ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"AUDITORÍA DE SEGURIDAD EN REDES DE DATOS"

PROYECTO DE TÓPICO DE GRADUACIÓN

Previa a la obtención del título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por

Luis Andrés Mideros Romero
Marjorie Alexandra Chalén Troya
Washington Antonio Caraguay Ambuludi

Guayaquil – Ecuador

2007

A mi familia y amigos

que supieron estar ahí

cuando los necesite y

me apoyaron siempre.

Andrés Mideros R.

Agradezco a Dios, a mis

padres y a todas las

personas que siempre

me apoyaron.

Marjorie Chalén T.

A mi familia por el apoyo

recibido y especialmente

a ti Lenin Stalin,

Washington Caraguay A.

TRIBUNAL DE GRADUACIÓN

Ing. Holger Cevallos U.
Presidente

Ing. José Escalante A.
Director

Dr. Boris Ramos S.
Miembro Principal

Ing. Ivonne Martín M.
Miembro Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado. Me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

Luis Andrés Mideros Romero.

Marjorie Alexandra Chalén Troya.

Washington Antonio Caraguay Ambuludí.

RESUMEN

En el primer capítulo se hace referencia a los conceptos básicos de la transferencia de información a través de las redes de comunicación. Se parte de lo más básico, conceptualizando qué es un protocolo, la jerarquía en la que se basan para el desempeño de sus funciones, el medio en el cual se transmiten y la manera en la que éstos viajan a través de los medios. De este modo se logra poner las bases al entendimiento de lo que es una red de comunicación y se incorpora el conocimiento de una LAN. En base a lo mencionado anteriormente, se logra definir lo que requiere la seguridad y el control de acceso hacia una red.

En el segundo capítulo se tratará qué se entiende por Auditoría de seguridad en una red de datos, se explicará las fases y tipos de Auditorías que se aplican. Dada la interconexión de redes públicas y privadas y el uso compartido de los recursos de información, se hará referencia a los métodos, técnicas y herramientas empleados para proteger y evaluar el flujo de información en una red. Además se mencionará que perfil debe cumplir un

auditor.

En el tercer capítulo se emplearán las herramientas de Auditoría estudiadas en el capítulo 2 y se aplicarán en la implementación de una red SOHO, SMALL OFFICE / HOME OFFICE; en donde se evaluará el funcionamiento de las mismas. Esto se realizará mediante el desarrollo de un procedimiento de evaluación de un sistema de seguridad en una red de comunicaciones.

En el cuarto capítulo se analizará el costo de implementación de la red y la realización de la Auditoría, en donde se detallaran gastos por equipos utilizados, materiales y mano de obra.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO

ACK - (Acknoledgment). Acuse de Recibo. Es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

ACLs - (Access control list). Lista de Control de Acceso. Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

ANSI - (American National Standards Institute). Instituto Nacional Estadounidense de Estándares. Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. Es miembro de la Organización Internacional para la Estandarización (ISO).

ARP - (Address Resolution Protocol). Protocolo de Resolución de

Direcciones, determina la dirección de Hardware del Host.

ARQ - (Automatic Repeat Request). Petición de Repetición Automática. Es un protocolo utilizado para el control de errores en la transmisión de datos, garantizando la integridad de los mismos.

BHC - (Bose Ray-Chaudhuri Hocquenghem Code) Código de Bose Ray-Chaudhuri Hocquenghem. Es un código de corrección de errores.

BSI - (British Standard Institute). Instituto de Estándares Británicos. Es una organización de estandarización y normalización.

Cable UTP - Cable de par trenzado no apantallado. Es el más simple y empleado, sin ningún tipo de pantalla adicional y con una impedancia característica de 100 Ohmios. El conector más frecuente con el UTP es el RJ45, aunque también puede usarse otro (RJ11, DB25, DB11,etc), dependiendo del adaptador de red.

CISA - (Certified Information Systems Auditor). Auditor Certificado de Sistemas de Información emitida por ISACA es la certificación más importante a nivel mundial para demostrar conocimiento, experiencia y habilidad en las áreas de Auditoría, Control, Gobernabilidad y Seguridad de

Tecnologías.

CSMA/CD - (Carrier Sense Multiple Access with Collision Detection). Acceso Múltiple con Escucha de Portadora y Detección de Colisiones. Es una técnica usada en redes Ethernet para mejorar sus prestaciones.

Dirección IP - (Dirección de Protocolo de Internet). La forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono es único dentro de una red telefónica. La dirección IP consta de cuatro números separados por puntos y cada número es menor de 256; por ejemplo 192.200.44.69. El administrador del servidor Web o su proveedor de servicios de Internet asignará una dirección IP a su equipo.

DNS - Es el acrónimo de Domain Name Server (servidor de nombres de dominio). Un servidor de nombres de dominio es un servidor ubicado en Internet que traduce las URLs (Uniform Resource Locator o localizador uniforme de fuentes) como www.adslayuda.com en direcciones IPs. Muchos ISPs no necesitan que se introduzca esta información en el router. Si está usted utilizando un tipo de conexión de IP estática, entonces puede necesitar introducir una dirección de DNS y una dirección de DNS secundaria específicas para que su conexión funcione adecuadamente. Si su tipo de conexión es dinámica o PPPoE, es muy probable que no necesite introducir

una dirección de DNS.

DoD - (Departament of Defence). Departamento de Defensa. Es el ministerio del gobierno de los Estados Unidos encargado de las fuerzas militares del país, en tiempos de guerra y en tiempos de paz.

DOS - (Disk Operating System). Sistema Operativo de Disco. Fue el primer sistema operativo para la plataforma IBM PC, que utilizaban los procesadores Intel 8086/8088 de 16 bits. Tiene una interfaz de línea de órdenes vía su intérprete de órdenes.

DSSS - (Direct Secuence Spread Spectrum). Espectro Ensanchado por Secuencia Directa. Es un método de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas.

Ethernet - Red de área local (LAN) de medios compartidos desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN que más se utiliza (seguido por Token Ring). Todos los mensajes se diseminan a todos los nodos en el segmento de red. Ethernet conecta hasta 1,024 nodos a 10 Mbps sobre un par trenzado, un cable coaxial y una fibra óptica

Fast Ethernet - Ethernet de alta velocidad a 100 Mbps (la Ethernet regular

es de 10 Mbps).

FCC - (Federal Comunications Commission). Comisión Federal de las Comunicaciones. Es una agencia estatal independiente de Estados Unidos, bajo responsabilidad directa del Congreso. Es la encargada de la regulación de telecomunicaciones interestatales e internacionales por radio, televisión, redes inalámbricas, satélite y cable.

FDDI - (Fyber Distributed Data Interface). Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local mediante cable de fibra óptica.

FDM - (Frecuency Division Multiplexing). Multiplexación por División de Frecuencia. Es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos.

FEC - (Forward Error Correction). Corrección de Error Delantera. Es un tipo de mecanismo de corrección de errores que permite su corrección en el receptor sin retransmisión de la información original.

Firewall - Corta Fuegos. Es un filtro que controla todas las comunicaciones que se manejan en una red y en función de lo que se establezca, este le

permite o deniega el paso.

FTP - (File Transfer Protocol), Protocolo Estándar de Transferencia de Ficheros. Su misión es permitir a los usuarios recibir y enviar ficheros de todas las máquinas que sean servidores FTP. El usuario debe disponer del software que permita hacer la transferencia (actualmente todos los navegadores, ya disponen de ese software para recibir ficheros). Los ficheros pueden ser documentos, textos, imágenes, sonidos, programas, etc., es decir, cualquier cosa que se pueda almacenar en un fichero o archivo.

GNU GPL - Licencia Pública General. Es una licencia orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

HTTP - (Hiper Text Transfer Protocol). Protocolo de Transferencia de HiperTexto. Es el protocolo de Internet que permite que los exploradores del WWW recuperen información de los servidores.

HTTPS - Este protocolo es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las SSL para crear un canal cifrado más

apropiado para el tráfico de información sensible en el protocolo HTTP. El puerto estándar para este protocolo es el 443.

ICMP - (Internet ControI Message Protocol). Protocolo de Control de Mensajes de Internet. Protocolo usado por el IP para informar de errores y excepciones. El ICMP también incluye mensajes informativos usados por algunos programas como ping

ICMP ECHO_Reply - (Respuesta de Eco en el Protocolo ICMP). Es un mensaje generado como contestación a un mensaje Echo Request.

ICMP ECHO_Request - (Petición de Eco en el Protocolo ICMP). Es un mensaje que se envía a un host para que éste le responda con un Echo Reply. Todo host debe responder a un Echo Request con un Echo Reply que contenga exactamente los mismos datos que el primero.

IDS - (Intrusion Detection System). Sistema de Detección de Intrusos. Es un programa usado para detectar accesos desautorizados a un computador o a una red.

IEEE - (Institute of Electric and Electronic Engineers). Instituto de Ingenieros Eléctricos y Electrónicos. Es una asociación técnico-profesional mundial

dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación e ingenieros en telecomunicación.

Internet - Conjunto de redes de ordenadores creado a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de miles de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza TCP/IP para proporcionar comunicaciones de ámbito mundial.

IP - (Internet Protocol). Protocolo de Internet. Es el protocolo principal ya que brinda el enrutamiento de los paquetes; es el que trasporta los datos desde su origen a su destino. No corrige errores.

IP Address - Dirección IP. Matrícula que identifica a un ordenador de la red. A los ordenadores personales se les asigna una IP address para que naveguen por la red.

ISO - (Internacional Standard Organization). Organización Internacional para la Estandarización. Es una organización internacional no gubernamental, que produce normas internacionales industriales y comerciales.

KBPS - Kilobits por segundo. Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit esta formado por mil bits.

LAN - Local Area Network o Red de Área Local. Una LAN es un grupo de ordenadores y dispositivos conectados juntos en un área relativamente pequeña (como una casa o una oficina): Su red doméstica es considerada una LAN.

MAC - Significa Media Access Control o Control de Acceso al Medio. Una dirección MAC es la dirección hardware de un dispositivo conectado a una red.

Máscara de Subred - Cifra de 32 bits que especifica los bits de una dirección IP que corresponde a una red y a una subred. Las direcciones de bits no cubiertas por la máscara corresponden a la parte del host. También llamado máscara de dirección.

MCP - Modulación por Codificación de Pulsos.

MD - Modulación Delta.

MSDOS - (MicroSoft Disk Operating System). Sistema Operativo de Disco de Microsoft. Es un sistema operativo comercializado por Microsoft perteneciente a la familia DOS.

MTA - Multiplexación Asíncrona en el Tiempo.

MTS - Multiplexación Síncrona en el Tiempo.

NRZ - (No Return To Zero). No Retorno a Cero. En telecomunicaciones, se denomina NRZ porque el voltaje no vuelve a cero entre bits consecutivos de valor uno.

NTFS - (New Technology File System). Sistema de Archivos de Nueva Tecnología. Es un sistema de archivos diseñado específicamente para Windows NT (incluyendo las versiones Windows 2000, Windows 2003, Windows XP y Windows Vista), con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base.

OSI - (Open System Interconection). Interconexión de Sistemas Abiertos. Es el modelo de red descriptivo creado por ISO.

POP3 - (Post Office Protocol verisión 3). Protocolo usado para obtener los

mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores de los proveedores de internet acceden a sus correos a través de POP3.

Protocolo - Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor).

POSIX - (Portable Operating System Interface; la X viene de UNIX). Interfaz de Sistema Operativo Portable basado en UNIX. Especifica las interfaces de usuario y software al Sistema Operativo.

RARP - (Reverse Address Resolution Protocol). Protocolo de Resolución de Direcciones Inverso. Realiza el proceso contrario ARP, pues a partir de una MAC determina la dirección IP del equipo.

RS - (Reed Solomon). Es un subconjunto de los códigos BCH.

RJ45 - Conector estándar de 8 alambres usados en LANs.

Router - Enrutador. Originalmente, se identificaba con el término gateway, sobre todo en referencia a la red Internet. En general, debe considerarse

como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.

Sistema de ventanas X - Fue desarrollado para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste.

SMTP - (Simple Mail Transfer Protocol). Protocolo Simple de Trasferencia de Correo. Protocolo que se usa para trasmitir correo electrónico entre servidores.

SNMP - (Simple Network Management Protocol). Protocolo de Gestión Simple de Redes. Protocolo mediante el cual se administra la red, en base a monitoreo, control de dispositivos y administración de configuraciones.

SSL - (Secure Sockets Layer). Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

Switch - Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de

datos del modelo OSI. En general se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

TCP - (Transmission Control Protocol). Protocolo de Control de Transmisión. Es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, entre otras.

TCP/IP - (Transmission Control Protocol over Internet Protocol) Protocolo de Control de Transmisión sobre Protocolo de Internet. Éste es el protocolo estándar para la transmisión de datos por Internet. Proporciona comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y distintos sistemas operativos.

TDM - (Time División Multiplexing). Multiplexación por División de Tiempo. En Esta modulación el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

Telnet - (TELetype NETwork), Protocolo Estándar de Internet. Permite al usuario conectarse a un ordenador remoto y utilizarlo como si estuviera en una de sus terminales.

TFTP - (Trivial File Transfer Protocol). Protocolo de Transferencia de Archivos Trivial. Permite el intercambio de archivos de configuración y archivos entre los sistemas que admitan este protocolo; no es orientado a conexión, utiliza UDP, User Datagram Protocol.

UDP - El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP, pero varía en el sentido de que no es fiable y no esta orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS.

UPS - (Uninterruptible Power Supply). Sistema de Alimentación Ininterrumpida. Es un dispositivo que puede proporcionar energía eléctrica, tras un apagón o un desenchufe, a todos los dispositivos existentes en una red eléctrica. Otra de las funciones es la de regular el flujo de electricidad, controlando las subidas-bajadas de tensión y corriente existentes en la red eléctrica.

VLAN - (Virtual LAN). Red de Área Local Virtual. Es un método de crear redes lógicamente independientes dentro de una red física. Varias VLANs pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el dominio de broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.

VNC - (Virtual Network Computing). Computación en Red Virtual. Aplicación que permite acceso remoto a través de un escritorio remoto de otra computadora dentro de una red (como una LAN o internet). Permite controlar una computadora remota enviando eventos como las pulsaciones del teclado y los movimientos y clics del mouse. El programa muestra una captura de imagen de la computadora remota cada un período determinado de tiempo. De esta manera un usuario puede ver exactamente qué eventos se producen en otra computadora y también controlarlos.

WAN - Red de área amplia. Cualquier red pública es de este tipo. Su característica definitoria es que no tiene límites en cuanto a su amplitud. Existen redes privadas de gran cobertura soportadas en estructuras físicas que son propiedad de operadores nacionales o internacionales.

WEP - (Wired Equivalent Privacy). Protocolo para Redes Wireless que permite cifrar la información que se transmite. Utiliza claves de 64 bits o de 128 bits.

WI-FI - Es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Creado para ser utilizado en redes locales inalámbricas y para acceder a Internet.

Windows XP - Es una línea de sistemas operativos desarrollada por Microsoft, orientada a cualquier entorno informático incluyendo computadoras domésticas o de negocios y computadoras portátiles. Es el primer sistema operativo de Microsoft orientado al consumidor que se construye con un núcleo y arquitectura de Windows NT y que se encuentra disponible en versiones para PC de 32 y 64 Bit.

WWW - (World Wide Web). Telaraña o malla mundial. Sistema de información con mecanismos de hipertexto creado por investigadores del CERN. Los usuarios pueden crear, editar y visualizar documentos de hipertexto.

INTRODUCCIÓN

Las redes de comunicación son implementadas en base a varias tecnologías, la mayor parte de las organizaciones cuentan con una red de área local, LAN, mediante la cual transfieren información. La información representa uno de los activos más importantes en una organización, por lo que se debe considerar una protección adecuada.

La seguridad de una red va ligada a las políticas de seguridad de la organización que la utiliza; por lo que hay varios frentes que se deben cubrir: Lan, Servidores y PCs, Wan, Wireless. La red que se va a considerar es una LAN, SOHO, que representa una red pequeña; en la cual se considera las bondades del sistema operativo de las computadoras que se utilizan, básicamente las configuraciones de los equipos que conforman y las aplicaciones de un firewall para proteger la red principalmente de manera interna; en este caso el Isa Server 2004.

Existen muchas maneras de lograr la seguridad de una red, pero también hay muchas vulnerabilidades que pueden alterar dicha seguridad. En base a la norma ISO 17799 se considera un procedimiento que se divide en fases para lograr una implementación dedicada, de acuerdo a las políticas de la organización que solicita la red. Para su evaluación se ha considerado la utilización de un firewall, de manera que se permita la protección de la red y monitorear los sucesos que se presentan en ella; con la finalidad de obtener una visión del comportamiento de la red.

CAPÍTULO 1

PROTOCOLOS DE RED

1.1 INTERFACES Y PROTOCOLOS DE COMUNICACIÓN DEL ENLACE DE DATOS

1.1.1 TCP / IP

El protocolo es una descripción formal de un conjunto de reglas y procedimientos que rigen la transmisión de datos y comunicación de dispositivos en una red[1].

Con el propósito de facilitar el entendimiento de la complejidad y múltiples funciones empleadas para establecer comunicación a través de una red de computadores, se ha desarrollado una arquitectura de capas.

[1] Network Security Bible. Chapter 11. Network Protocols. Página 370

La arquitectura de capas más importante en la comunicación actual es la familia de protocolos TCP/IP. Ésta, es la base de la comunicación del Internet e Intranet, sirve de estándar en la comunicación de una variedad de plataformas y sistemas operativos.

Este modelo de referencia fue creado en los años setenta por el DoD, de los Estados Unidos con el fin de tener una red de comunicación confiable, en cualquier circunstancia.

TCP/IP se divide en cuatro capas que se distribuyen de manera similar a las capas del modelo OSI; que fue desarrollado por ISO, para servir de modelo base en la comunicación en una red de computadores. Sin embargo, el modelo TCP/IP fue desarrollado antes que el modelo OSI. La tabla 1, detalla la comparación entre estos dos modelos.

<table>
<tr><th>Modelo OSI</th><th>Modelo TCP/IP</th></tr>
<tr><td>Capa 7. Aplicación
Provee servicios como e-mail, transferencia de archivos y servidores</td><td rowspan="3">Capa 4: Aplicación
Equivalente a las capad de Aplicación, Presentación y Sesión del Modelo OSI. Comunica a través de sockets y puertos</td></tr>
<tr><td>Capa 6. Presentación:
Provee encriptación, codificación y formato de la información</td></tr>
<tr><td>Capa 5: Sesión
Negocia y establece conexión con otra computadora</td></tr>
<tr><td>Capa 4: Transporte
Proporciona la entrega confiable de los datos</td><td>Capa 3: Transporte
Proporciona la entrega confiable de los datos, asegura la integridad de los datos</td></tr>
<tr><td>Capa 3: Red
Realiza el enrutamiento de los paquetes a través de la red</td><td>Capa 2: Internet
Maneja las conexiones a través de la red. Uitliza los protocolos para una transmisión lógica de los paquetes a través de la red; controla la comunicación a través de los host. Asigna direcciones de IP a los nodos de la red.</td></tr>
<tr><td>Capa 2: Enlace de Datos
Provee corrección de error y transferencia de mensaje de tramas</td><td rowspan="2">Capa 1: Control de acceso al medio
Combina las capas Física y de Enlace de Datos del modelo OSI
Incluye mapeo de dirección IP a dirección MAC, utilizando software drivers; encapsulación de datagramas en tramas a ser transmitidas en la red. También tiene que ver con las conexiones de hardware y software, conectores, niveles de voltaje y cableado.</td></tr>
<tr><td>Capa 1: Física
Interfaces con medios de transmisión y envío de los datos a través de la red</td></tr>
</table>

Tabla 1. Similitud entre Modelo TCP/IP y el Modelo OSI.

El modelo TCP/IP trabaja con protocolos y estándares a nivel de capas, los cuales ejecutan funciones específicas y añaden información a los datos a medida que viajan de capa en capa. Cuando una computadora desea transmitir información, ésta viaja desde la capa superior hacia la capa inferior, a medida que traspasa una capa se agrega información; lo que se conoce como proceso de encapsulamiento. La computadora que recibe la

información realiza el proceso inverso, cada protocolo separa y examina la información que fue añadida por el equipo transmisor.

Capa de Aplicación

Se encarga de la representación, codificación y control de dialogo; verificando que los paquetes estén empaquetados correctamente[2]. Esta capa trabaja con protocolos de alto nivel, algunos de ellos se detallan a continuación: FTP, TFTP, HTTP, DNS, TELNET, SMTP, POP, SNMP.

Capa de Transporte

Se encarga de transportar la información de un extremo a otro, es un enlace lógico entre un host trasmisor y un host receptor. Se encarga de la segmentación de los datos mediante los protocolos TCP, Transfer Control Protocol y UDP. Sin embargo, cuando se utiliza TCP se realiza el control del flujo de la información, lo que ofrece confiabilidad en la transmisión de datos.

Capa de Internet

Define el formato de los paquetes y protocolos a utilizar. Su objetivo principal es dirigir los paquetes hacia la mejor ruta y los envía a donde estos se supone que tienen que ir. Los protocolos que se utilizan en esta capa son: IP, ICMP, ARP, RARP.

[2] Cisco Networks. CCNA Móldulo 1 Capítulo 9.1.2

Capa de Acceso al medio

Se realiza la transmisión de los paquetes hacia el medio de transporte que se utilice, y de receptar estos paquetes.

1.1.2 Codificación de datos

La base para la transmisión de la información está en la codificación digital y la digitalización, de tal manera que se manejen tantos datos analógicos y digitales mediante señales digitales respectivamente. Las señales digitales son las que gobiernan el mundo tecnológico que nos rodea, por medio de ellas se rigen los equipos y dispositivos en una red de datos.

La codificación digital, es la transformación de las señales analógicas en pulsos eléctricos binarios que tienen una secuencia preestablecida; de tal modo que se logra trasformar cualquier información en cadena de ceros y unos.

El esquema de codificación de las señales digitales se clasifica como: NRZ, Bifase y Bipolar.

NRZ

Codifica cada bit asignando un nivel de tensión específico para cada uno. La tensión negativa representa el ‘1’ y la positiva el ‘0’. La componente continua

en NRZ fluctúa de acuerdo a la proporción de ‘ceros’ y ‘unos’.

Otra codificación de este tipo es NRZI que codifica un bit de acuerdo a un cambio de tensión; considerando un tiempo de duración de un bit, se codifica un ‘1’, si no lo hay, entonces es ‘0’ ó viceversa. Esto se conoce como codificación diferencial.

Bifase

Conocida también como codificación Manchester, se trata de una codificación sincronizada. La señal de datos y la de reloj se combinan proporcionando una señal auto sincronizada; en el periodo de duración de cada bit codificado, en la mitad se realiza una transición, de tal modo que un bit '1' se indica haciendo en la primera mitad de la señal igual a la última mitad del bit anterior. Tal como se puede observar en la Fig1.1. La componente continua en Manchester es cero. Además, se observa una secuencia de bits codificados tanto en NRZ como en Manchester Diferencial.

Bipolar

Un tipo de codificación que intenta mejorar a NRZ y logra eliminar problemas de sincronización con respecto a cadenas de ‘unos’ es la Bipolar ó Multinivel. Consiste en codificar un ‘1’ cuando se realiza un cambio de nivel. Sin embargo, no se logra mejorar la tasa de errores con respecto a NRZ, es

menos eficaz. No existe componente en continua en el tipo de codificación.

En muchas ocasiones se requiere la conversión de datos analógicos a datos digitales, entonces se puede aplicar la PCM ó la MD.

La Modulación por codificación de pulsos es el método estándar empleado para transmitir una señal analógica por medios digitales. La PCM se basa en el teorema de muestreo para la transmisión de las señales; el cual consiste en muestrear una señal por instantes de tiempo. Es decir transformar la señal analógica en muestras espaciadas uniformemente en el tiempo. Para esto la frecuencia que se utiliza para muestreo de la señal debe dos veces mayor que la frecuencia más alta que emplee la señal a transmitir.

Para que la señal se transmita correctamente en este proceso de codificación se requiere un filtro pasabajo, con el fin de evitar el traslape de la señal original, luego sigue el proceso de muestreo, cuantificación y codificación.

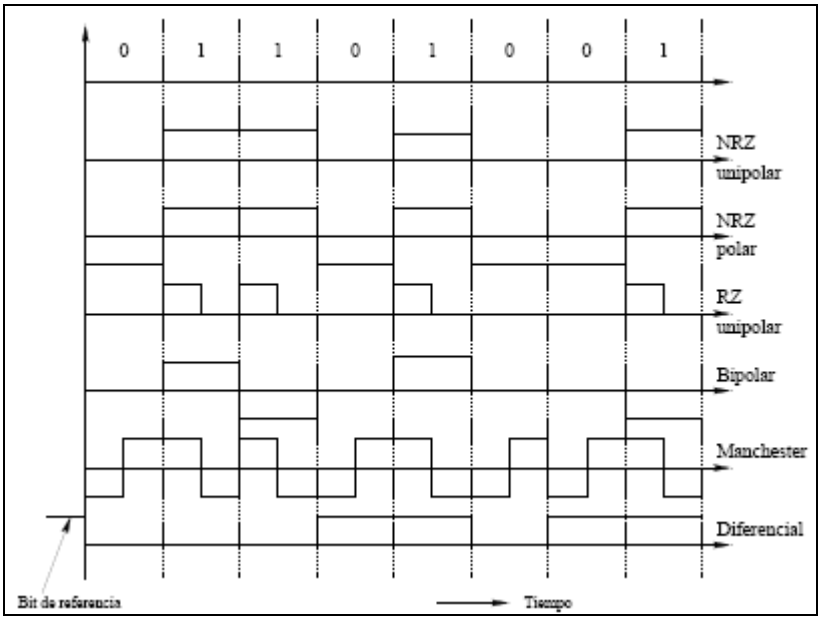


Figura 1.1 Modulación por codificación de pulsos

Otro método utilizado para la codificación de señales analógicas en señales digitales es la Modulación Delta, que sobremuestrea una señal de mensaje entrante[3], es decir utiliza una frecuencia de muestreo cinco veces mayor a la que Nyquist. De esta manera se aproxima la señal entrante a una señal escalonada para luego convertirla en una sucesión de dígitos binarios, los cuales indican la polaridad de los escalones.

[3] Libro de Sistemas de Comunicación. Capítulo 3.12 Página 218

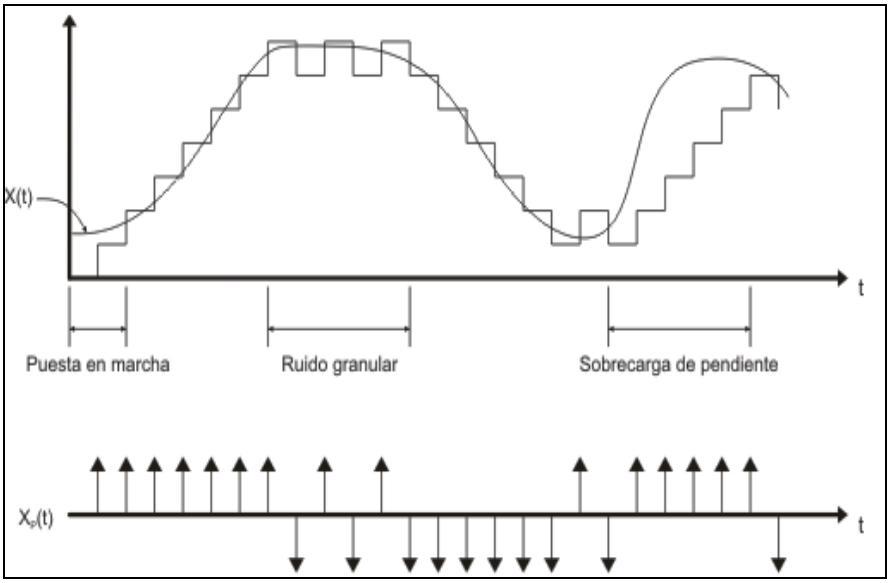


Figura 1.2 Modulación Delta

1.1.3 Errores en la transmisión

La información digital en el recorrido desde el origen hacia el destino puede verse afectada por diversos factores, por lo que se requiere que se implementen procesos de detección o corrección de errores.

Existen varios procesos que sirven para controlar los errores en la transmisión de los datos; entre ellos los más importantes son: paridad y códigos de redundancia cíclica, conocidos como códigos CRC. La base de estos métodos de detección de errores es verificando que en el transmisor se envía cierta cantidad de bits, a la que se le añade un código de detección de errores, mediante un cálculo en particular; y en el receptor por cada trama de entrada se realiza el mismo cálculo y se comparan ambos resultados. Si no coinciden entonces se detecta error.

El método comúnmente empleado para la detección de errores es el de la paridad que consiste en ubicar los datos en un bloque y aplicar control de paridad en dos dimensiones; es decir que se añade un bit al final de cada fila y al final de cada columna.

También es común aplicar CRC en la comunicaciones, se han especificado algunas cadenas de chequeo bien conocidas llamadas CRC-12, CRC-16 y CRC-CCITT con R=12,16 y 16 bits respectivamente. Estas cadenas se interpretan como polinomios de la siguiente manera:

CRC-12 = 1100000001111 = X12 + X11 + X3 + X2 + X + 1.

CRC-16 = 11000000000000101 = X16 + X15 + X2 + 1

CRC-CCITT = 10001000000100001 = X16 + X12 + X5 + 1

La corrección de errores detectados en la transmisión de datos se realiza mediante dos técnicas: ARQ y FEC.

FEC es el mecanismo para corrección de errores mediante el cual se detecta y se corrige el error en receptor de la señal utilizando información redundante junto con la señal. De este modo no requiere de retransmisión de tramas para corregir errores. Sin embargo, este sistema demanda mayor ancho de banda.

Este procedimiento requiere que se codifique la información, por lo tanto la información luego de la codificación se conoce como bits de codificación. Luego de la codificación la cantidad de bits aumentan con relación a los bits de información original.

Existen dos variantes de FEC más conocidas, FEC a bloques y FEC convolucional. El FEC a bloques codifica los bits de información añadiéndole bits de paridad, utilizando un algoritmo algebraico; mientras que en el descodificador se usa el algoritmo inverso para identificar y corregir los errores luego. Los tipos de codificaciones más usados son BHC; y RS[4].

En cambio en el método FEC convolucional, a medida que los bits llegan al receptor se codifican, la codificación de cada bit lleva dependencia de los bits predecesores. Esta codificación se usa mediante el algoritmo de Vitervi.

1.1.4 Control de errores y control de flujo

Toda transmisión debe tener un control que prevea la pérdida de información, la cual se puede verificar a través de la capa de enlace que se encarga del control de flujo y del control de errores.

El control de flujo es la técnica que procura que la estación transmisora envíe

[4] http:// es.wikipedia.org/wiki/FEC

los datos a una velocidad, tal que la estación receptora pueda procesarlos. Para esto se considera el método de ventana deslizante

El control de errores se realiza mediante ARQ, que consiste en retransmitir la información sólo en caso de presentarse error. Existen tres métodos de ARQ que sirven para retransmitir la señal:

ARQ de parada y espera

Se basa en un tiempo de espera en el cual, luego de que el receptor envía la trama espera una respuesta de un ACK, que indica que la trama llegó. El tiempo de espera abarca el tiempo de transmisión, el tiempo de propagación, el tiempo del acuse de recibo y del proceso en el receptor.

En la Figura 1.3, se puede observar como opera de manera normal este método. El emisor envía la trama 0, no hay pérdida, entonces el receptor la recibe y envía un ACK1, indicando que espera la trama 1. El emisor recibe el ACK1, entonces envía la trama 1.

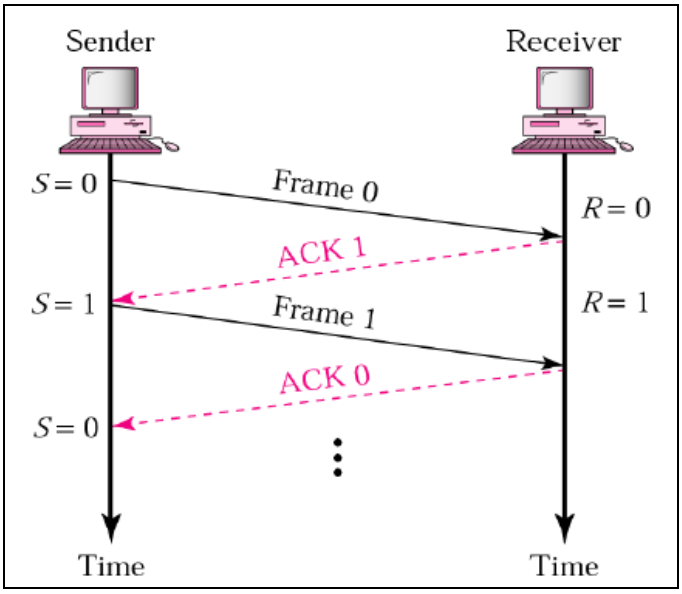


Figura 1.3 ARQ de parada y espera sin pérdida de trama

En la Figura 1.4, se representa el modo operativo de este método cuando se presenta pérdida de trama; de tal modo que el proceso empieza de la misma manera que se explica anteriormente. Sin embargo, se pierde la trama 1, por lo que existe una ventana en el emisor, con determinado tiempo de espera. Una vez transcurrido este tiempo, si no se obtiene respuesta de ACK, se envía nuevamente la trama de la cual no se recibió un ACK.

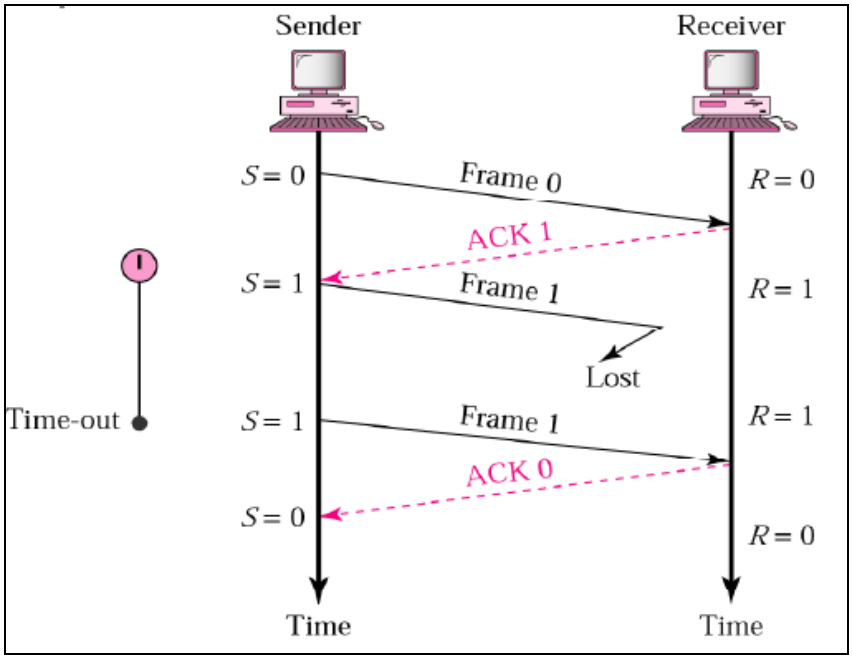


Figura 1.4 ARQ de parada y espera con pérdida de trama

En la Figura 1.5, se observa el mismo proceso mencionado anteriormente; pero con pérdida de ACK. De la misma manera, al momento de enviar una trama, se espera un ACK. Una vez que se termina el tiempo de espera, se envía nuevamente la trama, del mismo modo que ocurre si se pierde la trama. También puede suceder que se demore en llegar el ACK, en este caso, se rechaza la trama en el receptor, porque esta llegó anteriormente.

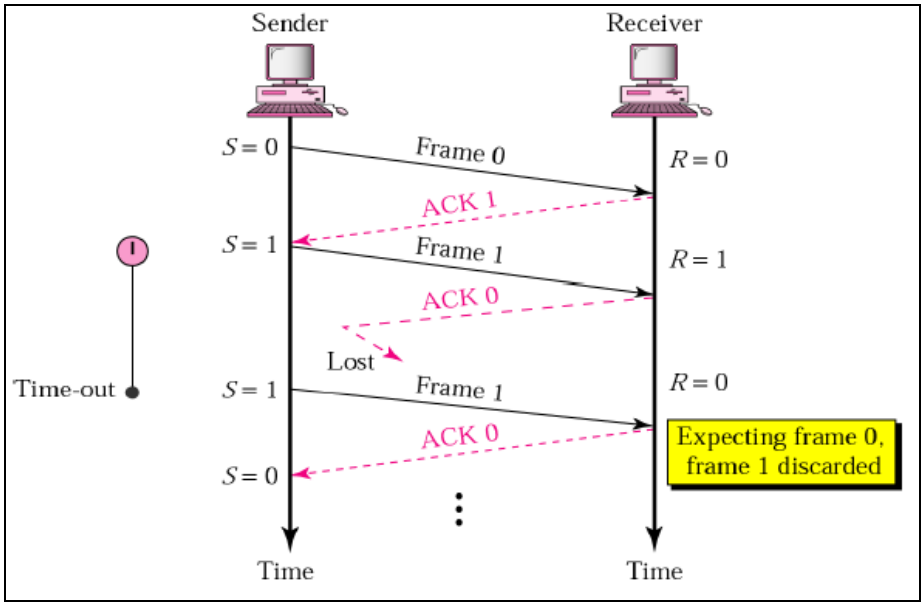


Figura 1.5 ARQ de parada y espera con pérdida de ACK

ARQ de envío continuo y rechazo simple

En este método las tramas son numeradas de manera secuencial, del 0 a 7, es decir 8 bits. En la Figura 1.6, se puede observar el funcionamiento de este método, existe una ventana deslizante; en el emisor en donde se toma en consideración la numeración de las tramas. En el receptor se numera la trama que está por recibirse.

La diferencia de este método con el anterior se debe a que si ocurre un error en el envío de una trama, se continúa con el envío de la siguiente. Sin embargo, una vez finalizado el tiempo de espera, si no llega un ACK, se reenvía únicamente la trama en la que se presentó el error. Para que no se presenten errores se procura que el tamaño de la ventana en el emisor sea

menor que 2^m; y en el receptor debe ser igual a 1.

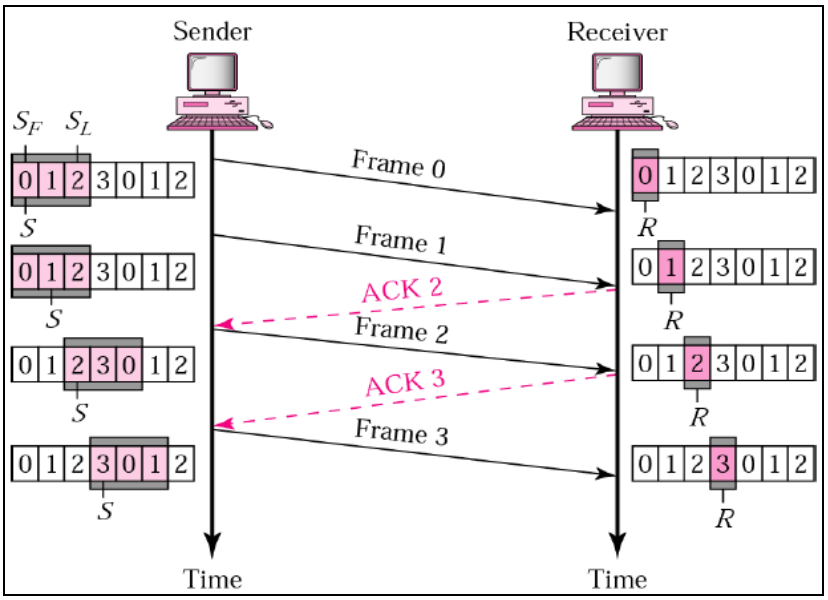


Figura 1.6 ARQ de envío continuo y rechazo simple.

ARQ de envío continuo y rechazo selectivo

En este caso el tamaño de la ventana tanto del emisor como del receptor debe ser máximo la mitad de 2^m.

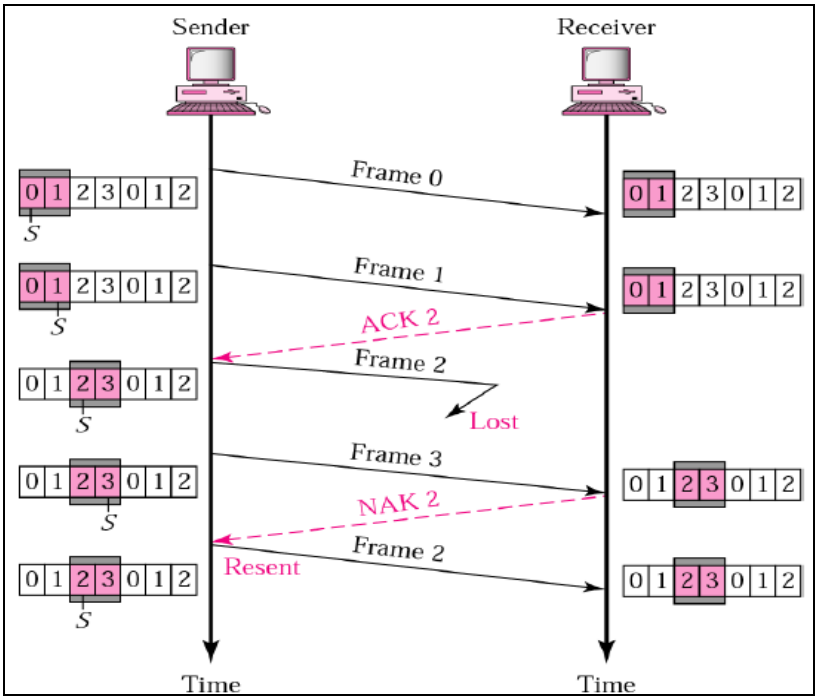


Figura 1.7 ARQ de envío continuo y rechazo selectivo

1.1.5 Multiplexación del enlace de datos

La multiplexación o multicanalización consiste generar una señal compuesta a partir de varias señales independientes que pueda ser canalizada por un canal común. Estas señales deben ser transmitidas de tal modo que no interfieran entre sí, pero que puedan ser separadas en el extremo receptor.

Esto se logra utilizando FDM y TDM; lo que se traduce a multicanalización por división de frecuencia y multicanalización por división de tiempo respectivamente.

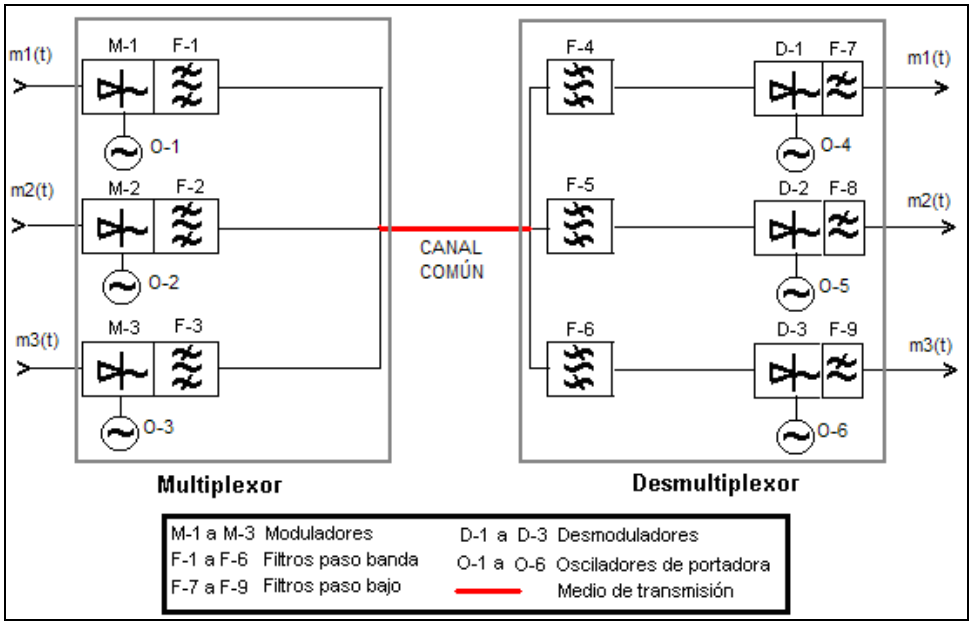


Figura 1.8 Representación de circuito conjunto de multiplexor-demultiplexor analógico[5].

En el caso de FDM se tiene como entrada varias señales con diferentes frecuencias y combina para formar un solo ancho de banda; este tipo de multiplexación es utilizada generalmente en sistemas de transmisión analógicos. La manera de lograr que las señales viajen por un mismo canal se logra aplicándole a cada señal de entrada un filtro pasabajo, de tal manera que se eliminen las frecuencias altas que puedan perturbar a las demás señales; luego se aplicará modulación a la señal haciendo que mediante una señal portadora se adquiera una frecuencia de portadora; ésta modulación produce una señal doble banda lateral. Entonces se le aplica un filtro pasabanda, se restringe el ancho de banda de cada señal. Así, se combinan paralelamente formando la entrada de canal común.

[5] http:// es.wikipedia.org/wiki/multplexación

En cambio para los sistemas digitales especialmente, se utiliza la FDM, este tipo de multiplexación asigna un todo el ancho de banda del canal a una señal en determinado intervalo de tiempo; de manera que no interfieran las señales entre sí.

Existen dos tipos de multiplexación en el tiempo: MTS, consiste en que cada emisor tiene un tiempo determinado para transmitir. En cambio la MTA, cada emisor puede transmitir en un intervalo de tiempo variable; con este método no se desperdicia ancho de banda como en el MTS, que cuando no se transmite información, se desperdicia ancho de banda.

En la Figura 1.9, se puede observar el diagrama de bloques que describe el proceso empleado para realizar la multiplexación por división de tiempo. Cada señal de entrada pasa por un filtro de señal antitraslape pasobajo para que se eliminen frecuencias no deseadas. Luego se aplica un conmutador que sirve para tomar una muestra de cada uno de los N mensajes a una frecuencia fs, un poco mayor a 2W, donde W es la frecuencia de corte del filtro antitraslape; entonces intercala las N muestras dentro de un intervalo de muestreo Ts[6]. Luego la señal pasa por un modulador de pulsos, para de ahí poder ingresar al canal de comunicación.

[6] Libro de Sistemas de comunicación. Capítulo 3.9 Página 211

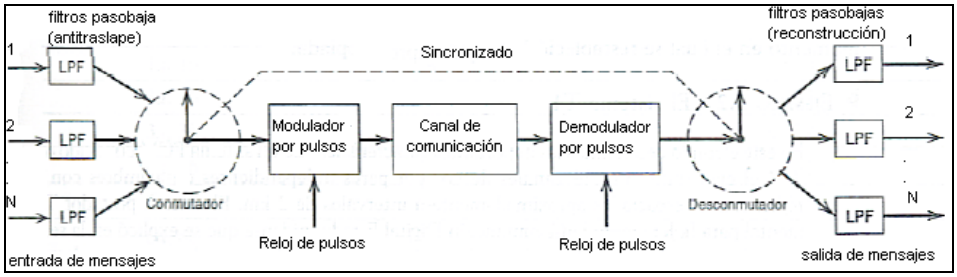


Figura 1.9 Diagrama de bloques del proceso de multiplexación por división de tiempo

1.2 REDES DE ÁREA LOCAL

1.2.1 Funcionamiento

Una red de área local es lo que se conoce como LAN, es la interconexión de equipos y periféricos. Las redes LAN son de dimensiones reducidas, su longitud geográfica abarca unas decenas de metros, por lo general un edificio. La función de una LAN es permitir que dos o más máquinas se comuniquen, con el objetivo de intercambiar información. El protocolo más utilizado en estas redes es el Ethernet 10/100/1000 Mbps.

Se logra construir una LAN aplicando diversas topologías que definen la estructura de la red. La topología de una red conlleva dos partes: topología física y topología lógica.

Topología física

Se refiere a la parte física de la red, que es la conexión de los cables y medios. En cambio la topología lógica representa la manera en que los host manejan el acceso de los datos. Se conocen las siguientes topologías físicas principales:

Topología en anillo

Los dispositivos se conectan en forma de bucle cerrado o anillo; de tal modo que cada host se conecte con el siguiente y el primero con el último.

Topología en estrella

El control está centralizado; todos los cables se conectan a un punto central.

Topología en bus

Los host se conectan a un solo cable de backbone, donde cada extremo debe terminar.

Topología en estrella expandida

Esta topología mediante hubs y switches conecta estrellas individuales.

Topología jerárquica

Es similar a la estrella expandida, con la diferencia que la parte central es un host, en vez de un hub o switch; que realiza el control central.

Topología en malla

En esta topología, todos los hosts están conectados entre si.

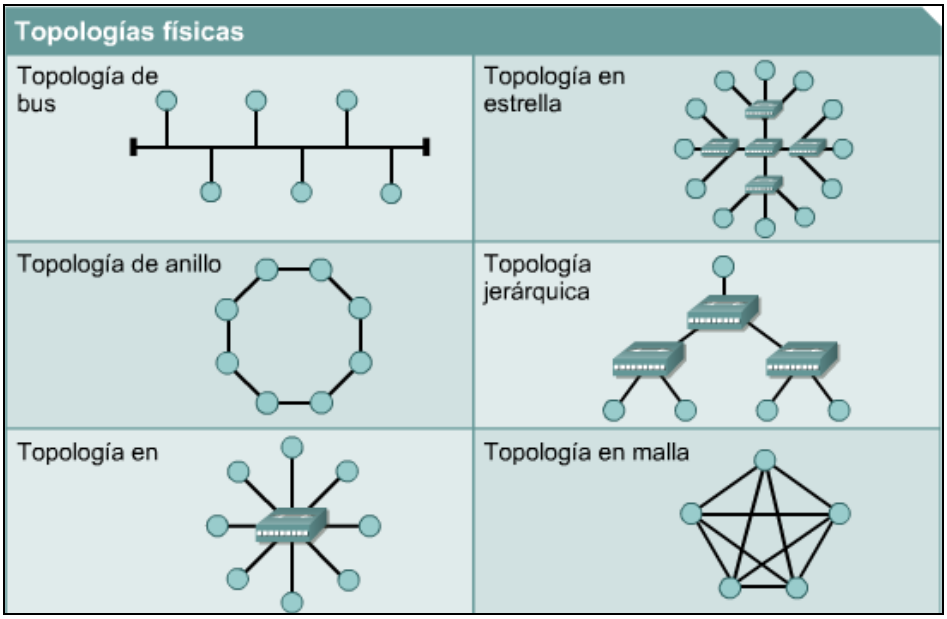


Figura 1.10 Topologías Físicas de Red[7]

Topología lógica

Entre las topologías lógicas se pueden citar broadcast y transmisión de tokens. En una transmisión broadcast cuando un host desea enviar datos los transmite a todos los host de la red. Por otro lado, en una transmisión de token, se envía un token electrónico a cada host de la red; si el host tiene datos para enviar, los envía. En caso de que no tenga datos para enviar, el host le transmite el token al siguiente, y se repite el proceso.

Con el objetivo de establecer la comunicación física y lógica entre los distintos dispositivos de red, se debe considerar el tipo de tecnología a emplearse en una red. Dentro de las más comunes se ubican:

---

[7] Cisco Networks CCNA 1 Módulo 1 Capítulo 2.1.4

- Ethernet
- Token Ring
- FDDI.

1.2.2 Control de acceso al medio (MAC)

El control de acceso al medio es conocido como MAC, es una subcapa de la capa de enlace. Se hace necesario establecer las reglas que definen cómo los distintos usuarios tienen acceso a ella, para evitar conflictos y asegurar que cada uno tenga iguales oportunidades de acceso.

La MAC presenta dos clases de control de acceso al medio:

- No Determinística

  El control de acceso al medio no determinístico ó aleatorio se basa en "el que primero llega, primero se sirve"[8]. Lo cual indica que si un host desea transmitir información y la red está descongestionada, enviará la información, pero si otra máquina desea transmitir información deberá esperar a que la anterior termine el proceso que haya iniciado.

- Determinística.

  Esta clase de control da prioridades dependiendo del tiempo necesario

[8] Cisco Networks CCNA 1. Módulo 1 Capítulo 62.1

para acceder al medio.

1.2.3 LANs con control de acceso aleatorio

La IEEE 802.3 ha creado un mecanismo de control de acceso al medio, CSMA/CD. Este mecanismo funciona de la siguiente manera: Si se tiene una estación que desea enviar un mensaje, verifica que otra estación no esté enviando un mensaje. Si escucha que no hay envío de mensaje, entonces envía la transmisión. Pero cuando dos o más estaciones o host desean enviar un mensaje, puede ocurrir que transmitan casi al mismo instante de tiempo, ocasionando una colisión en la red. En ese momento los host receptores ignoran cualquier transmisión que se presente.

Cuando un host transmisor detecta una colisión se envía una señal de alerta a todos los dispositivos conectados notificando que ha ocurrido una colisión. Por lo tanto, cada estación deja de transmitir y esperará un periodo de tiempo aleatorio para que un host transmita nuevamente. De ahí nace el término dominio de colisión; que indica cual computador puede enviar datos en una red.

La técnica CSMA/CD no es adecuada para soportar aplicaciones de procesos en tiempo real. La tecnología que se emplea frecuentemente es la Ethernet; es la base de la especificación 802.3 de la IEEE; de las cuales se

derivan la 802.3u, conocida como Fast Ethernet; 802.3z y 802.3ab Gigabit Ethernet, transmitido en fibra óptica y UTP respectivamente.

Se recomienda emplear a nivel de usuario la tecnología Ethernet, dado que admite velocidades de 10 Mbps. Pero cuando se trata de que los usuarios accedan a los dispositivos se requiere emplear Fast Ethernet; permite velocidades de 100 Mbps. También se puede emplear dispositivos que manejan velocidades hasta de 1Gbps; tecnología Gigabit Ethernet.

1.2.4 LANs con control de acceso por paso de testigo

La tecnología que emplea esta categoría de control de acceso por paso de testigo o determinístico, es Token Ring. Se denomina control de acceso por testigo; los computadores, hosts o estaciones individuales se colocan en forma de anillo, de tal forma que por cada host se transmite un token, que es una trama. Cuando un host desea transmitir, lo retiene y utiliza este token para enviar los datos al destino, transmite los datos por un tiempo limitado y luego envía el token al siguiente host del anillo. Este tiempo normalmente es de 10 ms. En caso de que una estación quiera transmitir requiere que le llegue un token vacío. En un entorno que emplea Token Ring no hay colisiones ya que sólo transmite un host a la vez.

También se ubica dentro del control de acceso determinístico la tecnología

FDDI. Se basa en Token Ring pero de doble anillo, lo cual permite una comunicación tipo full duplex. El tráfico en cada anillo viaja en direcciones opuestas, estos anillos se conocen como primarios y secundarios; el anillo secundario sirve de respaldo al anillo primario que se emplea para la transmisión de datos.

Permite una velocidad hasta de 100 Mbps, emplea una topología física de estrella y lógica de doble anillo al igual que Token Ring, que como su nombre lo indica el material que utiliza para su cableado es la fibra óptica, mientras Token Ring se conecta a través de par trenzado blindado o no.

1.2.5 LANs inalámbricas

Una red inalámbrica se basa principalmente en estándares de la IEEE, estos estándares han sido creados por el Comité Federal de Comunicaciones, FCC[9].

Se han desarrollado estándares que emplean distintas tecnologías como 802.11 que utiliza DSSS; el cual permite trabajar a velocidades de 1 a 2 Mbps. Mediante esta tecnología también es posible llegar a velocidades de 11 Mbps basándose en el estándar 802.11b, conocido como WI-FI.

[9] Cisco Networks CCNA 1 Módulo 1 Capítulo 5.1.8

Para brindar mayor velocidad se desarrolla el estándar 802.11a que puede transmitir a 54 Mbps, pero los dispositivos no son compatibles con los que se basan en el estándar 802.11b. Luego en el 2003 se implementa el estándar 802.11g que es compatible tanto con el 802.11a como con el 802.11b, con una velocidad de 54 Mbps.

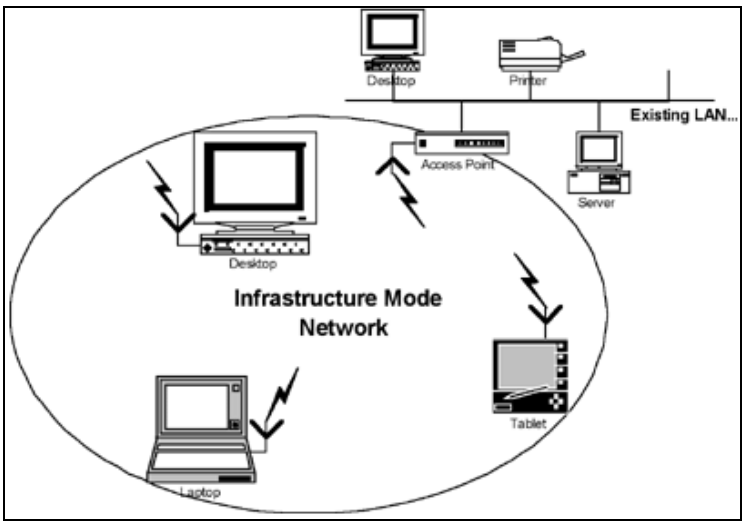


Figura 1.11. Red en modo de Infraestructura

Para la implementación de una red inalámbrica se conocen dos principales topologías: infraestructura y ad hoc. La topología de infraestructura requiere de una red LAN que conecta dispositivos inalámbricos mediante una estación base, que se denomina punto de acceso. Éste ofrece la interoperabilidad entre la red cableada y la red inalámbrica y controla la red inalámbrica. De esta manera se pueden tener varios puntos de acceso que cubran a una red inalámbrica mucho mayor.

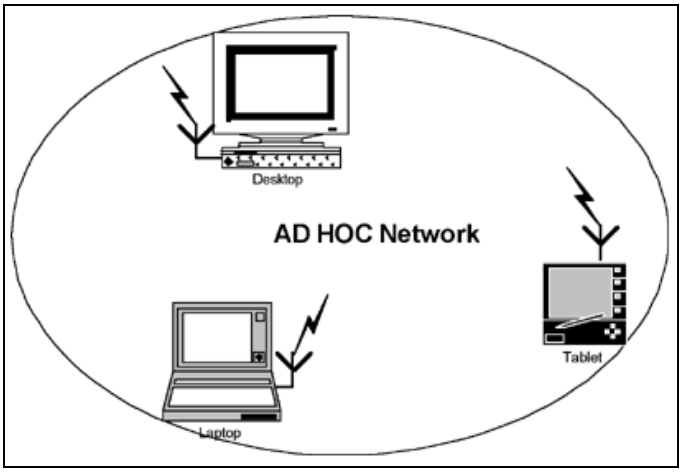


Figura 1.12. Red Ad Hoc

En una red Ad hoc no se requiere de cable ni hay puntos de acceso, los propios dispositivos inalámbricos forman la red. Cada dispositivo se comunica directamente con los demás. Generalmente esto se puede realizar entre pequeños grupos de dispositivos que requieran comunicación.

1.2.6 Interconexión de LANs

El DoD en la década 1960 hasta 1990 desarrollo redes de área amplia, WAN, de gran extensión y alta confiabilidad para uso militar y científico. Una WAN es la interconexión de LANs; de ahí nace el Internet. Para hacer esto posible se requieren diferentes equipos y dispositivos que sirvan de interconexión entre LANs. Los dispositivos más comunes son: switches, bridges, routers y firewalls.

Los switches suelen ser descritos como bridge multipuerto, ambos

dispositivos operan en la capa de enlace del modelo OSI, por lo que se los llama dispositivos de capa 2. El bridge es un dispositivo inteligente, porque es capaz de verificar si deja o no transmitir la información entre un segmento de red y otro; esto lo realiza mediante la dirección MAC destino. Por ejemplo, si el dispositivo destino está en el mismo segmento en donde se origina la trama, el bridge no permite que la trama vaya a otros segmentos. Pero si el dispositivo está en otro segmento, el bridge lo direcciona hacia el segmento correspondiente. En caso de no conocerse la dirección destino se envía a todos los dispositivos, menos al dispositivo del cual se recibe la trama.

La misma función es realizada por el switch con la diferencia de que el bridge puede conectar dos segmentos y el switch más de dos segmentos de red. Por lo tanto el switch es un dispositivo más sofisticado que un puente; dado que tiene varios puertos a los cuales puede conectar segmentos, al momento de recibir una trama debe verificar a que puerto debe enviarla de acuerdo a una tabla; también incluyen otras funciones como VLAN. Por esta razón los switches deben trabajar a velocidades superiores a los bridges.

Los routers de acuerdo al modelo OSI son llamados dispositivos de capa 3, realizan la función de enrutar los paquetes; verificar cual es la ruta más adecuada. Se comunican y comparten información mediante protocolos de enrutamiento. Manejan distintos tipos de conexiones como seriales, BRI

RDSI, DSL, cable MODEM; dando paso a conectar diversos tipos de tecnologías. También se han desarrollado routers inalámbricos.

El firewall es el elemento de interconexión entre una red interna y una red externa que sirve para controlar las comunicaciones de acuerdo a las políticas de red que se establezcan por el encargado de la red. Esto puede ser implementado tanto en hardware como en software, su función es proteger a la red interna de accesos no autorizados. Básicamente lo que brinda un firewall es seguridad en la red, actúa como filtro controlando el tipo de información que pasa de una red a otra, permitiendo o no el paso de información.

1.3 SISTEMAS OPERATIVOS

LAN cliente/servidor

El término cliente/servidor describe un sistema en el que una máquina cliente solicita a una segunda máquina llamada servidor que ejecute una tarea específica.

El cliente suele ser una computadora personal común conectada a una LAN. Generalmente el servidor es una máquina anfitriona como un servidor de archivos, una macrocomputadora ó computadora de rango medio. El programa cliente cumple dos funciones distintas: Gestiona la comunicación

con el servidor, solicita un servicio y recibe los datos. Por otro lado, maneja la interfaz con el usuario: Presenta los datos en el formato adecuado, brinda las herramientas y comandos necesarios para que el usuario pueda utilizar las prestaciones del servidor de forma sencilla.

El programa servidor se encarga de transmitir la información de forma eficiente; no tiene que atender al usuario. De esta forma, un mismo servidor puede atender a varios clientes al mismo tiempo. Algunas de las principales LAN cliente/servidor con servidores especializados que pueden realizar trabajos para clientes incluyen a Windows NT, NetWare de Novell, LINUX; los cuales se tratará más a fondo en este capítulo. Todos estos sistemas operativos de red pueden operar y procesar solicitudes de aplicaciones que se ejecutan en clientes.

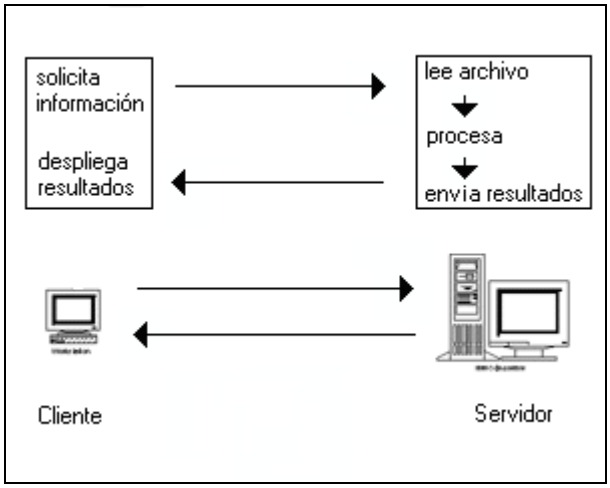


Figura 1.13 Esquema LAN cliente/servidor

1.3.1 Netware de Novell

El enfoque de Novell de servicio al usuario de LAN es único; ha elegido concentrar esfuerzos en la producción de softwares que funcionan en el hardware de redes de otros fabricantes. NetWare funciona en prácticamente cualquier IBM o compatible, y opera en todo el hardware de los fabricantes más importantes de LAN incluyendo los productos de Apple Macintosh y ARCnet. La filosofía de Novell es convertirse en un estándar de la industria, por medio del dominio del mercado.

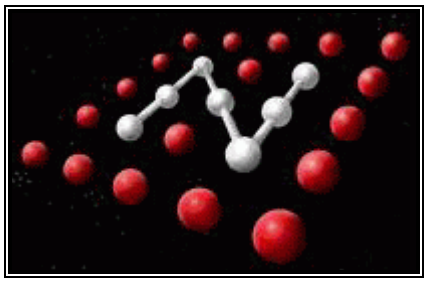


Figura 1.14. Logotipo de Netware de Novel

Arquitectura de NetWare

NetWare está diseñado para ofrecer un verdadero soporte de servidor de archivos de red. En el modelo OSI, el software de servidor de archivos de Novell reside en la capa de aplicaciones, mientras que el sistema operativo de disco reside en la capa de presentación. El software de servidores de archivos forma una cubierta alrededor de los sistemas operativos, como el DOS, y es capaz de interceptar comandos de programas de aplicaciones antes de que lleguen al procesador de comandos. El usuario de las

estaciones de trabajo no se da cuenta de este fenómeno, simplemente pide un archivo de datos o un programa sin preocuparse acerca de dónde está ubicado.

Administración de archivos en NetWare

NetWare permite que el supervisor defina el acceso a directorios. El administrador del sistema puede determinar que un programa o archivo sea compartible o no compartible. NetWare también contiene una función predeterminada de bloqueo de archivos, lo cual significa que los programas de un solo usuario podrían ser utilizados por diferentes usuarios, uno a la vez. Si un archivo no es compartible, los diferentes usuarios pueden ver el archivo en el modo de sólo lectura, pero no pueden escribir en él mientras otro usuario lo esté utilizando en modo de lectura o escritura. Los programas o archivos que se designan como compartibles con capacidad de bloqueo de registros operan en modo multiusuario real; varios usuarios pueden leer y escribir en ellos en forma simultánea, siempre que sólo un usuario escriba en un registro específico en un momento determinado. NetWare requiere que se tenga acceso a los directorios de la red a través de unidades de red específicas. Las unidades de red apuntan a directorios de la red y no a unidades físicas de discos.

Cada estación de trabajo puede asignar 21 letras de unidades lógicas (de la

F a la Z). Esto supone que DOS utiliza las letras predeterminadas de la A a la E. Las unidades de búsqueda de NetWare permiten que el sistema operativo localice los archivos de programas en directorios diferentes del directorio predefinido correspondiente. Al colocar los programas que se usan universalmente en directorios de acceso público y luego mapearlos en una unidad de búsqueda, el servidor de archivos localiza los programas solicitados aún si no se encuentran en el directorio actual desde donde se hace la solicitud. NetWare de Novell ofrece los sistemas de seguridad más importantes del mercado, proporcionando seguridad de servidores de archivos en cuatro formas diferentes: procedimiento de registro de entrada, derechos encomendados, derechos en directorio y atributos de archivo.

Medidas de Seguridad

La seguridad de NetWare se basa en perfiles de usuario definiendo a un usuario como usuarios autorizado en la red. El usuario obtiene una serie de privilegios de uso de los recursos de la red y las impresoras u otros periféricos.

El control del inicio de la sesión de NetWare permite al supervisor controlar el acceso a la red de usuarios no autorizados. Para evitar este tipo de accesos normalmente se emplea el sistema de claves de acceso, pudiendo limitarse la conexión de usuarios autorizados a ciertas estaciones de trabajo, o fuera

de un cierto margen de tiempo. Estos aspectos de la seguridad evitan que los usuarios del sistema puedan usarlo sin el personal responsable. Por razones de seguridad, también es posible cerrar e inhabilitar cuentas temporalmente.

Los directorios de NetWare tienen ocho tipos diferentes de derechos, varios de los cuales no son soportados por DOS. Estos derechos son: Read, Write, Open, Create, Delete, Parental, Search y Modify. Por ejemplo, cualquier usuario tiene la capacidad de cambiarse a un directorio que se encuentre en un nivel superior al suyo, pero si no tiene los derechos adecuados, no tendrá la capacidad de accesar la información contenida por este, es decir, verá el directorio vacío. Las facilidades de seguridad de NetWare permiten al Supervisor:

- Inhabilitar una cuenta de usuario.
- Especificar una fecha de expiración para una cuenta.
- Obligar a un usuario a emplear una clave de acceso.
- Especificar la longitud mínima para dicha clave.
- Obligar a un usuario a cambiar la clave en forma periódica.
- Impedir a un usuario emplear una clave de acceso que haya sido usada antes.
- Fijar el número de veces que un usuario puede iniciar una sesión.

- Restringir el número de estaciones de trabajo desde las cuales el usuario pueda iniciar sesiones de trabajo.
- Delimitar el número de conexiones simultáneas que puede tener cada usuario.
- Señalar la cantidad de espacio en disco que puede utilizar un usuario.
- Llevar un registro de control con todos los inicios y finales de sesión.
- Monitorear los intentos de conexión no permitida y bloqueos de cuentas.
- Comprobar las fallas de seguridad de la red.

Cada media hora, NetWare realiza una comprobación de seguridad para verificar que los usuarios tienen derecho a seguir conectados a la red. Cinco minutos antes de la finalización automática de la sesión, da un aviso[10].

Términos de Licencia

El Sistema Operativo es un Software no libre y para su uso se exige regirse bajo las condiciones de uso dictadas en su respectiva licencia.

Versiones Netware

Cada nivel de NetWare ofrece facilidades superiores a las de niveles inferiores. Las características determinarán cual es la versión adecuada

[10] http://www.geocities.com/v.iniestra/apuntes/dipl_redes/novell.html

dependiendo del número de estaciones de trabajo o de usuarios que se desee tener, si el servidor debe ser dedicado o no, si se han de establecer conexiones con otras redes o no, el grado de seguridad deseado, etc. A continuación se describen algunas de estas facilidades.

NetWare 286

Esta versión de NetWare supone una solución para pequeñas redes donde el costo sea un factor importante. Soportan redes con un solo servidor que no necesitan de utilidades de conexión con otras redes ni fiabilidad.

NetWare 386

Esta es una versión modificada de NetWare 286. Se trata de una versión completamente nueva escrita específicamente para los microprocesadores 386 y 486. El sistema de archivos de NetWare se ha rediseñado para mejorar y aumentar el rendimiento, las facilidades o prestaciones y la capacidad del sistema operativo de atender a diversos sistemas operativos clientes.

NetWare 386 posee un gran número de las facilidades proporcionadas por SFT NetWare, tales como el Hot Fix, el TTS, disco y canal duplicados. Además, las futuras versiones de NetWare 386 tendrán la capacidad de mantener duplicado perfecto del servidor de archivos, por lo que cualquier falla que pudiera presentarse en el sistema resulta totalmente transparente al

usuario. Con SFT Level III, si falla un servidor, el sistema operativo utiliza al servidor duplicado, y los usuarios no percibirán cambios en el funcionamiento del sistema[11].

NetWare 2.2

NetWare 2.2 es la novena generación de la línea NetWare 286, una madurez evidente en los servicios de administración para usuarios y archivos. Configurar los usuarios, establecer los derechos de cuentas y administrar la estructura de directorios son tareas que se realizan con una serie de servicios de menús bien diseñados o con líneas de comandos.

NetWare 3.11.

NetWare 3.11 sigue siendo un líder fuerte y flexible en la arena de los NOS para las compañías pequeñas o grandes. Su única desventaja para los que necesitan una solución a nivel de empresa es que carece de un servicio global de directorios.

Ofrece la habilidad de compartir archivos e impresoras, velocidad, seguridad, apoyo para la mayoría de los sistemas operativos, y una gran cantidad de Hardware, aunque tiene algunas dificultades con la administración de memoria, pero aun así vale la pena, pues tiene algunas otras características

[11] http://www.geocities.com/v.iniestra/apuntes/dipl_redes/novell.html

que lo hacen importante. NetWare 3.11 está diseñado en su mayoría para redes desde pequeñas a moderadamente grandes que consisten en servidores individuales, principalmente porque sus servicios de directorios no integran a la red en su totalidad. Cada uno de los servidores mantiene una base de datos centralizada de verificación individual llamada el Bindery. El Bindery del servidor mantiene la información como los nombres de conexión, las contraseñas, los derechos de acceso y la información de impresión. Si los usuarios necesitan conectarse a más de un servidor para compartir recursos, deben hacerlo manualmente con cada servidor[12].

NetWare 4.0.

NetWare 4.0 ofrece la conexión simplificada de múltiples servidores, la capacidad de compartir recursos en la red y la administración centralizada en un producto coherente lleno de características.

NetWare 5.0.

El sistema operativo de red de Novell, NetWare, puede funcionar en varias topologías diferentes. Dependiendo del hardware que se seleccione, NetWare puede ejecutarse en una red configurada como estrella, agrupamiento de estrellas, Token Ring e incluso en un bus.

---

[12] http://www.monografias.com/trabajos12/sisope/sisope.shtml

Ventajas de Netware

- Multiusuario.
- No requiere demasiada memoria RAM, y por poca que tenga el sistema no se ve limitado.
- Brinda soporte y apoyo a la MAC.
- Apoyo para archivos de DOS y MAC en el servidor.
- El usuario puede limitar la cantidad de espacio en el disco duro.
- Permite detectar y bloquear intrusos.
- Soporta múltiples protocolos.
- Soporta acceso remoto.
- Permite instalación y actualización remota.
- Muestra estadísticas generales del uso del sistema.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar auditorías de acceso a archivos, conexión y desconexión, encendido y apagado del sistema, etc.
- Soporta diferentes arquitecturas.

Desventajas de NetWare.

- No cuenta con ACLs administradas en base a cada archivo.
- Algunas versiones no permiten criptografía de llave pública ni privada.
- No carga automáticamente algunos manejadores en las estaciones de

trabajo.

- No ofrece mucha seguridad en sesiones remotas.
- No permite el uso de múltiples procesadores.
- No permite el uso de servidores no dedicados.

1.3.2 Windows NT Server de Microsoft

Microsoft Windows NT Server es un sistema operativo diseñado para su uso en servidores de LAN. Ofrece la potencia, la manejabilidad y la capacidad de ampliación de Windows NT en una plataforma de servidor. Este sistema operativo incluye características, como la administración centralizada de la seguridad y tolerancia a fallos más avanzada, que hacen de él un sistema idóneo para servidores de red.

Windows NT Server es un sistema operativo para computadoras personales; y a su vez, un sistema operativo para red. Puesto que incorpora funciones de red, las redes de Windows NT Server se integran de forma óptima con el sistema operativo básico, facilitando el uso y la administración de las funciones.

Figura 1.15 Logotipo de Windows NT de Microsoft

Características

Windows NT de Microsoft es un sistema operativo de 32 bits, que está disponible en versiones cliente y servidor. Entre las características clave de NT está la multitarea prioritaria, procesos de multilectura o hebras, portabilidad y soporte para multiprocesamiento simétrico. La multitarea prioritaria permite la realización de múltiples tareas preferentes y subordinadas. Es NT y no los programas específicos quien determina cuando deberá interrumpirse un programa y empezar a ejecutar otro.

Procesos de lectura múltiple o hebras, es un término que en NT, se refiere a los hilos que funcionan como agentes de ejecución. Tener hebras de ejecución múltiple dentro de un mismo proceso, significa que un proceso ejecuta, de manera simultánea, diferentes partes de un programa en diferentes procesadores. El multiprocesamiento simétrico permite que los requerimientos de sistema y aplicación se distribuyan de manera uniforme

entre todos los procesadores disponibles, haciendo que todo funcione mucho más rápido. Windows NT emplea el sistema de archivos NT, NTFS. Este sistema de archivos soporta nombres de archivo de hasta 256 caracteres. También permite el rastreo de transacciones. Esto significa que si el sistema falla, NT regresa los datos al estado inmediato anterior a la caída del sistema. Microsoft diseñó Windows NT para que fuera portátil. Está compuesto de un kernel o núcleo, así como de diferentes subsistemas del sistema. Hay subsistemas disponibles para aplicaciones que ejecutan programas basados en OS/2 y POSIX. Un procesador DOS virtual (VDM) ejecuta MS-DOS y aplicaciones Windows de 16 bits. NT incluye software de red de punto a punto para que los usuarios de NT puedan compartir archivos y aplicaciones con otros usuarios que ejecuten NT o Windows para Trabajo en Grupo[13].

Medidas de Seguridad en NT

Windows NT requiere que los usuarios introduzcan una contraseña cada vez que inician el sistema operativo, estén o no conectados a un servidor. Cada vez que se inicia NT, éste solicita una contraseña. Una función de seguridad de NT es el administrador de usuarios. Este programa garantiza que las contraseñas se sujeten a la política de la compañía. También permite que cada máquina NT sea configurada para cierto número de usuarios, dando a

[13] http://www.geocities.com/SiliconValley/8195/noscs.html

cada uno de ellos su propio nivel de privilegios. Además es posible crear grupos y dar los mismos privilegios a todos los integrantes de un grupo. Otra función de seguridad clave es el visor de eventos. Este programa le permite a los administradores de red visualizar una bitácora de todos los errores e infracciones a la red, incluyendo la hora, fecha y tipo de infracción, así como el lugar donde ocurrió el evento y el nombre del usuario implicado[14].

Términos de Licencia

Existen 2 tipos de licenciamientos los cuales se nombran y explican a continuación:

Licenciamiento por servidor:

Cada licencia para acceso de cliente se asigna a un servidor en particular y permite acceder a este equipo para ser usado y así poder utilizar los servicios de red (archivos, impresión, comunicaciones). La conexión se establece a un servidor, y no a un recurso compartido individual.

Licenciamiento por sitio

Una licencia para acceso de cliente es aplicada a una estación de trabajo en particular. De esta manera, un ilimitado número de computadoras pueden acceder al servidor. Si la computadora está ejecutando alguno de los

[14] http://www.geocities.com/SiliconValley/8195/noscs.html

sistemas operativos clientes de Microsoft como WFW, W95, WNT WKS, se requiere una licencia de acceso al servidor por cada uno de ellos antes de que el cliente se conecte y utilice los recursos del servidor[15].

Ventajas de Windows NT Server

- La instalación es muy sencilla y no requiere de mucha experiencia.
- Multitarea.
- Multiusuario.
- Apoya el uso de múltiples procesadores.
- Soporta diferentes arquitecturas.
- Permite el uso de servidores no dedicados.
- Soporta acceso remoto.
- Ofrece mucha seguridad en sesiones remotas.
- Brinda apoyo a la MAC.
- Apoyo para archivos de DOS y MAC en el servidor.
- El sistema está protegido del acceso ilegal a las aplicaciones en las diferentes configuraciones.
- Ofrece la detección de intrusos.
- Permite cambiar periódicamente las contraseñas.
- Soporta múltiples protocolos.
- Carga automáticamente manejadores en las estaciones de trabajo.

[15] http://www.monografias.com/trabajos5/miwi/miwi.shtml

- Trabaja con impresoras de estaciones remotas.
- Soporta múltiples impresoras y asigna prioridades a las colas de impresión.
- Muestra estadísticas de Errores del sistema, Caché, Información del disco duro, Información de Manejadores, Número de archivos abiertos, Porcentaje de uso del CPU, Información general del servidor y de las estaciones de trabajo, etc.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar diferentes tipos de auditorías, tales como del acceso a archivos, conexión y desconexión, encendido y apagado del sistema, errores del sistema, información de archivos y directorios, etc.

Desventajas de Windows NT:

- Tiene ciertas limitaciones por RAM, como; Número. máximo de archivos abiertos y almacenamiento de disco total.
- Requiere como mínimo 16 Mb en RAM, y procesador Pentium a 133 MHz o superior.
- El usuario no puede limitar la cantidad de espacio en el disco duro.
- No soporta archivos de NFS.
- No ofrece el bloqueo de intrusos.
- No soporta la ejecución de algunas aplicaciones para DOS.

- No permite criptografía de llave pública ni privada.
- No permite realizar algunas tareas en sesiones remotas, como instalación y actualización.

1.3.3 Linux

Linux es un clon del sistema operativo UNIX que corre en varias plataformas, especialmente en computadoras personales con procesadores Intel 80386 o mejores. Linux puede convertir cualquier computadora personal en una estación de trabajo con las mejores cualidades de UNIX y sin costo. Fue y todavía es desarrollada por un grupo de voluntarios, principalmente de Internet, quienes intercambian código, reportan trucos y resuelven problemas en un ambiente completamente abierto. Existe un conjunto de documentos de estandarización publicados por la IEEE denominados POSIX. Linux antes que nada satisface los documentos POSIX-1 y POSIX-2. Linux tiene una ante memoria o caché que mejora el rendimiento del disco. Esto significa que temporalmente guarda en RAM información perteneciente al sistema de almacenamiento permanente. Las diferencias entre lo que Linux cree que hay en el disco y lo que efectivamente está almacenado en él, se sincronizan cada 30 segundos. En Linux se puede correr la mayoría del software popular para UNIX, incluyendo el sistema de ventanas X.

El Sistema X Window, o simplemente X, es una interfaz gráfica de usuario

estándar para máquinas UNIX y es un poderoso ambiente que soporta muchas aplicaciones. Usando el Sistema X Window, se pueden tener múltiples ventanas de terminales en la pantalla a la vez (consolas virtuales), cada una teniendo una diferente sesión de trabajo. El sistema Linux es mayormente compatible con varios estándares de UNIX al nivel fuente, incluyendo IEEE POSIX.1, UNIX System V, y Berkeley System Distribution UNIX, BSD. Todo el código fuente para el sistema Linux, incluyendo el kernel o núcleo, drivers, librerías, programas de usuario y herramientas de desarrollo son gratis.

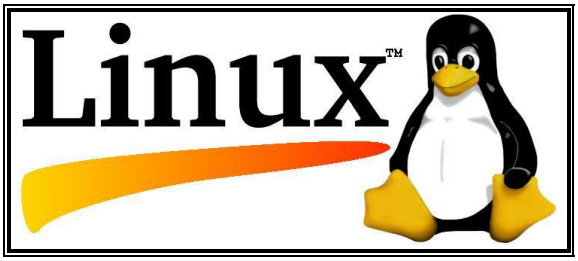


Figura 1.16. Logotipo de Linux

Arquitectura

Linux es un núcleo monolítico híbrido. Los controladores de dispositivos y las extensiones del núcleo normalmente se ejecutan en un espacio privilegiado conocido como anillo 0, con acceso irrestricto al hardware, aunque algunos se ejecutan en espacio de usuario. A diferencia de los núcleos monolíticos tradicionales, los controladores de dispositivos y las extensiones al sistema operativo se pueden cargar y descargar fácilmente como módulos, mientras

el sistema continúa funcionando sin interrupciones. A diferencia de los núcleos monolíticos tradicionales, los controladores pueden ser pre-volcados, detenidos momentáneamente por actividades más importantes, bajo ciertas condiciones. Esta habilidad fue agregada para manejar correctamente interrupciones de hardware, y para mejorar el soporte de Multiprocesamiento Simétrico.

El kernel de Linux puede correr sobre muchas arquitecturas de máquina virtual tanto como host del sistema operativo como cliente. La máquina virtual usualmente emula la familia de procesadores Intel x86, aunque en algunos casos también son emulados procesadores de Power PC o AMD.

Medidas de Seguridad

Linux ofrece seguridad en muchos campos y áreas, Seguridad en el sistema de cuentas, como el control de los passwords. El control de las cuentas, seguridades el es sistema de ficheros, como seguridad en las bibliotecas compartidas, encriptación de ficheros, control de los dispositivos, seguridad en la red, como clonación de maquinas (MAC), autenticación de la red, hosts compartidos, terminales seguros, seguridad dl sistema NFS, seguridad del NIS, seguridad del DNS, seguridad de FTP y Telnet, Seguridad en protocolos POP y SMTP para correos electrónicos, Firewalls. Sin duda este último campo es el más importante para un administrador de red; con una red

insegura la información de una empresa esta muy vulnerable.

Términos de Licencia

Inicialmente, Linus Torvalds, creador de Linux, distribuyó Linux bajo los términos de una licencia que prohibía la explotación comercial. Pero esta licencia fue reemplazada, poco tiempo después, por la GNU GPL. Los términos de esta última licencia permiten la distribución y venta de copias o incluso modificaciones, pero requiere que todas las copias del trabajo original y trabajos de autoría derivados del original sean publicados bajo los mismos términos, y que código fuente siempre pueda obtenerse por el mismo medio que el programa licenciado. Torvalds se ha referido a haber licenciado Linux bajo la GPL como "lo mejor que he hecho nunca"; en inglés, "the best thing I ever did[16]".

Ventajas

- Linux es muy robusto, estable y rápido: Ideal para servidores y aplicaciones distribuídas. A esto se añade que puede funcionar en máquinas humildes: Linux puede correr servicios en un x86 a 200 MHz con calidad.
- Linux es libre: Esto implica no sólo la gratuidad del software, sino también que Linux es modificable y que Linux tiene una gran cantidad

[16] http://es.wikipedia.org/wiki/Linux_(n%C3%BAcleo)#Arquitectura

de aplicaciones libres en Internet. Todo ello apoyado por la inmensa documentación de Linux que puede encontrarse en la Red.

- Linux no está restringido a personas con grandes conocimientos de informática: Los desarrolladores de Linux han hecho un gran esfuerzo por dotar al sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente. Distribuciones Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows.

Desventajas

- Incompatibilidad con aplicaciones de otros sistemas operativos por ejemplo el Autocad de Windows.
- Poco soporte técnico profesional: Pocas empresas se dedican a dar soporte técnico profesional en este sistema operativo.

CAPÍTULO 2

AUDITORÍA DE LA SEGURIDAD

2.1 FASES Y TIPOS DE AUDITORÍA

2.1.1 Fases de la Auditoría

La auditoría de la seguridad en una red de comunicación es el estudio que comprende el análisis y gestión de sistemas para determinar y corregir las diversas vulnerabilidades que se pueden presentar.[17]

Para realizar una auditoría se debe realizar una planeación de la misma; ésta se expresa a manera de fases de la auditoría. Se las puede numerar de la siguiente manera:

[17] http://es.wikipedia.org/wiki/Auditoría_de_seguridad_de_sistemas_de_información

Identificación del sistema

El sistema comprende la empresa en la que se realiza la auditoría, en donde se observan las personas y las aplicaciones para las cuales se utiliza la red. Se debe considerar las políticas de la empresa, lo cual es fundamental para el momento de la evaluación; es la referencia para verificar el tipo de control que se posee. Se identifica el sistema, la distribución de la empresa; es decir el organigrama de las áreas en el sistema, las funciones que poseen las personas que comprenden el sistema.

Lo que se desea es analizar el modo de empleo de la red, detallar un manual que sirva de guía utilizando procedimientos en el manejo de la red, identificar las personas que están autorizadas a la administración de la red. Esto se logra mediante claves de acceso, de manera que se brinde seguridad en la aplicación.

Análisis de procesos y recursos en la red

Consiste en identificar los procesos y dependiendo del tamaño del sistema, subprocesos, en base a los flujogramas que determinan el recorrido de los procesos y de la información; esto es manejado por los administradores de la red. Cuando se habla de recursos en la red, pues se trata de los dispositivos que se emplean en la red y las funciones que realizan.

Estos dos aspectos están ligados; los dispositivos cumplen las funciones que los usuario les exigen, por lo que es importante seguir los procesos establecidos en el sistema.

Análisis de riesgos y amenazas

Se identifican los riesgos que se presentan en la red, lo que incluye el riesgo de dispositivos y pérdida de recursos. Los dispositivos corren el riesgo de dañarse, de ser robados; de esta manera existe el riesgo de pérdida de información, con ello, la integridad de los datos. Esto provoca que las operaciones y procesos que se realizan sean ineficientes. En esta parte se procura verificar cuales son los errores que existen con el manejo de la información.

Para identificar los riesgos antes mencionados, se deben analizar cuales son las amenazas que se presentan; luego verificar que amenaza a los equipos, los documentos fuente y principalmente a los programas de aplicación. Se relacionan los recursos, los riesgos y las amenazas en el ambiente propio de trabajo en el cual se están suscitando.

Análisis y evaluación de controles

Se debe controlar a los grupos que utilizan los recursos, codificando a cada grupo de acuerdo a los recursos que maneje. Debe haber uno o más

controles sobre los recursos, los riesgos y las amenazas. El análisis de los controles procura determinar si los controles aplicados que el auditor consideró necesario brindan la protección requerida de los recursos.

Informes de la Auditoría y Recomendaciones

Una vez identificado el tipo de red, los recursos, las aplicaciones, los riesgos, las amenazas; se realiza un informe detallando cuales son las partes débiles de la red que están siendo amenazadas, y los riesgos que representan para la seguridad e integridad de la información.

La última fase que se presenta en una auditoría, es el seguimiento de las recomendaciones que se indicaron. Se detalla un informe de dicho seguimiento y se evalúan los resultados de acuerdo a los controles que se implementaron luego de indicar las recomendaciones.

2.1.2 Tipos de Auditoría

La auditoría de seguridad en una red de datos se debe analizar de manera interna, como de manera externa. La integridad de los datos se puede ver afectada en por los usuarios de la red, y por agentes externos que amenacen o quieran penetrar la red. Por lo tanto existen dos tipos generales de auditoría: Auditoría de Seguridad Interna y Auditoría de Seguridad Perimetral.

2.1.2.1 Auditoría de Seguridad Interna

La Auditoría de Seguridad Interna evalúa la seguridad de las redes internas y corporativas de la empresa. Esta evaluación permite determinar las debilidades de los sistemas de información internos, de manera que se puede simular y establecer las consecuencias de un ataque desde dentro de la propia organización ó de un hacker que haya conseguido alcanzar la intranet.

Características

- Proporciona una visión detallada del estado de la seguridad en la red interna.
- Conectando un sistema a la red interna se intenta obtener acceso a los servidores e información privilegiada que está localiza en esta red.
- Se simula la actuación de un hacker que ha conseguido penetrar en la red interna. El objetivo es que se detecte la presencia de alguien ajeno a la red.
- Se simula la actuación de un empleado de la empresa que intenta utilizar recursos de la red interna para los que no tiene permisos. De esta manera se verifica que los accesos y los privilegios estén funcionando de manera adecuada.

- Se utiliza la misma metodología y técnicas que en los test de intrusión, excepto que ahora se ha de tener en cuenta que los ataques se realizan desde dentro de la red interna.
- Se incluye la revisión de la política de seguridad de la empresa.
- La auditoría debe realizarse en el lugar en donde se ejecutan las aplicaciones, en donde está manejándose la red.[18]

2.1.2.2 Auditoría de Seguridad Perimetral

En esta auditoría, el perímetro de la red local o corporativa es analizado y evaluado de acuerdo a las entradas exteriores, al tipo de acceso que pudiese tener un agente externo. Se desea determinar la seguridad de la frontera de las redes internas y el Internet.

Para establecer la seguridad perimetral se pueden implementar varias opciones, entre ellas se exponen las siguientes, que se complementan:

Control de Accesos de entrada y salida a la red corporativa

Se logra mediante firewalls, herramienta que permite poner una barrera de control, aislando a la red del exterior de una manera segura. Además, da la posibilidad de auditar y gestionar las conexiones de la red y el acceso a los recursos de la empresa.

[18] http://www.isecauditors.com/es/auditoria-interna.html

Sistemas de Detección de intrusos, IDS

Se logra mantener vigilada la red corporativa de posibles intrusos, de tal manera que se puede establecer medidas reactivas de protección ante determinadas alarmas de seguridad.

2.2 TÉCNICAS, MÉTODOS, HERRAMIENTAS DE AUDITORIA DIAGNÓSTICO DE REDES DE COMUNICACIÓN.

2.2.1 Técnicas y Métodos para proteger una red

Existen distintos tipos de técnicas de seguridad, se debe tener conocimiento de la mayor parte de estos; de modo que al momento de implementar dichas técnicas se utilicen las más adecuadas. Muchas de éstas técnicas requieren de un usuario que maneje y controle la prueba. Sin embargo, también hay otras pruebas que se manejan prácticamente de manera automática y requieren menor interacción con el usuario.

Para un resultado eficiente se implementa más de una prueba a la red, estas pruebas deben complementarse; con el objetivo de tener una visión más completa de cómo está la red.

Se citan ciertos tipos de técnicas de testeo a continuación:

Escaneo de Red

Emplea un puerto de escaneo para detectar todos los computadores conectados a la red, los servicios empleados en la red, como FTP y http, y el tipo de aplicación específica que está utilizando. El escaneo nos brinda como resultado una lista en donde se muestran los computadores conectados y los servicios que utilizan, las impresoras, los switches, ruteadores que operan en la parte de la red que se escanea mediante la herramienta de puerto de escaneo; cualquier dispositivo que tenga una dirección de red o que tenga acceso.

El puerto de escaneo identifica los computadores activos que están conectados en el rango de direcciones de red que especifique el usuario mediante paquetes de TCP/IP, ICMP, ECHO e ICMP ECHO_Reply. Una vez que se identifican estos computadores son escaneados con el objetivo de abrir los puertos TCP y UDP que sirven para identificar los servicios que operan en la red de dichos computadores. De esta manera dependiendo el número de puerto que se utilice se puede verificar por ejemplo el tipo de sistema operativo que utiliza el computador; así como la aplicación que se maneja, si se identifica que el puerto TCP 80 está abierto, se sabrá que se está teniendo acceso a un servidor web.

El auditor es quien debe estar capacitado para analizar la información que

ofrece esta herramienta, ciertas organizaciones se enfocan en:

- Verificar los computadores que no están autorizados a conectarse a la red de la organización.
- Identificar servicios que presentan vulnerabilidad.
- Identificar desviaciones en los servicios permitidos definidos por las políticas de seguridad de la organización.
- Preparar para la prueba de penetración.
- Asistir en la configuración de IDS.
- Recoger evidencia forense.

Los resultados del escaneo de la red deben ser documentados y corregir las deficiencias de estos; se debe corregir de la siguiente manera:

- Investigar y desconectar los computadores no autorizados.
- Deshabilitar y remover los servicios innecesarios y vulnerables.
- Modificar los computadores que sean vulnerables y restringir el acceso a los servicios vulnerables en un número limite de computadores.
- Modificar en el firewall la restricción al acceso de servicios conocidos como vulnerables.

Escaneo de Vulnerabilidad

Se caracteriza por ser el siguiente nivel con respecto al escaneo de puerto. Actúa de la misma manera que el escaneo de puerto, identificando los

computadores y los puertos abiertos; además provee información con respecto a las vulnerabilidades. Este tipo de escaneo identifica daños en un sistema operativo ó una aplicación; por ejemplo, si una versión de software está vencida, la actualización de un sistema operativo. También brindan corrección y arreglo automático con respecto a ciertas vulnerabilidades que se identifiquen.

La desventaja de este tipo de escaneo es que puede advertir de riesgos falsos; por lo tanto, un administrador de red debe estar capacitado para interpretar los resultados de este escaneo. Además, el escaneo de vulnerabilidad congestiona más el tráfico de la red que el escaneo mediante puerto, dado que requiere mayor información. Otro factor importante que afecta a la red con el uso de esta herramienta, es la actualización constante de la base de datos de acuerdo a las últimas vulnerabilidades encontradas.

Lo que se obtiene mediante un escaneo de vulnerabilidades pueden ser:

- Identificación de los computadores activos en la red.
- Identificación de los servicios activos y vulnerables en los puertos en la red.
- Identificación de aplicación.
- Identificación de sistemas operativos.
- Identificación de vulnerabilidades asociadas con los sistemas

operativos y aplicaciones encontrados.

- Identificación de configuraciones erróneas.
- Verificar si las aplicaciones de los computadores están se manejan de acuerdo al uso y políticas de la empresa.
- Establecer fundamentos para la prueba de penetración.

Existen dos tipos de escáner: escáner de red y escáner de computadora. El escáner de red, se lo instala en la red realizando el escaneo a los computadores que pertenezcan a ella. El escáner de computadora en cambio se instala en cada computadora para que sea examinada e identificar las vulnerabilidades del sistema operativo y las aplicaciones erróneas. El escáner de computadora pueden detectar vulnerabilidades en un nivel mucho mayor que el escáner de red.

Los resultados del escaneo de vulnerabilidad deben ser documentados y corregir las deficiencias de estos; se debe corregir de la siguiente manera:

- Actualizar o parchar sistemas vulnerables.
- Tomar medidas de precaución en caso de que un sistema operativo no pueda ser parchado inmediatamente, de manera que se minimice la probabilidad de que este sistema se vea afectado.
- Mejorar la administración de los programas de configuración y los procesos, de manera que los sistemas sean actualizados

constantemente.

- Asignar una persona que monitoree las alertas de vulnerabilidad y las listas de correo, analice las aplicaciones de acuerdo al ambiente de trabajo y realice los cambios apropiados.
- Modificar las políticas de seguridad de la organización, arquitectura y documentación.

Craqueo de Claves

Se emplean programas que se utilizan para identificar claves débiles; verificando que los usuarios utilicen claves fuertes que sean difíciles de descifrar. Las claves suelen almacenarse y transmitirse de forma encriptada en una función de correspondencia. Cuando un usuario ingresa su clave en un computador, una función de correspondencia se genera y se compara con el que esta almacenado. Si coinciden ambas funciones, el usuario es autenticado.

Durante una prueba de penetración ó un ataque real, este programa captura la función de correspondencia de la clave. Estas claves pueden ser interceptadas cuando viajan a través de la red ó pueden ser recuperadas mediante el sistema. Una vez que se obtiene esta función de correspondencia este programa rápidamente genera funciones de correspondencia hasta que se encuentre la que coincida.

Dos de los métodos más comunes de craqueo de claves es mediante ataque de diccionario y el ataque híbrido, que se basa en el ataque de diccionario añadiendo caracteres de símbolo y numéricos. El método más poderoso en craqueo de claves es el llamado fuerza bruta; genera aleatoriamente claves y las funciones de correspondencia asociadas a estas.

Revisiones de Registro de usuarios

Implica varios tipos de registro de sistemas que se pueden utilizar para identificar desviaciones de las políticas de seguridad. No es considerada propiamente una prueba; sin embargo la revisión de registro y el análisis del mismo brinda un panorama del las actividades del sistema, se puede verificar que se realicen de acuerdo a las políticas de seguridad.

Este tipo de programas debe aplicarse con frecuencia, se aplica en servidores y firewall. Las medidas que corresponde tomar cuando un sistema no está funcionando de acuerdo a las políticas:

- Remover los servidores vulnerables si es que no son necesarios.
- Reconfigurar el sistema como se requiere para disminuir el riesgo.
- Cambiar la política del firewall limitando el acceso a servicios y sistemas vulnerables.
- Cambiar la política del firewall limitando el acceso desde sub red IP que sea riesgosa.

Evaluación de la Integridad de los archivos

El evaluador de la integridad de los archivos analiza y almacena un checksum de cada archivo y establece una base de datos de los checksum de los archivos. Esto debe ser verificado de manera regular para comparar el valor actualizado con el almacenado e identificar si se ha producido algún cambio. Esta evaluación de integridad de los archivos usualmente se incluye en los sistemas de detección de intrusos.

Detector de Virus

Los virus, troyanos, gusanos pueden contraerse de varias maneras: mediante la conexión a Internet, usando dispositivos de almacenamiento removibles y ciertos tipos de software en donde se comparte información. Se utilizan las técnicas de escaneo de virus y prevención de infección de virus para identificar problemas de virus y detección de intrusos y responder ante esta situación[19].

El escaneo de virus se basa en un algoritmo que puede escanear entre diferentes fuentes al mismo tiempo; de tal modo que es capaz de detectar troyanos y gusanos, sean conocidos o desconocidos. Esta herramienta escanea los discos duros y si detecta este tipo de amenazas las pone en cuarentena ó las remueve.

[19] Network Security Bible. Chapter 17. Intrusion Detection and Response. Página 567

Por otro lado las herramientas de prevención de virus, éste se almacena en la memoria y monitorea la actividad del sistema, y filtra los programas ejecutables y archivos específicos.

Testeo de LAN Inalámbricas

Las redes inalámbricas han crecido rápidamente, actualmente el protocolo más popular empleado en las redes inalámbricas es el 802.11b; pero presenta fallas en la implementación WEP. Por lo tanto, el riesgo es significativo dado que la mayoría de los equipos utilizan este protocolo y están siendo configurados de manera insegura, con una configuración defectuosa. Dada esta situación, si alguna persona esta cerca de una red inalámbrica puede tener acceso a ella si no está protegida adecuadamente.

Desafortunadamente, existen varias vulnerabilidades con respecto al protocolo de red 802.11b:

- Ataques de inserción.
- Intercepción y monitoreo del tráfico inalámbrico.
- Denegación de servicio.
- Ataque de cliente a cliente.

Prueba de penetración

La prueba de penetración es una prueba de seguridad en la que el evaluador intenta burlar las medidas de seguridad de un sistema basado en su conocimiento del diseño e implementación. El propósito es identificar los métodos para tener acceso usando herramientas y técnicas que usan los atacantes comúnmente; se detecta el grado de vulnerabilidad de los sistemas frente a los ataques externos y se evalúa la capacidad de detección frente a estos ataques.

2.2.2 Herramientas de Auditoría y Diagnóstico de Redes de Comunicación.

La herramienta de software que más se utiliza se denomina analizador de protocolo, es un programa que permite a la computadora la capturar tramas de una red, posteriormente o en tiempo real, y proceder a su análisis. Un programa es capaz de reconocer que la trama capturada transporta información asociada a un protocolo concreto: por ejemplo a TCP, a ICMP; y muestra al usuario la información convenientemente decodificada[20].

El funcionamiento de un analizador de protocolo se basa en las tramas, por medio de estas se envía la información; cada trama contiene la siguiente información:

[20] http://www.planeta-digital.com/cursos/mod/forum/discuss.php?d=234

- Dirección de origen, dirección del adaptador de red en el que se origina la trama.
- Dirección de destino, dirección del adaptador de red que debe recibir la trama; la cual puede especificar a un grupo de adaptadores.
- Información de encabezado, identifica el protocolo que se utiliza para enviar la trama.
- Datos

Los analizadores de protocolos proporcionan varias ventajas para el monitoreo de las redes:

- Analizar y soportar demandas de nuevas aplicaciones; ejemplo VoIP.
- Obtener mayor eficiencia de la red, al analizar todo lo que pasa por ella y detectar problemas concretos.
- Analizar redes remotas.
- Analizar y monitorear varias redes al mismo tiempo

Es importante considerar que para realizar una auditoría se debe establecer el perfil el auditor de seguridad de redes de datos; quien será la herramienta clave en el proceso de la auditoría. Se debe examinar la actuación del auditor frente a la ocurrencia de delitos, estrategias para evitarlos, recomendaciones adecuadas, conocimientos requeridos, de manera que se eviten de delitos informáticos.

Perfil del Auditor

El perfil que se requiere para llevar a cabo auditorias de seguridad en redes de datos no está regulado, pero es evidente que es necesaria una formación y sobre todo una experiencia acorde con la función, e incluso con las áreas a auditar como la seguridad física, sistemas operativos concretos, gestores de bases de datos o plataformas e incluso códigos si hubiera que llegar a revisar programas. Actualmente existe una certificación internacional, "CISA", que certifica a los auditores de sistemas informáticos, la misma que es otorgado por una organización reconocida internacionalmente identificada como es Asociación de Control y Auditoria de Sistemas de Información, "ISACA"[21].

El auditor como encargado de la verificación y certificación de la seguridad en las redes de datos dentro de las organizaciones, deberá contar con un perfil que le permita poder desempeñar su trabajo con la calidad y la efectividad esperada. Para ello a continuación se establecen algunos elementos con que deberá contar[22]:

Conocimientos generales.

- Todo tipo de conocimientos tecnológicos, de forma actualizada y especializada respecto a las plataformas existentes en la organización.
- Normas estándares para la auditoría interna.

[21] Security Managment Handbook. Cap 56. Pag 1121
[22] Security Managment Handbook. Cap 71. Pag 1315

- Políticas organizacionales sobre la información y las tecnologías de la información.
- Características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, compensaciones monetarias a los empleados, extensión de la presión laboral sobre los empleados, historia de la organización, cambios recientes en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, entre otros.
- Aspectos legales.

2.3 NORMAS DE SEGURIDAD

2.3.1 ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y

maximizar el retorno de las inversiones y las oportunidades de negocio.

Historia

En 1995 el BSI publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información. En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información. Tras una revisión de ambas partes del BS 7799 en 1999, la primera es adoptada como norma ISO en el 2000 y denominada ISO/IEC 17799 la cual se caracteriza por:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Aplicable para toda organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de seguridad concreta y recomendaciones neutrales con respecto a la tecnología.

La seguridad de la información se define como la preservación de:

Confidencialidad

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Integridad

Garantía de la exactitud y completitud de la información y de los métodos de

su procesamiento.

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Estructura de la Norma

Dominios de Control

La norma ISO/IEC 17799 establece 4 grupos de seguridad, los cuales tienen en conjunto diez dominios de control que cubren por completo la gestión de la seguridad de la información:

Seguridad organizativa

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.

- Gestión de continuidad del negocio.

Seguridad lógica

- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.

Seguridad física

- Seguridad física y del entorno.

Seguridad legal

- Conformidad con la legislación.

De estos dominios se derivan objetivos de control que son los resultados que se esperan alcanzar mediante la implementación de controles, los cuales son las prácticas, procedimientos o mecanismos que reducen el nivel de riesgo.

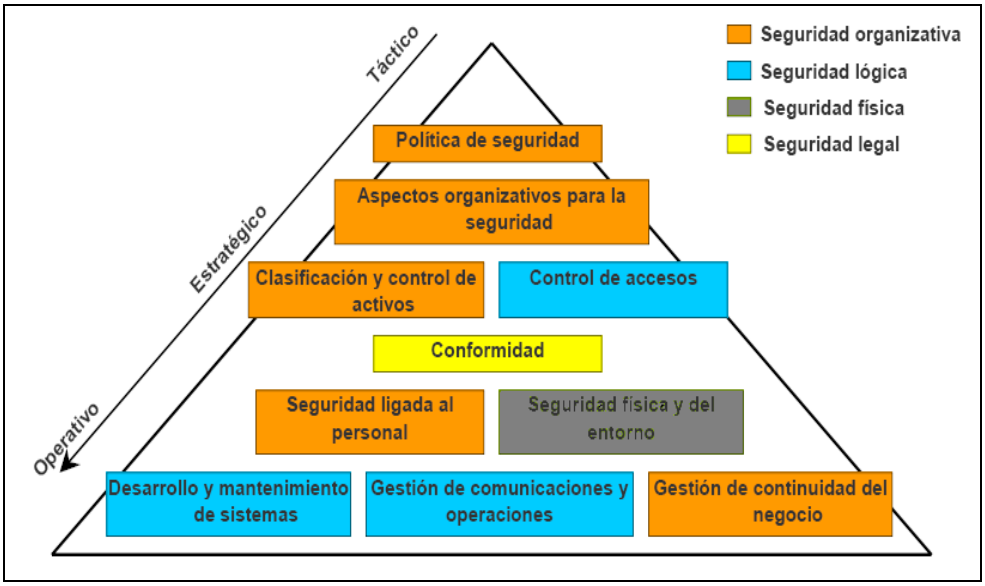


Figura 2.1. Proceso Jerárquico de los dominios de control

Objetivos de Control

1. POLÍTICA DE SEGURIDAD

- Dirigir y dar soporte a la gestión de la seguridad de la información.

La alta dirección de la organización debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicarla de la forma adecuada a todo el personal implicado en la seguridad de la información.

La política se constituye en la base de todo el sistema de seguridad de la información. La alta dirección debe apoyar visiblemente la seguridad de la

información en la compañía.

2. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- Gestionar la seguridad de la información dentro de la organización.
- Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.
- Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma. Dicha estructura debe poseer un enfoque multidisciplinario: los problemas de seguridad no son exclusivamente técnicos.

3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

- Mantener una protección adecuada sobre los activos de la organización.
- Asegurar un nivel de protección adecuado a los activos de información.

Debe definirse una clasificación de los activos relacionados con los sistemas

de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

4. SEGURIDAD LIGADA AL PERSONAL

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.
- Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Las implicaciones del factor humano en la seguridad de la información son muy elevadas. Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global. Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc. Procesos de notificación de incidencias claros, ágiles y conocidos por todos.

5. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres.

Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados. Estos planes de contingencia deben ser probados y revisados periódicamente.

Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Minimizar el riesgo de fallos en los sistemas.
- Proteger la integridad del software y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

- Evitar daños a los activos e interrupciones de actividades de la organización.
- Prevenir la perdida, modificación o mal uso de la información intercambiada entre organizaciones.

Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para el negocio.

7. CONTROL DE ACCESOS

- Controlar los accesos a la información.
- Evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles:

sistema operativo, aplicaciones, redes, etc.

8. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- Asegurar que la seguridad está incluida dentro de los sistemas de información.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura.
- Mantener la seguridad del software y la información de la aplicación del sistema.

Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización, sea en: especificación de requisitos, desarrollo, explotación, mantenimiento, etc.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

- Evitar accesos no autorizados, daños e interferencias contra la información de la organización.

- Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

Las áreas de trabajo de la organización y sus activos deben ser clasificados y protegidos en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física, esta sea robo, inundación, incendio, etc.

10. CONFORMIDAD CON LA LEGISLACIÓN

- Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.
- Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.
- Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

Se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.

Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

Ventajas

La adopción de la norma ISO 17799 proporciona diferentes ventajas a cualquier organización:

- Aumento de la seguridad efectiva de los sistemas de información.
- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Mejora continua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de los clientes y socios de la organización
- Aumento del valor comercial y mejora de la imagen de la organización.

CAPÍTULO 3

PROYECTO.- IMPLEMENTACIÓN Y APLICACIÓN DE LA AUDITORÍA EN UNA RED

3.1 PROCEDIMIENTO PARA EVALUAR UN SISTEMA DE SEGURIDAD EN UNA RED DE COMUNICACIONES

Basándonos en la NORMA ISO 17799 se debe tener conocimiento de los objetivos, organización y las políticas de una empresa; de acuerdo a esto se realizará la evaluación del sistema de seguridad de una red de comunicaciones en dicha organización.

Identificación del sistema

Lubtechnology Cía. Ltda. es la empresa a la cual se implementará una red de comunicación y sobre esta se realizará la auditoria de seguridad.

Descripción de la Empresa

La empresa se dedica a la distribución de lubricantes, llantas y aditivos, y servicios automotrices; tales como: lavado de vehículos, cambios de aceite, alineación, balanceo y enllantajes.

Organigrama de la Empresa

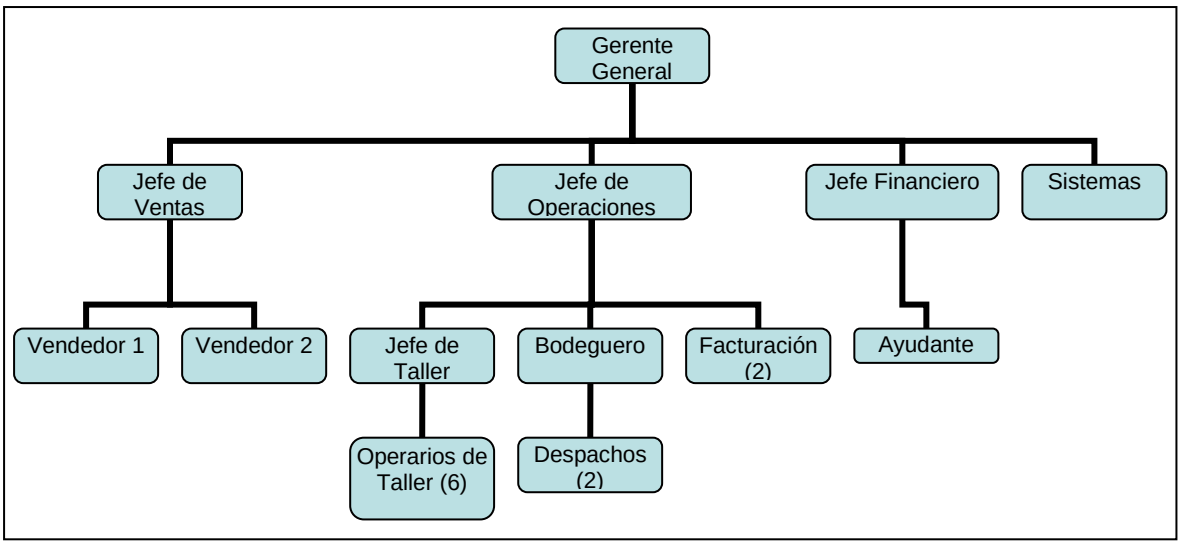


Figura 3.1. Organigrama Funcional de la empresa a auditar

Análisis de procesos y recursos en la red

La gestión de los procesos está directamente relacionada a los recursos de la red. De acuerdo a los procesos se acondicionarán los recursos de la red.

El Departamento de Ventas se encarga de la venta de productos y servicios; por lo que se requiere que se utilicen 3 computadores dentro de una misma VLAN que se nombrará VENTAS.

- Acceso al sistema para revisar inventarios, costos, cuentas por cobrar
- Comunicaciones mediante correo electrónico.

El Departamento de Operaciones maneja la facturación, la logística, es decir, la compra, almacenamiento y transporte de productos hasta las instalaciones de los clientes; y maneja también el taller de servicio. Este departamento verifica qué productos hay en inventario, y realiza los pedidos de renovación del mismo. Además realiza la facturación de las ventas, tanto las que realizan los vendedores externos como las del Taller. Este departamento requiere el acceso a 7 computadoras que estarán en el mismo switch correspondiente al departamento de ventas. Estas computadoras pertenecerán a una VLAN que se nombrará OPERACIONES.

- Facturación, acceso al sistema y modificación de inventario.
- Ingreso de Compras al Inventario, acceso al sistema y modificación de inventario
- Control de Inventarios.
- Comunicaciones mediante correo electrónico.

Este departamento tendrá diferentes tipos de privilegios en el sistema entre la gente que lo conforma.

El Departamento de Sistemas brinda soporte técnico a la red y gestiona privilegios en el sistema interno; debe tener acceso a todas las máquinas y

equipos de comunicaciones de la red. Se requieren 1 computador: configurado en una VLAN que se nombrará SISTEMAS.

Este departamento realiza las siguientes gestiones:

- Acceso mediante VNC a cada usuario de la red.
- Monitorea y controla mediante firewall y analizador de protocolos los servicios y aplicaciones empleados por los usuarios.
- Acceso a la red externa, Internet.
- Actualización de aplicaciones, servidores y firmware de equipos de comunicación.
- Comunicaciones mediante correo electrónico.

En este Departamento también se encontrarán los servidores configurados en una VLAN denominada SERVIDORES.

- Cada departamento tendrá acceso a los servidores de acuerdo a privilegios basados en las políticas de seguridad de la empresa.

El Departamento Financiero se encarga de las funciones de Crédito, de Caja y Bancos, y de Contabilidad e Impuestos. Analiza y aprueba los créditos que se concede a los clientes, maneja los ingresos y egresos, y el control de caja y bancos, lleva los registros contables y los estados financieros de la empresa, y efectúa las declaraciones de impuestos. Se configurará en una

VLAN denominada FINANCIERO; se requiere de 2 computadores.

- Acceso al sistema con privilegio para realizar; asientos de Pagos realizados por los clientes, análisis de crédito y definición de cupo de crédito de los clientes, pagos a proveedores y pagos de gastos, control de Caja y Bancos, Tributación, y asientos contables y estados financieros
- Comunicaciones mediante correo electrónico.
- Acceso limitado a la red externa, Internet; sitios Web de bancos, Sitio Web del SRI y demás sitios donde sea requerido el acceso.

El Departamento de Gerencia monitorea las actividades que se efectúan en el sistema y realiza los cambios que se requieran. Posee el privilegio absoluto en cuanto al manejo del sistema. Se requiere de una computadora. Se configurará en una VLAN denominada GERENCIA.

- Acceso total a la información de los servidores que contiene el sistema.
- Posee acceso total a la red externa, Internet.

Análisis de riesgos y amenazas

- Existe el riesgo de que personas no autorizadas manipulen los equipos. Por lo tanto, se debe verificar que los equipos de comunicación están ubicadas en un área segura; es decir área restringida.

- Riesgo de daño de equipos; se debe mantener equipos en una zona seca, lejos de la humedad y aislados de materiales inflamables.
- Interrupción física de los enlaces de comunicación, se debe verificar que estén protegidos adecuadamente; mediante canaletas. También se debe verificar periódicamente el estado del cableado.
- Interrupción en los procesos de los negocios. Puede ser provocada por pérdida de energía eléctrica o por daño en el servidor. Se requiere un UPS por equipo de comunicación y un servidor de respaldo que se deberá actualizar de manera periódica.
- Riesgo de robo ó acceso no autorizado a la información. Como medida preventiva el sistema a emplearse tendrá su base de datos en un servidor; cada usuario debe autenticarse.
- Riesgo de manipulación de la información por parte de los usuarios de la red. Se debe establecer privilegios de acuerdo a los departamentos.

Análisis y evaluación de controles

En esta fase se analizará las medidas preventivas con respecto a los riesgos y amenazas en la red.

- Confirmar que el cuarto de sistemas esté cerrado bajo llave cuando no estén personas autorizadas dentro de él.
- Verificar que cada departamento de la empresa debe tener una codificación y privilegios de acuerdo a las actividades que les está

permitido realizar. Esto estará considerado en la autenticación y división de departamentos en la configuración de los equipos de comunicación.

- Mediante un analizador de protocolos se debe monitorear la red para determinar que aplicaciones están siendo utilizadas por los usuarios.
- Se utilizará arbitrariamente aplicación de VNC para monitorear las actividades de los usuarios. Esta herramienta también será empleada para que el departamento de sistemas pueda auxiliar remotamente a los usuarios con respecto al manejo de las aplicaciones.

Informes de la Auditoría y Recomendaciones

Para proveer un informe se requiere del análisis de los datos antes mencionados, se debe exponer detalladamente lo que se ha realizado, explicando el objetivo de cada implementación realizada y cual es el resultado obtenido.

Con relación a la red que se implementa en este capítulo, se obtendrá un informe final mediante el uso del Firewall ISA Server; en donde se observa todo el tipo de tráfico empleado en la red, y las horas en las que se incrementa dicho tráfico.

Las recomendaciones son las medidas correctivas de acuerdo a lo que se observa en el informe; esto radica en que los controles aplicados deben ser

cambiados o reforzados.

3.2 PROYECTO.- DESCRIPCIÓN E IMPLEMENTACIÓN DE UNA RED

La red a implementarse se ajusta a las políticas y necesidades de la empresa. Se requiere de seis áreas de trabajo, cada una se creará bajo una red local virtual de computadores; éstas se regirán en base a las políticas ya establecidas.

3.2.1 Diagrama esquemático de la LAN a implementarse

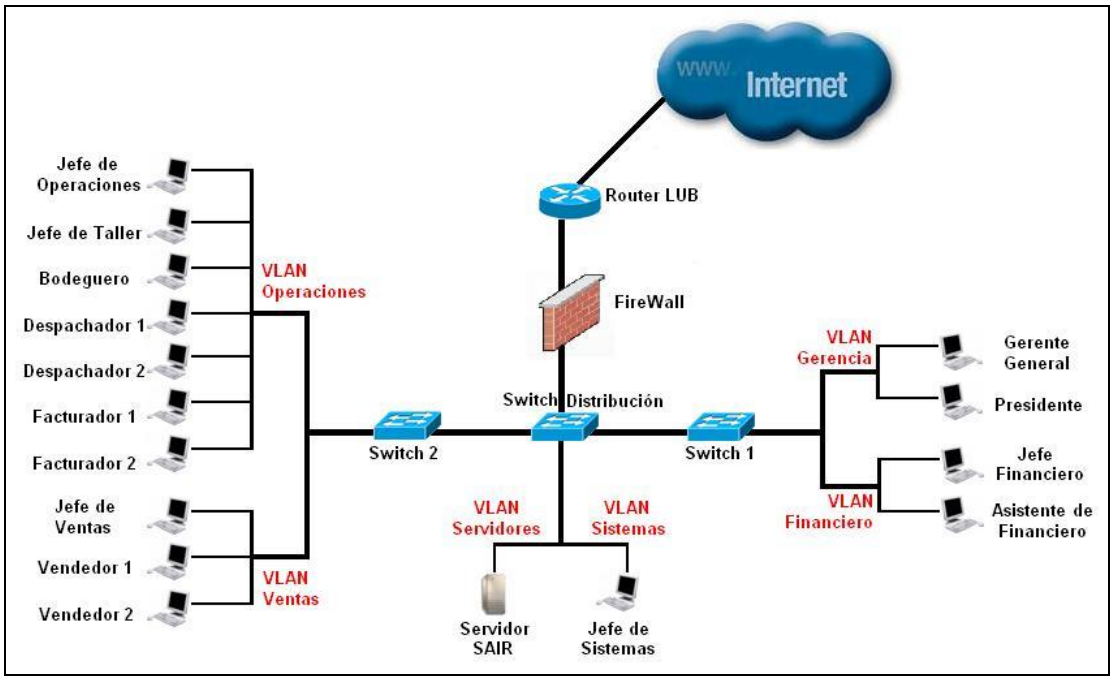


Figura 3.2 Diagrama esquemático de la Red.

Se puede observar en la Figura 3.2 la distribución del personal de la empresa correspondiente a su respectiva área de trabajo. El personal de la empresa labora en un edificio de dos pisos; por lo que se ubica en el primer piso el switch 1 y el switch de distribución, que está conectado al firewall, y éste al router. En el switch 1 están configuradas y conectadas las computadoras de los departamentos de Gerencia y Financiero. En el switch de distribución está destinado para la localización del área de sistemas y servidores. En el switch 2 están configuradas y conectadas las computadoras de los departamentos de Operaciones y Ventas.

3.2.2 Requerimientos de la LAN a implementarse

3.2.2.1 Equipos a usarse en la LAN

A continuación, en las tablas 3.1 y 3.2 se muestran los modelos y se detallan las especificaciones de lo equipos usados en la implementación de la red de comunicación.

EQUIPO	**MODELO**
SWITCH 1	CISCO C2960
SWITCH DE DISTRIBUCIÓN	CISCO C2960
SWTICH 2	CISCO C2960
ROUTER	CISCO 2801

Tabla 3.1 Modelo y marca de los equipos de comunicación de la LAN

COMPUTADORAS	CARACTERISTICAS	SISTEMA OPERATIVO
SERVIDOR	▪ Procesador: Intel Xeon Dual Core 3040 (1.87 Ghz, bus de 1066 Mhz). ▪ Memoria RAM: 2GB, DDR PC400. ▪ Disco Duro: 120 GB IDE de 7200 rpm. ▪ Monitor 17". ▪ Mouse y Teclado.	WINDOWS SERVER 2003
PC	▪ Procesador: Amd Sempron 2600+ (1.8 Ghz, bus de 800 Mhz). ▪ Memoria RAM: 1 GB, DDR2 PC5300. ▪ Disco Duro: 120 GB IDE de 7200 rpm. ▪ Monitor lcd de 14". ▪ Mouse y Teclado.	WINDOWS XP

Tabla 3.2 Especificaciones de las computadoras de la LAN

3.2.3 Configuraciones de Seguridad

Para realizar la implementación de la red siguiendo un estándar de seguridad se requieren de diversas configuraciones. Hay muchas herramientas que se pueden usar para garantizar la seguridad en una red de comunicación. Para este caso se han usado los equipos proporcionados por la empresa a la cual se audito.

Conexiones y Direcciones IP estáticas de los equipos terminales

		IP
SWITCH DISTRIBUCION		192.168.100.4
VLAN2	VLANSISTEMAS	192.168.100.17
VLAN3	VLANSERVIDORES	192.168.100.33

PUERTOS	**CONECTADO A**	**IP**
F0/1	JEFE DE SISTEMAS	192.168.100.18
F0/2	SISTEMAS	NO USADO
F0/3	SISTEMAS	NO USADO
F0/4	SISTEMAS	NO USADO
F0/5	SISTEMAS	NO USADO
F0/10	SISTEMASAIR	192.168.100.34
F0/11	SERVIDORES	NO USADO
F0/12	SERVIDORES	NO USADO
F0/13	SERVIDORES	NO USADO
F0/22	F0/24 SWITCH1	
F0/23	F0/24 SWITCH2	
F0/24	F0/1 ROUTER	

		IP
SWITCH 1		192.168.100.5
VLAN4	VLANGERENCIA	192.168.100.49
VLAN5	VLANFINANCIERO	192.168.100.65

PUERTOS	**CONECTADO A**	**IP**
F0/1	GERENTE GENERAL	192.168.100.50
F0/2	PRESIDENTE	192.168.100.51
F0/3	GERENCIA	NO USADO
F0/4	GERENCIA	NO USADO
F0/5	GERENCIA	NO USADO
F0/10	JEFE FINANCIERO	192.168.100.66
F0/11	ASISTENTE DE FINANCIERO	192.168.100.67
F0/12	FINANCIERO	NO USADO
F0/13	FINANCIERO	NO USADO
F0/14	FINANCIERO	NO USADO
F0/15	FINANCIERO	NO USADO
F0/24	F0/22 SWITCH DISTRIBUCION	

		IP
SWITCH 2		192.168.100.6
VLAN6	VLANOPERACIONES	192.168.100.81
VLAN7	VLANVENTAS	192.168.100.97

PUERTOS	**CONECTADO A**	**IP**
F0/1	JEFE DE OPERACIONES	192.168.100.82
F0/2	JEFE DE TALLER	192.168.100.83
F0/3	BODEGUERO	192.168.100.84
F0/4	FACTURADOR1	192.168.100.85
F0/5	FACTURADOR2	192.168.100.86
F0/6	DESPACHADOR1	192.168.100.87
F0/7	DESPACHADOR2	192.168.100.88
F0/8	JEFE DE VENTAS	192.168.100.98
F0/9	VENDEDOR1	192.168.100.99
F0/10	VENDEDOR2	192.168.100.100
F0/11	VENTAS	NO USADO
F0/24	F0/23 SWITCH DISTRIBUCION	

ROUTER		
PUERTOS	**CONECTADO A**	**IP**
F0/1	F0/24 SWITCH DISTRIBUCION	192.168.100.1
F0/0	ISP	

Tabla 3.3 Conexiones y Direcciones IP estáticas de cada equipo de la LAN

En la tabla 3.3 se detallan las conexiones puerto a puerto de cada equipo de comunicación y las IP correspondientes a cada equipo usado en la LAN. Tener esta información es importante porque facilita el trabajo al momento de hacer algún mantenimiento, tratar de rastrear algún problema o cualquier cambio que se desea hacer en la red.

Para administrar y monitorear una red de datos se deben considerar las políticas de la empresa, para esto se han implementado listas de acceso en el router, la configuración de un firewall y seguridad en Windows XP que se basan en dichas políticas de acuerdo a los requerimientos de la red.

Configuración de Router y Switches

El acceso al router y los switches esta encriptado con contraseñas altamente seguras. Existe una contraseña diferente para cada acceso, ya sea vía consola o vía telnet, y además otra para el acceso al modo privilegiado de la configuración en los equipos de comunicación. Las contraseñas difieren por equipo, y solo el jefe de sistemas y el gerente general tienen conocimiento de estas.

Cada puerto de los switches tiene configurada la dirección Mac del dispositivo de red que esta conectado a este, así solo un dispositivo de red único puede acceder a la red en cada puerto; de tal forma que se evitara que

equipos extraños o intrusos accedan de forma física a la información de la empresa. Las direcciones Mac de cada dispositivo de red son de conocimiento exclusivo del jefe de sistemas y del gerente para así evitar clonamientos de estas.

Las Listas de Acceso en el router se configura en la interface mediante la cual se accede al internet, de esta manera se logra que sólo se utilicen puertos específicos de acuerdo a los requerimientos establecidos y las políticas de seguridad de la empresa.

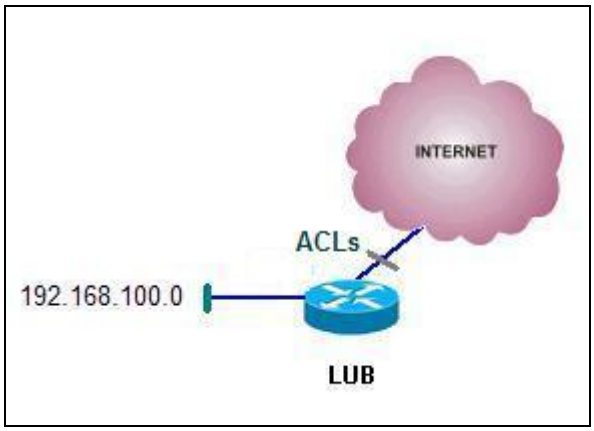


Figura 3.3 Esquema indicativo de ubicación de ACLs.

Configuración de Listas de Acceso en el Router:

access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq www

access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq smtp

access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq pop3

access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq 443

access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq 1863

access-list 101 permit tcp 192.168.100.16 0.0.0.15 any eq 7

Se puede observar que las Listas de Control de Acceso permiten que los todos usuarios de la red 192.168.100.0 tengan acceso los puertos:

- www, 80
- smtp, 25
- pop3, 110
- https, 443
- Messenger, 1863
- icmp, 7

De esta manera se obtiene un control más rígido, con respecto a los datos que se pueden enviar y recibir a través de la red hacia el Internet.

Configuración del Firewall

El Firewall usado es el Microsoft ISA Server 2004 y esta alojado en un servidor con el sistema operativo Windows Server 2003. El acceso a este servidor esta encriptado con una contraseña conocida solo por el jefe de sistemas y el gerente general de la compañía. Esta contraseña es una combinación de números, letras y símbolos, y es altamente segura.

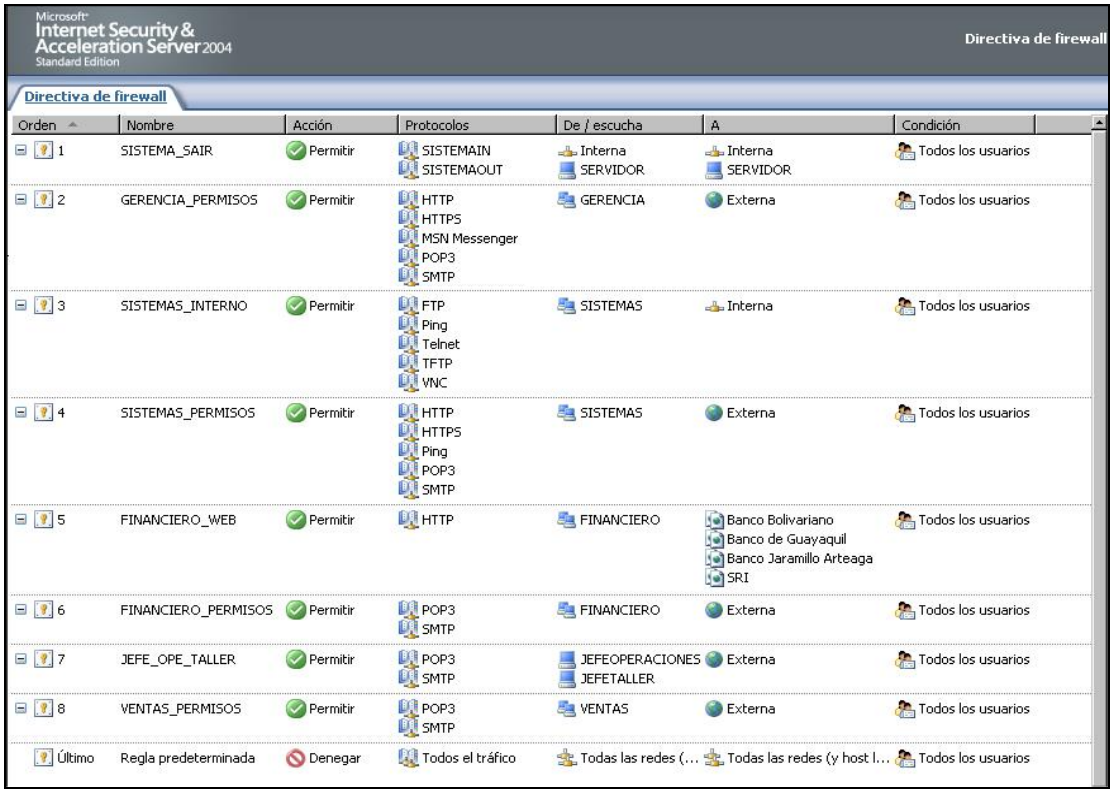


Figura 3.4 Directivas del Firewall

Las Directivas de Firewall se configuran desde lo más específico hasta lo más general, para esto se crean reglas de acceso.

En la figura 3.4 se pueden observar las reglas creadas de acuerdo a las diferentes áreas de la empresa indicando los permisos asignados.

La primera regla, SISTEMA_SAIR, habilita los puertos 445 y 1545, ambos pertenecientes al protocolo tcp; con el objetivo de permitir el intercambio de información entre el sistema de facturación y los usuarios. El sistema de facturación está contenido en un servidor.

La segunda regla, GERENCIA_PERMISOS, permite a los usuarios del área de Gerencia la utilización de los puertos que usan los protocolos http, https, el uso de correo electrónico: pop3, smtp y además los puertos que permiten la utilización del Messenger.

La tercera regla, SISTEMAS_INTERNO, permite a los usuarios del área de Sistemas la utilización de los puertos que usan los protocolos ftp, icmp, telnet, tftp y los puertos 5000 y 5100, asignados a la aplicación del Real VNC; estos permisos están asignados hacia la intranet.

La cuarta regla, SISTEMAS_PERMISOS, permite a los usuarios del área de Sistemas la utilización de los puertos que usan los protocolos http, https, icmp, y el uso de correo electrónico: pop3, smtp. Estos permisos están asignados hacia el Internet.

La quinta regla, FINANCIERO_WEB, permite a los usuarios del área de Sistemas el acceso limitado del protocolo http a ciertos sitios web que constan con información pertinente al área de finanzas.

La sexta regla, FINANCIERO_PERMISOS, permite a los usuarios del área de Sistemas el uso de correo electrónico, habilitando los puertos que utilizan los protocolos pop3, smtp.

La séptima regla, JEFE_OPE_TALLER, permite a los usuarios: JEFEOPERACIONES y JEFETALLER el uso de correo electrónico, habilitando los puertos que utilizan los protocolos pop3, smtp.

La octava regla, VENTAS_PERMISOS, permite a los usuarios del área de Ventas el uso de correo electrónico, habilitando los puertos que utilizan los protocolos pop3, smtp.

La última regla se establece por defecto indicando el bloqueo de los puertos con respecto a cualquier usuario de la red.

La manera como se ejecutan las reglas del firewall, es verificando una a una de manera jerárquica, de menor a mayor. Por lo tanto, si coincide una de las peticiones de algún usuario con una de las reglas establecidas, la ejecuta y no verificará las siguientes.

Configuración de directivas de los usuarios en Windows XP

La Seguridad en Windows XP debe de ser configurada usuario a usuario según los privilegios que da la empresa a cada uno de sus subordinados; todos los usuarios deben conocer los privilegios y restricciones que poseen. En algunos casos aún teniendo conocimiento de sus limitaciones, éstos tratan de acceder a información restringida o muchas veces causan algún

tipo de daño por el mal manejo de las herramientas que este sistema operativo le proporciona. Para controlar estos posibles ataques se han creado medidas de seguridad a cada uno de los usuarios usando las herramientas de Windows XP.

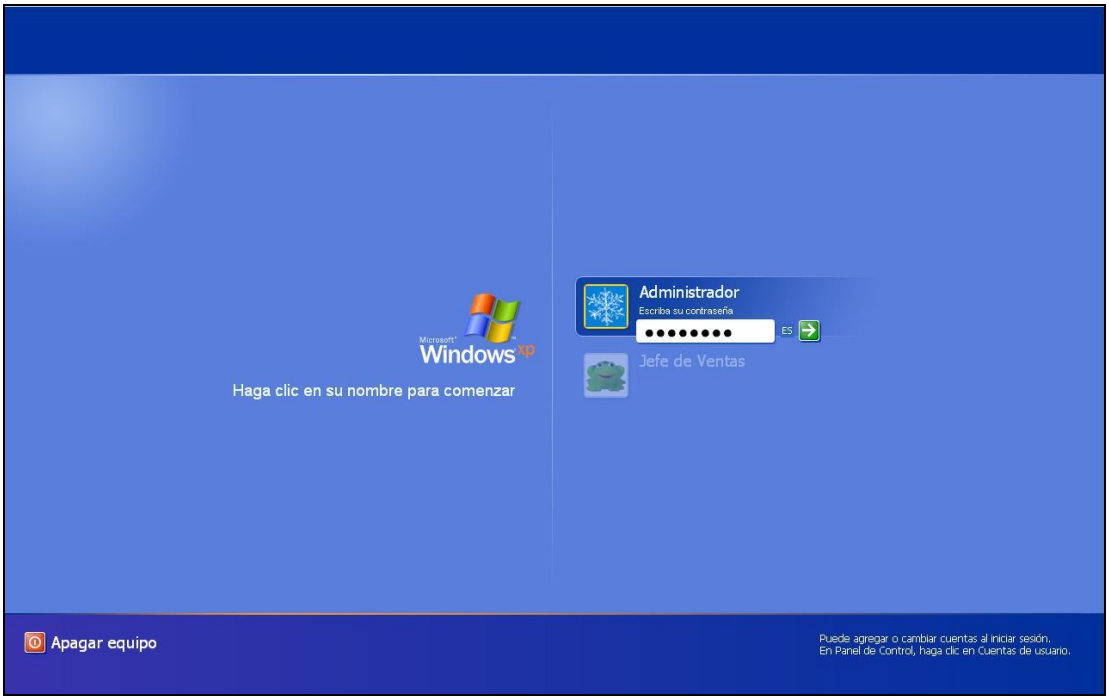


Figura 3.5 Cuentas usuario en un computador con Windows XP

Como se puede observar en la Figura 3.5 a cada usuario Windows XP se le ha creado 2 cuentas uno como administrador y otra como usuario este con el nombre del cargo que desempeña y con sus respectivas restricciones. Tanto el acceso a la cuenta administrador como la de usuario están encriptados con contraseñas. El derecho al acceso a la cuenta administrador y por ende el conocimiento de la contraseña la tiene el jefe de sistemas y el gerente

general de la empresa. La contraseña de acceso como usuario es única por computador y solo debe de ser conocida por la persona encargada de ese puesto de trabajo.

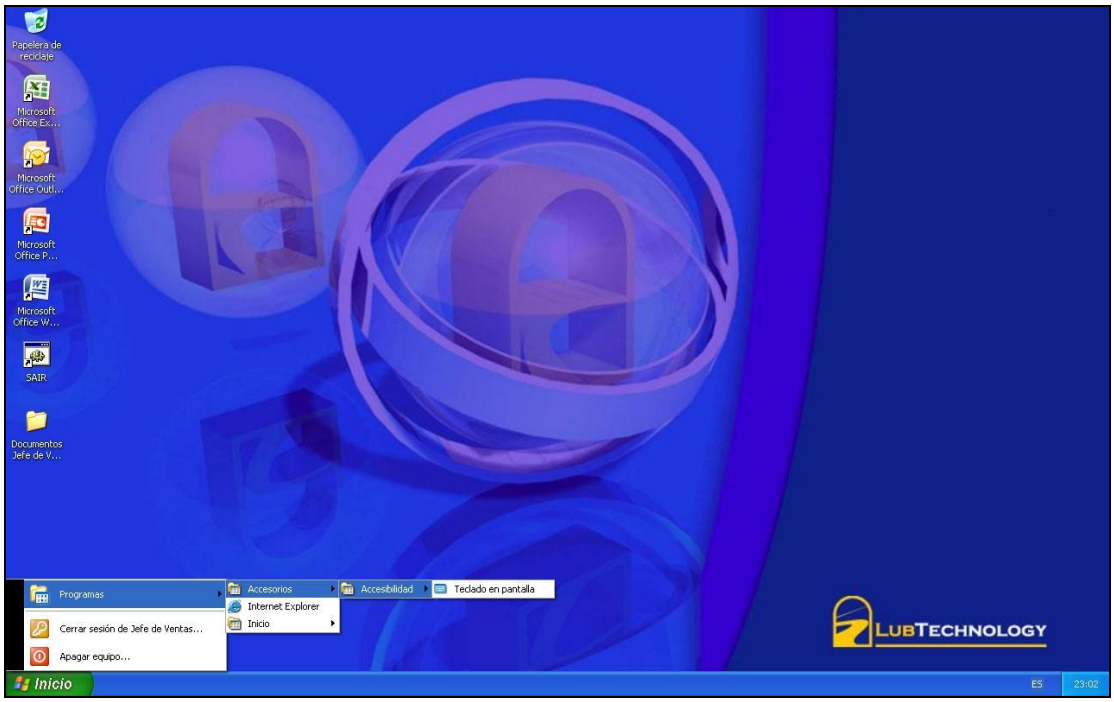


Figura 3.6 Vista del escritorio de una cuenta definida como usuario en Windows XP

Como podemos observar en la Figura 3.6 la cuenta usuario solo tendrá acceso a las aplicaciones concernientes al área de trabajo; tales como al sistema de facturación SAIR alojado en el servidor, al procesador de palabras Microsoft Word, la hoja de cálculo Microsoft Excel, al programa de presentaciones Microsoft Power Point, al programa de agenda ofimática y cliente de email Microsoft Outlook y al explorador web Internet Explorer. Los usuarios tienen bloqueado el permiso para realizar instalaciones de

programas y de crear o eliminar archivos en el escritorio, para esto cuentan con una carpeta donde podrán guardar todo lo que consideren necesario. Esta carpeta será revisada periódicamente.

Lo usuarios tienen restringido el acceso a todo lo que concierne a archivos del sistema, símbolo de sistema o MSDOS, panel de control, opciones de internet, opciones de Ctrl+Alt+Sup, actualizaciones automáticas, configuración de los dispositivos de red, propiedades de componentes de una conexión LAN, publicación de carpetas compartidas, configuración de pantalla y la barra de tareas y reproductores de video y música, como el Windows Media Player. Además tienen oculto el área de notificación, de este modo estos no pueden saber en que momento se le esta monitoreando sus actividades vía VNC.

Antivirus

Cada estación de trabajo y cada servidor cuenta con la protección de un antivirus, para este caso se ha usado el NOD32. Este es un antivirus fiable, eficaz y rápido; siendo una de sus principales ventajas el bajo consumo de recursos al momento de un análisis. Este antivirus es actualizado periódicamente y se lo hace fuera del horario de trabajo, porque se necesita de la habilitación de un puerto en el firewall y además para evitar congestionamiento en la red.

Configuraciones del Software de facturación

A empresa utiliza un software de facturación llamado SAIR, que permite dar privilegio al usuario con respecto a los cambios que se requieran realizar en el inventario de los productos. Estos privilegios los ingresa directamente el área administrativa, el Gerente General, quien tiene la clave maestra que permite realizar los cambios que se requieran, asociados al proceso de facturación y a los usuarios de la empresa.

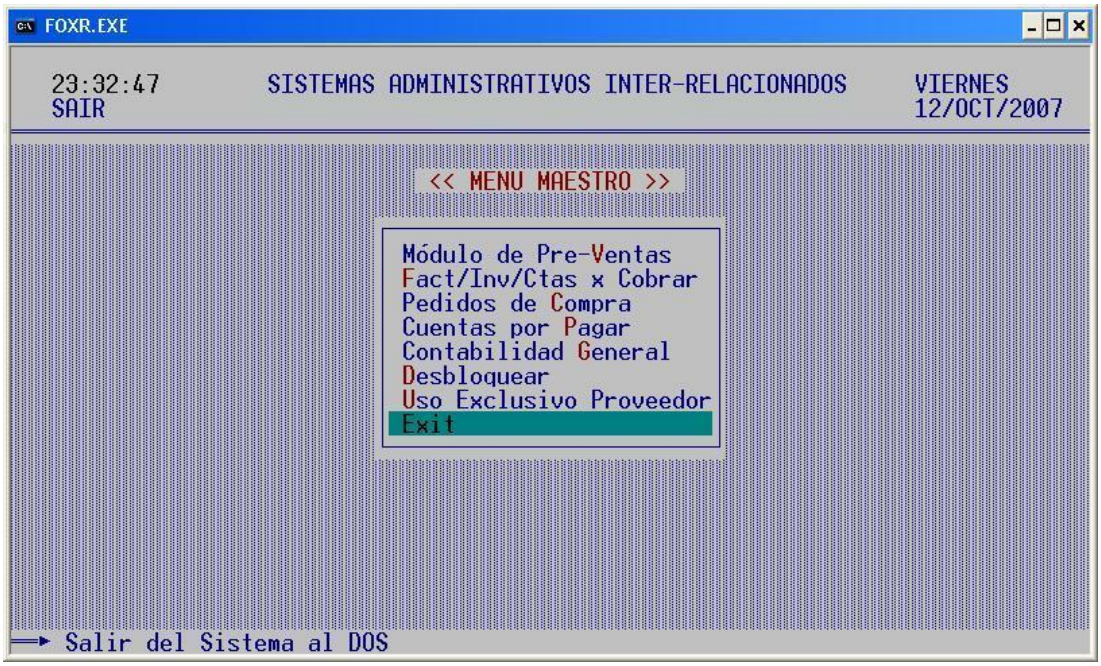


Figura 3.7 Menú principal del sistema SAIR

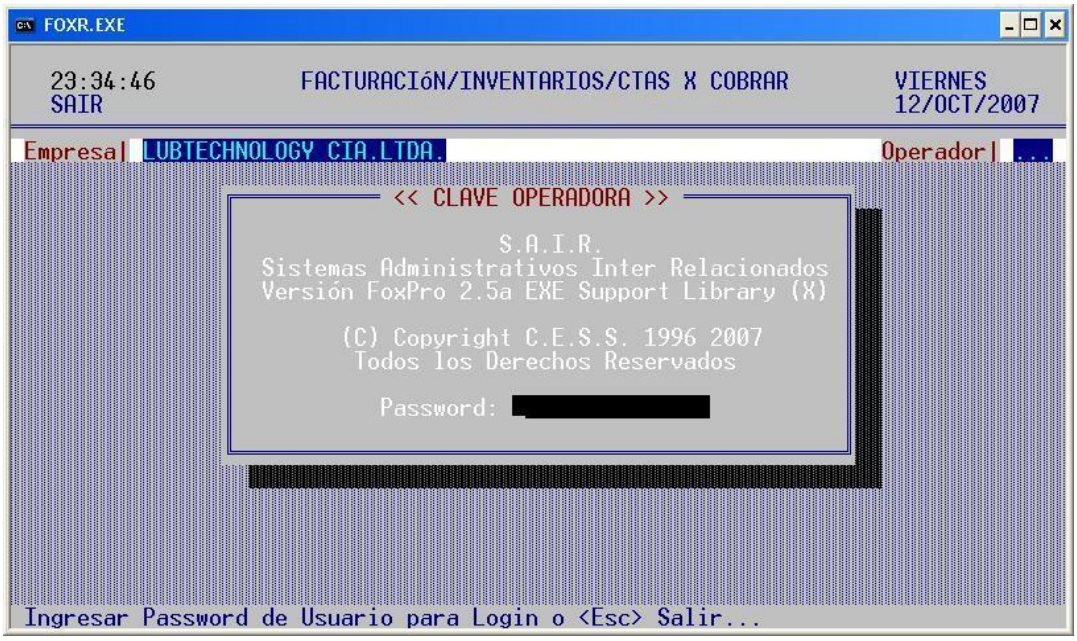


Figura 3.8 Petición de Password del sistema SAIR

En la figura 3.8 se observa la pantalla del software solicitando la contraseña, en donde se reconoce al usuario que ingresa.

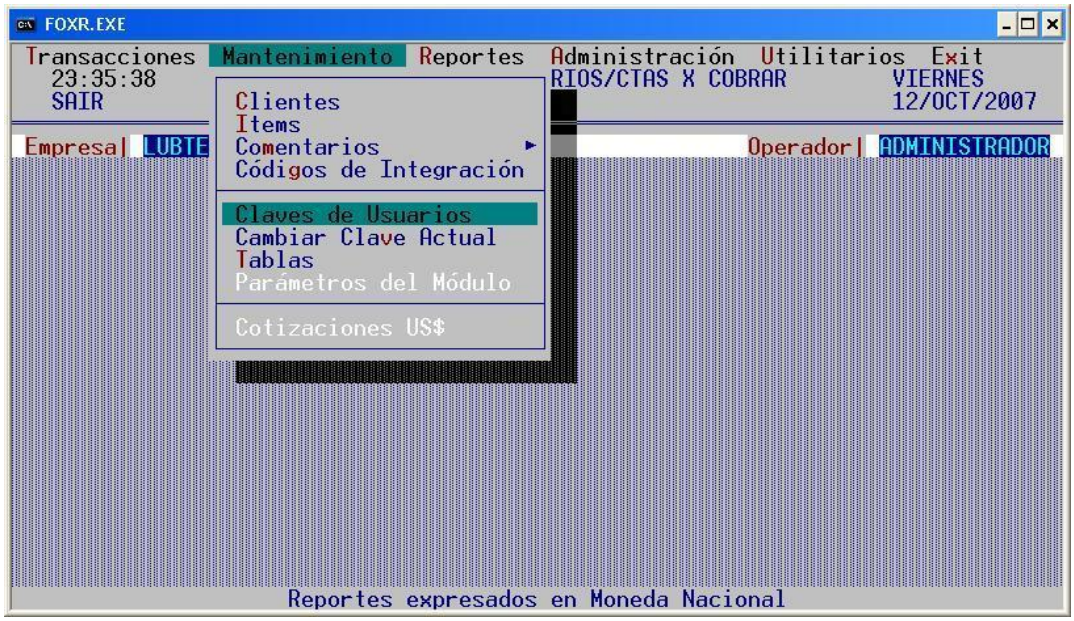


Figura 3.9 Claves de Usuario del sistema SAIR

En la figura 3.9 se observa el acceso a las claves de usuario, en donde se pueden cambiar las claves de acuerdo a los usuarios, esta opción sólo la tiene el Gerente General. Si uno da click en donde indica claves de usuario, mostrará la pantalla que se observa en la figura 3.10, en donde aparece cada usuario con su respectiva clave. Por cuestiones de seguridad de la empresa en mención no se muestra dicha información.

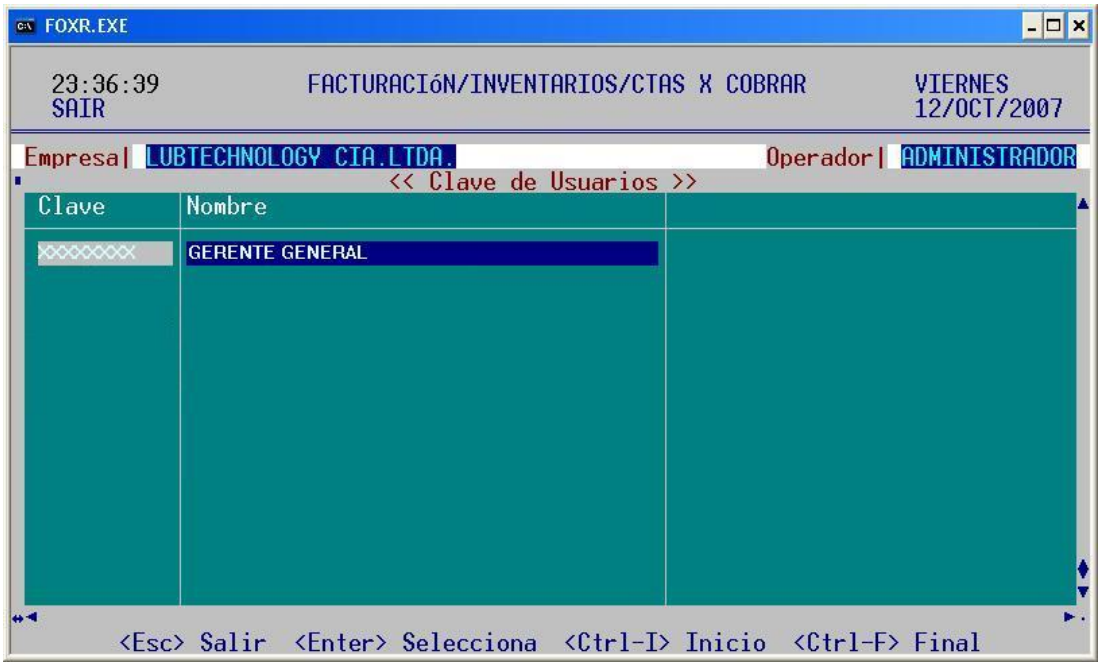
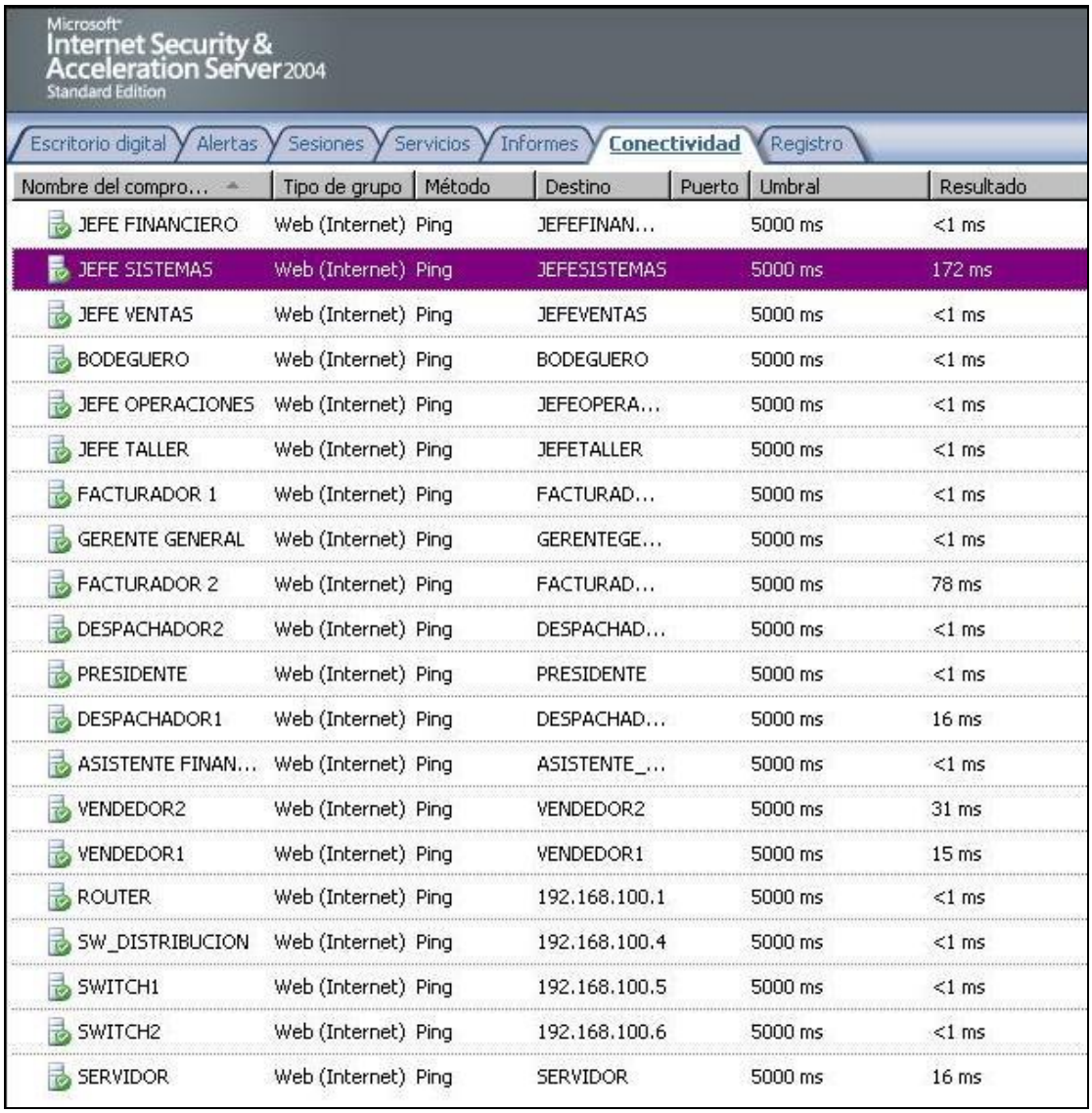


Figura 3.10 Lista de usuarios con las contraseñas en el sistema SAIR

Figura 3.11 Privilegios por usuario en el sistema SAIR

En la figura 3.11 se observan los privilegios que se pueden asignar a los diferentes usuarios. De tal manera que los ítems que tienen una x, representan los accesos que poseen cada usuario.

3.2.4 Revisión y comprobación de los enlaces.



Nombre del compro...	Tipo de grupo	Método	Destino	Puerto	Umbral	Resultado
JEFE FINANCIERO	Web (Internet)	Ping	JEFEFINAN...		5000 ms	<1 ms
JEFE SISTEMAS	Web (Internet)	Ping	JEFESISTEMAS		5000 ms	172 ms
JEFE VENTAS	Web (Internet)	Ping	JEFEVENTAS		5000 ms	<1 ms
BODEGUERO	Web (Internet)	Ping	BODEGUERO		5000 ms	<1 ms
JEFE OPERACIONES	Web (Internet)	Ping	JEFEOPERA...		5000 ms	<1 ms
JEFE TALLER	Web (Internet)	Ping	JEFETALLER		5000 ms	<1 ms
FACTURADOR 1	Web (Internet)	Ping	FACTURAD...		5000 ms	<1 ms
GERENTE GENERAL	Web (Internet)	Ping	GERENTEGE...		5000 ms	<1 ms
FACTURADOR 2	Web (Internet)	Ping	FACTURAD...		5000 ms	78 ms
DESPACHADOR2	Web (Internet)	Ping	DESPACHAD...		5000 ms	<1 ms
PRESIDENTE	Web (Internet)	Ping	PRESIDENTE		5000 ms	<1 ms
DESPACHADOR1	Web (Internet)	Ping	DESPACHAD...		5000 ms	16 ms
ASISTENTE FINAN...	Web (Internet)	Ping	ASISTENTE_...		5000 ms	<1 ms
VENDEDOR2	Web (Internet)	Ping	VENDEDOR2		5000 ms	31 ms
VENDEDOR1	Web (Internet)	Ping	VENDEDOR1		5000 ms	15 ms
ROUTER	Web (Internet)	Ping	192.168.100.1		5000 ms	<1 ms
SW_DISTRIBUCION	Web (Internet)	Ping	192.168.100.4		5000 ms	<1 ms
SWITCH1	Web (Internet)	Ping	192.168.100.5		5000 ms	<1 ms
SWITCH2	Web (Internet)	Ping	192.168.100.6		5000 ms	<1 ms
SERVIDOR	Web (Internet)	Ping	SERVIDOR		5000 ms	16 ms

Figura 3.12 Pruebas de conectividad del ISA Server de los equipos conectados a la Red.

En la Figura 3.12 se puede observar que los usuarios de la red están conectados, se ha realizado una prueba de eco, ping, utilizando los recursos del ISA Server.

3.3 EVALUACIÓN DE LA SEGURIDAD EN UNA RED DE COMUNICACIONES

3.3.1 Monitoreo y Evaluación de la red

A continuación se detallan las capturas del firewall, permitiendo que se observe que tipo de puertos se están empleando y como es el desarrollo de la red, de acuerdo a lo que utilicen los usuarios

Se detallan 2 informes uno antes de la auditoria en el que se puede apreciar como todos los usuarios tienen acceso ilimitado, y un segundo, después de la auditoria, donde se puede observar que se cumplen los requerimientos de la red de acuerdo a las políticas de seguridad de la empresa.

Informes del ISA Server 2004 antes de la auditoria

RESUMEN

En la figura 3.13 se puede observar protocolos de comunicación que se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe. Los protocolos que se usaron con mayor frecuencia se muestran primero. Este reporte contiene el tráfico tanto de web como el que no es de web.

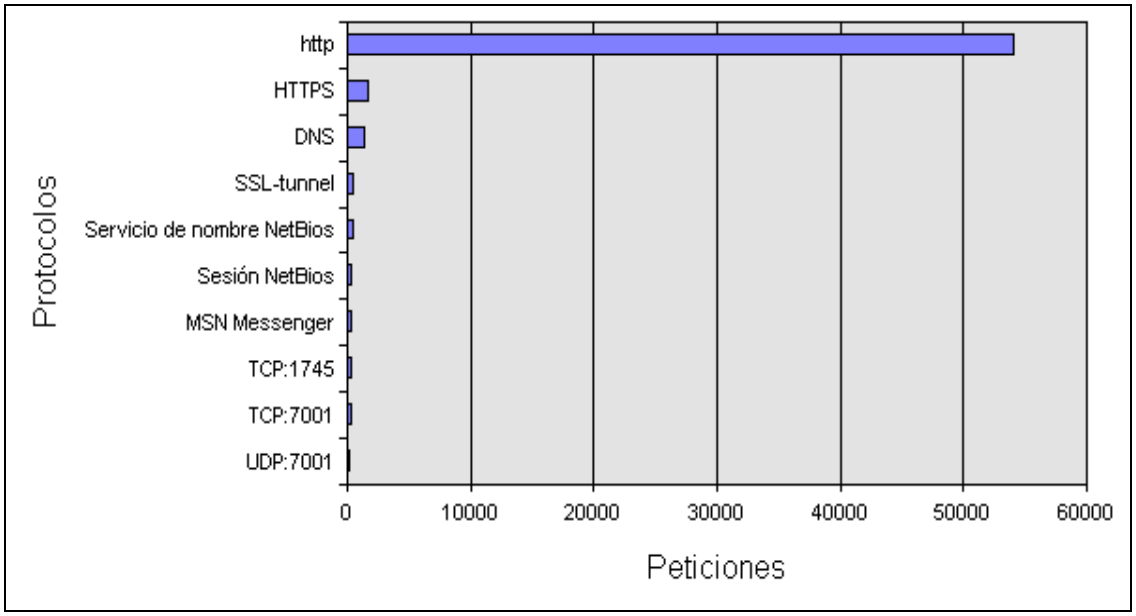


Figura 3.13 Diagrama de barras de los protocolos que se utilizan en la comunicación de la red antes de la auditoria.

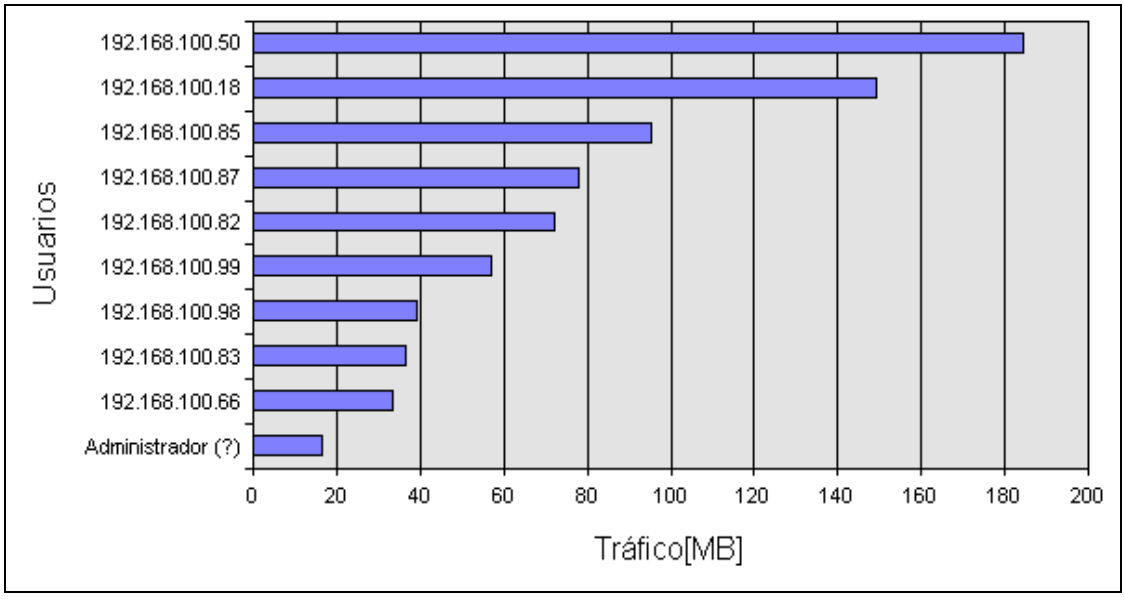


Figura 3.14 Diagramas de barras de los usuarios más frecuentes antes de la auditoria.

En la figura 3.14 se observan los usuarios que generaron la mayor cantidad de tráfico de red a través del servidor ISA, durante el periodo del informe. Los

usuarios que generaron el mayor tráfico se muestran primero. Este informe contiene tanto el tráfico de web como otros diferentes.

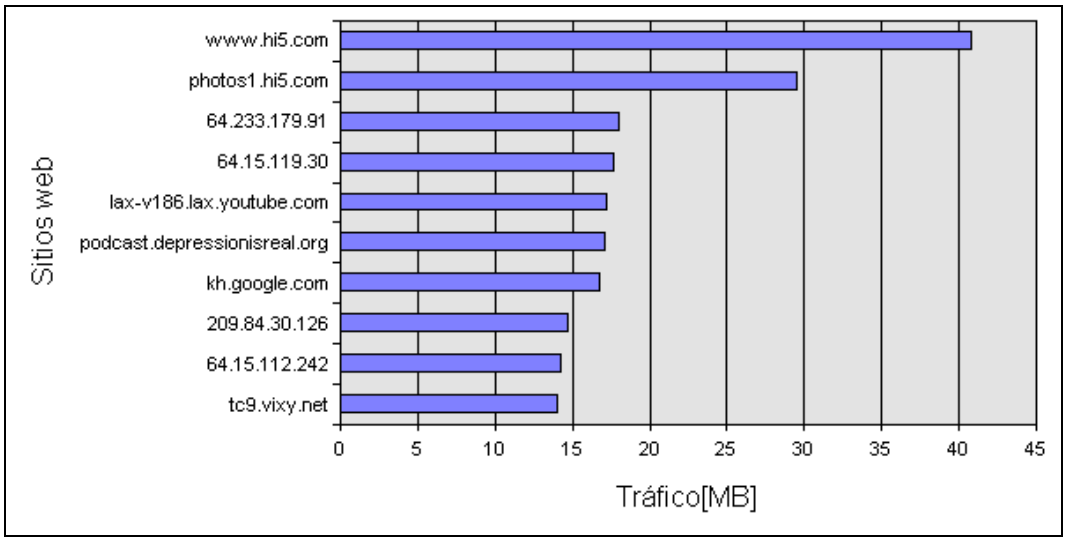


Figura 3.15 Diagrama de barras de los sitios Web más frecuentes antes de la auditoria.

En la figura 3.15 se observan sitios web que fueron solicitados con mayor frecuencia por los clientes, durante el periodo del informe. Los sitios web más visitados se muestran primero.

Al observar los gráficos 3.13, 3.14 y 3.15 se observan que los usuarios, sin importar cual sea su nivel en el organigrama, acceden libremente a las páginas de Internet, por lo que no se tiene un control adecuado de las actividades que se realizan. Las páginas web visitadas no tienen relación alguna con las actividades de la empresa. Esto es una debilidad que será considerada en el informe de recomendaciones.

Núm.	Sitio	Usuarios únicos	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	www.hi5.com	7	2029	3,70 %	38,51 MB	5,50 %	2,27 MB	4,60 %	40,78 MB	5,40 %
2	photos1.hi5.com	7	4060	7,40 %	26,49 MB	3,80 %	3,02 MB	6,10 %	29,51 MB	3,90 %
3	64.233.179.91	2	646	1,20 %	17,64 MB	2,50 %	347,98 KB	0,70 %	17,98 MB	2,40 %
4	64.15.119.30	1	1	0,00 %	17,61 MB	2,50 %	888,00 N	0,00 %	17,61 MB	2,40 %
5	lax-v186.lax.youtube.com	1	2	0,00 %	17,23 MB	2,50 %	1,98 KB	0,00 %	17,23 MB	2,30 %
6	podcast.depressionisreal.org	1	78	0,10 %	17,04 MB	2,40 %	60,39 KB	0,10 %	17,09 MB	2,30 %
7	kh.google.com	1	1676	3,10 %	15,69 MB	2,20 %	1,01 MB	2,00 %	16,70 MB	2,20 %
8	209.84.30.126	1	731	1,30 %	14,45 MB	2,10 %	205,05 KB	0,40 %	14,65 MB	2,00 %
9	64.15.112.242	1	1	0,00 %	14,18 MB	2,00 %	952,00 N	0,00 %	14,19 MB	1,90 %
10	tc9.vixy.net	1	2	0,00 %	14,00 MB	2,00 %	1,37 KB	0,00 %	14,00 MB	1,90 %
11	216.178.36.27	1	5	0,00 %	11,52 MB	1,60 %	3,64 KB	0,00 %	11,52 MB	1,50 %
12	74.220.202.10	1	13	0,00 %	11,44 MB	1,60 %	6,10 KB	0,00 %	11,45 MB	1,50 %
13	lax-v209.lax.youtube.com	1	1	0,00 %	11,31 MB	1,60 %	0,99 KB	0,00 %	11,31 MB	1,50 %
14	64.15.112.222	1	1	0,00 %	11,31 MB	1,60 %	932,00 N	0,00 %	11,31 MB	1,50 %
15	207.138.234.48	5	212	0,40 %	10,82 MB	1,50 %	65,26 KB	0,10 %	10,88 MB	1,50 %
	Todo el resto		**45148**	**82,70 %**	**450,98 MB**	**64,40 %**	**42,23 MB**	**85,80 %**	**493,21 MB**	**65,80 %**
	Total	**11**	**54606**	**100,00 %**	**700,20 MB**	**100,00 %**	**49,21 MB**	**100,00 %**	**749,41 MB**	**100,00 %**

Tabla 3.4 Detalle de los sitios web más frecuentes antes de la auditoria.

En la tabla 3.4 se puede observar una tabla que indica el tráfico por sitios web, se resume los sitios más frecuentes. La página más visitada es una red virtual, que no guarda relación con las actividades de la empresa.

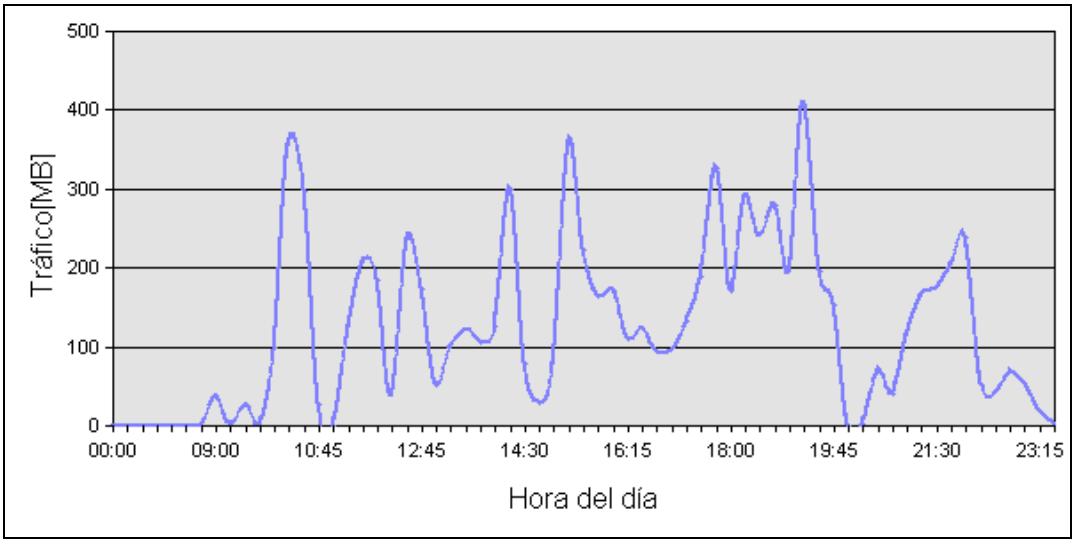


Figura 3.16 Tráfico antes de la auditoria.

La figura 3.16 resume la cantidad de tráfico de red, por hora del día, enviado a través del servidor ISA. El tráfico tanto de web como el que no es de web. Esto nos indica las horas en las cuales la red tiende a congestionarse a consecuencia de las actividades de los usuarios, tal como observamos en los gráficos anteriores, dichas actividades no están controladas, por lo que la red está congestionada casi a toda hora del día.

USO DE WEB

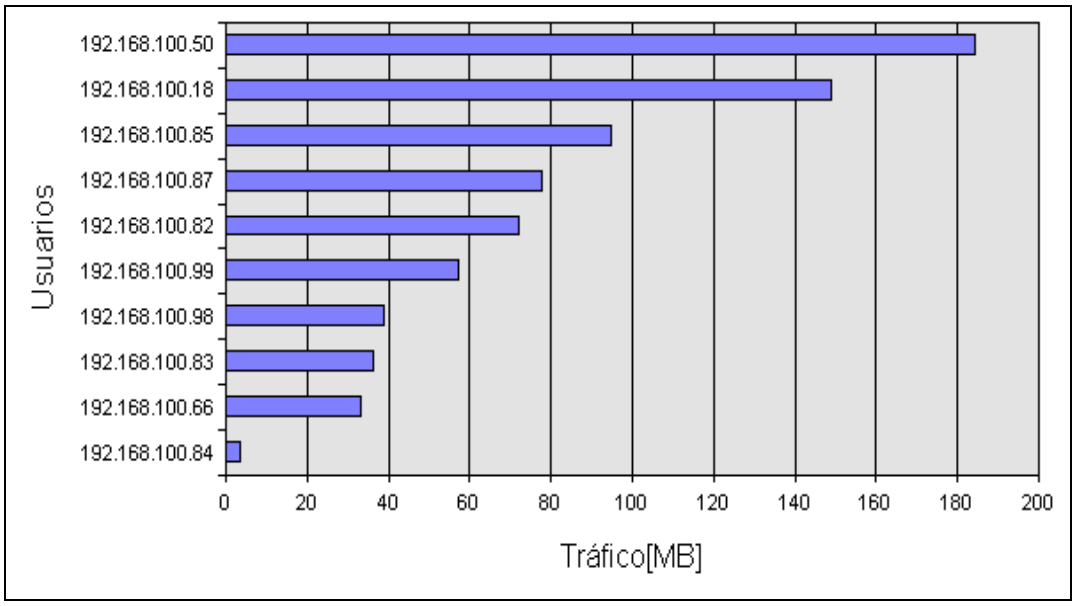


Figura 3.17 Diagrama de barras de los usuarios de web más frecuentes antes de la auditoria.

En la figura 3.17 se observan los usuarios de web que generaron la mayor cantidad de tráfico de web a través del servidor ISA, durante el periodo del informe. Los usuarios que generaron el mayor tráfico se muestran primero.

En este gráfico se identifica que personal de alto y bajo nivel en la escala del organigrama empresarial cuentan con los mismos privilegios de acceso de Internet.

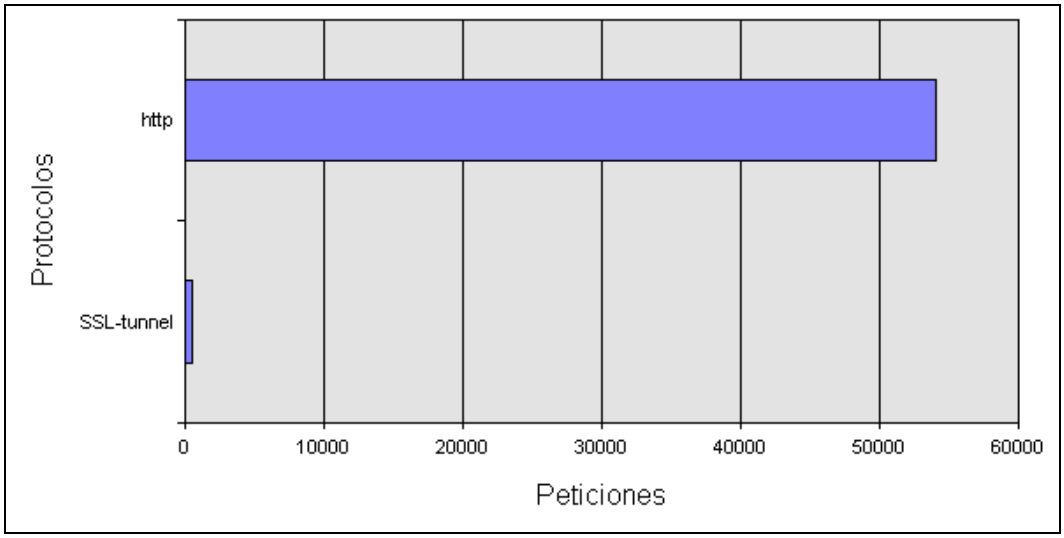


Figura 3.18 Diagrama de barras del tráfico por protocolo de web antes de la auditoría.

Los siguientes protocolos web se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe.

El ISA Server utiliza el túnel SSL cuando un usuario realiza una solicitud usando HTTPS por medio del explorador, generando un túnel a través del ISA Server.

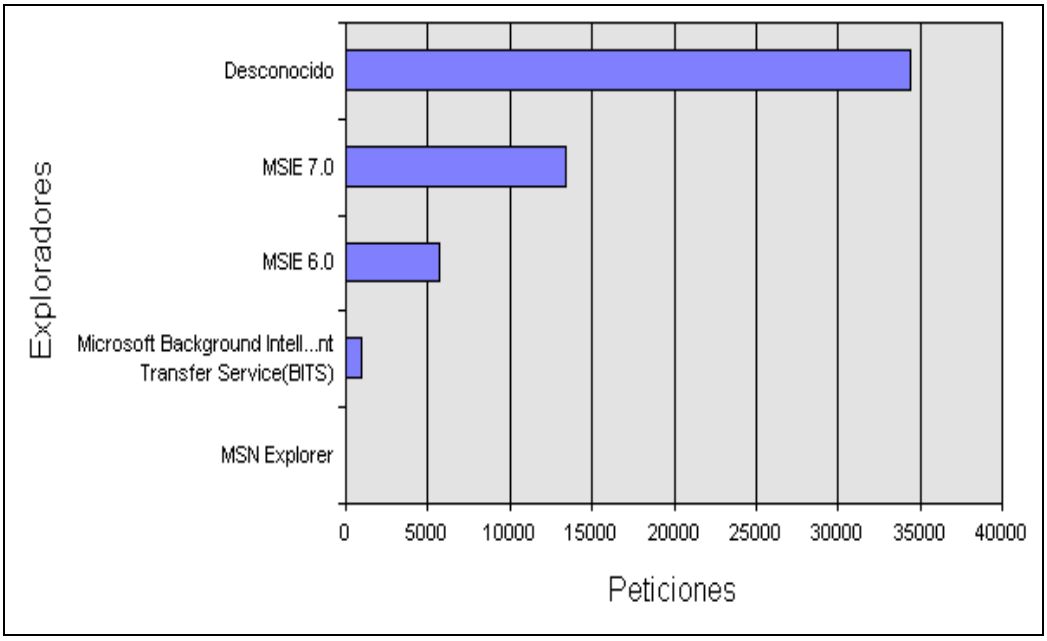


Figura 3.19 Diagrama de barras del tráfico de web por explorador antes de la auditoría.

En la figura 3.19 se observa el gráfico que resume qué exploradores web se usaron para conectarse a Internet por medio del servidor ISA, durante el periodo del informe. Los exploradores web usados con mayor frecuencia se muestran primero. Se identifica que no existen controles con respecto a la utilización de un explorador de manera unificada, por lo tanto se puede inferir que no se posee las licencias de los mismos.

Núm.	Explorador	Usuarios únicos	Peticiones	% de número total de peticiones
1	Desconocido	11	34456	63,10 %
2	MSIE 7.0	6	13369	24,50 %
3	MSIE 6.0	9	5695	10,40 %
4	Microsoft Background Intelligent Transfer Service(BITS)	4	998	1,80 %
5	MSN Explorer	7	32	0,10 %
	Todo el resto		**56**	**0,10 %**
	Total	**11**	**54606**	**100,00 %**

Tabla 3.5 Detalle de los Exploradores web utilizados en la LAN antes de la auditoria.

En la tabla 3.5 se observa que el explorador más utilizado es el de Microsoft Internet Explorer 6.0 y se deduce que el explorador desconocido corresponde a Mozilla Firefox, se identificó que es utilizado por algunos usuarios.

USO DE APLICACIONES

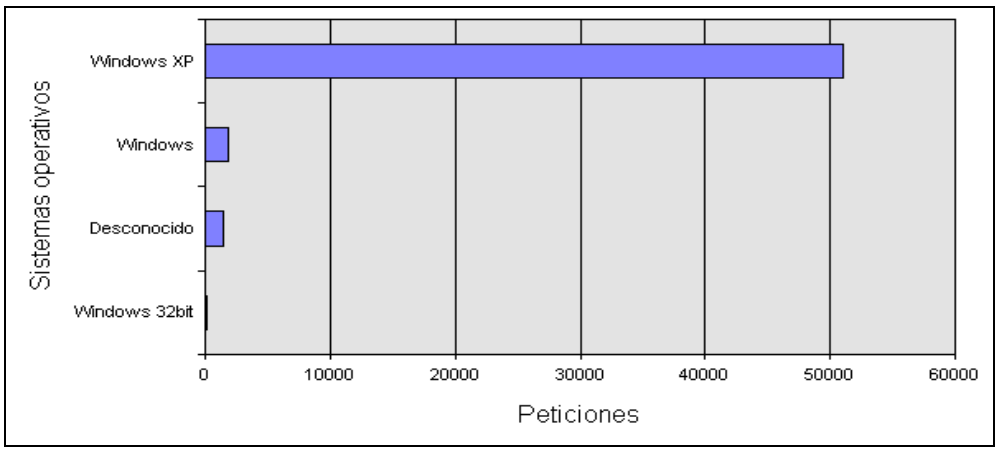


Figura 3.20 Diagrama de barras del tráfico por Sistema Operativo antes de la auditoria.

En la figura 3.20 se observan los sistemas operativos de equipos de usuarios usados con mayor frecuencia para solicitar contenido a través del servidor ISA, durante el periodo del informe. Se usa "desconocido" para los sistemas operativos que no pueden determinarse. (Los sistemas operativos más frecuentes para los informes de uso de aplicaciones no contienen el tráfico de web). Esto indica que no existe un estándar a nivel de plataforma de usuario

Núm.	SO	Usuarios únicos	Peticiones	% de número total de peticiones
1	Windows XP	11	51085	93,60 %
2	Windows	10	1912	3,50 %
3	Desconocido	11	1514	2,80 %
4	Windows 32bit	10	95	0,20 %
	Total	**11**	**54606**	**100,00 %**

Tabla 3.6 Resumen de Sistemas Operativos usados en la LAN antes de la auditoria.

PROTOCOLOS

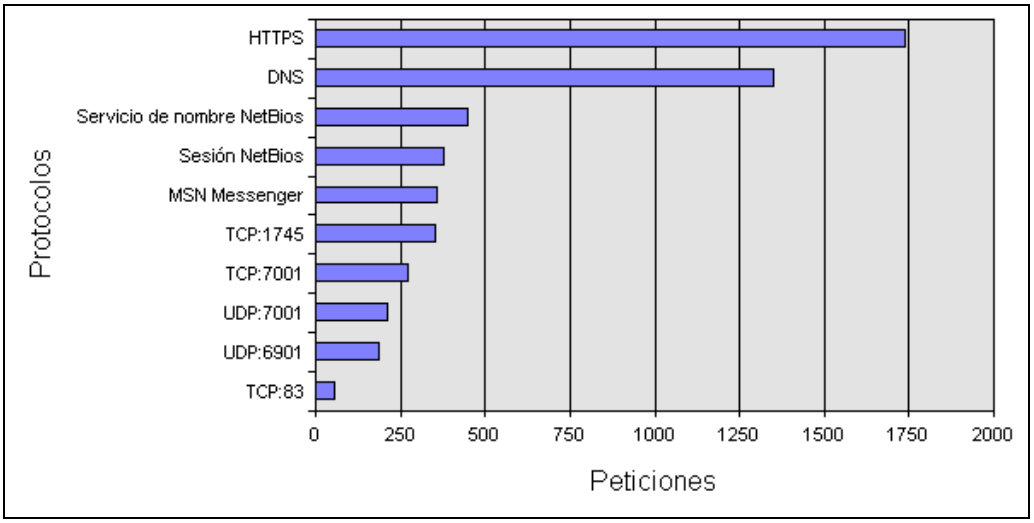


Figura 3.21 Diagrama de barras del tráfico por protocolos de aplicación antes de la auditoria.

En la figura 3.21 se observan los protocolos de comunicación que se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe. Los protocolos que se usaron con mayor frecuencia se muestran primero. Este informe no contiene el tráfico de web. No se refleja un control

en la utilización de protocolos, varios protocolos utilizados son empleados para acceso a centros de Chat.

Núm.	Protocolo	Usuarios únicos	Peticiones	% de número total de peticiones
1	HTTPS	5	1739	23,60 %
2	DNS	3	1349	18,30 %
3	Servicio de nombre NetBios	14	448	6,10 %
4	Sesión NetBios	13	378	5,10 %
5	MSN Messenger	4	358	4,90 %
6	TCP:1745	11	352	4,80 %
7	TCP:7001	4	271	3,70 %
8	UDP:7001	4	210	2,80 %
9	UDP:6901	2	188	2,60 %
10	TCP:83	2	56	0,80 %
11	UDP:6903	2	48	0,70 %
12	UDP:11113	2	47	0,60 %
13	Ping	8	45	0,60 %
14	TCP:31001	3	41	0,60 %
15	UDP:1077	1	33	0,40 %
	Todo el resto		**1808**	**24,50 %**
	Total	**21**	**7371**	**100,00 %**

Tabla 3.7 Resumen de Protocolo de Aplicación usados en la LAN antes de la auditoria.

APLICACIONES MÁS USADAS

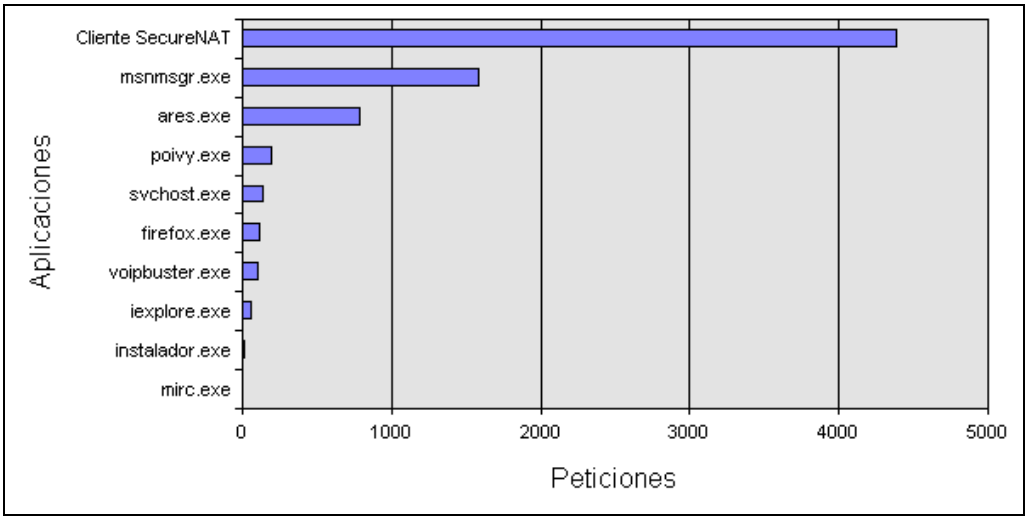


Figura 3.22 Diagrama de barras de las aplicaciones no web más usadas antes de la auditoria

En la figura 3.22 se puede observar las aplicaciones cliente que generaron la mayor cantidad de tráfico de red durante el periodo del informe. Las aplicaciones que generaron el mayor tráfico se muestran primero. El tráfico de aplicaciones contiene todo el tráfico excepto el tráfico de web. Se observa una variedad de aplicaciones tipo ejecutable no locales que influyen en el funcionamiento de la red, las cuales no son actividades propias de la empresa.

TRÁFICO Y USO

Conexiones

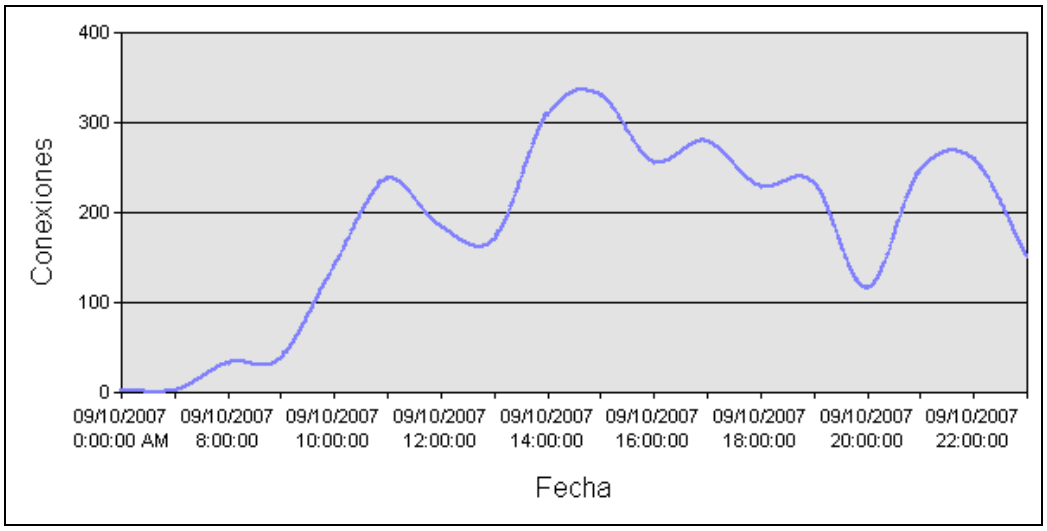


Figura 3.23 Máximo de conexiones simultáneas por fecha antes de la auditoria.

En la figura 3.23 se observa el gráfico que resume el número máximo de conexiones simultáneas durante cada día del periodo del informe. Se observan varias peticiones al mismo tiempo en el transcurso del dìa, no existe un control adecuado.

Rango de tiempo	Número máximo de conexiones simultáneas
09/10/2007 0:00:00 AM	2
09/10/2007 1:00:00	2
09/10/2007 8:00:00	33
09/10/2007 9:00:00	37
09/10/2007 10:00:00	138
09/10/2007 11:00:00	236
09/10/2007 12:00:00	184
09/10/2007 13:00:00	170
09/10/2007 14:00:00	310
09/10/2007 15:00:00	330
09/10/2007 16:00:00	255
09/10/2007 17:00:00	278
09/10/2007 18:00:00	229
09/10/2007 19:00:00	233
09/10/2007 20:00:00	116
09/10/2007 21:00:00	245
09/10/2007 22:00:00	259
09/10/2007 23:00:00	151

Tabla 3.8 Resumen de máximo de conexiones simultáneas antes de la auditoria.

SEGURIDAD

Paquetes Perdidos

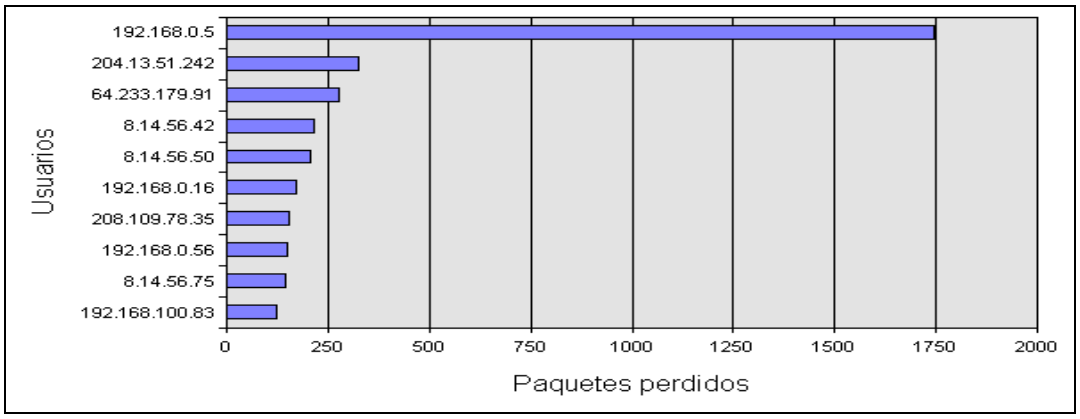


Figura 3.24 Diagrama de barras de los paquetes perdidos por usuario de la LAN antes de la auditoria.

En la figura 3.24 se observan el gráfico muestra los usuarios con la mayor cantidad de paquetes de red perdidos durante el periodo del informe. Los usuarios con la mayor cantidad de paquetes perdidos se muestran primero.

Núm.	Usuario	Paquetes perdidos	% de número total de paquetes perdidos
1	192.168.0.5	1744	19,80 %
2	204.13.51.242	325	3,70 %
3	64.233.179.91	276	3,10 %
4	8.14.56.42	214	2,40 %
5	8.14.56.50	208	2,40 %
6	192.168.0.16	172	1,90 %
7	208.109.78.35	153	1,70 %
8	192.168.0.56	151	1,70 %
9	8.14.56.75	146	1,70 %
10	192.168.100.83	124	1,40 %
11	169.254.47.213	113	1,30 %
12	80.154.37.11	108	1,20 %
13	209.17.65.6	108	1,20 %
14	192.168.100.2	100	1,10 %
15	192.168.100.66	95	1,10 %
	Todo el resto	**4785**	**54,20 %**
	Total	**8822**	**100,00 %**

Tabla 3.9 Resumen de paquetes perdidos por usuario de la LAN después de la auditoria.

Informes del ISA Server 2004 después de la auditoria

RESUMEN

En la figura 3.25 se puede observar protocolos de comunicación que se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe. Los protocolos que se usaron con mayor frecuencia se

muestran primero. Este reporte contiene el tráfico tanto de web como el que no es de web. Se puede verificar que los protocolos utilizados en la comunicación no van en contra de la política de seguridad de la empresa. Por ejemplo, ya no se observa el ingreso al Messenger.

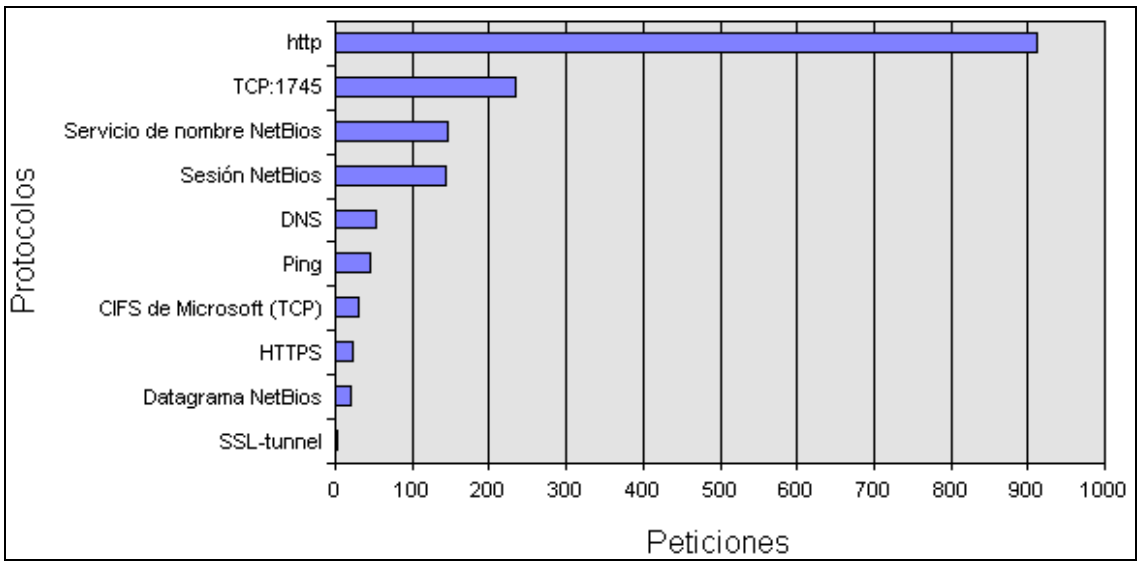


Figura 3.25 Diagrama de barras de los protocolos que se utilizan en la comunicación de la red después de la auditoria.

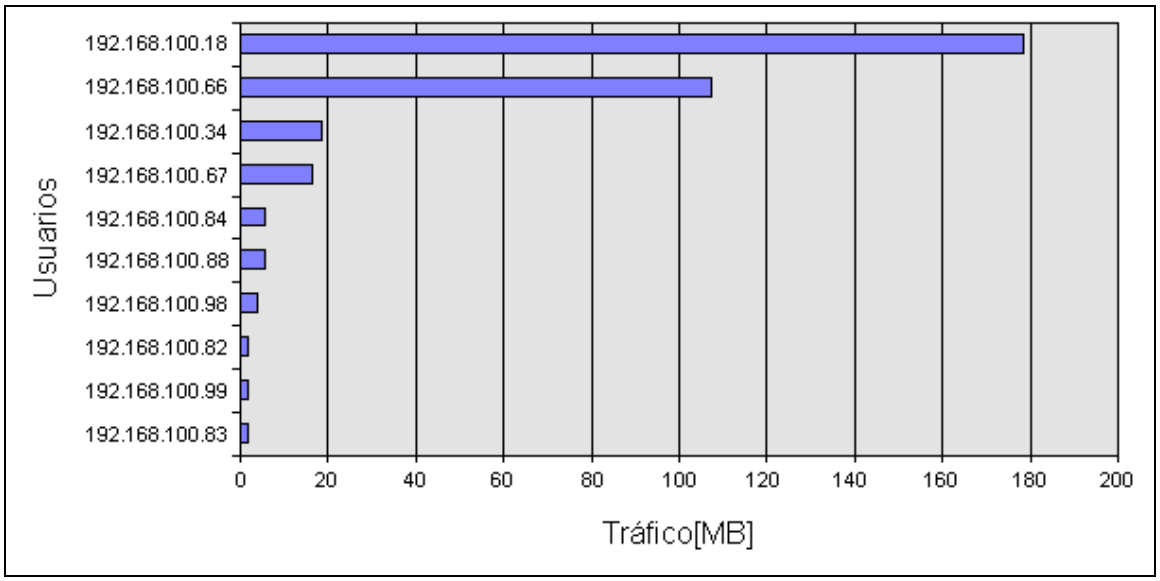


Figura 3.26 Diagramas de barras de los usuarios más frecuentes después de la auditoria.

En la figura 3.26 se observan los usuarios que generaron la mayor cantidad de tráfico de red a través del servidor ISA, durante el periodo del informe. Los usuarios que generaron el mayor tráfico se muestran primero. Este informe contiene tanto el tráfico de web como el que no es de web. El tráfico de la red está controlado, el mayor porcentaje lo realiza el personal de sistemas ya que da soporte al usuario y está en constante comunicación con ellos.

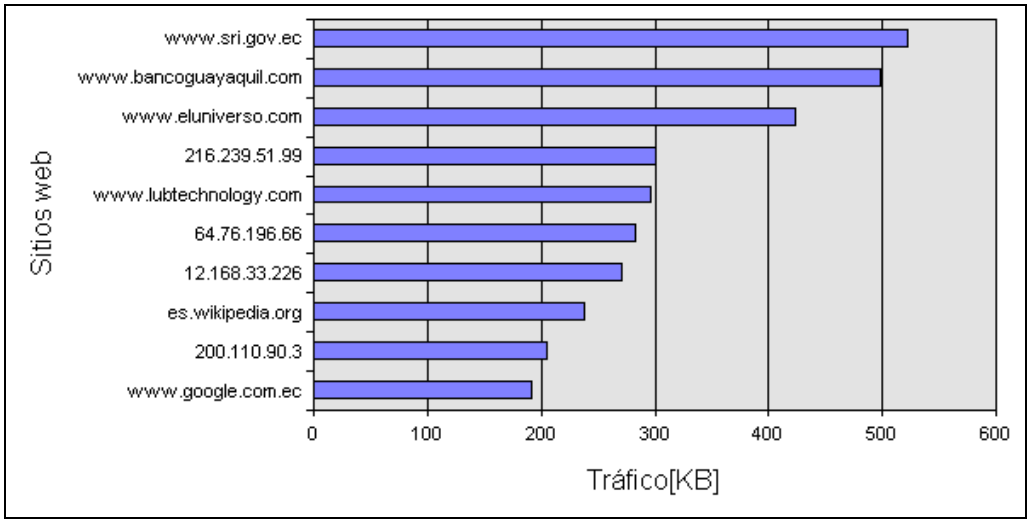


Figura 3.27 Diagrama de barras de los sitios Web más frecuentes después de la auditoria.

En la figura 3.27 se observan sitios web que fueron solicitados con mayor frecuencia por los clientes, durante el periodo del informe. Los sitios web más visitados se muestran primero. El acceso a las páginas WEB se cumple sólo para los sitios permitidos según el perfil del usuario, definido en el firewall.

Núm.	Sitio	Usuarios únicos	Peticiones	% de número total de peticiones	Bytes de entrada	% de número total de bytes de entrada	Bytes de salida	% de número total de bytes de salida	Número total de bytes	% de número total de bytes
1	www.sri.gov.ec	2	116	12,70 %	474,78 KB	10,40 %	46,81 KB	12,00 %	521,59 KB	10,60 %
2	www.bancoguayaquil.com	1	111	12,10 %	444,01 KB	9,80 %	53,94 KB	13,80 %	497,95 KB	10,10 %
3	www.eluniverso.com	1	67	7,30 %	392,41 KB	8,60 %	31,34 KB	8,00 %	423,75 KB	8,60 %
4	216.239.51.99	1	26	2,80 %	289,11 KB	6,40 %	11,61 KB	3,00 %	300,72 KB	6,10 %
5	www.lubtechnology.com	1	15	1,60 %	291,40 KB	6,40 %	4,51 KB	1,20 %	295,91 KB	6,00 %
6	64.76.196.66	1	43	4,70 %	268,58 KB	5,90 %	14,49 KB	3,70 %	283,08 KB	5,70 %
7	12.168.33.226	1	9	1,00 %	268,14 KB	5,90 %	2,47 KB	0,60 %	270,61 KB	5,50 %
8	es.wikipedia.org	1	25	2,70 %	229,88 KB	5,10 %	8,45 KB	2,20 %	238,33 KB	4,80 %
9	200.110.90.3	1	51	5,60 %	189,64 KB	4,20 %	14,80 KB	3,80 %	204,44 KB	4,10 %
10	www.google.com.ec	2	37	4,00 %	175,34 KB	3,90 %	16,04 KB	4,10 %	191,38 KB	3,90 %
11	200.32.70.37	1	36	3,90 %	171,53 KB	3,80 %	13,58 KB	3,50 %	185,10 KB	3,80 %
12	157.100.119.165	1	42	4,60 %	111,19 KB	2,40 %	13,46 KB	3,50 %	124,65 KB	2,50 %
13	8.6.13.62	1	13	1,40 %	105,03 KB	2,30 %	4,04 KB	1,00 %	109,07 KB	2,20 %
14	www.ceemp.espol.edu.ec	1	30	3,30 %	89,16 KB	2,00 %	10,51 KB	2,70 %	99,67 KB	2,00 %
15	latam.msn.com	1	6	0,70 %	91,43 KB	2,00 %	3,73 KB	1,00 %	95,16 KB	1,90 %
	Todo el resto		**288**	**31,50 %**	**953,47 KB**	**21,00 %**	**140,37 KB**	**36,00 %**	**1,07 MB**	**22,20 %**
	Total	**9**	**915**	**100,00 %**	**4,44 MB**	**100,00 %**	**390,16 KB**	**100,00 %**	**4,82 MB**	**100,00 %**

Tabla 3.10 Detalle de los sitios web más frecuentes después de la auditoria.

En la tabla 3.10 se puede observar una tabla que indica el tráfico por sitios web, se resume los sitios más frecuentes. Las páginas visitadas van de acuerdo a las reglas creadas con respecto a los perfiles de usuario, guardan relación con los intereses del negocio.

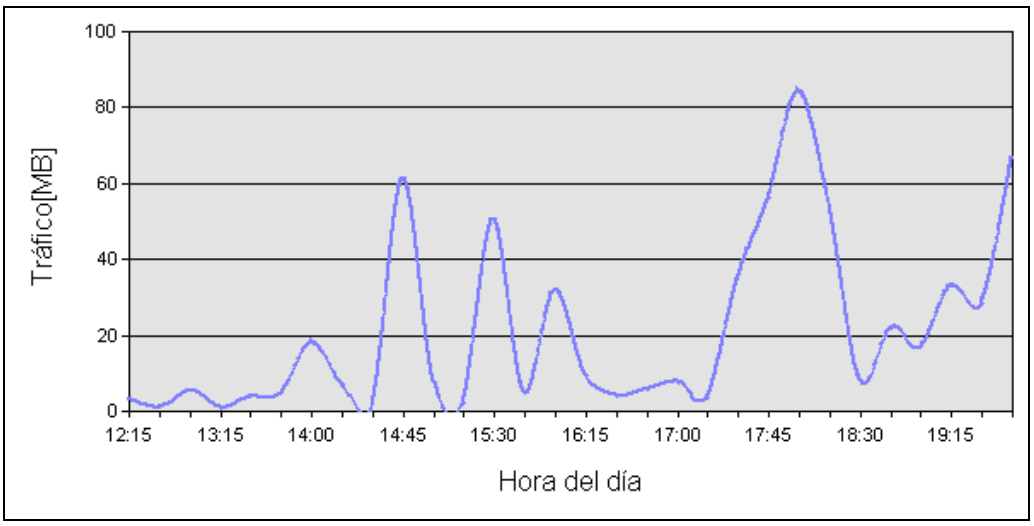


Figura 3.28 Tráfico después de la auditoria.

El siguiente gráfico resume la cantidad de tráfico de red, por fecha, enviado a través del servidor ISA. El informe contiene tráfico tanto de web como el que no es de web. El tráfico de la red es moderado, se incrementa al final del día laboral, pero es controlado.

USO DE WEB

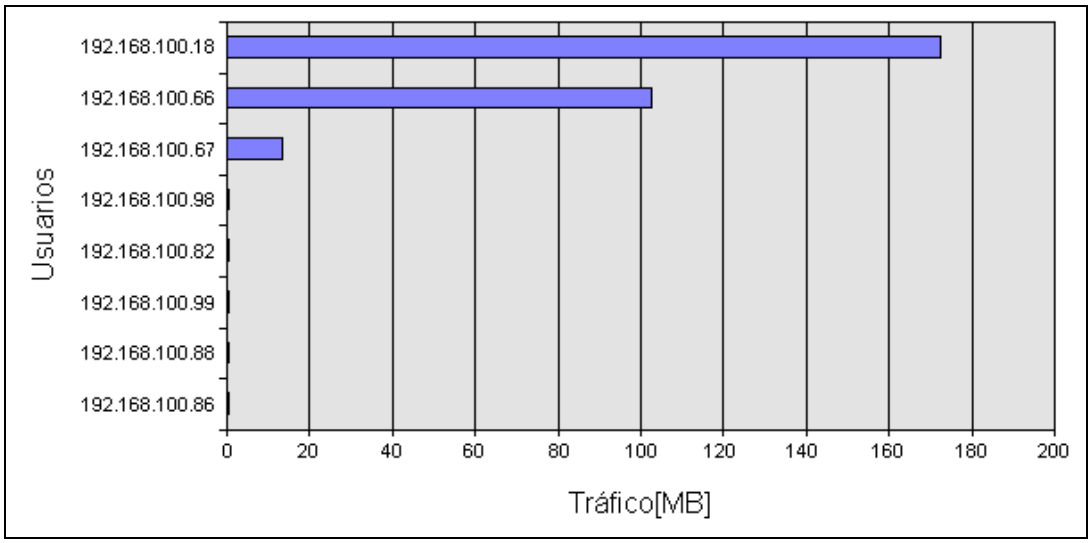


Figura 3.29 Diagrama de barras de los usuarios de web más frecuentes después de la auditoria.

En la figura 3.29 se observan los usuarios de web que generaron la mayor cantidad de tráfico de web a través del servidor ISA, durante el periodo del informe. Los usuarios que generaron el mayor tráfico se muestran primero. El tráfico de la red está controlado, el mayor porcentaje lo realiza el personal de sistemas ya que da soporte al usuario y está en constante comunicación con ellos. El acceso a páginas WEB está restringido de acuerdo al perfil del usuario.

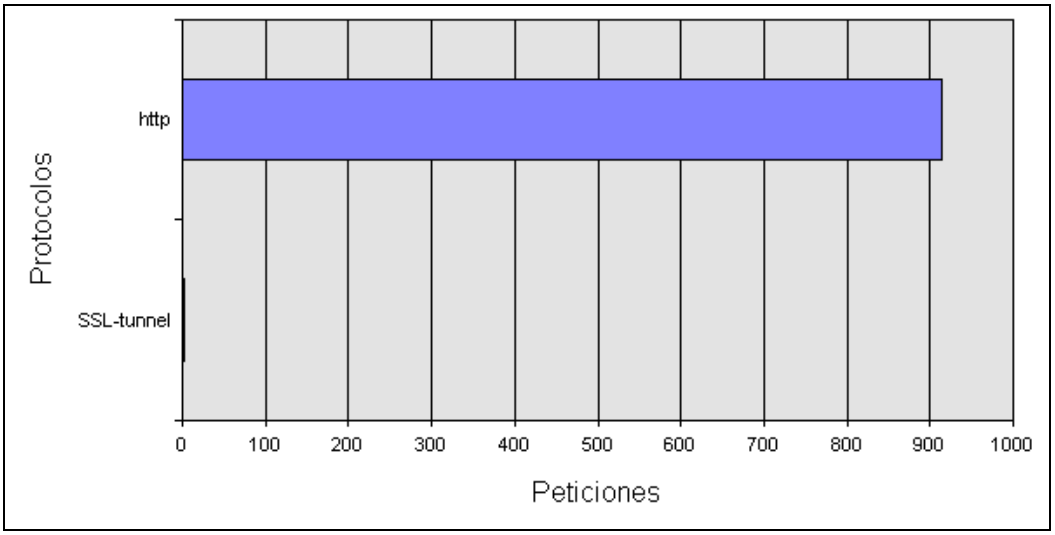


Figura 3.30 Diagrama de barras del tráfico por protocolo de web después de la auditoria.

En la figura 3.30 de observan los protocolos web que se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe. Los protocolos web que se usaron con mayor frecuencia se muestran primero. El nivel de peticiones se controla notablemente, actualmente se observa un número máximo de peticiones es 900, en comparación que sobrepasa las 10000 peticiones.

El ISA Server utiliza el túnel SSL cuando un usuario solicita una solicitud usando HTTPS por medio del explorador, generando un túnel a través del ISA Server.

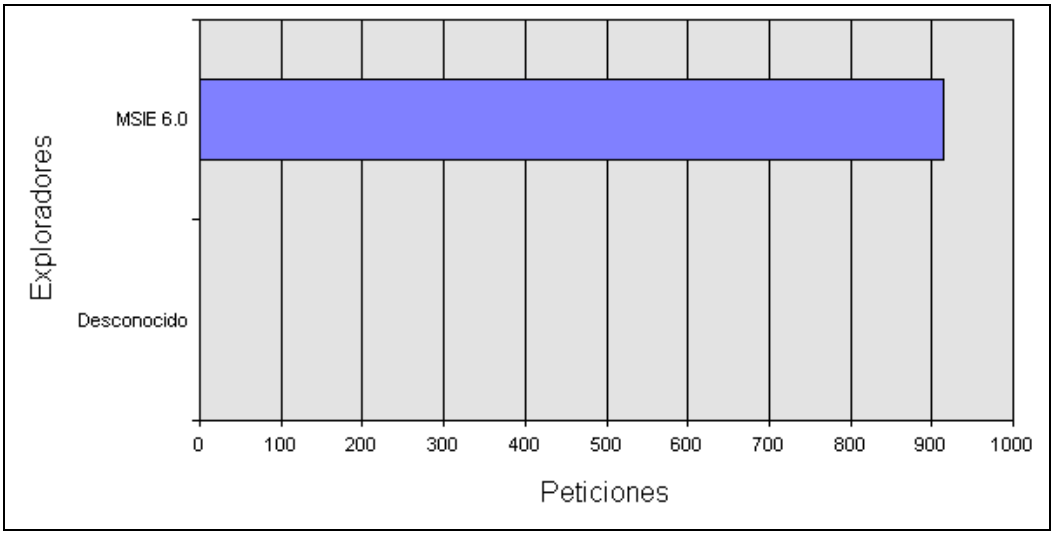


Figura 3.31 Diagrama de barras del tráfico de web por explorador después de la auditoria.

En la figura 3.31 se observa el gráfico que resume qué exploradores web se usaron para conectarse a Internet por medio del servidor ISA, durante el periodo del informe. Los exploradores web usados con mayor frecuencia se muestran primero. Se usa "desconocido" para las peticiones en las que el encabezado del agente de usuario HTTP no está disponible. Se observa un estándar con respecto al explorador que se utiliza a nivel de la red.

Núm.	Explorador	Usuarios únicos	Peticiones	% de número total de peticiones
1	MSIE 6.0	9	914	99,90 %
2	Desconocido	1	1	0,10 %
	Total	**9**	**915**	**100,00 %**

Tabla 3.11 Detalle de los Exploradores web utilizados en la LAN después de la auditoria.

En la tabla 3.11 se observa que el explorador más utilizado es el de Microsoft Internet Explorer 6.0 y se deduce que el explorador desconocido corresponde a Mozilla Firefox que utiliza el Jefe de Sistemas.

USO DE APLICACIONES

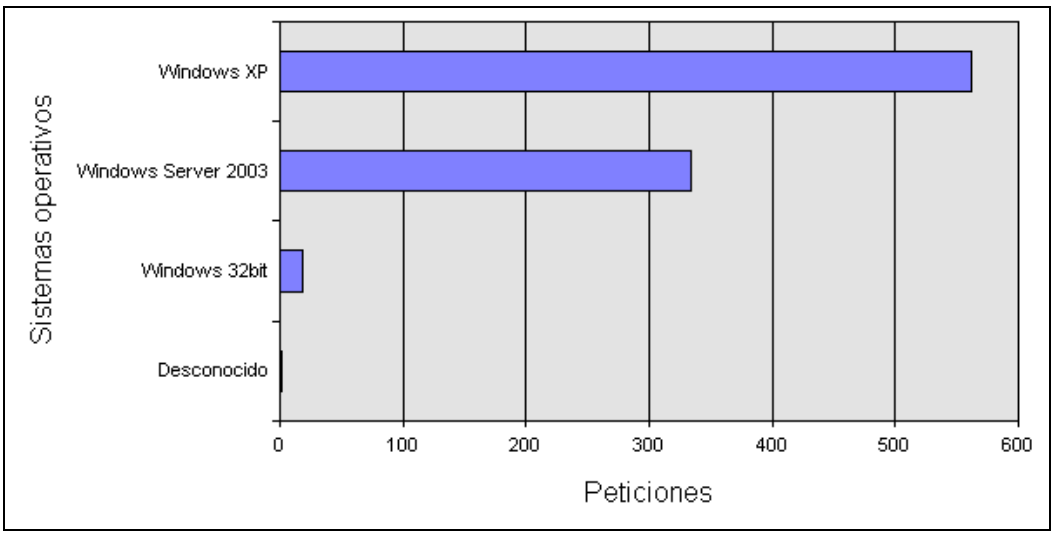


Figura 3.32 Diagrama de barras del tráfico por Sistema Operativo después de la auditoria.

En la figura 3.32 se observan los equipos que usaron los siguientes sistemas operativos con mayor frecuencia para solicitar contenido a través del servidor ISA, durante el periodo del informe. Se usa "desconocido" para los sistemas operativos que no pueden determinarse. (Los sistemas operativos más frecuentes para los informes de uso de aplicaciones no contienen el tráfico de web). Se observa que el nivel de sistemas operativos desconocido es casi

nula. El término desconocido puede indicar la falta de licencia; por lo tanto en su mayoría las PC's tienen licencia.

Núm.	SO	Usuarios únicos	Peticiones	% de número total de peticiones
1	Windows XP	3	562	61,40 %
2	Windows Server 2003	1	334	36,50 %
3	Windows 32bit	8	18	2,00 %
4	Desconocido	1	1	0,10 %
	Total	**9**	**915**	**100,00 %**

Tabla 3.12 Resumen de Sistemas Operativos usados en la LAN después de la auditoria.

Protocolos

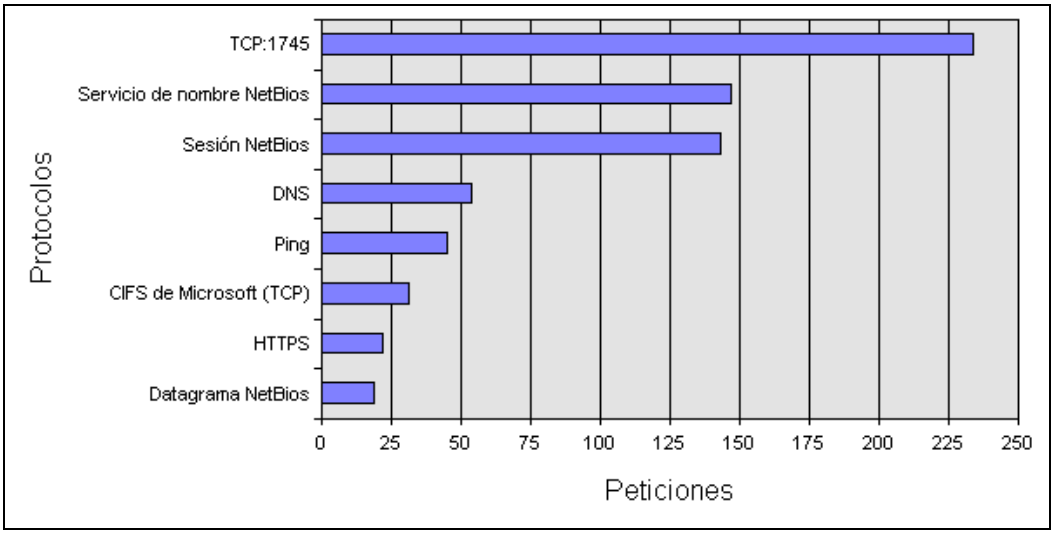


Figura 3.33 Diagrama de barras del tráfico por protocolos de aplicación después de la auditoria.

En la figura 3.33 se observan los protocolos de comunicación que se usaron para conducir tráfico de red a través del servidor ISA, durante el periodo del informe. Los protocolos que se usaron con mayor frecuencia se muestran primero. Este informe no contiene el tráfico de web; éste se proporciona en el informe de uso de web. Los protocolos evidenciados son usados por las diferentes aplicaciones permitidas por las políticas de la empresa.

Núm.	Protocolo	Usuarios únicos	Peticiones	% de número total de peticiones
1	TCP:1745	19	234	33,70 %
2	Servicio de nombre NetBios	17	147	21,20 %
3	Sesión NetBios	15	143	20,60 %
4	DNS	2	54	7,80 %
5	Ping	1	45	6,50 %
6	CIFS de Microsoft (TCP)	1	31	4,50 %
7	HTTPS	1	22	3,20 %
8	Datagrama NetBios	3	19	2,70 %
	Total	**21**	**695**	**100,00 %**

Tabla 3.13 Resumen de Protocolo de Aplicación usados en la LAN después de la auditoria.

Aplicaciones más Usadas

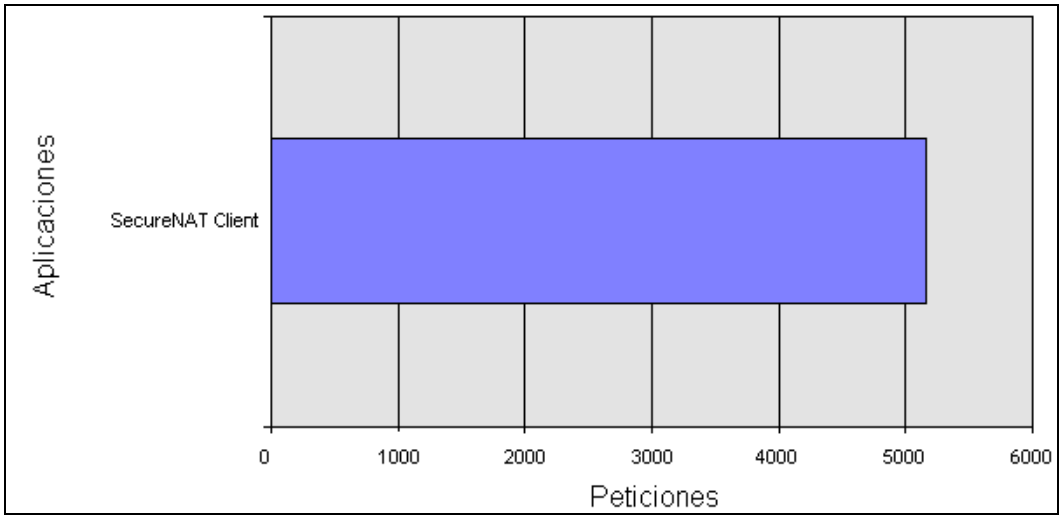


Figura 3.34 Diagrama de barras de las aplicaciones no web más usadas después de la auditoria

En la figura 3.34 se puede observas las aplicaciones cliente que generaron la mayor cantidad de tráfico de red durante el periodo del informe. Las aplicaciones que generaron el mayor tráfico se muestran primero. El tráfico de aplicaciones contiene todo el tráfico excepto el tráfico de web. Se ha controlado el uso de las aplicaciones que utilizan los usuarios. Sólo se observa el uso de SecurityNat para la traducción de una IP tipo LAN a una IP tipo WAN.

TRÁFICO Y USO

CONEXIONES

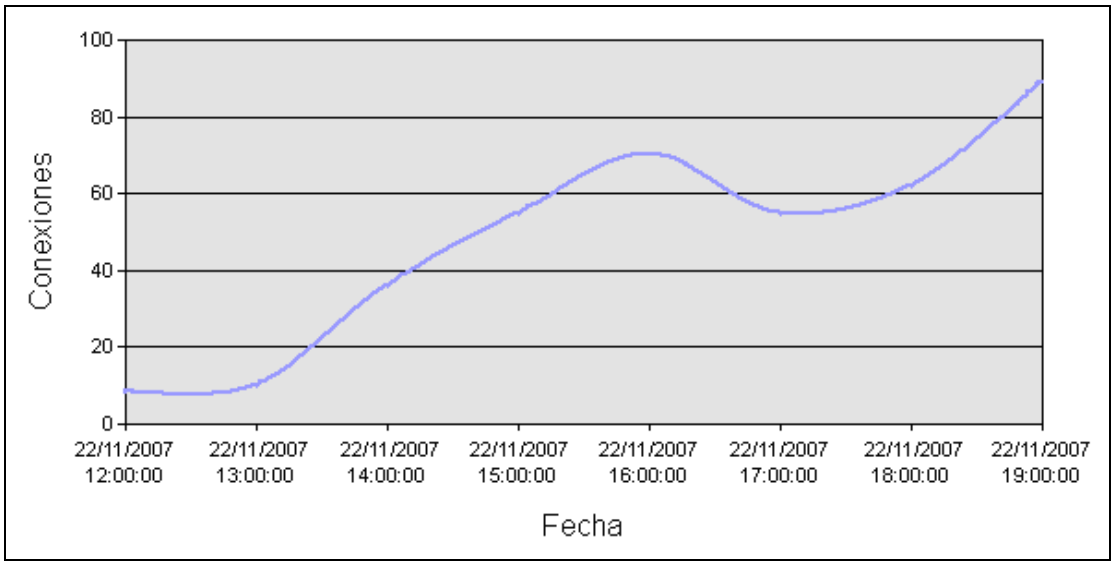


Figura 3.35 Máximo de conexiones simultáneas por fecha después de la auditoria.

En la figura 3.35 se observa el gráfico que resume el número máximo de conexiones simultáneas durante cada día del periodo del informe. Las conexiones simultáneas disminuyen con respecto a lo que se tenía inicialmente.

Del mismo modo en la Tabla 3.14 se observa el resumen máximo de conexiones simultáneas durante cada día del periodo del informe.

Rango de tiempo	Número máximo de conexiones simultáneas
22/11/2007 12:00:00	8
22/11/2007 13:00:00	10
22/11/2007 14:00:00	36
22/11/2007 15:00:00	55
22/11/2007 16:00:00	70
22/11/2007 17:00:00	55
22/11/2007 18:00:00	62
22/11/2007 19:00:00	89

Tabla 3.14 Resumen de máximo de conexiones simultáneas después de la auditoria.

SEGURIDAD

Paquetes Perdidos

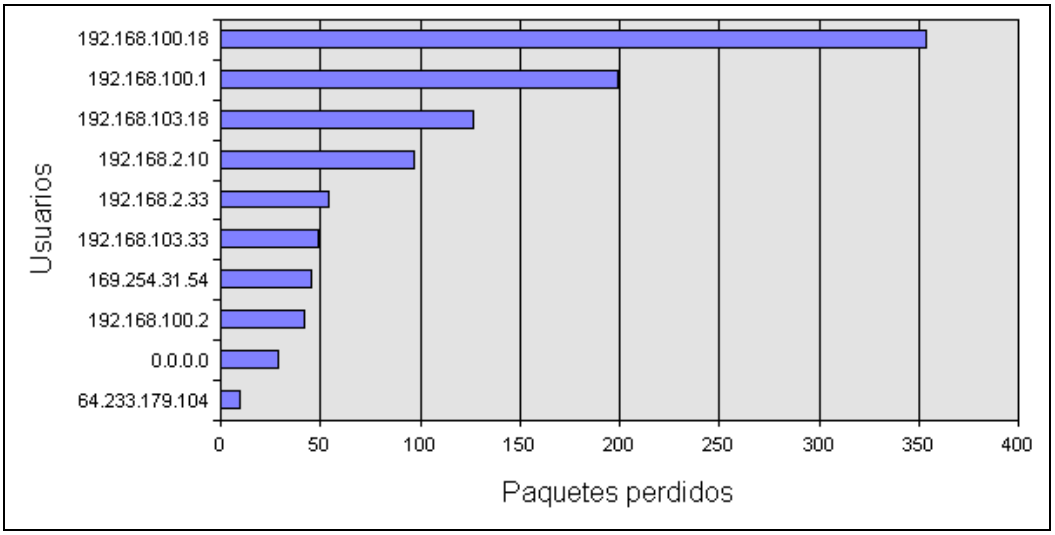


Figura 3.36 Diagrama de barras de los paquetes perdidos por usuario de la LAN después de la auditoria.

En la figura 3.36 se observan el gráfico muestra los usuarios con la mayor cantidad de paquetes de red perdidos durante el periodo del informe. Los usuarios con la mayor cantidad de paquetes perdidos se muestran primero.

La cantidad de paquetes perdidos disminuyó considerablemente, de tal modo que no afecte la disponibilidad de la información.

Núm.	Usuario	Paquetes perdidos	% de número total de paquetes perdidos
1	192.168.100.18	354	33,00 %
2	192.168.100.1	199	18,50 %
3	192.168.103.18	127	11,80 %
4	192.168.2.10	97	9,00 %
5	192.168.2.33	54	5,00 %
6	192.168.103.33	49	4,60 %
7	169.254.31.54	45	4,20 %
8	192.168.100.2	42	3,90 %
9	0.0.0.0	29	2,70 %
10	64.233.179.104	10	0,90 %
11	8.6.13.59	9	0,80 %
12	65.54.183.203	7	0,70 %
13	72.246.25.43	6	0,60 %
14	205.217.153.53	6	0,60 %
15	192.168.100.82	5	0,50 %
	Todo el resto	**34**	**3,20 %**
	Total	**1073**	**100,00 %**

Tabla 3.15 Resumen de paquetes perdidos por usuario de la LAN después de la auditoria.

INFORME DE AUDITORÍA

1. IDENTIFICACIÓN DEL INFORME

   Auditoria de la red de datos

2. IDENTIFICACIÓN DEL CLIENTE

   La red de área local

3. IDENTIFICACIÓN DE LA ENTIDAD AUDITADA

   Lubtechnology Cía. Ltda.

4. OBJETIVOS

   - Verificar que los procesos en la red estén de acuerdo a las políticas de seguridad de la empresa.
   - Verificar si existen medidas de seguridad en los equipos de comunicación para proteger la integridad de la información.
   - Verificar la disponibilidad de la información en todo momento.

5. HALLAZGOS POTENCIALES

   - Falta de licencias de software.
   - Falta de monitoreo de la red.
   - Carece de seguridad en Acceso a los equipos de comunicación.
   - Acceso ilimitado al Internet.

- Aplicaciones no actualizadas, como Antivirus.
- Dominios de broadcast muy elevados, todos los departamentos conectados a un mismo switch.

6. ALCANCE DE LA AUDITORIA

La auditoria comprende el período del 2007 y se ha realizado en toda la red de comunicaciones, LAN, bajo la norma ISO 17799.

El análisis a realizarse define el manejo de la seguridad con respecto al acceso de la información principalmente en la Intranet, y los privilegios de los usuarios con respecto al Internet, además seguridades en el acceso a la información de la aplicación contable de la empresa.

7. DEBILIDADES ESPECÍFICAS DETECTADAS

Debilidades detectadas	**Referencia**	
	Tabla	**Figura**
1. No se tiene un control adecuado. Las páginas web visitadas no tienen relación alguna con las actividades de la empresa. La red se congestiona casi a toda hora del día.	3.4	3.13, 3.14, 3.15, 3.16
2. Se identifica que personal de alto y bajo nivel en la escala del organigrama empresarial cuentan con los mismos privilegios de acceso de Internet. No existe una definición de perfiles de usuarios. Se observa un número alto de peticiones con respecto al protocolo http, usado para la navegación web.		3.17, 3.18
3. Se identifica que no existen controles con respecto a la utilización de un explorador de manera unificada, por lo tanto se puede inferir que no se posee las licencias de los mismos.	3.5	3.19
4. No existe un estándar a nivel de plataforma de	3.6	3.20

usuario.		
5. No se refleja un control en la utilización de protocolos, varios protocolos utilizados son empleados para acceso a centros de Chat.	3.7	3.21
6. Se observa una variedad de aplicaciones tipo ejecutable no locales que influyen en el funcionamiento de la red, las cuales no son actividades propias de la empresa. Se detectan conexiones simultáneas altas.	 3.8	3.22 3.23
7. El índice de paquetes perdidos es alto, lo que indica una deficiencia en la disponibilidad de la información.	3.9	3.24

Tabla 3.16 Debilidades encontradas durante la Auditoria de Seguridad.

8. CONCLUSIONES

- Como resultado de la auditoría se puede informar que se ha cumplido con la evaluación de los objetivos indicados anteriormente.
- Se obtienen deficiencias con respecto al cumplimiento de las normas de seguridad; no se presentan las restricciones adecuadas con respecto a los equipos de comunicación.
- No existe un procedimiento definido sobre respaldo de información, ni mantenimiento preventivo de sus equipos computacionales y de comunicación.
- No existe un plan de contingencia formal debidamente documentado, con los pasos a seguir cuando sucede un incidente.
- No existe un plan de recuperación y rescate de los equipos al momento de suceder un desastre.
- Escasez de personal debidamente capacitado.

9. RECOMENDACIONES

- Implementación de un Firewall que permita las restricciones adecuadas de acuerdo a las políticas de la empresa.
- Pruebas que verifiquen la conectividad de lo equipos. Estás pruebas se deben de realizar mediante el monitoreo continuo de los enlaces de la red, priorizando las conexiones críticas.
- Autenticación de ingreso por usuario en una estación de trabajo.
- Restricción de acceso a aplicaciones en cada estación de trabajo.
- Configuración de los equipos de comunicación que permita autenticar la conectividad de un equipo terminal.
- Implementación de VLANs por departamento para reducir el dominio de broadcast en la red, de tal manera que se descongestionaría notablemente el tráfico de red, volviendo a esta más ágil y rápida.
- Configuración de listas de acceso en el router que respalde la configuración del Firewall.
- Manual de funciones para cada puesto de trabajo dentro del área.
- Elaborar un calendario de mantenimiento de rutina periódico de los equipos de cómputo y de comunicaciones, así se disminuirá el tiempo promedio de caídas de los sistemas en el año, asegurando aún mas la disponibilidad de la información. Además también se alargará el tiempo de vida útil de los equipos de cómputo y comunicación

- Manual de procedimiento de respaldos donde se defina la periodicidad y alcance de los respaldos, así como los procedimientos de logística y técnicos para realizar estos. Se debe de guardar en un lugar seguro los respaldos realizados, en donde solo personal autorizado pueda acceder a estos. También mantener una copia de los respaldos fuera de las instalaciones de la empresa, de igual manera de una forma segura.
- Llevar una bitácora de respaldos en donde se documentara los sucesos ocurridos al momento de llevar a cabo el procedimiento de respaldo de la información de la empresa.
- Manual de procedimientos sobre el plan a seguir al momento de ocurrir un desastre, como un incendio, inundación, y demás. En este plan se deberá incluir que hacer por cada miembro del personal de la empresa al momento de ocurrir una calamidad, también estará dedicado a las personas encargadas del área de sistemas de cómo proseguir en lo posible, sin poner en riesgo su integridad física, para salvar la información de la empresa.
- Aislar los servidores y equipos de comunicación críticos en un cuarto, que llamaremos centro de computo, en donde solo el personal autorizado pueda acceder y manipular físicamente de estos. Además este centro de cómputo debe de tener las mas altas seguridades

físicas, como una debida refrigeración, piso falso, alarmas contra incendios, extintores, cámaras de vigilancia, UPS.

- Capacitar debidamente al personal sobre el uso de las aplicaciones computadorizadas para disminuir el riesgo de posibles fallos por mal uso de los privilegios dados a cada uno de ellos.

10. FECHA DEL INFORME

	Planeamiento	***Ejecución***	***Informe***
Fechas	01-09-07 al 15-09-07	16-09-07 al 20-09-07	21-09-07 al 28-09-07

11. IDENTIFICACIÓN Y FIRMA DEL AUDITOR

Nombre y Apellidos	**Cargo**
Marjorie Chalén Troya	Auditor
Andrés Mideros Romero	Auditor
Washington Caraguay A.	Auditor

CORRECCIONES REALIZADAS MEDIANTE EL FIREWALL

Las correcciones realizadas fueron mostradas en la sección 3.3.1 donde se muestran los reportes del ISA Server 2004 luego de aplicar las recomendaciones descritas en el informe una vez concluida la auditoría de seguridad en una red de datos.

Correcciones mediante el firewall	Referencia	
	Tabla	**Figura**
1. Se puede verificar que los protocolos utilizados en la comunicación no van en contra de la política de seguridad de la empresa. Por ejemplo, ya no se observa el ingreso al Messenger.	3.10	3.25, 3.26, 3.27, 3.28,
2. El acceso a páginas WEB está restringido de acuerdo al perfil del usuario. El tráfico de la red es moderado, aunque se incrementa al cierre del día por los procesos de cierre del mismo. El tráfico de la red está controlado, el mayor porcentaje lo realiza el personal de sistemas ya que da soporte al usuario y está en constante comunicación con ellos.		3.29, 3.30
3. Se observa un control con respecto al explorador que se utiliza a nivel de la red.	3.11	3.31
4. Se observa que el nivel de sistemas operativos desconocido es casi nula. El término desconocido puede indicar la falta de licencia; por lo tanto en su mayoría las PC's tienen licencia.	3.12	3.32
5. Los protocolos evidenciados son usados por las diferentes aplicaciones permitidas por las políticas de la empresa.	3.13	3.33
6. Se ha controlado el uso de las aplicaciones que utilizan los usuarios. Sólo se observa el uso de SecurityNat para la traducción de una IP tipo LAN a una IP tipo WAN. Las conexiones simultáneas disminuyen con respecto a lo que se tenia inicialmente.	3.14	3.34 3.35

7. La cantidad de paquetes perdidos disminuyó considerablemente, de tal modo que no afecte la disponibilidad de la información.	3.15	3.36

Tabla 3.17 Correcciones realizadas mediante el Firewall.

3.3.2 Detección de intrusos en la red

Se puede detectar un intruso a través del monitoreo de la red, el firewall ISA Server brinda esta función ya que realiza el escaneo de los puertos, proporcionando información sobre los protocolos utilizados; como se observa en lo expuesto anteriormente.

También permite la configuración de alertas que indiquen cuando se genere algún tipo de ataque; por lo tanto, se pueden tomar medidas de seguridad dependiendo del tipo de alerta generado. Una medida de seguridad puede ser el bloqueo de un puerto e incluso el bloqueo total de acceso a red.

En la figura 3.37 se pueden observar el tipo de alertas que ofrece el firewall y en la figura 3.38, las acciones a tomar como medidas de seguridad.

Figura 3.37 Alertas del firewall

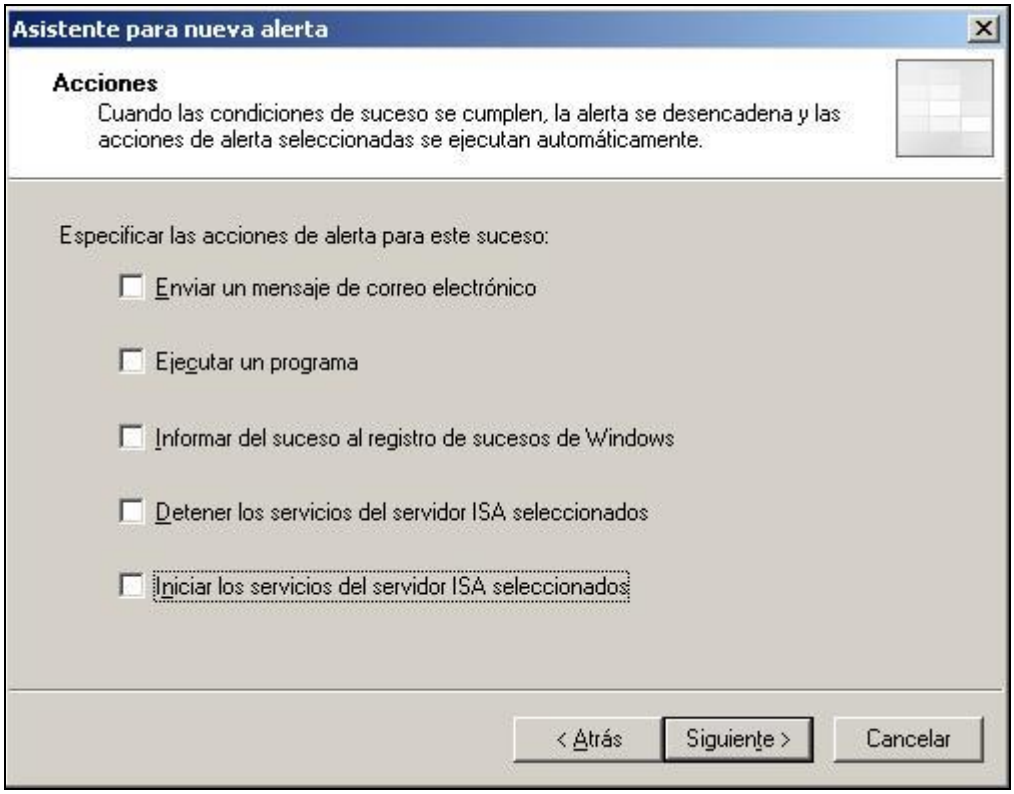


Figura 3.38 Acciones del firewall

CAPÍTULO 4:

ANÁLISIS DE COSTOS

4.1 COSTOS DE LA AUDITORIA

COSTO DE LA AUDITORÍA DE SEGURIDAD DE LA RED DE DATOS			
FASES A REALIZAR	**COSTO X FASE**	**TIEMPO DE TRABAJO**	**FORMA DE PAGO**
Diseño del mapa de la red a auditar. Revisión de conexiones físicas de la red. Captura, análisis y filtrado de datos. Confirmación de vulnerabilidades. Capacitación de personal Informe final de auditoría.	\$200 \$200 \$300 \$100 \$200 \$500	10 dias laborables	50 % a la firma del contrato 50 % al finalizar el proyecto
COSTO TOTAL	\$1500 + IVA	(Mil quinientos dólares americanos + impuestos)	
Andrés Mideros R. **Washington Caraguay A.** **Marjorie Chalén T.** *AUDITORES DE SEGURIDAD DE REDES DE DATOS*			
ACUERDO DE CONFIDENCIALIDAD La empresa y el personal de trabajo acuerdan que cualquier información intercambiada entre la empresa y los auditores será mantenida confidencialmente. Toda información que se intercambie se transmitirá exclusivamente por medios de comunicación seguros, bajo acuerdo mutuo entre las partes.			

Tabla 4.1 Costo de la Auditoria de Seguridad de la Red de Datos

El costo total de la Auditoria de una red de datos con todas las características vista anteriormente en la tabla 4.1 es de $ 1500,00 sin incluir impuestos.

4.2 COSTOS DE LA IMPLEMENTACIÓN

EQUIPOS DE COMUNICACIÓN			
DESCRIPCIÓN	**CANT.**	**COSTO UNITARIO**	**COSTO TOTAL**
CISCO C2960 SWITCH CATALYST 24 PUERTOS	3	$ 500,00	$ 1.500,00
CISCO 2801 ROUTER	1	$ 400,00	$ 400,00
TOTAL:			$ 1.900,00

Tabla 4.2 Costos de equipos de comunicación

EQUIPOS TERMINALES			
DESCRIPCIÓN	**CANT.**	**COSTO UNITARIO**	**COSTO TOTAL**
PC DE ESCRITORIO	15	$ 485,00	$ 7.275,00
SERVIDORES	2	$ 935,00	$ 1.870,00
TOTAL:			$ 9.145,00

Tabla 4.3 Costos de equipos terminales

LICENCIAS			
DESCRIPCIÓN	**CANT.**	**COSTO UNITARIO**	**COSTO TOTAL**
MICROSOFT WINDOWS XP	15	$ 110,00	$ 1.650,00
MICROSOFT OFFICE 2007	8	$ 149,95	$ 1.199,60
MCROSOFT WINDOWS SERVER 2003	2	$ 440,00	$ 880,00
MICROSOFT ISA SERVER 2004	1	$ 450,00	$ 450,00
ANTIVIRUS NOD32 VERSION PROFESIONAL MULTIUSUARIO (10 USUARIOS)	2	$ 243,00	$ 486,00
SAIR	1	$ 1.000,00	$ 1.000,00
TOTAL			$ 5.662,60

Tabla 4.4 Costos de Licencias

MATERIALES VARIOS			
DESCRIPCIÓN	**MEDIDA (m)**	**COSTO por metro**	**COSTO TOTAL**
CABLE UTP	500	$ 1,30	$ 650,00
CONECTORES RJ-45	42	$ 0,15	$ 6,30
JACK DE PARED PARA RJ-45	20	$ 1,50	$ 30,00
CANALETAS	150	$ 1,50	$ 225,00
ARMARIO GRANDE	0,7x0.4x2		$ 130,00
ARMARIO PEQUEÑO	0,7x0.4x0.7		$ 80,00
TOTAL			$ 1.121,30

Tabla 4.5 Costos de Materiales varios

SERVICIO DE INTERNET		
DESCRIPCIÓN	**COSTO MENSUAL**	**COSTO PRIMER MES**
ANCHO DE BANDA DE 320 Kbps, CONEXIÓN DSL SIMÉTRICO	$ 156,00	$ 156,00
INSTALACION		$ 120,00
TOTAL		$ 276,00

Tabla 4.6: Costos de los servicios de internet

MANO DE OBRA (3 PERSONAS)			
DESCRIPCIÓN	**HORAS**	**COSTO por hora**	**COSTO TOTAL**
CABLEADO ESTRUCTURADO	30	$ 60,00	$ 1.800,00
CONFIGURACION DE LOS EQUIPOS DE COMUNICACIÓN	8	$ 80,00	$ 640,00
CONFIGURACION DE LOS EQUIPOS TERMINALES	16	$ 60,00	$ 960,00
CONFIGURACION DEL ISA SERVER 2004	8	$ 100,00	$ 800,00
TOTAL			$ 4200,00

Tabla 4.7: Costos de mano de obra de implementación

El costo total de la implementación de una red de datos con todas las características vista anteriormente en las tablas es de **$ 22.307,90** sin incluir impuestos.

BENEFICIOS

El beneficio de la empresa es a presente y futuro en toda la gestión de la esta, al hacer una pequeña comparación, el costo de $1500 dólares de la auditoria es aceptable, ya que equivale aproximadamente al 7% del costo total de la implementación de la red de datos, como se puede observar en la tabla 4.1. A continuación se hace énfasis en los principales beneficios, ya sean estos tangibles o intangibles

BENEFICIOS TANGIBLES

- Antes de realizar la auditoría existía un consumo desmedido de ancho de banda, lo que frecuentemente ocasionaba congestionamiento en la transmisión de datos, esto se debía a que todo el personal tenía acceso al Internet y no existían restricciones de ninguna clase. Con la intervención, se redujo el ancho de banda de 512 a 320 Kbps debido a que solo se permitió el acceso a Internet solo al personal autorizado por la gerencia.
- Del mismo modo se mejora la eficiencia en la productividad y optimización de los procedimientos administrativos por parte de empleados debido a la asignación del Internet solamente a personal autorizado,
- El mayor beneficio adquirido por la empresa luego de realizada la auditoría es la evaluación y posterior protección de su activo mas

importante, los datos financieros de la empresa, ya que en el sistema se encuentra desde la venta de un producto o servicio sencillo hasta compras con altas sumas de dinero, ya que situaciones de pérdidas de insumos y materiales se habían suscitado con anterioridad en el interior de la empresa, es decir en la documentación soporte había más de lo que en el sistema estaba registrado, es decir que por la falta de seguridad en el sistema contable la posibilidad de un fraude era latente. (debido a acuerdos de confidencialidad no se precisa con mayor detalle otros problemas suscitados).

BENEFICIOS INTANGIBLES

- La implementación de VLANS en la red de datos, trae consigo un mejoramiento en la gestión de red, así la inclusión de un nuevo empleado a la empresa, no traería mayores problemas en asignarle un equipo de computación personal y conectarlo a la Intranet. Además, al remodelarse la red de datos, se reubicó el personal de trabajo, mejorando el ambiente de confiabilidad y privacidad en la organización jerárquica de la empresa, eliminándose la posibilidad de espionajes de claves y contraseñas.
- La implantación de un sistema de seguridad en general, beneficia desde el punto de vista preventivo y correctivo, ya que un pequeño corte de energía eléctrica puede causar severos daños en los equipos

de cómputo y de comunicaciones, como también la extracción de información confidencial de la empresa de parte de empleados; puede llevar abajo el crecimiento económico debido a la excesiva competencia de ventas de servicios en el mercado automotriz.

- Vale mencionar que a más de la protección física y lógica de equipos de computación y comunicaciones, se capacitó al personal de sistemas y se analizaron novedades tecnológicas y se incorporaron aquellas que mejoraron la eficiencia y los servicios.

A continuación una tabla donde se detalla la estimación anual de valores de los beneficios adquirido

BENEFICIO	ESTIMACIÓN MENSUAL	ESTIMACIÓN ANUAL
Disminución del ancho de banda	$ 100,00	$ 1.200,00
Eficiencia en la productividad por hora de trabajo	$ 20,00	$ 240,00
Disminución de fraudes en inventarios y sistemas	$ 50,00	$ 600,00
Mejoras en la gestión de red	$ 25,00	$ 300,00
Prevención de daños en equipos eléctricos	$ 20,00	$ 240,00
TOTAL	$ 215,00	**$ 2.580,00**

Tabla 4.8: Estimación en valores monetarios de Beneficios

Ya que generalmente las auditorias se realizan anualmente, podemos hacer uso del valor obtenido de la estimación anual de los beneficios que se obtendrán una vez realizada la auditoría para obtener el impacto financiero.

Así, la relación de beneficios a costo es de 1,72 dólares por cada dólar invertido.

En conclusión, podemos afirmar que es valida la inversión realizada por la empresa por los beneficios obtenidos y el poco capital invertido.

CONCLUSIONES Y RECOMENDACIONES

Conforme a la información recopilada y en base a la norma ISO 17799 se desarrolló un procedimiento para la realización de la auditoría, el mismo que se divide en fases; esto se logra con la investigación realizada y presentada en el capítulo 2. El procedimiento busca seguir una metodología al momento de analizar una red.

La implementación de la auditoria nos permitió un detectar las falencias de seguridad más relevantes que existían en la red SOHO de la empresa Lubtechnology. De acuerdo a las actividades del negocio, la debilidad más resaltante detectada fue la falta de políticas en la empresa y una falta de definición de funciones de los miembros de la misma, por ende una falta de control en las actividades de los usuarios.

Participamos de la implementación de una restructuración en la red como un trabajo adicional al trabajo realizado, ya que la auditoria cubre los procedimientos de entendimiento, evaluación, validación de controles en

caso de requerirlos, mas no de implementación. Para lo que empleamos una herramienta tipo software, firewall ISA Server 2004 para el control de accesos y de monitoreo de una red SOHO, bajo su utilización limitamos los accesos de los usuarios de acuerdo a las actividades que deben realizar los usuarios de acuerdo al cargo y funciones que desempeñan en la empresa; obteniendo un resultado favorable, disminuyendo el trafico de la red y un ambiente de control, lo que no se observaba antes.

Por otro lado, mediante relevamientos de los procesos más importantes de la compañía identificamos los puntos más críticos relacionados al sistema contable Sair, en los cuales se enfocó nuestra revisión. Identificando así personal que tenían acceso a transacciones sensitivas las cuales no estaban ligadas a sus actividades normales. Esto fue informado a la gerencia y por ende corregido, disminuyendo brechas de seguridad; reforzando así el ambiente de control de accesos en el sistema Sair, y por consecuencia de todos los procesos importantes de la compañía.

La seguridad no sólo depende de la herramienta que se emplee para la ejecución de los controles pertinentes a la seguridad de la información; un factor que posee un alto nivel de importancia, es el usuario. Por lo tanto, en una organización se debe capacitar a cada empleado con respecto al manejo de los equipos terminales, de cuáles son los accesos y el tipo de información

que manejan; también deberán ser notificados de las sanciones que se impondrán en caso de violar las políticas de seguridad.

Se debe considerar que para cubrir las diferentes áreas con respecto a seguridad, existen varios caminos a seguir. Sin embargo, para lograr la protección adecuada de la información, se requiere el análisis pertinente y dirigido a lo que realmente requiere la organización. Es decir, no se trata de utilizar cualquier herramienta con el fin de indicar que hay cierta protección, sino de identificar cual es la más apropiada.

Mediante la auditoria conseguimos beneficios tangibles como intangibles, a corto y a largo plazo logrando una optimización del desempeño de la red, disponibilidad de la información y mejora en la eficiencia en la producción y productividad.

Recomendamos a la gerencia de la empresa Lubtechnology, luego de la implementación de la auditoria informática, hacer revisiones periódicas de sus procesos y operaciones relacionado a sus sistemas, para de esta forma se garantice que estos se estén llevando de acorde a lo estipulado en la políticas internas de la compañía. Estas revisiones deberán ser realizadas por agentes externos a las operaciones normales de la compañía para que

de esta forma no quede en duda la validez de la revisión ya que se mantiene su independencia.

ANEXOS

ANEXO 1

Propuesta de Auditoria

Guayaquil, Septiembre 04 de 2007

EMPRESA LUBTECHNOLOGY CIA. LTDA.
Presente.-

De mis consideraciones:

Nos complace en presentarle nuestra propuesta para realizar una AUDITORÍA DE SEGURIDAD DE LA RED DE DATOS de su distinguida empresa en la ciudad de Guayaquil, de acuerdo a las políticas de seguridad establecidos por la alta gerencia.

Esperando cumplir con sus expectativas, estamos a sus órdenes para aclarar las dudas que tuviere y recibir sugerencias.

Atentamente.

Andrés Mideros. **Washington Caraguay.** **Marjorie Chalén.**

AUDITORES DE SEGURIDAD DE REDES DE DATOS

A continuación se adjunta detalladamente la propuesta.

COSTO DE LA AUDITORÍA DE SEGURIDAD DE LA RED DE DATOS

El costo total de la auditoría es de $ 1,500 (mil quinientos dólares americanos), sin incluir impuestos. Lo que incluye el costo total de la auditoría de acuerdo a los términos, condiciones y requerimientos establecidos por el personal.

Forma de pago

50 % a la aceptación de esta propuesta.

50 % al finalizar la auditoría

Tiempo de Entrega

A partir de la entrega de la orden de aceptación, el proyecto tiene una duración de 30 días y para la entrega del reporte final de auditoría.

Acuerdo de Confidencialidad

La empresa y el personal de trabajo acuerdan que cualquier información intercambiada entre las partes será mantenida de manera confidencial.

Toda información que se intercambie se transmitirá exclusivamente por medios de comunicación seguros, bajo acuerdo mutuo entre las partes.

ANEXO 2

Certificación de trabajo de auditoría

LUBTECHNOLOGY

CERTIFICADO

Certificamos que los señores **Marjorie Alexandra Chalén Troya, Luis Andrés Mideros Romero y Washington Antonio Caraguay Ambuludi,** trabajaron en nuestras instalaciones durante los meses de septiembre y octubre, realizando una auditoría completa a nuestro sistema de información y a nuestra red de computadoras y equipos de comunicaciones.

Al final de la auditoría recibimos un completo reporte de diagnóstico y recomendaciones, el cual fue aprobado e implementado, contando durante todo el proceso con el apoyo y participación de los señores mencionados.

Atentamente

Guayaquil, Noviembre 8 de 2007

Ing. Liseth Neira
Gerente de Finanzas & RRHH
Lubtechnology Cia Ltda

Guayaquil: Norte Av. Tanca Marengo Km. 4.5 - Machala . Arizaga y Tarqui esquina

Tfnos 2276908-2276903-2276852-2388042-2445490

ANEXO 3

Comandos de las Configuraciones de los Equipos de Comunicación

Configuración Router

```
------------------ show running-config ------------------

Current configuration : 1960 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname LUB
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$m8.R$TIUSMULRygltYU/wRTJsW0
enable password 7 060A1A23735A0C1A0D4745450F0B242D2D2F
!
no aaa new-model
ip cef
!
!
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
interface FastEthernet0/0
 ip address xxx.xxx.xxx.xxx 255.255.255.0
ip access-group 101 out
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.100.1 255.255.255.240
!
```

```
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.100.17 255.255.255.240
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 192.168.100.33 255.255.255.240
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.100.49 255.255.255.240
!
interface FastEthernet0/1.5
 encapsulation dot1Q 5
 ip address 192.168.100.65 255.255.255.240
!
interface FastEthernet0/1.6
 encapsulation dot1Q 6
 ip address 192.168.100.81 255.255.255.240
!
interface FastEthernet0/1.7
 encapsulation dot1Q 7
 ip address 192.168.100.97 255.255.255.240
!
 interface BRI0/2/0
 no ip address
 encapsulation hdlc
 shutdown
!
interface Serial0/3/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 2000000
!
!
ip default-gateway xxx.xxx.xxx.xxx
!
!
ip http server
 no ip http secure-server
!
access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq www
access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq smtp
access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq pop3
access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq 443
access-list 101 permit tcp 192.168.100.0 0.0.0.255 any eq 1863
access-list 101 permit tcp 192.168.100.16 0.0.0.15 any eq 7
!
```

```
!
!
control-plane
!
!
!
gateway
 timer receive-rtp 1200
!
!
!
 line con 0
 password 7 020A115934120A22441E5E572836313F33280B061617041401
 login
line aux 0
line vty 0 4
 password 7 020A115934120A22441E5E570C191519091725
 login
!
scheduler allocate 20000 1000
end
```

Configuración Switch Distribución

```
------------------ show running-config ------------------

Current configuration : 1981 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname distribucion
!
enable secret 5 <removed>
enable password 7 <removed>
!
no aaa new-model
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

```
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/5
 switchport access vlan 2
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
 switchport access vlan 3
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/11
 switchport access vlan 3
```

```
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/12
 switchport access vlan 3
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/13
 switchport access vlan 3
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/15
 switchport access vlan 3
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
 switchport mode trunk
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
```

```
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.100.4 255.255.255.240
 no ip route-cache
!
ip http server
!
control-plane
!
!
line con 0
 password 7 <removed>
 login
line vty 0
 password 7 <removed>
 login
line vty 1 4
 no login
line vty 5 15
 no login
!
!
end
```

Configuración del Switch 1

```
------------------ show running-config ------------------

Current configuration : 1927 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname switch1
!
enable secret 5 <removed>
enable password 7 <removed>
!
no aaa new-model
ip subnet-zero
!
!
```

```
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
 switchport access vlan 4
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/2
 switchport access vlan 4
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/3
 switchport access vlan 4
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/4
 switchport access vlan 4
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/5
 switchport access vlan 4
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
```

```
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/11
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/12
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/13
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/14
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/15
 switchport access vlan 5
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
```

```
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.100.5 255.255.255.240
!
ip classless
ip http server
!
!
!
control-plane
!
!
line con 0
 password 7 <removed>
 login
line vty 0 4
 password 7 <removed>
 login
line vty 5 14
 password 7 <removed>
 login
line vty 15
 no login
!
!
End
```

Configuración del Switch 2

```
------------------ show running-config ------------------

Current configuration : 1909 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname switch2
!
```

```
enable secret 5 <removed>
enable password 7 <removed>
!
no aaa new-model
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/2
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/3
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/4
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/5
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/6
 switchport access vlan 6
 switchport mode access
```

```
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/7
 switchport access vlan 6
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
 switchport access vlan 7
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/15
 switchport access vlan 7
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/16
 switchport access vlan 7
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/17
 switchport access vlan 7
 switchport mode access
switchport port-security
 switchport port-security mac-address sticky
 port secure max-mac-count 1
!
interface FastEthernet0/18
!
```

```
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.100.6 255.255.255.240
 no ip route-cache
!
ip http server
!
control-plane
!
!
line con 0
 password 7 <removed>
 login
line vty 0 4
 password 7 <removed>
 login
line vty 5 15
 no login
!
!
end
```

BIBLIOGRAFÍA

- Cole, E., Krutz, R., and Conley, J. W. (2005). Network security bible. Indianapolis: Wiley Publishing, Inc.
- Carlson, B. (2007). Sistemas de comunicación. Mexico. D.F.: Mc Graw-Hill.
- Tipton, H. F., Krause, M. (2004). Information security management handbook. New York: Auerbach Publications, Co.
- Strebe, M. (2004). Network security foundations. San Francisco: SYBEX, Inc.
- Peltier, T. R., Peltier, J., Blackley, J. (2004). Information security fundamentals. New York: Auerbach Publications, Co.
- Rhee, M. Y. (2003). Internet security. Indianapolis: Wiley Publishing, Inc.
- Stallings, W. (2003) Data and computer communications. New Jersey: Prentice hall.
- Briceño, J. (2003). Transmisión de datos. Mérida: Departamento de publicaciones de la Universidad de los Andes

OTRAS REFERENCIAS

- Cisco Networks. CCNA Módulo 1, 2 y 3
- http:// es.wikipedia.org/wiki/FEC
- http:// es.wikipedia.org/wiki/multplexación
- http://grouper.ieee.org/groups/802/3/10G_study/public/july99/azadet_1_0799.pdf
- http://www.textoscientificos.com/redes/area-amplia
- http://lmi.bwh.harvard.edu/papers/pdfs/2003/martin-fernandezCOURSE0i.pdf
- http://www.ifent.org/Lecciones/digitales/secuenciales/Teorema_Muestreo.asp
- http://www.textoscientificos.com/redes/ethernet/control-acceso-medio-csma-cd
- http://genesis.uag.mx/edmedia/material/comuelectro/uni1_2_7.htm
- http://vgg.uma.es/redes/topo.html
- http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wireles

slan/intro.asp

- http://www.it.uniovi.es/docencia/Telecomunicaciones/arss/material/arssTema5-Conmutacioncircuitos.pdf
- http://www.eie.fceia.unr.edu.ar/ftp/Comunicaciones/MUX.pdf
- http://metabolik.hacklabs.org/alephandria/txt/RSC-0_6_0.pdf
- http://www.it.aut.uah.es/juanra/docencia/fundamentosdetelematica/materiales/ARQ.pdf
- http://www.fi.uba.ar/materias/7543/m7543t/datalink.pdf
- http://www.coitt.es/antena/pdf/162/06B_Reportaje_Auditorias.pdf
- http://www.hispasec.com/corporate/auditoria.html
- http://www.fistconference.org/data/presentaciones/gestiondeauditoriasdeseguridad.pdf
- http://www.amereiaf.org.mx/3reuniondeverano/materiales/Departamento_de_Seguridad_de_Computo_de_la_UNAM.pdf
- http://www.monografias.com/trabajos6/audi/audi.shtml
- http://es.wikipedia.org/wiki/Auditor
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/23d9f2a8-5484-4123-85ca-5e1c46921d59.mspx?mfr=true