UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"

SISTEMA DE SEGURIDAD DE DATOS DE UNA EMPRESA TELEVISORA MEXICANA

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO MECÁNICO ELECTRICO (ÁREA EN COMUNICACIÓNES)
P R E S E N T A :
JOSÉ CARLOS RAMÍREZ CORTÉZ

DIRECTOR DE TESIS M. I. LAURO SANTIAGO CRUZ

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO 200

DEDICATORIA:

El presente trabajo lo dedico a mis compañeros Ing. Carlos Landa Díaz, Miguel Ángel Luna, Miguel Ángel López y Sergio Guerra sin cuya colaboración hubiera sido imposible completar esta tesis.

A mi asesor el M en I Lauro Santiago Pérez, por su amable disponibilidad en apoyarme en este proyecto.

Así mismo a mi esposa, hijo y madre por el ánimo que me pudieron inyectar en cada momento.

Esperando en Dios, que los conocimientos adquiridos en la práctica profesional los pueda aplicar para resolver problemas en favor de la sociedad y nunca de una forma egoísta.

Muchas, muchas gracias:

ATTE. Ing. José Carlos Ramírez Cortéz

ÍNDICE

ÍNDICE DE FIGURAS

PÁG

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad informática corporativa, es el proceso por medio del cual las organizaciones pueden garantizar la confidencialidad, integridad y la disponibilidad de sus datos, sistemas y aplicaciones. Ésta, implementada de manera adecuada, incluye la autentificación (tú eres quien dice ser) y la autorización (permitir a los usuarios autentificados acceder a los datos, sistemas y aplicaciones permitidas).

La seguridad es un compromiso en el cual debe existir un balance entre la protección de un sistema, la facilidad de acceso y uso del mismo. Este compromiso se obtiene al considerar el riesgo que se tiene, observando la posibilidad de que ocurra una amenaza y cuanto le importa al interesado que dicha amenaza se presente.

Estadísticamente, los sistemas de seguridad son frecuentemente empleados para proteger a las organizaciones contra ataques internos, más que para protegerlas contra ataques externos planeados. No obstante, la seguridad está presente a menudo en noticias referentes a ataques de los llamados *hackers*, en fraudes cometidos a entidades financieras y espionaje industrial, entre otras, pero esa es solamente una pequeña parte a contemplar en la seguridad informática empresarial.

Con la introducción de Internet, "la Red de Redes", y por lo tanto de los negocios electrónicos, "eBusiness", con sus diferentes variantes como son: Negocio a Negocio, Negocio a Empleado, Negocio a Consumidor y Sistemas de Gobierno Digital, se han desarrollado nuevas formas de ataques en contra de la seguridad informática empresarial, como es el cyber-activismo (actividades vandálicas informáticas), las negaciones de servicio, la infección por virus, robo de información, intrusiones y el uso indebido de los activos de la empresa; por tal razón es necesario el uso de una estrategia integral de seguridad empresarial, basada en estándares y políticas que se estén empleando en dichos sistemas de seguridad.

Para cumplir con esta estrategia es crucial seguir con los pasos necesarios, iniciando con entender los procesos claves de la empresa -en cuanto a seguridad se refiere- , seguido de la composición de los principales activos de la misma -lo que se pretende proteger-, y a partir de ahí, realizar la evaluación de los riesgos de que la empresa pierda cualquiera de sus activos, para posteriormente implementar las políticas de protección con las tecnologías adecuadas.

La seguridad informática no es estática, ésta tiene que mantenerse continuamente actualizada, principalmente en cuanto a las nuevas amenazas que puedan surgir y las tecnologías que puedan cubrir las mismas. La mejor forma de llevar a cabo este mantenimiento, es auditando y revisando el esquema de protección de activos empresariales de forma continua.

Dentro del desarrollo del presente trabajo nos adentraremos en un caso real, consistente en una empresa televisora de nuestro país, que debido a su importancia como medio de comunicación, y a la alta tecnología con la que convive, deberá de contar con una fuerte protección de activos de datos, videos, nóminas ejecutivas al igual que la protección al acceso de los sistemas de sus socios, proveedores y público en general. Esta situación se presenta de forma generalizada en la mayoría de las empresas en nuestro país, y es nuestra tarea el contribuir con aportaciones como este trabajo, para entender cada vez más estos conceptos, ya que la única razón por la cual las empresas son vulnerables, es por la falta de cultura de seguridad informática.

La seguridad informática es de gran amplitud y por lo tanto es necesaria llevarla a cabo por etapas, de tal forma que en el planteamiento de este trabajo se estarán cubriendo: conceptos básicos -referentes a la constitución e implementación de una red de datos con sus diferentes componentes-, tomando esto como base para el mejor entendimiento y posterior análisis del sistema de seguridad propuesto; se diseñará una solución que evite el robo de información dentro de la red de esta empresa, y que impida el envío de la misma hacia el exterior; se tendrá control en los sitios de Internet a los que los empleados internos o externos acceden, complementando con herramientas contra ataques de virus y de análisis de vulnerabilidades para estos sistemas.

Lo anterior se desarrollará partiendo de los conceptos básicos en lo referente a la integración de una red de datos, los estándares y protocolos más utilizados actualmente, para posteriormente explicar la seguridad informática, desde los niveles del Sistema Operativo de Red, en nuestro caso, una red con Sistema Operativo *Microsoft Windows NT*, hasta las políticas más utilizadas y prácticas ligadas para este caso específico.

Este trabajo tiene también la intención de concientizar a las áreas informáticas y de seguridad de las empresas mexicanas en lo referente a la seguridad informática empresarial, lo cual impulsa a las mismas hacia los conceptos de empresa de clase mundial en nuestro país.

CAPITULO 1

TERMINOLOGÍA Y CONCEPTOS DE REDES

En la actualidad existen varios tipos de redes de cómputo, con variadas plataformas tecnológicas, desarrolladas por distintos fabricantes. En el presente capítulo se verán los principios básicos de implementación de una red de datos, junto con los diversos estándares, protocolos y componentes de red involucrados en la misma.

1.1. Modelos de redes

Históricamente las redes de cómputo se han desarrollo paso a paso, adoptando tres modelos básicos:

- Modelo de red Centralizada.
- Modelo de red Distribuida.
- Modelo de red Cooperativa.

Modelo de red Centralizada

El primero de estos tres modelos, también llamado de procesamiento centralizado, es una configuración de red en donde un sólo servidor procesa tareas para múltiples terminales. En este modelo todas las terminales se pueden comunicar con la computadora central, también llamada *mainframe*, quien realiza la tarea de procesamiento de información. Las terminales no realizan procesamiento de los datos y sirven sólo como receptores y transmisores de los mismos. En este modelo las terminales deben de compartir la potencia de procesamiento de la computadora central.

Modelo de red Distribuida

En el modelo de red Distribuida existe una mayor intervención del usuario final, donde el procesamiento de datos se realiza en mayor parte en la computadora central y una porción menor en la estación de trabajo del usuario. Este modelo requiere que las terminales tengan capacidad de procesamiento, esto es que cuenten con un *CPU (Central Processor Unit: Unidad Central de Procesamiento)*.

Modelo de red Cooperativa

Este modelo de red permite a los equipos que se encuentran dentro de un ambiente de cómputo distribuido, compartir poder de procesamiento, además de datos, recursos y servicios. Dentro de este modelo un equipo puede prestar poder de procesamiento al correr un programa en otra computadora de la red, o los procesos podrían ser designados para llevarse a cabo en una o más computadoras.

Las redes generalmente caen en alguna de las dos categorías de configuración siguientes:

- Redes tipo punto a punto *(peer to peer)*.
- Redes tipo Cliente/Servidor.

En el primer modo cada computadora conectada trabajará al mismo nivel jerárquico y todas pueden solicitar o pedir datos, servicios o recursos. Actuando como servidor o cliente. Sus principales características son:

- Todos los nodos pueden ser servidores y estaciones de trabajo a la vez, compartiendo sus discos duros, *CD-ROM's* e impresoras.
- El *NOS (Network Operating System: Sistema Operativo de Red)* debe instalarse en cada nodo, consume poca memoria y por lo tanto no se requiere de servidores dedicados.
- La administración e instalación de la red es muy sencilla, por lo que no se requiere de personal altamente calificado.
- Se pueden formar redes a partir de 2 nodos.
- Su sistema de seguridad es básico, pero puede ser suficiente para aplicaciones pequeñas.
- La principal ventaja de este tipo de redes es que son económicas, sencillas y fáciles de instalar, orientadas a cubrir el mercado de las pequeñas empresas.
- Sus desventajas consisten en su poca seguridad y limitantes de comunicaciones externas.

Las redes punto a punto llenan una necesidad que otras arquitecturas no cubren, que todos los nodos de la red compartan sus recursos, y no solamente los servidores. Hoy en día es común que coexistan en una misma red un Sistema Operativo de Red Cliente/Servidor y un sistema punto a punto, para aprovechar todas las ventajas de estas diferentes arquitecturas.

En el modo Cliente/Servidor se debe de partir que en una red existe un proceso distribuido, donde el procesador del Servidor ejecuta las instrucciones del Sistema Operativo de Red, generalmente de servicios de archivos, y el procesador de las estaciones de trabajo procesa los trabajos locales. No obstante lo anterior las aplicaciones cada día requieren de mayor poder en el procesador, lo que

implicaría que las estaciones de trabajo tuvieran procesadores muy poderosos, con las respectivas consecuencias económicas, pero si se parte del hecho que los servidores cuentan con este tipo de procesadores, la arquitectura Cliente/Servidor implica aprovechar estos procesadores poderosos para hacer las tareas pesadas y los trabajos ligeros dejárselos al procesador de las estaciones de trabajo.

Para poder manejar realmente una plataforma Cliente/Servidor se requiere que la aplicación esté diseñada específicamente bajo esta arquitectura y que el Sistema Operativo de Red dé soporte a estas aplicaciones.

La ventaja del modelo Cliente/Servidor, es que permite que las tareas se repartan en forma más eficiente entre los elementos involucrados (Clientes y Servidores) y que se minimice el intercambio innecesario de información entre ellos.

En la actualidad la arquitectura Cliente/Servidor se explota principalmente en las aplicaciones de base de datos y sistemas de correo electrónico. En estas aplicaciones el archivo completo es el que viaja desde el servidor de archivos a la estación de trabajo, ésta última procesa la información después de una serie de 'preguntas y respuestas' que se llevan a cabo entre el servidor y la estación, para que finalmente se devuelva el archivo. El servidor procesa la información y devuelve el resultado, o sea el registro, no el archivo completo que el cliente demandó.

El proceso Cliente/Servidor que se lleva a cabo en un servidor de intercomunicación o *Gateway de* comunicaciones es muy similar. Éste se encarga de las labores de comunicación entre el *host (también llamada computadora central)* y la estación de trabajo (cliente), a quien le envía solamente las pantallas necesarias y toma la información del teclado, pero el proceso de comunicaciones se lleva a cabo por completo en el Gateway.

1.2. Redes de cómputo

Existen los siguientes tipos de redes:

Una *LAN (Local Area Network: Red de Área Local)*, es un conjunto de computadoras interconectadas dentro de un área geográfica (física) limitada, como por ejemplo un edificio, una universidad, un hospital, etc. Las redes LAN suelen caracterizarse por velocidades de transferencia de datos relativamente altas y una relativamente baja incidencia de errores.

Las PC's que conforman la red LAN son llamadas nodos[1] y pueden ser tanto estaciones de trabajo como servidores, a las cuales se les ha instalado una Tarjeta de Interfaz de Red en sus ranuras de expansión, para conectarse al circuito LAN de la red.

A la forma física de conectar los nodos dentro de la LAN -es decir, el cableado- se le llama topología física. Dependiendo de la forma en que los nodos estén conectados podrá ser una red física de tipo estrella, anillo, bus, árbol o estrella-anillo.

La manera en que los datos pasan por el circuito de red se llama topología lógica. Siendo esencialmente de dos formas:

- *Bus*. Los datos pueden salir de todos los nodos simultáneamente, descartando los datos que no vayan dirigidos a sí mismos.
- *Anillo*. Los datos recorren todo el circuito, una vez por cada tiempo, quedándose en la computadora a donde el dato fue dirigido.

Una *WAN (Wide Area Network: Red de Área Amplia)*, se reconoce comúnmente como una serie de LAN's interconectadas entre sí y cuya extensión geográfica es ilimitada, la infraestructura de interconexión generalmente no depende en forma directa de la organización que controla la LAN. En este tipo de red la velocidad de transmisión de datos es relativamente baja, comparada a la de las LAN's.

La *MAN (Metropolitan Area Network: Red de Área Metropolitana)*, se encuentra entre la LAN y la WAN, con una cobertura que comprende desde unos kilómetros hasta cientos de kilómetros, y una velocidad de transmisión de unos cuantos kbps a Gbps, sirve como espina dorsal o *backbone* que interconecta varias LAN's distribuidas o puede proveer acceso a la red metropolitana o a una red pública de cobertura amplia.

1.3. Internet e Intranet

Hace aproximadamente una década, se inventaron los llamados exploradores o navegadores, aprovechando las facilidades visuales de las nuevas interfaces gráficas, en los sistemas operativos visuales como *Windows*, las cuales permitían "ver" el contenido de un servidor. Estos navegadores nos permiten recorrer un servidor con su contenido multimedia (datos, voz y video). De lo anterior se desprenden las redes que se definen como *Intranets* e *Internet*.

Una Intranet la definimos como una LAN o un conjunto de LANs cuya propiedad y administración es privada y pertenece a una empresa o un consorcio empresarial específico. Esta definición nos hemos permitido hacerla para distinguir entre la Internet y el medio ambiente "atrás" de la Internet, es decir, dentro de la red de una empresa conectada a la Internet. Porque si bien cualquier computadora, estación de trabajo o host que tenga acceso a la Internet, dentro de una empresa, está por definición "en línea" o conectada con la Internet. Para fines prácticos, distinguimos como una Intranet al conjunto de computadoras interconectadas dentro de una empresa o una LAN.

También definimos que cualquier máquina estará en línea con la Internet si cumple con los siguientes requisitos:

- Opera con la pila de protocolos TCP/IP.
- Tiene una dirección de IP asignada.
- Puede enviar paquetes o *frames* de IP a los servidores que lo soliciten y se encuentren conectados a la red global.
- Está conectada al router del *IPS (Internet Provider Server: Proveedor de Servicios de Internet).*

La Internet como es sabido es la "súper carretera" de la información. La gran WAN basada en los protocolos TCP/IP, desde su declaración oficial en 1983, con sus dos características más sobresalientes: la de conmutación de frames, que permite que un frame llegue desde su origen a su destino sin importar la trayectoria que éste siga y la de que cualquier LAN pueda conectarse a ella sólo con emplear los protocolos TCP/IP. Actualmente la Internet se compone de tres niveles de conectividad: el llamado backbone, que son redes de computadoras conectadas por un medio físico de muy alta velocidad, como fibra óptica; las redes de nivel medio o redes regionales, donde generalmente se conectan los *ISP's (Internet Service Providers: Proveedores de Servicios de Internet)* y el último nivel compuesto por las LANs y los host que son propiamente los usuarios finales de la Internet.

Dentro de los servicios que la Internet puede proveer distinguimos:

- Correo electrónico.
- Noticias o intercambio de mensajes noticiosos y foros.
- Sesión remota como Telnet, *rlogin (remote login: acceso remoto a la red),* donde se puede entrar a una máquina con una cuenta autorizada.
- *FTP (File Transfer Protocol: Protocolo de Transferencia de Archivos),* para intercambio directo de archivos desde un servidor de FTP.
- *WWW (World Wide Web: Malla de Red Mundial),* término idiomático empleado para describir al término más popular de Internet, la de despliegue de páginas de contenido multimedia (texto, imagen, voz y video) en una computadora.

Vale la pena mencionar que la llamada Red de Redes o WWW es una parte de Internet y no la Internet misma, como a veces se suele confundir. Ésta es un servicio específico de Internet, que se usa para visualizar páginas contenidas dentro de servidores de la Internet, mediante el uso de un explorador.

1.4. Servicios de red

Los servicios de red son la razón básica por la que interconectamos las computadoras. Basados en los servicios que una compañía ofrece, se puede comprar un programa y/o Sistema Operativo de Red específico. Dentro de una

red, las PCs deben tener un *software* especial que les permita funcionar en un ambiente de gestión de redes.

Los servicios de archivo permiten a las computadoras conectadas a una red compartir archivos entre sí. Este servicio incluye el almacenamiento, recuperación, o movimiento de archivos de datos, así como leer, escribir y manejar archivos y datos entre las computadoras. Los servicios de archivo son una parte importante de los ambiente Cliente/Servidor y de servicios Web. Las computadoras que proporcionan este tipo de servicios son llamadas servidores de archivo. Dos tipos de servidores existen: *dedicados* y *no dedicados*.

Los servidores *no dedicados* tienen una doble función: permitir a un usuario ir hacia la máquina que actúa como servidor de archivo y pedir el uso de archivos de otras máquinas; al mismo tiempo, estos servidores proporcionan archivos a los usuarios que les piden desde otras computadoras en la red. Los servidores *dedicados* cumplen solamente con conectar a los clientes a una red de computadoras.

Los servicios de archivo centralizados generalmente son más recomendados para organizaciones. Los términos centralizado y distribuido en este contexto describen el método de manejo de recursos del procesador, recursos de archivo, o las tareas administrativas.

Una tarea importante es proporcionar y regular el acceso a los programas y datos guardados en la unidad de disco duro del servidor de archivo. Esto es conocido como compartir archivos. Ésta es una de las razones principales por la que las compañías invierten en una red, las compañías pueden ahorrar dinero en adquirir una sola versión de alguna aplicación para red, en vez de adquirir tantas versiones individuales como equipos necesiten de su utilización.

Situar archivos de datos creados también por usuarios en un servidor, sirve a varios propósitos, incluyendo a la seguridad, al control de los documentos, actualización y respaldo de la información o *backup*.

La mayoría de las redes tienen alguna forma de almacenamiento de archivo centralizado. Durante muchos años, las compañías han usado el almacenamiento en línea u *online*, guardando información directamente al disco duro, a una cinta o disco óptico, para acceder a sus archivos, limitando la cantidad de espacio en disco disponible. Otro método común para guardar archivos es el almacenamiento fuera de línea u *offline*, que consiste en cerrar las aplicaciones, para de ahí ejecutar el procedimiento de backup de archivos a los medios comentados anteriormente. Otro sistema de almacenamiento para eficientar el espacio en disco es el llamado *HSM (Herarchical Storage Management: Sistema de Administración Jerárquico de Almacenamiento)*, éste consiste en migrar los datos de menos uso a alguno de los medios comentados anteriormente, pudiendo ser accesados en línea.

Otro servicio que ofrece la red es la actualización y sincronización de archivos o *file-update synchronization*. Éste asegura que todos los usuarios tienen la más reciente copia de un archivo. File-update synchronization puede supervisar la fecha y marca de tiempo en archivos y determina qué archivos fueron salvados recientemente.

Después de los servicios de archivo, imprimir probablemente es la segunda necesidad más importante para instalar una red. Imprimir basado en "cola de impresión" siempre será más económico que la impresión local, porque las estaciones de trabajo o *workstations* pueden compartir el recurso. El Servicio de Mensajería/Comunicación es el encargado de transferir información de un lugar a otro. Esta comunicación de información puede dividirse en tres sub-áreas:

- Correo electrónico o *Email*.
- Correo de voz o *voice mail*.
- Servicios de fax.

Servicios Web

Los servicios Web (SW) es el último paradigma hacia donde se dirige el mundo de las tecnologías de información. Éste consiste en combinar los servicios de aplicaciones tanto al interior como al exterior de la empresa; al interior consiste en compartir las aplicaciones entre los empleados de la organización, ofreciendo acceso de una forma sencilla a este tipo de sistemas; hacia el exterior, el compartir los sistemas con las entidades externas a la empresa, tanto proveedores, clientes, socios, aliados, etc. De esta forma proporciona un acercamiento con medios de alta automatización para incrementar los niveles de productividad en los diferentes procesos empresariales.

Para llevar a cabo este tipo de procesos es necesario integrar la infraestructura y las aplicaciones existentes en una sola visualización adaptada para cada usuario, en donde la tecnología juega un papel fundamental, desde los servidores que contienen a los equipos de conectividad y telecomunicaciones, el Sistema Operativo de Red, bases de datos, sistemas de Email, hasta los sistemas centrales como los *ERP's (Enterprise Resource Planning: Sistemas de Planeación y Administración de Recursos)*.

Las aplicaciones para este tipo de servicios ya no pueden actuar de forma independiente, por lo que actualmente, para cada una de estas aplicaciones, es necesario que estén ligadas a plataformas de servicios comunes, y es de ahí de donde provienen los conceptos B2x , Negocio a x o mayormente denominados sistemas *B2C (Business to Customer: Negocio a Cliente), B2E (Business to Employee: Negocio a Empleado), y B2B (Business to Business: Negocio a Negocio), entre otros*.

Servicio de Acceso Remoto

Es un servicio de información para los ISP's, el cual utiliza software y hardware de una computadora (una combinación de acceso local, " pools de módem", servidores de terminales, enrutamiento y capacidades para traducción de protocolo, todo ello en una sola solución) que está hecha para manejar usuarios que buscan acceso a un ISP desde un lugar remoto (en corporaciones, personas en subsidiarias, usuarios remotos y personas que viajan, etc).

El *RAS (Remote Access Services: Servicio de Acceso Remoto)*, soporta dos conjuntos de protocolos: los protocolos de acceso remoto y los de LAN. Cuando se utiliza el Servicio de Acceso Remoto, *Windows NT* utiliza los protocolos de acceso remoto para que a través del RAS se pueda conectar a otro equipo, a Internet o a un ISP. En estos protocolos se incluyen: el *SLIP (Serial Line Internet Protocolo: Protocolo de Linea Serial)*, el protocolo del Servicio de Acceso Remoto de *Microsoft* y el *PPTP (Point-to-Point Tunneling Protocol: Protocolo de Túnel Punto a Punto)*. El protocolo LAN que *Windows NT* utiliza para comunicarse sobre una conexión al Servicio de Acceso Remoto puede ser cualquiera de los protocolos que se utilizan en *Windows NT*, incluyendo *NetBEUI, NWLINK* o TCP/IP.

Red Privada Virtual

La *VPN (Virtual Private Network: Red Privada Virtual)* es una alternativa a la conexión WAN mediante líneas telefónicas y Servicio de Acceso Remoto, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autentificación, cifrado y el uso de túneles para las conexiones. Una VPN es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. La idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une dos o más redes que pertenecen a la red privada.

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para el personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrian ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública, se hace estableciendo túneles virtuales entre dos puntos, para los cuales se negocian esquemas de cifrado y autentificación, que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Cuando se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de cifrado y autentificación.

La tecnología de túnel o *tunneling* es un modo de transferir datos en la que se encapsula un tipo de paquete de datos dentro del paquete de datos de algún

protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan cifrados.

Las técnicas de autentificación son esenciales en las VPNs, ya que aseguran a los participantes de la misma, que están intercambiando información con el usuario o dispositivo correcto. La autentificación en la VPN es conceptualmente parecida al login en un Sistema Operativo de Red, como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autentificación usados en la VPN están basados en un sistema de claves compartidas.

La autentificación es llevada a cabo generalmente al inicio de una sesión, y luego en forma aleatoria durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya introметido en la conversación. La autentificación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo para derivar un valor incluido en el mensaje como *checksum*. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Típicamente las VPN's trabajan en los protocolos TCP/IP y UDP, y pueden utilizar diferentes tipos de cifrado, entre ellos se pueden mencionar *RSA, Public Key Cryptosystem 1024, 3DES, DES56 ó DES40*.

1.5. Estándares de red

Un estándar es un conjunto de reglas y procedimientos ampliamente utilizados u oficialmente especificados.

El mercado de las redes locales se debate en ofrecer soluciones estándares que permitan la comunicación de dispositivos de diferentes marcas, o bien ofrecer soluciones únicas para un sólo producto, sacrificando la estandarización en beneficio de un mejor rendimiento. La estandarización es la única vía que garantiza la compatibilidad de los equipos y la posibilidad de expandirse en un futuro evitando que queden obsoletos. Así, se permite la independencia de los fabricantes, en el sentido de que sí los productos están estandarizados serán compatibles entre sí y en todo momento el comprador podrá evaluar las distintas ofertas. Se cuenta además con la garantía de soportar un conjunto de servicios bien conocidos basados en métodos y técnicas bien probadas. Y se cuenta también con la facilidad de la expansión, permitiendo añadir en un futuro nuevos equipos y nuevos protocolos a la configuración existente.

Organizaciones de estándares

Muchas organizaciones contribuyen a establecer los estándares de interconectividad de redes, ofreciendo foros de discusión, generando

especificaciones formales a partir de discusiones informales y difundiendo las especificaciones una vez que han sido aprobadas.

La mayoría de las organizaciones generan estándares formales utilizando procesos específicos: organizando ideas, analizando métodos, votando acerca de aspectos de los estándares y posteriormente, liberando el estándar al público.

Algunas de las organizaciones más conocidas que contribuyen a la publicación de estándares de interconectividad de redes son las siguientes:

- *ISO (International Standar Organization: Organización Internacional para la Estandarización)*, es una organización internacional responsable de una gran variedad de estándares, entre ellos muchos relacionados con las redes. Su contribución más conocida fue el desarrollo del modelo *OSI (Open Systems Interconnection: Interconexión de Sistemas Abiertos)*, y su grupo de *protocolos OSI*.
- *ANSI (American National Standards Institute: Instituto Nacional Americano de Estándares)*, es el cuerpo que coordina a los grupos voluntarios de estandarización dentro de los Estados Unidos.
- *EIA (Electronic Industries Association: Asociación de Industrias Electrónicas)*, especifica los estándares de transmisión eléctrica, incluyendo los que se utilizan en la conectividad de redes. La *EIA* desarrolló el estándar *RS-232* que es ampliamente utilizado en la conexión de equipos periféricos.
- *IEEE (Institute of Electrical and Electronics Engineers: Instituto de Ingenieros en Electrónica y Electricidad)*, es una organización profesional que define la conectividad de redes y otros estándares. El IEEE desarrolló estándares de LAN ampliamente utilizados como el IEEE 802.5.
- *ITU-T (International Telecommunications Union_Telephony: La Unión Internacional de Telecomunicaciones)*, originalmente Comité Consultivo Internacional de Telegrafía y Telefonía, es una organización internacional que ha desarrollado estándares de comunicación como *X.25* y otros.
- *IAB (Internet Architecture Board: Consejo para la Arquitectura de Internet)*, es un grupo de investigadores de interredes que analizan problemas relacionados con Internet y establecen sus políticas a través de decisiones y grupos de trabajo. El *IAB* designa algunos *RFC (Request for Comments: Petición de Comentarios)*, como estándares de Internet, incluyendo el *TCP/IP (Transmision Control Protocol/Internet Protocol: Protocolo de Control de Transmisión/Protocolo de Internet)* y el *SNMP (Simple Network Management Protocol: Protocolo Simple de Administración de Red)*.

1.6. Modelo de referencia OSI

El modelo de referencia OSI es la arquitectura de red actual más prominente. OSI es un modelo de siete capas, donde cada capa define los procedimientos y las reglas (protocolos estandarizados) que los subsistemas de comunicaciones deben

seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. La figura 1.1. Muestra el modelo de referencia OSI de siete capas.

Figura 1.1 Modelo de referencia OSI.

Algunas de las funciones de cada capa o nivel se describen a continuación:

Nivel de Aplicación. Se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las cuáles gestionan:

- Transferencia de archivos FTP.
- Intercambio de mensajes (Email).

Nivel de Presentación. En esta capa se realizan las siguientes funciones:

- Se da formato a la información para visualizarla o imprimirla.
- Se interpretan los códigos que estén en los datos (conversión de código).
- Se gestiona el cifrado de datos.
- Se realiza la compresión de datos.

Nivel de Sesión. Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos. Algunas de las funciones que realiza son las siguientes:

- Establecimiento de la conexión de sesión.
- Intercambio de datos.
- Liberación de la conexión de sesión.
- Sincronización de la sesión.
- Administración de la sesión.

Nivel de Transporte. Esta capa asegura que se reciban todos los datos en orden adecuado. Realiza un control de transmisor a receptor. Algunas de las funciones que realiza son:

- Acepta los datos del Nivel de Sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al Nivel de Red.
- Multiplexaje.
- Regula el control de flujo de tráfico de transmisor a receptor.
- Reconoce los paquetes duplicados.

Nivel de Red. En esta capa se determina el establecimiento de la ruta de transmisión. Algunas de sus principales características son:

- Verifica las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.
- Realiza control de tráfico de datos.

Nivel de Enlace de Datos. Este nivel es responsable de la transferencia fiable de cada paquete al Nivel de Red. Algunas de sus funciones son:

- Detección y control de errores mediante el empleo del *CRC (Ciclyc Redundancy Test: Prueba Cíclica de Redundancia).*
- Control de secuencia.
- Control de flujo de datos.
- Control de enlace lógico.
- Control de acceso al medio.
- Sincronización del frame.

Nivel Físico. Este nivel engloba los medios mecánicos, eléctricos, funcionales y de procedimiento para acceder al medio físico. Es el encargado de la activación y desactivación física de la conexión. Otras de sus funciones son:

- Define las características físicas (componentes y conectores mecánicos).
- Define las características eléctricas (niveles de tensión).
- Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Solamente reconoce bits individuales, no reconoce caracteres, ni frames multi-carácter. Por ejemplo *RS-232* y *RS-449.*

1.7. Familia de estándares *IEEE 802.xx*

La *IEEE 802.xx* es una serie de estándares que fueron establecidos a partir de 1980, con el objetivo de llevar a cabo una conectividad entre las *NIC's (Network Interface Cards: Tarjetas de Interfaz de Red),* y el medio de transmisión. La familia *802* se divide en trece grupos, en donde a cada grupo se le tiene asignado una tarea especifica dentro de las redes. Sus principales características se mencionan a continuación:

- El estándar *IEEE 802.1* provee estándares para el manejo de red y cubre desde la Capa Física hasta la Capa de Transporte en el modelo OSI.
- El estándar *IEEE 802.2* define el *LLC (Logical Link Control: Control Lógico de Enlace)*, apoyado en el protocolo *MAC (Media Access Control: Control de Acceso al Medio)*.
- El estándar *IEEE 802.3* define una red derivada del *Ethernet* y su técnica de acceso denominada *CSMA/CD (Carrier Sense Multiple Access with Coallision Detection: Acceso Múltiple con Detección de Portadora y Detección de Colisiones)*.
- El estándar *IEEE 802.4* describe una red *Token Ring* con topología de bus.
- El estándar *IEEE 802.5* fue derivado de las redes Token Ring de *IBM*, con Topología en Anillo, utilizando un dispositivo llamado *MSAU (Multistation Access Unit: Unidad de Acceso a Estaciones Múltiples)*.
- El estándar *IEEE 802.6* describe una red MAN basada en tecnología *DQDB (Distribuited Queue Dual Bus: Canal Dual de Cola Distribuida)*.
- Los estándares *IEEE 802.7* y *802.8 son* comités creados para apoyar y supervisar los desarrollos de tecnologías existentes, que puedan migrar hacia fibra óptica o tecnologías en banda ancha.
- El estándar *IEEE 802.9* se enfoca en arquitecturas e interfaces estándares que permitan aplicaciones de escritorio con servicios integrados de voz, video y datos. Este estándar es compatible con *ISDN (Integrated Services Digital Network: Red Digital de Servicios Integrados)*.
- El estándar *IEEE 802.10* está ligado con normas de seguridad y cifrado.
- El estándar *IEEE 802.11* está diseñado para redes locales inalámbricas.
- El estándar *IEEE 802.12* se le conoce como *100VGAnyLAN*, y se basa en una Topología de Estrella y en un método de acceso de competencia, por lo que el propósito de este estándar es de manejar redes de alta velocidad que puedan operar tanto en Token Ring como Ethernet.
- El estándar *IEEE 802.14* normaliza la transmisión de datos sobre cable de líneas de TV.

1.8. Especificaciones para interfaces de red

Los adaptadores de red necesitan software capaz de controlar sus operaciones desde el Sistema Operativo de Red. De este modo, las aplicaciones tienen controlados los accesos al hardware del sistema. Este software es un controlador o *driver* de muy bajo nivel, que es específico para cada Tarjeta de Interfaz de Red dependiendo del fabricante.

Sobre este controlador pueden establecerse otros programas de más alto nivel y que tienen funciones específicas, relacionadas con los protocolos de la red en la que se va a instalar el sistema. A estos programas se les llama *packet-drivers* , ya que son los encargados de los frames que circulan por la red, además de que sobre la misma Tarjeta de Interfaz de Red puedan soportarse distintos protocolos sin interferencias entre ellos.

Hay dos tecnologías básicas para realizar el enlace entre las capas de alto nivel del modelo OSI y la Tarjeta de Interfaz de Red; una de ellas es el *NDIS (Network Driver Interface Specifications: Especificación de Interfaz del Controlador de Red)* de *Microsoft* y *3COM* y el *ODI (Open Datalink Interface: Interfaz Abierta de Enlace de Datos)* de *Novell* y *Apple*. El driver de estas aplicaciones actúa como interfaz entre los protocolos de transporte y la Tarjeta de Red.

Tanto el NDIS como ODI se configuran a través de archivos de texto especiales, *(PROTOCOL.INI)*, que indican al driver cómo utilizar los recursos de la tarjeta, así como los parámetros que definen la red local. Algunos parámetros son el *IRQ (Interrupt Request Line: Petición de Interrupción de Línea)* de la tarjeta, el canal *DMA (Direct Memory Access: Acceso Directo a Memoria)*, el tipo de frame de red que se ha de generar, datos de identificación de la red, etc.

1.9. Medios de transmisión

Como base del entendimiento de la seguridad en redes de datos, es importante conocer los medios de transmisión entre las computadoras, finalmente es por ahí por donde fluyen los datos y la información crítica de las empresas.

Dentro del concepto de los medios de trasmisión es importante diferenciar la velocidad de transmisión y el ancho de banda. La velocidad de transmisión tiene como unidad el *baud y* ésta es la velocidad de señalización igual al número de condiciones discretas o eventos en la señal por segundo. Los bauds son equivalentes a los *bits* por segundo cuando cada evento en la señal presenta exactamente un bit. El ancho de banda es la diferencia entre la frecuencia más alta y la más baja de las señales de una red, también puede describir la tasa máxima de transmisión de información en un medio de comunicación.

El medio de comunicación es el medio físico por el que viaja la información entre dos o más equipos, puede ser el espacio si se utilizan ondas de radio o luminosas, un cable si se utilizan impulsos eléctricos, fibra óptica o cualquier otro medio que sea capaz de transportar algún tipo de energía útil para enviar información. La manera en que se realiza esta comunicación es mediante una forma binaria y el ancho de banda de la transmisión se va a ver limitado por el tipo de medio empleado por la red. En el momento de seleccionar un medio para la transmisión, se deben de tomar en cuenta las siguientes características: costo, requerimiento de instalación, ancho de banda, señalización, atenuación y la inmunidad a interferencias.

En la transmisión de datos se puede utilizar el cable coaxial y suelen emplearse dos tipos: para las redes de tipo locales cables de 50 ohms *(RG58)*, para señales digitales; y cable de 75 ohms *(RG70)*, para señales analógicas y digitales de alta velocidad. El cable coaxial puede ser delgado (6 mm), llamados *thinlan* para 10BASE2, con una capacidad de soportar tramos máximos de hasta 185 metros; o

los llamados gruesos, *thicklan* para 10BASE5, que pueden llegar a cubrir tramos de hasta 500 metros. Estos dos tipos de cable pueden soportar un ancho de banda máximo de 10 Mbps.

Otro tipo de cableado utilizado en las redes es el par trenzado, debido a su bajo costo; una característica especial es que el trenzado de los cables evita la interferencia electromagnética, además reduce el ruido producido por las frecuencias de radio que intervienen con los cables y componentes electrónicos, tiene una capacidad de transmisión de 500 Mbps y puede soportar una longitud máxima de 100 m.

Estos cables son actualmente los más utilizados, ya que pueden aprovechar la misma conexión para voz y datos, integrando los llamados cableados estructurados.

Los tipos de cables de par trenzado son: *STP (Shielded Twisted Pair: Par Trenzado Blindado)* y *UTP (Unshielded Twisted Pair: Par Trenzado no Blindado)*. El UTP puede clasificarse en nivel 1, nivel 2, nivel 3, nivel 4 y nivel 5, los cuales dependerán del ancho de banda soportado y de la longitud máxima del segmento. Actualmente los más utilizados son el nivel 1 y el nivel 5.

De los cables de par trenzado comentados anteriormente, el que se utiliza en la mayor parte de las instalaciones es el UTP, debido a la flexibilidad que ofrece, lo que facilita su manejo durante la instalación. Es recomendable utilizar el STP sólo en casos en los que existan segmentos de alta interferencia, como plantas de luz, transformadores o cualquier otro dispositivo que se encuentre cerca del segmento a instalar. Los conectores más comúnmente empleados en este tipo de cableados son el *RJ 45* y el *RJ 11*.

Otro medio de transmisión no menos importante es la fibra óptica, aparece dentro de la especificación de Capa Física 10BASE-FL, éste es el medio más adecuado para transmisión de datos a grandes distancias, ya que se puede extender por kilómetros, soportando un gran ancho de banda y resulta inmune a las interferencias electromagnéticas. Aunque la fibra óptica ofrece muchos beneficios, su instalación eleva su costo, principalmente por la extrema precisión con que se tienen que hacer los empalmes o uniones de las fibras.

Las nuevas tecnologías de cables, en conjunto con el desarrollo de nuevas especificaciones para la Capa Física, han permitido definir beneficios importantes para transmitir ya sea, a través de cable coaxial, par trenzado o fibra óptica, en todas ellas a 100 Mbps. De ahí se han generado nuevas especificaciones como el 100VGAnyLAN, definido en el estándar IEEE 802.12, tanto para redes IEEE802.3 ó 802.5. Estas redes pueden utilizar UTP o STP nivel 1, 5 o fibra óptica. Otra nueva especificación es el 100BASE-X, también llamado *Fast Ethernet*, éste puede utilizar UTP o STP nivel 5 *(100BASET4 ó 100BASETX)* o fibra óptica *(100BASEFX)*.

La implementación de redes inalámbricas, en la actualidad, se está incrementando rápidamente debido a los avances tecnológicos. Estos tipos de redes tienen grandes ventajas como medio de transmisión; pero desventajas en el rubro de seguridad, ya que abren la posibilidad de robo de datos o información.

Un medio de transmisión, también inalámbrico, muy utilizado principalmente en las redes WAN y MAN, son las microondas, éstas son punto a punto, a nivel terrestre o satelital. Las frecuencias de operación están en el rango de los Gigahertz (GHz) y van de 4-8 GHz a 21-23 GHz y su capacidad de ancho de banda va de 1 a 10 Mbps, las características de atenuación son determinadas por la potencia del transmisor, frecuencia y tamaño de la antena, aunque para altas frecuencias, las condiciones meteorológicas pueden afectar.

Como los sistemas de microondas son susceptibles a la interferencia atmosférica y pueden ser vulnerables a equipos electrónicos, típicamente los datos para este medio se encuentran cifrados.

1.10. Arquitecturas y topologías de red

Las arquitecturas y topologías de red son importantes factores a tomar en cuenta en la implementación de un sistema de seguridad, ya que basándose en las mismas se podrán deducir los protocolos utilizados. Los protocolos son un conjunto de reglas y convenciones que gobiernan la forma en que los dispositivos de una red intercambian información, y esta información es la que tenemos que resguardar ante su mal aprovechamiento.

Las redes integran una variedad de estándares o arquitecturas, cada una de ellas contemplan componentes tales como hardware compatible, protocolos, medios de transmisión y una topología. Una topología es un mapa de la red que indica cómo se va a cablear de un punto otro.

La definición de una topología para una red empresarial, va ligada al método de acceso que mejor se adapte a las necesidades de la empresa. Un método de acceso es un conjunto de reglas que definen el cómo los nodos comparten el medio de transmisión. Los métodos de acceso más importantes son:

- El método de Competencia o *Contention*. Éste es un método de acceso en el cual los dispositivos de la red compiten por los derechos de acceso al medio físico. Se recomienda en aquellas redes donde tienen eventos de ráfaga o *burst* tales como transferencia de datos intermitentes y para redes con pocas computadoras.
- *Polling*. Un dispositivo es el responsable de llamar o transmitir los datos de otros dispositivos. Éste integra un controlador maestro, quién se encarga de verificar si los nodos están listos para transmitir o recibir datos, este método es poco usado en redes ya que tiende a sobrecargar de tráfico la red.

- *Token Passing.* Las computadoras toman su turno para usar el medio de transmisión. Para ello utiliza un paquete llamado ficha o *token,* el cual circula alrededor de la red. Aquella computadora que reciba el token tendrá la capacidad, en forma única, de recibir o transmitir datos y una vez terminado, pasa el token a otro dispositivo.

Topologías de Red

Una topología define los arreglos entre nodos, cableado y conectividad de diferentes dispositivos dentro de la red. Ésta contempla dos categorías: la topología física y la topología lógica. La primera define el diagrama de interconexión entre los dispositivos y la segunda, las reglas lógicas por donde se van a transmitir los datos. Tanto las topologías físicas y lógicas tienen diferentes formas de configuración. Las topologías físicas más importantes son:

- *Topología de Bus.* Las estaciones de trabajo se conectan a un medio de transmisión común consistente en una línea de cable o bus que corre de un extremo a otro de la red. Su instalación es muy sencilla, pues basta que una estación se conecte al bus para integrarse a la red, por lo que su mantenimiento es relativamente sencillo. Las estaciones de trabajo compiten por el acceso al medio, lo cual se convierte en una desventaja ya que sólo una estación puede transmitir a la vez sin que existan colisiones. Esta tecnología es utilizada principalmente en redes Ethernet.
- *Topología de Anillo.* Ésta se cablea en forma de círculo. Cada nodo es conectado a un nodo vecino y los datos van fluyendo de uno a otro. Cada dispositivo integra un receptor y un transmisor, así mismo también, un repetidor que pasa la señal de un dispositivo a otro. Dado que la señal es regenerada en cada dispositivo, la degradación de la misma es muy poca. Esta topología predomina en los métodos de acceso Token Ring, en donde el token va circulando alrededor del anillo. Por tanto, aquel dispositivo que tenga el token tendrá la posibilidad de transmitir o recibir datos en ese momento. Las topologías físicas de anillo no son muy comunes, típicamente ésta es más usada a nivel lógico, utilizando una topología física en forma de estrella.
- *Topología de Estrella.* En la Topología de Estrella, los equipos se conectan a un concentrador o *hub* central. El hub recibe las señales de los dispositivos de red y la trasmite a su destinatario. Estas topologías pueden estar configuradas en forma de árbol o inclusive pueden ser jerarquizadas.
- *Topología de Malla.* Éste es un modelo híbrido ya que puede mezclar todas las topologías físicas y lógicas comentadas anteriormente. Así, cualquier dispositivo podrá ser conectado a cualquiera de las mismas. Cuando un nuevo dispositivo es agregado, se lleva a cabo la conexión a todos los dispositivos. Por tanto el nivel de redundancia ante fallas disminuye considerablemente, pero a cambio, el nivel de intervención para administración de la misma se eleva, así como la complejidad del cableado.

Arquitecturas de red

La arquitectura de red es el diseño de interconexión de todos los dispositivos. Ésta integra al cableado, las Tarjetas de Interfaz de Red y los mecanismos por los cuales los datos son enviados de un dispositivo a otro.

El camino que siguen los datos en una arquitectura es de extrema importancia, ya que de ella depende el buen diseño de un sistema de seguridad de datos. Para nuestro caso, se analizarán las arquitecturas más conocidas en el mercado.

- *Ethernet.* Es la arquitectura, o especificación de red, más utilizada en las redes empresariales, su topología lógica es de bus, aunque su topología física puede ser en bus o estrella. Ésta última se puede configurar a través de los concentradores. Ethernet utiliza el método de acceso llamado CSMA/CD, el cual es un mecanismo de acceso a canal, en donde los dispositivos que deseen transmitir primero verifican la existencia de la portadora en el canal, si no se detecta la portadora en un cierto lapso, los dispositivos pueden transmitir, en caso de que dos de ellos transmitan a la vez, ocurre una colisión que es detectada por dispositivos especiales retardando la retransmisión durante un periodo de tiempo aleatorio.
  Es importante aclarar que la banda base o *baseband*, tiene como característica el siempre utilizar una portadora. La banda base se diferencia de la banda amplia o *broadband*, ya que ésta última integra múltiples frecuencias de portadoras.
  Estas redes pueden operar a 10 ó 100 Mbps utilizando banda base para su transmisión. Las especificaciones de la Capa Física soportadas son: *10BASE2, 10BASE5, 10BASE-T, 10BASE-FL, 100VGAnyLAN y 100BASE-X.*
- *Token Ring.* La topología física se encuentra típicamente en forma de estrella, aunque el token utiliza el anillo para pasar de estación a estación. Cada nodo debe conectarse a un concentrador llamado *MSAU (Multistation Access Unit: Unidad de Acceso a Estaciones Múltiples).* El MSAU tiene la capacidad de determinar si una de las estaciones está fuera de operación y de ahí hacer y dar un salto o *bypass* a la siguiente estación. Las Tarjetas de Interfaz de Red de Token Ring pueden ser configuradas a 4Mbps ó 16Mbps. Dentro de una red, todas las Tarjetas de Interfaz deben estar configuradas a una sola velocidad.
  El cableado usado para redes Token Ring lo definió *IBM* y es el siguiente:
  - *Tipo 1.* Éste es STP, integra dos pares de par trenzado con recubrimiento. La distancia máxima es de 100 metros.
  - *Tipo 2.* Usa un total de seis pares de par trenzado con recubrimiento STP y cuatro pares de UTP para líneas telefónicas. La máxima distancia soportada por segmentos es de 100 metros.
  - *Tipo 3.* Es una alternativa de menor costo a diferencia de los tipos anteriores. Éste utiliza par trenzado sin recubrimiento UTP y no

puede ser utilizado para la configuración de 16Mbps. La máxima distancia de cableado es de 45 metros.

- Existen otras variantes de cables poco utilizados dentro de Token Ring, algunos son: Tipo 5 para fibra óptica, Tipo 6 llamado *Data Pach Cable*, el Tipo 8 llamado *Carpet Grade* y el Tipo 9 llamado *Plenum Grade*.

Red de Interfaz de Datos Distribuida por Fibra

La *FDDI (Fiber Distributed Data Interface: Red de Interfaz de Datos Distribuida por Fibra)*, es una MAN que sigue un estándar *ANSI*, pero que fue creada pensando en la compatibilidad con la norma IEEE 802. Sus características generales son:

- Está orientada hacia redes de área metropolitana, cuya cobertura es de 100 km aproximadamente, los entornos para los que se diseñó son:
    - Red *backend*: Concepto tradicional de red, con varias estaciones conectadas a un mismo medio.
    - Red *backbone*. Red cuya función principal es interconectar otras redes.
- Velocidad: 100 Mbps.
- Topología física: anillo.
- Topología lógica: de anillo.
- Medio físico: fibra óptica.
- Alta fiabilidad: se produce en promedio un error cada $2.5X10^{10}$ bits y, además, hay posibilidad de que la red se reconfigure y siga funcionando en caso de que se rompa una fibra.
- Soporta del orden de 500 nodos, aunque no todos transmitiendo al mismo tiempo.

Topología FDDI

En FDDI la topología física es de doble anillo, así en caso de que fallase un tramo de fibra óptica de uno de los anillos, se podría seguir transmitiendo por el otro. Incluso si se rompiesen los dos tramos de fibra entre dos estaciones, el anillo se reestablecería formando un sólo anillo con las dos fibras, como se ve en la figura 1.2.

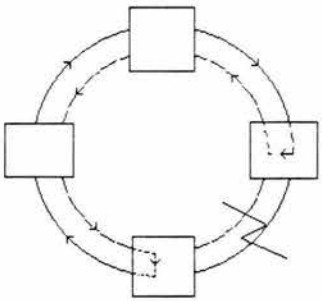


Figura 1.2 Topología física de FDDI.

Aparte de las estaciones, otro tipo de elementos en FDDI son los concentradores, a los cuales se conectan varias estaciones mediante cable coaxial de buena calidad y con longitudes inferiores a 100 metros. Los concentradores también pueden tener una única conexión de fibra *SAC (Single Attachment Concentrator: Concentrador de un Solo Enlace)*, o doble *DAC (Dual Attachment Concentrator: Concentrador de Enlace Dual)*.

Modo de Transferencia Asíncrona

El *ATM (Asynchronous Transfer Mode: Modo de Transferencia Asíncrona)* puede ser considerado como una tecnología de conmutación de paquetes de alta velocidad, que cuenta con las siguientes características:

- Los paquetes son de pequeño y constante tamaño (53 bytes).
- Es una tecnología de naturaleza conmutada y orientada a la conexión.
- Los nodos que componen la red no tienen mecanismos para el control de errores o control de flujo.
- El encabezado o *header* de las células tiene una funcionalidad limitada.

Simplificando al máximo, podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos son capaces de encaminar la información empaquetada en células a través de unos caminos llamados *conexiones de canales virtuales*.

Frame Relay

Frame Relay, considerado como un estándar industrial, comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25. Sus especificaciones fueron definidas por el Instituto Nacional Americano de Estándares, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada "salto" de la red.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

Las redes Frame Relay se construyen partiendo de un equipo de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8250 bytes, aunque por defecto es de 1600 bytes.
También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

En Frame Relay, los dispositivos del usuario se interrelacionan con la red de comunicaciones, haciendo que sean aquellos mismos los responsables del control de flujo y de errores. La red sólo se encarga de la transmisión y conmutación de los datos, así como de indicar cual es el estado de sus recursos. En el caso de errores o de saturación de los nodos de la red, los equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas, y si es preciso, reducirán la velocidad de transmisión para evitar la congestión.

La clave para que Frame Relay fuera aceptado rápidamente, es su gran facilidad como tecnología, para ser incorporado a equipos ya existentes: ruteadores, conmutadores, multiplexores, etc., y que éstos pueden, con Frame Relay, realizar sus funciones de un modo más eficiente.

Por ello, Frame Relay es una solución ampliamente aceptada, especialmente para evitar la necesidad de construir mallas de redes entre ruteadores, y en su lugar multiplexando muchas conexiones a lugares remotos a través de un solo enlace de acceso a la red Frame Relay.

1.11. Tarjetas de red

Las Tarjetas de Interfaz de Red (NIC), se instalan en una de las ranuras o *slots* de la PC. Los datos dentro de una computadora fluyen en forma paralela, la tarjeta debe cambiar la señal a una forma serial hacia el medio de transmisión. Una vez que fluye por el canal de transmisión, esta señal serial deberá volverse a transformar en una señal paralela, para ser introducida a la PC.

Para la configuración de las Tarjetas de Interfaz de Red es importante tener claros los siguientes conceptos, los cuales pudieran tener algunas variantes dependiendo del Sistema Operativo de Red:

- *IRQ*. La Petición de Interrupción de Línea se encargará de reservar una línea de interrupción para la Tarjeta de Interfaz de Red con el fin de que se comunique con la Unidad de Procesamiento Central.
- *Dirección de Puerto Base* o *I/O*. Este parámetro define las direcciones de memoria de donde vienen y van los datos hacia la Tarjeta de Interfaz de Red. Esta dirección de memoria simula un puerto y define el canal entre la Tarjeta de Interfaz de Red y el procesador.
- *Dirección de Memoria Base*. En ésta se reserva una pila de memoria o *buffer* que usa la computadora para la Tarjeta de Interfaz de Red.

- *DMA (Direct Memory Access:Acceso Directo de Memoria)*. Ésta es una memoria de acceso a la Tarjeta de Interfaz de Red.
- *PROM (Programmable Read Only Memory: Memoria Programable de Sólo Lectura)*. Éste es un circuito integrado que permite que la Tarjeta de Interfaz de Red arranque y se realice la conexión a la red; en la memoria de este circuito se aloja el software de arranque de red. La PROM de arranque es utilizada frecuentemente en aquellas computadoras que no cuentan con disco duro, para alojar el software de arranque y reconocimiento de red.
- *La Dirección MAC*. La dirección de Control de Acceso al Medio es grabada en la Tarjeta de Interfaz de Red y es la que define la dirección de los nodos dentro de una red. Estas direcciones son hexadecimales y son únicas para cada Tarjeta de Interfaz de Red. La IEEE es la responsable de asignar estas direcciones a cada fabricante de Tarjetas de Interfaz de Red. La MAC se ubica en la Capa de Enlace del modelo de referencia OSI.
- *Velocidad de Anillo*. Esta característica sólo aplica en las Tarjetas de Interfaz de Red Token Ring, y puede ser de 4Mbps ó 16Mbps.

La configuración de la Tarjeta de Red va a depender del Sistema Operativo a utilizar, y en algunos casos, como *Windows 95*, esto se puede llevar a cabo de forma automática. Para el caso de *Windows NT* esta configuración se puede llevar a cabo a través de la aplicación del Panel de Control.

1.12. Dispositivos de conectividad y mecanismos de transporte

Entre los dispositivos de conectividad más importantes se encuentran los siguientes:

- *Modems*. La palabra viene de Modulador-Demodulador. Este dispositivo convierte señales digitales a una forma adecuada para la transmisión sobre medios de comunicación analógicos y viceversa. Estos pueden ser asíncronos o síncronos. En el primero se utiliza un bit para sincronizar los dispositivos en cada frame que será transmitido dentro de la red, para el segundo se utiliza un mecanismo de reloj para mantener sincronizada la transferencia y recepción de datos.
- *Repetidor*. Éste es un dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red, permitiendo extender físicamente distancias

entre equipos. Los repetidores operan en la Capa Física del modelo de referencia OSI y no requieren de una asignación de dirección, ya que sólo repite bits de datos.

- *Hubs*. Estos son el punto central de conexión de cableado, pueden ser clasificados como activos o pasivos. Los hubs pasivos no contienen componentes electrónicos, por tanto no procesan la señal de datos, el único objetivo de este tipo de dispositivos es el combinar señales de diferentes segmentos de red. Los hubs activos incorporan componentes electrónicos que amplifican y limpian la señal electrónica que fluye a través de él y de la red, este proceso de limpieza de señal es llamado regeneración, lo que hace que la red sea menos sensible a errores, además de incrementar la distancia entre dispositivos.
- *Los switches*. Son hubs activos con mejoras tales como el soporte a protocolos de administración y monitoreo en forma remota de los mismos, lo que permite el desactivar o activar puertos de conexión que estén generando errores. Los switches integran circuitos para el ruteo a alta velocidad de datos entre el hub y la computadora; algunos dispositivos de este tipo tienen la posibilidad de elegir la mejor ruta para que el frame llegue más rápido. Actualmente los switches están reemplazando a dispositivos como los puentes y ruteadores.
- *Puentes o bridges*. Estos dispositivos se encargan de extender al máximo tamaño una red. Opera en la Capa de Enlace de Datos del modelo de referencia OSI. La diferencia contra un repetidor es que el bridge puede ser selectivo en cuanto al tipo de información que puede pasar por él o hacia una red diferente. Esta selección que pudiera llamarse también filtrado, la hace sobre la base de las direcciones físicas de los dispositivos, por tanto, el frame es transmitido sólo al lugar que tiene que enviarse. Los bridges permiten dividir redes muy cargadas de tráfico de datos logrando segmentos más pequeños, no pueden integrar LAN's con diferente dirección, porque dependen de las direcciones físicas de los dispositivos y no de una Capa de Red en donde residen las direcciones lógicas de la misma.

  Ruteadores o routers. Este dispositivo se utiliza para direccionar información de una red a otra mediante direcciones lógicas. El router funciona en la Capa de Red del modelo de referencia OSI. Dado que los routers pueden determinar las rutas más eficaces, éstos son empleados para conectar redes LAN a una WAN.
- *Gateways*. A este elemento también se le conoce como convertidor de protocolo y se emplea como interfaz de protocolos de redes diferentes. Se utiliza en una gran variedad de aplicaciones donde las computadoras de diferentes manufacturas y tecnologías deben comunicarse. La información que pasa a través del Gateway es información "punto a punto", que viene de las aplicaciones, de las interfaces y de los programas del usuario final.

1.13. Protocolo de transporte

Muchos de los protocolos existentes han sido diseñados tomando al modelo OSI como referencia, más esto no significa que todos ellos sigan esta estructura de capas, muchos de ellos tienen sus orígenes antes de que el modelo OSI se creara.

Los protocolos describen la forma en que los datos de la red son encapsulados en frames desde la fuente de datos y enviados a un destino, el cual se encarga de reconstruir los mismos, ya sea en el archivo, petición o instrucción necesaria. Entre más pequeños sean los paquetes, estos pueden fluir más ágilmente de un punto a otro, además de reducir el porcentaje de errores en el mismo; en un momento dado si un frame pequeño contiene errores la retransmisión sólo implica el reenvío del paquete dañado.

Los frames se encuentran estructurados y seccionados de la siguiente forma:

- *El header.* Indica el inicio de paquete y contiene información de las direcciones de la fuente y del destino, además de información de tiempo y sincronización.
- *Datos.* Esta sección define los datos originales a transmitir.
- *Elemento de Cola o Trailer.* Esta parte marca el fin del paquete y tipicamente integra información de la Prueba Cíclica de Redundancia.

Cada capa de protocolo desempeña su propia función, tal como formar una interfaz con una aplicación, convertir el formato de datos necesario o el adicionar ya sea direcciones o parámetros de verificación de errores. El mismo protocolo está compuesto por un subconjunto de protocolos llamado pila de protocolos o *protocol stack,* que integra capas de software de protocolo relacionadas, que juntas funcionan para realizar una arquitectura específica de comunicaciones.

Cuando un frame llega al medio de trasmisión, las Tarjetas de Interfaz de Red de otras computadoras en la red del mismo segmento lo examinan, verificando la dirección del mismo; si la dirección destino coincide con alguna de ellas, la Tarjeta de Interfaz de Red realiza una interrupción en el procesador y las capas de protocolo de la computadora destino procesan el frame de entrada.

Muchos de los servicios de verificación de dirección, verificación de errores y retransmisión asociados a la red, se llevan a cabo en las Capas de Red y Transporte del modelo de referencia OSI. Los nombres de los protocolos normalmente integran un protocol stack de la dos Capas comentadas anteriormente. Un ejemplo es el protocolo TCP/IP, TCP es el protocolo de la Capa de Transporte e IP es el protocolo de la Capa de Red; *IPX/SPX (Internet Packet Exchange/Standard Protocol Exchange: Intercambio de Paquetes Internet/Protocolo de Interacambio Estandar)* es otro protocol stack que integra en

su denominación la Capa de Transporte y la de Red, respectivamente para *Novell Netware*.

La Capa de Enlace de Datos y la Física del modelo de referencia OSI están basadas en fundamentos puramente de hardware, en donde se integran las direcciones de los dispositivos, el método de acceso y el medio de transmisión. Los protocolos de las Capas de Transporte y de Red tales como TCP/IP e IPX/SPX se apoyan en la Capa Física y de Enlace de Datos, y con el apoyo de los estándares NDIS y ODI, diferentes bloques de protocolos pueden operar a través de una sola Tarjeta de Interfaz de Red.

Los protocolos de capas superiores van muchos más orientados a servicios tales como programas de ruteo, esquemas de direccionamiento y servicios de archivo e impresión.

1.13.1. Protocolo TCP/IP

El protocolo TCP/IP fue desarrollado por el Departamento de Defensa de los Estados Unidos de América, para proveer un servicio robusto en grandes redes internas con diferentes tipos de equipo conectados. Actualmente es el protocolo más utilizado para redes en Internet, y esto ha sido debido a que es un protocolo abierto del cual ningún fabricante es propietario.

TCP/IP fue desarrollado para ser independiente al hardware, y ha sido integrado en la mayoría de las tecnologías de las Capas Física y de Enlace de Datos del modelo de referencia OSI. A continuación se observa en la Figura 1.3. el diagrama del protocol stack de TCP/IP.

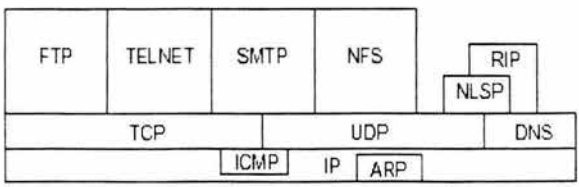


Figura 1.3 El protocol stack de Internet o TCP/IP.

Los siguientes son los servicios TCP/IP más utilizados actualmente:

- *DNS (Domain Name System: Nombre del Dominio del Sistema).* Este protocolo provee el servicio de resolución de nombre y dirección IP para las aplicaciones de la empresa. Los nombres pueden ser hasta de 260 caracteres.
- *FTP (File Transfer Protocol: Protocolo de Transferencia de Archivo).* Es el protocolo para compartir archivos entre nodos conectados a la red.

- *SMTP (Simple Mail Transfer Protocol: Protocolo de Transferencia de Correo Simple).* Éste es un protocolo de ruteo de correo electrónico dentro de redes internas. SMTP utiliza a los protocolos TCP e IP.

- *TELNET (Remote Terminal Emulation: Emulación de Terminal Remota).* Es un protocolo de emulación de terminal. Permite a computadoras y estaciones de trabajo el operar como una terminal tonta.
- *NFS (Network File System: Sistema de Archivo de Red).* Éste fue desarrollado por *Sun Microsystems* y es un protocolo que permite el acceso a archivos, los cuales necesitan ser accesados más ágilmente que un FTP o TELNET. Dado que éste se convirtió en un servicio abierto, en la actualidad ha tenido una gran popularidad.
- *ARP (Address Resolution Protocol: Protocolo de Resolución de Dirección).* Este protocolo va a permitir la ubicación de una dirección IP mediante la Capa de Enlace y la Capa Física del modelo de referencia OSI, ya que son tablas de contenido de direcciones IP *locales*.
- *ICMP (Internet Control Message Protocol: Protocolo de Control de Mensaje de Internet).* Este protocolo tiene la función de detectar errores que se originen en el envío de un mensaje y comunicárselo al IP.
- *RIP (Routing Information Protoco: Protocolo de Información de Ruta).* Proporciona la información que un frame sigue en su camino.
- *UDP (User Datagram Protocol: Protocolo de Datos de Usuario).* Es utilizado para la transmisión de datos en forma moderada.

Como se observa en la figura 1.4. TCP/IP integra cuatro capas y cada una de ellas corresponde a una o más capas del modelo de referencia OSI.

Figura 1.4 Comparación del Modelo OSI y TCP/IP.

- *Capa de Acceso a Red o Network Access.* Ésta cubre las dos capas inferiores del modelo OSI y esta correspondencia permitió al Departamento de Defensa de los Estados Unidos de Norteamérica el poder coexistir con los estándares de las capas existentes de Enlace de Datos y Capa Física del modelo de referencia OSI.

- *La Capa de Internet.* Se equipara a la Capa de Red del modelo OSI, aquí se realiza el movimiento de datos entre los dispositivos de la red.

- *La Capa de Equipo a Equipo o Host a Host.* Puede ser comparada con la Capa de Transporte. Los protocolos en esta capa permiten llevar a cabo conexiones directas entre equipos centrales y la red interna. Cabe comentar que la denominación de host dentro de TCP/IP puede referir a cualquier tipo de dispositivo dentro de una red, el concepto Cliente/Servidor no existe en este modelo.
- *La Capa de Proceso/Aplicación o Process/Application.* Cubre la funciones de la Capas de Sesión, Presentación y Aplicación del Modelo de referencia OSI. Los protocolos en esta capa proveen fundamentalmente servicios.

Uno de los grandes beneficios del protocolo TCP/IP es su denominación como el protocolo utilizado para Internet, por lo cual éste puede operar como un backbone. Una de sus desventajas es que el tamaño de los bloques en serie del protocolo lo hace difícil de implementar, principalmente en equipos viejos u obsoletos. TCP/IP ha sido clasificado algunas veces como un protocolo lento en su transmisión, esto principalmente debido al análisis que se lleva acabo en la Capa de Red.

Características de los Protocolos de Transporte TCP/IP

Igual que con cualquier otro protocolo, el esquema de direccionamiento de IP es fundamental en el proceso de ruteo de la información a través de la red. Cada dirección IP tiene componentes específicos y un formato básico.

A cada host en una red TCP/IP se le asigna una dirección lógica única de 32 bits, que se subdivide en dos partes principales: el número de red y el número de host. El número de red identifica a una red, el número de host identifica a un host en la red.

La dirección IP es una dirección de 32 bits, consta de cuatro octetos separados por un punto y representados en formato decimal (conocido como *notación decimal de puntos*). Cada bit en el octeto tiene un peso binario. El valor mínimo de un octeto en decimal es 0, y el valor máximo en un octeto es 255, algunos ejemplos son:

28.200.78.69
2.6.38.123

Las direcciones IP pueden ser clasificadas en cinco diferentes clases A, B, C, D y E. Solamente las clases A, B y C están disponibles para su uso comercial.

En la clase "A", el primer octeto partiendo de la izquierda debe caer en un número entre 1 y 127, antes del primer punto. Por lo tanto una dirección 76.32.123.150 representaría un número de nodo 32.123.150 en la red 76.

Las direcciones clase "B" y "C" se definen de forma similar a la clase "A". Para el caso de la clase "B", el primer grupo de decimales de la izquierda cae en un rango de entre 128 y 191, en este caso los primeros dos grupos de tres decimales partiendo de la izquierda son los que definen la dirección de red, y los últimos dos octetos definen la dirección del nodo. Para el caso de la direcciones tipo "C", el primer grupo de decimales puede caer en los rangos de entre 192 y 223, los primeros tres grupos de decimales, partiendo de la izquierda definen la dirección de red.

Para las clases "D" y "E", el primer grupo de decimales puede caer en rangos mayores a 223, estas direcciones actualmente no se encuentran disponibles ya que se están reservadas para otros propósitos. La tabla 1.1. muestra ejemplos de cada clase.

Cada dispositivo dentro de una red, ya sea una impresora, un router o una computadora requiere de una dirección IP única, no puede haber dos direcciones IP iguales dentro de la misma red.

Clases y Direcciones			
Clase	**Dirección IP**	**Dirección de Red**	**Dirección de Host**
Clase A	105.34.8.120	105	34.8.120
Clase B	140.109.23.45	140.109	23.45
Clase C	190.78.34.77	190.78.34	77

Tabla 1.1. Ejemplos de Clases y Direcciones IP.

Características del Protocolo de Internet

TCP/IP provee servicios de frames IP. IP es un protocolo de switcheo de frames, que permite seleccionar y direccionar el ruteo del mismo. Un header IP se añade en cada paquete integrando una dirección, la cual es comprendida por los protocolos de niveles más bajos. IP rutea estos frames a través de las redes internas, utilizando tablas de ruteo integradas en cada paso por un ruteador. Las elecciones de ruteo se realizan basándose en la información de dispositivos de direcciones lógicas y físicas, esto es provisto por él o por el ARP.

IP ensambla y desensambla los frames según está establecido en las Capas de Enlace y Física del modelo de referencia OSI. También contempla la verificación de errores en los datos del header, a través del método de suma de control o *checksum*, que corresponde a un número entero calculado a partir de secuencias de grupos decimales y por medio de una serie de operaciones aritméticas, el valor se recalcula en el lado receptor y es comparado para su verificación.

Características del Protocolo de Control de Transmisión

TCP permite la transmisión confiable de datos en un ambiente IP, además corresponde a la Capa de Transporte del modelo de referencia OSI. Entre los servicios que ofrece TCP están: la transferencia de datos en burst, confiabilidad, control de flujo eficiente, operación full-duplex y multiplexaje.

Con el servicio de transferencia de datos en burst, el protocolo entrega una ráfaga no estructurada de bytes identificada por una secuencia de números. Este servicio beneficia a las aplicaciones, ya que éstas no tienen que fragmentar los datos en bloques antes de entregarlos a TCP. TCP agrupa los bytes en segmentos y los pasa al protocolo IP para su entrega.

El protocolo TCP ofrece confiabilidad de extremo a extremo, orientada a la conexión a través de una interred. El mecanismo de confiabilidad de TCP permite que los dispositivos puedan lidiar con frames mal leídos, duplicados, retrasados o perdidos. Un mecanismo de expiración de tiempo permite a los dispositivos detectar frames perdidos y solicitar su retransmisión.

El protocolo TCP ofrece un control de flujo eficiente, lo cual significa que cuando se envían confirmaciones de regreso al origen, el proceso TCP de recepción indica el número de secuencia más grande que puede recibir sin saturar sus dispositivos de almacenamiento internos.

La operación full-duplex significa que los procesos de TCP se pueden enviar y recibir al mismo tiempo.

El multiplexaje de TCP significa que es posible multiplexar varias conversaciones de las capas superiores de manera simultánea a través de una sola conexión.

En el desarrollo de este primer capítulo se han presentado los conceptos básicos de redes, que van a permitir comprender de una manera clara la importancia del manejo de los datos dentro de una empresa y la seguridad que se debe tener para toda red, en donde, se pueda accesar y controlar el manejo de la información con el fin evitar pérdidas para la empresa y sus clientes. En el siguiente capítulo se analizará la importancia de la seguridad en redes, así como, la existencia de soluciones que permitan implementar dicha seguridad.

CAPÍTULO 2

SEGURIDAD EN REDES

En este capítulo haremos un bosquejo teórico en lo referente a la seguridad en redes de cómputo, comenzando por conceptos generales, en lo que se refiere a la clasificación de diversos tipos de amenazas, pasando por las mejores prácticas para llegar a un sistema de seguridad a un nivel altamente cualitativo y finalizar con los conceptos de soluciones de seguridad puntuales e interoperatividad de las mismas.

2.1. Seguridad y administración de seguridad en redes *Microsoft*

El tema de seguridad en redes es muy amplio y alcanza grados de profundidad increíbles; en este trabajo sólo se abordarán los conceptos esenciales para comprender el sistema de seguridad de datos propuesto en una plataforma del Sistema Operativo del *Microsoft Windows NT*.

La seguridad en redes es uno de los aspectos de la administración de un sistema de cómputo que garantiza que los recursos del sistema, dentro de la red, sean empleados únicamente por usuarios autorizados, asegurando la disponibilidad, privacidad e integridad de los recursos de la red.

Al hablar de seguridad se mencionarán dos nuevos conceptos: seguridad implícita y seguridad explícita. La primera se refiere a la seguridad que se obtiene manipulando el Sistema Operativo, tanto el de la estación de trabajo como el del servidor o el de red en general. El segundo se referirá a la seguridad obtenida con elementos explícitamente diseñados para proteger el sistema y no por Sistema Operativo, aunque deben de ser soportados por éste. Los elementos técnicos explícitos que manejaremos son esencialmente cinco: Antivirus, Firewalls, Sistemas de Detección de Intrusos, Sistemas de Inspección de Contenido y Sistemas de detección de vulnerabilidades y riesgos.

El propósito de la seguridad de redes será proteger los recursos de la empresa. Esto nos lleva invariablemente a que primero debemos de definir explícitamente los requerimientos de la empresa, para así poder definir los tipos de seguridad que ésta necesita, recordando que cualquier sistema en red afecta a otros sistemas homólogos, y que las responsabilidades de un sistema de seguridad muchas veces se deben de extender fuera del entorno de la Internet, hasta abarcar si es

necesario otras empresas. Debemos así definir nuestra política de seguridad para el sistema de red, que abarque el factor costo, de una manera responsable, advirtiendo que una red comprometida o insegura puede afectar otras redes conectadas a ella, revisando periódicamente nuestras políticas de seguridad implementadas, para garantizar que sus objetivos fundamentales sean los correctos en cada tiempo.

La seguridad de un sistema de red puede medirse cualitativamente de acuerdo a los siguientes puntos:

- El grado en que un recurso está disponible en red cuando se necesite.
- La calidad de certeza en que los recursos sean accesibles sólo por las personas autorizadas y de acuerdo a los privilegios que los mismos usuarios tengan dentro del sistema.
- Que los recursos no puedan ser destruidos, corrompidos o robados dentro y fuera de la red.

Las fallas que un sistema de red puedan llegar a tener, sean intencionales o involuntarias, se llaman amenazas a la seguridad del sistema. Por ende para determinar la seguridad de una red hay que conocer todas las posibles amenazas que ésta pueda llegar a sufrir, implementando las medidas necesarias para evitarlas lo mejor que sea posible.

Una clasificación simple de las posibles amenazas a una red sería el siguiente:

- *Interna/externa.* Una amenaza interna es la producida por un malfuncionamiento del hardware o software del sistema de red en sí. Una amenaza externa es derivada por un agente externo a la red.
- *Intencional/accidental.* Una amenaza que puede ser sometida a un proceso judicial de responsabilidad legal por daños y perjuicios es intencional (el daño inflingido por descuido de algún empleado se puede llegar a evaluar como daño por negligencia); accidental, es en los casos en que la amenaza no pueda ser inculpada a alguna persona.
- *Activa/pasiva.* Es activa cuando alguien penetra el sistema de seguridad de la red y su principal objetivo es dañar. Pasiva si el ataque no lleva la intención de dañar (aunque puede resultar un efecto colateral de este ataque).
- *Por hardware.* Son ataques a medios físicos del sistema de red, que pueden ser naturales y provocados: los primeros son generalmente atribuidos al envejecimiento propio de los equipos interconectados a la red. Los provocados varían desde el robo de una parte del equipo de la red hasta el uso no autorizado de algún dispositivo.
- *De software.* Amenazas a los programas de aplicación y de sistema de la red.

- *De información.* Amenazas a los datos de la empresa, sea intencional o accidental.
- *A la funcionalidad de la red.* Pueden ser amenazas a las actividades ordinarias de la red, como por ejemplo, a la administración o al monitoreo de la red.

Para evitar este tipo de amenazas es necesario contar con un sistema de seguridad, con la capacidad de proteger y asegurar a la red, además de disminuir los efectos de las amenazas sobre el sistema si éstas ya se presentaron.

En forma más específica los objetivos de un sistema de seguridad consisten en:

- Prevenir daño malintencionado a la red y sus recursos.
- Prevenir el uso malintencionado del hardware o software de la red.
- Prevenir el robo de los componentes de la red.
- Limitar el daño o destrucción de software o hardware tanto por descuido como por accidente.
- Proteger la privacidad de los datos del sistema.
- Prevenir el acceso a la red y el uso no autorizado de sus recursos.

Teóricamente una red se considera segura si reúne los siguientes requisitos:

- Está disponible siempre que un usuario autorizado lo necesite.
- Sus recursos pueden ser modificados sólo por usuarios autorizados.
- El contenido de información de la red puede ser leído sólo por usuarios autorizados.

Las medidas de seguridad a emplearse en un sistema de red pueden ser:

- Asegurar físicamente el hardware contra robo, accidentes o daños naturales.
- Asegurar lógicamente el hardware mediante, por ejemplo, circuitos integrados de cifrado en Tarjetas de Red.
- Emplear dispositivos de control de potencia como por ejemplo, una *UPS (Uninterruptible Power Supply: Fuente de Poder Ininterrumpida).*
- Usar sistemas de servidores con tolerancia a las fallas.
- Aplicar sistemas de cableado y Tarjetas de Red redundantes.
- Administrar un sistema de respaldo de información.
- Implementar sistemas de redundancia de información y datos como el uso de *RAID (Redundant Array of Inexpensive Disks: Serie Redundante de Discos de Bajo Costo).*
- No instalar sistemas de copiado de CD's en las estaciones de trabajo.
- Emplear sistemas de módem con llamada de regreso o *callbacks modems* para usuarios fuera del sistema de la red local.
- Inspección automática de áreas del disco antes de escribir en él.

- Monitoreo de todas las actividades de sesión del usuario.
- Control de acceso a archivos.
- Control de privilegios de escritura de archivos para los usuarios del sistema.
- Uso adecuado de contraseñas de acceso al sistema.
- Cifrado de transmisiones.
- Empleo de códigos de autentificación de mensajes y firmas digitales.
- Reporte de actividades de intrusiones al sistema.

Todas estas medidas de seguridad están basadas en la regla de costo/eficiencia, en donde se toman en cuenta las características particulares de la empresa. Es elemental el saber que entre más medidas se implementen el costo será mayor. Se debe llegar a un punto de equilibrio entre las medidas a tomar y el costo de éstas, sobre los beneficios reales que la empresa obtenga.

Existen cuatro niveles de seguridad reconocidos que un sistema de red puede llegar a tener, dependiendo de la naturaleza misma de éste. Esta clasificación es tomada del llamado libro naranja: "*Trusted Computer System Evaluation Criteria*", una publicación gubernamental de los Estados Unidos de Norteamérica. La clasificación es la siguiente: clase D, clase C, clase B y clase A.

- Los sistemas de seguridad *clase D (seguridad mínima)*. No pueden considerarse seguros, ya que el Sistema Operativo que gobierna los equipos no dispone de medidas para asegurar el sistema. Tal es el caso del MS DOS.
- Los sistemas de seguridad *clase C (protección a discreción)*. Se pueden subdividir en dos: C1 y C2, los primeros son sistemas de red como *UNIX*, que contienen elementos de seguridad consistentes en contraseñas de acceso, permisos de uso de archivos, prevención de destrucción de programas del sistema y restricción del uso de recursos. Los C2 además registran todas las operaciones de los usuarios, restringiendo sus privilegios dentro de la red.
- Los *clase B (protección obligatoria)*. Ejecutan rastreos de amenazas y protección contra fallas. Son considerablemente mucho más seguros que cualquiera de sus predecesores, sólo superados por la clase A.
- Los *clase A (protección verificada)*. Emplean algoritmos matemáticos complejos que garantizan en todo instante el óptimo funcionamiento de la red, apegados a la política de seguridad de éste.

De lo anterior se desprende que para instalar un sistema de seguridad en una empresa, es necesario primero conocer las necesidades de la misma para, con base en ello, se pueda escoger un sistema que lo respalde.

Para asegurar un sistema de red es necesario controlar los elementos del mismo. Existen tres tipos de control que podemos ejercer sobre un sistema de red: el control administrativo, el operativo y el control técnico.

- *El control administrativo.* Es un conjunto de técnicas empleadas en la gestión del sistema red.
- *El operativo.* Son controles ejecutados por el personal a cargo de administrar el sistema de red.
- *El control técnico.* Es el efectuado por el mismo sistema de cómputo programado para tal efecto.

En el rubro del control administrativo del sistema de red sobresalen dos aspectos fundamentales:

- *Protección de datos.*
- *Reducción del tiempo fuera de servicio.*

Para la protección de datos del sistema, podemos hacer dos cosas: un respaldo de los datos y conectar un sistema de respaldo de energía.

Los respaldos en el rubro administrativo del sistema, se efectúan mediante comandos del Sistema Operativo de Red, enviando los datos a respaldarse a unidades *DAT (Digital Audio Tape: Cinta de Audio Digital)* diseñadas para tal fin, y son cintas magnéticas de alta capacidad y bajo costo por Gigabyte de información.

Existen varios tipos de respaldos que se pueden hacer: completos, incrementales, diferenciales y de copia diaria. Éstos ya dentro de un ambiente de trabajo del Sistema Operativo de Red de *Windows*.

En un respaldo completo se copian todos los archivos de datos del sistema (y algunos programas críticos) a los módulos DAT. En el respaldo incremental se copian sólo los archivos que han cambiando desde el último respaldo. Los diferenciales permitirán respaldar sólo algunos tipos de archivos a conveniencia del sistema. Por último, los de copia diaria son aquellos que automáticamente respaldan la información hayan estado o no en uso.

Un sistema de protección de datos mediante respaldos debe estar dentro de un plan de respaldo de datos de sistema. Pudiendo hacerse, por ejemplo, un respaldo diario de tipo incremental o uno diferencial y semanalmente uno completo.

La instalación de UPS, es una de las características típicas de la administración de un sistema, para proteger los datos del mismo contra fallas del suministro eléctrico. Consiste en un banco de potencia (tipo batería) o un pequeño generador de voltaje, que permite que el sistema siga funcionando aún después de que el suministro de energía ha fallado, permitiendo así, salir del sistema correctamente sin perder datos, como ocurriría en caso de una interrupción súbita, además de evitar una falla del propio sistema al apagarlo intempestivamente. Se pueden agregar estas UPS a los ruteadores de la red para, permitir el apagado lento del sistema, además de que hay unidades UPS con software que avisa cuando una

eventualidad ha surgido para cerrar voluntariamente nuestra sesión de red sin perder datos.

Para reducir el tiempo de fuera de servicio de un sistema de red, se han generado varias medidas de acción:

Las que sobresalen en el ámbito de administración de red, son las referidas a la misma unidad de disco duro, estas medidas se han llamado de tolerancia a las fallas o *fault-tolerant* y se basan en la redundancia de recursos de información, es decir, se copian los datos doble vez al mismo tiempo, y para lograr esto, se han diseñado las llamadas unidades RAID. En estas unidades de disco, son copiados los datos en uso por el sistema, mediante la tarjeta controladora de disco en diferentes niveles de RAID y proporcionando cada nivel mayor seguridad.

Existen seis niveles de configuración de RAID, desde el nivel 0 al nivel 5. El nivel 0 no proporciona ningún tipo de tolerancia a fallas. El nivel 1 proporciona un poco de tolerancia a fallas, ya que éste utiliza dos discos para el respaldo de la información. En el nivel 2 la información es escrita en diferentes *drives*, entrelazando la información. El total de la información es escrita en drives especiales o *drives Checksum*, que se utilizan como una estrategia basada en la evaluación de los bytes transmitidos en paquetes para la detección de errores, por lo que este nivel es muy lento e inestable. El nivel 3 se asemeja al nivel 2, sólo que éste utiliza un bit de paridad y drives de paridad, en lugar de drives Checksum, resultando más estable que el nivel 2. El nivel 4 es semejante al nivel 3, sólo que un bloque entero (sector) se escribe a cada disco duro en todo momento. El nivel 5 es el nivel más rápido y fiable de los niveles antes mencionados, siendo también el más utilizado, ya que es donde trabaja el Sistema Operativo de Red de *Windows NT Server*. Básicamente consiste en un sistema redundante donde los bits de los datos en uso se van escribiendo alternados en tercias de discos de RAID. De forma que sí se escriben por ejemplo ocho bits de un dato en el primer disco, y otros ocho bits en un segundo, en el tercero se escribirá la suma binaria de los dos discos anteriores. Después los bits del siguiente dato se escriben en el disco segundo y los del siguiente dato en el disco tercero quedando el disco primero la suma binaria de estos dos, siguiendo este ciclo alternadamente. En una falla de alguno de los tres discos se podrá recuperar la información completa con la información contenida en los otros dos. Esta configuración de RAID admite hasta 32 discos a la vez.

Dentro de los sistemas de reducción del tiempo fuera de servicio de la red, se han implementado dos más, que vale la pena considerar aquí: el Servidor Espejo y el Súper Servidor. El primero consiste en dos máquinas tipo servidor, independiente entre sí, pero que ambas contienen una réplica del contenido de las dos; de forma tal, que si un equipo falla, el "espejo" lo suplirá inmediatamente, de manera automática mediante un software especial que detecta cualquier contingencia en el equipo.

El Súper Servidor es un equipo especialmente diseñado para que ante cualquier falla de algún componente del equipo, éste pueda ser substituido inmediatamente sin necesidad de interrumpir el servicio.

2.1.1. Modelos generales de administración de redes

Existen cuatro modelos de seguridad normalmente utilizados para la conexión de una red de computadoras. Éstos son:

Grupos de Trabajo

Este modelo administrativo está diseñado para operar sistemas como *Windows 95, Windows para Workgroups* y *Windows NT.*

En un Modelo de Grupos de Trabajo o *Workgroups*, no hay ninguna base de datos centralizada o servidor que guarde la información en una cuenta de usuario, debido a que este tipo de modelo de seguridad se encuentra en una red de tipo punto a punto y además hay una o más máquinas que tienen recursos para compartir.

Un Grupo de Trabajo es simplemente un nombre que se le da a un grupo de computadoras para fines de organización.

Bindery-Based

En este modelo existe un servidor y varios clientes. El servidor tiene una base de datos con cuentas de usuarios en orden alfabético para poder controlar el acceso al sistema, pudiendo también asignar derechos o privilegios de los recursos que la red dispone. Estos derechos o se asignan en una base tipo *user-by-user* o una base del tipo *group-by-group*.

El servidor también es responsable de contener todos los servicios en la red y las máquinas-cliente no se diseñan para proporcionar servicio alguno, lo que permite una dirección más centralizada de la red.

Una máquina-cliente sólo se conectará a un servidor central, el cuál autentificará a la máquina-cliente contra la base de datos de cuenta de usuario. El usuario proporcionará un nombre válido que existe dentro de la base de datos de cuenta de usuario *o login name* y una contraseña o *password* asociada. Si el nombre y la contraseña existen dentro de la base de datos de cuenta de usuario del servidor, al usuario se le concede permiso para usar la red.

En este modelo se tiene el beneficio de centralizar la base de datos para realizar todas las tareas de dirección. Un problema del Modelo Bindery-Based se presenta cuando se tienen muchos servidores en la red, ya que este modelo no permite compartir sus listas de la base de datos de cuenta de usuarios entre los servidores, y debido a esta limitación, un administrador necesitaría hacer la tarea

repetitiva de dar de alta al nuevo usuario en la base de datos de la cuenta de usuarios para mantener la seguridad de la red.

Modelo de Dominio

El Modelo de Dominio o *Domain Model,* es un modelo de seguridad tipo Cliente/Servidor, que se usa en *Windows NT Server y OS/2 networks.* Es similar a Bindery-Based en su administración centralizada de cuentas de usuario, pero con la diferencia de que la base de datos se guarda en una o más computadoras conocidas como Controladores de Dominio o *Domain Controllers.* Este modelo está diseñado para redes más grandes.

Cuando un servidor de *Windows NT* se instala, se debe de configurar uno de los tres parámetros siguientes para el servidor:

- El *PDC (Primary Domain Controller: Controlador de Dominio Primario).*
- El *BDC (Backup Domain Controller: Controlador de Dominio de Respaldo).*
- Servidor Miembro *o Member Server.*

PDC y BDC realizan esencialmente la misma función, guardan la base de datos de las cuentas de usuarios, la diferencia es que el PDC guarda la copia maestra de la base de datos, mientras que el BDC es la copia del PDC. Se pueden agregar cuantas BDC se requieran.

El papel del Member Server es contener los recursos como archivos, impresoras y aplicaciones a las que los usuarios quieran acceder de la red. Por sí mismo, el Member Server no guarda una base de datos de dominio de usuario, pero en cambio da el acceso a los recursos basado en la lista de cuentas de usuarios de los directores del dominio. Los servidores del Member Server no procesan el login del cliente, esta función sólo es realizada por los directores del dominio.

Algunas desventajas que presenta el Modelo de Dominio son que debe de existir una utilería separada para realizar funciones administrativas diferentes, es decir, hay una utilería para crear a los usuarios y otra para manejar las impresoras, o si se instalara un servidor del facsímil, habría una nueva utililería para manejar este servidor del facsímil. Otro problema importante con este modelo, es que no se diseño para soportar no más de 40,000 cuentas. En una cuenta queda registrado el grupo y el dominio al que corresponde la máquina, así, en algunas redes más grandes es necesario crear dominios múltiples.

Modelo de Servicios de Directorio

El Modelo de Servicios de Directorio o *Directory Services,* también conocido como la norma de X.500, es utilizado actualmente por *Banyan Vines, Novell NetWare 4.x* y *higher* y *Windows NT 5.*

Directory Services es un poderoso sistema de seguridad para la red, puede adecuarse desde redes pequeñas hasta redes sumamente grandes, además de que resuelve muchas de las limitaciones vistas en los modelos anteriores.

Directory Services está basado en un modelo de base de datos jerárquicos distribuidos. Este modelo permite la dirección de todos los recursos a través de una utilería, proporcionando también un alto nivel de tolerancia a fallas dentro del sistema. En este modelo no se guardan los archivos en un directorio dentro de su propia unidad de disco duro, sino que se agrupan los archivos en los directorios de tal forma que se ponen archivos que se relacionan entre sí, para lograr una fácil referencia. Esto mismo se aplica para el servicio de cuenta de la base de datos.

En lugar de los directorios, se guardan juntos a todos los usuarios de un trabajo o que acceden a los mismos recursos. De hecho, muchos Directory Services organizan la base de datos de manera similar a mapas orgánicos corporativos.

La dirección de recursos no se limita a los usuarios y grupos dentro de una base de datos de servicios de directorio. Otros recursos en la red también tienen los objetos dentro de la base de datos. Así, cuando una impresora se instala, su objeto también se instalará en la base de datos; la dirección de esta impresora puede, de igual forma, hacerse en la base de datos de servicios de directorio. Esta funcionalidad permite a los administradores usar una utilería para la mayoría de sus direcciones de la red.

El tercer beneficio principal de este modelo es que se puede fraccionar la base de datos en servidores diferentes. Esto significa que si un usuario se agrega en Paris, el servidor de México, no deberá ser actualizado. En un Modelo del Dominio, todas las cuentas del usuario se deben de copiar a todos los BDCs, siempre que una cuenta del usuario se agregue.

En general este modelo es la norma hacia la que todos los Sistemas Operativos están emigrando.

2.1.2. Manejo de cuentas de grupos y usuarios

El manejo de cuentas de grupos y usuarios es muy importante para la seguridad de la red. Algunas compañías podrían creer que sus documentos cotidianos no requieren de seguridad, pero no consideran sus archivos de nómina u otros datos que son fundamentales para ésta. *Windows NT*, como un modelo administrativo, presenta una manera práctica de manejar esta información, por medio de cuentas de grupos y usuarios.

Cuentas de los usuarios

En la mayoría de los casos, una cuenta de usuario se crea para cada individuo en la red y sólo es para uso de una persona. Esto se hace a través de la utilería "Gerente de Usuario para los Dominios". Esta cuenta de usuario generalmente es

un formulario extraído del nombre de la persona y sin que estas cuentas se repitan.

En su nivel más básico, una cuenta de usuario normalmente contiene las tres siguientes propiedades:

- Un nombre de usuario o *username*. Este elemento distingue una cuenta de otra.
- Una contraseña. Este elemento confirma la identidad del usuario. Deben guardarse las contraseñas individuales de manera privada para evitar accesos desautorizados. Esta propiedad puede ser optativa, dependiendo de las restricciones de seguridad.
- Los grupos en los cuáles el usuario es un miembro. Estos grupos determinan los derechos del usuario y permisos en la red. Ésta es una propiedad optativa.

Existen otras propiedades optativas, como un directorio de casa o *home directory* (es el lugar dónde un usuario puede guardar los archivos personales en la red) o disponer de información específica sobre el usuario, como su nombre completo y descripción. Ninguna de estas propiedades es crucial para el funcionamiento de la cuenta.

En la creación de las cuentas de los usuarios y sus contraseñas, se debe tener un equilibrio entre la seguridad y facilidad de recordar la contraseña para el usuario. Las contraseñas deben de tener fechas de expiración, y tienen que ser fáciles de recordar para el propio usuario.

Cuentas de grupos

Después de que el usuario ha sido establecido, el próximo paso consiste en asignar los permisos apropiados, y debe hacerse creando un grupo o un juego de grupos, asignando los permisos a los grupos, y poniendo entonces al usuario dentro de él o los grupos apropiados.

Como ya se menciona anteriormente, una red *Windows* puede incluir dos tipos de recursos de grupos específicos: Global y Local, teniendo cada uno de estos grupos funciones muy específicas.

- En el *Grupo Global*. Sólo se pueden crear Grupos Globales, como las cuentas del usuario, en el Controlador del Dominio Primario en el dominio de *Microsoft*. Estos grupos funcionan principalmente como recipientes para las cuentas del usuario. Se diseñan los Grupos Globales para contener agrupaciones generales de usuarios, como por ejemplo ventas, contabilidad o recursos humanos.

- El *Grupo Local*. Puede crear grupos locales, tanto en *Windows NT Server* como en la Estación de Trabajo o *Workstation*, pudiéndose incluir en ambos cuentas de usuarios y Grupos Globales, así como asignar permisos a estos grupos. La premisa detrás de los Grupos Locales es que un administrador puede crear un Grupo Local para un uso específico.

Los permisos

Los permisos se refieren específicamente al nivel de confianza que el dueño de un recurso tiene en las personas con las que él comparte el recurso. Por defecto, *Windows NT* y *Windows 95* comparten los recursos con el mando total, por lo que no sólo se pueden ver los recursos del usuario, sino que también se pueden añadir, modificar, e incluso anular. Un buen compromiso es conceder permisos de sólo lectura, que permiten a otros ver sus archivos o imprimir una copia, pero no modificar ni eliminar.

Los derechos

Los derechos son atributos generales que tienen usuarios particulares o grupos. Estos derechos incluyen la capacidad de registrar de forma local o de cargar y descargar controladores de dispositivos. Los derechos se refieren al nivel de mando de un usuario en particular o grupos que tienen por encima de un recurso específico.

2.1.3. Implementación de seguridad por Sistema Operativo

Como se mencionó oportunamente al comienzo del presente trabajo, se escogió como Sistema Operativo a *Windows*, por ser éste el del cliente donde se instalará un Antivirus (AV), uno o más Firewalls, un *IDS (Intrusión Detection System: Sistema de Detección de Intrusos)*, Sistemas de Inspección de Contenido y un Sistema de detección de vulnerabilidades y riesgos. Por ende, durante todo el trabajo cuando se refiera al Sistema Operativo de Red hablaremos de *Windows*, salvo que se especifique lo contrario.

La seguridad implícita o por Sistema Operativo de Red (NOS) es un tópico de vital importancia para el administrador de la red. Nosotros no pretendemos modificar las funciones administrativas de dicho personal, ya que nuestro trabajo será una implementación explícita con los componentes de seguridad ya mencionados, sin embargo resultará muy útil conocer como se lleva a cabo la seguridad dentro del Sistema Operativo de Red.

La base de la seguridad por Sistema Operativo de Red es la creación y la asignación de permisos, para poder usar los recursos de la red; estos recursos varían desde servicios, como por ejemplo impresión, hasta datos que pueden estar agrupados por carpetas y archivos.

Partiendo de los modelos generales de administración de redes, y del manejo de cuentas de grupos y usuarios mediante el uso del NOS, podemos conocer como es posible implementar la seguridad en éste.

Al crear y asignar permisos a una carpeta compartida en el NOS (en este caso *Windows NT*), podemos crear un directorio con un nombre cualquiera y asignarle el permiso de que se pueda compartir, y esto es una asignación de un permiso, en este caso, sobre un directorio dentro del disco que contiene el NOS. Al compartir un directorio estamos dando permisos de lectura (*read*), además de que también podemos especificar otros permisos sobre de este directorio al compartirlo.

En realidad, al otorgar un permiso lo estamos haciendo a un grupo ya sea local o general dentro del sistema. Este grupo puede tener variados niveles de control sobre el directorio compartido. Al especificar un directorio a compartir, también los subdirectorios y los archivos dentro de éste estarán compartidos.

Cuando se asignan los permisos para compartir carpetas, directorios, subdirectorios o archivos dentro del Sistema Operativo de Red debemos de especificar si lo estamos haciendo dentro de una partición de disco tipo *FAT (File Allocation Table: Cuadro de Asignación de Archivo)*, que es la más común en un Sistema Operativo básico como *Windows 95 ó 98 (W9x)*, o en una partición del tipo *NTFS (Native File System: Sistema de Archivo Nativo para Windows NT)* que es la más empleada en servidores de red con NOS.

Con el sistema de FAT la seguridad no puede ser completa, ya que muchos permisos y derechos a usuarios no se pueden restringir. En cambio con la partición NTFS es posible realizar restricciones de permisos y derechos a usuarios para uso de archivos y directorios, aún localmente NTFS ofrece mayor seguridad.

También podemos agregar que al asignar los recursos de la red para ser compartidos, en nivel de compartir, se trabaja con el Modelo de Dominio del NOS, pero a nivel local es posible trabajar con el Modelo de Grupos de Trabajo o con un Sistema Operativo, por ejemplo W9x. Esto puede reducir costos sobre licencias.

En este último caso, si se decide emplear un Sistema Operativo, como *W9x*, para trabajar con un equipo designado como servidor, la implementación de seguridad puede ser de dos tipos: *nivel compartir y nivel usuario*.

El *nivel compartir* para un Sistema Operativo es soportado por el Modelo de Grupos de Trabajo y también cuando el equipo es parte del dominio del NOS. Bajo esta premisa la seguridad es mediante asignación de contraseñas para cada directorio o impresora del sistema. Existen tres asignaciones de contraseñas posibles:

- Sólo lectura o *Read Only*. En esta asignación se puede entrar a directorios, subdirectorios y archivos sin poderlos borrar, mover o escribir.

- Acceso total o *Full Access*. En donde con una sola contraseña se puede acceder a todos los recursos del sistema.
- Depende de la contraseña o *Depends on Password*. Donde hay una contraseña para acceso de lectura y otra para acceso total.

A *nivel usuario*, con el Sistema Operativo Local se tiene mayor seguridad, ya que admite una identificación de usuario con su correspondiente autentificación, además de la contraseña necesaria para acceder a los recursos del sistema. Para lograr esto, es necesario tomar prestada una base de datos de usuarios del NOS (por ejemplo *Windows NT*). Así, el equipo con el Sistema Operativo requerirá los datos para la autentificación del usuario que quiere entrar del sistema a un servidor externo de red.

En este mismo nivel de usuario, es posible compartir directorios y la seguridad se trabaja asignándole privilegios a los usuarios o grupos a acceder al sistema. Los privilegios pueden ser de tres tipos:

- Sólo lectura. Donde no se podrán borrar o copiar los directorios o los archivos dentro de estos.
- Acceso Total. Donde el usuario podrá realizar cualquier operación de gestión de archivo o directorio en el sistema.
- A la Medida o *Custom*. Que es una combinación de privilegios más específicos, como son:

    - Lectura de archivos.
    - Escritura a archivos.
    - Creación de archivos.
    - Desplegado de archivos.
    - Borrado de archivos.
    - Cambio de atributos de archivo.
    - Cambio de permisos.

En este nivel de usuario, por la forma de trabajo con Sistema Operativo, se puede compartir una impresora; en este caso hay necesidad de habilitar un modo especial para el sistema llamado "modo de cliente" y un servicio llamado "compartir archivos e impresora"

2.1.4. Monitoreo de la red

Dentro de una operación de red ocurren eventos relevantes, normalmente invisibles al usuario así como al administrador. Pero cuando ocurre una falla, son estos eventos los que nos pueden ayudar a determinar cual es el problema, para así solucionarlo.

Monitoreo de eventos

Un evento es un incidente que tiene algún interés potencial, de hecho, muchos eventos tienen muy poco interés. El visor de eventos supervisa tres categorías de eventos, los cuáles se almacenan en sus respectivos registros:

Eventos de sistema. Son generados por el Sistema Operativo de Red y son almacenados en el registro de sistema. Los eventos que están almacenados en el registro de sistema se dividen en tres categorías:

- *Errores.* Los errores son eventos de sistema que representan una posible pérdida de datos o de la funcionalidad de la red, lo que puede ser un fallo de una unidad o de un componente del sistema encargado de la carga durante el inicio.
- *Alertas.* Son menos serias que los errores, las alertas son eventos menores que se deben tener en cuenta ya que pueden indicar fallas a futuro. Las alertas se pueden generar como resultado de eventos, como la proximidad de un disco lleno, por dar un ejemplo.
- *Información.* Ésta engloba a los registros "Información", "Seguridad con éxito" y "Seguridad fallida". Se pueden incluir eventos como la sincronización entre controladores o la carga satisfactoria de un programa de base de datos.

Eventos de aplicación. Generados por las aplicaciones y almacenados en el registro de aplicación. Los eventos de aplicación representan un número bastante menor que el de los otros eventos almacenados. Las aplicaciones los registran en el sistema y son muy variados.

Eventos de seguridad (eventos de auditoría). Generados por el NOS y almacenados en el registro de seguridad cuando la actividad seleccionada aparece o falla. Los eventos de seguridad y el registro de seguridad son el punto de mayor interés para el administrador. Las opciones de los eventos de seguridad que se van a registrar, se configuran en el administrador de usuarios para dominios. Se pueden realizar auditorías de eventos correctos y erróneos en todas las categorías, por lo que en determinado tiempo podemos tener un registro de sistema de exageradas dimensiones.

Se pueden utilizar filtros para seleccionar eventos de acuerdo a los siguientes campos.

- Ver desde y ver hasta. Utilizados para reducir los eventos por fecha.
- Tipos. Utilizados para seleccionar el tipo de eventos que se pretende ver.
- Origen. Utilizado para escoger los eventos que se registrarán en un determinado origen, como, por ejemplo, una unidad.
- Usuario. Utilizado para ver todos los eventos que ocurren mientras un usuario en particular inicia una sesión.

- identificador. Utilizado para ver eventos dentro de una categoría, con una identidad en particular.

2.1.5. Tareas de auditoría

Un servicio de auditoría rastrea las operaciones sobre los objetos. El sistema acumula información sobre como se usan los objetos, almacena información en archivos de registro y permite visualizar eventos para identificar fallos en la seguridad. Si se descubriera un fallo en la seguridad, el registro puede ayudar a determinar la extensión del daño para que pueda ser recuperado el sistema y también puede ser bloqueado para evitar intrusiones futuras.

El sistema puede decir cual es la cuenta que está en operación, pero no puede decir quien es la persona que está utilizando dicha cuenta.

El registro de seguridad del Visor de eventos puede mostrar una lista de eventos por categorías y por identificador de evento:

- Administración de Usuarios y Grupos o *Account Management*. Estos eventos describen los cambios de alto nivel en la base de datos de cuentas de usuarios, como son la creación de usuarios o cambios en la pertenencia de un grupo.
- Seguimiento de Procesos o *Detailed Tracking*. Estos procesos proporcionan información detallada del seguimiento de un sujeto, como puede ser la activación de un programa, la duplicación manual y el acceso indirecto a objetos.
- Inicio y Cierre de Sesión o *Logon/Logoff*. Estos eventos describen un intento de Inicio o Cierre de Sesión, y si ha tenido éxito o no.
- Acceso a Archivos y Objetos u *Object Access*. Estos eventos describen ambos accesos con o sin éxito a objetos protegidos.
- Cambio en el Plan de Seguridad o *Policy Change*. Estos eventos describen cambios de alto nivel en la base de datos en el plan de seguridad, como lo es la asignación de privilegios.
- Cambio en el Uso de Privilegios o *Privilege Use*. Estos eventos describen ambos intentos fallidos o no de utilización de privilegios.
- Eventos del Sistema o *System Event*. Estos eventos indican que ha ocurrido algo que afecta a la seguridad del sistema entero o del registro de auditoría.

El sistema de auditoría puede también ser utilizado para detectar virus. Puede visualizar intentos no esperados para acceder a archivos ejecutables *(.EXE)* y a bibliotecas de programas *(.DDL)*, o intentos de modificar estos archivos o crear nuevos archivos ejecutables.

2.1.6. Recuperación de datos del sistema

Dentro de todo plan de seguridad se debe de tomar en cuenta la recuperación de datos en caso de una intrusión, ya que hay información que es muy importante para toda empresa y de la cuál depende.

Se tienen que identificar las aplicaciones y los servicios más críticos en la organización, y de igual forma se tienen que identificar los sistemas de hardware que requieren estas aplicaciones y cualquier dependencia con otros sistemas.

Es importante que toda empresa, de acuerdo a sus posibilidades económicas, cuente con equipos de copias de seguridad, que pueden estar conformados hasta por equipos que ha venido desechando, lo que le puede permitir en un momento dado actuar con rapidez en caso de que una emergencia sea suscitada.

Las copias de seguridad son las herramientas de recuperación más importantes, por lo que se deben de comprobar constantemente que los procedimientos para restaurarlas sean los adecuados. Los servidores duplicados, como ya se mencionó, pueden proteger frente a desastres locales por copiar información en tiempo real a servidores en otras localizaciones. También se debe considerar la creación de conexiones múltiples entre localizaciones para protegerse de los fallos entre los enlaces. Idealmente estos enlaces deben de estar interconectados, por lo que deben seguir distintas rutas para comunicarse con los proveedores de distintos servicios.

Dentro de un plan de emergencia para la recuperación de datos, es importante que se tenga una respuesta inmediata cuando se descubre un problema; además de contar con la gente necesaria para reconstruir los sistemas, reintroducir la información crítica que haya sido pérdida o administrar la restauración de la información sensible.

2.2. Recursos externos de seguridad en redes

Dentro de los requerimientos primarios para la creación de una red donde la seguridad sea prioridad, sin llegar a entorpecer la acción de compartir recursos entre usuarios, es la creación de normas y directrices que conlleven al conveniente uso de los recursos, al igual que la interacción de diversos sistemas que protejan a la red y sus recursos de ataques externos e internos.

2.2.1. Definición de política de seguridad de red

El documento que describe las características de seguridad de la red, dentro de una organización específica, se llama la política de seguridad de la red. Este documento deberá de detallar, de una manera muy completa, todas las características del sistema de seguridad a implementar, abarcando principalmente los siguientes puntos:

- Identificación de los recursos que hay que proteger.
- Identificación de las amenazas a los recursos a proteger.
- Como deberá de ser usada la red.
- Responsabilidades de cada uno de los usuarios de la red.
- Acciones a tomar en caso de que la política de seguridad sea violada.
- Procedimientos de administración, configuración y recuperación de la red.

Una definición adecuada de la política de seguridad, conllevará la consulta de varios expertos, dentro y fuera de la organización donde se planea implementar el sistema de seguridad de la red, para que dicha política pueda ser efectiva y salvaguarde los recursos del sistema.

La política de seguridad de la red es un instrumento de trabajo indispensable en el mantenimiento del sistema de seguridad en su totalidad; es como un mapa de referencia que nos permitirá saber con precisión como está funcionando la seguridad de la red, así como, facilitarnos la toma de decisión para tomar las acciones correctivas en caso de ser víctimas de un ataque.

Para asegurar que la política de seguridad de la red sea adecuada a la empresa, es indispensable realizar juntas de trabajo con los miembros experimentados de dicha empresa, esto es para conocer sus necesidades reales de uso del sistema y definir con claridad:

- Qué recursos deben tener una protección máxima.
- Protección contra las amenazas en la red.
- Contra quién queremos proteger estos recursos.
- La importancia relativa del recurso en sí.
- Las medidas a implementar para proteger estos recursos de una manera económica.
- Un plan para revisar la misma política periódicamente y observar si los objetivos y circunstancias de la red siguen vigentes.

La definición de la política de seguridad de la red deberá de especificar lo más precisamente posible todos estos factores de una manera clara y veraz.

A continuación, a manera de ejemplo, en la tabla 2.1. presentamos algunos aspectos que nos ayudarán a comprender mejor como se lleva acabo, en un principio, la definición de la política de seguridad de la red.

Esta tabla nos indica, en la primera columna, recursos de la red y como podrían especificarse para ser protegidos. Mediante un inventario podemos asignarle un número a cada recurso, un nombre y ponderar la importancia que tiene dicho recurso para los usuarios de la red con respecto a su importancia dentro del sistema de red. La segunda columna nos indica el tipo de usuario contra quien podemos proteger el recurso: Interno, externo, huésped o un grupo de usuario dentro de la red. La tercera columna nos pide que asignemos un número (0-100%)

que indique la probabilidad de que el recurso sea amenazado. En la última columna se especificarán las medidas que se hallan seleccionado para garantizar la seguridad del recurso.

En este ejemplo se muestra un solo recurso, un disco duro *F423*, de acuerdo al inventario de la empresa. Pero en una gran organización, esta tabla puede ser una verdadera hoja electrónica, con una enorme cantidad de renglones clasificados según el tipo de recurso de que se trate, hardware, software, datos, documentación, discos y cintas de respaldo, entre otros.

Recursos de la red			Tipos de usuarios contra quien proteger los recursos	Probabilidad de amenaza	Mediadas a implementar para proteger el recurso
Número	Nombre	Importancia del recurso			
F423	Disco duro	90%	Grupo de usuarios de contabilidad	40%	Permisos por NOS para archivo y directorio. Alarmas de accesos.

Tabla 2.1. Tabla auxiliar para implementar la política de seguridad de red.

El punto fino a recordar en la definición de la política de seguridad de red de la empresa, es que debe de indicarnos la medida más económica posible contra el costo de recuperar un recurso afectado por una amenaza. Al elaborar la política debemos siempre tener en mente que no podemos implementar una medida cuyo costo supere al valor del mismo recurso.

Asimismo, para llevar acabo una definición de la política de seguridad de la red, es fundamental conocer la importancia de los riesgos, en función de la pérdida del recurso y su importancia dentro del sistema.

Este análisis de riesgo es fundamental para definir la política de seguridad de la red, y debe de extenderse a cada recurso dentro de la red, con los criterios de ponderación elegidos adecuadamente por los analistas expertos.

La política de seguridad de la red de la empresa, deberá de especificar también las responsabilidades de cada usuario del sistema, debidamente jerarquizadas de acuerdo al tipo de grupo de usuario que se trate, ante cualquier contingencia de la red. Especificará quien accesará a los recursos, el uso adecuado para el recurso con respecto al usuario que lo va a usar. Detallará los distintos tipos de abusos que un usuario puede incurrir en el uso de un recurso del sistema, quién podrá obtener acceso a otros recursos dentro de la operación de la red, quién en

determinado momento tendrá los privilegios de la administración del sistema. Así mismo, definirá en detalle el manejo de las contraseñas para los diferentes usuarios de la red, los derechos y responsabilidades de cada grupo de usuarios, cómo se dispondrá de la información de vital importancia o información sensible dentro de la empresa y las sanciones por cada falta cometida dentro del rubro de la responsabilidad de los usuarios, de acuerdo a la política de seguridad.

En este último aspecto hay que considerar que las sanciones por violar la política de seguridad de la red, siendo éstas debidamente clarificadas, publicadas, explicadas, entendidas y aceptadas, deben de ser aplicadas invariablemente de acuerdo a la misma política sirviendo de base para un continuo perfeccionamiento de la misma.

En este sentido, la mayoría de las empresas recurren a la estrategia de "proteger y proceder"; esto es, proteger la red y reestablecer el servicio bloqueando al intruso, sin pretender "atraparlo". Hay, sin embargo, empresas cuya información es muy sensible y que por ende eligen la estrategia de "perseguir y consignar", permitiendo al intruso continuar hasta reunir suficiente evidencia para atraparlo y remitirlo a un proceso jurídico. Estas empresas cuentan, lógicamente, con todo un aparato judicial bien consolidado y mecanismos de protección de la información que, sin embargo, permitan al intruso continuar sin que éste perciba que ha sido descubierto. La política de seguridad de la red deberá declarar en cada caso las acciones legales a tomar.

Por último, la política de seguridad de la red desplegará quien se encargará de la interpretación de la misma, o qué comités dentro de la empresa son los encargados de administrar lo concerniente a la política de seguridad; quiénes son los encargados de publicarla y enseñarla dentro de la empresa, detallando los itinerarios para las juntas y seminarios de trabajo en torno al aprendizaje de la política de seguridad de la red.

2.2.2. Tipos de ataques

Existen varios tipos de ataques a la red, pero el más común es la usurpación de privilegios del administrador. Un punto muy importante que debe enfatizarse sobre los ataques en la red, es que el punto de origen del ataque no siempre estará fuera del Firewall. El riesgo de un ataque interior, dónde el empleado carga un código ejecutable directamente de un disco flexible en el sistema, es tan real como la amenaza de un usuario que entra por la Internet. Sin tener en cuenta donde el ataque se origina, el primer paso es encontrar una vulnerabilidad que conceda el acceso y control al usuario desautorizado.

La lista de opciones disponibles para un usuario malicioso es considerable:

- IP falso.
- Ataques al servicio File Transfer Protocol.

- Ataques de frames fragmentados.
- Uso de Email.
- Uso del DNS.
- Ataques a passwords.
- Ataques al servidor Proxy.
- Ataques al Servicio de Acceso Remoto.
- Carga de programas específicos.
- Exploración de puertos.
- Manipulación de la secuencia del TCP/IP.
- Ataques al Web Server.
- Control del ActiveX.

Todos éstos son puntos potenciales de vulnerabilidad, pero ciertamente el mejor ejemplo de un problema conocido es el desbordamiento del buffer. Éste, junto con algunos otros puntos mayores, merece la pena ser mencionados.

- *Desbordamiento del Buffer o Buffer Overflow*. Los medios clásicos en los que un usuario desautorizado puede engañar a un dispositivo es desbordando el buffer, y puede ocurrir cuando un programador descuida los parámetros específicos sobre la cantidad de datos que pueden pasar en un campo de entrada. De tal manera que si un usuario llena un campo hasta saturarlo de datos causará el desbordamiento de la memoria local, forzando la aplicación, al punto dónde dicho usuario pudiera asumir el mando.
- *Mala Protección de Contraseñas*. Otro punto vulnerable es cuando el usuario desautorizado verifica si el administrador de la red aplica una política de control de contraseña. En *Windows NT* las contraseñas son bien conocidas ya que vienen predefinidas y son fáciles de usar; si éstas quedan inalteradas, entonces el usuario desautorizado no necesita usar algo más que una conexión de Internet para tomar el mando.
- *Malware*. El software malévolo, o malware, es un término genérico usado para describir "herramientas de hacker", que son colecciones de programas que pueden ser usados para explorar una red, determinar sus puntos de vulnerabilidad e incluso descubrir contraseñas. El malware incluye los kernelkits los cuales pueden usarse para alterar el Sistema Operativo de Red. Otros ejemplos son los olfateadores o *sniffers*, diseñados para observar e identificar la actividad de la red, e informar sus resultados al usuario desautorizado.
- *Spyware*. Es un software por medio del cual se vigilan las actividades en Internet y envía un informe, generalmente al creador del mismo, cada vez que se abre el navegador. Por ejemplo, el *Aureate Spy*, se instala en los archivos DLLs de los equipos *Windows*. Este archivo crea una ventana oculta cada vez que se abre el navegador y envía 4 paginas de información a los servidores de *Aureate* usando el puerto 1749 del sistema, estas páginas incluyen el nombre (según como conste en el registro del sistema), la dirección IP, las DNS de la dirección; les dice qué proveedor de servicios de Internet es usado, el área del país donde se encuentra, y también un

listado de todo el software instalado que se muestra en el registro de *Windows*. El administrador no tiene ninguna manera de saber de que esta acción está pasando a menos que cada máquina se verifique y se supervise.

- *Los virus*. Puede usarse un virus para obtener el control de redes, aunque su uso no se restringe sólo a este propósito. El uso de un virus puede formar parte de un frente de ataque para implantar malware, que se usará después para lograr el control completo de la red; alternativamente, estos se podrían usar para consumir los recursos disponibles, podrían cambiar o corregir archivos, y generalmente suelen ser una molestia para los usuarios.
  Los puntos de infección van desde el *boot-sector* hasta *file-types*, a través de macros, correo y redes habilitadas. Los más conocidos tipos de virus que hay en la actualidad son los Troyanos y gusanos; estos tienen la habilidad para reproducirse en redes vulnerables (que no cuentan con la vigilancia del usuario).
- *Ataques al administrador*. Dado que la principal prioridad de un hacker es obtener el más alto grado de privilegios del administrador, resulta en que la tarea del personal de seguridad de red es prevenirlo a toda costa, o, asegurar que la actividad del intruso pueda ser descubierta y que ésta pueda ser eliminada en un corto plazo de tiempo.
- *Negación de servicios (DoS, Denial of service)*. Éste es el más común de los ataques a redes. En su forma más simple, ocurre cuando una demanda legítima para el servicio no puede responderse por la red, ya que sus recursos disponibles están siendo consumidos por demandas desautorizadas. Este tipo de ataque puede usarse contra un blanco que el usuario no autorizado ha previsto, sólo basta con que éste reúna un numeroso grupo de sistemas, a los que se les llama *'zombies'*. Como se muestra en la Figura 2.1, estos *zombies* (Z) son máquinas infectadas que responden a comandos u órdenes hacia direcciones especificas como una simple demanda de servicio. Normalmente estas demandas se manejarán por una o más máquinas maestras, mientras que la unidad de control opera con una IP falsa para disfrazar el ataque. Cuando una máquina requiere un servicio, la respuesta al recurso es mínima, pero cuando esta demanda llega al mismo tiempo por decenas de máquinas, el tráfico generado puede 'tirar' al sistema.
  Es muy fácil lanzar un ataque DoS una vez armado y organizado un grupo de host, redes o máquinas individuales. Existen miles de ataques DoS mensuales. Se tienen como ejemplo al ya famoso *Yahoo!*, *Amazon*, y paros de *eBay* en el 2000, mientras que en 2002 hubo un ataque directo contra los 13 DNSs que habilitan la búsqueda de direcciones de Internet.
  Existen distintas variaciones de DoS, como reflejar y cifrar las señales para dificultar el poder encontrar la fuente del ataque, y para minimizar la oportunidad que un administrador encuentre que su o sus redes están arregladas. Pero las dos amenazas del DoS permanecen claras; que se

puede ser la víctima de un ataque, o que nuestra red está participando 'tirando' el sistema de otro.

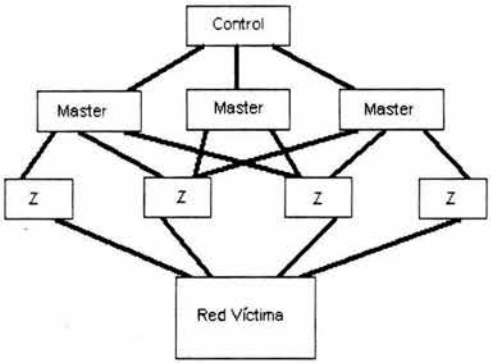


Figura 2.1. Negación de servicios provocado por varios host.

Los ataques están ahora mezclados en caracteres o cifrados, y trabajan en particular con herramientas muy flexibles capaces de asaltar al sistema en una gran variedad de formas. La red debe defenderse por consiguiente de maneras múltiples, con un mayor grupo de herramientas primarias para habilitar esta defensa y manejar los ataques virales, como el bloqueo del tráfico desautorizado dentro y fuera de la red, y monitorear la red para descubrir eventos inesperados (y por consiguiente sospechosos).

Los elementos en la defensa de la red deben consistir por consiguiente en un Anti-virus, uno o más Firewalls, un Sistema de Detección de Intrusos, Sistemas de Inspección de Contenido y un Sistema de detección de vulnerabilidades y riesgos. Cuando las acciones de estos componentes, tradicionalmente separados, se reúnen con una eficaz política de seguridad, el resultado es un ambiente capaz de bloquear ciertos ataques e identificar las amenazas antes de que el daño pueda ser grande. Esta es una meta realista y completamente factible, y es hacia donde todo administrador de red debe dirigirse.

2.2.3. Antivirus

Los virus han existido desde principios de los 80's, y anteceden a la Internet por algún tiempo. Sin embargo, esta unión (virus e Internet) se ha convertido en una amenaza global; antes de la interconectividad ofrecida por la Web, las oportunidades para los virus de extenderse estaban sumamente limitadas, y su amenaza se contuvo eficazmente en las redes individuales. Antes de extenderse la Internet a casi todos los aspectos de la vida moderna, el medio más común de

infección entre computadoras era un artículo infectado, como un disco flexible o un CD-ROM, y la amenaza era relativamente fácil de contener.

La Internet ha cambiado esto completamente. La transmisión de malware y los virus es ahora más fácil. Además, este problema aumenta por el hecho de que los usuarios mal intencionados con pocas habilidades de programación pueden adquirir herramientas automatizadas a través del Internet. La creación de virus por programadores y la disponibilidad de estas herramientas, se han convertido en un serio problema para la seguridad.

La amenaza de un ataque por un virus varía de acuerdo al uso del sistema. La facilidad con que un sistema puede ser contagiado por un virus ha obligado el uso de Antivirus (AV), convirtiéndolos en una necesidad. Estudios llevados por el *DTI (Department of Trade and Industry: Departamento de Reino Unido de Comercio e Industria*), indica que el 83% de los negocios, incluyendo el 94% de grandes negocios, emplean algún tipo de AV tanto en el escritorio como en servidores.

Tipos de virus

Un virus puede describirse como un simple código ejecutable, a menudo capaz de infectar o vincularse para unirse al código en una red y reproducirse. Aunque hay literalmente miles de variaciones de virus, pueden considerarse cinco categorías generales:

- *Virus de sector de arranque o Boot Sector.* Este tipo de virus infecta las áreas del disco dónde se localizan las órdenes de inicialización, comprometiendo la habilidad de la máquina a iniciar desde el disco duro.
- *Virus de archivo o File Virus.* Un virus de aplicación se extiende cuando un documento infectado se abre, o cuando se corren o ejecutan las aplicaciones asociadas.
- *Virus de Macro o Macro Virus.* Éste es un tipo muy común de virus, algunas estimaciones sugieren que el 75% de virus pertenecen a esta categoría. Los Virus de Macro afectan las aplicaciones de *Microsoft Office*, utilizado el mismo lenguaje de programación, modifican las características del *Office* y ejecutan programas sin el consentimiento o conocimiento del usuario.
- *Virus Múltiple o Multipartite Virus.* Estos virus infectan sectores de arranque y archivos simultáneamente, siendo muy difícil de erradicar de un sistema a menos que se limpien ambos ambientes totalmente.
- *Virus Polimórficos o Polymorphic Virus.* Este virus cambia su código al pasar de una máquina a otra, con el fin de burlar a los AV. Los filtros basados en AV, que buscan características del código, podrían ser engañados por estos cambios, pero en la práctica la mayoría de sistemas de AV avanzados (*Computer Associates, Symantec, McAfee*, y *Sophos*, como los ejemplos obvios) pueden reconocer estos cambios.

Aunque los primeros virus tendieron a encajar bastante estrechamente en estos tipos, los virus más avanzados son capaces de poseer varios, o incluso todos los atributos referidos anteriormente. Más allá de estos tipos genéricos, dos variaciones específicas de virus merecen una discusión más en profundidad: los Troyanos y los Gusanos.

- *Los Troyanos.* El caballo de Troya de la leyenda era un objeto aparentemente benigno que ocultó una carga útil peligrosa. El equivalente viral moderno trabaja exactamente de la misma manera, con la carga útil que normalmente involucra códigos ejecutables que intentan crear los privilegios del administrador. Otro nombre que reciben es *RATS (Remote Access Trojans: Troyanos de Acceso Remoto).* Estos son programas que habilitan el acceso desautorizado a la red una vez instalados en la computadora víctima.
  No todos los Troyanos pueden entregar el mando total de un sistema en las manos de un usuario remoto; la magnitud del mando robado dependerá de la habilidad y las opciones utilizadas por el creador original del Troyano. El riesgo es claro, un reto del administrador consiste en no permitir la entrega del mando a ningún usuario desautorizado.
- *Los Gusanos o Worms.* Los Worms se introducen y viajan entre las redes, se han vuelto las herramientas más sofisticadas en los últimos años, y hoy son capaces de infectar plataformas múltiples, atributos polimórficos los hacen muy difíciles de identificar, pudiendo explotar varias estrategias para impactar en la actuación de la red. Por ejemplo, el tomar listas de distribución de sistemas de Email para distribuirse.

Valoración de severidad del virus

Cada vendedor de AV categoriza la peligrosidad de un nuevo virus a su propia manera. Algunos virus son nada más que una molestia, mientras otros son capaces de derrumbar una red, desde unos cuantos minutos hasta en algunos días. Para que los administradores determinen qué necesita ser examinado urgentemente, se utilizan los siguientes atributos, para ponderar la importancia de cada virus:

- Peligrosidad del virus.
- Habilidad de reproducción.
- Daño de la carga útil.

Valoraciones continuas y un equipo de seguridad que informe de nuevos ataques, así como de ataques anteriores, debe de ser parte de la política de una red. Mantener un conocimiento y control de cambios será un punto importante para asegurar defensas más flexibles que puedan localizar amenazas más severas.

Software Antivirus

Las soluciones de AV deben adaptarse para responder a las nuevas formas de virus y sus formularios de ataque, la habilidad de poner al día los elementos que nos puedan ayudar a reparar el sistema es el centro del valor del producto.

En general, todas las soluciones de AV requieren de tres componentes principales:

- *Aplicación de escaneo.* Esta acción proporciona una interfaz entre el usuario y las opciones de configuración presentes en el sistema, que se utilizarán para identificar qué archivos serán examinados. Es necesaria la comunicación entre los usuarios y administradores para manejar esta aplicación utilizando alarmas cuando un virus sea detectado.
- *Un motor de escaneo.* Este sistema es responsable de examinar los archivos, pudiendo descubrir líneas de código y/o firmas, o si éste emplea modelos heurísticos, también puede identificar comportamientos anormales en ausencia de un código viral conocido, y lleva a cabo cualquier acción de reparación de archivo, junto con una acción de inmunización.
- *Biblioteca de Definición de Virus.* Consiste en una base de datos de firmas de virus conocidos, con instrucciones de acciones a seguir para limpiar y corregir los archivos dañados.

Se reconocen a los virus como una amenaza para los negocios de cualquier tamaño y forma. Fabricantes de seguridad y especialistas de administración están convergiendo sus esfuerzos para encontrar un producto que cubra las demandas variantes de este mercado.

Las políticas de seguridad se deben bosquejar firmemente. La actualización constante de las vacunas contra virus es necesaria, y siempre debe tomar como base la definición de la política definida para la empresa.

2.2.4. Firewalls

Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet, además de que va a permitir que el usuario pueda contar con cierta información proveniente del Internet, siempre y cuando esté permitida por el Firewall de la empresa. Cuando se trata de usuarios externos, este sistema determina quién puede ingresar para utilizar los recursos de la red pertenecientes a la empresa, lo que permite que exista un control en el manejo y acceso a la información.

El Firewall es parte de una política de seguridad integral, que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda, donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de

servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de tono de entrada *o dial-in* o *tono de salida o dial-out*, reglas para cifrar los datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

Existen tres tipos principales de Firewalls:

- *Filtrado de frames en forma estática.* Son extremadamente rápidos, ya que actúan sobre los frames de información, en función de unas reglas definidas por el administrador de red. Esto consiste en que se obtienen los frames de información provenientes de la Internet, verifica la dirección de red y conforme a la programación con que cuente el Firewall, los rechaza o acepta dependiendo si se encuentran o no. Es un buen filtro, pero no es suficiente ya que puede ser vulnerable a ataques, debido a que constantemente hay muchas amenazas por las innovaciones en los protocolos que se realizan.
- *Filtrado de paquetes en forma dinámica.* Consiste en que el Firewall verifica toda la información del paquete, además de que monitorea el estado de la conexión de dicha información en todo momento. Es más confiable que el primer tipo de filtrado.
- *Servidor Proxy.* Actúa como un intermediario para las peticiones de los usuarios, estableciendo una segunda conexión a la fuente requerida, de manera que nunca existe una conexión directa entre las dos redes.

Dentro de los beneficios que se encuentran disponibles con la implementación de un Firewall, es que va a permitir al administrador mantener la red segura contra los usuarios desautorizados, pero ello no significa que este tipo de sistema no sea vulnerable a ataques, por lo que se deberá contar con otros sistemas de seguridad que sirvan de complemento a la red. También sirve para simplificar los trabajos de administración, una vez que se consolida el sistema de seguridad basado en las políticas de la empresa. Además, la seguridad puede ser monitoreada, y si aparece alguna actividad sospechosa, el sistema generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos.

El administrador de red va a contar con beneficios como la auditoría o registro del uso de Internet, lo que va a permitir justificar gastos en cuanto a conexión de IP.

Dentro de un Firewall, también se encuentra un traductor de direcciones de red, lo que permite que se guarden y eliminen las direcciones necesarias, en caso de que la empresa se cambie de proveedor de Internet.

El Firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, como son los ocasionados por los usuarios internos en el que la información puede ser copiada y utilizada con fines ajenos a la empresa.

También es vulnerable en cuanto a los virus que puedan ser adquiridos mediante archivos tomados del Internet, lo que puede provocar un daño en la red de la empresa. Finalmente, un Firewall puede ser vulnerable durante la transferencia de datos, por lo que es recomendable la instalación de un servidor Proxy que va a permitir contar con una mayor seguridad.

El costo de la implementación de un Firewall va a depender del número de sistemas a proteger y sobretodo, con que herramientas de seguridad se va a contar, las cuáles deben estar basadas en las políticas de la empresa. Lo anterior permitirá que la información que se esté manejando sea la necesaria, para beneficio de todas aquellas organizaciones que cuenten con Firewalls. También puede implementarse como un hardware o software que se encuentre dentro de un Sistema Operativo de Red.

2.2.5. Sistema de Detección de Intrusos

Los IDS, son aquellos que se encargan del monitoreo y registro de todo el tráfico de una red, de tal forma que pueden estos sistemas actuar de manera preventiva ante un ataque, y así evitar daños en la red. La velocidad de respuesta es un factor crítico, por lo que los IDS actúan al Nivel de Aplicación, mediante el uso de diversas técnicas, como son desde la detección de patrones estáticos hasta técnicas de inteligencia artificial y extracción de datos. Existen tres diferentes tipos de IDS´s:

- *HIDS (Host based Intrusion Detection System: Sistema de Detección de Intrusos basado en Equipo).* Protegen a un único host, intentando detectar anomalías que hacen suponer un ataque, evitándolo en caso de ser necesario, y verifica la integridad de los archivos del sistema. Generalmente son programas que se ocultan dentro del sistema, para evitar que sean desactivados por el intruso. El HIDS se puede apoyar de Verificadores de Integridad del Sistema, que van a monitorear los cambios en los archivos críticos del host, para evitar modificaciones que afecten la seguridad del mismo.
- *NIDS (Network based Intrusion Detection System: Sistemas de Detección de Intrusos basados en Red).* Este sistema de detección va a proteger segmentos de red de la información que entre o salga, para prever ataques como DoS, peticiones mal intencionadas a servidores, etc. Se puede instalar en una máquina para el monitoreo de la red, en la que un administrador de red debe estar pendiente en caso de alarmas que afecten a la misma. Un ejemplo de este tipo de Sistema de Detección de Intrusos es el llamado *Etrust IDS.*
- *DNIDS (Distributed NIDS: Sistema de Detección de Intrusos Distribuido).* Consiste en el monitoreo de varias redes con un enfoque global, cuyo objetivo es encontrar datos que puedan servir a servicios de espionaje que afecten a la industria a nivel mundial.

Dentro de una empresa, es recomendable la instalación de HIDS y NIDS en conjunto, para tener una protección a nivel general, de igual forma al surgir un problema, es necesario que el administrador de red se apoye de dichos sistemas de seguridad, y así evitar que la red o el host se vean afectados. Cuando surge una alarma estos sistemas son capaces de enviar un mensaje de alerta al administrador de red, ya sea vía correo electrónico, pager, desplegado en pantalla o fax, según sea configurado.

Dentro de los IDS, pueden existir falsas alarmas, como es el caso del olvido de un password, o el equívoco en el uso de passwords. De igual manera un ataque real puede estar encubierto por una falsa alarma. Los IDS pueden estar de igual forma apoyados por los *IPS (Intrusion Prevention System: Sistemas de Prevención de Intrusos)*, los cuáles son una variación de los IDS, con diferencia en que al detectar una anomalía en la red, automáticamente actúan sobre el problema.

Al hablar sobre este tipo de sistemas de seguridad, es muy conveniente concientizar a las empresas en el uso de este tipo de implementos, que están hechos con la finalidad de proteger la información, aunque también es importante que dentro de la misma empresa, la gente sea parte de la solución y no del problema.

2.2.6. Sistemas de Inspección de Contenido y detección de vulnerabilidades y riesgos

El CI *(Content Inspection System: Sistema de Inspección de Contenido)*. Es un software que detecta la actividad de algún código dañino e interviene inmediatamente para frenar el ataque, valiéndose de la detección, el bloqueo y la notificación automática de todos los contenidos peligrosos. Este sistema ofrece una seguridad proactiva basada en el Gateway de Internet, restringiendo las direcciones y bloqueando el acceso a sitios Web que contengan palabras clave inadecuadas, protegiendo a los servidores de eBusiness contra virus y aplicaciones mal intencionadas de *Java*, controles de *ActiveX* y demás códigos que pudieran ser descargables a través del Internet, los cuales pueden dañar al sistema o robar información crítica.

Con esta herramienta es factible proteger a las empresas frente a las amenazas procedentes de Internet, inspeccionando de modo dinámico el comportamiento del sistema. También permite desplegar y utilizar con seguridad las aplicaciones empresariales de Internet basadas en código móvil.

Este sistema ofrece una solución en tiempo real protegiendo a la red empresarial de los archivos ejecutables y las descargas de Internet que no cumplan las políticas de seguridad de la misma empresa, y forma un excelente complemento para los Firewalls y los Antivirus que pudieran encontrarse instalados previamente en la red.

Sistema de deteccion de vulnerabilidades y riesgos. Es un sistema de seguridad empresarial que identifica áreas problemáticas potenciales, facilitando su solución y previniendo problemas recurrentes mediante el monitoreo cercano a los sistemas de seguridad. Este sistema realiza una auditoría a las directrices de seguridad que se han programado en los diversos servidores y aplicaciones, desde una sola consola, lo que permite que el administrador realice una evaluación del estatus en la seguridad de los sistemas, detectando fácilmente las vulnerabilidades existentes en la política de seguridad y además permite que administre efectivamente los riesgos que éstas conllevan.

Esta aplicación permite que el administrador rectifique las directrices en los elementos de seguridad con los que cuenta la red, sin perder tiempo en auditar a cada uno de los componentes del sistema de seguridad de la red, reduciendo considerablemente el tiempo en el que un hueco en la seguridad queda expuesto, manteniendo lo más cerca de la red en condiciones ideales de trabajo en cuanto a seguridad se refiere.

2.2.7. Interoperatividad y administración de seguridad

Por lo mencionado anteriormente, consideramos que los principales productos de seguridad para una red deben ser los Antivirus, los Firewalls, los IDS, los CI y un Sistema de detección de vulnerabilidades. Estos deben de trabajar en forma integrada y no mutuamente excluyente para obtener los mayores beneficios. Esta interoperatividad de los componentes de las capas de seguridad de la red, es fundamental para garantizar que los objetivos de seguridad del sistema se satisfagan.

Fallas en la interoperatividad abren brechas de oportunidad para ser explotadas por ataques al sistema de seguridad, en lo referente a la prevención de entrada de ataques, detección de amenazas y respuesta a eventos de manera oportuna.

Así, los elementos que constituyen nuestro bloque de seguridad deberán de ser seleccionados tomando en consideración su grado de interoperatividad entre cada componente del sistema. Si una solución en una capa, por ejemplo, un poderoso Antivirus, no presenta una adecuada respuesta en cuanto a su interoperatividad con los demás componentes del sistema, deberá de ser descartado.

Existen dos enfoques para crear una arquitectura de capas de seguridad:

- El modelo híbrido.
- El modelo consolidado.

El *modelo híbrido* representa una arquitectura multicapa, donde se han seleccionado las mejores tecnologías disponibles para cada capa. Por ejemplo: se puede tomar un Antivirus de *McAfee* que trabaje a lo largo de la red, mientras que *Computer Associates* puede ofrecer protección en los Gateways del sistema y

Check Point podría aportar el Firewall y en los routers tener la tecnología IDS de *CISCO*.

Este modelo híbrido puede, sin embargo, presentar problemas de falla de interoperatividad de sus componentes.

Estas fallas de interoperatividad se pueden reflejar en los siguientes términos:

- Las soluciones líderes ofrecen una interfaz gráfica, en donde de forma visual se representan las opciones de configuración del producto, así como una manera de presentar las mediciones y eventos que acontecen dentro del campo de acción del producto. Dichos parámetros vitales para la administración del sistema de seguridad de la red pueden competir entre diversos productos, causando fallas de interoperatividad, por ejemplo, pueden competir con los puertos del sistema.
- Una de las ventajas de un sistema de seguridad por capas, es que cubre un amplio margen de actividad de la red, pero esta virtud es opacada debido a que los distintos productos tienen sus propias consolas de monitoreo de la red, imposibilitando al administrador del sistema poder cubrirlas todas en un tiempo óptimo.
- Otro término donde las fallas de interoperatividad se puede reflejar, es en lo referente a la actualización de las diferentes soluciones adoptadas, las cuales en un sistema híbrido deben de realizarse una por una, en turno, a varios dispositivos de la red y la necesidad de múltiples reinicios del sistema, perdiendo tiempo valioso y permitiendo incrementar la probabilidad de amenazas al equipo.
- La responsabilidad en casos de fallas en un sistema híbrido no puede ser claramente establecidas, sobre todo, considerando que los ataques actuales son del tipo multicanal, donde el intruso trata de penetrar al sistema en distintos niveles de seguridad al mismo tiempo.
- Cuando un producto es actualizado tecnológicamente, antes que otros del sistema, pueden perder comunicación entre sí.

El *modelo consolidado*, por otra parte, tomará el menor número de productos (preferiblemente uno solo) para armar su estructura de seguridad de red. En este modelo se han incorporado productos que han desarrollado muy buenas plataformas de administración de red, con soluciones de seguridad multicapa muy atractivas dentro de un marco centralizado y gráfico. Estas ofertas de paquetes consolidados permiten un ahorro, ya que sólo se debe pagar a un solo proveedor con el correspondiente descuento por volumen.

Con un modelo consolidado la responsabilidad en caso de falla es fácilmente asignada. Este modelo consolidado ofrecerá la mayor interoperatividad posible en un sistema multicapa como el recomendado, sin embargo, podemos puntualizar algunos rubros donde debemos de tener cuidado al incorporar a la red un sistema consolidado:

- Un solo proveedor muchas veces no será suficientemente competente al ofrecer una solución óptima en cada una de las capas de seguridad del sistema.
- Al estar dependiendo de un solo proveedor, podemos vernos en serias dificultades si algo falla, estamos poniendo todos "los huevos en una sola canasta". Debemos por lo tanto tener mucho cuidado al elegir al proveedor de nuestro sistema de seguridad de red.
- Al ser un único proveedor, los ahorros actuales pueden no serlo, al intentar actualizar el único producto del cual depende enteramente para la seguridad de toda la estructura de la red.
- Debemos saber explícitamente cuales son las compensaciones que ofrece el producto, en caso de fallas que afecten a nuestro sistema.

Dentro de las consideraciones de la administración de un sistema de seguridad de red, la administración del sistema de seguridad es precisamente el punto clave de todo el proceso de aseguramiento de la misma. Las funciones operacionales del sistema deben de estar claramente establecidas y comprendidas por el personal encargado de la seguridad del mismo. Un sistema excelente puede venirse abajo si el personal a su cargo no ha sido suficientemente entrenado para su uso.

Se debe de tomar lo anterior en cuenta, siempre que optemos por un producto cualquiera, sin importar que modelo necesitemos realizar, híbrido o consolidado. Siempre nos deben de ofrecer todos los medios posibles para garantizar que el personal a cargo de la administración del sistema pueda ser entrenado competentemente en todos los aspectos del producto a implementar.

2.3. Modelos y arquitecturas de seguridad

La mayoría de las arquitecturas de administración de redes utilizan el mismo conjunto de relaciones y estructuras básicas. Las estaciones terminales y otros dispositivos de red, corren software que les permite enviar señales de alerta cuando descubren que hay un problema. En el momento en que reciben estas señales de alerta, se pueden ejecutar una o varias acciones, incluyendo la notificación al administrador. Las arquitecturas más utilizadas son: la *DMZ (Demilitarized Zone: Zona Desmilitarizada)* y la *MZ (Militarized Zone: Zona Militar).*

2.3.1. Arquitectura de Zona Desmilitarizada y Militarizada

La arquitectura de Zona Desmilitarizada, también conocida como red perimétrica, es la más utilizada e implantada hoy en día, ya que añade un nivel de seguridad en las arquitecturas de Firewalls situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al *host bastion* (entendiéndose por este término al arreglo formado por un par de Firewalls colocados a la entrada y salida del servidor).

Es posible implementar una DMZ con un único router que posea tres o más interfaces de red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno.

También podemos, si necesitamos mayores niveles de seguridad, definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas, a estas áreas protegidas se les conoce como Zonas Militarizadas; así, el atacante habrá de saltar por todas y cada una de ellas para acceder a nuestros equipos; evidentemente, si en cada red perimétrica se siguen las mismas reglas de filtrado, niveles adicionales nos proporcionarán mayor seguridad.

Estas arquitecturas de Firewalls eliminan puntos únicos de fallo antes de llegar al host bastion. La arquitectura DMZ es más segura, pero también la más compleja; se utilizan dos routers, denominados exterior e interior, conectados ambos a la red perimétrica como se muestra en la figura 2.2. En esta red perimétrica, que constituye el sistema Firewall's, se incluye el host bastion y también se podrían incluir sistemas que requieran un acceso controlado, como baterías de modems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red. El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica; así, un atacante habría de romper la seguridad de ambos router para acceder a la red protegida.

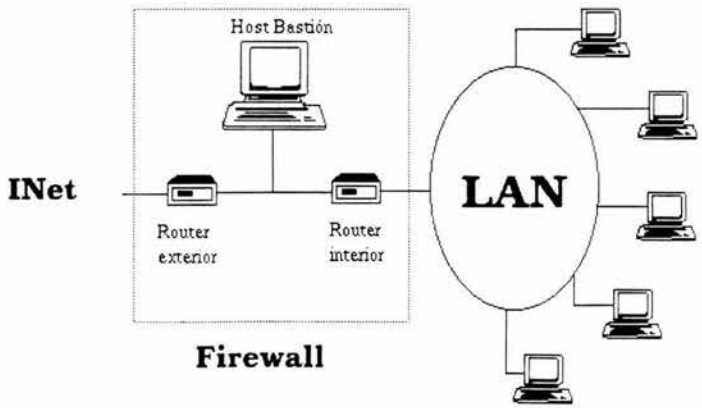


Figura 2.2. Arquitectura DMZ.

Estas arquitecturas de Firewall eliminan puntos únicos de fallo: antes de llegar al host bastion (por definición, el sistema más vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el router externo. Si lo consigue, como hemos aislado al host bastion en una subred, estamos reduciendo el impacto de un atacante que logre controlarlo, ya que antes de llegar a la red interna ha de comprometer también al segundo router. En caso extremo, si un usuario no autorizado logra comprometer el segundo router, la arquitectura DMZ no es mejor que un solo Firewall a la entrada del servidor. Por supuesto, en cualquiera de los tres casos (comprometer al router externo, al host bastión, o al router interno) las actividades de un usuario no autorizado pueden violar nuestra seguridad, pero de forma parcial. por ejemplo, si simplemente accede al primer enrutador, puede aislar toda nuestra organización del exterior, creando una negación de servicio importante, pero esto suele ser menos grave que si lograra acceso a la red protegida.

2.3.2. Estructura por capas de seguridad

En la protección de los recursos de una organización, el implementar la seguridad sólo con la utilización de un Firewall, podría dejarla vulnerable a la intromisión de virus a través del Email, o que un hacker pudiera atravesarlo, en busca de información valiosa. Al tener una estructura por capas es posible minimizar las oportunidades de que los recursos se encuentren comprometidos.

Una estructura de capas incluye tener otros elementos de seguridad, además de los Firewalls, como son los Antivirus, detectores de contenido y los IDS's. Es de tomarse en cuenta que entre más capas existan, los recursos se encontrarán más seguros, con la desventaja que esto representa, la utilización de monitoreos más complejos y el natural aumento en las tareas de administración.

Las políticas que soportan los componentes de software y hardware, son de crucial importancia para la creación de una capa de defensa, para la seguridad de los recursos, ya que es ésta quien define las necesidades y aplicaciones a proteger. La relación entre la política de seguridad y el nivel de protección, definirá el camino a seguir de la compañía, para adquirir el máximo de seguridad, de acuerdo a los parámetros establecidos.

2.3.3. Métodos complementarios de seguridad

El modelo de seguridad de la red puede ser integrado utilizando varios componentes colocados alrededor de una política central de seguridad, utilizando medios prácticos y previniendo el equilibrio entre el costo y los resultados.

La creación de un sistema de seguridad modular ofrece la oportunidad para hacer un armazón que anulará las amenazas conocidas, y advertirá a un administrador sobre las actividades de la red raras e inesperadas. Las tecnologías útiles en tal armazón serán aquéllas que se han mencionado a lo largo de este trabajo, AV, Firewalls, detectores de contenido, y soluciones de IDS.

El concepto de armazón, como una serie congregada de componentes, nos lleva a reforzar el uso de soluciones o servicios en áreas específicas. Este proceso de señalar los sitios vulnerables importantes puede ser crítico en conjunto para el éxito de todos los otros elementos de seguridad de la red.

El servidor del correo electrónico se ha considerado como un punto de alto riesgo, para ésta y cualquier otra organización, y el servidor de Web entra en la misma categoría. Los administradores podrían agregar capas adicionales de seguridad existentes a estos puntos, por ejemplo, desplegando una solución de AV de un segundo vendedor al nivel del servidor; sin embargo, algunos productos de seguridad específicos se han diseñado para diferentes puntos de peligro dentro de la empresa.

Dado que cada compañía posee sus propias necesidades operacionales, es imposible proporcionar una lista comprensiva de componentes de seguridad útiles, que puedan complementar la política de seguridad de sus compañías; sin embargo, se recomiendan tres áreas generales a considerar, por su importancia para el manejo de una red: cumplimiento de la política de seguridad, contenido y filtración de la Web y la auditoría.

Cumplimiento de la política de seguridad

La política de seguridad carece de valor si no se aplica a todos los usuarios, o si los sistemas poseen configuraciones que no reúnen las normas y capacidades mínimas de seguridad. Por consiguiente, es esencial supervisar elementos tecnológicos y humanos de la red en todo momento.

La mayoría de soluciones de seguridad disponibles en el mercado actual, proporcionan soluciones de control centralizadas, además de dar la dirección de actualizaciones de producto. Ésta es una demanda obvia para soluciones como los productos de AV y Firewalls que utilizan la información puesta al día.

Cuando una organización sigue un modelo de seguridad basado en componentes, creando de esta manera un armazón de varias tecnologías, proporciona un obstáculo mucho más serio a un hacker. Pero uno de los costos inevitables, será una mayor demanda en tiempo y habilidades del personal responsable para la red.

El segundo problema con la política de seguridad involucra los elementos humanos de la red, es decir, los empleados de la organización. El mal uso e impropio del correo electrónico, por ejemplo, de los usuarios, ha llegado a producir problemas corporativos, por lo que se debe de crear conciencia entre los usuarios de la red, como una medida de seguridad.

Contenido y filtración de la Web

La habilidad de impedir que cierta información entre a la red, es potencialmente un componente muy útil para agregarse a la política de seguridad. Un buen ejemplo es la habilidad de bloquear el acceso a un *URL (Universal Resource Locator: Localizador de Recursos Universal)* específico, no requiere el soporte de algún otro producto en particular; sin embargo, algunos están disponibles para simplificar el proceso. Si en una revisión de tráfico de Web se indica que uno o varios empleados están gastando más tiempo que lo que la política permite en sitios como *eBay o Amazon* (por mencionar algunos), entonces simplemente se bloquean esos URLs. Esto evita cualquier repercusión negativa de empleados que puedan quejarse de que no se les permite la comunicación entre ellos. De igual forma se puede impedir que estos bajen información de la red o que accedan a sitios que son evidentemente sólo para adultos.

Si un informe indica, por ejemplo, que se tienen conexiones punto a punto, se presenta una brecha clara a la política de seguridad. Puede que se trate de información que no tenga nada que ver con la compañía, como por ejemplo, el intercambio de música o material de video, produciéndose niveles altos de consumo del ancho de banda, perjudicando la disponibilidad de recursos cuando son requeridos por el negocio. El ancho de banda es caro de mantener, y hay una tendencia fuerte a pagar por medios de transmisión de mayor capacidad, en lugar de manejar lo que ya se tiene de manera más eficaz. También se tiene el inconveniente de que dicho archivo podría portar un virus. Si el riesgo de acceder un servicio no tiene ningún propósito comercial, entonces el riesgo no debe tomarse en absoluto.

La auditoría

La necesidad de intervenir la actividad de la red debe ser una prioridad clara por el administrador. Saber que se está haciendo, por quién y en dónde, y qué recurso se está consumiendo en la red. El uso inesperado de recursos resalta a menudo la actividad del "computomaníaco", por lo que esta información resulta ser muy valiosa.

Las herramientas de la auditoría pueden ser consideradas como los componentes para simplificar la adquisición y presentación de datos de la red, que tienen valor considerable para el armazón de seguridad. En caso de un fracaso de la red debido a una falla de seguridad, puede ser crucial determinar lo que ocurrió para minimizar el tiempo exigido en devolver al estado totalmente operacional a la red. En este caso, está también claro que la información de la auditoría necesita ser guardada estrechamente de intrusos, que intentarán enmendarlos para cubrir sus huellas.

2.3.4. Estándares e instituciones reconocidas en seguridad

Hay una gran variedad de estándares e instituciones responsables para el análisis de las soluciones y productos de seguridad. En esta sección se mencionan algunas de las más sobresalientes.

CERT (Computer Emergency Response Team: Equipo de Respuesta a emergencias en cómputo). Este grupo de trabajo, con centro coordinador en el Instituto de Software de la Universidad de Carnegie Mellon, tiene a su cargo, la respuesta oportuna a las amenazas que llegan a ocurrir en toda la Internet: tales como ruptura a sistemas de cómputo, denegaciones de servicio, etcétera. Además de que es responsable de la publicación de una serie de documentos sobre vulnerabilidades de sistemas que vayan apareciendo en Internet, comentándolas y haciendo recomendaciones para incrementar la seguridad de Internet como un todo. El sitio de este equipo de trabajo se localiza en la siguiente dirección de Internet: http://www.cert.org.

ITSEC (Information Technology Security Evaluation and Certification Scheme: Esquema de Certificación y Evaluación de Seguridad de la Tecnología de la Infoirmación). Este estándar permite conocer si algún software comercial proveerá de un nivel de garantía de seguridad. El software es probado en forma independiente del proveedor y es examinado contra un criterio estándar mediante una metodología formal. Este estándar tiene por sede en el Reino Unido a la *CESG (Communications Electronics Security Group: Grupo de Seguridad en Comunicación Electrónica)* y es adoptado también por los siguientes países: Francia, Alemania, los Países Bajos, Finlandia, Grecia, Italia, Noruega, España, Suecia y Suiza.

El ITSEC define siete niveles de garantía de seguridad que un producto puede ofrecer; desde el más bajo (E0) que indica que "el producto fallo la prueba" hasta el más alto (E6) que indicará que el producto si cumple con todas las especificaciones. Este estándar es accesible en la siguiente dirección de Internet: www.cesg.gov.uk .

Los niveles de clasificación, llamados de aseguramiento, que utiliza esta institución son los siguientes:

- E0. Indica un funcionamiento inadecuado y que el producto ha fallado en la prueba.
- E1. Un nivel básico de funcionamiento, que ha pasado varias normas y métodos de la documentación.
- E2. El vendedor ha proporcionado un plan detallado informal y documentación de pruebas. Acredita la prueba y la del diseñador.
- E3. El vendedor ha proporcionado el código fuente y de diseño, mostrando correspondencia entre éste y los fines a alcanzar.

- E4. El vendedor ha proporcionado un modelo formal de seguridad, arquitectura y de diseño. Comparado con el criterio anterior, también logra acreditar los criterios de seguridad.
- E5. El diseño arquitectónico explica la interrelación entre los componentes de seguridad, incluidos en el criterio para transferir información sobre procesos de integración y librerías que se han corrido.
- E6. El vendedor ha proporcionado una descripción formal de la arquitectura y funciones de seguridad. Se ha proporcionado correspondencia entre la especificación formal de las funciones de seguridad a través del código fuente y pruebas.

Este estándar es muy confiable, ya que es una entidad independiente de alguna compañía proveedora de software de seguridad.

IACS (Information Assurance and Certification Services: Servicios de Aseguramiento y Certificación de la Información). Un servicio de certificación desarrollado para responder a la demanda creciente de productos y sistemas de seguridad. Este estándar es adoptado por más países que el ITSEC y tiene también, su sede en el Reino Unido en la CESG. Los países que han adoptado este estándar son principalmente: Australia, Nueva Zelanda, Canadá, Francia, Alemania, Reino unido, Estados Unidos, Finlandia, Grecia, Italia, Israel, Países Bajos, Noruega y España. Los productos usados en México, son importados de alguno o algunos de estos países. La IACS como un estándar de certificación en seguridad de productos de la tecnología de la información se compone de las siguientes secciones fundamentales:

- Un *Criterio Común (CC).* Derivado del ITSEC, y que incluye los estándares de pruebas y reporte de pruebas: EN45001 e ISO17025, en su conformación. Este elemento del estándar permite una certificación del producto en un plano internacional.
- El *SYS (Level System Evaluations: Evaluación de los Niveles del Sistema).* Utiliza las pruebas y metodologías de revisión del ITSEC y del Criterio Común. Sin embargo, esta certificación no es reconocida internacionalmente.
- Las Valoraciones Registro Rápido o *Fast Track Assessments.* Los usuarios de esta sección del estándar requieren seguridad informal en la funcionalidad de un producto. Es un servicio pensado para usuarios específicos y no se otorga certificado.
- Una Revisión de Inmunidad o *Health Check.* Que otorga un servicio de verificación de las vulnerabilidades conocidas para un sistema de seguridad o producto de seguridad.
- Cifrado de Datos o *Cryptography.* Se proveen servicios de verificación criptográfica para cumplir con estándares gubernamentales, además de verificar la correcta implementación de soluciones de seguridad en redes y sistemas.

IPSec (Internet Protocol Security: Seguridad del Protocolo de Internet). Es un nuevo estándar de seguridad proveniente del *IETF (Internet Engineering Task Force: Fuerza de Trabajo en Ingeniería de Internet)*, define las características que debe de tener el protocolo mismo de Internet, y opera en la Capa de Red del modelo de referencia OSI. Muchas aplicaciones para Internet toman como punto de partida a este estándar para la elaboración de sus programas.

El IPSec se ocupa principalmente de los siguientes dos aspectos de seguridad del protocolo de Internet:

- *ESP (Encapsulating Security Payload: Seguridad del Encapsulado de la Carga Útil).* Se refiere a la seguridad del contenido de los frames que circulen por la Internet.
- *AH (Authentication Header: Autentificación del Encabezado).* La seguridad que debe imperar para el manejo del encabezado de un frame.

OPSEC (Open Platform for Security: Plataforma Abierta para Seguridad). Este estándar, originario de la empresa de seguridad *Check Point*, pero que actualmente cuenta con unos 300 socios, provee a los desarrolladores de software de seguridad de un estructura sólida que les facilite poder edificar soluciones de seguridad, tanto a nivel de aplicaciones integradas como de plataformas de desarrollo de software. Muchos productos cuentan con el certificado de la OPSEC y garantizan su confianza.

Plan SEGURO (SAFE Blueprint). La empresa *Cisco, Inc.*, ha desarrollado *SAFE Blueprint*. Éste está basado en la Arquitectura de Cisco para voz, video y datos (AVVID). Esta arquitectura está pensada para ayudar a los negocios a competir en "la Internet". *SAFE Blueprint* cubre la seguridad en redes para:

- Empresas.
- Usuarios remotos.
- LANs Inalámbricas.
- Telefonia IP.

ICSA. Los Laboratorios de ICSA son una división de la sociedad *TruSecure*. Su sitio Web (www.icsalabs.com) menciona que "la meta para la ICSA es reforzar y mejorar aplicaciones de seguridad de red e Internet mejorando la seguridad comercial con el uso de productos de seguridad apropiados, servicios, políticas, técnicas, y procedimientos". Actualmente, los Laboratorios de ICSA reconocen que su certificación no ampara que los sistemas sean impenetrables, pero si que pueden reducir significativamente el riesgo de ataques a la vulnerabilidad de los sistemas.

ISMS (The Standard for Information Security Management System: Estándar para la Administración de Sistemas de Seguridad de la Información). Es un estándar de

enorme importancia actual en el rubro de la seguridad de la tecnología de la información. Más frecuentemente conocido como el estándar BS7799, de procedencia británica, pero acogido en forma universal, nos especifica las características que un sistema de seguridad efectivo debe de tener, así como, los pasos a seguir para lograrlo.

ISO17799. Este estándar creado para ofrecer una referencia internacional que asegure un óptimo desempeño de un sistema de información seguro dentro de una compañía. Abarca todos los aspectos de seguridad de una red. Basado en el estándar británico BS7799, revisado y actualizado hasta mayo de 1999 y meses después, en diciembre del 2000, aprobado como el estándar internacional ISO 17799. Este estándar está compuesto por diez secciones: planeación de la continuidad del negocio, sistema de control de accesos, mantenimiento y desarrollo del sistema, seguridad física y ambiental, fidelidad con otras entidades, seguridad del personal, seguridad organizacional, administración del equipo de cómputo y la red, control y clasificación de recursos y valores de la empresa y todo lo referente a la política de seguridad que una empresa debe de tener. El ISO 17799 se ha convertido en un punto de partida que garantiza la efectividad de nuestro plan de seguridad. Nosotros basaremos nuestro desarrollo e implementación en este estándar y se verá reflejado en la sección correspondiente de este trabajo.

2.3.5. Metodologías de comparación de productos

La clave para escoger la metodología adecuada para seleccionar un tipo de producto, será siempre el nivel de protección requerido, contra lo que se está protegiendo del sistema. No podemos elegir un producto que sobrepase el costo de lo que se desea proteger.

Aunque existen una multitud de enfoques a seguir para establecer criterios de comparación de productos en el mercado, para poder escoger al mejor en nuestro caso particular. Definiremos primero los aspectos que queremos comparar, puesto que los consideramos necesarios para nuestra red.

Dentro de los aspectos a considerar destacan unos indicadores de mercado o directrices, que nos ayudarán a seleccionar a los mejores productos para nuestra red. Estas directrices del mercado de seguridad son:

- *Popularidad*. Esta directriz nos indica que tanto un producto de seguridad está siendo empleado. Un producto en general, no una marca particular; así, por ejemplo, podemos detectar si se está empleando más un sistema contra virus o uno de detección de intrusos, un Firewall, o algún otro. Existen dos peligros al considerar esta directriz como método auxiliar en la selección de un tipo de producto a emplear: la prensa y los vendedores. En el primer caso, muchas veces se exagera la importancia de contar con una medida de seguridad, por ejemplo: un Antivirus, siendo que quizás nos convenga invertir más en un Firewall, por ejemplo, y seleccionar un

Antivirus en segundo término. En el caso de los vendedores, tenemos que cuidar que muchas veces exageran la importancia de su producto; si es éste un IDS, por ejemplo, nos pueden querer convencer que es el más importante dentro de la mezcla de seguridad de la red y reelegar la importancia de un Firewall, por ejemplo, si la compañía que representan no lo proporciona.

- *Incremento de conectividad.* Esta directriz nos puede guiar también a conocer que productos son los empleados con mayor frecuencia por otras empresas. El incremento de redes interconectadas acarrea una gran demanda de productos de seguridad y por ende, de competidores; entonces será el indicador que muestra en que aspectos de la conectividad está interviniendo algún producto de seguridad.
- *Estándares.* Esta directriz indicará si algún producto está, o no está, de acuerdo con los "estándares de seguridad de red", como se definió anteriormente en este trabajo, acerca de la importancia de los estándares de seguridad de red. Este rubro puede ser decisivo para seleccionar un producto en particular.
- *Tecnología.* Las mejoras tecnológicas se reflejan en el mercado inmediatamente y pueden ser la explicación de la selección de un producto o una marca en particular. Estas mejoras deberán de ser plenamente identificables y cuantificables, para no caer en productos mejorados sólo en su apariencia o diseño exterior, en vez de su funcionalidad.
- *Integración de productos.* Esta directriz nos marcará si el producto que queremos estará perfectamente integrado en todos los niveles establecidos de seguridad del sistema. Una falla en este aspecto puede resultar en una mala selección del producto. También el enfoque unificado o consolidado, donde se recurre a un solo proveedor de servicios de seguridad, debe de considerarse, ya que no obstante, sus sistemas están bien integrados, a veces es una solución poco práctica para empresas pequeñas.
- *Percepción de complejidad.* Se dice que la tecnología de la información es compleja, esto puede originar compras por encima de las necesidades reales de la empresa. Esta directriz nos posicionará con productos accesibles y de fácil uso, que puedan sencillamente calificarse. Sin descuidar, lógicamente, el aspecto de su funcionalidad.
- *Solución única.* Existen, además, empresas que han querido implementar una solución de seguridad completa para sus clientes, sin ser un producto totalmente consolidado. Estas empresas han implementado una medida llamada de fin a fin o "*end to end*", donde pretenden abarcar a todo el complejo de la red. Hay que considerar esta directriz, para observar si la solución prometida realmente cumple con las especificaciones publicitadas, o es una medida producto de la fusión de está empresa con subsidiarías alquiladas para completar el "paquete".

Dentro de las metodologías de comparación de productos de seguridad, además de las directrices, también debemos de ver ciertos aspectos de adopción de un

producto de seguridad para una compañía en particular. Entre estos aspectos destacamos los siguientes:

- *ROI (Return On Investment: Regreso de la Inversión).* Este es un problema en el campo de la seguridad; es como conocer cuando la inversión hecha para una solución de seguridad será retribuida con una ganancia de capital. En este aspecto, debemos de pensar como en una inversión por aseguramiento, como un seguro comercial, y considerar más bien el costo que provocaría una amenaza real para nuestra empresa, de perpetrarse ésta; cuánto daño nos costaría de no tener implementada la medida de seguridad.
- *Soluciones modulares.* Este aspecto nos mostrará que la medida puede suministrar una solución de seguridad adquirida por etapas, de acuerdo a nuestras necesidades reales de seguridad. Estos módulos adquiridos pueden estar debidamente integrados mediante un tipo de programa *API (Application Programming Interface: Interfaz de Programación de Aplicaciones),* el cual nos presenta en una sola consola de mando y administración todos los programas de seguridad que vayamos adquiriendo. Nosotros, sin embargo, preferiremos la solución consolidada, con un solo proveedor, debido a las razones expuestas en la sección correspondiente a "interoperatividad" de este trabajo, y a las necesidades de la empresa en la cual instalaremos nuestro sistema.
- *Pruebas independientes.* Este aspecto nos permitirá verificar si la solución que buscamos adquirir está realmente certificada, con base en los estándares de seguridad, como los expuestos en la sección "estándares de seguridad" de este trabajo (ITSEC, IACS, IPSec, OPSEC, ICSA labs Certification). También podemos alquilar una empresa que pruebe definitivamente si el producto a adquirir efectivamente es competente para evitar alguna amenaza. Esta empresa intentaría penetrar nuestro sistema de seguridad instalado y si lo logra, la solución puede ser descartada.

Por último, dentro de la metodología para seleccionar los productos de seguridad se deben considerar también las siguientes áreas:

- *Costos adicionales de operación.* Si al comprar algún producto éste no demandará recursos adicionales que deberán de ser incluidos en el costo total del producto, muchas empresas esconden este factor, previendo luego que el cliente deberá de solventar estos costos.
- *Facilidad de uso del producto.* Siempre el producto más fácil de usar será el que nos moverá a emplearlo, ya que será inevitablemente más seguro y su uso podrá ser plenamente entendido.
- *Pre-configuración.* Muchos productos vienen previamente arreglados para combatir eficazmente la mayoría de las amenazas actuales, este aspecto es importante al comparar la calidad de pre-configuración con que cuenta un producto dado.

- *Alertas y reportes.* La calidad de su sistema de comunicación con el administrador del sistema es un área vital para comparar un producto. Si un producto no tiene una plataforma eficaz para advertir al administrador de una amenaza en curso, puede provocar una error de decisión grabe, implicando una falla de seguridad.
- *Respuesta ante nuevas amenazas.* Al elegir un producto, debemos de verificar si éste está preparado para actualizarse rápidamente contra las nuevas vulnerabilidades que vayan apareciendo en la red. Se seleccionara siempre al producto con el mejor sistema que permita una respuesta inmediata a un nuevo riesgo de seguridad.
- *Expansión en el mercado.* Igualmente consideraremos si la solución ofrecida está siendo demandada por otras empresas, ya que en el campo de la seguridad, tenemos que confiar que nuestro proveedor estará lo suficientemente fuerte en el mercado para ofrecer la mejor solución de seguridad a largo plazo.
- *Estrategia.* Este aspecto nos ayudará a decidir el producto adecuado para nuestra red, al reflejarnos que inventiva empleará el proveedor del servicio de seguridad para continuar existiendo en el mercado. Un proveedor demasiado temerario posiblemente no sobreviva al embate del tiempo.

Con todos estos puntos a considerar, podremos elaborar unas herramientas que nos permitan elegir el producto más adecuado a nuestro sistema.

2.3.6. Comparación de estrategias de proveedores

En cuanto al desarrollo de los sistemas de seguridad, se analizarán las estrategias de siete de los principales proveedores que ofrecen sus servicios en el mercado de sistemas de seguridad.

Cysco Systems, Inc.

Esta empresa se ha caracterizado principalmente por la venta de routers y switches. En lo que refiere a la seguridad en redes, nos presenta el denominado sistema *SAFE Blueprint*, en donde se encuentran Firewalls, como el *modelo PIX 515E*, que son Firewalls reconocidos en el mercado y que están dirigidos a pequeñas y medianas empresas. Estos productos presentan deficiencias en cuanto a la seguridad que proporcionan, por lo que al implementarlos en una red tienen que estar apoyados de software adicional. Pueden ser sencillos en su manejo pero no muy funcionales.

En cuanto a los IDS's, se presenta la serie 4200, que para su implementación dentro de una red se debe de adquirir producto adicional como el *CiscoWorks Monitoring Center for Security*, que lo hace más confiable, pero que aumenta el costo para la empresa, por lo que no lo hace un producto muy competitivo dentro del mercado.

Check Point Software Technologies

Este proveedor se enfoca al mercado gubernamental, finanzas, inmunidad y ventas al mayoreo principalmente; además de que es una de las más importantes en cuanto al desarrollo de Firewalls se refiere. Su fuerte relación con *Nokia* le ha permitido la entrega de hardware con el nombre de *Nokia*. En cuanto a sus ventas se refiere, se enfoca a grandes empresas y a la solución de sus problemas, mediante un contacto directo, lo que le ha permitido un gran lugar en el mercado. Su producto es el denominado *OPSEC (Open Platform for Security: Plataforma Abierta de Seguridad)* que permite la integración y estandarización de una red.

Dentro de los Firewalls, su modelo principal es el *Nokia IP330* con una VPN-1, que a diferencia de sus competidores, una vez que se adquieren sus componentes adicionales, resulta simple su manejo y muy funcional.

Computer Associates

Esta empresa se ha preocupado por conocer los problemas, las necesidades y las capacidades con la que cuentan sus clientes; por lo que su estrategia de mercado se basa en proveer soluciones en cuanto a seguridad en redes se refiere, de manera ascendente y para todos tamaños de empresas, de tal forma que conforme crece la empresa. Las soluciones que ofrece también se desarrollan a mayor escala, lo que le ha permitido tener gran aceptación en el mercado.

Dentro de sus productos presentan el AV *eTrust 6.0*, resultando muy eficiente y no requiere de complementos adicionales. En cuanto a IDS´s se presenta *el eTrust Intrusion Detection 2.0*, que es muy versátil, se amolda al tamaño de la empresa, por lo que entre mayor sea la red, va a requerir de componentes adicionales, que le permitan un manejo eficiente en cuanto a seguridad en la red se refiere.

Entercept Security Technologies

Esta empresa está enfocada a medianas empresas. Sus productos tienen la característica de poder operar con otros sistemas, su alianza con *Cisco* es lo que le ha permitido salir adelante.

Dentro de sus productos presenta un Sistema de Prevención de Intrusos, denominado *Entercep 2.5*, y que sólo puede ser desarrollado sobre plataformas *Linux, UNIX y AIX*.

Network Associates

Esta empresa se ha enfocado en la implementación de un sistema de seguridad basado en herramientas eficientes de defensa, apoyadas en las políticas de seguridad de los clientes.

Su principal producto es el *McAffe Active Virus Defence*, reconocido más por su uso a nivel residencial, pero que puede contar con otros complementos cuando se trata a nivel de red, como es el *ePolicy Orchestrator*.

Sophos Plc.

Esta compañía se enfoca a todo tipo de empresas, de cualquier tamaño, y sus Antivirus se encuentran dentro del producto *QoS (Quality of Service: Servicio de Calidad)*. Sus principales productos son *Sophos Antivirus, MailMonitor y Entreprise Manager* y se caracterizan principalmente por sus procesos de actualización y el soporte que proporciona a sus clientes.

Symantec Corporation

Es una de las principales proveedoras en cuanto a sistemas de seguridad se refiere, y esto se debe a que ofrece soluciones en todas las áreas en lo referente a seguridad. También ofrece el llamado "Internetworking", que es capaz de proveer la infraestructura de red que permita una eficiente fluidez de la información, con la confiabilidad de que la información va a ser manejada con gran seguridad e integridad en donde sea requerida.

Dentro de sus productos se encuentra el *Symantec Antivirus Enterprise Edition 8.5*, que ha tenido gran aceptación en el mercado, debido a que permite al administrador de red desarrollar habilidades en cuanto a seguridad se refiere. Presenta la limitante de que no se pueden establecer reglas fuera de las que ya vienen configuradas. En cuanto a Firewalls, se encuentra el *Symantec Enterprise Firewall 7.0*, que es enfocado a medianas y grandes empresas y todo el software que sea requerido es proporcionado por *Symantec*.

2.3.7. Evaluación y comparación de otras tecnologías

Los siguientes productos que se presentan están enfocados a ofrecer soluciones en la administración de sistemas de seguridad. Tienen la capacidad de ser utilizados en diferentes Sistemas Operativos, además de que permiten el manejo de la gente que conforma la red de la empresa. Hay empresas que han sobresalido en el manejo de este tipo de soluciones, como son: *IBM Tivoli* y *Active Ned Steward*.

IBM Tivoli Risk Manager 4.1

Esta solución está diseñada para minimizar la complejidad que puede existir para la administración de un sistema de seguridad en una red, debido a que integra diferentes aplicaciones dentro de la red, como son los Sistemas Operativos, routers, Firewalls, IDS´s y demás dispositivos que se encuentren conectados. Lo anterior permite al administrador de red el manejo de ésta de manera segura,

aunque no sea un experto en lo que respecta a los sistemas de seguridad, creando un sistema de seguridad inteligente y autónomo.

Esta solución está enfocada básicamente a empresas grandes, debido a que está diseñado para el soporte de este tipo de infraestructuras.

Active Ned Steward

Éste ha sido desarrollado por una empresa inglesa de nombre *Security Designers*, y cuyo producto se ha enfocado a pequeñas y medianas empresas y al sector público. Su producto se ha diseñado con el fin de proporcionar un alto nivel de seguridad en cuanto a la administración de un sistema de seguridad se refiere, ya que se amolda a las necesidades de la empresa a contratar y de las políticas que ésta presente. Dentro de las soluciones que propone se encuentra un sistema de control central, el cuál es configurado de acuerdo a lo requerimientos que se pidan por parte de la empresa; el servidor de administración central es el que va a almacenar toda la información en tiempo real, lo que va a permitir la identificación de ataques, intrusiones o malos manejos en la red, para encontrarles una rápida solución.

Este producto únicamente es manejado por el administrador de la red, lo que le va a permitir tener una base de datos de los problemas que surjan en la red, sin que los empleados de una empresa estén por enterados.

Utilizando como base la información anterior, en cuanto a conceptos y soluciones de seguridad para una red, en el capítulo siguiente se presentará el análisis del caso que es de nuestro interés, con la finalidad de obtener los resultados que nos permitan desarrollar un sistema de seguridad adecuado para la red en estudio.

CAPÍTULO 3

ANÁLISIS DEL CASO

El conocimiento del estado actual de la compañía, así como el método utilizado para la obtención de esta información son puntos críticos del presente trabajo. El método utilizado es por medio de cuestionarios, los cuales muestran como se encuentra estructurada la seguridad de la compañía. A través de esta información se llevará a cabo el diseño de la solución de seguridad para la empresa televisora.

3.1. Planteamiento del problema

La empresa televisora cuenta con un gran prestigio en México, ofreciendo sus servicios al público en general. Dentro de sus servicios más importantes de la misma se encuentra la comercialización de producciones televisivas propias y de otras empresas televisoras alrededor del mundo. Esta última incluye telenovelas, noticias, espectáculos, programas de opinión y deportes. La compañía produce más de 10,000 horas de programación al año. El ingreso principal para sustentar la operación de la empresa proviene de la publicidad, ésta sobrepasa los mil millones de pesos al año, por tanto también esta empresa interactúa continuamente con empresas privadas de diversos tipos de mercado.

La empresa televisora se ha caracterizado por ofrecer planes flexibles de publicidad a sus clientes, que han redituado en buenos resultados en cuanto ingresos en los últimos años, y como lo hacen una gran cantidad de empresas, busca ofrecer cada vez más un mejor servicio a sus clientes, proveedores, empleados y accionistas, y es ahí donde la tecnología y más aún el Internet puede apoyar para alcanzar esta meta.

Esta empresa televisora ha sido pionera en el área de sistemas y siempre ha buscado altos niveles de productividad, utilizando medios tecnológicos para lograr sus objetivos. Ha integrado una red de telecomunicaciones con dispositivos tecnológicos de punta, así mismo ha desarrollado sistemas para las diferentes áreas que componen su infraestructura, con la finalidad de compartir la información para la operación y toma de decisiones.

Aprovechando recursos como la Internet, la empresa busca poner a disposición de empleados, proveedores y clientes, servicios Web. Así también, ha automatizado

la comunicación dentro y fuera de la empresa, por medio de la implementación de servicios de correo electrónico.

Como consecuencia del desarrollo tecnológico planteado anteriormente, se ha llegado a situaciones de eventos que han detenido su operación, principalmente por ataques de virus a través del correo electrónico, así mismo, la empresa ha detectado que diversos proyectos de alta confidencialidad han caído en manos de su competencia, sin tener la seguridad de que la fuga de información se haya realizado por medio de la red.

Otro problema que se presentó fue el uso indiscriminado de la red para acceder a sitios de Internet ajenos a la operación de la empresa, provocando mayor tráfico en el medio de transmisión y alentando de esta manera los procesos que se llevan a cabo en la red, con la consecuente pérdida de tiempo y dinero y en algunas ocasiones la caída de los enlaces de red tanto LAN y WAN.

Con el desarrollo de servicios Web, la compañía ha extendiendo sus aplicaciones a proveedores, clientes, empleados y socios, dejando sus sistemas expuestos a posibles accesos no autorizados.

Los problemas y necesidades planteados por la empresa televisora coinciden con encuestas y estadísticas de instituciones reconocidas en el ámbito de seguridad. Estas encuestas y estadísticas nos apoyarán para el diseño de la arquitectura del sistema de seguridad, implementando las mejores prácticas hoy existentes.

Dentro de las varias encuestas que se relacionan con las necesidades de la empresa televisora, se puede mencionar la correspondiente al *Instituto de Seguridad en Cómputo*, que forma parte del *FBI (Federal Bureau of Investigation: Departamento Federal de Investigaciones)* de los Estados Unidos de Norteamérica. Esta institución reportó que en el año 2001 el número de intrusiones, en cantidad de incidentes, fueron aproximadamente un 50% internas y un 50% externas, a diferencia del año anterior en donde la cantidad de incidentes de intrusiones internas llegó a ser hasta de un 80%. Para los años 2000 y 2001 la misma encuesta arrojó que los tipos de ataques -entendiendo por ataques cualquier situación que comprometa el buen funcionamiento de la red- más usuales fueron en primera instancia los virus informáticos, seguidos por el abuso de los enlaces de red y el robo de equipos portátiles, lo que ocasionó un gran impacto financiero en las empresas afectadas.

3.2. Estado actual del sistema de seguridad

La empresa televisora cuenta con una infraestructura de red tipo Ethernet, con una LAN central establecida en la Ciudad de México y un backbone para integrar una WAN de tipo Frame Relay. Ésta última utiliza principalmente como medio de transmisión fibra óptica para enlazar tres localidades estratégicas ubicadas en Monterrey, Guadalajara y Puebla. Para lograr estos enlaces cuenta con ruteadores de marca *Cisco* y arreglos de switches y hubs a nivel local marca *3COM*, en una

topología física en configuración de estrella a 100 Mbps, utilizando el estándar 100VGAnyLan.

La empresa televisora cuenta con un total aproximado de 1600 computadoras integradas en la red, además de los servidores con los que provee servicios de archivos, impresión, correo electrónico, aplicaciones, RAS y Web. La estructura general de las redes LAN y WAN se observa en la figura 3.1.

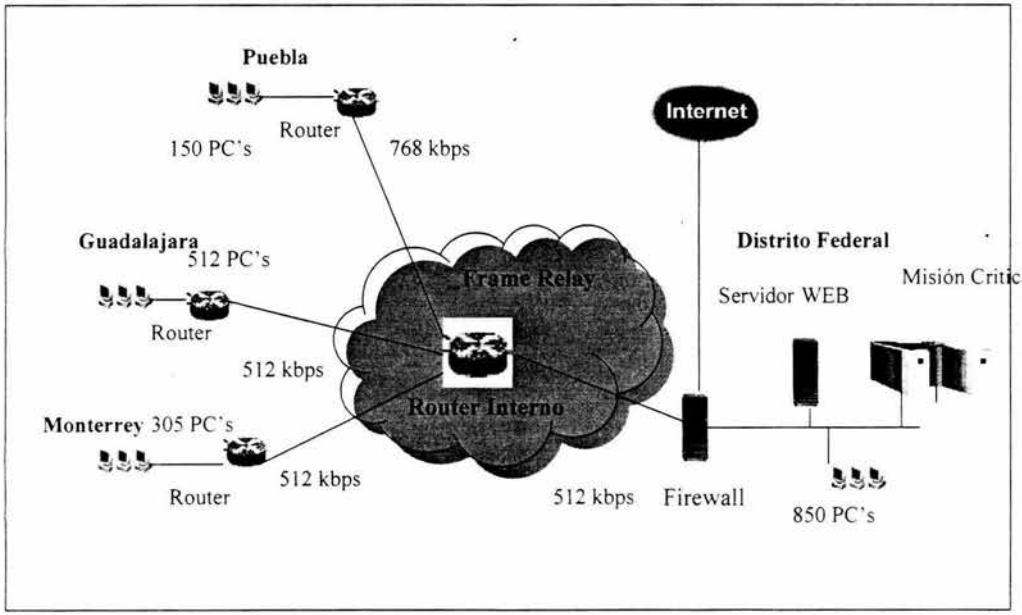


Figura 3.1. Arquitectura de Red WAN.

La red cuenta con Sistema Operativo *Microsoft Windows NT* con el *SP6 (Service Pack 6: Paquete de Servicios Versión 6)*, y los nodos cuentan con un sistema operativo *Microsoft Windows 2000 o anterior.* El ancho de banda de la red de datos hacia Monterrey es de 512 kbps, el segmento que va hacia Puebla es de 768 kbps, el que va hacia Guadalajara es de 512 kbps y el implementado en México es de 512 kbps. La diferencia en anchos de banda es debida a que en Puebla se encuentra localizado el servidor que aloja la videoteca. El tipo de configuración de la dirección IP es tipo A. Los ruteadores se encuentran ubicados en cada una de las localidades y se cuenta con un servicio de correo electrónico

Microsoft Outlook Versión 9.0.0.2711. Cabe comentar que en la Ciudad de México se cuenta con un servidor de servicios Web marca *IBM Web Sphere.*

3.3. Levantamiento de la información

El levantamiento de información para desarrollar el sistema de seguridad solicitado partió de conocer la situación de la empresa en el rubro de seguridad, en lo referente a su operación y procesos diarios. Para llevar a cabo lo anterior se desarrollaron cuestionarios con el objetivo de proveer un análisis de los problemas de seguridad de la empresa. Estos cuestionarios fueron aplicados a dos personas claves del área de sistemas de la empresa.

3.3.1. Método

El método usado para conducir el estudio correspondiente al levantamiento de información se realizará en tres fases: generación de cuestionarios, aplicación de cuestionarios y análisis y exposición de resultados, tal como se muestra en la figura 3.2.

Figura 3.2. Método para el levantamiento de Información.

Generación de cuestionarios

En esta fase se crearon unos cuestionarios para ser aplicados al personal administrativo de la red actual, siendo estos el Director de Sistemas y el Gerente de Seguridad Informática de la empresa, con el propósito de investigar el estado actual de seguridad de la compañía. Para elaborar este instrumento, se procederá mediante el apoyo de diversa bibliografía en el rubro de la seguridad de datos, en particular, el estándar británico BS17799, el estándar ISO7799, y en

recomendaciones hechas por *Gartner Group*, compañía especializada en sistemas de seguridad.

Aplicación de cuestionarios

La aplicación de los cuestionarios al personal administrativo consiste en una entrevista que integra un total de diez cuestionarios, cubriendo los siguientes temas:

I. Cuestionario de organización y políticas de seguridad. Este cuestionario cuenta con 48 preguntas.
II. Cuestionario para la prevención de seguridad. Este cuestionario cuenta con 27 preguntas.
III. Cuestionario para la administración de usuarios. Este cuestionario se encuentra conformado por 24 preguntas.
IV. Cuestionario para el control de accesos. Este cuestionario es el más extenso, contando con 77 preguntas.
V. Cuestionario para la seguridad física. Este cuestionario tiene 23 preguntas.
VI. Cuestionario para la evaluación de activos. Aquí sólo contamos con 9 preguntas.
VII. Cuestionario para el análisis de seguridad. Se tienen 7 preguntas.
VIII. Cuestionario para el análisis de continuidad de negocio. Se tienen 14 preguntas.
IX. Cuestionario para el análisis de auditoría. Este cuestionario presenta 7 preguntas.
X. Cuestionario para el análisis del ambiente aplicativo. Se cuenta con 9 preguntas.

Se cuenta con un total de 245 preguntas, de las cuales 4 de ellas carecen de una calificación, pidiendo una respuesta escrita. Las restantes 241 preguntas mantienen un puntaje específico.

Estos cuestionarios fueron aplicados al Director de Sistemas y el Gerente de Seguridad Informática de la empresa en forma individual. Los cuestionarios, junto con una breve explicación de su importancia, se muestran a continuación.

I. Cuestionario de organización y políticas de seguridad

Este cuestionario pretende sondear aspectos del rubro de seguridad, correspondientes a las políticas implementadas hasta este momento por la empresa en lo que se refiere a seguridad física, continuidad de negocio, estructura organizacional, el trato con terceras personas tanto físicas como morales, aspectos de confidencialidad y cultura de seguridad dentro de la empresa. Ver Tabla 3.1.

Pregunta	Actual	Meta	Explicación
1¿Existe una política completa de seguridad?			0 = no hay; 5 = completa
2¿Existen políticas individuales?			0 = ninguna; 5 = cobertura completa
3Ellas cumplen con:			
3.1 Control de acceso			0 = no; 5 = completa
3.2 Aplicación			0 = no; 5 = completa
3.3 Activos de la empresa			0 = no; 5 = completa
3.4 Auditoría			0 = no; 5 = completa
3.5 Autentificación			0 = no; 5 = completa
3.6 Backup y Recovery			0 = no; 5 = completa
3.7 Administración de la continuidad del Negocio			0 = no; 5 = completa
3.8 Control de cambios			0 = no; 5 = completa
3.9 Confidencialidad			0 = no; 5 = completa
3.10 Aspectos legales y contractuales (incluyendo terceros)			0 = no; 5 = completa
3.11 Manipulación de medias y documentos			0 = no; 5 = completa
3.12 Educación			0 = no; 5 = completa
3.13 Correo electrónico			0 = no; 5 = completa
3.14 Encriptación			0 = no; 5 = completa
3.15 Manejo de incidentes			0 = no; 5 = completa
3.16 Uso de redes			0 = no; 5 = completa
3.17 Uso de equipo fuera del sitio			0 = no; 5 = completa
3.18 Personal			0 = no; 5 = completa
3.19 Seguridad física			0 = no; 5 = completa
3.20 Acceso remoto			0 = no; 5 = completa
3.21 Violación a las políticas de seguridad			0 = no; 5 = completa
3.22 Configuración de Sistemas Operativos y servidores			0 = no; 5 = completa
3.23 Software			0 = no; 5 = completa
3.24 Desarrollo de software			0 = no; 5 = completa
3.25 Virus y software malicioso			0 = no; 5 = completa
3.26 Acceso a Internet			0 = no; 5 = completa
4¿Con qué frecuencia es revisada la política de seguridad de la empresa?			0 = nunca; 2 = una vez; 3 = cada año; 4 = cada 6 meses; 5 = cada 4 meses
5¿La política de seguridad se aplica a todo el personal?			0 = no; 5 = sí
6¿Qué política es distribuida?			Información
7¿Hay alguna organización de seguridad?			0 = no; 5 = completa
8¿Hay algún miembro de la mesa directiva a cargo de toda la seguridad de la TI?			0 = no; 5 = sí
9¿Hay algún foro de alto nivel?			0 = no; 5 = completa
10¿Hay algún foro interorganizacional de seguridad de TI?			1 = no; 5 = completa

Tabla 3.1. Organización y políticas de seguridad.(Continúa)

Pregunta	Actual	Meta	Explicación
11¿Qué tan frecuentes son estos foros?			0 = 1 vez; 2 = anualmente; 3 = cada 6 meses; 4 = cada 4 meses; 5 = cada mes
12¿La instalación de cualquier facilidad de TI es aprobada y autorizada?			1 = no; 5 = completa
13¿Son llevadas a cabo revisiones independientes?			1 = no; 5 = sí
14¿Qué tan frecuente son llevadas a cabo estas revisiones?			0 = nunca; 2 = 1 vez; 3 = cada 2 años; 4 = anualmente; 5 = cada 6 meses
15¿ Se tienen analizados los riesgos asociados de acceso de terceras personas a las facilidades de TI?			0 = no; 5 = completa
16¿Los contratos con terceras entidades especifican condiciones de seguridad?			0 = no; 5 = completa
17¿La auditoria de la organización es reportada a la mesa directiva?			0 = no; 5 = sí
18¿Hay algún equipo de respuesta a incidentes?			0 = no; 5 = completa
19¿Existen roles de y responsabilidades de seguridad definidos para todo el personal?			0 = no; 5 = completa
20¿Hay trabajos sensitivos que requieren privilegios especiales?			0 = no; 5 = completa
21¿Todo el personal firma un acuerdo de confidencialidad?			0 = no; 5 = completa
22¿Existen procesos disciplinarios para cuestiones de seguridad?			0 = no; 5 = completa

Tabla 3.1. Organización y políticas de seguridad.

II. Cuestionario para la prevención de seguridad

Este cuestionario tiene la finalidad de conocer el nivel de prevención, educación y actualización del personal de la empresa en el rubro de seguridad. También integra información de su situación actual en lo que se refiere tanto a comunicación vía correo electrónico y comunicados no electrónicos internos, así como la documentación existente en aspectos de seguridad en general. Ver Tabla 3.2.

Pregunta	Actual	Meta	Explicación
1¿Existe un programa de prevención de seguridad?			0 = no; 5 = completa
2¿Existen mediciones de efectividad de seguridad?			0 = no; 5 = completa

Tabla 3.2. Prevención de seguridad.(Continúa)

Pregunta	Actual	Meta	Explicación
3¿Se producen posters de seguridad?			0 = nunca; 2 = una vez; 3 = 2 veces al año; 4 = anualmente; 5 = cada 6 meses
4¿Se emiten regularmente boletines de seguridad?			0 = no; 5 = completa
5¿Se distribuyen objetos?			0 = no; 5 = completa
6¿Existe entrenamiento para usuarios respecto a la prevención?			0 = no; 5 = completa
7¿Qué tan frecuente ocurren estos entrenamientos?			0 = no; 5 = completa
8El entrenamiento cubre:			
8.1. Procesos de reporte			0 = no; 5 = completa
8.2. Virus y software malicioso			0 = no; 5 = completa
8.3. Procedimientos de seguridad física			0 = no; 5 = completa
8.4. Ingeniería social			0 = no; 5 = completa
8.5. Actividad inusual			0 = no; 5 = completa
8.6. Administración de passwords			0 = no; 5 = completa
8.7. Pruebas de marketing vagas			0 = no; 5 = completa
8.8. Teléfono / correo electrónico			0 = no; 5 = completa
8.9. Datos / baja de programas			0 = no; 5 = completa
8.10. Licenciamiento de software			0 = no; 5 = completa
8.11. Respaldos y restauración			0 = no; 5 = completa
9¿Los usuarios saben donde encontrar los estándares y políticas de seguridad?			0 = no; 5 = completa
10¿Hay un programa de prevención para el staff?			0 = no; 5 = completa
11¿El personal va a presentaciones y seminarios de seguridad?			0 = no; 5 = completa
12¿El personal va a cursos externos reconocidos de seguridad?			0 = no; 5 = completa
13Se reciben alertas de seguridad:			
13.1. Alertas del CERT			0 = no; 5 = sí
13.2. Boletines de seguridad de Microsoft			0 = no; 5 = sí
13.3. Alertas de vendedores de seguridad			0 = no; 5 = completa
13.4. Otros			0 = no; 5 = completa
14¿Los usuarios son informados de cualquier monitoreo corporativo que se lleva a cabo?			0 = no; 5 = completa

Tabla 3.2. Prevención de seguridad.

III. Cuestionario para la administración de usuarios

El siguiente cuestionario se encarga de integrar la información correspondiente al control de la administración de los perfiles y roles de los usuarios que utilizan los sistemas o activos dentro de la empresa, así mismo, integra lo correspondiente a la administración de passwords de los mismos. Ver Tabla 3.3.

Pregunta	Actual	Meta	Explicación
1¿Se pueden fácil y rápidamente borrar todas las cuentas de un usuario cuando ellos dejan la organización?			0 = no; 5 = completa
2¿Existe un proceso para manejar las cuentas de los usuarios cuando ellos dejan la organización?			0 = no; 5 = completa
3¿Hay un proceso para manejar adecuadamente los activos asociados con las cuentas cuando han sido suspendidos, borrados o el usuario deja la organización?			0 = no; 5 = completa
4¿Existe una base de datos central de usuarios?			0 = no; 5 = completa
5¿Existe un procedimiento de autorización para agregar nuevos usuarios a los sistemas?			0 = no; 5 = completa
6¿Existen facilidades para la administración de usuarios?			0 = no; 5 = completa
7¿Es dependiente de la localidad?			Información
8¿Es dependiente del sistema?			Información
9¿Es controlado por software?			0 = no; 5 = completa
10 ¿Los usuarios son autentificados por software?			0 = no; 5 = completa
11 ¿La administración de cuentas de usuarios utiliza mecanismos de tiempo (expiración)?			0 = no; 5 = completa
12 ¿Se tienen cuentas compartidas?			0 = no; 5 = no
13 ¿Se tienen cuentas con acceso público o guest?			0 = no; 5 = no
14 ¿Existen estándares para la construcción de user id?			0 = no; 5 = completa
15 ¿Son uniformes en todas las plataformas?			0 = no; 5 = completa
16 ¿Los user id son únicos en la plataforma?			0 = no; 5 = completa
17 ¿Todas las cuentas pueden ser correlacionadas hacia un usuario real?			0 = no; 5 = completa
18 ¿Las cuentas del sistema tienen los passwords por default?			0 = no; 5 = completa
19 ¿Las cuentas administrativas pueden ser asociadas a un usuario real?			0 = no; 5 = completa
20 ¿La política de seguridad se aplica a todo el personal?			0 = no; 5 = completa
21 ¿Los usuarios son administrados por grupos o roles?			0 = no; 5 = completa
22 ¿Los privilegios de acceso de los usuarios son revisados regularmente?			0 = no; 5 = completa
23 ¿Se les pide a los usuarios seguir prácticas de seguridad definidas en la sección de passwords?			0 = no; 5 = completa

Tabla 3.3. Administración de usuarios.(Continúa)

Pregunta	Actual	Meta	Explicación
24 ¿Existe una sincronización de passwords entre las diferentes aplicaciones y plataformas?			Información

Tabla 3.3. Administración de usuarios.

IV. Cuestionario para el control de accesos

El siguiente cuestionario permite conocer el grado de complejidad que la compañía televisora presenta en lo que se refiere a los accesos de servicios y sistemas, combinando desde biométricos, conexiones autorizadas y sistemas asignados a los usuarios autorizados y acreditados. El conocimiento sobre el control, administración y limitación de acceso de los usuarios con jerarquía de supervisor de red, controles de acceso al nivel de código de las aplicaciones de misión crítica de la empresa, es también parte de este cuestionario. Como información adicional al mismo, se hace un sondeo en lo correspondiente a la información de los horarios de uso de los sistemas internos, inhabilitación de aplicaciones, control de acceso a los servidores, redes de datos, cifrado y monitoreo de los mismos. Ver Tabla 3.4.

Pregunta	Actual	Meta	Explicación
1¿Qué métodos de autentificación son empleados?			
1.1. Smartcard			0 = no; 5 = sí
1.2. Token			0 = no; 5 = sí
1.3. Password de una sola vez			0 = no; 5 = sí
1.4. Dispositivos biométricos			0 = no; 5 = sí
1.5. Username / passwords			0 = no; 3 = sí
1.6. Con password			0 = no; 5 = sí
2¿Las terminales son identificadas automáticamente para autentificar la la conexión a localidades específicas?			0 = no; 5 = completa
3¿Existen alarmas mediante las cuales los usuarios puedan ser cohesionados?			0 = no; 5 = sí
4¿Las actividades en computadoras pueden ser asociadas a individuos?			0 = no; 5 = completa
5¿El acceso a los sistemas de negocios es restringido a cada usuario o grupo de usuarios de acuerdo a requerimientos de negocio documentados?			0 = no; 5 = completa
6¿Los administradores están restringidos a iniciar alguna transacción de nivel aplicativo a menos que estén autorizados a realizarlo?			0 = no; 5 = completa

Tabla 3.4. Control de accesos. (Continúa)

Pregunta	Actual	Meta	Explicación
7¿Los usuarios tienen restringido el acceso a los datos más allá del alcance de las aplicaciones?			0 = no; 5 = sí
8¿Los usuarios tienen restringido el acceso a datos y funciones de acuerdo a los requerimientos de la descripción de su trabajo?			0 = no; 5 = completa
9¿Las cuentas privilegiadas de emergencia son revisadas, monitoreadas y controladas?			0 = no; 5 = completa
10¿El acceso a las bitácoras de eventos y del sistema es controlado?			0 = no; 5 = completa
11¿Los intentos fallidos de acceso son restringidos?			0 = no; 5 = completa
12¿Las cuentas son deshabilitadas después de un número predefinido de intentos fallidos?			0 = no; 5 = completa
13¿El acceso a los datos es otorgado bajo la base de privilegios *"need to know"*?			0 = no; 5 = completa
14¿Se puede asegurar la integridad del código y de los binarios de la aplicación?			0 = no; 5 = completa
15¿Existe un procedimiento estándar para los equipos no atendidos?			0 = no; 5 = completa
16¿Existen restricciones por hora y día de la semana para las aplicaciones y servicios sensibles?			0 = no; 5 = completa
17¿Existen tiempos límites para la desactivación de aplicaciones y servicios sensibles en caso de inactividad?			0 = no; 5 = completa
18¿Existe un mensaje de aviso de advertencia antes de cada login?			0 = no; 5 = completa
19¿Existe un mensaje de aviso para desplegar el último login?			0 = no; 5 = completa
Control de acceso a servidores			
20¿Se restringe el acceso de cuentas administrativas a nodos específicos y a la consola del sistema?			0 = no; 5 = completa
21¿El acceso a las utilerías del sistema se encuentra restringido y controlado?			0 = no; 5 = completa
Control de acceso a la red			
22¿Cada usuario es autentificado antes de tener acceso a los servicios de red (archivos e impresoras)?			0 = no; 5 = completa
23¿El tráfico LAN sensible se encuentra cifrado?			0 = no; 5 = completa
24¿El tráfico WAN sensible se encuentra cifrado?			0 = no; 5 = completa

Tabla 3.4. Control de accesos. (Continúa)

Pregunta	Actual	Meta	Explicación
25¿Se encuentra habilitada la seguridad en el correo electrónico?			0 = no; 5 = completa
26¿Los correos electrónicos tienen firmas digitales?			0 = no; 5 = completa
27¿Los correos electrónicos se encuentran cifrados?			0 = no; 5 = completa
28¿Los correos electrónicos son monitoreados?			0 = no; 5 = completa
29¿La seguridad de los Sistemas Operativos de red se encuentra habilitada?			0 = no; 5 = completa
30¿Se utilizan VPN's para usuarios remotos?			0 = no; 5 = sí
31¿Se utilizan VPN's para conexiones seguras entre los sitios de cómputo?			0 = no; 5 = completa
32¿La ruta de una terminal hacia un servidor es controlada por la creación y mantenimiento de una ruta reforzada?			0 = no; 5 = completa
33¿El acceso a los puertos de diagnóstico es controlado de una manera segura?			0 = no; 5 = completa
34¿Las redes se encuentran divididas en dominios lógicos separados?			0 = no; 5 = sí
35¿Las conexiones entre redes tienen controles de ruteo?			0 = no; 5 = completa
36¿Existen identificadores de usuarios genéricos de ruteadores para propósitos administrativos?			0 = no; 5 = completa
37¿Se evita el uso de SNMP para la administración de recursos de red?			0 = no; 5 = sí
Control de acceso Web			
38¿Existen restricciones en la descarga de software de lugares públicos?			0 = no; 5 = completa
39¿Se realiza un registro del software descargado de sitios públicos?			0 = no; 5 = completa
40¿Se revisa la seguridad del sitio Web por recomendaciones del vendedor?			0 = 1 vez; 2 = anualmente; 3 = cada 6 meses; 4 = 3 meses; 5 = mensual
41¿Se prohibe el acceso directo a los datos internos via servicios Web?			0 = no; 5 = completa
42¿Se prohibe el uso de *'includes'* en el Website?			0 = no; 5 = completa
43¿Hay necesidad de cuentas de login en el sitio Web?			0 = no; 5 = sí
44¿Se emplean mecanismos de autentificación robustos para los logins?			0 = password; 5 = Token Físico/Smart- Cards
45¿Se utiliza SSL ú otra forma de cifrado para proteger información sensible del cliente cuando ésta transita por la Web?			0 = no; 5 = completa

Tabla 3.4. Control de accesos. (Continúa)

Pregunta	Actual	Meta	Explicación
46¿Se tienen mecanismos de no repudiación para transacciones basadas en la Web?			0 = no; 5 = completa
47¿Las transacciones de Web utilizan certificados digitales?			0 = no; 5 = completa
Control de Acceso Dial-in			
48¿Se emplean controles dial-back?			0 = no; 5 = completa
49¿Hay un control de los modems conectados a la red?			0 = no; 5 = completa
50¿Existe un segundo mecanismo de autentificación para usuarios dial-up?			0 = no; 5 = completa
51¿Se restringen los servicios disponibles a los usuarios del dial-in?			0 = no; 5 = completa
52¿Se restringen las conexiones con mecanismos de *Caller ID Blocking*?			0 = no; 5 = completa
53¿Se han realizado consideraciones especiales para terceras entidades para el soporte a través de los servicios dial-up?			0 = no; 5 = completa
Control de acceso a bases de datos			
54¿Se encuentra habilitada la seguridad para base de datos?			0 = no; 5 = completa
55¿Se prohibe el acceso a la base de datos con id's a nivel aplicativo?			0 = no; 5 = completa
Control de acceso a Internet			
56¿El acceso a Internet está adecuadamente configurado y monitoreado?			0 = no; 5 = completa
57¿Las conexiones de acceso a Internet son revisadas regularmente?			0 = 1 vez; 2 = anualmente; 3 = cada 6 meses; 4 = 3 meses; 5 = mensual
58¿Existe una política de Internet que describa los tipos de sitios y servicios que los usuarios pueden o no puedan acceder?			0 = no; 5 = completa
59¿Se monitorea el tráfico de Internet?			0 = no; 5 = completa
60¿Los Firewalls son utilizados para reforzar las políticas de Internet?			0 = no; 5 = completa
61¿Se emplean DMZ's para alojar servers públicos?			0 = no; 5 = completa
62¿Se tiene una DMZ con uno o dos Firewalls?			0 = 1; 5 = 2
63¿Se utilizan sistemas de inspección de contenido para reforzar las políticas de seguridad de Internet?			0 = no; 5 = completa
64¿La red interna está particionada con Firewalls?			0 = no; 5 = completa
65¿Hay una auditoría sobre el tráfico de Internet o su uso? (que sitios son visitados)			0 = no; 5 = completa
66¿Se revisan periódicamente las políticas del Firewalls?			0 = 1 vez; 2 = anualmente; 3 = cada 6 meses; 4 = 3 meses; 5 = mensual

Tabla 3.4. Control de accesos. (Continúa)

Pregunta	Actual	Meta	Explicación
67¿Son autentificados los usuarios antes de que puedan accesar a Internet?			0 = no; 5 = completa
68¿Se encuentra restringido el acceso para administrar los Firewalls y software de monitoreo?			0 = no; 5 = completa
69¿Se utilizan mecanismos de autentificación para los usuarios de Internet que accesan a los recursos internos?			0 = no; 5 = completa
70¿La información sensible que transita en Internet se encuentra cifrada?			0 = no; 5 = completa
71¿Se instalan los parches y actualizaciones de software tan pronto como se reciben los avisos?			0 = no; 5 = completa
72¿Todos los sistemas visibles externamente están sujetos a revisiones rigurosas de seguridad?			0 = no; 5 = completa

Tabla 3.4. Control de accesos.

V. Cuestionario para la seguridad física

De este cuestionario obtendremos información crucial para el análisis de vulnerabilidades. Típicamente se cree que la seguridad informática sólo se encarga de evitar los accesos vía red no deseados a la información sensible de la empresa, pero ésta no sería completa si no se cubren también aspectos físicos, por lo que el nivel de efectividad de los equipos de vigilancia que autorizan los accesos a las instalaciones deben formar parte de la misma. La seguridad física llega hasta el nivel de orden y compromiso con el que cuentan todos y cada uno de los empleados dentro de la organización. Así, el portar un gafete con identificación y la cultura de orden en los escritorios forman parte de ésta entre otros rubros. A través de este cuestionario se obtendrá información en lo referente a la existencia de un centro de recuperación ante desastres, éste debe contemplar sistemas UPS, una planta de emergencia eléctrica, y un sitio alterno en donde resguardar la información con la cual opera la empresa. Hoy la información es considerada unos de los activos más importantes de la empresa y es parte de la sobrevivencia de la misma. Ver Tabla 3.5.

Pregunta	Actual	Meta	Explicación
1¿El acceso a las líneas telefónicas analógicas se encuentra restringido?			0 = no hay; 5 = completa
2¿El Firewall se encuentra en un área segura?			0 = no hay; 5 = completa
3¿Existen UPS para proteger los sistemas más sensibles?			0 = no hay; 5 = completa
4¿Se tiene un sistema de poder de emergencia?			0 = no hay; 5 = completa

Tabla 3.5. Seguridad física.(Continúa)

Pregunta	Actual	Meta	Explicación
5¿Se tiene acceso mediante llaves o códigos a los cuartos de los equipos sensibles?			0 = no; 5 = completa
6¿Existen señalamientos en el directorio del edificio que hagan a la localización de los centros de cómputo?			0 = sí; 5 = no
7¿Existen guardias en los puntos de entrada y salida?			0 = no; 5 = completa
8¿Se tienen sistemas especiales para prevención de fuego instalados en los cuartos de cómputo?			0 = no; 5 = completa
9¿Se tienen sistemas de circuito cerrado de televisión para monitorear las áreas sensibles?			0 = no; 5 = completa
10¿El *Site* es manejado en un período de 24 X 7?			0 = no; 5 = completa
11¿Existe una política de escritorio limpio?			0 = no; 5 = completa
Equipo de seguridad			
12¿Existen dispositivos antirrobos empleados para equipos portátiles o PC portables?			0 = no; 5 = completa
13¿Todos los archivos de TI tienen marcas permanentes?			0 = no; 5 = completa
14¿Existe un procedimiento para mover o remover equipos?			0 = no; 5 = completa
Seguridad personal			
15¿Se requiere que todos los empleados lleven identificación todo el tiempo?			0 = no; 5 = sí
16¿Los visitantes son escoltados todo el tiempo?			0 = no; 5 = sí
17¿Se monitorea y controla el trabajo de los empleados después de la hora de la salida?			0 = no; 5 = sí
18¿Se tienen controles para prohibir el acceso en áreas sensibles?			0 = no; 5 = completa
Manejo de cintas de respaldo			
19¿Los medios magnéticos de respaldo son almacenados de acuerdo con las instrucciones del fabricante?			0 = no; 5 = completa
20¿Hay un proceso en operación para documentar y destruir los respaldos basados en la clasificación del contenido?			0 = no; 5 = completa
21¿Existe un almacenamiento seguro para las cintas removibles?			0 = no; 5 = completa
22¿Las cintas removibles se encuentran claramente etiquetadas?			0 = no; 5 = completa
23¿La cinta en tránsito se encuentra protegida de pérdida, daño o acceso no autorizado?			0 = no; 5 = completa

Tabla 3.5. Seguridad física.

VI. Cuestionario para la evaluación de activos

Una de las realidades en lo que se refiere a contemplar un sistema eficiente de seguridad será siempre definir prioridades. Aunque es imposible llegar a un 100% de seguridad en todos los sistemas (ya que esto hace prácticamente inoperable a cualquier red), si es importante el tratar de cubrir al máximo aquellos activos con mayor sensibilidad para la empresa. La valuación de los activos se convierte en algo de extrema importancia. Esta valuación también permite definir el presupuesto que se va a asignar a este rubro, el cual obviamente será diferente para cada empresa. Así mismo, esta información permitirá poder justificar ante las instancias de administración y finanzas el riesgo de no invertir en un sistema de seguridad. El inventario y la valuación de activos es un punto a contemplar y que forma parte de las metodologías más comunes, entre ellas el BS7799. El siguiente cuestionario nos permitirá sondear todos estos aspectos. Ver Tabla 3.6.

Pregunta	Actual	Meta	Explicación
1¿Existe un inventario para los activos de TI?			0 = no hay; 5 = completa
2¿Existen clasificaciones de seguridad para la información?			0 = no hay; 5 = completa
3¿Existe una persona designada para la contabilidad de cada activo?			0 = no hay; 5 = completa
4Se ha evaluado el impacto de cada activo en términos de:			
4.1. Pérdida de confidencialidad			0 = no; 5 = completa
4.2. Pérdida de disponibilidad			0 = no; 5 = completa
4.3. Pérdida de integridad			0 = no; 5 = completa
5¿Se ha producido una lista de activos fijos?			0 = no; 5 = completa
6¿Se ha realizado un estudio de dependencia de los activos?			0 = no; 5 = completa
7¿Éstos se realizan regularmente?			0 = nunca; 2 = una vez; 3 = anualmente; 4 = cada 6 meses; 5 = cada 3 meses

Tabla 3.6. Evaluación de activos.

VII. Cuestionario para el análisis de seguridad

Sería irresponsable en la implementación de un sistema de seguridad de datos el no contemplar, previo al mismo, un Análisis de Vulnerabilidades o *Risk Assesment*. El no hacerlo pudiera repercutir en la implementación de un sistema no efectivo y por tanto en una inversión no redituable para la empresa. A partir del análisis de vulnerabilidades se pueden empezar a definir las políticas de seguridad de la empresa, y con el mismo, se pueden integrar los sistemas de administración y mantenimiento de las mismas políticas. Un sistema de seguridad de datos y sus políticas puede llegar a ser muy dinámico, y este dinamismo dependerá de los cambios que viva la empresa en el tiempo. Este cuestionario nos permitirá conocer la situación de la empresa televisora en lo que refiere a estos puntos. Ver Tabla 3.7.

Pregunta	Actual	Meta	Explicación
1¿Existe un análisis de seguridad de la empresa formal y documentado?			0 = no hay; 5 = completa
2¿Existe una metodología de Risk Assessment formal?			0 = no hay; 5 = completa
3¿El Risk Assessment identifica las amenazas, vulnerabilidades e impactos?			0 = no; 5 = completa
4¿Se modifica el Risk Assessment cuando ocurre un cambio en el sistema?			0 = nunca; 2 = una vez; 3 = anualmente; 4 = cada 6 meses; 5 = cada 3 meses
5¿Se tiene una estrategia de administración del riesgo?			0 = no; 5 = completa
6¿Se revisa regularmente la estrategia de administración de riesgo?			0 = nunca; 2 = una vez; 3 = anualmente; 4 = cada 6 meses; 5 = cada 3 meses
7¿Todas las áreas dentro de la organización son sujetas a entrevistas regulares para determinar el nivel de cumplimiento de las políticas de seguridad?			0 = nunca; 2 = una vez; 3 = anualmente; 4 = cada 6 meses; 5 = cada 3 meses

Tabla 3.7. Análisis de seguridad.

VIII. Cuestionario para el análisis de continuidad de negocio

Por medio de este cuestionario obtendremos información en el rubro de continuidad de negocio. El sistema de seguridad a implementar tiene como objetivo mantener a la empresa televisora en operación. Este cuestionario integrará información sobre los acuerdos de niveles de servicio entre el área de tecnología de información y los diversos departamentos de la empresa, en lo referente a los procedimientos para la resolución de incidentes de seguridad y pruebas de los mismos, así como también la verificación de procedimientos de los sistemas de respaldo y restauración de información de la empresa. Ver Tabla 3.8.

Pregunta	Actual	Meta	Explicación
1¿Existe un plan de continuidad del negocio?			0 = no hay; 5 = completa
2¿Existe un proceso especifico que cubra los activos más valiosos?			0 = no hay; 5 = completa
3¿En caso de interrupción en el servicio, éste es investigado?			0 = no; 5 = completa
4¿Se tienen acuerdos de niveles de servicios con terceras entidades?			0 = no; 5 = completa
5El procedimiento de respuesta a incidentes contempla:			
5.1. Prevención			0 = no; 5 = completa
5.2. Detección			0 = no; 5 = completa
5.3. Contención			0 = no; 5 = completa
5.4. Remedio			0 = no; 5 = completa
5.5. Retorno a operación normal			0 = no; 5 = completa

Tabla 3.8. Continuidad del negocio.(Continúa)

Pregunta	Actual	Meta	Explicación
6¿Se prueba el procedimiento de respuesta a incidentes?			0 = nunca; 2 = una vez; 3 = anualmente;4 = cada 6 meses; 5 = cada 3 meses
7¿Se tiene más de un carrier de telecomunicaciones para TI?			0 = no; 5 = completa
Respaldo y recuperación			
8¿Los procedimientos de recuperación son verificados continuamente?			0 = nunca; 2 = una vez; 3 = anualmente; 4 = cada 6 meses; 5 = cada 3 meses
9¿Se emplean facilidades de backup off-site?			0 = no; 5 = completa
10¿Se realizan respaldos en línea con los datos críticos de los sistemas de información?			0 = no; 5 = completa

Tabla 3.8. Continuidad del negocio.

IX. Cuestionario para el análisis de auditoría

La información que integrará este cuestionario nos ayudará a verificar la habilidad que tiene la empresa televisora en el manejo sus auditorías. Las auditorías sirven para verificar el buen funcionamiento y uso del sistema, por lo que bien utilizadas, siempre son de gran ayuda, pudiendo llegar incluso -en el caso de cualquier violación a las normas de seguridad- detectar al usuario infractor. Para llevar a cabo una auditoría eficiente es necesaria la integración de información de los sistemas y elementos de seguridad en consolas centrales para el monitoreo de la red. Analizar este tipo de información también permite ajustar o crear nuevas políticas para la empresa. La integración de los diferentes eventos de seguridad y la correlación de los mismos son cruciales para los responsables de la auditoría de sistemas. Ver Tabla 3.9.

Pregunta	Actual	Meta	Explicación
1¿La información es archivada para uso en procedimientos legales?			0 = no hay; 5 = completa
2¿Se pueden rastrear las transacciones desde el inicio hasta el final?			0 = no; 5 = completa
3¿Se mantienen las auditorías de los eventos de seguridad?			0 = no; 5 = completa
4¿Se generan alertas de seguridad al detectar una brecha de seguridad?			0 = no; 5 = completa
5¿Las alertas de seguridad son monitoreadas centralmente?			0 = no; 5 = completa
6¿Las bitácoras son revisadas frecuentemente en busca de actividad sospechosa?			0 = nunca; 3 = manualmente; 5 = automáticamente
7¿Se encuentra sincronizado el tiempo en los sistemas?			0 = no; 5 = completa

Tabla 3.9. Análisis de auditoría.

X. Cuestionario para el análisis del ambiente aplicativo

La vigilancia de aplicaciones internas en cualquier empresa es en la mayoría de las veces una labor la cual se descuida, a pesar de ser parte, y en la mayoría de las veces, de los activos más sensibles y críticos de la empresa. Por medio de este cuestionario se obtendrá información en lo referente a los procedimientos actuales que la compañía televisora presenta. Para el mantenimiento y actualización de estos sistemas es crucial el control de cambios de los mismos y de las versiones generadas. Con esta información complementaremos nuestras recomendaciones en lo que refiere a seguridad para la empresa televisora. Ver Tabla 3.10.

Pregunta	Actual	Meta	Explicación
Desarrollo de aplicaciones			
1¿La entrada de datos en los sistemas aplicativos es válida para asegurar que sea correcta?			0 = no; 5 = completa
2¿Los datos procesados (salida) por los sistemas aplicativos son validados para asegurar que sean correctos?			0 = no; 5 = completa
Administración de cambios			
3¿Existe una administración de cambios para cualquier modificación en el software? 3.1. PC's 3.2. Servidores de red 3.3. Aplicaciones			 0 = no; 5 = completa 0 = no; 5 = completa 0 = no; 5 = completa
4¿Existe un ambiente de producción y pruebas separados para preservar la integridad de los datos productivos?			0 = no; 5 = completa
5¿Existe un procedimiento para asegurar que las nuevas aplicaciones cumplan con los requerimientos de seguridad (incluyendo el software que se obtiene a través del Internet)?			0 = no; 5 = completa
6¿Existe un procedimiento para asegurar que los nuevos sistemas cumplan con los requerimientos de seguridad?			0 = no; 5 = completa
7¿Existe un procedimiento formal de control de cambios para todas las etapas del ciclo de vida de un desarrollo de sistemas?			0 = no; 5 = completa

Tabla 3.10. Análisis del ambiente aplicativo.

Respuestas a los cuestionarios

La Tabla 3.11. muestra los resultados de la encuesta practicada al Director de Sistemas, mientras que la Tabla 3.12. contiene las respuestas del Gerente de Seguridad Informática. El resultado de cada respuesta se encuentra justo al frente

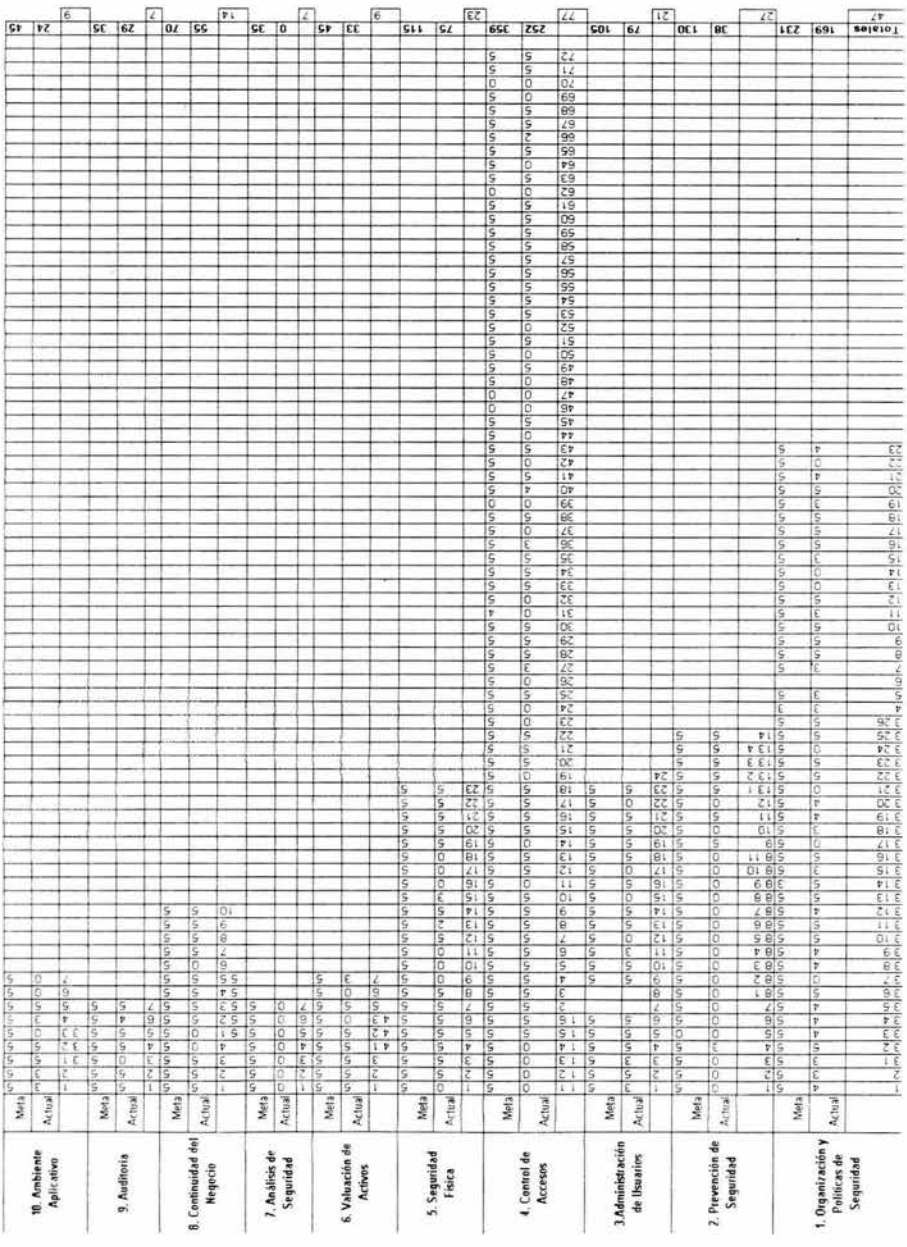


Tabla 3.11. Respuestas ofrecidas por el Director de Sistemas.

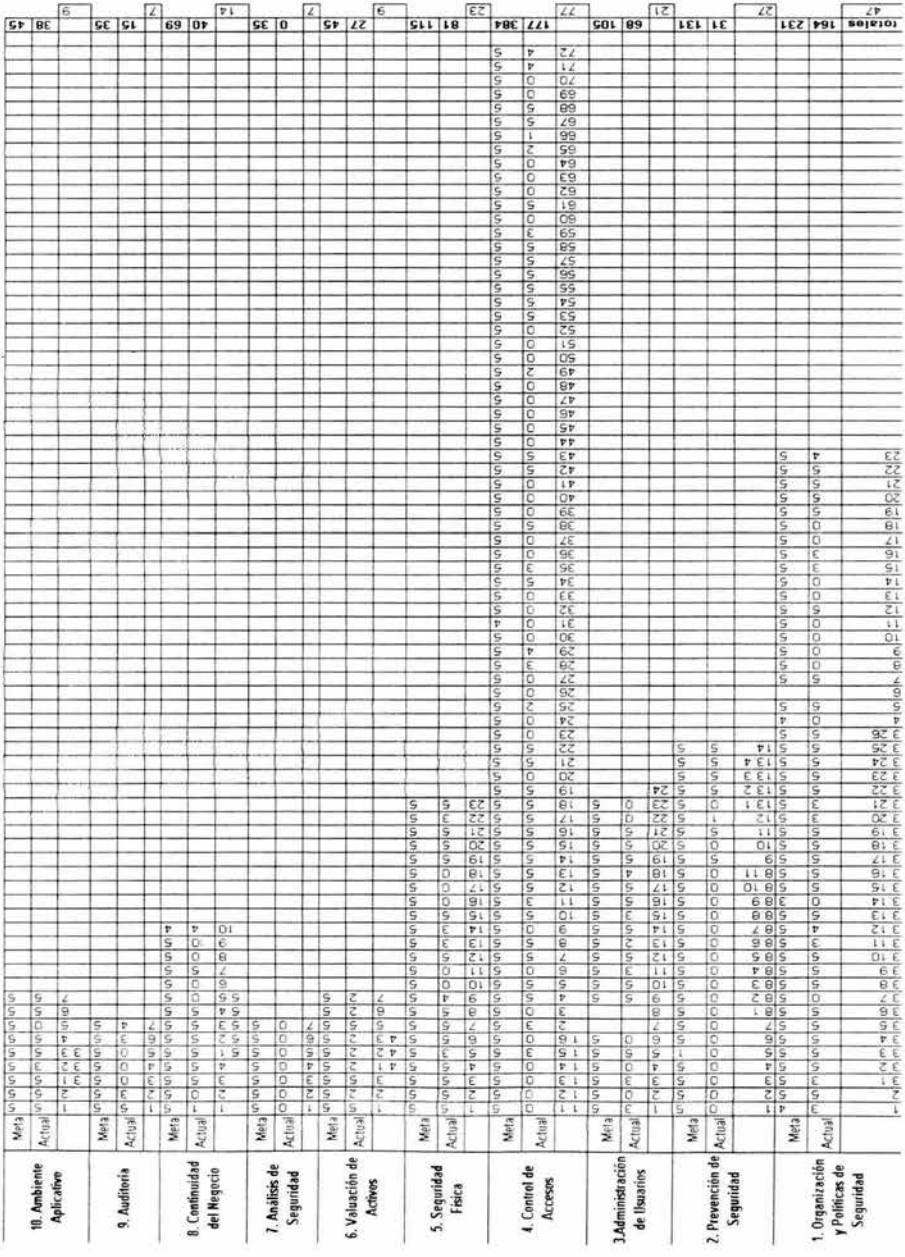


Tabla 3.12. Respuestas ofrecidas por el Gerente de Seguridad Informática .

de su propia pregunta, así como también el cuestionario al que pertenecen. Se utilizó una ponderación o calificación que va desde 0 (Nula) a un 5 (Total o completa) a cada una de las respuestas, pidiendo que cuando no fuera el caso de una respuesta 0 o 5, se indique la solución con un número entero. Se tienen excepciones, en las cuales en algunas preguntas se solicitó una respuesta verbal y carente de calificación, pero que sirven para la obtención de la solución de seguridad a implementar. También se piden respuestas concretas cuya calificación se da de acuerdo a la respuesta, quedando a criterio del propio entrevistado la mejor ubicación a dicha respuesta. En estas tablas se presenta también un valor meta, que representa el valor ideal a alcanzar. Este valor no se especifica en los cuestionarios anteriores para no condicionar la respuesta del entrevistado.

3.4. Integración y correlación de la información

La Tabla 3.13. muestra los porcentajes obtenidos de las respuestas ofrecidas por el Director de Sistema y el Gerente de Seguridad en los cuestionarios. En la primera columna se tienen el número de preguntas que se realizaron, seguido de la calificación obtenida por la suma de puntos de todas las respuestas a cada uno de los cuestionarios. Al lado se tiene el valor meta esperado. En la columna siguiente se calcula el porcentaje del promedio de cada una de las respuestas por cuestionario. Esto con el fin de poder ver que tan cerca se encuentran las respuestas del valor esperado. Le sigue el porcentaje meta, el cual nos dice que tan cerca nos encontramos del valor ideal de un sistema de seguridad funcional. Los promedio de ambos resultados se pueden ver al final de la tabla y nos sirven para darnos una muy clara idea de cómo se encuentra la compañía en lo referente a su seguridad informática, detectando cuales son los puntos más vulnerables a los cuales se les prestará mayor atención. Es importante mencionar -como se puede ver en la columna "Promedio Meta"- que en algunos casos no será necesario cubrir el 100% de las expectativas, esto es debido a la gran cantidad de medidas preventivas que se deberán tomar para la solución del apartado en cuestión.

3.4.1. Expresión gráfica de los resultados

En la Figura 3.3. se muestran los componentes clave de seguridad que pudieran afectar la protección de los activos más valiosos de la empresa.

Al Director de Sistemas y al Gerente de Seguridad se les solicitó ponderar la importancia de esos componentes para la empresa, así como la efectividad actual de los procesos y herramientas de soporte. La diferencia entre la importancia y la efectividad de cada componente indica el rendimiento logrado. Las diferencias más grandes serán las que tendrán una mayor prioridad para iniciar las acciones apropiadas.

	Preguntas	Director de Sistemas	Meta	Porcentaje Pregunta	Porcentaje Meta	Gerente de Seguridad	Meta	Porcentaje Pregunta	Porcentaje Meta	Promedio Respuestas	Promedio Meta	Promedio Preguntas	Meta
1. Organización y Políticas de Seguridad	47	169	231	72%	73%	164	231	70%	71%	166.5	231	71%	98%
2. Prevención de Seguridad	27	38	130	28%	29%	31	131	23%	24%	34.5	130.5	26%	97%
3. Administración de Usuarios	21	79	105	75%	75%	68	105	65%	65%	73.5	105	70%	100%
4. Control de Acceso	77	252	359	65%	70%	177	384	46%	46%	214.5	371.5	56%	96%
5. Seguridad Física	23	75	115	65%	65%	81	115	70%	70%	78	115	68%	100%
6. Valuación de Activos	9	33	45	73%	73%	27	45	60%	60%	30	45	67%	100%
7. Análisis de Seguridad	7	0	35	0%	0%	0	35	0%	0%	0	35	0%	100%
8. Continuidad del Negocio	14	55	70	79%	79%	40	69	57%	58%	47.5	69.5	68%	99%
9. Auditoria	7	29	35	83%	83%	15	35	43%	43%	22	35	63%	100%
10. Ambiente Aplicativo	9	24	45	53%	53%	38	45	84%	84%	31	45	69%	100%

Promedio General	66%

Tabla 3.13. Porcentajes de las respuestas a los cuestionarios.

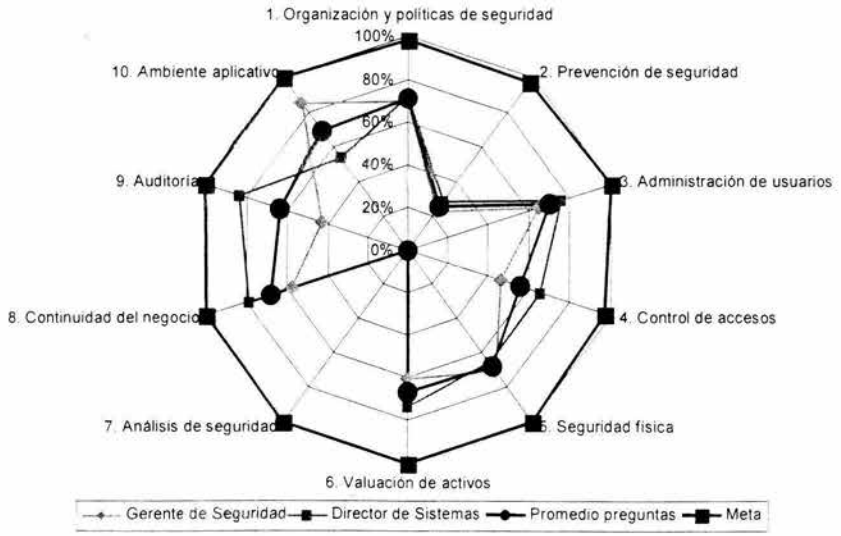


Figura 3.3. Gráfica de rendimiento de seguridad empresarial relativa.

3.5. Análisis y exposición de los resultados

Los siguientes resultados nacen del análisis de la Tabla 3.13. y de la Figura 3.3.

Al realizar el análisis de la información recopilada en la empresa televisora, se deduce que las dos áreas en donde la diferencia entre el estado actual y la meta es mayor son:

2. Prevención de seguridad
7. Análisis de seguridad

Por otro lado, los puntos con menor diferencia entre el estado actual y la meta son:

1. Organización y políticas de seguridad
3. Administración de usuarios

En las áreas donde hay más diferencias entre las percepciones de la seguridad en entre los entrevistados en la empresa televisora son:

8. Continuidad del negocio
9. Auditoría
10. Ambiente aplicativo

Áreas con menores diferencias en las percepciones de la seguridad en la empresa televisora de los entrevistados son:

1. Organización y políticas de seguridad
7. Análisis de seguridad

La diferencia entre el estado actual y la meta promedio que existe es de 56% y eliminando las muestras mas bajas (0 % y 26 %) se obtiene un indicador del 66% promedio general de cumplimiento de la seguridad a primer nivel dentro de la empresa televisora.

Para las respuestas escritas carentes de puntaje, algunos puntos singulares que se decubrieron son:

- No existe una restricción de terminales de las cuentas privilegiadas.
- No hay una revisión constante de privilegios de usuarios.
- No existe una política de escritorio limpio.
- No se han realizado estudios de dependencia de los activos.
- No se mantienen las auditorías de eventos de seguridad.
- Aunque se aplican controles de seguridad, no hay definido un programa para la prevención de seguridad. No hay que olvidar que finalmente lo que nos interesa es proteger la información a la cual tienen acceso los usuarios

de acuerdo a sus roles, y por lo tanto deben tener una cultura para el manejo de información.

- No existe un proceso para realizar un análisis formal de los activos. La empresa televisora tiene inventariados los activos, pero no se tiene un análisis de riesgo de cada uno de ellos.
- No existe un estudio de dependencia de los activos. La falta de estudios de dependencia de los activos es necesaria para tener identificados los servidores y componentes críticos, y evaluar sobre ellos con un mayor detalle la aplicación de políticas de seguridad.

Finalmente se puede observar en la Figura 3.3. que en la mayoría de los casos se tiene una deficiencia promedio en instancias de seguridad de un 30% aproximadamente.

La información resultante de este análisis será utilizada en el siguiente capítulo para el desarrollo de la arquitectura del sistema de seguridad para la compañía televisora mexicana.

CAPÍTULO 4

DISEÑO E IMPLEMENTACIÓN

Tomando como base la información obtenida en el capítulo anterior, en lo referente a la situación de la seguridad de la empresa televisora, se pueden definir claramente las prioridades para las cuales es necesaria dar una solución de seguridad. En el presente capítulo se obtendrá la solución del sistema de seguridad, integrando desde el diseño de la arquitectura, el presupuesto para la implementación, la creación de las políticas y la justificación e implementación del mismo.

4.1. Sistema de seguridad

Con base en los resultados de la gráfica de la Figura 3.3., del capítulo 3, denominada gráfica de rendimiento de seguridad empresarial relativa, basada en la encuesta realizada, se determinó que los rubros que más resaltaron en la misma fueron una baja prevención de seguridad, así como también, la falta de un análisis de seguridad actual de sus sistemas y procesos. Cabe comentar, que el análisis de la seguridad debe ser en toda organización un proceso continuo, por tal razón éste no termina, por lo que debe estar definido como parte de la estrategia corporativa de la empresa televisora.

En lo que refiere a la prevención de la seguridad, como punto prioritario expuesto en los resultados, se deduce la necesidad de implementar un sistema de seguridad ligado a las posibles amenazas que pueda vivir la empresa televisora. Existen otros puntos menos prioritarios, los cuales no se tomarán en cuenta en el diseño de la presente arquitectura, mas su solución se integrará al final de este trabajo como parte de las recomendaciones.

Como parte del rubro correspondiente a la prevención de la seguridad, ya se había validado la existencia de un sistema de respaldo y restauración de datos y sistemas, éste se encuentra en operación y configurado de forma distribuida, utilizando la herramienta de marca *Brighstor* de *Computer Associates*. Ésta realiza respaldos diarios de forma incremental de los servidores de misión crítica y equipos de cómputo de la alta gerencia, sobre estos equipos también se tienen configurados respaldos automáticos semanales de forma diferencial. Estos respaldos se llevan a cabo en horarios nocturnos, todos los viernes para evitar carga en los anchos de banda de la red. Los servidores de misión crítica se

encuentran en la Cd. de México y éstos son: nómina, finanzas, tesorería, bases de datos de videos, producción, servicios Web y correo electrónico.

En lo correspondiente a protección de ataques de virus, el cliente ha venido siendo usuario de la herramienta *Etrust Antivirus* de *Computer Associates*. En el pasado han tenido varios eventos de ataques de virus de diferentes tipos, predominando los gusanos. Esta herramienta hasta ahora ha cubierto las expectativas de la empresa televisora, aunque será necesaria la validación de la configuración del mismo.

Actualmente, todo lo correspondiente a seguridad intrínseca de administración de usuarios y servicios de directorio, se encuentra configurados a nivel del Sistema Operativo *Windows NT*, esto se muestra en los resultados de la Figura 3.3. mostrada en el capítulo 3, correspondientes a la administración de usuarios, control de acceso y ambiente aplicativo, en donde los promedios se encuentran por arriba del un 60%.

La solución deberá constar de la reconfiguración de la arquitectura de hardware actual y la integración de herramientas de software que cubran amenazas tales como intrusiones a los sistemas de misión crítica, robo de información, caídas de sistemas por eventos de DoS y el mal uso de los enlaces de red de la empresa televisora.

4.1.1. Justificación del diseño

La necesidad de herramientas extrínsecas de seguridad se hace más que necesaria después de analizar los resultados de la encuesta. La definición de las herramientas de seguridad extrínsecas se eligió basándose en un modelo de seguridad consolidado y no híbrido. La empresa televisora, bajo recomendación nuestra, tomó la decisión de optar por un sólo fabricante en soluciones de software de seguridad, para aprovechar la integración de las soluciones y eliminar mayores vulnerabilidades por falta de ésta, además de poder tener un solo frente ante un problema de cualquier tipo y reducir la curva de conocimiento de su staff técnico.

Basados en la información recabada de una empresa líder especializada en el análisis de productos de seguridad, *The Butler Group*, se obtuvieron las siguientes figuras y tablas que apoyaron la decisión de integrar una arquitectura consolidada. Recordemos que la empresa televisora busca una solución integral, efectiva, de fácil uso y económica.

The Butler Group considera ocho puntos importantes para la comparación de diversos productos, estos son:

- *Costos operacionales extras*. Además del precio de la compra inicial, se consideran las demandas en los recursos y la inversión financiera adicional para usar la solución eficazmente.

- *Facilidad de uso.* Cuando la administración de la seguridad tiende a ser compleja, debido al tamaño de la red, se debe de considerar que la solución sea amigable, esto es que sea fácil de manejar y mantener.
- *Preconfiguración y reglas.* Estos productos vienen preconfigurados contra ataques específicos. Aquí se analiza que tan completa es esta preconfiguración contra los ataques más conocidos y cuales son las reglas a seguir para cada ataque.
- *Reportes y alertas.* El conocimiento de que un ataque se está realizando es de crucial importancia. Este punto se refiere a la forma y el tiempo en que una alarma es enviada al administrador del sistema.
- *Administración.* Se refiere a la manera en que nuestro producto puede ser actualizado contra nuevas amenazas.
- *Protección contra nuevas amenazas.* Se refiere a los mecanismos que puede adoptar nuestra solución contra nuevas amenazas.
- *Desarrollo.* Considerando la complejidad del sistema a proteger, para este punto se consideran las formas en que la solución puede proteger al sistema de un ataque.
- *Estrategia contra ataques.* Se considera en este punto las estrategias a tomar contra ataques futuros.

Para la elección de un Antivirus, se compararon los tres productos más solicitados en el mercado, *eTrust Antivirus* de *Computer Associates*, *Symantec Antivirus Enterprise Edition 8.5* de *Symantec Corporation* y *McAfee Active Virus Defence de Network Associates*. De la Tabla 4.1. lo primero que salta a la vista es el precio, siendo el producto de *Computer Associates* el más económico. Los siguientes puntos mostrados en la Tabla 4.1. nos dicen que todas estas soluciones se encuentran prácticamente a la misma altura, presentando prácticamente idénticas caracteristicas. *The Butler Group* presenta también gráficas tipo radar para estos productos en las cuales podemos comparar de manera visual los puntos anteriormente explicados

En la Figura 4.1.a. se presenta la solución de *Computer Associates*, teniendo sus puntos fuertes en los costos operacionales extras, administración y desarrollo. Le sigue la solución de *Network Associates*, Figura 4.1.b., presentando las mejores caracteristicas que se esperan para este tipo de soluciones. La valuación nos dice que *McAfee Active Defence* es el mejor producto en la rama de Antivirus. Para la solución de *Symantec Corporation*, Figura 4.1.c., los puntos fuertes son: reportes y alertas, protección ante nuevas amenazas y su desarrollo.

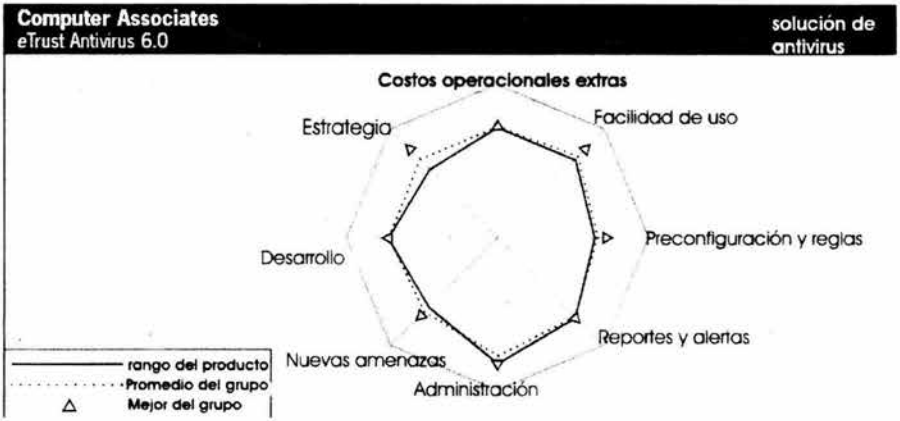
La compañía televisora ya contaba con una solución Antivirus, que resultó ser la presentada por *Computer Associates*. Como se mencionó anteriormente, ya se tenian antecedentes de ataques por virus, los cuales fueron controlados de manera efectiva por el producto *eTrust Antivirus*. Este antecedente es importante, ya que nos dice que el personal que labora en la compañía televisora se encuentra familiarizada con esta solución y la opinión que se tiene de este producto -en cuanto a su servicio- es calificada como buena por parte del cliente.

Comparación de soluciones Antivirus. The Butler Group 2003.		*Computer Associates. eTrust Antivirus 6.0.*	*Network Associates. McAfee Active Virus Defence.*	*Symantec Corporation. Symantec Antivirus Enterprise Edition.*
Fuera de la caja		SÍ	SÍ	SÍ
Costo	Por 1000 usuarios	EU$35,000	£41,000	EU$48,450
Esfuerzo administrativo		Moderado	Moderado	Moderado/alto
Licencias	Suscripción	NO	SÍ	NO
	Perpetua	SÍ, con descuentos por volumen	SÍ	SÍ, descuentos por volumen
	Anual	NO	NO	NO
Soporte	Ajustado según costo	SÍ	SÍ	SÍ
	Estándar 24x7	NO	NO	NO
Consola Central de manejo		SÍ	SÍ	SÍ
Especificación de hardware		Moderado	Moderado	Moderado
Servidor dedicado		Recomendado	Recomendado	Recomendado
Productos Adicionales		SÍ, administración	SÍ	SÍ
Protección	Computadora de usuario	SÍ	SÍ	SÍ
	Servidor de archivos	SÍ	SÍ	SÍ
	Servidor de grupo de trabajo	SÍ	SÍ	SÍ
	Compuerta	SÍ	SÍ	SÍ
Facilidad de uso		Buena	Buena	Buena
Actualizaciones	Manual	NO	SÍ	SÍ
	Automática	SÍ	SÍ	SÍ
Control del tamaño de las descargas		Buena	Buena	Regular

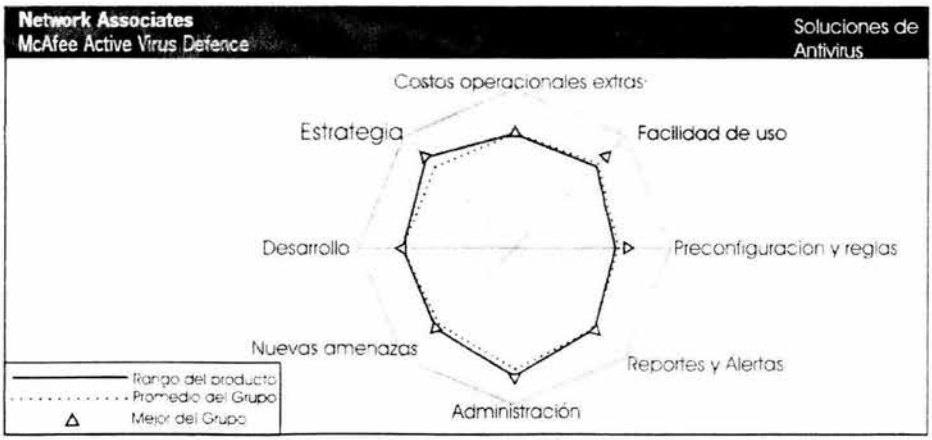
Tabla 4.1. Comparación de productos por fabricante de AV.(Continúa)

Comparación de soluciones Antivirus. The Butler Group 2003.		*Computer Associates. eTrust Antivirus 6.0.*	*Network Associates. McAfee Active Virus Defence.*	*Symantec Corporation. Symantec Antivirus Enterprise Edition.*
Actualización digitalmente firmadas		SÍ	SÍ	SÍ
Reglas Propias	Escribe reglas propias	NO	NO	NO
	Asistente de reglas	NO	NO	NO
Opciones de interacción de usuarios finales		Controlado	Controlado	Controlado
Reportes	Medio de reporte	Varios	Adecuado	Varios
	Opciones de reporte	Detallado	Detallado	Regular, o detallado con costo extra
Discriminación entre amenazas	Respuestas Configurables	SÍ	SÍ	SÍ
Respuesta automatizada		SÍ, Buena	SÍ, Buena	SI, alta calidad
Procedimientos de escalamiento		SÍ	SÍ	SÍ
Número de usuarios potenciales		No especificado	250.000	No especificado
Integración con productos de la competencia		NO	SÍ	SÍ
Soporte de plataformas		Extensiva	Sólo Productos de Microsoft	Sólo Productos de Microsoft
Funcionamiento modular		SÍ	SÍ	SÍ
Dispositivo remoto de monitoreo de ordenes		SÍ	SÍ	SÍ
Alertas de usuario configurables		SÍ	SÍ	SÍ
Almacenaje de reportes de eventos	Tiempo Real	SÍ	SÍ	SÍ
Facilidades de investigación 24x7		SÍ	SÍ	SÍ
Certificación	ICSA	SÍ	SÍ	SÍ

Tabla 4.1. Comparación de productos por fabricante de AV.

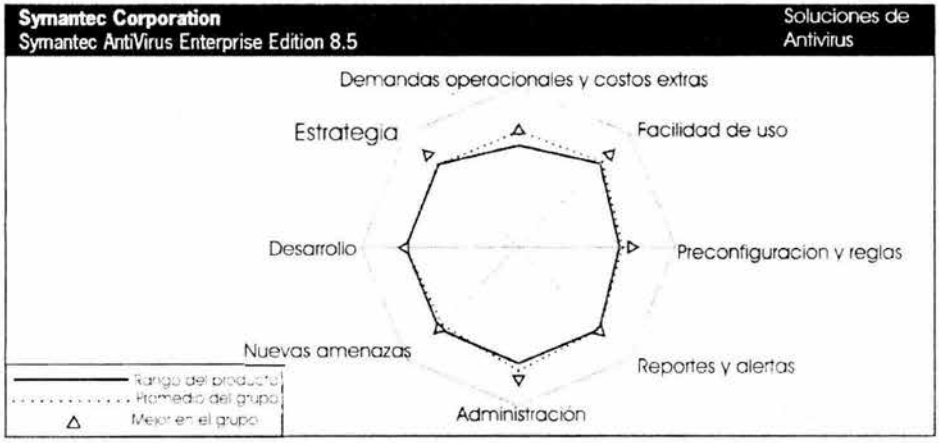


a) Solución Antivirus de Computer Associates.



b) Solución de Antivirus McAfee Active Virus Defence.

Figura 4.1. Productos Antivirus más reconocidos del mercado.(Continúa)



c) Solución Antivirus de Symantec Corporation.

Figura 4.1. Productos Antivirus más reconocidos del mercado.

Para la elección de un Sistema Detector de Intrusos o IDS, consideraremos la Tabla 4.2., proporcionada también por *The Butler Group*. Se comparan los siguientes productos: *Cisco Systems Inc.*, con *Cisco IDS 4210; Computer Associates*, con *eTrust Intrusion Detections 2.0; Entercept Security Technologies*, con *Entercept 2.5* y *Open Source Software*, con *Snort*. La primera diferencia notoria la tenemos en el esfuerzo administrativo, donde el producto *Snort* demanda un alto conocimiento de la herramienta, mientras que *Cisco IDS 4210* demanda un esfuerzo moderado, y en los productos restantes el esfuerzo es bajo. *Snort* no cuenta con una consola central de manejo, mientras que los restantes productos sí. Tanto *Cisco Systems Inc.* como *Entercept Security Technologies* presentan productos adicionales o complementarios para un mejor funcionamiento de su producto. Todos estos productos pueden escribir reglas propias y sólo *Cisco Systems Inc.* proporciona un asistente para el desarrollo de reglas. Los productos *eTrust Intrusion Detection 2.0* y *Entercept 2.5* presentan un mayor número de mecanismos de alerta, siendo este punto muy importante, ya que un conocimiento rápido del problema se traduce en una rápida respuesta para mantener al sistema y a la compañía en funcionamiento. Todos los productos menos *Cisco Systems Inc.* presentan alertas configurables. Se tiene una buena actualización de firmas para nuevos ataques en los productos de *Computer Associates* y *Entercept Segurity Technologies*, siendo el mejor en este punto el producto de *Snort*. Para el seguimiento de auditorías los productos *eTrust Intrusion Detection 2.0* y *Entercept 2.5* no requieren de software adicional.

The Butler Group presenta también para estos productos cuatro figuras que muestran de forma gráfica su funcionamiento, en comparación con el resto de los productos. La Figura 4.2.a. presenta la solución de *Computer Associates*,

mostrando como puntos fuertes su facilidad de uso, el manejo de reportes y alertas, su administración, su prevención ante nuevas amenazas y desarrollo. Para la solución de *Cisco Systems Inc.* se tienen costos extras y mayor número de demandas para su manejo, el equipo viene preconfigurado, presentando un alto grado de desarrollo y estrategia. Para *Entercept Segurity Technologies*, se tiene una mayor demanda operacional junto con un costo en productos extras, es fácil de usar, presenta buenos reportes y alertas, una buena administración, desarrollo y prevención contra nuevas amenazas. Esta última es una muy buena solución, pero su gran desventaja es que no cuenta con soporte técnico local a través del fabricante. Para *Open Source* software se tiene también una alta demanda operacional y costos extras, es difícil de usar, siendo su punto fuerte el desarrollo que el producto presenta.

Comparación de soluciones IDS. The Butler Group 2003.		*Cisco Systems, Inc. Cisco IDS 4210.*	*Computer Associates. eTrust Intrusion Detection 2.0.*	*Entercept Security Technologies. Entercept 2.5.*	*Open Source Software. Snort.*
Fuera de la caja		SÍ	SÍ	SÍ	Descarga
Tipo	Basado en red	SÍ	SÍ	Si se requiere	SÍ
	Basado en Host	NO	NO	NO	NO
Aparato		SÍ	NO	NO	NO
Costo	Aparato	US$7,995	Información no disponible	Información no disponible	Información no disponible
	Software	Incluido en el aparato	US$25,000	£2,995 consola central £895 por servidor	gratis
Censores múltiples o únicos		Múltiples	Múltiples	Múltiples	Múltiples
Licencias	Licencia Pública General (GPL)	Información no disponible	Información no disponible	Información no disponible	SÍ
	Perpetua	NO	SÍ	SÍ	Información no disponible
	Evento Único	SÍ	NO	NO	Información no disponible
Esfuerzo Administrativo		Moderado	Bajo	Bajo	Alto
Soporte	Mediante revendedor Europeo	SÍ	NO	NO	Información no disponible

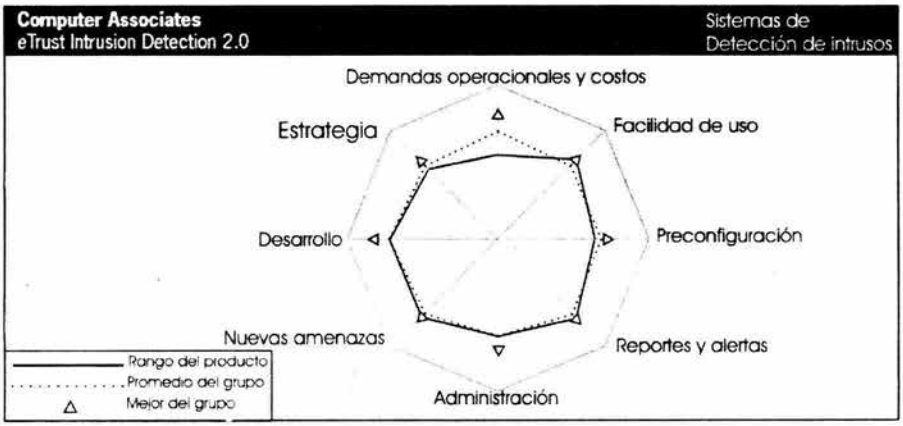
Tabla 4.2. Comparación de soluciones de IDS.(Continúa)

Comparación de soluciones IDS. The Butler Group 2003.		*Cisco Systems, Inc. Cisco IDS 4210.*	*Computer Associates. eTrust Intrusion Detection 2.0.*	*Entercept Security Technologies. Entercept 2.5.*	*Open Source Software. Snort.*
soporte	Foro en línea	NO	NO	NO	SÍ
	Adaptable al costo	NO	SÍ	NO	Información no disponible
	Porcentaje del costo original	NO	NO	25%	Información no disponible
Interfaz	GUI	SÍ	SÍ	SÍ	NO
	Línea de comandos	NO	NO	NO	SÍ
Consola Central de manejo		SÍ	SÍ	SÍ	NO
Especificación de Hardware		Información no disponible	Moderado	Moderado	Poca
Productos Adicionales		SÍ	NO	SÍ	NO
Facilidad de uso		Buena	Buena	Buena	Requiere experiencia
Actualizaciones	Cifrada	SÍ	SÍ	SÍ	NO
	Firmada Digitalmente	NO	NO	NO	SÍ
Control del tamaño de las descargas		Buena	Buena	Buena	Regular
Reglas Propias	Escribe reglas propias	SÍ	SÍ	SÍ	SÍ
	Asistente de reglas	SÍ	NO	NO	NO
Mecanismos de Alertas	Página	SÍ	SÍ	SÍ	NO
	Correo Electrónico	SÍ	SÍ	SÍ	NO
	Teléfono	SÍ	SÍ	SÍ	NO
	Ventanas de Windows	NO	NO	NO	SÍ
	Otros formatos	NO	SÍ	SÍ	NO
Plataformas soportadas		Varias	Varias	Windows, Sun Solaris	Extensiva
Alertas de usuario configurables		NO	SÍ	SÍ	SÍ
Almacenaje de reportes de eventos	Local, directo a consola	SÍ	NO	NO	NO
	Definido por el administrador	NO	SÍ	SÍ	SÍ
Identifica tipos de ataques		SÍ	SÍ	SÍ	SÍ

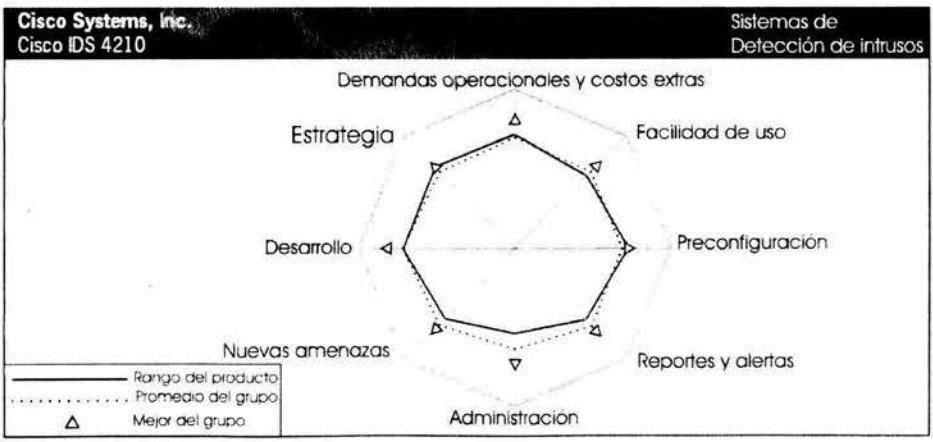
Tabla 4.2. Comparación de soluciones de IDS.(Continúa)

Comparación de soluciones IDS. The Butler Group 2003.		*Cisco Systems, Inc. Cisco IDS 4210.*	*Computer Associates. eTrust Intrusion Detection 2.0.*	*Entercept Security Technologies. Entercept 2.5.*	*Open Source Software. Snort.*
Actualización de firmas de nuevos ataques	Frecuente	Información no disponible	SÍ	SÍ	Información no disponible
	Base a la demanda	SÍ	NO	NO	NO
	Constate	NO	NO	NO	SÍ
Regla: "Permitir todo"		SÍ	NO	SÍ, pre configurado	NO
Capacidad de correlación		NO	SÍ	NO	NO
Procedimientos de escalamiento		SÍ	SÍ	SÍ	NO
Software de reporte adicional		NO	SÍ	SÍ	NO
Protocolos monitoreados	TCP/IP	SÍ	SÍ	SÍ	SÍ
	Aplicación	SÍ	SÍ	SÍ	SÍ
Entrenamiento	Disponible por el vendedor	SÍ	SÍ	SÍ	Información no disponible
	Documentado en línea	Información no disponible	Información no disponible	Información no disponible	SÍ
Seguimiento de auditorías	Incluido	NO	SÍ	SÍ	NO
	Herramientas de un tercero	SÍ	Información no disponible	Información no disponible	Información no disponible
Clasificación por prioridades		SÍ	SÍ	SÍ	SÍ
Dispara respuesta en otro sistema	Firewall de CISCO	SÍ	NO	NO	SÍ
	Computer Associates	NO	SÍ	NO	NO
	Check Point	NO	SÍ	SÍ	SÍ
	Compatible con OPSEC	NO	SÍ	SÍ	NO
Modo de operación "ciego"		NO	SÍ	NO	SÍ

Tabla 4.2. Comparación de soluciones de IDS.

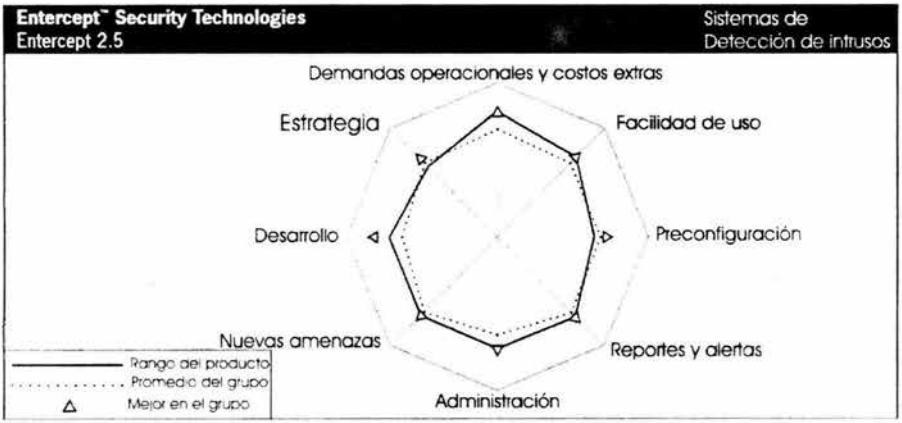


a) Solución IDS de Computer Associates.

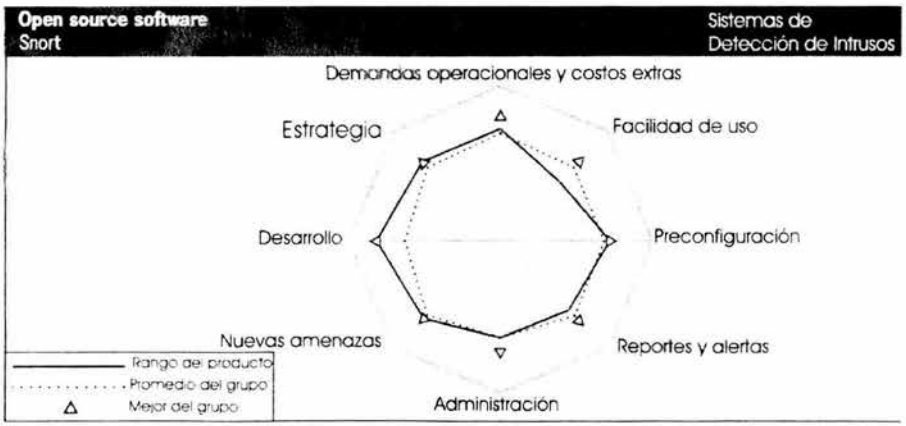


b) Solución IDS de Cisco Systems.

Figura 4.2. Productos IDS más reconocidos en el mercado.(Continúa)



c) Solución IDS de Entercept Security Technologies.



d) Solución IDS de Open Source Software.

Figura 4.2. Productos IDS más reconocidos en el mercado.

Para una solución de tipo consolidado es necesario conocer, además de las características de cada producto, que otras soluciones presentan las diversas compañías especializadas en seguridad. En la Tabla 4.3. se puede observar un portafolio de productos de las compañías líderes en la esta rama, la cual nos da una muy buena referencia de la capacidad de cada compañía para desarrollar una solución con un sistema consolidado de seguridad.

Área de Solución.	*Computer Associates.*	*Network Associates.*	*Symantec.*	*IBM/Tivoli.*	*Check Point Software.*	*Otro.*
Protección Antivirus	Inoculate/T (eTrust Antivirus)	McAfee VirusScan	Norton AntiVirus	Norton AntiVirus	No hay Solución	Sophos Anti-Virus Trend Micro OfficeScan
Antivirus para Equipos Inalámbricos/PDA	Inoculate/T for Windows CE Inoculate/T for Palm OS (eTrust Antivirus)	McAfee VirusScan Wireless	No hay Solución	Norton AntiVirus	No hay Solución	F-Secure Anti-Virus for EPOC
Antivirus para Aplicaciones GroupWare	Inoculate/T (eTrust Antivirus) MS-Exchange Option Lotus Notes Option	McAfee GroupShield Exchange McAfee GroupShield Domino	Norton AntiVirus for Microsoft Exchange Norton AntiVirus for Lotus Notes	Norton AntiVirus	No hay Solución	Sophos Anti-Virus for Notes/Domino Trend Micro ScanMail Sybari Antigen
Antivirus para Gateway	eTrust Content Inspection	McAfee WebShield SMTP McAfee WebShield Proxy McAfee WebShield Solaris	Norton AntiVirus for Gateways Norton AntiVirus for Firewalls	Norton AntiVirus	*OPSEC-Content Vectoring Protocol*	Trend Micro InterScan VirusWall Aladdin eSafe Protect Gateway

Tabla 4.3. Comparación de diversos fabricantes en seguridad.(Continúa)

Área de Solución.	*Computer Associates*	*Network Associates.*	*Symantec.*	*IBM/Tivoli.*	*Check Point Software.*	*Otro.*
Firewall	eTrust Firewall	Gauntlet Firewall	Raptor Firewall VelociRaptor (Appliance)	IBM SecureWay Firewall	Firewall-1	Cisco PIX Firewall Microsoft Proxy Microsoft ISA Server
Firewall Personal o para PC	eTrust Firewall PE	McAfee Firewall	Symantec Desktop Firewall	No hay Solución	No hay Solución	Ositis WinProxy Network ICE BlackICE Defender
Virtual Private Network (VPN)	eTrust VPN	PGP VPN Gauntlet VPN	PowerVPN	IPSec VPN support in IBM SecureWay Firewall, no separate product	VPN-1	F-Secure VPN+ Lucent VPN Gateway
Content Inspection (Malware)	eTrust Content Inspection eTrust Intrusion Detection	McAfee WebShield SMTP McAfee WebShield Proxy McAfee WebShield Solaris	Norton AntiVirus for Gateways Norton AntiVirus for Firewalls	SurfinGate MIMEsweeper	*OPSEC-Content Vectoring Protocol*	Finjan Software SurfinGate Finjan Software SurfinGuard Content Technologies MIMEsweeper
Intrusion Detection Basado en Red	eTrust Intrusion Detection	CyberCop Monitor	NetProwler	No hay Solución	Check Point RealSecure	ISS RealSecure Intrusion.Com SecureNet Pro
Intrusion Detection Basado en Host	eTrust Audit eTrust Access Control	CyberCop Monitor	Intruder Alert	No hay Solución	Check Point RealSecure	ISS RealSecure Intrusion.Com Kane Security Monitor

Tabla 4.3. Comparación de diversos fabricantes en seguridad.(Continúa)

Área de Solución.	*Computer Associates.*	*Network Associates.*	*Symantec.*	*IBM/Tivoli.*	*Check Point Software.*	*Otro.*
Herramientas de Análisis de Riesgo y Vulnerabilidad	*e*Trust Policy Compliance	CyberCop Scanner	Symantec Retriever Symantec Expert NetReconn Enterprise Security Manager	Tivoli SecureWay Risk Manager	No hay Solución	ISS Internet Scanner ISS System Scanner ISS Database Scanner
Solución de Single Sign-On	*e*Trust SSO	No hay Solución	PassGO SSO	Tivoli SecureWay Global Sign-On	No hay Solución	Novell Single Sign-On Entrust Entrust/Sign On
Administración de Usuarios	*e*Trust Admin	No hay Solución	Resource Manager for UNIX	Tivoli SecureWay User Manager	No hay Solución	Systor Security Administration Manager (SAM)
Solución de Control de Accesos	*e*Trust Access Control	No hay Solución	Privilege Manager for UNIX	Tivoli SecureWay Security Manager Tivoli SecureWay Privacy Manager	No hay Solución	Systor Security Administration Manager (SAM)
Seguridad para Aplicaciones y WebServer	*e*Trust Access Control *e*Trust SSO - Web SSO	No hay Solución	Defender Webthority	Tivoli SecureWay Policy Director	No hay Solución	Systor Security Administration Manager (SAM)
Soluciones para Directorio	*e*Trust Directory	No hay Solución	No hay Solución	IBM SecureWay Directory	No hay Solución	Novell NDS iPlanet Directory Server Critical Path InJoin Dir. Server Microsoft Active Directory

Tabla 4.3. Comparación de diversos fabricantes en seguridad.(Continúa)

Área de Solución.	*Computer Associates.*	*Network Associates.*	*Symantec.*	*IBM/Tivoli.*	*Check Point Software.*	*Otro.*
Solución de PKI (Public Key Interface)	*e*Trust Certificate	Net Tools PKI Server	No hay Solución	Tivoli SecureWay PKI	No hay Solución	Baltimore UniCERT Entrust Entrust/PKI RSA Keon Advanced PKI
Herramienta para Certificación de Estado de PKI	*e*Trust OCS Pro	No hay Solución	No hay Solución	No hay Solución	No hay Solución	Valicert

Tabla 4.3. Comparación de diversos fabricantes en seguridad.

Ahora, de la Figura 4.3. podemos ver una gráfica de participación y tendencias del mercado por fabricante, que tiene como fuente a una de los analistas independientes más reconocido a nivel mundial, *IDC Select*, 2001.

Basados tanto en la Tabla 4.3. como en la Figura 4.3., podemos observar que los dos fabricantes más importantes a considerar para la implementación del sistema consolidado de seguridad son *Computer Associates* y *Network Associates*. Ambos presentan una solución para Antivirus, Firewall, Content Inspection, Sistema de Detección de Intrusos y Sistema de detección de vulnerabilidades y riesgos. Estas herramientas son las indicadas para lograr un aseguramiento razonable de la red, apoyado por los resultados de las encuestas hechas en el capítulo anterior.

Comparando productos encontramos que *Netwok Associates* presenta un mejor Antivirus, cuyas ventajas ya se discutieron anteriormente. Para la solución en Firewall, *Network Associates* presenta una buena propuesta, superada sólo por *Computer Associates*, por su interfaz gráfica, lo cual hace fácil la administración del producto. Para la opción de Content Inspection ambas compañías cuentan con variados productos, de parte de *Network Associates* tenemos *McAfee WebShield SMTP, McAfee WebShield Proxy* y *McAfee WebShield Solaris*, todos ellos confiables en su uso pero limitados en su manejo y áreas de protección. *Computer Associates* presenta un producto especializado para este rubro, llamado *eTrust Content Inspection,* y otro que funciona de apoyo, llamado *eTrust Intrusión Detection*. Este segundo producto entra también como solución al siguiente punto, correspondiente a la Detección de Intrusos. *Network Associates* presenta su producto *CyberCop* monitor, el cual cubre de manera satisfactoria este punto en cuanto a intrusiones se refiere. Para el análisis y riesgos de vulnerabilidades *Computer Associates* presenta a *eTrust Policy Compliance* mientras que *Network Associates* presenta a *CiberCop Scanner*. Ambos productos son fáciles de manejar y administrar.

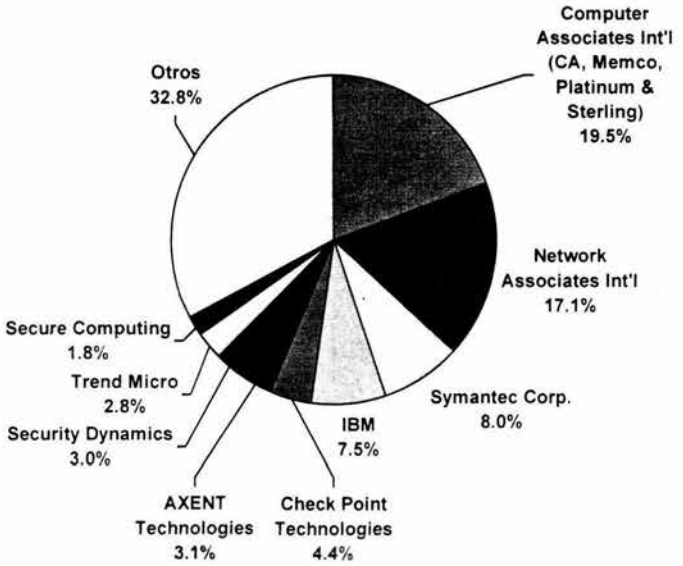


Figura 4.3. Participación y tendencias de mercado por fabricante. (IDC 2001).

Las compañías mencionadas cumplen perfectamente con la solución a implementar, sin embargo se adoptó finalmente a *Computer Associates* como proveedora del software.

Computer Associates cuenta con el portafolio más amplio en el rubro de soluciones de seguridad, con un alto nivel en lo referente a la administración centralizada, facilidad de manejo de los productos, alarmas que indican una actividad anormal del sistema y manejo de inventarios.

Como ventaja extra, para futuras etapas del sistema de seguridad, *Computer Associates* podrá aportar un valor agregado adicional y cubrir necesidades subsecuentes, gracias a que actualmente cuenta con el mayor número de soluciones en lo que a seguridad se refiere.

La empresa televisora estuvo de acuerdo en la elección de este proveedor, ya que contaba con buenos antecedentes de servicio y compatibilidad comercial, esto dado que ya eran usuarios de sus soluciones de respaldo y restauración de datos, además de su solución Antivirus.

4.1.2. Diseño de la arquitectura del sistema de seguridad

Una vez tomada la decisión del portafolio de soluciones de seguridad a implementar, se integró la arquitectura que se observa en la Figura 4.4. Las zonas MZ y DMZ se encuentran definidas por un Firewall utilizando *eTrust Firewall de Computer Associates*. La configuración utilizada integra tres Tarjetas de Red, una de ellas asignada a la DMZ -donde se encuentran el servidor de servicios Web-, otra de ellas hacia la Zona Militarizada -donde se concentran los servidores de misión crítica- y por último la tercer Tarjeta de Red, que conecta a la Intranet en donde se encuentra la red WAN a la cual tienen acceso los empleados, apoyándose en los ruteadores internos *Cisco* ya presentes en la arquitectura de la televisora. No se dispuso de un ruteador exterior por limitante presupuestal. El Firewall se encuentra en un servidor dedicado por la necesidad de procesar grandes frames de información, entre ellos videos que deben ser procesados rápidamente sin afectación de la WAN.

Así también, para la formación de la arquitectura presentada en la Figura 4.4. se están integrando las herramientas de *eTrust Intrusión Detection*, con dos licencias cubriendo los segmentos de red de la zona MZ y DMZ. Con esta herramienta la empresa televisora tendrá la capacidad de monitorear el tráfico de la red, eliminando la posibilidad de ataques DoS tanto internos como externos, así mismo, evitará que información interna confidencial salga a través de Internet, esto lo hará utilizando la funcionalidad de filtrado que integra la misma herramienta. También con el uso de esta misma herramienta se evitará que los empleados usen indiscriminadamente los anchos de banda de red, evitando accesos a sitios no autorizados por la empresa.

Una de las necesidades más importantes de la empresa televisora es el proporcionar servicios Web de forma segura, este servidor se encuentra en la zona DMZ definida en la Figura 4.4. Además de estar cubierta por la herramienta de Detección de Intrusos, el Servidor Web incluye una licencia de *eTrust Policy Compliance*; a través de la funcionalidad de este producto, el servidor será validado continuamente en cuanto a sus vulnerabilidades como host, cubriendo desde el Sistema Operativo de Red *Windows NT*, la base de datos -en este caso *MS SQL Server*- y el servidor de aplicación Web -*WEBSphere* de *IBM*-. Ésta misma herramienta se encargará de verificar los últimos "parches" emitidos por cada uno de los fabricantes de estos sistemas, así como de instalarlos y mantenerlos actualizados en forma automática. De esta forma se mantendrán en operación y disponibilidad los servicios Web implementados por la empresa televisora.

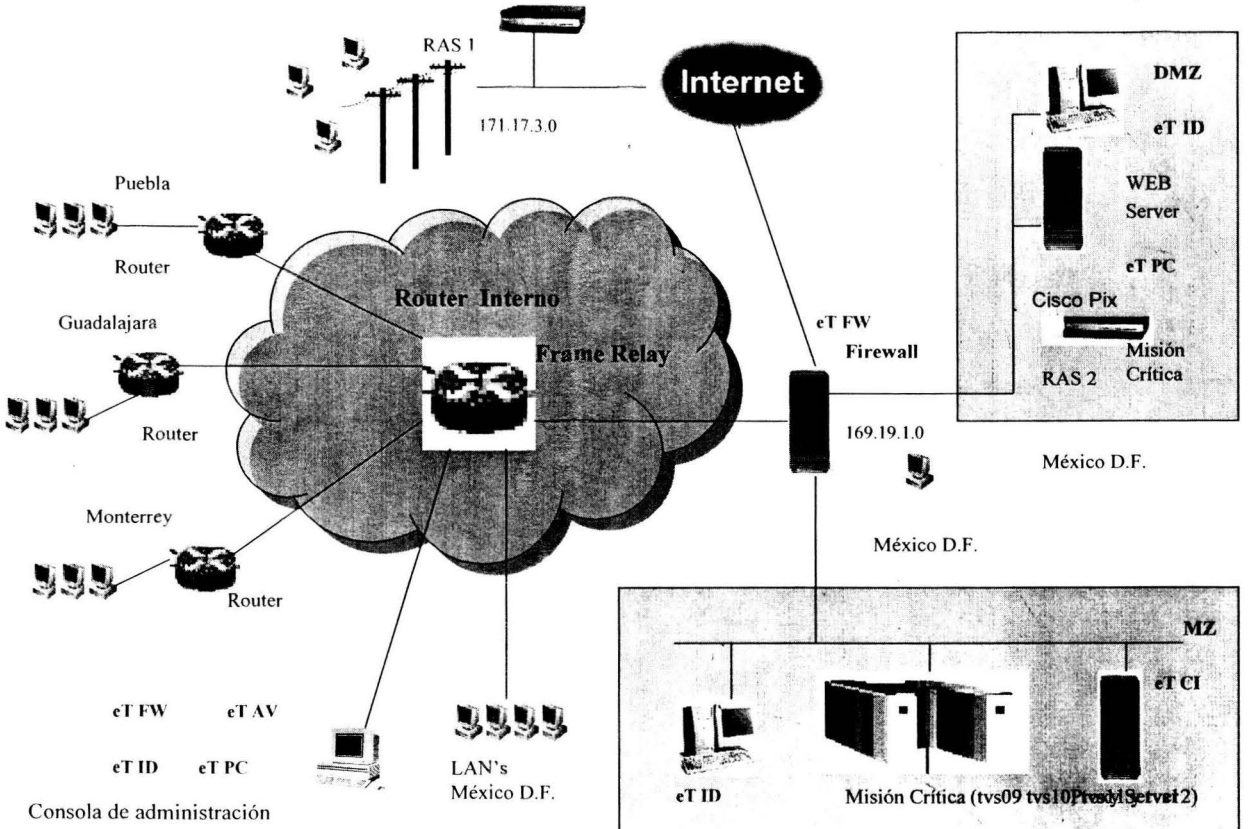


Figura 4.4. Arquitectura del Sistema de Seguridad

En el Proxy ubicado en la MZ se integró una licencia de *eTrust Content Inspection*. Esta licencia se encargará de realizar la inspección de contenido para captar posible malware que pueda llegar a introducirse a esta zona, tanto por fuera como dentro de la empresa.

Para las cinco soluciones de software comentadas anteriormente, se está integrando una consola de administración centralizada en la Cd. De México, ésta tendrá la posibilidad de configurar o ajustar parámetros de forma remota, así como también de recibir las alarmas ante cualquier evento sospechoso o amenaza de ataque.

Para la solución Antivirus, ya utilizada por la empresa televisora, tan solo se integró una política de seguridad que se tocará más adelante. Las 1600 computadoras personales ya cuentan con la última versión de *eTrust Antivirus* en el presente diseño.

Cabe comentar que el Firewall *Cisco Pix* denominado como RAS 2 deberá integrar seguridad estricta, ya que es la entrada de Internet abierta al público en general, siendo de esta forma, el primer filtro de entrada. También el Firewall sirve para prevenir un alto nivel de tráfico en la red.

Los seis servidores que aparecen en el diseño de la arquitectura ya eran propiedad de la empresa televisora y fueron aprovechados para el diseño de la solución, estos servidores corresponden a dos equipos con *eTrust Intrusión Detection*, el Proxy con *eTrust Content Inspection*, el Web Server con *eTrust Policiy Compliance*, un servidor con *eTrust Firewall* y la consola de administración con equipos marca *Hewlett Packard Pentium III* a 800Mhz con 256Mb de Ram y 5 GB en disco duro, Sistema Operativo *Microsoft Windows 2000*.

A continuación se integra un detalle de los beneficios adicionales de cada una de las herramientas de software propuestas.

eTrust Antivirus

Entre sus funciones se encuentra un doble escaneo de las Zonas de Riesgo, que van a permitir al administrador organizar las máquinas de los usuarios, ya sea por departamentos o por localización geográfica; la opción *Bloqueo de Virus* encierra los archivos contaminados para evitar una propagación en la red de un virus. Cuenta además con un sistema de actualización automática y con base en las políticas de información, se identifican y aíslan aquellos códigos maliciosos que puedan causar algún daño.

Como beneficios se pueden señalar los siguientes:

- Reducción de riesgos y caídas de tiempos de trabajos, ya que está certificado y respaldado por otro componente denominado *eTrust TARGET (Threat Analysis and Response Global Emergency Team: Análisis de*

Amenazas y Equipo de Respuesta Global ante una Emergencia), que permite una mayor protección y confianza en el producto.
- Cuenta con mecanismos de alerta y desplegado de funciones.
- Permite un uso confiable del Internet, sin temor de ser contaminados por un virus.

Funcionalidades distintivas:

- Administración centralizada, ya que el administrador en una sola consola podrá monitorear fácilmente toda la red WAN. Entre estas herramientas se encuentran los agentes para *Microsoft Exchange, Lotus Notes*, el soporte para usuarios remotos, el Bloqueo de Virus y la instalación y desinstalación de forma remota.
- Escaneo de virus y malware, en los distintos protocolos de SMTP, FTP, HTTP y POP3. Prevé protección para todos los correos electrónicos, descargas de sitios de Internet y transferencia de archivos.
- Este producto se encuentra certificado por: *ICSA Labs, West Coast Labs* y *Virus Bulletin*.

Este Antivirus soporta ambientes *Windows 9x/ NT / 2000 / XP / Me*.

eTrust Intrusion Detection

Este producto detecta intrusiones potenciales, ataques y abusos por parte de los usuarios. Además presenta gran flexibilidad y manejo; centraliza el monitoreo, lo que permite al administrador ver más de una estación de trabajo ya sea local o remota. Este producto puede ser instalado en distintos segmentos de la red, permitiendo al administrador ver alertas y generar reportes.

Los beneficios que ofrece son los siguientes:

- El IDS provee un modo de operación sordo, ya que no es posible para los intrusos el detectarlo.
- Conserva los recursos de ancho de banda de la red, al no permitir que mucha de la capacidad de la red sea utilizada por actividades ajenas a los protocolos HTTP, SMTP, TELNET y FTP.
- Productividad de los empleados, en cuanto a la restricción existente de información no deseada proveniente del Internet.

Funcionalidades distintivas.

Para Administración:

- Alto desempeño, ya que es capaz de balancear el tráfico de redes.
- Actualización automática de URL's, para una máxima protección.

- Administración de una consola centralizada, lo que permite al administrador de red monitorear y controlar toda una red desde una consola, permitiéndole al administrador diseñar las reglas y políticas de la red y en caso de alerta, responder inmediatamente.
- Administración remota, que permite a los usuarios remotos conectarse a la red de la empresa monitoreando y verificando los reportes de la red.

Para protección de la red:

- Protección de red completa, debido a que se instala en diferentes segmentos de la red, monitorea y previene contra intrusiones.
- Escaneo de la red, para localizar virus, malware y generación de alertar en caso de encontrarlos.

Para monitoreo de sesión:

- Registro y reporte de una red en uso, que permite a los administradores contar con una herramienta de visualización, logrando un monitoreo sencillo de lo que sucede en la red, llevando seguimiento de los usuarios, aplicaciones, protocolos, servidores, etc. Esto ayuda a crear reportes, mejorar las políticas de uso y contar con una mejor protección contra abusos.
- Monitoreo de contenidos de los protocolos HTTP, SMTP, TELNET y FTP, lo que permite ver el uso del correo electrónico y el Internet.
- Análisis y registro de Intrusiones, por medio de un sistema que captura la información y la pone a disposición para su posterior análisis.

Para el bloqueo de contenido de Internet:

- Bloqueo de direcciones URL y control de acceso, evitando la improductividad, ya sea de forma individual o por grupos de direcciones.
- Vigilancia, ya que los administradores verifican el tráfico, y si el usuario viola las políticas, finaliza su sesión de red.

eTrust Intrusion Detection es soportado por *Windows 98 / Me / 2000 / NT 4.0* y Redes TCP/IP.

eTrust Firewall

Los principales beneficios del *eTrust Firewall* son:

- Visualización de seguridad. El *eTrust Firewall* permite a los administradores visualizar los recursos de la red, pudiendo personalizar la pantalla a conveniencia de la compañía.
- Despliegue de la seguridad basada en una política unificada. El *eTrust Firewall* permite definir una política de red centralizada. Estas políticas se

pueden hacer extensivas a todas las instalaciones de *eTrust Firewall*, permitiendo la seguridad a lo largo de la empresa.

- La funcionalidad del estado de alerta de tecnología de filtrado de paquetes, ofrece la más alta tecnología para el filtrado de protocolos complejos, rastreando los frames TCP y filtrando paquetes IP basados en el estado de la sesión, esto lo hace en forma inteligente, ya que mantiene la eficiencia del mismo filtrado.
- Sistema de alerta y reporte. El *eTrust Firewall* mantiene el tráfico de la red y la administración de la operación de otros Firewalls en forma centralizada. La información, como el organizador del Firewall, estado, la conexión actual y tablas de ruteo, están disponibles para su supervisión.
- Soporte por calendario. Las reglas del Firewall pueden activarse y/o desactivarse por medio de calendarios.
- *Internet Firewall Wizard*. El *eTrust Firewall* se puede instalar y personalizar fácilmente a través del uso de pantallas paso a paso *(wizards)*, diseñado con las reglas para los servicios de Internet más populares.
- Traducción de direcciones de red. El *eTrust Firewall* protege a los servidores sensibles de intrusos, a través de su facilidad de traducción de dirección. Los usuarios pueden acceder desde fuera de los sistemas y servicios sin revelar el IP del servidor.
- El Dominio de NT. Permite crear reglas basado en el ID del usuario o grupos de usuarios dentro de un solo dominio, esto elimina la necesidad de la utilización de bases de datos separadas por usuario.
- Interfaz para otros productos. Mantiene un método de autentificación, haciendo reglas dinámicas para otra aplicación, como pueden ser los Detectores de Intrusos.
- Administración centralizada. El administrador de la red puede manejar múltiples Firewalls desde una sola consola.

eTrust Firewall es soportado por *Windows 98 / Me / 2000 / NT 4.0, Sun Solaris, HP-UX* y *IBM AIX*.

eTrust Policy Compliance

eTrust Policy Compliance es un administrador de riesgo y solución de seguridad para empresas, que permite identificar las áreas vulnerables a problemas y, con ello, facilitar su resolución y prevenir la repetición del mismo supervisando la seguridad del sistema. Ayuda a los administradores a detectar las vulnerabilidades de las políticas de seguridad y permite manejar los riesgos en cualquier parte de sus ambientes comerciales.

Esta solución también permite a las organizaciones salvaguardarse contra uso desautorizado del sistema o ataques. Dentro de los beneficios que este producto presenta se encuentran los siguientes:

- Mejora la seguridad y reduce el riesgo, identificando los puntos débiles potenciales en las políticas de seguridad, proporcionando la corrección para estas vulnerabilidades de forma inmediata. El *eTrust Policy Compliance* supervisa a los sistemas y aplicaciones, y en especial, a las violaciones de las reglas en específico.
- Reduce el costo y complejidad de manejar la seguridad del sistema a través de una administración centralizada, mostrando informes de riesgos con sus posibles soluciones.
- Mantiene la seguridad actualizada a través del acceso directo a la Web.
- Mejora los niveles de servicio, permitiendo a administradores observar excepciones o desviaciones de las políticas de seguridad definidas, e inmediatamente tomar la acción para corregirlas.

Funcionalidades distintivas:

- Verificación centralizada de sistemas heterogéneos. El *eTrust Policy Compliance* permite a administradores intervenir en servidores y aplicaciones desde una sola consola. También varios administradores pueden intervenir simultáneamente, pudiendo supervisarlos, los sistemas incluidos son: *Windows NT/2000/XP / .NET, UNIX, Linux* y sistemas de *OpenVMS, Oracle, MS SQL* y bases de datos *Sybase, Apache Web Servers*, y otros.
- Reparación automática. Que les permite a los administradores rectificar la seguridad crítica inmediatamente.
- Actualización de Web dinámica. Lo que proporciona un acceso fácil a actualizaciones de seguridad, con el fin de encontrar debilidades en el sistema.
- Controles predefinidos de seguridad. El *eTrust Policy Compliance* proporciona una colección de controles predefinidos que pueden llevar a cabo metas particulares. Pueden asignarse valores de peso que representan el nivel de severidad de una violación de seguridad a los controles y organizadores, permitiendo a administradores enfocarse en tareas más críticas.
- Cuentas del usuario y análisis de política de contraseña. El *eTrust Policy Compliance* identifica las cuentas de usuario que están inhabilitadas o que son utilizadas por usuarios múltiples. También descubre cuentas que tienen las contraseñas perdidas que pueden ser utilizadas por hackers.

Este producto puede ser soportado en plataformas *Windows NT / 2000 / XP*.

eTrust Content Inspection

Las funcionalidades distintivas que presenta este producto son:

- Esta solución se conecta fácilmente al Firewall y asegura una conexión a Internet libre de riesgos de contenido activo, tal como *JAVA y ActiveX*. Sin

esta solución, el código activo pasa fácilmente por el Firewall debido a que lo considera parte del protocolo HTTP.

- Proporciona protección de código activo. Dicha protección es personalizable a cada empresa. El *eTrust Active Content Inspection* bloquea código malicioso y emite reportes.
- La solución puede ser administrada de manera centralizada a los diferentes componentes en cada segmento.

eTrust Content Inspection soporta plataformas *Windows NT*.

4.2. Requerimientos para el sistema de seguridad

Los requerimientos de las configuraciones de software necesarias para la implementación de estos sistemas, basado en la arquitectura definida en la Figura 4.4., está compuesto de acuerdo a la Tabla 4.4.

Productos Involucrados	Cantidad de Licencias
eTrust Intrusion Detection (eID)	2
eTrust Policy Compliance (ePC)	1
eTrust Content Inspection (eCI)	1
eTrust Firewall (eFW)	1

Tabla 4.4. Requerimientos de configuración.

Requerimientos de plataforma para la Consola de Administración

Los requerimientos mínimos para la implementación de la Consola de Administración, en la cual se administrará de forma centralizada la vigilancia de la red, contará de los siguientes elementos:

Cantidad de Equipos: 1

Características principales:

- 128 Mb en RAM
- 2 GB Libres de Disco Duro
- *Windows NT 4.0 (SP6a) / Windows 2000*
- JRE 1.1.8 o superior (viene en la media de *eTrust Firewall*)
- *Microsoft Windows Script 5.1* (Disponible en *Internet Explorer*)

Requerimientos de plataforma para eTrust Intrusion Detection

Los requerimientos mínimos para la implementación de este software serán los siguientes:

Cantidad de Equipos: 2

Características principales:
- 256 MB en RAM
- 2 GB Libres de Disco Duro
- Procesadores con por lo menos 500 MHz
- *Windows NT 4.0 (SP6a) / Windows 2000*

Requerimientos de plataforma para eTrust Firewall

Los requerimientos mínimos para la implementación del Firewall son los siguientes:

Cantidad de Equipos: 1

Características principales:
- 256 MB en RAM
- 2 GB Libres de Disco Duro
- Procesadores con por lo menos 500 MHz
- *Windows NT 4.0 (SP6a) / Windows 2000*
- JRE 1.1.8 o superior (viene en la media de *eTrust Firewall*)
- *SQL Server 7.0* (opcional)
- Tres Tarjetas de Red Ethernet 100VGAnyLAN

Requerimientos de plataforma para el servidor Proxy con eTrust Content Inspection

Los requerimientos mínimos para implementar el software *eTrust Content Inspection* en el Servidor Proxy son los siguientes:

Cantidad de Equipos: 1

Características principales:
- 256 MB en RAM
- 2 GB Libres de Disco Duro
- Procesadores de por lo menos 500 MHz
- *Windows NT 4.0 (SP6a) / Windows 2000*

Requerimientos de plataforma para el Servidor Web con eTrust Policy Compliance

Los requerimientos mínimos para la implementar en el Servidor Web del producto *eTrust Policy Compliance* son:

Cantidad de Equipos: 1

Características principales:

- Al menos 64 MB en RAM
- 1 GB Libres de Disco Duro
- *Windows NT 4.0 (SP6a) / Windows 2000*

Para la implementación de todos los productos antes mencionados, los actuales anchos de banda para la red de datos no tuvieron que ser modificados, ya que son suficientes para la configuración.

4.3. Plan de trabajo e implementación del sistema de seguridad

Para la implementación del proyecto se definió junto con el cliente una serie de actividades, basadas en las prioridades por parte del cliente y la disponibilidad de personal técnico y equipo de operación. Este plan de implementación contempla el levantamiento de información y análisis -obtenido en el Capítulo 3-, pasando por sesiones de trabajo con la empresa televisora para la definición de políticas a ser cumplidas por las soluciones de software a implementar. Lo anterior se cubre en la Etapa 1 de implementación. La Etapa 2 contempla la instalación de cada una de las soluciones de software en los servidores definidos en la arquitectura del sistema de seguridad, observado en la Figura 4.4. Finalmente, en la Etapa 3 se integra la configuración de estas soluciones junto con la documentación correspondiente. En la Tabla 4.5. se muestra este Plan de Implementación integrando las actividades de cada etapa.

4.3.1. Plan de trabajo

El plan de trabajo se llevó en etapas, éste se organizó de acuerdo a la Tabla 4.5.

- Etapa 1. **Análisis de seguridad**

Para el análisis de la operación de la compañía, referente a las políticas de acceso y generación de reportes de seguridad, se tomó como base la encuesta realizada al Gerente de Seguridad y al Director de Sistemas, descritas en el Capítulo 3. Este análisis contempla los rubros prioritarios para la empresa televisora. A partir de este análisis se tuvo la posibilidad de definir e implementar una serie de políticas nuevas y una mejor cobertura ante vulnerabilidades, todo a través de la tecnología de software seleccionada en este capítulo.

- Etapa 2. **Generación de un esquema de seguridad**

Los consultores estuvieron apoyados por el equipo técnico de la empresa televisora para llevar a cabo las siguientes actividades:

- Definición de reglas de acceso para el *eTrust Firewall.*
- Definición de reglas y políticas para *eTrust Intrusion Detection.*
- Definición de reglas de *eTrust Intrusion Detection* para configuración dinámica del Firewall.

ID	ACTIVIDAD	DURACION	INICIO	FIN	PRED	% AVANCE
1	**Plan de Actividades para Implementación del Sistema de Seguridad Empresa Televisora**	**55 days?**	**Mon 03/02/03**	**Fri 18/04/03**		**100%**
2	**Seguridad en la red**	**55 days?**	**Mon 03/02/03**	**Fri 18/04/03**		**100%**
3	**Etapa 1. Análisis de Seguridad**	**14 days**	**Mon 03/02/03**	**Thu 20/02/03**		**100%**
4	Análisis de la operación actual	11 days	Mon 03/02/03	Mon 17/02/03		100%
5	Análisis de las politicas de acceso	11 days	Mon 03/02/03	Mon 17/02/03	4	100%
6	Generación del reporte de Análisis de Seguridad	3 days	Tue 18/02/03	Thu 20/02/03	5	100%
7	**Etapa 2. Generación de un esquema de seguridad**	**5 days**	**Mon 24/02/03**	**Fri 28/02/03**	**3**	**100%**
8	Definición de reglas de acceso para el firewall	3 days	Mon 24/02/03	Wed 26/02/03		100%
9	Definición de reglas y políticas para eTrust Intrusion Detection	3 days	Mon 24/02/03	Wed 26/02/03	8	100%
10	Definición de reglas de eTrust Intrusion Detection para configuración dinámica del firewall	3 days	Mon 24/02/03	Wed 26/02/03	9	100%
11	Sesión de trabajo con Empresa Televisora para validar las reglas y politicas	1 day	Fri 28/02/03	Fri 28/02/03	10	100%
12	**Etapa 3. Instalación de las herramientas**	**14 days?**	**Mon 03/03/03**	**Thu 20/03/03**		**100%**
13	**eTrust Firewall**	**6 days?**	**Mon 03/03/03**	**Mon 10/03/03**	**3**	**100%**
14	Revisión de los requerimientos y adecuación	0.75 days	Mon 03/03/03	Mon 03/03/03		100%
15	Instalación de las tarjetas	1 day	Tue 04/03/03	Tue 04/03/03	14	100%
16	Instalación del producto	0.5 days	Tue 04/03/03	Tue 04/03/03	15	100%
17	Configuración de la DMZ y la MZ	1 day	Wed 05/03/03	Wed 05/03/03	16	100%
18	Pruebas de conectividad	3 days	Wed 05/03/03	Fri 07/03/03	17	100%
19	Instalación de la Consola de Administración	1 day?	Mon 10/03/03	Mon 10/03/03		100%
20	**eTrust Intrusion detection**	**5 days**	**Tue 11/03/03**	**Mon 17/03/03**		**100%**
21	Revisión de los requerimientos y adecuación	1 day	Tue 11/03/03	Tue 11/03/03		100%
22	Instalación de los servidores de eTrust Intrusion Detection	3 days	Wed 12/03/03	Fri 14/03/03	21	100%
23	Instalación de la Consola de Administración	1 day	Mon 17/03/03	Mon 17/03/03		100%
24	**eTrust Policy Compliance**	**2 days**	**Tue 18/03/03**	**Wed 19/03/03**		**100%**
25	Instalación de eTrust Policy Compliance en Servidor WEB	1 day	Tue 18/03/03	Tue 18/03/03		100%
26	Instalación de la Consola de Administración	1 day	Wed 19/03/03	Wed 19/03/03		100%
27	**eTrust Antivirus y Content Inspection**	**2 days**	**Wed 19/03/03**	**Thu 20/03/03**		**100%**
28	Instalación de eTrust Content Inspection en Servidor Proxy	1 day	Wed 19/03/03	Wed 19/03/03		100%
29	Instalación de la Consola de Administración	1 day	Thu 20/03/03	Thu 20/03/03		100%
30	**Etapa 4. Configuración de las herramientas**	**21 days?**	**Fri 21/03/03**	**Fri 18/04/03**	**7**	**100%**
31	**Firewall**	**1 day**	**Fri 21/03/03**	**Fri 21/03/03**		**100%**
32	Configuración de reglas en el Firewall	1 day	Fri 21/03/03	Fri 21/03/03		100%
33	**eTrust Intrusion Detection**	**11.75 days**	**Fri 21/03/03**	**Mon 07/04/03**	**31**	**100%**
34	Análisis del tráfico inicial	0.75 days	Fri 21/03/03	Fri 21/03/03		100%
35	Definición de reglas y politicas	0.75 days	Mon 24/03/03	Mon 24/03/03	34	100%
36	Monitoreo del sistema	10 days	Mon 24/03/03	Fri 04/04/03	35	100%
37	Ajuste de reglas y politicas despues del monitoreo	0.75 days	Mon 07/04/03	Mon 07/04/03	36	100%
38	**eTrust Policy Compliance**	**1 day**	**Tue 08/04/03**	**Tue 08/04/03**		**100%**
39	Definición del Modelo de Verificación de Vulnerabilidades	1 day	Tue 08/04/03	Tue 08/04/03		100%
40	Documentación	4 days	Wed 09/04/03	Mon 14/04/03	33	100%
41	Entrenamiento al Personal Técnico	5 days?	Mon 14/04/03	Fri 18/04/03		100%

Tabla 4.5. Actividades del Plan de Implementación.

Falta página

N° 132

En la sesión de trabajo con la empresa televisora, para validar las reglas y políticas de seguridad, se consideraron los resultados emitidos del estudio de vulnerabilidades generales llevado a cabo en el Capítulo 3. La finalidad fue el tomar las vulnerabilidades más importantes ligadas a los objetivos de este proyecto, tomar estas políticas, llevarlas a la arquitectura de solución definida y finalmente implementarlas utilizando la tecnología de software seleccionada. Para esa segunda Etapa se utilizaron principalmente las soluciones de *Computer Associates, eTrust Intrusion Detection* y *eTrust Firewall.*

El Staff mínimo requerido por ambas partes (proveedor y empresa) fue:

- Proveedor: Consultor de Seguridad y Líder de Proyecto.
- La empresa televisora: Administrador de la Seguridad (responsable del proyecto) y Gerentes de las áreas involucradas con la red externa.

- Etapa 3. **Instalación de las herramientas de software**

Para la instalación de las herramientas de software se requirió de:

- 2 Servidores *Microsoft Windows NT*, en donde se instaló *eTrust Intrusion Detection.*
- 1 Servidor *Microsoft Windows NT* con 3 interfaces de red, donde se instaló eTrust *Firewall.*
- 1 Servidor *Microsoft Windows NT* con *Web Application Server*, en donde se instaló *eTrust Policy Compliance.*
- 1 Servidor *Microsoft Windows NT* e *Internet Información Server*, en donde se instaló *eTrust Content Inspection.*
- 1 Consola *Microsoft Windows NT* para instalar los módulos de administración de las soluciones de software *eTrust Intrusion Detection, eTrust Policy Compliance, eTrust Antivirus* y *eTrust Firewall.*

Los consultores fueron apoyados por el equipo técnico de la empresa televisora, y llevaron a cabo las siguientes actividades:

- Revisión de los requerimientos y adecuación de *eTrust Firewall.*
- Instalación de las Tarjetas de Red.
- Instalación del producto.
- Configuración de la DMZ y la MZ.
- Pruebas de conectividad.
- Instalación de la Consola de Administración.

Cabe comentar que la instalación de la herramienta fue llevada a cabo de forma muy ágil, ya que esta herramienta cuenta con un método de instalación muy claro, llevando al instalador paso a paso. Es tal el nivel de facilidad de instalación, que la misma herramienta puede identificar los componentes que estarán tanto en la MZ,

DMZ y la Intranet, identificando cada Tarjeta de Red instalada en el servidor. Por otro lado, la herramienta cuenta con reglas básicas definidas para la configuración de los puertos de cada servicio Web, correo electrónico, transferencia de datos, etc. Esto evita la programación dentro de la herramienta y por tanto un costo mayor para la administración de la misma.

Para la instalación de *eTrust Intrusión Detection* fue necesario:

- Revisión de los requerimientos y adecuación de *eTrust Intrusion Detection*.
- Instalación de los servidores *eTrust Intrusion Detection*.
- Instalación de la Consola de Administración de *eTrust Intrusión Detection*

Se instaló esta solución de software en los servidores correspondientes, definidos para los segmentos de red mostrados en la Figura 4.4.

Para *eTrust Policy Compliance* fue necesario:

- Instalación *eTrust Policy Compliance* en el servidor Web.
- Instalación de la Consola de Administración de *eTrust Policy Compliance*.

Para esta solución de software se instalaron los módulos de *Client Manager*, *Agent* y *eTrust Web Update*. Para la instalación de este tipo de herramienta debe existir un módulo Client y un módulo Agent. El método de instalación es 'paso a paso', lo que hace la instalación muy fácil. Durante la implementación se solicitó la definición del password para el módulo Agent y Client. Para la instalación es importante que el protocolo TCP/IP se encuentra previamente instalado y definido.

Durante la instalación esta herramienta se mapea al puerto de servicio TCP/IP 1827 de la red. Los pasos a seguir son:

- Instalación en el Servidor Proxy de *eTrust Content Inspection*.
- Instalación de las Consolas de Administración de *eTrust Antivirus* y *Content Inspection*.

eTrust Content Inspection se va a instalar en un servidor *Microsoft Proxy*, es muy importante verificar que los requerimientos mínimos se cumplan. De esta forma, una vez instalada esta herramienta, se evitarán posibles cuellos de botella por el procesamiento del filtrado de contenido. La instalación de la consola de Antivirus no tuvo ninguna particularidad, ya que de forma automática identificó todos los nodos remotos con el Antivirus y las versiones de sus vacunas.

Revisados los requerimientos se procedió a instalar las siguientes herramientas:

- *eTrust Firewall* en 1 equipo.
- *eTrust Intrusion Detection* en 2 equipos.
- *eTrust Policy Compliance* 1 equipo.

- *eTrust Content Inspection* 1 equipo.

El Staff mínimo que se requirió por ambas partes (proveedor y empresa televisora) fue:

- Proveedor: Consultor de Seguridad, Líder de Proyecto.
- La empresa televisora: Administrador de la Seguridad (responsable del proyecto).

Etapa 4. **Configuración de las herramientas de software**

Los equipos configurados fueron:

- 2 Servidores *Microsoft Windows NT*, con *eTrust Intrusion Detection*.
- 1 Servidor *Microsoft Windows NT* con 3 interfaces de red con *eTrust Firewall*.
- 1 Servidor *Microsoft Windows NT*, con *eTrust Policy Compliance*.
- 1 Servidor *Microsoft Windows NT*, con *eTrust Content Inspection*.
- 1 Consola en donde se configuraron las herramientas *eTrust Intrusion Detection, eTrust Policy Compliance, eTrust Antivirus* y *eTrust Firewall*.

Los consultores, apoyados por el equipo técnico de la empresa televisora, llevarán a cabo las siguientes actividades:

Para *eTrust Firewall* es necesario:

- Configuración de reglas en el Firewall.

Para eTrust Intrusion Detection es necesario:

- Análisis del tráfico inicial.
- Definición de reglas y políticas.
- Monitoreo del sistema.
- Ajuste de reglas y políticas después del monitoreo.

Para *eTrust Policy Compliance* es necesario:

- Definición del modelo de verificación de vulnerabilidades.

Utilizando la herramienta *eTrust Intrusion Detection* se realizó un análisis del tráfico de la red externa, con el objetivo de ajustar las reglas en las herramientas *(eTrust Intrusion Detection, eTrust Firewall* y *eTrust Policy Compliance).*

Se configuró la herramienta de *eTrust Policy Compliance* en el servidor Web, de tal forma que ya se tuvieran los modelos de análisis de vulnerabilidades predefinidos, y de la misma forma los reportes a ser emitidos.

El Staff mínimo requerido por ambas partes (proveedor y empresa televisora) fue:

- Proveedor: Consultor de Seguridad, Líder de Proyecto.
- La empresa televisora: Administrador de Seguridad. (responsable del proyecto).

Entregables:

- Memorias técnicas.

4.3.2. Implementación del sistema de seguridad

Se determinó la cantidad de recursos humanos y el mínimo tiempo de ejecución del proyecto, tomando en cuenta los tiempos, disponibilidad y necesidades de negocio de la empresa televisora. Así mismo, la empresa televisora nombró a uno de sus empleados como el responsable por los Servicios de Implementación, quedando éste autorizado para aprobar las fases, resolver dudas y responder a nombre de la empresa televisora durante la ejecución de los mismos.

Para la ejecución de los servicios de implementación se establecieron horarios de atención, lunes a viernes de 9:00 AM a 6:00 PM.

Para los servicios realizados en fines de semana u horarios distintos al establecido, fue necesaria la previa coordinación con el Gerente del Proyecto.

4.3.3. Presupuesto del sistema de seguridad

El presupuesto para un sistema de seguridad como el expuesto debe estar balanceado, de acuerdo a los activos a proteger.

El presupuesto asignado sólo se limitó al proyecto de implementación y licencias de los productos de software involucrados, la empresa ya contaba con el hardware necesario para la implementación de cada uno de los sistemas, previa validación de la configuración mínima de cada uno de los equipos y basándose en las recomendaciones del presente documento.

El importe de mantenimiento anual cubre el soporte técnico y la protección a actualización de versión de los productos citados.

Los servicios de implementación tuvieron un costo total de $39,600.00 (treinta y nueve mil seiscientos dólares americanos 00/100).

En lo correspondiente al licenciamiento de los productos de software, el presupuesto requerido es el que se muestra en la Tabla 4.6

Productos a Licenciar		Cantidad de Licencias	Precio Unitario	Importe Total	Mant. Anual
eTrust Firewall		1	$499	$499	$100
eTrust Intrusion Detection		2	$25,000	$50,000	$10,000
eTrust Policy Compliance		1	$998	$998	$200
eTrust Content Inspection		1	$3,493	$3,493	$699
					$0
				$54,990	$10,998

Tabla 4.6 Presupuesto de Licenciamiento.

El valor total de proyecto incluyendo productos, mantenimiento y servicios correspondieron a un total de $105,588.00 (ciento cinco mil quinientos ochenta y ocho dólares americanos 00/100).

Todos los precios anteriormente citados fueron dólares americanos y no incluyeron el IVA.

4.4. Políticas **de Seguridad de la red**

El documento que describe las características de seguridad de la red, dentro de una organización específica, se llama Política de Seguridad de la red. Este documento detalla todas las características del sistema de seguridad a implementar, abarcando los siguientes puntos:

- Identificación de los recursos que hay que proteger.
- Identificación de las amenazas a los recursos a proteger.
- Como deberá de ser usada la red.
- Responsabilidades de cada uno de los usuarios de la red.
- Acciones a tomar en caso de que la política de seguridad sea violada.
- Procedimientos de administración, configuración y recuperación de la red.

Este documento, por sí mismo, es muy extenso, ya que debe de contemplar todos y cada uno de los elementos que conforman a la red, apoyados por un inventario de todos los equipos y sistemas a proteger. Por razones de espacio, en el presente trabajo sólo se mostrarán los puntos más importantes a discusión en los foros y reuniones que se llevaron a cabo dentro de la compañía televisora, para la conformación de la política de seguridad para las áreas que constituyen a la compañía.

Cabe mencionar que la mayoría de las Políticas de Seguridad las obtenemos directamente de los cuestionarios que se aplicaron al Director de Sistemas y el Gerente de Seguridad, estos cuestionaros se encuentran basados en el estándar

ISO17799 (el cual se encuentra apoyado por el estándar ingles BS7799). Este estándar define que una buena seguridad depende un 70% de los procesos y un 30% de la tecnología. Tomando lo anterior tenemos una referencia de cuán importante es la definición de estas políticas y que la tecnología no lo es todo en la resolución de este tipo de necesidades. Las políticas están reforzadas con el uso de tecnología, pero siempre será necesario que una vez definidas estas políticas, las mismas sean auditadas y revisadas continuamente.

Las políticas básicas definidas son las siguientes:

- Contar con sistemas UPS en caso de interrupción de energía.
- Contar con vigilancia continua en áreas donde se encuentre equipo con información de gran importancia.
- Llevar un inventario del equipo con el que se cuenta y en caso de mover un equipo, notificarlo al personal autorizado.
- Para lo empleados, es necesario portar un gafete y en caso de que se labore en tiempos fuera de lo establecido, se debe de avisar al encargado en turno.
- Control seguro en la utilización de cintas DAT.
- Tener una clasificación de seguridad para la información con la que se cuenta.
- Se restringe el acceso a cuentas administradas a nodos específicos y a la consola de sistemas.
- Debe existir tiempo límite en las aplicaciones y servicios en caso de inactividad.
- El acceso a las utilerías del sistema debe estar restringido y controlado.
- El tráfico LAN y WAN sensible deberá estar cifrado.
- Los correos electrónicos deberán estar monitoreados.
- Las redes deberán encontrarse en dominios segmentos lógicos separados.
- Las conexiones entre redes deberán ser establecidas por controles de ruteo.
- Se prohíbe el acceso a los datos internos vía servicios Web.
- Deben existir restricciones en la descarga de software de lugares públicos.
- El acceso a Internet deberá estar restringido y monitoreado.
- Control de accesos a los servidores de misión crítica con la implementación de la MZ, configurada ésta a partir del agente del detector de intrusos ID y Content Inspection (CI) sobre del Servidor Proxy, evitando que usuarios no autorizados ingresen a directorios clasificados o intentos de intromisión de malware por los mismos.
- Control de aplicaciones, especialmente a las bases de datos del *MS SQL Server* en los servidores de misión crítica de nómina, finanzas, tesorería, bases de datos de videos y producción.
- En cuanto al control de accesos se debe de tener un control de los logins y el personal debe de contar con claves de autentificación para el ingreso a la red.

- Debe existir una seguridad para el acceso a la base de datos, con el personal calificado y sus correspondientes claves de autentificación.
- Apoyo a la red mediante la utilización de Firewalls.
- Se deben borrar todas las cuentas de usuario cuando éste deja la organización.
- Debe existir una base central de usuarios.
- Debe existir un procedimiento de autorización para agregar nuevos usuarios a los sistemas.
- Los usuarios deben ser autentificados a través de un password.
- Se deben tener cuentas de acceso público o guest.
- Todas las cuentas deben ser correlacionadas hacia un usuario real.
- Los privilegios de usuarios deben ser revisados periódicamente.
- Se deben de seguir prácticas de seguridad definidas en la selección de passwords.
- Las cuentas deben tener un tiempo de expiración determinado.
- Las terminales deben ser identificadas automáticamente para autentificar la conexión a localidades específicas.
- Deben existir alarmas mediante las cuales los usuarios puedan ser notificados.
- Las actividades en computadoras deben ser asociadas a un usuario en específico.
- Los administradores deben estar restringidos a iniciar transacciones de nivel aplicativo.
- Los usuarios deben estar restringidos al acceso a datos y funciones fuera del perfil de su puesto.
- Las cuentas privilegiadas y de emergencia deben ser revisadas constantemente.
- El acceso a bitácoras de eventos debe estar controlado.
- Los intentos fallidos de acceso deben estar restringidos deshabilitando la cuenta después de un número determinado de intentos.
- Deben existir restricciones de horario en las aplicaciones y servicios.
- Se debe de realizar un análisis de vulnerabilidad, documentando las fallas, amenazas e impactos sobre el sistema cuando estos llegaran a ocurrir.
- Se debe de llevar a cabo una estrategia de administración de riesgo con pasos a seguir en caso de contingencia. Estas estrategias de administración de riesgos deben de ser revisadas al menos cuatro veces por año.
- Todas las áreas dentro de la empresa deben ser sujetas a entrevistas o supervisiones continuas para asegurar el cumplimiento de las políticas de seguridad.
- Se debe de crear un plan de continuidad de negocio que considere el buen funcionamiento de los activos principales por área de la empresa.
- En caso de interrupción de los servicios, se debe de buscar la causa real del problema y debe ser documentada junto con su solución.

- Se debe crear un plan de procedimientos a respuestas de incidentes que contemple: prevención, detección, contención, solución y retorno a operación normal del sistema.
- Se deben de crear procedimientos de respaldo y recuperación de información crítica para cada área de la empresa.
- Se deben de revisar siempre las bitácoras en busca de actividades sospechosas y la información recopilada debe ser siempre almacenada.
- Se debe de crear un procedimiento que nos asegure que los nuevos sistemas cumplen con los requerimientos de seguridad, así como también un control de cambios en estos sistemas.
- Nadie en la organización deberá bajar de Internet ningún tipo de software no autorizado.
- Cualquier tercer parte que tenga que trabajar con la información de la organización tendrá que firmar un acuerdo de confidencialidad para la seguridad de la información.
- Todos los empleados deberán firmar un acuerdo de confidencialidad como parte de sus términos y condiciones de empleo.
- El responsable de la administración de incidentes deberá asegurar una respuesta rápida y efectiva ante cualquier incidente de seguridad.
- Las áreas de desarrollo de aplicaciones y pruebas deberán estar completamente separadas a los ambientes de operación.
- Los sistemas de respaldo (medios magnéticos) en donde se mantenga información sensible deben ser destruidos en caso de no ser utilizados.
- Se deberá contar con un inventario completo de los activos, integrando su identificación, ubicación, valuación, responsable asignado y su clasificación de seguridad completamente documentada.
- Los activos podrán ser definidos como procesos, información, documentos en papel, activos en software, activos físicos, personal, imagen y reputación de la compañía y servicios.
- La valuación deberá estar relacionada con el valor de impacto al negocio, ésta deberá referenciar pérdida de confidencialidad, de integridad y disponibilidad. El valuar en forma monetaria en muchos casos pudiera ser complicado. Se podrá definir una escala de 1 al 5 para identificar los mismos.
- El nivel de impacto de un activo deberá también clasificarse en Muy Alto (más de 5 Millones de Dólares), Alto (Menos de 5 Millones de Dólares), Medio (Menos de Quinientos Mil Dólares) y Bajo (menos de cinco mil Dólares).

Algunos puntos de interés son:

- Aunque se aplican controles de seguridad, no hay definido un programa para la prevención de seguridad de la empresa televisora. No hay que olvidar que finalmente lo que nos interesa proteger es la información a la cual tienen acceso los usuarios de acuerdo a sus roles, y por lo tanto deben tener una cultura para el manejo de información.

- No existe un proceso para realizar análisis formal de los activos. La televisora tiene inventariados los activos, pero no se tiene un análisis de riesgo de cada uno de los activos.
- No existe un estudio de dependencia de los activos. La falta de estudios de dependencia de los activos es necesaria para tener identificados los servidores y componentes críticos y evaluar sobre ellos con un mayor detalle la aplicación de políticas de seguridad.
- No se cuentan con sistemas de auditoría.

4.5. Memorias técnicas

Las memorias técnicas son parte de la solución del problema, éstas cuentan con información sobre los productos a instalar, y la manera de cómo se llevó a cabo la instalación. Por razones de confidencialidad, no se muestran los passwords reales, y en algunos casos, no fue posible incluir esta información en el presente trabajo, a petición propia de la empresa, por razones de confidencialidad. A continuación se presentan las memorias técnicas por solución.

Memoria técnica de eTrust Firewall

La arquitectura de de esta herramienta de software se encuentra compuesta por los siguientes módulos:

1) *eTrust Firewall Admin Server*. Este módulo se encarga de guardar en su base de datos las políticas definidas para el Firewall. Por otro lado, este módulo se encarga también de administrar otros Firewalls dentro de la red.

2) *eTrust Firewall Admin Client*. Permite administrar de forma remota el *eTrust Admin Server*.

3) *eTrust Firewall Engine*. Este módulo se encarga de interceptar el tráfico de la red y asegura la política definida.

4) *eTrust Firewall User Client*. Ésta es la interfaz de administración de usuario, se instala en aquello nodos que acceden al Firewall.

5) *eTrust Firewall Login Agent*. Éste facilita el acceso a las reglas del Firewall utilizando la autenticación del Sistema Operativo.

Como puntos adicinales se tiene:

- La comunicación entre estos módulo está completamente asegurada.

Todos los componentes fueron insalados en un equipo definido para esta función:

Equipo: tvs00
Función: servidor de Firewall
IP: 169.19.1.0
Versión SO: *Windows 2000 Profesional*

Se configuró el Firewall para la Intranet utilizando dos NIC's, se definió una dirección de resguardo del archivo de configuración, contenido en:

Directorio: c:\program files\Computer Associates\eTrust\Firewall

Admin Credentials:

User Name: fwadmin
Password: fwtv00

Reglas definidas:

1. Nadie desde la Internet se podrá conectar a las redes internas o Intranet- Activada.
2. Usuarios internos podrán realizar accesos a Internet, servicios FTP y correo electrónico al exterior sólo y únicamente a través de la DMZ- Activada.
3. La conectividad de correo electrónico, hacia y desde Internet, será a través del servidor de correo en la DMZ- Activada (El servidor Web dispuesto en la DMZ tiene activados los servicios SMTP).
4. Todo el tráfico proveniente de la Internet y FTP está autorizada en la DMZ.

Estas reglas fueron definidas a través de las pantallas paso a paso de *eTrust Firewall,* todas y cada una de ellas fueron adicionadas en una base de datos, integrada en el módulo *eTrust Firewall Admin Client.*

Para la creación de nuevas políticas será necesario desarrollar el procedimiento paso a paso que contempla esta herramienta de software.

Las reglas definidas fueron simuladas antes de ser implementadas, a través del módulo de *Security Policy,* contenido en la herramienta. La simulación de estas reglas implementadas fue satisfactoria.

Memoria técnica de eTrust Intrusion Detection

Se utilizaron NIC's Ethernet de *3Com 3C595 10/100 PCI.* De estos, dos equipos fueron configurados en modo promiscuo, esto permitirá que el tráfico de la red del segmento pase en su totalidad por la misma.

Dado que *eTrust Intrusión Detection* se da de alta como un servicio en *Windows NT,* éste se dio de alta como usuario "admin22" con password "admin33" con derechos de administración y configuración de acceso a una impresora local conectada a este equipo.

Se llevo a cabo la implementación de dos licencias en los segmentos de red a 100Mbps, tanto de la DMZ como MZ. Cada uno de estos equipos fueron conectados al puerto RAP de los switches *3COM Superstack II*. Se integró una configuración en esta herramienta de software el monitoreo, reporteo y bloqueo de las sesiones TCP/IP (TCP y UDP), http y POP, TNP e IMAP; estos últimos tres para el monitoreo de los componentes de MS Exchange y el contenido de virus dentro de mensajes de correo electrónico. Así mismo, se integraron filtros para detección de acciones sospechosas en la red de datos y configuración de monitoreo, reportes y categorías de acceso a URL's para http. El contenido de datos en la red de la empresa televisora estará siendo monitoreado en el Intranet, como datos de salida hacia Internet a través del servidor Proxy o aquellos datos de entrada a través del servidor Web, antes de llegar al Firewall. El filtro de datos configurado fue a nivel de tipos de archivo y cadenas de caracteres específicos.

La dirección de los servicios SMTP correspondiente al servidor de correo electrónico de la empresa televisora configurada fue:

Equipo: tvs09 (integrado en la granja de servidores en la MZ)
Función: servidor de correo electrónico
IP: 15.94.4.44
Versión SO: *Windows 2000 Profesional*

La dirección del servicio Proxy correspondiente al servidor de correo electrónico de la empresa televisora configurada fue:

Equipo: tvs01
Función: Proxy Server
IP: 15.94.3.2
Versión SO: *Windows 2000 Advanced Server*

Al reinicializar el equipo con *Windows NT* no será necesario arrancar el servicio de estos productos

Configuración de filtrado de archivos, cadenas de caracteres y URL's específicos:

El producto quedó configurado para filtrar:

1) Archivos:

.EXE, .COM, .JPEG, .MP3.

2) Cadenas de caracteres:

CONFIDENCIAL, USO INTERNO, CURRÍCULUM.

3) Bloqueo de acceso vía http a sitios de sexo, música, servicios *ICQ, AOL, Prodigy* y *hotmail*.

4) Bloqueo de mensajes de correo electrónico de máximo 2MB de tamaño.

5) Bloqueo para enlaces FTP de cualquier mensaje contenido entre los servidores tvs9, tvs10, tvs11, tvs12 y cualquier otro nodo dentro de la red que tardé más de 5 minutos entre el origen y destino.

6) Bloqueo de enlaces TELNET y protocolos no estándares en uso fuera de los logins y passwords de administrador de la red de la empresa televisora.

7) Para comportamiento extraño en la red fue configurada la detección de posibles:

   - MAC Spoofing. La activación evita que dos direcciones MAC existan en una misma red.
   - IP Spoofing.
   - Ping Abuse. Máximo paquete ICMP autorizado 1024 Mbytes.
   - Ping Flooding. Mínimo intervalo en el tiempo entre dos paquetes ICMP 2500 milisegundos. Máximo cantidad de frames ICMP enviados entre fuente y destino 30.
   - SYN Flooding. Máximo número de sesiones concurrentes por estación, 10.
   - Rastreo de puerto TCP. Mínimo promedio de tamaño por sesión, 10; máximo promedio de sesiones concurrentes abiertas por destinatario, 30; máximo número promedio de sesiones concurrentes por originario, 50; mínimo promedio del tamaño de sesión de originario, 500.

Los consultores de la empresa televisora tendrán la posibilidad de integrar más filtros a través de la administración de esta herramienta de software y de acuerdo a la nueva generación de políticas para la detección de contenido crítico para la empresa televisora.

Configuración de filtrado de archivos y cadenas de caracteres:

El producto quedó configurado para filtrar las siguientes cadenas de caracteres:

.EXE, .COM,.JPEG,.MP3, CONFIDENCIAL, USO INTERNO, CURRÍCULUM.

Se configuraron dos plantillas de reportes para las dos consolas de monitoreo de cada una de estas reglas definidas, estás podrán emitirse en cualquier de las consolas o directamente en la consola de administración de seguridad de la empresa televisora.

Memoria técnica de eTrust Content Inspection V 2.4

Los siguientes puntos describen la configuración tanto de ubicación, denominación, función y dirección IP correspondientes a la herramienta de software *eTrust Content Inspection*, esto permitirá darle a la empresa televisora la posibilidad de reconfigurar la herramienta cuando sea necesario, se logró:

Instalación del producto: adecuada.

Para los servidores:
Equipo: tvs01
Función: Proxy Server
IP: 15.94.3.2
Producto: *eTrust Content Inspection V 2.4* (MS Proxy Gateway)
eTrust Content Inspection V 2.4 (Policy Manager)
eTrust Content Inspection V 2.4 (Control Center)
eTrust Content Inspection V 2.4 (Audit Viewer)
Directorio: c:\program files\Computer Associates\eTrust\Content Inspection
Versión SO: *Windows 2000 Advanced Server*

Para la consola:
Equipo: tvs02
IP: 15.94.4.35
Producto: *eTrust Content Inspection V 2.4* (Policy Manager)
eTrust Content Inspection V 2.4 (Audit Viewer)
Directorio: c:\program files\Computer Associates\eTrust\Content Inspection
Versión SO: *Windows 2000 Profesional*

El password para el administrador fue: XXXXXX

La instalación del producto *eTrust Content Inspection V2.4* se realizó en un servidor con *Microsoft Proxy V 2.0*. El módulo instalado fue el Gateway para *Microsoft Proxy*, y se instaló en una consola.

La arquitectura de la herramienta de software se puede observar en la Figura 4.5. Esta figura permite entender cuales son los flujos de información o alarmas de esta herramienta.

La herramienta se compone de cuatro módulos, que son:

1) El *Gateway*. Es el encargado de interceptar las requisiones HTML que realiza el proxy, y pasarlas al Control Center para su análisis por contenido malicioso del código de programación *Java* y de virus.

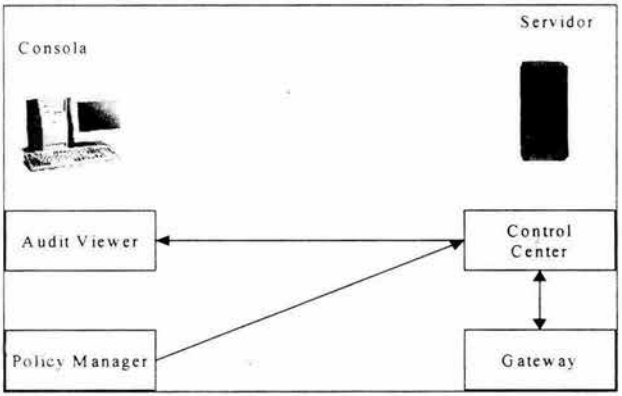


Figura 4.5. Arquitectura de la Herramienta de Software eTrust Content Inspection.

2) El *Control Center*. Es el que aplica las reglas definidas por el Policy Manager sobre el contenido que recibe del módulo Gateway. Este módulo siempre debe de estar activo en el servidor, ya que el Gateway constantemente se comunica con él. Un ejemplo de pantalla se puede observar en la Figura 4.6.

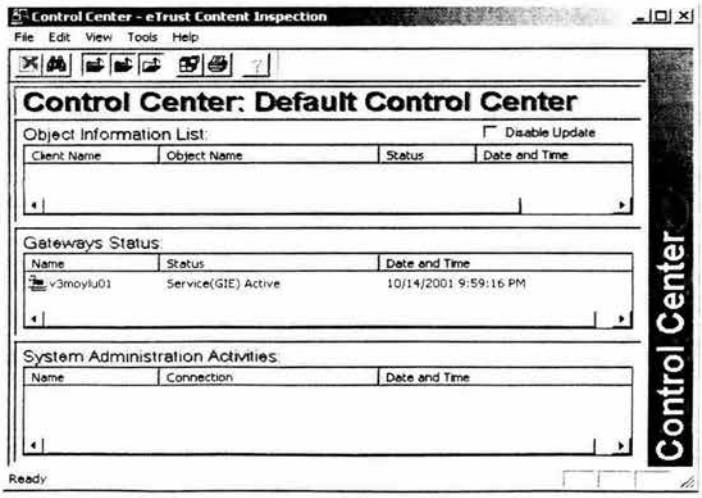


Figura 4.6. Pantalla del Control Center.

3) El *Audit Viewer*. Se conecta con el Control Center para recibir los resultados del escaneo por código malicioso. El detalle de la misma se puede observar en la Figura 4.7.

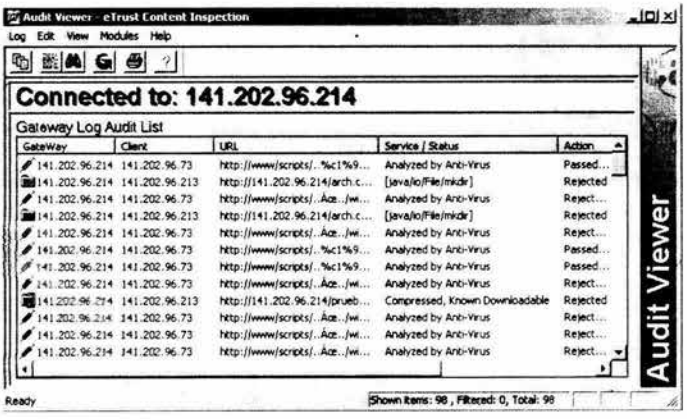


Figura 4.7. Pantalla del Audit Viewer del eTrust Content Inspection.

4) El *Policy Manager*. Es una interfaz gráfica donde se definen las reglas y políticas que aplicará el Gateway. La pantalla que presenta se puede ver en la Figura 4.8.

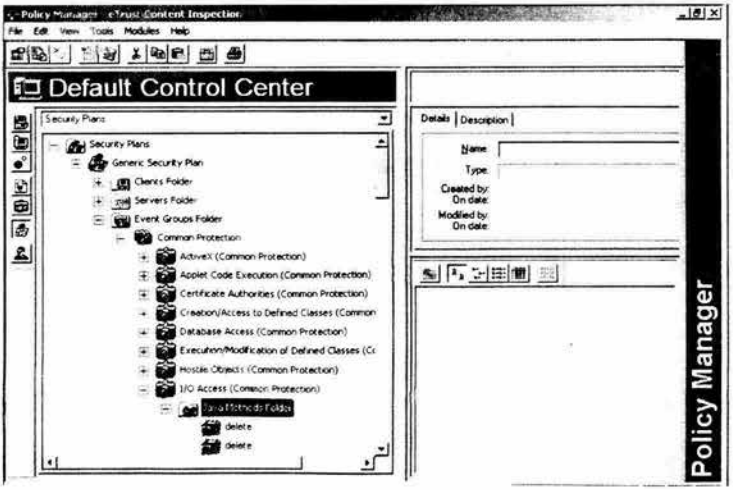


Figura 4.8. Pantalla Policy Manager del eTrust Content Inspection.

Configuración de la herramienta

Para definir las clases *JAVA* activadas, se hizo la contratación de un experto en programación en este lenguaje, de ahí se tomo como referencia el modelo predefinido que contempla *eTrust Content Inspection* llamado *Common Protection.*

Para la reconfiguración de eTrust *Content Inspection* se deben tomar en cuenta los siguientes puntos:

- Siempre que se instale el módulo de Gateway es necesario reinicializar el servidor.
- Después de instalar el producto, es necesario conectarse al Policy Manager para definir el password del administrador. La primera vez que se abre el Policy Manager pide un usuario y un password, éste es:

  Usuario: Admin
  Password: Admin

  Acto seguido el software pedirá se defina el nuevo usuario administrador, el cual es independiente al usuario *Windows NT* que se encuentra conectado en ese momento.

- Es muy importante conocer la dirección IP del Gateway y configurarla adecuadamente la primera vez que se accede la herramienta, ya que de lo contrario será necesario modificar el Control Center al cual se conecta el Gateway, esto se hace manualmente a través de las llaves del Registry.
- Es necesario que el Control Center siempre se encuentre activado, ya que es el encargado de la generación de los eventos y la aplicación de las políticas.

Memoria técnica eTrust Antivirus V 6.0

Como parte del proceso de instalación del *eTrust Antivirus*, se presentó un plan de actualización de la nueva vacuna para el Antivirus, ésta se actualizó utilizando la herramienta de distribución propia del mismo Antivirus. Se actualizó la vacuna hasta la versión 28.40, para esto se bajo la vacuna de esupport.ca.com, y se extrajo bajo el directorio f:\etrustci\vs.

Se copiaron los siguientes archivos:

filelist.txt, inoculatelT.txt, avh32dll.dll, virboot.dat, virsig.da0 y virsig.dat

del directorio:
f:\etrustci\vs
al directorio:
c:\programfiles\computer associates\etrust\contentinspection\gateway

Posteriormente se reinicializó el equipo. Se instaló la consola de administración en la Cd. de México, con configuración de actualización de vacuna diaria y distribución automática de las firmas a todos los equipos servidores y PC's en la WAN.

Licencias

En adición a la actualización de vacunas se configuró el archivo e aprobación de licenciamiento de *eTrust Antivirus*, para ello, se instaló en el servidor de la consola de administración bajo el directorio c:\licenseIT el producto License IT con el que se generó la requisición por la licencia, la cual se encuentra bajo el directorio c:\LicenseIT\lrf.

Memoria Técnica eTrust Policy Compliance V 1.0

Para la instalación del producto se requirió el siguiente software y equipo:

Para los servidores:

Equipo: tvs01
Función: Web Server
IP: 162.10.1.6
Producto: *eTrust Policy Compliance V 7.3* (Agente)
eTrust Policy Compliance V 7.3 (Cliente)
Directorio: e:\program files\epc
Versión SO: *Windows 2000 Advanced Server*
Password del Agente: antar99

Para la consola:

Equipo: tvs03
IP: 15.94.4.108

Producto: *eTrust Policy Compliance V 7.3* (Cliente)
Directorio: c:\program files\Computer Associates\eTrust\Policy Compliance
Versión SO: *Windows 2000 Profesional*

Podemos ver la arquitectura del producto *eTrust Policiy Compliance* en la Figura 4.9.

Se instaló el producto *eTrust Policy Compliance*, el módulo agent en el servidor tvs01 y el módulo Client en la consola Tvs03. Esta configuración tiene la peculiaridad que la comunicación entre el servidor y la consola se realiza a través del Firewall, por lo que fue necesario habilitar el acceso de la consola hacia el servidor mediante el puerto 1827. La arquitectura de *eTrust Policiy Compliance* se explica en la Figura 4.10.

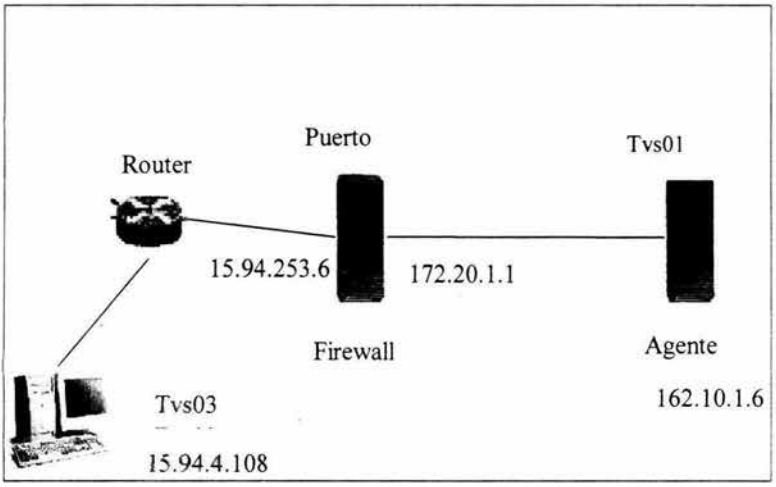


Figura 4.9. Configuración de eTrust Policy Compliance.

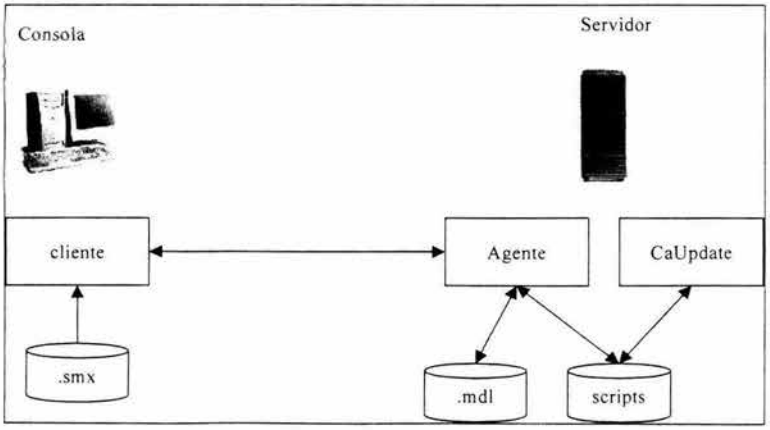


Figura 4.10. Arquitectura del Producto eTrust Policy Compliance.

Como se observa en la Figura 4.10, esta herramienta de software se compone de tres módulos:

1) El *Agente*. Que se encarga de correr los scripts para revisión del equipo y que levanta el servicio *eTrust Policy Compliance*, Figura 4.11.

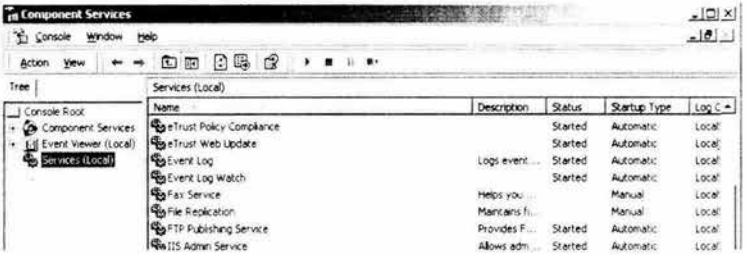


Figura 4.11. Pantalla de Configuración de eTrust Policy Compliance.

2) El cliente. Es la interfaz gráfica con la cual se definen las auditorias a realizar.

3) El *CA Update*. Es una interfaz gráfica y un servicio en donde a través de un enlace a Internet están bajando actualizaciones de los nuevos parches o actualizaciones de Sistema Operativo, base de datos o servidor de aplicaciones Web. Un ejemplo de esta pantalla se observa en la Figura 4.12.

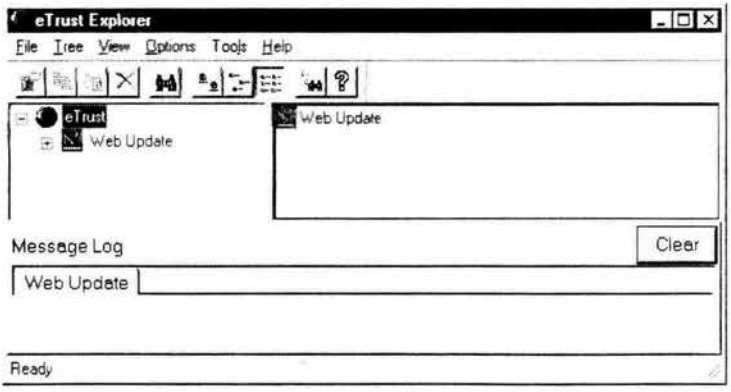


Figura 4.12. Pantalla de eTrust Policy Compliance CA Update.

En el cliente se pueden seleccionar las pruebas a ejecutar dependiendo del tipo de servidor y el nivel de seguridad deseado, generando lo que se conoce como una auditoria, la cual se guarda en el cliente bajo un archivo con extensión .smx.

El agente es el responsable de revisar el equipo y enviar los resultados al cliente. Este agente adicionalmente puede generar un modelo con extensión.mdl que son los resultados de las auditorías, con el objeto de que cualquiera de estos modelos

pueda ser utilizado posteriormente como una base y a partir del cual se puedan realizar comparaciones contra auditorías que se ejecuten posteriormente.

Modelos Configurados

Estos modelos se localizan bajo el directorio c:\ca\audits, y fueron obtenidos a través del nivel de seguridad predeterminado "NT-SRV". Para facilitar el entendimiento de los análisis, se configuraron 3 modelos diferentes, los cuales podemos ver en la Tabla 4.7. Cada uno de ellos presenta una observación, la cual explica su funcionamiento.

Estos tres modelos tienen configurados los siguientes parámetros de password:

Passwords\Password Aging\Password Age After Expiration	30
Passwords\Password Aging\Password Maximum Age	35
Passwords\Password Aging\Password Minimum Age	1
User Accounts\Old Accounts\Maximum Account Age	365

Title: an.tvs01 **Data source:** Live **Save data into model:** $HOST_an.mdl **Baseline comparison:** . **Targets:** tvs01 **Observaciones:** Tiene como objetivo agrupar todas aquellas pruebas que se utilizan para recabar información únicamente del equipo, en las cuales el resultado de las pruebas no es un error o falla en la seguridad, sino información que deberá analizarse para ver si la configuración es la adecuada.
Title: chk.tvs01 **Data source:** Live **Save data into model:** $HOST_chk.mdl **Baseline comparison:** . **Targets:** tvs01 **Observaciones:** Tiene como objetivo agrupar todas aquellas pruebas en las cuales deben cumplir con las políticas definidas para la televisora.

Tabla 4.7. Ejemplos de los modelos configurados.(Continúa)

Title:	base.tvs01
Data source:	Live
Save data into model:	$HOST_an.mdl
Baseline comparison:	$HOST_base.mdl
Targets:	tvs01
Observaciones:	
Tiene como objetivo definir las pruebas tanto de an.tvs como de chk.tvs para que como resultado de estas pruebas se generé un archivo que servirá como base.	

Tabla 4.7. Ejemplos de los modelos configurados.

Las pruebas que agrupan cada uno de estos modelos se describen a continuación. Un detalle de las pruebas de auditoría que se pueden aplicar se observan en la siguiente pantalla, Figura 4.13., y en la Tabla 4.8.

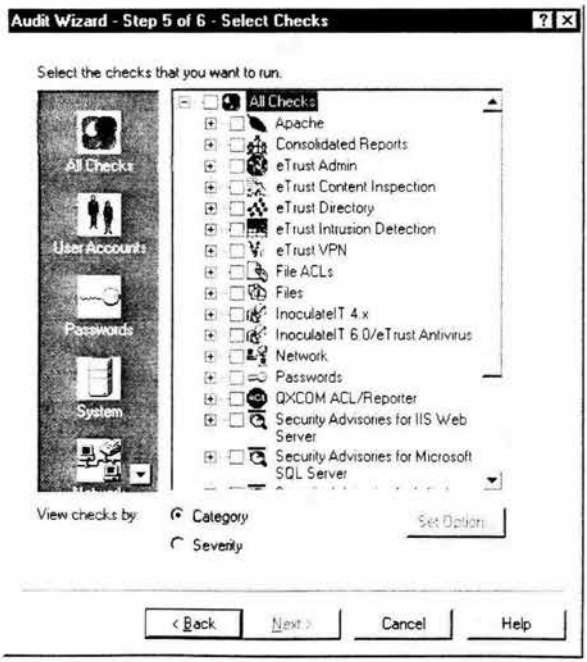


Figura 4.13. Producto eTrust Policy Compliance- Proceso de Auditoría.

Consolidated Reports		Srv.	An	Chk	Base
Changes from Baseline	I				☐
Detailed Audit Report.	I		☐		☐
Summary Audit Report	I		☐		☐
Summary Monitor Report	I				
Web Update Readme	I				
Web Update Status	I				

File ACLs		Srv.	An	Chk	Base
ACL Audit	L				
Unprotected System Files	H		☐		☐
Unprotected User Files	H	☐	☐		☐

Network		Srv.	An	Chk	Base
All Shared Directories	L		☐		☐
Hidden Shares	L		☐		☐
Shared Printers	L		☐		☐
User-Visible Shared Directories	L		☐		☐
World-Accessible Shared Objects	M		☐		☐

Passwords		Srv.	An	Chk	Base
Expired Passwords	M	☐		☐	☐
Locked Passwords	M	☐		☐	☐
Password Aging	M	☐	☐	☐	☐
Password LifeTime	M		☐		☐
Password Not Required	H	☐	☐		☐
Password Summary	I	☐	☐		☐

Security Advisories for Windows 2000		Srv.	An	Chk	Base
CAID-2124 (SCM Named-Pipe Impersonation Vulnerability)	H	☐		☐	☐

Tabla 4.8. Reporte de Auditoría de eTrust Policy Compliance.(Continúa)

Security Advisories for Windows 2000		Srv.	An	Chk	Base
CAID-2129 (Telnet Vulnerability)	H	□		□	□
CAID-2130 (Desktop Separation Vulnerability)	M	□		□	□
CAID-2133 (Protected Store Key Length Vulnerability)	M	□		□	□
CAID-2104 (Net BIOS Protocol Spoofing Vulnerability)	H	□		□	□
CAID-2125 (Relative Shell Path Vulnerability)	M	□		□	□
CAID-2132 (Frame Vulnerabilities)	M	□		□	□
CAID-2134 (IP Fragment Vulnerability)	M	□		□	□
CAID-2135 (Malformed Environment Variable Vulnerability)	M	□		□	□
CAID-2143 (TCP/IP Print Request Vulnerability)	M	□		□	□

System		Srv.	An	Chk	Base
Device Drivers	I	□	□		□
Device Summary	M	□	□		□
Registry ACLs	M	□	□		□
Registry Audit	M	□	□		□
Registry Protection	H	□	□		□
Services	I	□	□		□
Windows Version and Service Pack Info	I				

User Access Rights		Srv.	An	Chk	Base
Access Computer form the Network	M	□	□		□

Tabla 4.8. Reporte de Auditoría de eTrust Policy Compliance.(Continúa)

User Access Rights		Srv	An	Chk	Base
Act as Part of the operating system	M	□	□		□
Add Workstation to Domain	M	□	□		□
Backup Files and Directories	M	□	□		□
Bypass Traverse Check	M	□	□		□
Change System Time	M	□	□		□
Create a Page file	M	□	□		□
Create a Token Object	M	□	□		□
Create a Permanent Shared Objects	M	□	□		□
Debug Programs	M	□	□		□
Force Shutdown form Remote System	M	□	□		□
Generate Security Audits	M	□	□		□
Increase Quotas	M	□	□		□
Increase Scheduling Priority	M	□	□		□
Load and Unload Device Drivers	M	□	□		□
Lock Pages in Memory	M	□	□		□
Logon as a Service	M	□	□		□
Logon as Batch Job	M	□	□		□
Logon Locally	M	□	□		□
Manage Audit and Security Logs	M	□	□		□
Modify Firmware Environment Variables	M	□	□		□
Profile Single Process	M	□	□		□
Profile System Performance	M	□	□		□
Receive Unsolicited Device Input	M	□	□		□
Replace Process-Level Token	M	□	□		□
Restore Files and Directories	M	□	□		□
Shutdown the System	M	□	□		□
Take Ownership of Files and Other Objects	M	□	□		□

Tabla 4.8. Reporte de Auditoría de eTrust Policy Compliance.(Continúa)

User Accounts		Srv	An	Chk	Base
Account Groups	I	□	□		□
Account Policy	I		□		□
Account Statistics	I		□		□
Account Summary	I		□		□
Accounts with Guest Privileges Allowing Password Changes	H			□	□
Accounts with Missing Descriptions	M				
Accounts with No Full Name	L				
Accounts with no Home Directory	M				
Accounts with no Home Drive	M				
Accounts with no Logon script	M				
Accounts with no profile	M				
Automatic Login	H			□	□
Disabled Accounts	M	□		□	□
Duplicate UIDs	M	□		□	□
Enabled User Accounts with Guest Privileges	H		□		□
Expired Accounts	M	□	□	□	□
Group Summary	I	□	□		□
Guest Account	M			□	□
Locked Accounts	M	□		□	□
Login Failures	M	□		□	□
Never Expire Accounts	M	□	□		□
Never User Accounts	M	□		□	□
No Time restrictions	L	□	□		□
No Workstation Restrictions	L	□	□		□
Old Accounts	M	□	□		□
Privileged Accounts	H	□	□		□
With Time Restrictions	L	□	□		□
Workstation Restrictions	L	□	□		□

Tabla 4.8. Reporte de Auditoría de eTrust Policy Compliance. (Continúa)

Windows System Security		Srv.	An	Chk	Base
Account Management Audit Policy Status	I	□	□		□
Applications Event Log Status	M	□	□		□
Auditing of Rights Status	M	□		□	□
Auto Run Status	M	□		□	□
Automatic Logon Status	M	□		□	□
Caching of Logon Status	M	□		□	□
CD-ROM Drive Status	M	□		□	□
Detailed Tracking Audit Policy Status	I	□	□		□
Directory Service Access Audit Policy Status	I	□	□		□
Display of Last User Name Status	M	□		□	□
Floppy drive Status	M	□		□	□
LAN Manager Password Hash Support Status	M	□		□	□
Logon Legal Notice Caption	M	□	□		□
Logon Legal Notice Text	M	□	□		□
Page file Clearing Status	M	□		□	□
Password Filtering Status	M	□	□		□
Policy Change Audit Policy Status	I	□	□		□
Privilege Use Audit Policy Status	I	□	□		□
SMB Client Secure Signing Required Status	M	□		□	□
SMB Server Secure Signing Required Status	M	□		□	□
SMB Server Secure Signing Status	M	□		□	□
Submit Control Status	M	□		□	□
System Event Log Status	M	□	□		□
System Logon/Logoff Audit Policy Status	I	□	□		□
System Shutdown/Restart Auditing Policy Status	I	□	□		□

Tabla 4.8. Reporte de Auditoría de eTrust Policy Compliance.

En la Tabla 4.8. se puede observar el diseño del modelo de reporte de auditoria efectuado por la herramienta en el servidor Web, como parte de la memoria técnica. La definición de este reporte se emitió por categoría más no de acuerdo a severidad, se denominaron los niveles de seguridad para las diferentes categorías: la letra H denomina una Alta Severidad, los rubros clasificados con esta letra tienen el más alto impacto en el sistema de seguridad; problemas encontrados en rubros bajo esta clasificación representan la más alta vulnerabilidad en seguridad; para la letra M, Mediana Severidad, los rubros tienen un mediano impacto en el sistema de seguridad, por tanto la vulnerabilidad presentada es moderada; la L, es de Baja Severidad, los rubros en esta categoría representan un bajo riesgo para el sistema; aquellos que contemplan la letra I, sólo reportan información acerca de su estado. Dentro de la herramienta se contemplan máscaras pre-configuradas para generar reportes basándose en el establecimiento de metas definidas dentro de la empresa, esto se deja a consideración de la empresa televisora a ser utilizada para próximas auditorías. Si en un momento dado la empresa quisiera darle un peso a cada nivel de severidad, deberá tomar en cuenta el siguiente registro: Alta Severidad = 75; Mediana Severidad = 50; Baja Severidad =25 e Información = 0. Para el diseño de este modelo de reporte de la seguridad del sistema se configuraron todos los rubros marcados de la siguiente manera: la columna denominada Svr define si se encuentra activo o no el nivel de severidad, basándose en la clasificación comentada. La siguiente columna de este modelo, define el guardar o no el último dato del reporte, en aquellos recuadros que aparecen marcados con Chk, estos son lo rubros escogidos del modelo de diseño de auditoria para la empresa televisora. La última columna, denominada como base, define el comparar los parámetros históricos iniciales del modelo de reporte de auditoría diseñado, estos muestran los datos de las diferencias presentadas en reportes futuros comparando el estado base inicial.

Recomendación de la memoria técnica del producto eTrust Policy Compliance:

- La ejecución de las auditorías es demandante de recursos, sin embargo, no se utiliza ningún recurso hasta que se manda a ejecutar desde el cliente la auditoria, de tal manera que el servicio *eTrust Policy Compliance* no ocupa CPU, ni memoria hasta que se ejecuta la auditoría.
- Si las auditorías no son muy frecuentes, el servicio *eTrust Policy Compliance* puede permanecer apagado.
- La instalación y desinstalación de *eTrust Policy Compliance* no requiere reinicialización del equipo.

Con todo lo expuesto anteriormente se llevó a cabo la implementación del software del sistema de seguridad, formulándose de paso nuevas políticas de seguridad, para obtener así, una solución integra al problema de seguridad para la compañía televisora. Quedando ahora pendientes, para la parte final del presente trabajo, los resultados y conclusiones.

RESULTADOS Y CONCLUSIONES

De acuerdo a lo planteado al inicio del presente trabajo de tesis, se propuso resolver el problema de seguridad en la red de datos de una empresa televisora Mexicana, permitiéndole tener un grado óptimo de confianza, sobre todo en cuanto al control y detección de ataques informáticos; un claro monitoreo de las actividades de cada uno de los usuarios de su red, el monitoreo del correo electrónico saliente y entrante a Internet y por último controlar el acceso de los usuarios a servidores de misión crítica. Todo lo anterior basándonos siempre en las requisiciones de la empresa y el consecuente diseño de la política de seguridad de redes de la compañía.

Nuestro trabajo se enfocó en conseguir dichos objetivos, siempre pendientes de las necesidades particulares de la empresa en cuestión, escuchando en cada momento sus observaciones conforme se desarrollaba nuestro plan, y evaluando en cada momento la calidad de lo propuesto, con el fin de conseguir un sistema seguro y económicamente viable. Si bien, muchas de las soluciones implementadas reflejan esto, no significa decir que el sistema implementado está terminado, creemos que puede y debe seguir siendo perfeccionado conforme los requerimientos de la empresa lo permitan.

El presente trabajo muestra todo un método práctico para el aseguramiento de una red de datos de una compañía televisora mexicana, el cual puede ser aplicado a cualquier tipo de compañía. Como se puede observar este es un proyecto con un alto nivel de responsabilidad.

Durante la implementación del sistema se pusieron en práctica los conocimientos adquiridos en la carrera, complementando con nuevos conocimientos que vinieron a cimentar lo que ya se sabía dentro del área de las comunicaciones.

Podemos asegurar que se alcanzó la meta propuesta, es decir el diseño y la implementación de un sistema de seguridad viable para una red de datos. De esta manera se obtuvo un grado óptimo de control en la confianza general del sistema, -algo que no se tenía anteriormente-.

Haremos a continuación un desglose de la metodología empleada en la consecución de los objetivos propuestos, resaltando los resultados obtenidos en cada momento. Por ultimo, concluiremos dando una evaluación cualitativa de nuestro proyecto a manera de conclusión.

El capítulo uno contiene una introducción a los conceptos básicos de la tecnología de redes. Este capítulo sirve de recordatorio para una mejor comprensión de lo que se expone en el capítulo dos, donde nos enfocamos en específico en la

seguridad de redes. La metodología a seguir se explicamos en el capítulo tres. Partimos primeramente de un análisis concienzudo del sistema de la red de datos de la empresa televisora. Tratando de vislumbrar cuales podrían ser sus necesidades. En seguridad se pudo observar de qué adolecía y en que aspectos también estaba bien provista. Para lograr esto, fue necesaria la elaboración de un cuestionario profesional que nos permitiera comprender cabalmente estos factores. Estos cuestionarios se elaboraron apoyados en los estándares más reconocidos a nivel internacional, como son el BS7799 y el ISO17799, de los cuales parten una gran variedad de mejores prácticas en seguridad, así como las recomendaciones de instituciones especializadas en este rubro, tales como *Gartner Group*. Este cuestionario lo consideramos como una herramienta valiosa y que puede ser aprovechado en cualquier sistema de red que se desee asegurar.

Elaborada la encuesta, procedimos a su análisis. Éste se realizó con el mayor grado de profesionalismo posible, ya que consideramos fue la fase vital del proyecto. Los resultados obtenidos en esta fase de la metodología fueron expuestos a los directivos de la compañía asignados al proyecto, para deducir soluciones posibles y viables de acuerdo al caso en particular. Del análisis de las encuestas se desprendieron las vulnerabilidades específicas de la red de datos, y de éstas los puntos que se debían fortalecer.

Considerando lo comentado en el párrafo anterior, se creó una nueva arquitectura de red, aprovechando la existente, como se observa en el capítulo cuatro del presente trabajo. Esta arquitectura cumple con los objetivos iniciales de proteger la red de datos en los puntos señalados anteriormente: control y detección de ataques informáticos, un claro monitoreo de las actividades de cada uno de los usuarios de la red, monitoreo del correo electrónico saliente y entrante a Internet y por último controlar el acceso de los usuarios a servidores de misión crítica.

Cabe comentar que el sistema contaba en un inicio con los enlaces necesarios para la WAN. Sin embargo, la necesidad de crear una interacción directa entre proveedores, personal laborando fuera de las áreas establecidas de trabajo y la empresa en sí, dio como resultado el requerimiento de datos y servicios desde un sitio Web. La nueva arquitectura cumple este punto.

El diseño fue plenamente justificado, muy en especial, en lo relacionado al uso de las herramientas de software comercial que necesitábamos implementar para conseguir los objetivos propuestos. Como resultado de esto se llego a la decisión de implementar una arquitectura basada en una solución consolidada de marca única. Esta marca nos proveía de las mejores expectativas a lo que nosotros requeríamos y lo que la empresa necesitaba.

Una vez que completamos la fase del diseño y elección de fabricante, procedimos a la última etapa de la implementación del sistema de seguridad. Para ello, nos pusimos en contacto con los proveedores del software de seguridad seleccionado, adquiriendo los servicios que ellos proveían. Estos incluían una garantía de satisfacción de su producto. Debemos de mencionar que toda la fase de

facturación y compra de los productos mencionados fue responsabilidad de la empresa televisora. También tuvimos que interactuar directamente con el personal de la empresa televisora a cargo de la red, para conseguir que el diseño se lograse efectuar. La implementación se llevo acabo de acuerdo al plan de trabajo formulado en el capítulo cuatro. Las distintas etapas de la implementación fueron comentadas en su momento en dicho apartado.

Los resultados del proyecto son una de las partes esenciales del trabajo, ya que son en general el reforzamiento real de la seguridad de la red de datos de la empresa y por consiguiente la consecución de los objetivos de la tesis.

Se dejó un sistema de red protegido por los diversos productos. Éstos cubren de manera concreta todas las vulnerabilidades y amenazas que nuestro estudio arrojó.

Asimismo, se redefinió la red LAN creando las zonas MZ y DMZ para las áreas estratégicas de la compañía, logrando de esta forma asegurar la información crítica de ésta.

Otro resultado del proyecto fue la creación de una verdadera reforma a las políticas de seguridad de la compañía. Estas abarcan todos los aspectos importantes de seguridad de la red de datos: desde las cuestiones de accesos físicos, utilización diaria de la red, los privilegios con los que cada usuario podrá contar y los procedimientos en caso de ataques y fallas del sistema con la finalidad de proteger los activos más importantes de la empresa, hasta consideraciones prácticas de actualización de los sistemas operativos. Estas políticas de seguridad fueron aplicadas por el personal a cargo de la red, una vez que completamos la implementación del sistema de seguridad.

Adicionalmente se facilitó la revisión de estas políticas mediante el mantenimiento de las reglas de control de la herramienta *eTrust Content Inspeccion*, de acuerdo a lo visto en el capítulo cuatro del presente trabajo.

En forma específica, los resultados más importantes de todo el proyecto en sí fueron:

- La administración del sistema se mejoró al implementar en nuestra arquitectura una consola central de administración (queriendo decir con esto que todos los sistemas de seguridad implementados pueden ser manejados desde una máquina, y no que es sólo una máquina la que lleva este proceso) que unifica todos los productos y permite una gestión de los recursos de seguridad de manera clara y expedita.
- La configuración del sistema operativo en distintos servidores de la red también se vio beneficiado al aplicarse el producto *eTrust Policy Compliance* sobre la estructura de la DMZ, que afectó a todo el sistema en general.

- Se mejoró el análisis de los posibles incidentes que pudieran ocurrir, al crearse un registro de incidentes bien administrado. Esto se logró mediante la herramienta *eTrust ID*, la cual almacena información del sistema en forma de archivos bien organizados para su estudio posterior. También permitió una mejor clasificación de los reportes correspondientes.
- Se consiguió una buena cobertura antivirus y de software malicioso al anexar el producto *eTrust ID* a todas las máquinas de la compañía televisora, aplicando su poderoso motor antivirus para los segmentos de red, antepuestos a los servidores donde ya estaba el antivirus instalado anteriormente a nuestra implementación.
- Se Incrementó la seguridad en el rubro de la política de continuidad del negocio, al aumentar la frecuencia y confiabilidad de las actualizaciones gracias a la implementación de la herramienta *eTrust Policy Compliance* sobre el servidor Web de la DMZ.
- Se reforzaron las políticas de seguridad en el manejo de documentos, archivos de audio, video y datos, a través de la herramienta *eTrust ID*, al bloquear las URLs no autorizadas, logrando detectar y sitiar patrones sospechosos que puedan representar un riesgo.
- Se reforzó la política de seguridad con respecto al uso de recursos, especialmente del correo electrónico, lo anterior se llevó acabo al interactuar con la herramienta *eTrust CI* sobre el servidor de correo electrónico en la MZ y filtrando además los JavaScripts o VBscripts que pudieran encontrarse en la página Web.
- Se consolidó la protección a los servidores de misión crítica, el servidor Web y la LAN de la empresa, mediante la implementación del software *eTrust Firewall*, esto a través de su propiedad de traducción de direcciones de red, permitiendo así, ocultar las direcciones IP auténticas, traduciéndolas por otras para evitar una posible penetración.
- Se fortaleció la política de tráfico de frames TCP sobre de toda la red, asegurando sólo el tráfico autorizado, esto se consiguió con la habilidad de la solución *eTrust Firewall* de filtrado de paquetes inteligente a nivel de aplicación. Pudiendo definir según la política, las direcciones IP de cada una de las Tarjetas de la Red, desde donde se podría recibir o enviar información al Internet.

Si hacemos un recuento del logro de los objetivos propuestos para el presente proyecto y los confrontamos con los resultados expuestos, podemos aseverar que se llego a una solución de los mismos. Esta solución queda declarada mediante la arquitectura completamente realizada, con el software funcionando correctamente y con las memorias técnicas que corresponden a la etapa posterior a la instalación del sistema. Dichas memorias, como se describió en el capítulo cuarto, nos indican que el producto y el procedimiento de seguridad trabajan adecuadamente y que por lo tanto el sistema está seguro. A partir de este momento, corresponde a la empresa televisora el juzgar los resultados en la práctica extendida durante varios meses. Si bien, confiamos que el software implementado ya habia sido probado por la empresa proveedora *Computer Associates* y certificado por varias

entidades internacionales como *ICSA*. Nosotros estamos seguros de que, conforme a lo expuesto en el capítulo cuatro, nuestra selección del software y de la arquitectura implementada fueron las más indicadas.

Las recomendaciones que hacemos a la compañía basándonos en los resultados y la experiencia obtenida en los análisis de la situación de la misma, son las siguientes:

- Se recomienda establecer VPN para enlaces seguros entre computadoras remotas.
- Sugerimos que se definan con anticipación y claridad todos aquellos trabajos especiales que requieran privilegios de red para los usuarios de la misma.
- Aconsejamos establecer una reglamentación en lo referente a la seguridad de la compañía, con obligaciones, derechos y sanciones, claramente definidas para todos los empleados, proveedores y clientes de la misma, siendo la misma compañía quien valúe las sanciones por violaciones a las políticas de seguridad cometidas.
- Se recomienda el incrementar el entrenamiento sobre seguridad a los encargados del mantenimiento de la red, en especial sobre aspectos de: reporte de amenazas y ataques, virus, seguridad física, ingeniería social (aprovecharse de la ignorancia del personal para lograr algún fin en específico), administración de cifrado de activos y accesos a servidores, licencias de software, descargas de archivos, estándares y políticas de seguridad y manejo de las alertas de seguridad de organizaciones acreditadas.
- Vemos la necesidad de extender la comunicación de las políticas de seguridad de la compañía mediante: carteles, folletos, boletines, foros, reuniones y talleres.
- Sugerimos la modernización de todos los accesos físicos de la empresa, especialmente a los de tecnología de Información.
- Aconsejamos que el plan de contingencia en caso de desastres sea reforzado y adecuado a los estándares vigentes en la actualidad.

Otro punto importante del presente trabajo fue el de sensibilizar e informar a la industria mexicana que la cultura en seguridad es muy pobre, por ejemplo: en el rubro de seguridad no existe el término de "retorno de inversión", y sólo se observa el "riesgo de no invertir", que dicho sea de paso, es muy alto.

Finalmente nuestra propuesta considera y advierte que no existe ningún sistema de red 100% seguro -a pesar de que algunos afirmen lo contrario-, ya que estamos hablando de máquinas y programas que siempre están en constante evolución y desarrollo, por lo que nuestra última recomendación es mantenerse siempre alerta ante nuevas amenazas, estar actualizado con respecto a las nuevas tecnologías y productos que nos pueden ayudar para contrarrestar estos ataques, buscar que la empresa mantenga el control de su operación de una

forma más efectiva y automatizada y hacer de las cuestiones complejas cosas prácticas y simples en su manejo, lo anterior debe de formar parte del trabajo diario de cualquier empresa.

BIBLIOGRAFÍA

Libros

1. Ford ,Merilee. *Tecnologías de interconectividad de redes*. Edit., Prentice Hall. México. 1998.
2. Russel, Charlie y Crawford, Sharon. *Guía Completa de Windows NT 4.0 Server*. Edit., Mc Graw Hill. España. 1997.
3. Tomasi, Wayne. *Sistemas de comunicaciones electrónicas*. Edit., Prentice Hall. México. 1996.
4. Stewart, James Michel. *MCSE Networking Essentials*. Edit., Coreolis. USA. 2001.
5. Forcada, Navarro. *Windows 2000 Server Curso Oficial de Certificación*. Edit., Mc Graw Hill. México. 2001.
6. E. Larson, Morris. *CCNP Routing*. Edit., Coreolis. USA. 2000.
7. A. Deal, Richard. *CCNP Switching*. Edit., Coreolis. USA. 2000.
8. Dennis, Craig. *Remote Access*. Edit., Coreolis. USA. 2000.
9. Feibel, Werner. *The Encyclopedia of Networking*. Edit., The Network Press. USA. 1996.
10. Berg,Glenn. *MCES Networking Essentials*. Edit., New Riders. USA. 2000.

Manuales

1. Computer Associates International. *Etrust Policy Compliance Administrator Guide 7.4*. USA. 2003.
2. Computer Associates International. *Etrust Firewall Getting Started*. USA. 1999-2000.
3. Computer Associates International. *Etrust Intrusion Detection 1.5 Installation Guideline*. USA. 2001.
4. Computer Associates International. *Etrust Intrusion Detection 1.5 Advanced Training*. USA. 2001.
5. Computer Associates International. *Etrust Content Inspection Quick Installation Guide*. USA. 2001.

Direcciones de Internet

1. http://www.techworld.com/
2. http://www.centrored.com/winproxy/manual.htm
3. http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
4. http://www.saulo.net/pub/tcpip/
5. http://support.real-time.com/windows/vpn/windows_nt_vpn.html
6. http://www.cert.org
7. http://www.cesg.org.uk
8. http://www.icsalabs.com
9. http://www.butlergroup.org

Boletines

1. *Infoworld México, El Periódico para la Estrategia en TI.* Edit., International Data Group. Num., 39. México D.F., México. Junio 2003-08-27.
2. *Technology Evaluation and Comparison Report: Network Security The Benefits and Pitfalls of Contemporary Network Security Technologies.* Edit., Butler Direct Limited. Londres, Inglaterra. Febrero 2003.

Conferencias

1. *II Conferencia Anual: Seguridad de la Información y el Mundo del eBusiness.* Gartner Group. México. Septiembre 2000.
2. *Using an Internationally Recognized Methodology for Risk Management.* USA. 2002.

APÉNDICE

GLOSARIO DE TÉRMINOS

ACL - Access Control List: Lista de Control de Accesos
Son tablas que indican al Sistema Operativo de aquellos privilegios que tiene el usuario y que son reconocidos por el sistema.

ANSI - American National Standars Institute: Instituto Nacional Americano de Estándares
Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos. ANSI es miembro de ISO.

ARP - Address Resolution Protocol: Protocolo de Resolución de Dirección
Protocolo de resolución de direcciones. Protocolo Internet usado para ligar una dirección IP a direcciones Ethernet / 802.2. Está definido en el documento RFC 826.

Broadband
Sistema de transmisión que multiplexa varias señales independientes en un solo cable. En la terminología de las telecomunicaciones, se refiere a cualquier canal que tenga un ancho de banda mayor que el requerido para transmitir voz (4 kHz). En la terminología de las redes locales, se refiere a un cable coaxial que maneja señales de tipo analógico.

Bypass
Modo de operación en redes FDDI y Token Ring en el cual se ha desviado una interfaz del anillo.

CERT - Computer Emergency Response Team: Equipo de Respuesta a Emergencias Computacionales
Situado en la Carnegie Mellon University en los Estados Unidos, es una organización líder en lo que respecta a consultores de seguridad en redes.

CSMA/CD - Carrier Sense Multiple Access with Coallision Detection: Acceso Múltiple con Detección de Portadora y Detección de Colisiones
Mecanismo de acceso al canal en el cual los dispositivos que desean transmitir primero verifican la existencia de portadora en el canal. Si no se detecta portadora en un cierto lapso, los dispositivos pueden transmitir. Si dos de ellos transmiten a la vez, ocurre una colisión, que es detectada por dispositivos especiales, que entonces retardan la retransmisión durante un período aleatorio.

DNIDS - Distributed NIDS: Sistema de Detección de Intrusos Distribuido
Consiste en el monitoreo de varias redes con un enfoque global, cuyo objetivo es encontrar datos que puedan servir a servicios de espionaje que afecten a la industria a nivel mundial.

DNS - Domain Name System: Nombre del Dominio del Sistema
Nombre de sistema distribuido usado en Internet.

DoS - Denial of Service: Negación de Servicio
En el momento que se tiene una petición legítima por parte del usuario y ésta no puede responderse, es debido a que el sistema está saturado por una demanda en exceso.

ESP - Encapsulating Security Payload: Encapsulamiento de Carga Útil de Seguridad
Se ofrece como un servicio de seguridad por parte del IPSec.

Ethernet
Especificación de la red LAN de banda base inventada por la corporación Xerox y desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet operan a 10 megabits por segundo utilizando CSMA/CD sobre cable coaxial. Es similar a una serie de estándares producidos por IEEE y conocidos como IEEE 802.3.

FDDI - Fiber Distributed Data Interface: Red de Interfaz de Datos Distribuida por Fibra
Estándar definido por ANSI que especifica una red token passing de 100 Mbps empleando cable de fibra óptica.

Frame Relay
Protocolo empleado en la interfaz entre dispositivos de usuario (por ejemplo, host y enrutadores) y equipo de redes (por ejemplo, nodos de conmutación). Es más eficiente que X.25; protocolo del cual generalmente se considera como reemplazo.

FTP - File Transfer Protocol: Protocolo de Transferencia de Archivos
Protocolo de aplicación IP para transferir archivos entre nodos de la red.

HIDS - Host based Intrusion Detection System: Sistema de Detección de Intrusos basado en Equipo
Este IDS es el que se localiza directamente en un host.

HTTP - HyperText Transfer Protocol: Protocolo de Transferencia de Hipertexto
Este protocolo se utiliza para intercambiar archivos sobre el WWW. Los archivos son pedidos de un servidor Web usando una URL y es enviada al cliente.

IAB - Internet Activities Board: Grupo de actividades de Internet
Investigadores de interconexiones entre redes que se reúnen regularmente para discutir asuntos pertinentes de Internet. El grupo define políticas de Internet mediante decisiones y asignación de fuerzas de trabajo para asuntos varios.

IACS - Information Assurance and Certification Services: Servicios de Certificación y Aseguramiento de la Información
Servicio de certificación independiente desarrollada para el crecimiento de los sistemas y productos de la IT.

ICMP - Internet Control Message Protocol: Protocolo de Control de Mensaje de Internet
Protocolo de la capa de red que permite que los paquetes de mensajes reporten errores e información reelevante al procesamiento de paquetes IP. Está documentado en RFC 792.

IDS - Intrusion Detection System: Sistema de Detección de Intrusos
Es un software de seguridad, empleado para prevenir ataques de intrusiones a un sistema. Puede ser configurado para un solo dispositivo o para una red completa.

IEEE - Institute of Electrical and Electronics Engineers: Instituto de Ingenieros en Electrónica y Electricidad
Organización profesional que define estándares de redes. Los estándares LAN de IEEE son los predominantes en la actualidad, e incluyen protocolos similares o virtualmente equivalentes a Ethernet y Token Ring.

IETF - Internet Engineering Task Force : Fuerza de Tarea en Ingeniería de Internet
Equipo de trabajo IAB que consiste en más de 40 grupos responsables de asuntos ingenieriles, relacionados con el Internet con la propuesta de soluciones a corto plazo.

IGP - Interior Gateway Protocol: Protocolo de Servidores de Intercomunicación Internos
Protocolo de Internet usado para intercambiar información de enrutamiento en un sistema autónomo. Ejemplos usuales de IGP Internet son IGRP, RIP y OSPF.

IMAP - Internet Message Access Protocol: Protocolo de Acceso de Mensaje de Internet
Es un método de acceso al correo electrónico que se mantiene en el servidor correspondiente.

IP - Internet Protocol: Protocolo de Internet
Protocolo de capa 3 (Capa de Red) que contiene información de direccionamiento y de control para permitir el enrutamiento de paquetes. Está documentado en el RFC 79 I.

IPSec - IP Security: Protocolo de Seguridad en Internet
Es un estándar de seguridad desarrollado por la IETF que provee una autentificación y cifrado de los paquetes de IP.

ISO - International Standar Organization: Organización Internacional para la Estandarización
Organización internacional responsable de una amplia gama de estándares, incluyendo aquellos reelevantes para las redes. ISO es la responsable del modelo OSI.

IT - Information Technology: Tecnología de la Información
Apoyados en los sistemas de hardware, son los procesos en cuanto al manejo de la información se refiere, con la finalidad de preservar la seguridad de los datos y el acceso a esta información.

LAN - Local Area Network: Red de Area local
Red que cubre un área geográfica relativamente pequeña (usualmente no mayor que un grupo local de edificios).

LLC - Logical Link Control: Control Lógico de Enlace
Subcapa de la capa de enlace OSI definida en la IEEE. Se encarga del control de errores, control de flujo y creación de marcos. El protocolo LLC más usado es IEEE 802.2, que incluye variantes sin y con conexión.

MAC - Media Access Control: Control de Acceso al Medio
Como está definida por la IEEE, se trata de la porción baja de la capa de enlace de datos del modelo OSI. La subcapa MAC se encarga de los asuntos de acceso al medio de comunicaciones, como por ejemplo determinar sí se usará token passing (paso de estafeta) o contention (competencia).

Malware
Software malicioso cuyo fin es comprometer las defensas de toda red.

MAN - Metropolitan Area Network: Red de Area Metropolitana
En términos generales se refiere a una red que ocupa un área metropolitana, geográficamente mayor que la ocupada por una red local (LAN), pero menor que la de una red amplia (WAN).

MSAU - Multistation Access Unit: Unidad de Acceso a Estaciones Múltiples
Una unidad MAU se conoce como transceiver (transmisor/receptor) en la especificación Ethernet. En el segundo caso (llamadas también MSAU), se trata de concentradores de cables a los cuales se conectan los nodos de token ring.

NFS - Network File System: Sistema de Archivo de Red
Es un conjunto de protocolos de sistemas de archivos distribuidos, que permite el acceso remoto de archivos en una red.

NIDS - Network Intrusion Detection System: Sistema de Detección de Intrusos de Red
Implementación de un IDS a nivel de red.

NTFS - Native File System: Sistema de Archivo Nativo for Windows NT
Seguridad que implementa Windows para la partición de archivos.

OSI - Open Systems Interconnection: Interconexión de Sistemas Abiertos
Programa internacional de estandarización, apoyado por ISO y la CCITT, para desarrollar estándares para redes de datos. Facilita la interoperabilidad de equipos hechos por diversos fabricantes.

Protocol Stack
Capas de software de protocolo relacionadas, que juntas funcionan para realizar una arquitectura específica de comunicaciones. Los ejemplos incluyen AppleTalk, DECnet y muchos otros.

POP - Point of Presence: Punto de Presencia
Es un punto de acceso Físico a una compañía de larga distancia.

POP3 - Post Office Protocol: Protocolo de Oficina de Correo
Protocolo que permite el acceso al correo electrónico.

RAS - Remote Access Services: Servicio de Acceso Remoto
Medio mediante el cual se realiza una comunicación entre una terminal local y una remota.

RFC - Request for Comments: Petición de Comentarios
Documentos empleados como el medio primario de la comunicación de información sobre Internet. Algunos RFC son designados por el IAB como "Estándares de Internet". La mayoría documenta especificaciones de protocolos, como Telnet y FTP. Están disponibles a través de los Centros de Información de la red Internet.

RIP - Routing Information Protocol: Protocolo de Información de Ruta
IGP proporcionado con los sistemas UNIX. Es el IGP más común en Internet.

SMTP - Simple Mail Transfer Protocol: Protocolo de Transferencia de Correo Simple
Protocolo que ofrece servicios de correo electrónico.

SNMP - Simple Network Management Protocol: Protocolo Simple de Administración de Red
Este protocolo de manejo de redes de Internet ofrece medios para seguir y determinar la configuración de la red y los parámetros al tiempo de ejecución.

TCP/IP - Transmision Control Protocol/Internet Protocol: Protocolo de Control de Transmisión/Protocolo de Internet
Los dos protocolos de Internet más conocidos, que erróneamente suelen confundirse con uno solo. TCP corresponde a la capa 4 (Capa de Transporte) del modelo de referencia OSI y ofrece transmisión confiable de datos. IP corresponde a la capa 3 (Capa de Red) del modelo de referencia OSI, y ofrece servicios de datagramas sin conexión. TCP/IP fue desarrollado por el Departamento de la Defensa de los Estados Unidos en los años 70, como apoyo a la construcción de interconexión de redes a escala mundial.

TELNET - Remote Terminal Emulation: Emulación de Terminal Remota
Protocolo estándar de Internet de emulación de terminales.

Token Ring
Red LAN tipo token-passing desarrollada y manejada por IBM. Es muy similar a la red LAN IEEE 802.5

TNP - Time Network Protocol: Protocolo de Tiempo en la Red
Este protocolo es utilizado para sincronizar los relojes de los equipos, dándoles una desviación de entre 100ms y 10ms, lo cual es importante en algunas aplicaciones, sobre todo de seguridad.

UDP - User Datagram Protocol: Protocolo de Datos de Usuario
Protocolo sin conexión de la Capa de Transporte que pertenece a la familia de protocolos de Internet.

URL - Universal Resource Locator: Localizador de Recursos Universal
Ubicación de la información dentro de la WWW.

VPN - Virtual Private Network: Red Privada Virtual
La VPN ofrece un medio mediante el cual existe una comunicación entre un sitio local y un sitio remoto, lo que le permite a toda organización un acceso seguro. El flujo de la información se lleva a cabo dentro de un "túnel".

X.25
Recomendación CCITT que define el formato de los paquetes para las transferencias de datos en redes públicas de datos. Muchos establecimientos tienen redes X.25 que les dan acceso a terminales remotas. Esas redes se pueden usar para otros tipos de datos, incluyendo los protocolos de Internet, DECnet y XNS.