Levantar el servicio mediante la instrucción:

   # service named restart

4. Verificar el si esta funcionando adecuadamente el DNS con la siguiente instrucción en la shell:

   # ping www.tesis.com

5. Configurar los fichero de configuración de e-mail, editando los archivos:

   /etc/mail/local-host-names

   /etc/mail/access

   /etc/mail/sendmail.mc

6. Compilar en la shell lo que sigue:

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

7. Activar los servicios imap, imaps, ipop2, ipop3s, ipop3

   # ntsysv

8. Crear usuarios para que se activen sus cuentas respectivas.

4.2.2.2 Instalación del sistema de seguridad para Linux Red Hat

Después de obtener el paquete o descargar iptables, se debe descomprimir. Para descomprimir se utiliza la orden:

bzip2 -cd iptables-1.2.5.tar.bz2 | tar -xvf

El paquete descomprimido debe estar en el directorio iptables-1.2.3/, para llevar a cabo la instalación, conviene consultar el fichero iptables-1.2.3/INSTALL, donde se indica como instalarlo, será algo muy similar a esto:

```
cd /root/iptables-1.2.2
make KERNEL_DIR=/usr/src/linux BINDIR=/usr/bin
LIBDIR=/usr/lib MANDIR=/usr/man
make install KERNEL_DIR=/usr/src/linux BINDIR=/usr/bin
LIBDIR=/usr/lib MANDIR=/usr/man
```

En las distribuciones RedHat superiores a la 7.1, el Kernel que se instala por defecto y viene configurado. Además también se incluye el paquete de iptables y si se selecciona en la instalación, aparece configurado. El único problema, es que puede que ipchains (Firewall para versiones inferiores a 7.1) este habilitado también. Para deshabilitar del arranque del sistema evitando que no cause conflictos con iptables basta ejecutar:

```
chkconfig --level 0123456 ipchains off; service ipchains stop
```

Finalmente, para arrancar el servicio iptables en el arranque del sistema ejecutaremos el comando siguiente:

```
hkconfig --level 235 iptables on; service iptables start
```

Naturalmente, no hay ninguna regla activa. Las reglas creadas con el comando iptables se almacenan solamente en RAM, es decir, que si

reiniciamos el sistema tras haber configurado varias reglas de iptables, éstas se perderán y tendremos que volver a teclearlas. Para incluir las reglas al inicio del sistema, podemos hacer varias cosas. La primera, editar el archivo script /etc/rc.d/init.d/iptables, éste script se ejecutará cada vez que se inicie el servicio iptables, que hemos configurado antes para iniciarse con el sistema. Otra opción, es introducir las reglas mediante el comando iptables y cuando el cortafuegos funcione como es debido, salvarlas en el fichero /etc/sysconfig/iptables. Es decir, introducimos las reglas de filtrado, y cuando el cortafuego funcione como esperamos, ejecutamos:

/sbin/service iptables save

Esto hace que el script de inicio de iptables (rc.d) ejecute el programa /sbin/iptables-save y escriba la configuración actual de iptables en el fichero /etc/sysconfig/iptables. Este fichero debería ser de sólo lectura para el usuario root, para que las reglas de filtrado de paquetes no sean visibles por el resto de los usuarios. La próxima vez que se inicie el sistema, el script de inicio de iptables volverá a aplicar las reglas guardadas en /etc/sysconfig/iptables usando el comando /sbin/iptables-restore.

Finalmente, podemos desinstalar el paquete de ipchains con el comando:

rpm -e ipchains

4.2.2.3 Estructura y funcionamiento de iptables.

Comentamos al principio del documento, que el módulo netfilter, integraba tres posibilidades en el manejo de los paquetes, cada una de esas posibilidades, se corresponde con una tabla donde se aplican las reglas. Con la opción iptables –t *tabla*, especificamos la tabla sobre la que queremos trabajar. Estas tablas son *filter*, *nat* y *mangling*. Veamos que

podemos hacer sobre cada una de ellas:

- ***nat***: La tabla *nat* se utiliza para configurar el protocolo de Network Address

Translation. Cuando un flujo de paquetes (una conexión TCP) atraviesa la tabla, el

primer paquete es admitido, el resto, son automáticamente identificados como parte del flujo de ese primer paquete y de manera automática se llevan a cabo sobre ellos las operaciones NAT o de enmascaramiento. Esta es la razón por la cual, no se lleva a cabo ningún tipo de filtrado en esta tabla. La tabla de *nat* tiene tres *chains* o cadenas sobre las que podemos añadir reglas. La cadena PREROUTING se utiliza para alterar los paquetes tan pronto llegan al cortafuegos (DNAT o NAT del destino). La cadena OUTPUT, se utiliza para alterar los paquetes generados localmente en el cortafuegos, antes de tomar ninguna decisión de enrutado. Finalmente tenemos la

cadena POSTROUTING para alterar los paquetes que acaban de dejar el cortafuegos (SNAT o NAT en el origen).

- ***mangle***: La tabla de *mangling* o "manipulación", permite manipular otros elementos de los paquetes, como el TTL, el TOS, etc..., ha excepción del NAT, que se realiza en la otra tabla. La funcionalidad de esta tabla está en expansión y aunque potencialmente puede ser muy valiosa, no tiene demasiada utilidad (salvo a hackers). Consta de dos cadenas, PREROUTING y OUTPUT.

- ***filter***: Esta es la reina de la casa. En la tabla *filter*, se llevan a cabo la funcionalidad principal de iptables, el filtrado de paquetes. Como las anteriores, consta de varias chains predefinidas, en este caso INPUT, FORWARD y OUTPUT. La primera hace referencia a los paquetes entrantes cuyo destino es el propio cortafuegos. La segunda se emplea para decidir que hacer con los paquetes que llegan al cortafuegos y tienen como destino otro host, así podemos decidir si encaminarlos o no. Por último, la cadena OUTPUT se utiliza para filtrar paquetes generados en el propio host con destinos externos.

Cuando un paquete entra en el cortafuegos, lo hace a través de alguna interfaz (tarjeta de red, MODEM...). El paquete se dirige al Kernel, entrando en las distintas cadenas de las tablas sólo si procede. En la figura que ofrecemos posteriormente, puede observarse el esquema general del procesado de paquetes en iptables. En la tabla siguiente podemos ver también ejemplos de las

desventuras de los paquetes en su tránsito por el módulo netfilter del kernel.

4.2.2.4 Pruebas de estabilidad y fiabilidad de la red informática

La estabilidad y fiabilidad en la red de la Universidad, es el producto entre compaginar restricciones y premisos autorizados. Para lo cual es necesario priorizar los servicios a los diferentes usuarios. Según la arquitectura de seguridad de red del diseño 4.1 el servidor Linux se conecta con un cliente Windows en donde comparten archivos según las políticas de seguridad enunciadas anteriormente. El servidor Linux tiene instalados los servicios de Php, Mysql, Apache, Samba.

Para la ejecución del sistema de seguridad se necesario encender tanto el servidor como el cliente y además entrar en una sesión de red. En el servidor Linux es conveniente ingresar como un <superusuario> para realizar cambios y modificaciones al kernel.

La actividad se basa esencialmente en tratar de acceder a diferentes servicios del servidor Linux a través del cliente Windows con el fin de determinar el grado de vulnerabilidad o certeza del Firewall, para lo cual se usaron las siguientes herramientas:

Linux	
Amenaza	**Seguridad**
Nmap.- Herramienta de exploración de puertos abiertos, elementos activos y sistema operativo.[4] Ping : # nmap –sF 192.168.1.0/24 –oN	*Snort.*- Es un sistema de detección de intrusos(IDS), este escucha las solicitudes de apertura de puerto, además dispone de firmas de autores públicos.[5]

[4] http://www.insecure.org/nmap.
[5] http://www.snort.org

Puertos: # nmap –I 192.168.1.10 Sistema Operativo: # nmap -O 192.168.1.10	
Herramientas de Linux Red Hat *Showmount.*- Explora elementos compartidos en Linux: # showmount –e 192.168.202.34 *Finger:* Muestra los recursos compartidos de los usuarios activos y su tiempo de actividad, debajo de finger en la cadena alimenticia se encuentra las utilidades rusers y rwho. # finger 0@192.168.202.34 # rwho 192.168.202.34 # rusers –l 192.168.202.34	Cortafuegos.- Usar un Firewall para Linux como es Iptables para asegurar que los Firewall filtre los paquetes a los puertos 111, 32771.
Nfs.-Exploración de recursos en un cliente nfs que funciona con el FTP, el cual consta en la siguiente dirección:[6] # nfs	Si no son necesarios deberían desactivar los **nfs** de los servidores relacionados tales como mound, statd y loockd, utilizar controles de acceso y de aplicaciones clientes y usuarios para permitir únicamente el acceso a los archivo a los usuarios autorizados.
Vulnerabilidades de Composición de Contraseña Crack.- Es una herramienta disponible para localizar la contraseña.[7] # John passwd Ejecutando John y colocando el archivo de con contraseña que se desea descifrar, los ficheros más comunes de contraseñas están en el directorio: /etc/passwd	Colocar una buena contraseña

Tabla 4.2 Pruebas de estabilidad para Linux

[6] ftp://ftp.cs.vv.nl/pub/leendert/nfsshell.tar.97
[7] http://www.openwall.com/john

Las pruebas mediante estos los servicios de red enunciados en la tabla 4.3 con su respectivo porcentaje de vulnerabilidad, representa la eficacia del Firewall Iptables y la satisfactoria seguridad para una red.

4.3 Análisis de Resultados del sistema de seguridad.

Los resultados de las pruebas obtenidas permite evaluar la funcionalidad del software Iptables, con lo cual se observa la capacidad y el alcance muy amplio en el campo de Seguridad Informática.

El Firewall Iptables con sus virtudes es por lo tanto el Firewall de Linux que bien se podría instalar en el servidor Linux de la Universidad, ya que presenta una interfaz grafica de fácil manejo, e interacción para el administrador de red.

- Seguridad: con una mejor seguridad para los puertos(ftp, telnet, http, smtp).
- Fiabilidad: los recursos que la Institución posee, son fiables con la seguridad que brinda el Iptables.
- Escalabilidad: los productos de Iptables poseen versiones en escala.
- Facilidad de configuración: su interfase gráfica facilita la configuración e instalación.
- Soporte en línea: lo realiza muy eficazmente, proporcionado por Red Hat en www.redhat.es/
- Conocimiento: Los Iptables consta con comandos en ingles que se tornan fáciles para la asimilación.

- Funcionabilidad: el funcionamiento y puesta en marcha es muy eficaz para las necesidades de la Universidad.
- Documentación: existen manuales del software fáciles de entender en la dirección: http://www.redhat.es/soport.
- Requerimiento adicional: no necesita adicionar a la red ningún software pues tan solo el Iptables que viene incorporado en el mismo sistema operativo.

CAPITULO V

5.1 Verificación de Objetivos e Hipótesis

Se realizó el análisis de la estructura de red informática de la Universidad Técnica de Cotopaxi, que comprende el estudio de la situación actual de los equipos informáticos, el análisis de las características de hardware, software e interconexión de red que poseen: Los Laboratorios de computación, Biblioteca, Departamento Financiero, Secretaría de Carreras, Usuarios Independientes y opcionales, por medio de encuestas realizadas al personal que labora en los mismos.

Se determinó las amenazas y vulnerabilidades que en la actualidad presenta la red informática de la Universidad Técnica de Cotopaxi, para describir en que condiciones informáticas se encuentra la misma.

Buscar, analizar y comparar alternativas de seguridad que proporcionen protección a la red informática de la Universidad Técnica de Cotopaxi, se realizó mediante un estudio de factibilidad operativa, técnica, económica, de los Firewall a nivel de Hardware y Software logrando la selección del mejor Firewall para los sistemas operativos Linux y Windows 2000 Server con sus respectivas conclusiones y recomendaciones.

Se determinó las políticas de seguridad consideradas necesarias para la red informática, que permitirá la integridad de los recursos Informáticos en la Red de la Universidad Técnica de Cotopaxi.

Se realizó la demostración de la seguridad informática propuesta, a través de herramientas hackers, para lo cual fue necesario instalar y configurar los sistemas operativos Linux red hat 7.3 y Windows 2000 Server con su respectivo Firewall software IpTable y Outpots,.

Para la propuesta se realizó un estudio de Firewall Hardware (Cisco Secure Pix 525) entre la señal de Internet y el servidor Linux Red hat 7.3, la función principal es filtrar la información de los usuarios externos y en caso de vulnerar al Firewall hardware (Cisco secure Pix 525) se presenta el Firewall Software para el Servidor Proxy llamado Iptables que es un programa que posee el sistema operativo Linux .Una medida de protección para el servidor de correo electrónico es instalar un segundo Firewall Hardware (Cisco secure Pix 525) con el fin de impedir el acceso a estudiantes o personas de la red LAN Interna que no tengan el permiso correspondiente de esta manera proteger de los intrusos internos. Esto permite una mayor confiabilidad en la información tanto externa como interna; con lo que se ha dado cumplimiento de proponer un sistema de seguridad informático para la red de datos de la Universidad Técnica de Cotopaxi.

5.2 Conclusiones:

En base al desarrollo de la tesis se ha concluido lo siguiente:

- El objetivo de la seguridad informática es el de proteger y fortalecer los recursos de todo el entorno computacional, con el fin de evitar que intrusos ingresen a la confídenciabilidad de los datos de la Universidad Técnica de Cotopaxi. La aplicación de un buen sistema de seguridad ayuda a cumplir con el propósito de la seguridad informática mediante la instalación de un Firewall, el cual constituye la alternativa ideal porque se acopla al diseño actual de la red y cubre los vacíos de seguridad en la red de datos de la U. T.C.

- El diseño propuesto presenta la forma óptima de protección para la red de datos de la Universidad, dicha propuesta demanda de varios recursos, sin embargo beneficiará a la integridad de los datos, no obstante la demostración es la forma básica que un sistema de información posee para cumplir con los objetivos de la seguridad informática y conseguir de esta forma fiabilidad y estabilidad en todos los datos que ingresen o salgan de la Universidad y además prestar un mejor servicio a todos los usuarios.

- Para la elección del Firewall software se ha considerado el sistema operativo instalado en el servidor y de acuerdo a ello seleccionar el más adecuado, según las políticas de seguridad propuestas, para el Firewall hardware se ha tomado en consideración la arquitectura de la red de datos de la Universidad para obtener el mejor rendimiento del sistema de seguridad.

- Mediante el estudio realizado se consideró tres alternativas por grupo de Firewalls, resultando como la mejor alternativa para el sistema operativo Windows 2000 Server el Firewall Outpost, para Linux el Firewall Iptables y Cisco Secure Pix 525 para el Firewall Hardware.

- La mejor forma de fortalecer la seguridad es promover actitudes maduras y responsables entre los usuarios. La verdadera seguridad solo se puede obtener a través de una adaptación libre y con principios de comportamiento aceptado por parte de los usuarios. Este compromiso aumentará a medida que la sociedad en conjunto tenga una mayor cultura informática y los usuarios comprendan el valor personal de la tecnología que utilizan.

5.3 Recomendaciones:

En el transcurso de la elaboración del presente trabajo se ha hallado las siguientes recomendaciones:

- Los sistemas de seguridad son útiles para mantener la fiabilidad de la información que circula a través de la red y para protegerla en mayor medida de personas inescrupulosas con fines de dañar esa información. Es importante, eso sí, que se eduque a la población informática, para que sepa como defenderse y protegerse, y además que se haga conciencia del valor de la información y de la gravedad del perjuicio a la misma.

- Para un mejor desempeño del administrador de red, es recomendable crear un departamento sistemas. Mediante el cual se puede trabajar mejor y no tener problemas respecto a la funcionalidad de la red, por el exceso de trabajo a pocas personas.

- El éxito o fracaso de instalar un sistema de seguridad depende de una buena arquitectura de seguridad de red, en donde deben estar detallados cada uno de los elementos que forman parte de dicha arquitectura, para no tener en el futuro contratiempos en la configuración por no tener todos los dispositivos contemplados en la arquitectura de red y además conocer el funcionamiento adecuado para poder cambiar las claves predeterminadas, puesto que si no se cambia estas claves el Firewall no beneficia en ninguna forma a la Universidad, porque es fácilmente vulnerable por los intrusos que tienen conocimiento sobre las claves, por defecto de los fabricantes.

BIBLIOGRAFIA

LIBROS

Arq. Ulloa Francisco, Investigación 2000.

Cobb, Stephen, Manual de seguridad para PC y redes locales, Madrid : McGraw-Hill, c1994.

Comer & Douglas, TCP/IP : redes globales de información con Internet México, Prentice Hall, c1996.

Eckel, George, Construya un servidor de internet con UNIX, México : Prentice Hall, c1996.

Forley, Marc, TOM STERORMS, JEFFREY MSU, Guía LAN TIMES de seguridad e integridad de datos 1997, México

Hahn& Harley, Internet : Manual de Referencia, Madrid : Osborne \ McGraw-Hill, c1994.

Karanjit & Siyan, Firewalls y la seguridad en internet México :Practice – Mall Hispanoamericano, S.A (1997)

Kris Jamsa y Ken Cope.(240)
Programación de Internet : El Mejor Curso sobre TCP-IP
México : McGraw-Hill, c1996.

Sheldon, Tom
Manual de seguridad de windows NT
Madrid : Osborne/McGraw-Hill. Xxvi

Sheldom Tom, Guia de interoperabilidad para redes, Osborne \ McGraw-Hill, c1996

DIRECCIONES ELECTRONICAS

Hacker mas famoso del mundo:

[http://www.el-mundo.es/navegante/99/marzo/18/mitnick.html], Lunes 11 de Febrero del 2002

Acción de hacker más sonada del mundo:

[http://www.el-mundo.es/navegante/98/septiembre/14/times.html], Miércoles 20 del Marzo del 2002.

Manual de la seguridad

[http://www.fundaciondike.org/notas/manualseguridad.htm], Martes 16 de Abril del 2002

Firewalls para Linux

[www.secuerepoint.cc/products], miércoles 15 de mayo del 2002

[http://www.its-intl.com/es/services/conectividad/seguridad/firewall.html], Lunes 10 de Junio del 2002

[http://www.linuxguruz.org/iptables], Viernes 19 de Julio del 2002

Firewall para Windows 2000 Server

[www.agnitum.com] , Jueves 15 de agosto del 2002

[www.kerio.com], Miércoles 18 de septiembre del 2002

[www.tinysoftware.com], Martes 22 de octubre del 2002

Laboratorio de Redes:

[http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html], Jueves 21 de noviembre del 2002

Firewall Hardware

[http://monografias.preciomania.com/search_attrib.php/], Viernes 10 de Enero del 2003

[http://www.cisco.com/en/US/products/hw/vpndevc/pc2030/index.html], Miércoles 12 de Febrero del 2003

[http://www.tribecaexpress.com/Cisco_PIX_501.htm], Martes 18 de Febrero del 2003

[http://www.tribecaexpress.com/Fortinet_Fortigate.htm], Martes 4 de Marzo del 2003

[http://www.linuxguruz.org/iptables/], Lunes 17 de Marzo del 2003

INSTALACIÓN DE LINUX

[www.redhat.es/], Martes 8 de Abril del 2003

[http://www.redhat.es/soport], Martes 8 de Abril del 2003

Pruebas con Windows

[http://www.foundstone.com], Jueves 1 de Mayo del 2003

[http://www.indiesoft.com], Viernes 2 de Mayo del 2003

[http://www.somarsoft.com], Lunes 5 de Mayo del 2003

Pruebas con Linux

[http://www.insecure.org/nmap], Lunes 2 de junio del 2003

http://www.snort.org], Martes 3 de Junio del 2003

[ftp://ftp.cs.vv.nl/pub/leendert/nfsshell.tar.97], Miércoles 4 de Junio del 2003

[http://www.openwall.com/john], Jueves 5 de Junio del 2003

Demostración de seguridad

[www.sistemseguridad.com], Martes 8 de julio del 2003

Piratas informáticos:

Sniffit

[http://reptile.rug.ac.be/~coder/sniffit/sniffit.html], Lunes 4 de Agosto del 2003

Spak

[http://freeport.xenos.net/~xenon/software/spak/index.html], Martes 5 de Agosto del 2003

Libnet

[http://www.packetfactory.net/libnet/], Miércoles 6 de Agosto del 2003

ANEXOS

ANEXO 1

ANÁLISIS DE LAS ENCUESTAS REALIZADAS A LOS LABORATORIOS DE COMPUTACIÓN

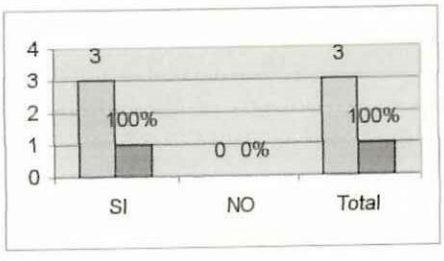
Las siguientes encuestas fueron realizados a los Operadores del centro de computo:

1 ¿Existen procedimientos y control para detectar el ingreso a los servidores por personas no autorizadas?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



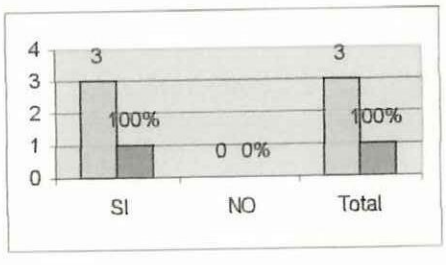
El 100 % de encuestados contestaron que si existe procedimientos para detectar el ingreso a los servidores por personas no autorizadas.

2. ¿Existe un plan de contingencia en caso de fallar el servidor principal?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



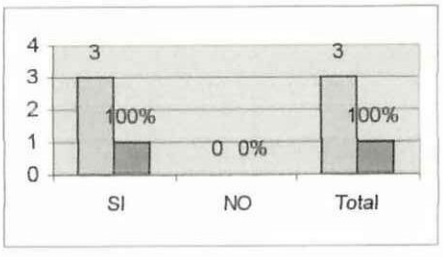
Al encuestar acerca de que existe o no un plan de contingencia en caso de fallar el servidor, el 100 % contestaron positivamente.

3. ¿Se encuentra capacitado el personal en caso de presentarse algún problema con los servidores?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



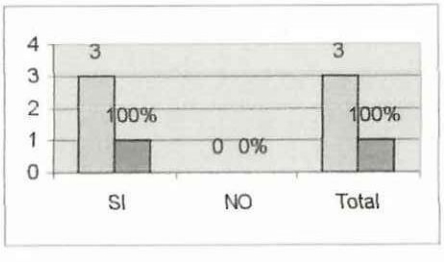
El 100% de encuestados se encuentran capacitados en caso de presentarse algún problema en los servidores.

4. ¿El servidor es apropiado para el trabajo que desempeña el departamento?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



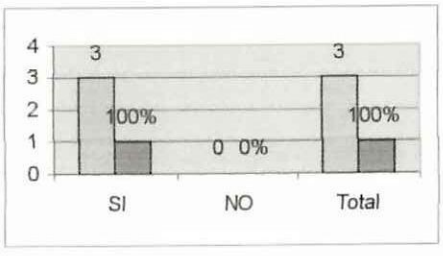
Al determinar que el servidor de Linux es apropiado para el trabajo que desempeña el departamento para administrar los laboratorios, el 100% contestaron que si.

5. ¿El software que se encuentra instalado en los servidores posee licencias?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



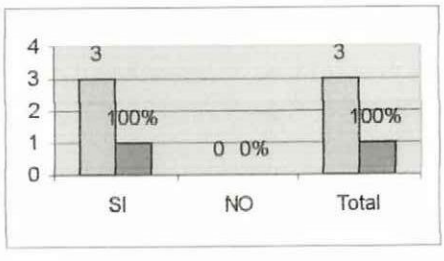
El 100 % de encuestados contestaron que el software instalado en los servidores poseen su respectiva licencia.

6. ¿Existe un control sobre la red?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



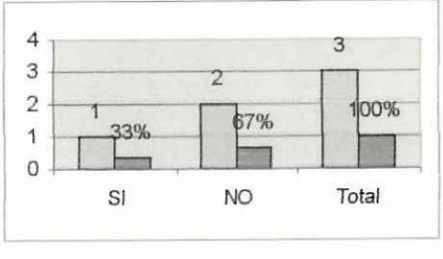
Al encuestar acerca del control sobre la red el 100% contestaron afirmativamente.

7. ¿Considera Ud. que la velocidad de la red es apropiada?

Tabla estadística

	No.	Porcentaje
SI	1	33%
NO	2	67%
Total	3	100%

Gráfico de Barras de la tabla Estadística



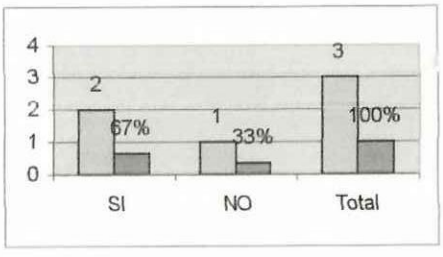
El 67% de encuestados consideran que la velocidad de la red no es apropiada; mientras que el 33% contestaron lo contrario.

8. ¿Existe antivirus para las computadoras del centro de computo?

Tabla estadística

	No.	Porcentaje
SI	2	67%
NO	1	33%
Total	3	100%

Gráfico de Barras de la tabla Estadística



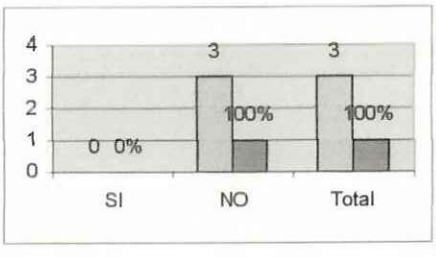
El 67% de encuestados contestaron que si existen antivirus para proteger la red informática, y el 33% contestaron que no.

9. ¿Existe un cuarto de equipos para la administración institucional?

Tabla estadística

	No.	Porcentaje
SI	0	0%
NO	3	100%
Total	3	100%

Gráfico de Barras de la tabla Estadística



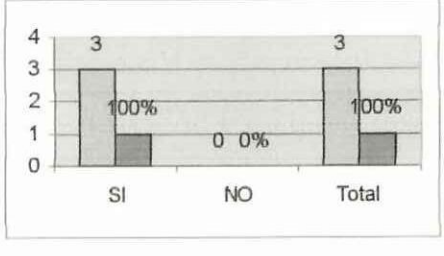
Al encuestar se obtuvo que el 100% contestaron que no existe un área donde se concentren todos los dispositivos que son parte de la red informática.

10. ¿Posee su departamento acceso a Internet?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



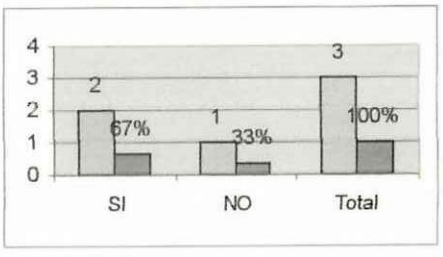
El centro de computo posee acceso a Internet por medio de la empresa IMPSAT.

11. ¿Considera Uds. Bueno este servicio que proporciona el proveedor de Internet?

Tabla estadística

	No.	Porcentaje
SI	2	67%
NO	1	33%
Total	3	100%

Gráfico de Barras de la tabla Estadística



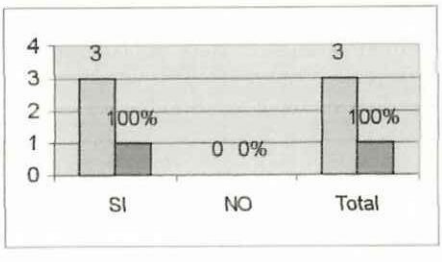
El 67% de encuestados indican que el servicio de Internet proporcionado por la empresa IMPSAT, es bueno; mientras que el 33% dicen lo contrario.

12. ¿Es restringido la clave de acceso a Internet?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



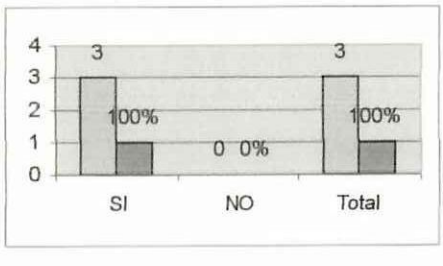
El 100% indican que la clave para el uso de Internet es restringida y la conocen únicamente los administradores y ayudantes.

13. ¿Cada que tiempo se cambia la clave de Internet y quien lo realiza?

Tabla estadística

	No.	Porcentaje
SI	3	100%
NO	0	0%
Total	3	100%

Gráfico de Barras de la tabla Estadística



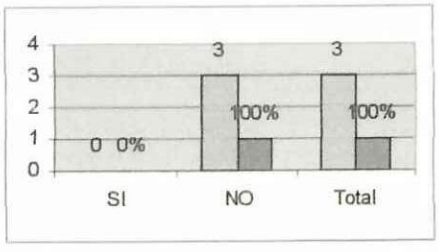
El 100% de encuestados mencionan que la clave para el uso de Internet se cambia diariamente por los administradores.

14. ¿Se divulga la clave de Internet por parte de los ayudantes del centro de computo?

Tabla estadística

	No.	Porcentaje
SI	0	0%
NO	3	100%
Total	3	100%

Gráfico de Barras de la tabla Estadística



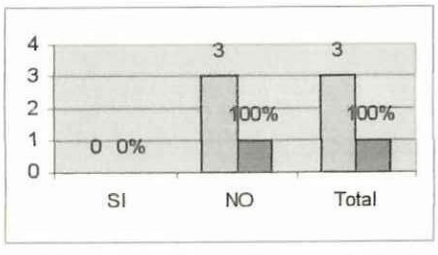
El 100% de los encuestados expresan que la clave de Internet es de uso exclusivo de los administradores.

15. ¿Existe algún manual o reglamento que trate acerca de la seguridad para el control de los servidores, red de datos e Internet?

Tabla estadística

	No.	Porcentaje
SI	0	0%
NO	3	100%
Total	3	100%

Gráfico de Barras de la tabla Estadística



El 100 de encuestados contestaron que no existe un reglamento de seguridad para los servidores para red de datos e Internet

INTERPRETACION DE RESULTADOS DE LOS LABORATORIOS DE COMPUTACIÓN

Los resultados son producto de cada una de las preguntas encuestadas, mediante la cual se ha obtenido las siguientes conclusiones:

Conclusión 1.- Los administradores controlan el ingreso de la áreas restringidas de los laboratorios para tener mayor seguridad en los servidores.

Conclusión 2.- Un mecanismo de seguridad es poseer un servidor auxiliar en caso de fallar el principal, así de esta manera se precautela que la red informática continúe trabajando normalmente.

Conclusión 3.- El personal es eficiente para desempeñar la función de administradores de la red informática, sin embargo falta capacitación por parte de la institución.

Conclusión 4.- El servidor es apropiado y se encuentra en perfectas condiciones, puesto que el mismo es innovado con tecnología actual.

Conclusión 5.- Las licencias de los software de los servidores se encuentran registradas de forma legal acordes a las leyes informáticas.

Conclusión 6.- Por medio de los ayudantes se controla el ingreso a las computadoras, de esta manera se vigila la red informática.

Conclusión 7.- Para un adecuado funcionamiento de la red informática es necesario adecuar procesos tales como: depuración y afinamiento que permitirá obtener mejor rendimiento.

Conclusión 8.- La mayoría de encuestados deducen que si existen antivirus instalados en las computadoras, los mismos que están desactualizados, el ingreso de un virus informático producirá un colapso en los servidores.

Conclusión 9.- Al no poseer la Institución educativa un cuarto de equipos, están propensos a ser averiados por personas no autorizadas, lo cual ocasionaría daños en los dispositivos activos que son parte de la red informática.

Conclusión 10.- El acceso a Internet es importante porque permite al usuario obtener información actualizada sobre temas de diferente índole.

Conclusión 11.- El servicio de Internet que proporciona IMPSAT cumple con las necesidades de navegación que solicitan los usuarios.

Conclusión 12.- La clave para el acceso al Internet la conocen los administradores y ayudantes para luego ser insertada en los diferentes usuarios que lo soliciten.

Conclusión 13.- Con esta medida de seguridad se precautela que los usuarios no puedan reconocer fácilmente la clave de acceso a Internet.

Conclusión 14.- La clave de Internet no es divulgada por los administradores o ayudantes con esta medida de seguridad se protege el servicio de Internet que proporciona el Centro de Computo.

Conclusión 15.- Al no poseer un reglamento para la seguridad en los servidores, red de datos e Internet está en riesgo de obtener la información fácilmente por cualquier usuario.

ANEXO 2

ANALISIS DE LOS USUARIOS OPCIONALES

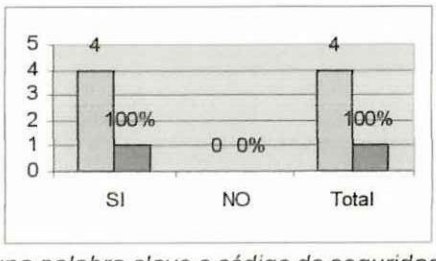
La encuesta es detallada a continuación son realizadas a las oficinas de Rectorado, Vicerrectorado, Relaciones Publicas y Dirección de CIYA:

1. ¿Esta su computador provisto de una palabra clave o código secreto de seguridad que restringe el acceso al **setup** de su computadora?

Tabla estadística

	No.	Porcentaje
SI	4	100%
NO	0	0%
Total	4	100%

Gráfico de Barras de la tabla estadística



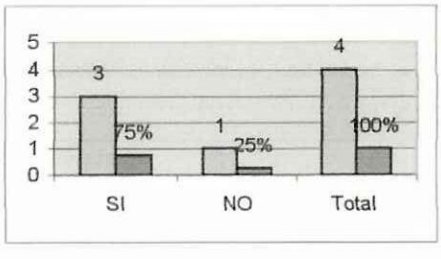
Con respecto que si el computador posee una palabra clave o código de seguridad para el acceso al setup los encuestados contestaron que si lo que equivale al 100%.

2. ¿Si la pregunta anterior es si. Con que frecuencia se cambia la clave de acceso?

Tabla estadística

	No.	Porcentaje
SIEMPRE	3	75%
NUNCA	1	25%
Total	*4*	*100%*

Gráfico de Barras de la tabla Estadística



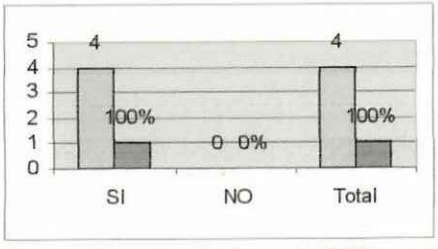
Al ver que la respuesta anterior es afirmativa los usuario indican que el 75% siempre cambian la clave de acceso del computador.

3. ¿En su computador posee un antivirus instalado?

Tabla estadística

	No.	Porcentaje
SI	4	100%
NO	0	0%
Total	4	100%

Gráfico de Barras de la tabla Estadística



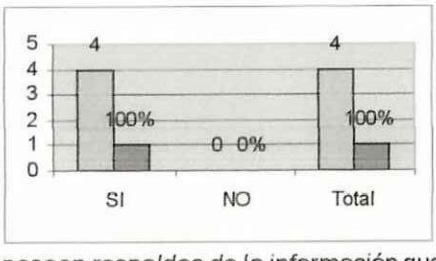
Con respecto a la instalación del antivirus en la computadora el 100% contestaron que si existe la instalación del mismo en cada una de las computadoras.

4. ¿Posee respaldos de la información de su oficina?

Tabla estadística

	No.	Porcentaje
SI	4	100%
NO	0	0%
Total	4	100%

Gráfico de Barras de la tabla Estadística



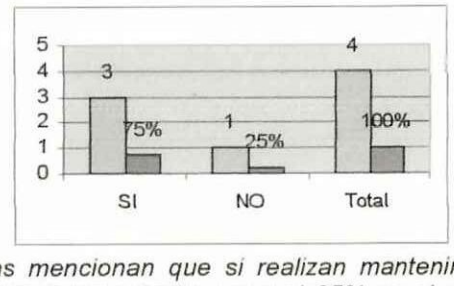
El 100% de los encuestados afirman que si poseen respaldos de la información que procesan.

5. ¿Se realizan mantenimiento preventivo o correctivo de la computadora?

Tabla estadística

	No.	Porcentaje
SI	3	75%
NO	1	25%
Total	4	100%

Gráfico de Barras de la tabla Estadística



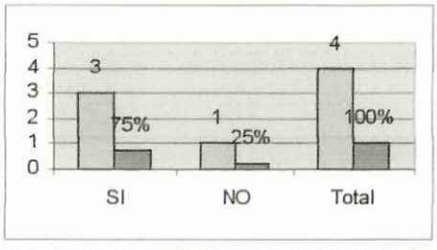
El 75% de las oficinas encuestadas mencionan que si realizan mantenimiento preventivo o correctivo de las computadoras; mientras que el 25% no ejecuta la función de mantenimiento.

6. ¿La computadora que esta en su oficina es apropiada para desempeñar su trabajo?

Tabla estadística

	No.	Porcentaje
SI	3	67%
NO	1	33%
Total	4	100%

Gráfico de Barras de la tabla Estadística



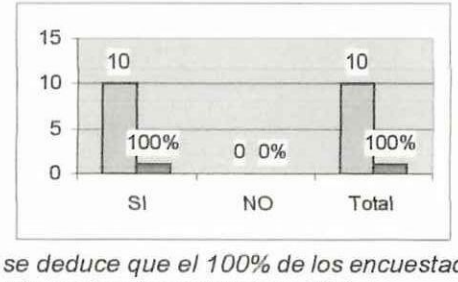
Al realizar las encuestas el 75% afirman que las computadoras son apropiadas para desempeñar su trabajo, lo que no sucede con el 25% donde deduce que no lo son.

7. ¿Tiene conocimientos suficientes sobre todos los programas que Ud tiene instalado en su computadora?

Tabla estadística

	No.	Porcentaje
SI	4	100%
NO	0	0%
Total	4	100%

Gráfico de Barras de la tabla Estadística



Con respecto a la preguntan anterior se deduce que el 100% de los encuestados se encuentran con conocimientos suficientes sobre los programas básicos

INTERPRETACIÓN DE RESULTADOS DE LOS USUARIOS OPCIONALES

Los resultados se derivan de cada una de la preguntas encuestadas, mediante lo cual se ha obtenido lo siguiente:

Conclusión1- Las encuestas realizadas en las principales oficinas de la Universidad Técnica de Cotopaxi se determinan que si poseen un password para ingresar al computador y poder realizar su trabajo de mejor manera.

Conclusión2.- Las oficinas encuestadas mencionan que cambian el password siempre lo que les permite obtener la información del computador con mayor seguridad.

Conclusión3.- existen antivirus instalados en las computadoras, lo que no confirma que los mismas se encuentren actualizados lo que podría ocasionar que las computadoras se infecten de virus informático.

Conclusión4.- Las personas quienes están a cargo de las oficinas mencionan que la fuente de respaldo que utilizan para guardar la información son los disquetes.

Conclusión5.- Las encuestas mencionan que es necesario realizar mantenimiento permanente de las computadoras para evitar daños en los mismos.

Conclusión6.- Las oficinas expresan que la computadora que se encuentra en su dependencia cumple con las características necesarias para desempeñar su trabajo.

Conclusión7.- El personal que labora en las diferentes dependencia perciben de conocimientos suficientes sobre los programas que se encuentran instalados en el computador.

ANEXO 3

ANÁLISIS DE LA RED DEL DEPARTAMENTO DE SECRETARIA DE CARRERAS Y FINANCIERO.

Las encuestas fueron realizadas a las siguientes oficinas en el Departamento Financiero: Dirección Financiera, Contabilidad y Auxiliar de Contabilidad, Guarda almacén y Tesorería.

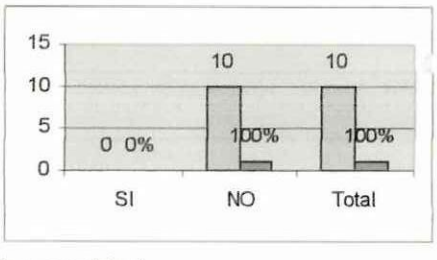
En secretaria de Carreras fueron las siguientes: Secretarias Ciencias Agropecuarias Ambientales y Veterinarias(CAAV), Secretaría de Carrera administrativas humanísticas y del Hombre(CC.AA.HH.H), Secretaría de Carrera de ciencias de la Ingeniería y Aplicadas(CIYA), Centro de Educación a Distancia, Centro de Investigación y Postgrado. Con las preguntas a continuación:

1. ¿Existe algún manual o reglamento que trate acerca de la seguridad física del departamento, de los equipos, y del software?

Tabla estadística

	No.	Porcentaje
SI	0	0%
NO	10	100%
Total	10	100%

Gráfico de Barras de la tabla Estadística



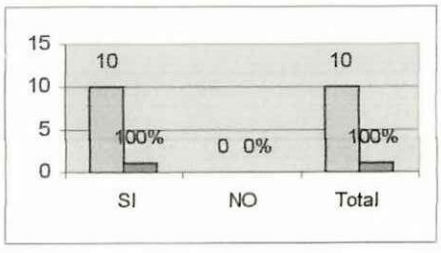
El 100% afirma que no posee un sistema de seguridad.

2. ¿Realiza respaldos o copias de la información que procesa?

Tabla estadística

	No.	Porcentaje
SI	10	100%
NO	0	0%
Total	100	100%

Gráfico de Barras de la tabla Estadística



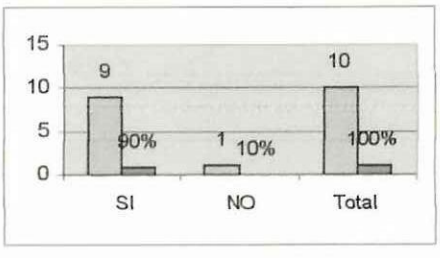
El 100% de los encuestados mencionan que si tienen respaldos de la información.

3. Existen manuales, documentación de importancia para desempeñar su trabajo?

Tabla estadística

	No.	Porcentaje
SI	9	90%
NO	1	10%
Total	100	100%

Gráfico de Barras de la tabla Estadística



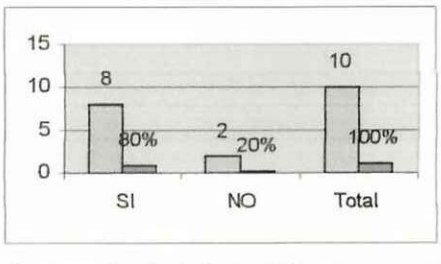
Al encuestar acerca de que si poseen manuales, documentación para el desempeño de su trabajo el 90% contesto que si, mientras que el 10% contesto que no.

4. ¿Se halla algún tipo de librería con llave para guardar los manuales, documentación, discos duros cintas magnéticas que son de importancia para el departamento?

Tabla estadística

	No.	Porcentaje
SI	8	80%
NO	2	20%
Total	10	100%

Gráfico de Barras de la tabla Estadística



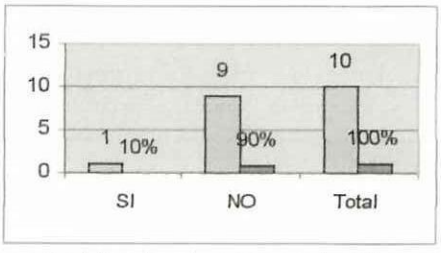
El 80% posee algún tipo de librería para sobreguardar la información que se procesa durante el periodo académico, mientras que el 20% no lo dispone de mencionado mueble.

5. ¿Tienen acceso a estos manuales y documentación otras personas?

Tabla estadística

	No.	Porcentaje
SI	1	10%
NO	9	90%
Total	100	100%

Gráfico de Barras de la tabla Estadística



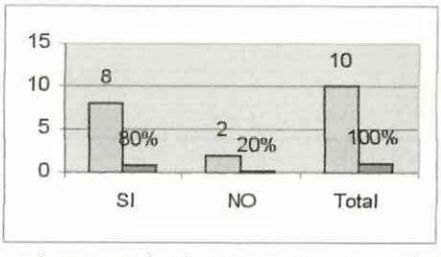
El 90% de los encuestados contestaron que es restringido el acceso a la información a otras personas, en cambio el 10% manifestaron que tienen acceso a la documentación otras personas.

6. ¿Esta su computador provisto de una palabra clave o código secreto de seguridad que restringe el acceso del **setup** de su computadora?

Tabla estadística

	No.	Porcentaje
SI	8	80%
NO	2	20%
Total	10	100%

Gráfico de Barras de la tabla Estadística



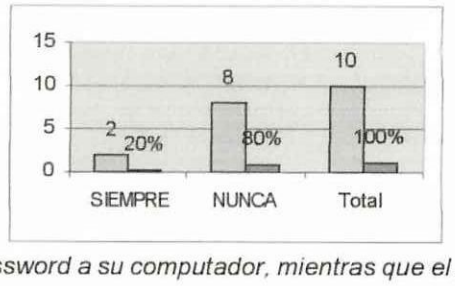
El 80% de los encuestados poseen un password para poder ingresar a su computadora y realizar su trabajo, mientras que el 20% carece de mencionada seguridad.

7. ¿Se cambia con frecuencia la palabra clave o código secreto del **setup**?

Tabla estadística

	No.	Porcentaje
SIEMPRE	2	20%
NUNCA	8	80%
Total	10	100%

Gráfico de Barras de la tabla Estadística



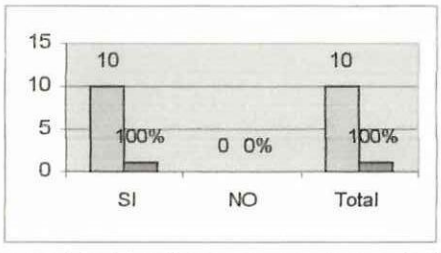
El 80% de los encuestados no ratifican el password a su computador, mientras que el 20% con frecuencia cambian la clave de ingreso.

8. ¿Es restringido el acceso a su computador personas no autorizadas?

Tabla estadística

	No.	Porcentaje
SI	10	100%
NO	0	0%
Total	10	100%

Gráfico de Barras de la tabla Estadística



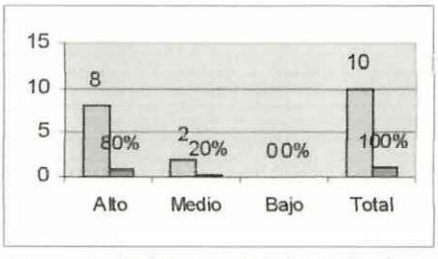
El 100% de los encuestados afirmaron que es restringido el acceso a su computador por personas impropias a su departamento.

9. ¿Que importancia tiene la información en su computador?

Tabla estadística

	No.	Porcentaje
Alto	8	80%
Medio	2	20%
Bajo	0	0%
Total	10	100%

Gráfico de Barras de la tabla Estadística



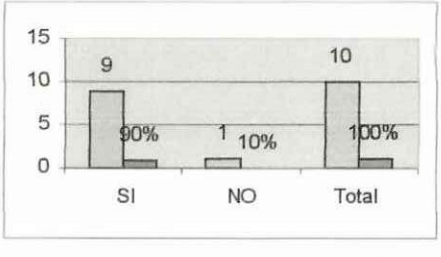
El 80% manifestaron que los datos que tiene su computador son muy importantes para el desenvolvimiento del departamento, sin embargo el 20% afirman que su información sirve para complementar el funcionamiento del departamento.

10. ¿El software con que usted trabaja funciona correctamente?

Tabla estadística

	No.	Porcentaje
SI	9	90%
NO	1	10%
Total	10	100%

Gráfico de Barras de la tabla Estadística



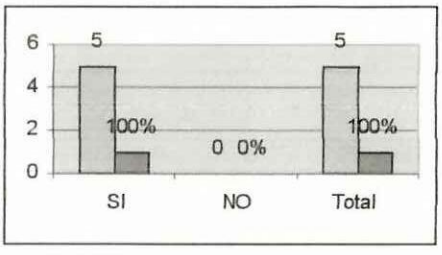
El 90% de los encuestados afirmaron que el software que dispone para laborar sus funciones esta funcionando correctamente y el 10% manifestó lo contrario.

11. ¿En su computador posee un antivirus instalado?

Tabla estadística

	No.	Porcentaje
SI	10	100%
NO	0	0%
Total	10	100%

Gráfico de Barras de la tabla Estadística



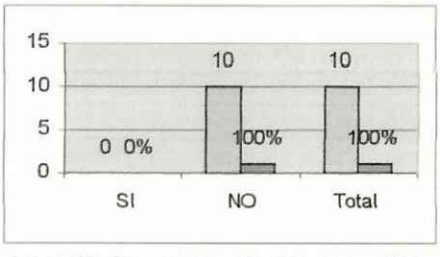
El 100% de los usuarios tienen antivirus para proteger a su computadora de virus informático.

12. ¿Esta usted capacitado en casos de producirse algún problema en la red?

Tabla estadística

	No.	Porcentaje
SI	0	0%
NO	10	100%
Total	10	100%

Gráfico de Barras de la tabla Estadística



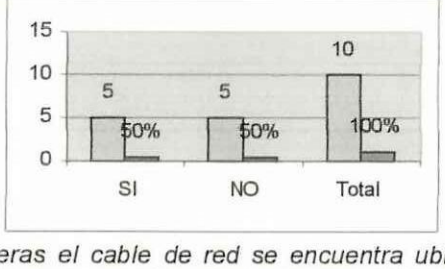
El 100% de los usuarios no se encuentran capacitados para solucionar problemas de averías que pueden presentar en la red de datos.

13. ¿El cableado de la red esta expuesto a que sea destruido?

Tabla estadística

	No.	Porcentaje
SI	5	50%
NO	5	50%
Total	100	100%

Gráfico de Barras de la tabla Estadística



En el departamento de Secretaria de Carreras el cable de red se encuentra ubicado pegado a la pared del mencionado departamento, en cambio el departamento Financiero posee canaletas por donde viaja el cable a los diferentes usuarios.

INTERPRETACIÓN DE RESULTADOS DEL DEPARTAMENTO FINACIERO Y SECRETARIA DE CARRERAS.

Los resultados se derivan de cada una de las preguntas encuestadas, mediante lo cual se ha obtenido lo siguiente:

Conclusión 1.- Para conocer los procedimientos que serían necesarios seguir, en caso de que algún empleado cause algún daño a los equipos de computación, es indispensable un manual o reglamento que disponga el departamento para conocer los procedimientos.

Conclusión 2.- Los respaldos de la información se realiza mediante dispositivos de almacenamiento como CD y disquetes.

Conclusión 3.- Existe un manual de funciones importante para ejercer correctamente su trabajo, y cumplir con las disposiciones legales del departamentos.

Conclusión 4.- La documentación confidencial que procesa cada usuario es protegida con mucha cautela y prevención en una librería que se encuentra dentro del departamento.

Conclusión 5.- En la mayoría de las oficinas encuestadas existen una adecuada restricción de la información que poseen.

Conclusión 6.- Las computadoras que poseen un password de alguna manera están protegiendo la información y con esta medida de seguridad están evitando que la información sea alterada o copiada por extraños.

Conclusión 7.- Es necesario cambiar con frecuencia el password porque en caso de que alguien intente ingresar al computador no lo pueda conseguir.

Conclusión 8.- Manteniendo un adecuado control de impedimento a su computador se evita que la información padezca algún tipo de alteración.

Conclusión 9.- La información que procesan los departamentos son referentes a todo el personal que labora en la Universidad Técnica de Cotopaxi.

Conclusión 10.- Según las entrevistas realizadas el rendimiento del software que utilizan para realizar su trabajo se encuentra en perfectas condiciones.

Conclusión 11.- Penosamente los antivirus se encuentran desactualizados lo que ocasionaría daños al sistema operativo y/o los archivos en caso de presentarse algún virus informático

Conclusión 12.- En caso de presentarse alguna avería en la red de datos los administradores del centro de computo acuden a solucionar el problema.

Conclusión 13.- Una excelente conexión comienza con un cableado seguro, lo cual se esta cumpliendo a cabalidad.

ANEXO 4

ANÁLISIS DE LAS ENCUESTAS DE USUARIOS INDEPENDIENTES.

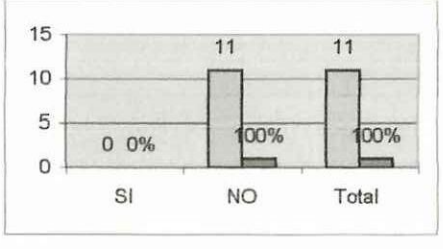
Se ha recopilado información de acuerdo al organigrama estructural de la UTC establecido el 20/04/98, con de los departamentos que tienen computadoras las cuales son: Dirección de Planeamiento y Planificación, Bienestar Universitario, Dirección Proyección Social, Dirección Administrativa, Procuraduría, Secretaria General, Proyectos Productivos, Laboratorios de Suelos, Sala de Profesores, Recepción, FEUE. Mediante encuestas que se presentan a continuación:

1. ¿Posee servicio de red Informática en su oficina?

Tabla estadística

	No	Porcentaje
SI	0	0%
NO	11	100%
Total	11	100%

Gráfico de Barras de la tabla estadística



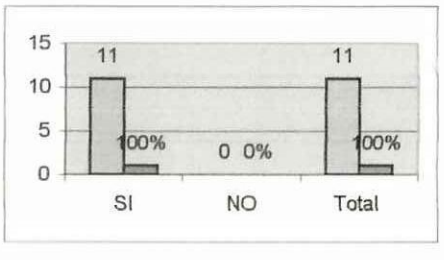
El 100% de oficinas encuestadas deducen que no tienen el servicio de red informática.

2. ¿Cree Ud. Que es necesario Instalar el servicio de red informática?

Tabla estadística

	No.	Porcentaje
SI	11	100%
NO	0	0%
Total	11	100%

Gráfico de Barras de la tabla estadística



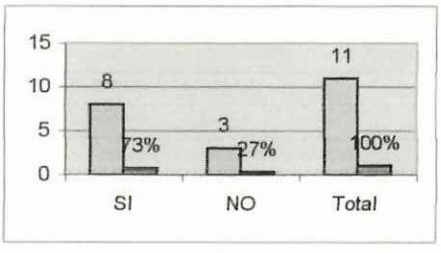
Al encuestar acerca de la importancia de instalar el servicio de red informática el 100% contestaron positivamente.

3. ¿Esta su computador provisto de una palabra clave o código secreto de seguridad que restringe el acceso al **setup** de su computadora?

Tabla estadística

	No.	Porcentaje
SI	8	73%
NO	3	27%
Total	11	100%

Gráfico de Barras de la tabla estadística



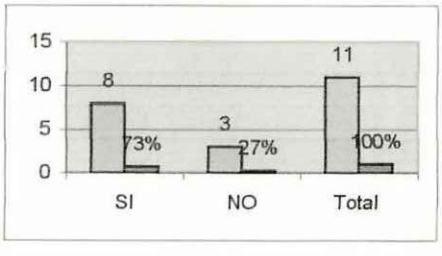
Según la encuesta se encontró que el 73% de los usuarios utilizan una palabra clave para el ingreso al computador, para realizar sus actividades diarias; mientras que el 27% dicen que no.

4. ¿Si la pregunta anterior es si. Con que frecuencia se cambia la clave de acceso?

Tabla estadística

	No.	Porcentaje
SI	8	73%
NO	3	27%
Total	11	100%

Gráfico de Barras de la tabla Estadística



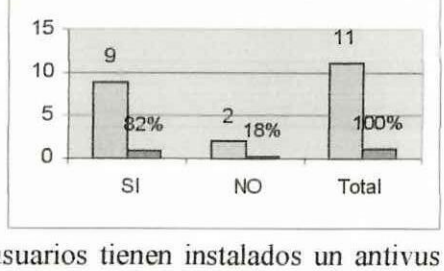
El 73% de encuestados mencionan que cambian la clave de acceso siempre, mientras que el 27% expresa que nunca cambian.

5. ¿En su computador posee un antivirus instalado?

Tabla estadística

	No.	Porcentaje
SI	9	82%
NO	2	18%
Total	11	100%

Gráfico de Barras de la tabla Estadística



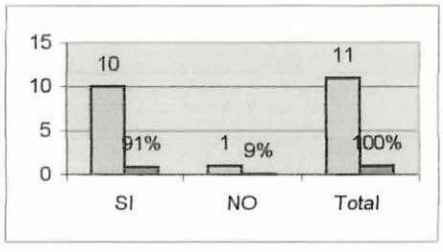
Se determina que el 82% de los usuarios tienen instalados un antivus en su computadora; mientras que el 18% no lo poseen.

6. ¿Posee respaldos de la información de su oficina?

Tabla estadística

	No.	Porcentaje
SI	10	91%
NO	1	9%
Total	11	100%

Gráfico de Barras de la tabla Estadística



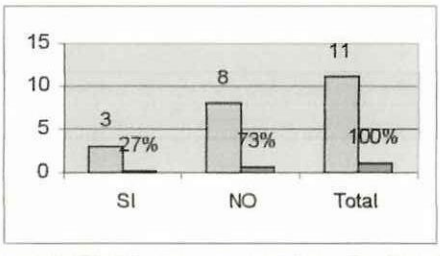
El 91% de encuestados no tienen el respaldo de la información que procesan durante el periodo académico y el 10% mencionan que no realizan respaldos de la información.

7. Se realizan mantenimiento preventivo o correctivo de la computadora

Tabla estadística

	No.	Porcentaje
SI	3	27%
NO	8	73%
Total	11	100%

Gráfico de Barras de la tabla Estadística



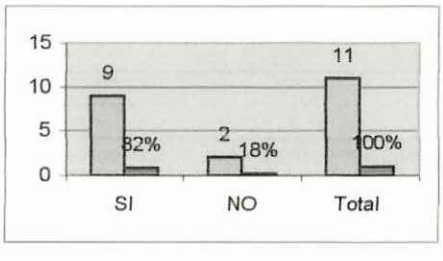
Se determina que el 73% las computadoras no se realiza la función de mantenimiento, y el 27% si ejecuta esta función.

8. ¿La computadora que esta en su oficina es apropiada para desempeñar su trabajo?

Tabla estadística

	No.	Porcentaje
SI	9	82%
NO	2	18%
Total	11	100%

Gráfico de Barras de la tabla Estadística



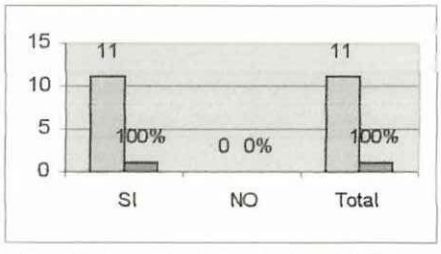
El 82% de los usuarios determinan que su computadora a cargo es apropiada para desempeñar su trabajo; y el 18 % manifestó lo contrario.

9. ¿Tiene conocimientos suficientes sobre todos los programas que Ud tiene instalado en su computadora?

Tabla estadística

	No.	Porcentaje
SI	11	100%
NO	0	0%
Total	11	100%

Gráfico de Barras de la tabla Estadística



El 100% de encuestados cuentan con los conocimientos necesarios sobre el software básico instalado en su computadora.

INTERPRETACIÓN DE RESULTADOS.

Los resultados se derivan de cada una de la preguntas encuestadas, mediante lo cual se ha obtenido lo siguiente:

Conclusión1.- Los departamentos encuestados no disponen de un servicio de red informático, por lo que dificulta compartir información entre sí.

Conclusión2.- Los encuestados mencionan que es de vital importancia implementar el servicio de red informática; de esta manera se compartirá información con la red de datos de la universidad.

Conclusión3- La mayoría de usuarios posee un password para ingresar al computador y de esta manera poder realizar su trabajo de mejor manera y además permite obtener la información de manera segura

Conclusión4.- Los usuarios que contestaron afirmativamente de que cambian el password en un espacio de tiempo de un año de un mes a tres meses permitiendo de esta manera obtener una información personalizadas.

Conclusión5.- Los usuarios deducen que es importante instalar un antivirus actualizado en el computador porque de esta manera se puede tener la información más segura.

Conclusión6.- Los usuarios que contestaron positivamente a la pregunta la fuente de respaldos para sus datos son los disquetes.

Conclusión7.- Al determinar que la mayoría de computadoras no ejecutan la función de mantenimiento estamos conceptualizando que están en peligro de sufrir daños; que pueden ser perjudiciales para el usuario.

Conclusión8.- Los usuarios se encuentran conformes con su computador para desempeñar su trabajo.

Conclusión9.- Los usuarios que laboran el las diferentes oficinas perciben de conocimientos sobre software que posee su computadora.

ANEXO 5

Anteproyecto

TEMA:

Propuesta de un sistema de seguridad informático para la red de datos de la Universidad Técnica de Cotopaxi.

INTRODUCCIÓN

Las redes han progresado en las ultimas décadas que van desde los sistemas basados en servidores centralizados a sistemas corporativos de computadoras descentralizados, en los cuales los recursos de información y las computadoras están distribuidos por toda la organización.

Perfeccionándose cada vez más hasta poder almacenar enormes cantidades de información. Pero desde luego el problema de robo de datos, corrupción y escuchas se incrementó. La situación empeoro cuando las empresas instalaron redes de área local (LAN) para conectar todo y en éste proceso aumentaron las oportunidades de aparición de brechas de seguridad.

Los servicios de red son muy beneficiosos pero así como existe multitud de ventajas también existen desventajas que pueden ser perjudiciales para cualquier empresa u organismo.

No es lo mismo proteger una computadora aislada que una computadora en red. En una red desde cualquier estación de trabajo puede eliminar carpetas o aún el sistema operativo de otra computadora dejándola sin sistema, este es uno de los múltiples problemas que puede presentarse dentro de una red.

Por este motivo la seguridad juega un papel muy importante dentro del uso de una red y mayormente cuando se trata de la red mundial de computadoras que es el Internet.

Un hecho de la vida de Internet que existe gente allá afuera que desea meterse en las redes de otras personas vía Internet las razones varían desde la inocente curiosidad hasta la maliciosa interferencia y el espionaje internacional. Al mismo tiempo en valor de Internet en las empresas y negocios es tan grande que los distribuidores están todo en tiempo corriendo para satisfacer las demandas de seguridad de Internet con los Firewall de Internet. Un Firewall es un impedimento que se encuentra entre su red interna y la Internet externa. Su

propósito es limitar el acceso a su red con base a las políticas de acceso de su compañía.
Según [Tim Evans]

El que quizá sea el hacker más famoso del mundo es Kevin Mitnik, detenido en 1995 por haber logrado entrar en los servidores del Pentágono, y además consiguió hacerse, ilegalmente, con ficheros electrónicos de empresas como Motorola y Sun Microsystems. Sus seguidores clamaban por su puesta en libertad emulándole. Su acción más sonada fue cuando lograron entrar en el diario estadounidense The New York Times, y cambiar todas sus fotografías.

El tema sobre seguridad en Internet surge como una necesidad a partir del aumento en el uso de nuevas tecnologías en las empresas; ya que estudios realizados en Estados Unidos por el FBI revelaron que 90% de las compañías detectaron problemas de inseguridad en su red y 74% reportaron que los incidentes terminaron en pérdidas financieras con un valor estimado entre $800 mil y $1 millón 400 mil dólares.

La Universidad Técnica de Cotopaxi posee cada uno de estos servicios como son la red e Internet; pero no tiene la suficiente protección contra los ataques que si bien en la actualidad se han presentado con fuerza; puede que lo posterior sufra percances que demanden recursos económicos, pérdida de información y lo que es más desprestigio de la Institución por ser tan vulnerables a ataques informáticos.

PROBLEMATIZACIÓN

El impacto tan grande que la Informática esta produciendo en la sociedad en cuanto a intercambio de información que es posible gracias a sus tecnologías y desarrollo.
Uno de los avances que tiene la tecnología es el servicio de red; este proporciona a los usuarios compartir recursos dentro de un ámbito de trabajo, desde una computadora hasta los servicios de impresión; es decir como en

sentido figurado tener una computadora gigantesca con múltiples recursos en contra replica con una computadora aislada o no conectada a una red.

Internet es una red mundial de computadoras que contiene un grupo muy grande de **recursos de información** que surgió espontáneamente y que hoy por hoy cuenta con muchos millones de usuarios conectados a ella, que cada día aumenta su cubrimiento en varios miles de equipos y personas conectándose en todas las latitudes del planeta.

Debido entonces al gran potencial que nos brinda la red y más aun Internet. La Universidad Técnica de Cotopaxi no ha podido quedarse al margen de la tecnología actual; por lo que esta dotada con los servicios de IMPSAT "Proveedor de Internet " el cual suministra 32 k de ancho de banda las 24 horas del día y los 7 días de la semana.

Para la administración del servicio de la red e Internet consta con 2 servidores Linux el primero es utilizado para navegar en Internet y el segundo para recibir y enviar correo electrónico posee un antivirus para la red e Internet, además un servidor de Windows NT alternativo con Microsoft Proxy que cumple las funciones de Firewall, que entra en funcionamiento en caso de caída del sistema del servidor Linux.

La seguridad del departamento financiero consta de contraseñas diferentes para cada usuario, también posee un software contable llamado "Olimpo" que maneja todo lo referente a los estados contables cuyo proveedor es la empresa Protocoltesa la misma que realiza las respectivas reparaciones y mantenimiento semestral; además posee respaldos en el mismo disco duro.

El departamento de secretaría posee contraseñas diferentes para cada computadora, la información que administra es todo lo referente a lo académico.

Los otros departamentos tienen de seguridad contraseñas de setup y también paquetes utilitarios para la información concerniente a su departamento tomando en consideración únicamente los departamentos que tienen computadoras. Para la administración de la biblioteca se tiene un software llamado Siabug, para la mejor y mayor rapidez en la utilización de los textos de consulta. A través de un terminal para los estudiantes.

Si bien éste software protege en cierto sentido la información, pero se descuida en otras tales como:

- Las calificaciones pueden ser modificadas a través de la red; a un profesor que presuroso se dirige a imprimir, el cual es interceptado por un estudiante que se encuentra en una estación de trabajo listo para la operación.
- Los archivos y servicios que están disponibles en la biblioteca de la Universidad pueden ser cambiados o eliminados fácilmente, con lo cual quedaría sin sistema éste beneficio.
- En cualquier departamento de la Universidad puede ser infectado con virus desde un disco flexible. Puesto que la mayoría de computadoras no poseen seguridad contra estos ataques.
- Los estudiantes constantemente eliminan, copian, destruyen los archivos de otras personas, incluso archivos de sistemas provocando así el bloqueo o destrucción del sistema operativo el cual permite que la computadora funcione.
- Si estos son problemas cuanto más significativo será. Cuando la Universidad cargue Bases de datos en Internet, al cual tienen acceso personas del todo el mundo con buenas y malas intenciones.

Es notorio que la seguridad que poseen los servidores es ínfima puesto que en la actualidad existen en Internet los piratas informáticos o Hacker los cuales son personas sin escrúpulos que destruyen los datos e introducen virus en las computadoras y eliminan información sin dejar rastro alguno.

Se dice que el mayor porcentaje de vulnerabilidad de la información es por parte de personas propias de la red y no de personas extrañas a la red; por lo que se tiene que proteger más de los ataques directos por los usuarios que de ataques indirectos.

Por este motivo se ha visto la necesidad de realizar un estudio de las alternativas de seguridad de los servidores de la Universidad para que en lo posterior se cuente con la estabilidad en los servidores, en la red y en la conservación de los datos y su integridad.

Esta es la razón por la cual nuestra actividad primordial esta orientada a buscar nuevas alternativas de Hardware y software para fortalecer la seguridad de los servidores y de la red.

OBJETIVO GENERAL

Establecer la Propuesta de un sistema de seguridad informático para la red de datos de la Universidad Técnica de Cotopaxi.

OBJETIVO ESPECIFICO

- Realizar el análisis de la estructura de red informática de la Universidad Técnica de Cotopaxi.
- Determinar las amenazas y vulnerabilidades que en la actualidad presenta la red informática de la Universidad Técnica de Cotopaxi.
- Buscar mecanismos de seguridad que proporcionen protección a la red informática de la Universidad Técnica de Cotopaxi.
- Analizar y comparar diferentes alternativas de seguridad de acuerdo a los sistemas operativos de la red.
- Determinar las políticas de seguridad que se consideren necesarias para la implementación de la misma.
- Realizar propuesta de funcionalidad de las seguridades.
- Realizar la demostración de las seguridades propuestas con datos reales.

JUSTIFICACIÓN

En todo el mundo todos los días se producen entradas no autorizadas y violación de la seguridad. Una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de computo. Este acceso puede tomar muchas formas, como el uso de la cuenta de otro usuario para tener acceso a la red y sus recursos. La gravedad del acceso no autorizados depende del sitio y la naturaleza de la perdida de potencial que puede causar daños irreparables por la cobertura negativa de los medios. En general las Universidades de prestigio, los sitios de gobierno y las zonas militares parecen traer más intrusos.

"Los intrusos utilizan los servidores para disfrazar acciones, marcando al servidor y teniendo acceso a la red. Si el servidor se lo permite el intruso puede

tener acceso a la red interna desde dicho servidor, y después de utilizar Telnet para salir de nuevo lo que dificulta rastrearlo. Así mismo, si el intruso la utiliza para atacar a otra red, parecerá que el ataque se originó en la red de Usted".
Según [Karanjit Siyan]

La principal vulnerabilidad de los sistemas de la Universidad Técnica de Cotopaxi es de que no poseen mecanismos de control que eviten el uso no autorizado de los recursos.

Muchos responsables de la administración de redes que se conectan a Internet tienen miedo de los riesgos desconocido que pueden ser introducidos en sus datos. Con un sistema seguridad eficiente en la red informática de la Universidad Técnica de Cotopaxi se logra que gente no autorizada ingrese a la red de computadoras y causar daños a la misma. Con la implantación de la seguridad se evitará que los hackers o piratas informáticos exploren o experimenten el funcionamiento de los sistemas tecnológicos que existen en la Universidad, de esta manera se conseguirá que la información no sea manipulada y que mantenga alejados a los piratas.

Con una solvente seguridad en el centro de computo se conseguirá confianza y sosiego de que los datos que se envían y receptan no serán explorados por otras personas

El sistema de seguridad a ser implantado beneficiará a la Universidad Técnica de Cotopaxi en particular en el laboratorio de computación, la seguridad se centrará en los servidores, en la red y en el Internet respectivamente. Se protegerá los sistemas contra los fallos comunes: Piratas, Virus y otros intrusos, etc. Con el análisis respectivo de la red informática por parte de los investigadores se tendrá un conocimiento exacto y adecuado de la tecnología de redes que hoy en día ha llegado hasta nuestras aulas de estudio y por ende a la vida profesional.

Observando los peligros eminentes que se presentan en la red informática no se puede obviar la seguridad en la red. El interés como investigadores se centra en conocer la situación actual de la administración de la red de la Universidad Técnica de Cotopaxi, a través de un análisis minucioso y cuidadoso para comprenderla en su totalidad. En el cual se encuentra el

servidor y la conectividad al Internet, para determinar de esta manera las vulnerabilidades y amenazas que presenta la misma.

El siguiente paso en la investigación es buscar alternativas de seguridad para la red de la Universidad Técnica de Cotopaxi a través de diversos libros de consulta por medio del Internet y organizaciones que posean un sistema de seguridad.

Para evidenciar el tema de investigación se realizará la demostración, utilizando software de Versión Veta, con sus respectivas pruebas de estabilidad y fiabilidad.

MARCO DE REFERENCIA

Mark Gibbs (1995)

"Las redes grandes requieren Usted sepa quien tiene acceso a cada equipo periférico y quien toma el control sobre dicho acceso. Hay muchas cosas a considerar cuando se trata de recuperación de desastres pero lo que no debe obviar es la importancia de contar con un plan. No sirve de nada tener el equipo si no se usa."

Redes para Todos

Ford Merilee (1998)

"Tecnología de interconectividad de redes proveerá de la información necesaria para tomar decisiones fundamentales en cuanto a redes se refiere. Pro ejemplo se dominará la terminología, los conceptos las tecnologías y los dispositivos de uso actual en la industria de interconectividad de redes en un entorno LAN/WAN así como la forma de aplicar el modelo de referencia OSI para categorizar protocolos tecnologías y dispositivos."

Tecnología de interconectividad de redes

Tom Sheldom

"Para que la empresa obtenga las máximas ventajas de toda la información disponible con frecuencia es necesario acceder a múltiplex plataformas y

brindar soluciones a problemas complejos de compatibilidad de sistemas. Compartir datos o acceder a enormes bases de datos requiere enlazar diferentes redes, aplicaciones y sistemas operativos."
Lan times "Guía de Interoperatibilidad para redes"

Harley Hahn. (1994)
"Mostrar como entender y utilizar Internet proporcionando conocimientos generales y enseñándole los detalles técnicos"
Internet Manual de Referencia

Douglas Comer (1996)
"Esta obra proporciona la introducción conceptual más actualizada para los protocolos TCP/IP y los últimos desarrollos de la tecnología en Internet para cualquiera que desee aprender o trabajar con el conjunto de protocolos TCP/IP"
TCP/IP : redes globales de información con Internet

Kris Jamsa y Ken (1996)
"La clave para diseñar una red de computadoras se encuentra por primera vez en la frase de Julio Cesar: Divide y vencerás. Para fragmentar esta meta o (tema) en pequeñas metas o subtemas entenderá con facilidad cada subtema y, tras un breve lapso tendrá un amplio panorama de los principios fundamentales de las redes "
El Mejor Curso sobre TCP-IP

Lois Kahn y Laura Logan (1997)
"Internet se ha convertido en la mayor y más accesible fuente de información del mundo. La Intranets permiten compartir información en una empresa y aprovechar al máximo las aplicaciones que se basan en este soporte "
Construye su propio Web

George, Eckel (1996)
"El tema construya un servidor de Internet con Unix contiene todo lo que Ud. necesita saber de principio a fin para crear con éxito un sitio de Internet. No

solo explica como hacerlo sino también porque es más importante conectarse como host, Al igual que los beneficios que debe tener Internet "

Construya un servidor de Internet con UNIX

sheldon, Tom

"Para realizar un buen plan de seguridad de la red se debe comenzar enfocando las causas del problema y posibles soluciones. El manual de seguridad de Windows NT ayudara en dicho cometido Tom Sheldon proporcionará información esencial para empezar a proteger su red correctamente".

Manual de seguridad de Windows NT

STEPHEN cobb (1998)

"En modelos de seguridades para PC y redes locales descubrirá los métodos más efectivos para proteger su computadora y los datos que encierra tanto contra indeseables intrusos. Stephen cobb, conocido experto en computadoras y autor de varios libros, trata a un enfoque practico y realista a estos problemas cada vez mas frecuentes.

Explica como proteger los sistemas, contra las fallas más comunes: Piratas, virus y otros intrusos, ladrones de datos "

Manual de seguridad para PC y redes locales

Karanjit, Siyan (1997)

"Segunda edición, revela cómo se implementa la seguridad en un mundo de información delicada, y señala lo inadecuado de los actuales productos de seguridad al demostrar que no logran mantener alejados a los intrusos, usted puede evaluar mejor sus requerimientos, riesgos y ventajas de seguridad."

Firewalls y la seguridad en Internet

Forley, Marc, TOM STERORMS, JEFFREY MSU (1997)

"La G.LT.SID.- es la respuesta.. Esta practica guía le enseñaron como mantener seguros y disponibles los datos de su empresa para las personas adecuadas.

Aprenderá sobre áreas de riesgo que puede no haber considerado y descubrirá como asegurar sus datos para que no puedan ser alterados, perdidos o salteados.

También ofrecer una visión en profundidad de las tecnologías que han sido diseñados para proteger los datos en las redes "

Guía LAN TIMES de seguridad e integridad de datos

Mcgraw – HIIL 1995

"Los partidos de mensaje entre sistemas incompatibles causan, además de muchas frustraciones, innumerable problemas de tiempo y oportunidad fallidos. Con tantos sistemas diferentes como hoy, ¿ cómo pueden conectarse entre sí de una manera fiable?

La guía LAN tipos de control electrónico, ofrece selecciones claras y practicas a los problemas de interconectividad, además de trucos y técnicas para maximizar el uso y la productividad del correo eléctrico."

Guía tan timer de correo electrónico

Herschell Gordon Lewis, Robert D. Lewis (2000)

"Si los hackers son verdaderamente son buenos (en realidad, crackers – quebradores; el término hakers se refiere a programadores extraordinarios, lo suficientemente buenos como para hacer pedazos –hack– programas complejos y descubrir como funcionan)"

Como vender en Internet

MARCO CONCEPTUAL

A continuación se describen los términos más usados en la investigación

Administrador de una Web

Operador del sistema de un sitio Web.

Ancho de banda

Medida de capacidad de comunicación o velocidad de transmisión de datos de un circuito o canal.

Backbone

Red de banda ancha para conexiones entre conmutadores.

Banda amplia

Ruta/circuito de comunicaciones de capacidad media. Suele indicar una velocidad de 64000 bps a 1544 Mbps.

Banda ancha

Ruta/circuito de comunicaciones de gran capacidad. Normalmente implica una velocidad superior a 1544 Mbps.

Base de datos

Conjunto de información para varios usuarios. Suele admitir la selección de acceso aleatorio y múltiples "vistas" o niveles de abstracción de los datos subyacentes.

Baudio (término antiguo que se está reemplazando por bps - bits por segundo):

Número de elementos de señalización que pueden transmitirse por segundo en un circuito.

BOT

"bot" es el término coloquial para programas que escuchan una conversación y responden en un canal IRC.

BPS

Bits por segundo. Medida de velocidad de un módem.

BBS (Sistema de boletín electrónico)

Boletín electrónico en el que los usuarios pueden dejar mensajes. En muchos BBS es necesario ser miembro de ellos.

Cern

European Laboratory for Particle Physics, el sitio donde se celebró la primera conferencia sobre World Wide Web y considerado el lugar de nacimiento de la tecnología de WWW. El trabajo sobre la tecnología de WWW y la elaboración de estándares se ha trasladado a la World Wide Web Organization (W3O, en w3.org). http://www.cern.ch/

CGI (Interfaz de gateway común)

Interfaz para programadores que crean archivos de comandos o aplicaciones que se ejecutan internamente en un servidor de Web. Estos archivos de comandos pueden generar texto y otros tipos de datos de forma inmediata, en respuesta a una entrada del usuario, o bien tomando la información de una base de datos.

Ciberespacio

Término utilizado originalmente en la novela "Neuromante", de Willian Gibson, sobre redes de equipos informáticos en el cerebro. Se refiere al campo colectivo de la comunicación asistida mediante equipos informáticos.

Conversación

Término que se utiliza para describir una conferencia en tiempo real. Las salas de conversaciones IRC, "WebChat", prodigy y aol son ejemplos de "conversación".

Dirección

Código exclusivo asignado a la ubicación de un archivo almacenado, un dispositivo en un sistema o red, o cualquier origen de datos de una red.

Dirección IP

Dirección de 32 bits del protocolo Internet asignada a un host. La dirección IP tiene un componente del host y un componente de la red.

Dirección URL (Uniform Resource Locator)

Formato de las direcciones de sitios que muestra el nombre del servidor en el que se almacenan los archivos del sitio, la ruta de acceso al directorio del archivo y su nombre.

Explorador

Programa de aplicación que proporciona una interfaz gráfica interactiva para buscar localizar, ver y administrar la información a través de una red.

FTP (Protocolo de transferencia de archivos)

Protocolo utilizado para transferir archivos a través de una amplia variedad de sistemas.

Gateway

Conversor de protocolos. Nodo específico de la aplicación que conecta redes que de otra forma serían incompatibles. Convierte códigos de datos y protocolos de transmisión que permiten la interoperatividad.

Gopher

Programa de búsqueda y exploración de bases de datos públicas en Internet.

GUI

Interfaz gráfica de usuario.

Hipervínculo

Conexiones entre una información y otra.

HTTP (Protocolo de transferencia de hipertexto)

Método mediante el que se transfieren documentos desde el sistema host o servidor a los exploradores y usuarios individuales.

IP (Protocolo Internet)

Define la unidad de información enviada entre sistemas, que proporciona un servicio de entrega de paquetes básico.

ISDN (Red digital de servicios integrados)

(También llamada RDSI) Juego de normas de la transmisión a gran velocidad de información simultánea de voz, datos e información a través de menos canales de los que serían necesarios de otro modo, mediante el uso de la señalización fuera de banda.

ListServ

"ListServ" es un programa gratuito para automatizar el mantenimiento

y la entrega de listas de correo electrónico. Hay listas de muchos temas; algunas son "abiertas" (cualquier persona de la lista puede enviar un mensaje a toda la lista, como en una conversación) y otras "cerradas" (sólo determinadas personas pueden enviar información a ellas).

Módem (Modulador-Desmodulador)

Conexión del equipo del usuario final que permite transmitir datos digitales a través de dispositivos de transmisión analógicos, como las líneas telefónicas.

"POP" (punto de presencia)

Conexión de acceso telefónico de los proveedores de servicios de Internet para usuarios de módem, que se utiliza principalmente para describir conexiones locales, de forma que los usuarios no tengan que hacer llamadas de larga distancia. Por ejemplo, un determinado ISP puede tener su base en San Jose, pero tener "POP" en Los Ángeles y Nueva York.

Portadora común

(Empresa de telecomunicaciones) Portadora que sirve al público (o a un segmento de él) de forma indiscriminada (es decir, sin tener en cuenta la identidad del cliente y sin discriminación indebida).

PPP (Protocolo punto a punto)

Conexión a Internet de acceso telefónico que utiliza el protocolo TCP/IP; algo más rápido que SLIP.

Privilegios de acceso

Privilegio para tener acceso a carpetas y hacer cambios en ellas.

Puntero

Dirección URL incrustada en los datos que especifica su ubicación en otro registro o archivo. El hipervínculo es un ejemplo de puntero.

Red

Sistema de elementos interrelacionados que se conectan mediante

un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, vídeo, datos, etc.) y facilitar el intercambio de información entre usuarios con intereses comunes.

Seguridad

Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor

En una red, estación host de datos que proporciona servicios a otras estaciones.

Servidor de archivos

Sistema informático que permite a usuarios remotos (clientes) tener acceso a archivos.

SGML

Standard Generalized Markup Language. Lenguaje para la descripción de otros lenguajes de documentos estructurales basados en etiquetas. Por ejemplo, el HTML está definido mediante el SGML.

Soporte

Formato de distribución y almacenamiento de información (p. ej. cinta de vídeo, disquete, disco óptico, impresora, etc.). Una ampliación de la capacidad de comunicación de la humanidad. Es el mensaje.

SSL

Nivel de socket de seguridad. Protocolo que utiliza Netscape para proporcionar transacciones seguras a través de la red.

TCP/IP

Protocolo de control de transmisiones/Protocolo Internet. Es el protocolo estándar de comunicaciones en red utilizado para conectar sistemas informáticos a través de Internet.

Telnet

Programa de red que ofrece una forma de conectarse y trabajar desde otro equipo. Al conectarse a otro sistema, los usuarios pueden tener acceso a servicios de Internet que quizás no tengan en sus

propios equipos.

Usenet (USEer NETwork)

Grupos de debate de Internet. Uno de los primeros formatos de "correo electrónico colectivo". Actualmente hay unos 10000 grupos de debate diferentes.

WAIS (Wide Area Information Server)

Potente sistema para buscar grandes cantidades de información muy rápidamente en Internet.

WWW (World Wide Web)

Sistema de Internet para vincular mediante hipertexto en todo el mundo documentos multimedia, permitiendo un fácil acceso, totalmente independiente de la ubicación física, a la información común entre documentos.

HIPÓTESIS

- La búsqueda de nuevas de alternativas de seguridad optimiza el control de acceso a la red de la Universidad Técnica de Cotopaxi.
- La creación de políticas y normas de seguridad mejora la utilización de la red de la Universidad Técnica de Cotopaxi.

CONTENIDOS

CAPITULO I

Temas involucrados en el proyecto

1.1. Las redes de computadoras
1.2. Tipos de redes de computadoras
1.3. Componentes de una red
1.4. Servidores
1.5. Estaciones de trabajo
1.6. Arquitectura de red
1.7. Tipos de arquitectura de red

1.8 Grupo de protocolos TCP/IP

1.8.1Síntesis general de TCP/IP

1.8.2Manejo de FPT

1.8.3 Relación entre FTP y telnet

1.9 Seguridades en una red

1.9.1 Definición de seguridad

1.9.2 Piratería de software y sus problemas

1.9.3 Seguridad de redes y comunicaciones

1.9.4 Medidas protectoras

1.9.5 Medidas de seguridad en Internet

1.9.6 Cortafuegos

1.9.7 Controles de acceso

1.9.8 Cuentas de usuarios

1.9.9 Inicio de sesión y contraseña

1.9.10 Protección de directorio y archivos

CAPITULO II

Análisis del dominio estudio

2.1 Estudio de la situación actual en los diferentes departamentos de la Universidad Técnica de Cotopaxi

2.1.1 Topología de red utilizada

2.1.2 Tipos de comunicación.

2.1.3 Sistema operativo de red.

2.2 Software de Aplicación

2.3 Software Utilitarios

2.4 Software Académico

2.5 Modelo de referencia OSI que utiliza la Universidad Técnica de Cotopaxi

2.5.1 Nivel1 : Físico

2.5.2 Nivel2: Enlace de datos

2.5.3 Nivel3 Red

2.5.4 Nivel4: Transporte

2.5.5 Nivel5: Sesión

2.5.6 Nivel6: Aplicación

2.6 Determinar las amenazas, vulnerabilidades que en la actualidad presenta la red Informática de la Universidad Técnica de Cotopaxi

CAPITULO III

3.1 Políticas de seguridad para los usuarios de la red de datos de la Universidad Técnica de Cotopaxi.

3.2 Estudio de Factibilidad

3.2.1 Búsqueda de tres alternativas de seguridad a nivel de software y hardware

3.2.2 Comparación de tres alternativas de seguridad

3.2.3 Selección de una alternativa de seguridad informática .

3.2.4 Propuesta

CAPITULO IV

4.1 Demostración de la seguridad para la red de datos de la Universidad Técnica de Cotopaxi.

4.1.2 Diseño

4.2 Instalación y configuración del Sistema de Seguridad

4.2.1 Instalación y configuración del Sistema de Seguridad

4.2.2 Instalación del sistema Operativo Windows 2000 Server y Linux Red Hat

4.2.3 Configuración de los servidores y servicios

4.2.4 Configuración del sistema de seguridad

4.2.4.1 Aplicación de políticas de seguridad

4.3 Análisis de resultados de los Sistemas de Seguridad.

CAPITULO V

Conclusiones

Recomendaciones

Bibliografía

Anexos

MÉTODOS Y TÉCNICAS

Los métodos y técnicas mas aplicados en la investigación son los siguientes:

Métodos

Deductivo: Este método se aplicará cuando se extrae o se separa las consecuencias del análisis de la información global.

Inductivo: El objeto de estudio será una prueba eminente que existe este y muchos problemas relacionados con la seguridad en otras organizaciones, que se aplicará a cada uno de los sistemas de seguridad.

Análisis: El análisis es la descomposición de un todo en sus partes. Toda la información del objeto de estudio será examinada por fragmentos para su mejor comprensión.

Síntesis: Este es el método es usado para llegar a la consecuencia de resultados muy próximos a la realidad, basándose en el análisis previo.

Técnicas

Fichaje: Se necesita acudir con frecuencia a libros, revistas y periódicos y documentos con la finalidad de obtener información que apoye al conocimiento científico producto de la investigación que se realizará.

Entrevista: Es la técnica de investigación que será dedicada a obtener información mediante un sistema de preguntas a los encargados del Centro de Computo, Departamento Financiero, Secretaria de Carreras motivo de la investigación.

Observación: Se usará en la administración de la red informática del laboratorio de la Universidad Técnica de Cotopaxi, Departamento Financiero, Secretaria de Carreras para la adquisición de la situación actual.

Cuestionario: Es la técnica de investigación dedicada a obtener información mediante un sistema de preguntas estructurado en formulario para los estudiantes, docentes y personal que labora en el objeto de investigación. Para obtener estadísticas de las seguridades que posee el Centro de Computo, Departamento Financiero, Secretaria de Carreras.

PRESUPUESTO

La magnitud del trabajo que se pretende realizar especialmente en la fase de recolección y sistematización de la información relativa requiere de innumerables gastos como los siguientes:

Recursos humanos

Director de tesis: Ing. Fernando Defaz

Asesor de tesis: Dr. Pedro Bedón

Asesor de campo: Ing. Adrián Mena

Personal de centro de computo

Personal docente de la Universidad Técnica de Cotopaxi

Ejecutores de tesis: Egdo. Marcelo Panchi

Egdo. Samuel Sinche

RECURSOS HUMANOS

Nomina	**H*semana**	**H* MES**	**H*6 Meses**	**Valor Hora**	**TOTAL**
Director de tesis:	2	8	48	0.25	12,00
Asesor de tesis:	2	8	76	2,00	152,00
Asesor de campo:	2	8	76	0.80	60,80
Ejecutores de tesis	25	100	600	1,00	600,00
Total Costo					824,80

RECURSOS MATERIALES

Materiales	**Presupuesto**
Utiles de oficina	50,00
Diskette	20,00
Textos Técnicos	160,00
Trascripción e Impresión	200,00
Anillados ejemplares	50,00
Empastado de texto	20,00
Transporte	40,00
Fotocopias	40,00
Horas de Internet	50,00
Horas de Uso de Computadora	20,00
Total	650,00

COSTO TOTAL

Costo Recursos humanos	824,80
Costos Directos	650,00
Costos Indirectos 10%	147,48
Total	1622,28

CRONOGRAMA DE ACTIVIDADES

MESES / ACTIVIDADES	AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				ENERO			
	1	2	3	4	1	2	1	1	1	2	3	4	1	2	3	4	2	3	4	2	3	4	3	4
Análisis y diseño actual de la red Informática.	X	X	X	X																				
Diseño de Instrumentos para la recolección de Información					X	X																		
Tabulación y procesamiento de datos y análisis de Información							X	X																
Estudio de la seguridad en la red de la U.T.C.									X	X														
Búsqueda de 3 alternativas de seguridad para la red de UTC											X	X	X	X										
Selección de una alternativa adecuada de seguridad para la UTC															X	X								
Diseño y aplicación en la red de la U.TC.																	X	X	X					
Pruebas de estabilidad y fiabilidad a la red																				X	X	X		
Comprobación de Hipótesis																							X	X
Documentación			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Lineamientos de documentación				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Presentación																					X	X	X	X

BIBLIOGRAFÍA

Cobb, Stephen

Manual de seguridad para PC y redes locales

Madrid : McGraw-Hill, c1994.

Comer, Douglas(75)

TCP/IP : redes globales de información con Internet

México, Prentice Hall, c1996.

Drummond, Rik y Nancy Cox

Guía de los Times de correo

Mcgraw-Hill

Madrid(1995)

Eckel, George

Construya un servidor de internet con UNIX

México : Prentice Hall, c1996.

Ford Merilee

Tecnología de Interconectividad de redes

PRENTICE-HALL

México 1998

Forley, Marc, TOM STERORMS, JEFFREY MSU

Guía LAN TIMES de seguridad e integridad de datos 1997

México :Cornelo Sanchez Gonzalez

Gordon Lewis, Herschell

Cómo vender en Internet: guía de

mercadotecnia / Gordon Lewis, Herschell. --