UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

SEGURIDAD DE LOS RECURSOS DE LA RED IMPLEMENTANDO CONTROLADORES DE DOMINIO EN UNA PLATAFORMA DE WINDOWS NT SERVER Y WORKSTATION

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

BARAJAS MARROQUIN NORA

ZIGA TELLEZ MARCO ANTONIO

MEXICO, D. F. DICIEMBRE DE 1999

A MIS PADRES Y HERMANOS :

POR APOYARME EN LOS MOMENTOS MAS DIFICILES, Y BRINDARME SU CONFIANZA Y CARIÑO.

A MI ESPOSO Y A MI HIJO:

PORQUE REPRESENTAN LO MAS IMPORTANTE EN MI VIDA, Y PORQUE GRACIAS A SU AMOR HE ALCANZADO UNA META MAS EN LA VIDA.

MARCO ANTONIO
Y PABLO

AGRADEZCO A LAS AUTORIDADES Y PROFESORES DE LA E.N.E.P. ARAGON QUE DIRIGIERON MI FORMACION PROFESIONAL.

N O R A

A MIS PAPAS :

A MIS DOS MEJORES AMIGOS QUE ME HAN DADO TODO SU CARIÑO, AMOR, COMPRENSION, SU VIDA, ES MAS DE LO QUE UN HIJO PUEDE PEDIR.

GRACIAS QUERIDOS
PAPA Y MAMA

A MIS HERMANOS :

EL ESTAR UNIDOS Y AL APOYARNOS TE DA SEGURIDAD Y FUERZA.

GRACIAS MARIO Y SILVIA

A MI ESPOSA :

LA LUZ MAS INTENSA DE MI VIDA LLEGO CUANDO TU LLEGASTE A ELLA. GRACIAS NORA SIEMPRE ESTARAS EN MI CORAZON.

A MI HIJO :

UN REGALO DIVINO LLEGO PARA BENDECIR MI VIDA CON FELICIDAD, ARMONIA Y PAZ. GRACIAS PABLO ERES LO MAS HERMOSO QUE HE RECIBIDO.

AGRADEZCO A LAS AUTORIDADES Y PROFESORES DE LA E.N.E.P. ARAGON QUE DIRIGIERON MI FORMACION PROFESIONAL.

AGRADEZCO A MIS AMIGOS EL CUARTETO INFERNAL POR TODO LO QUE HEMOS PASADO.

M A R C O A N T O N I O

INDICE

INTRODUCCION

Cualquier medida de seguridad corporativa, inclusive la utilización de complejos dispositivos de avanzadas tecnologías, podría ser inconducente sino se enmarca dentro de una estrategia organizacional que establezca las políticas de seguridad; las que deben considerar aspectos tales como autentificación, encripción[1], control de acceso físico y lógico, protecciones contra virus, etc. sobre las redes corporativas. El acceso no autorizado, daño o mal uso de la información de las empresas se puede traducir en pérdidas financieras a corto y mediano plazo, y así afectar su posición competitiva en el mercado con todos los prejuicios que ello podría significar. Para enfrentar este desafío, la empresa debe establecer sus propias políticas de seguridad, basadas en medidas tecnológicas, administrativas y organizacionales, cimentadas en la identificación de los riesgos, vulnerabilidades e impactos organizacionales a la que se expone a través de sus redes de comunicaciones.

La presente Tesis se basa en la implantación de técnicas de seguridad de los recursos de la red en una plataforma de Windows NT Server y Workstation, lo cual sirve para la administración de usuarios e información a través de *Controladores de Dominio*. Se desarrolló en la Empresa PEMEX (Petróleos Mexicanos), en la Unidad Corporativa de Sistemas de Información Geográfica (SICORI).

Los objetivos primordiales a cumplir en el desarrollo de está investigación se enlistan a continuación.

- Identificar los problemas originados en la implantación de *Controladores de Dominio* para la administración de usuarios e información.
- Desarrollar técnicas de seguridad para los miembros de un *Dominio*.
- Monitorear fallas, errores y accesos remotos, para garantizar el buen funcionamiento de los Recursos de la Red.
- Evaluar las necesidades de los diferentes grupos de trabajo dentro de la empresa, para otorgar privilegios en el uso de recursos dentro del sistema.

La empresa cuenta con equipo altamente calificado (tecnología de punta) que requiere trabajar con aplicaciones que corran a 32 bits, y Windows NT ofrece esta característica; además agrega una atractiva combinación de estabilidad y seguridad en cuanto a servicios de red se refiere, y a la administración de usuarios Con ello los usuarios obtienen un incremento en el desempeño de su

[1] Este tema se ve en el punto 1.4.3.4 del primer capítulo

trabajo, un amplio rango de nuevas y mejores características de conectividad y seguridad en accesos remotos

Entre las ventajas que ofrece Windows NT sobre otros sistemas operativos de red, es que restringe todo tipo de privilegios a los administradores, es decir, el administrador es el único que puede agregar o eliminar aplicaciones, e incluso volver a formatear un disco duro. Un administrador, en sí, es quien tiene el control de todas las opciones de seguridad que implica el trabajo en red Es quien puede asignar un extenso arreglo de permisos de acceso para grupos individuales y predefinidos, incluyendo por ejemplo. *Usuarios de Dominio, Grupos globales y locales*, etc

Una de las principales razones que llevó a la empresa a la necesidad de implantar técnicas de seguridad de los recursos de la red, es porque se cuenta con grupos de usuarios variados dentro de ésta, y se requiere que cada una de las áreas cuente con integridad y seguridad de su propia información, lo cual implica, generar las permisiones que negaran todos los servicios a los usuarios, excepto aquellos específicamente permitidos por los administradores de sistemas

La metodología empleada en la realización de este trabajo, fué en primera instancia, una investigación documental en libros, revistas y manuales especializados en el tema. Lo siguiente, fué la implementación de técnicas de seguridad de los recursos de la red, para llevar a cabo la administración de usuarios e información a través de los *Controladores de Dominio* de Windows NT El contenido de la presente Tesis, se encuentra dividido en cinco capítulos

En el Capítulo I. **Introducción a las Redes de Computadoras**.- Se desarrolla una introducción de las Redes de computadoras, mencionando antecedentes, conceptos, clasificación y seguridad de estas.

En el Capítulo II. **Sistema Operativo de Windows NT**.- Se detalla el Sistema Operativo Windows NT, y se presentan los principales modelos de Sistemas Operativos que existen en el mercado. Se presenta desde la historia, arquitectura, características, funcionamiento, seguridad, inconvenientes, etc. de Windows NT; así como también se especifican cualidades especiales de Windows NT Server y Windows NT Workstation.

En el Capítulo III **Administración de Windows NT**.- Se presenta la Administración de Windows NT, planteando la configuración de cuentas de usuarios y de grupos; así como las políticas, derechos y perfiles de usuarios. También se mencionan otras herramientas importantes en cuanto a seguridad se refiere, como son el Sistema de Archivos de Windows NT, el Administrador de Tareas, Impresión de Archivos y el Administrador de Discos.

En el Capítulo IV. **Controladores de Dominio: Construcción y Seguridad** - Es el capítulo más importante, ya que es donde se presenta y

desarrolla la Construcción y Seguridad de los Controladores de Dominio, tema principal de esta Tesis.

En el Capítulo V. **Pruebas de Desempeño de la Seguridad en Windows NT** - Se dan a conocer las pruebas de desempeño de la seguridad en Windows NT, presentándose las herramientas de administración de Windows NT para monitorear las configuraciones, rendimiento y actividades de los servidores y la red.

Al final de cada uno de los capítulos, se presenta el desarrollo prático que se siguió en está investigación.

Finalmente, se dan las conclusiones obtenidas en el desarrollo de este trabajo; así como también, se proporciona un glosario de términos y se enlista la bibliografía utilizada, los cuales pueden ser consultados para profundizar en el tema.

INTRODUCCION A LAS REDES DE COMPUTADORAS

Asegurar la información en una red de computadoras debe ser un objetivo ineludible para las organizaciones. Hasta el día de hoy, los sistemas abiertos con poco nivel de control preceden a los mecanismos de seguridad a favor de la integridad y de la confidencialidad de la información. La solución a este problema no es resolver solo un aspecto puntual o una parte del sistema, hay que abordar el conjunto de la red

Un administrador de sistemas debe decidir qué programas ejecutará en la red, qué miembros de la organización tendrán acceso, y qué conexiones se permitirán desde el exterior

Dependiendo del valor que el administrador de sistemas pone en la seguridad y el acceso, la política de seguridad puede ser conservativa o liberal. Una organización debe encontrar un balance que entregue la máxima seguridad mientras todavía se permitan accesos liberales y el uso del Software popular

Desarrollar una Política de Seguridad implica un balance entre la conveniencia y la protección de un sistema computacional.

1.1 ANTECEDENTES DE REDES DE COMPUTADORAS

Durante el siglo pasado se desarrollaron una gran variedad de redes de comunicaciones, hasta alcanzar la situación actual, en la que rodean el mundo y se extienden por el espacio El radio, la televisión y el teléfono permiten que millones de personas estén en contacto, a menudo salvando distancias de miles de kilómetros.

Se encuentran de moda las redes de computadoras y se empiezan a demandar cada vez más servicios, algunos especializados, sobre todo lo relacionado al modelo Cliente/Servidor. Otros de los aspectos que están siendo desarrollados, son las bases de datos con servidores especializados y la información suele estar distribuida y desde ambientes amigables es accesada.

Más allá del hardware y del software, las redes constituyen una infraestructura de integración corporativa, las empresas están descubriendo el efecto sinergético del trabajo de grupos a través de las redes Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de

información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento sin precedente de la industria de las computadoras, así como a la puesta en órbita de los satélites de comunicación.

Aunque los primeros sistemas de comunicación, como el telégrafo, utilizaban un código digital (el código Morse) para transmitir la información, el mayor peso de los desarrollos necesarios para dar lugar a estas redes de comunicación ha ido dirigido hacia la transmisión de voz e imagen, de forma analógica. Con la llegada de las computadoras, la situación ha cambiado de nuevo. La información se envía en forma digital, cada vez en cantidades mayores. La combinación de computadoras y redes de comunicaciones es una de las principales áreas de desarrollo en la actualidad, teniendo un impacto tan profundo en el estilo de vida de millones de personas como lo tuvieron la radio y el teléfono en su momento.

Un proceso cualquiera de comunicación está constituido por un *emisor* que envía *información* a través de un *canal* de transmisión, la cual es recibida por un *receptor*. Podemos por tanto, hablar de comunicación oral, escrita, etc., donde el canal será respectivamente el aire, el papel, etc.

La información no es transmitida directamente, sino que se utilizan unos *codigos* entendibles por el emisor y el receptor, y que se comunica mediante *señales* físicas. Los códigos serán el lenguaje utilizado y las señales las ondas sonoras, luminosas, etc.

El objetivo de un proceso de comunicación es que la información que se quiere transmitir sea idéntica a la que se recibe. Si falla cualquiera de los elementos que intervienen (transmisor, canal de transmisión o receptor), se producen pérdidas de información; para intentar evitarlo, se repiten los mensajes en su totalidad o en parte (redundancia), o se acompañan de códigos especiales (de control) que permitan reconstruir la información.

Las principales razones de ser de las comunicaciones informáticas son:

- La necesidad de transmitir y recibir datos
- El compartir recursos. No todos los usuarios de un sistema informático van a poder disponer de un sistema adecuado a sus necesidades Se ven pues obligados a compartir tanto los equipos como los programas
- La compartición de carga. Consiste en distribuir el trabajo que supone el proceso de datos entre varias computadoras (por ejemplo, en un banco, a la *hora pico*, la computadora central se puede encontrar saturada y puede pedir a otra computadora que le ayude, distribuyendo así la carga de trabajo entre las distintas computadoras).

1.2 CONCEPTO DE RED

Utilizaremos el concepto de "**redes de computadoras**" para dar a entender una colección interconectada de computadoras autómatas. Se dice que dos computadoras están interconectadas, si éstas son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicaciones. Una *red de computadoras* consiste de dos o más computadoras conectadas por un canal de comunicación de manera tal que sus usuarios pueden almacenar, manipular y compartir datos electrónicos, programas y dispositivos de E/S (periféricos). Las máquinas conectadas pueden ser, microcomputadoras, minicomputadoras, grandes computadoras, terminales, impresoras, dispositivos de almacenamiento, entre otros.

Los objetivos principales de una red son.

- Compartir información
- Comunicar usuarios.
- Tener flexibilidad en el manejo de la información

Una red de computadoras permite a los usuarios compartir instantáneamente y sin esfuerzo la información.

1.2.1 Sistemas Distribuidos

Un Sistema Distribuido es un conjunto de dispositivos heterogéneos enlazados de distintas formas, que les brindan a los usuarios y a las aplicaciones un acceso transparente a los datos, recursos y servicios que se encuentran a todo lo largo de la red. (Entendiendo por la *red* a todos los tipos de conexiones locales y remotas que se tengan)

Lo que se persigue, en última instancia, es que se tenga una Red Virtual, una colección de Redes locales de los grupos de trabajo, departamentos de la empresa o interempresas que sean tan fácilmente accesibles y tan invisibles a los usuarios, que éstos sólo necesiten ver la computadora que operan

Bajo esta definición general, existen una serie de funcionalidades que se deben brindar. Para un usuario será importante poder leer archivos de distintas computadoras, para otro será necesario utilizar servidores de comunicaciones para accesar información en otros ambientes, o otro más podría querer un ambiente en el cual dividir los procesos de una aplicación entre los servidores que estén disponibles, y así ejecutarla más rápidamente

1.2.2 Protocolo

El intercambio de información entre los distintos dispositivos tiene que estar regido por unos *protocolos* que lo regulen. Consisten en un conjunto de normas comunes para establecer la comunicación tanto para el receptor como para el emisor. Desde el comienzo de la industria informática, cada fabricante intentaba idear una serie de procedimientos, con los cuales podía controlar la información y así monopolizar el mercado de las ventas de los distintos elementos que componen la informática. Con el paso del tiempo esta industria se ha extendido tanto, que surge la necesidad de compatibilizar los procedimientos de la información Actualmente existen asociaciones de fabricantes de computadoras, y organizaciones internacionales como por ejemplo ISO (International Standard Organization - Organización Internacional para la Normalización), que establecen unas recomendaciones sobre los procedimientos normalizados de comunicación, que van a gobernar ese intercambio de información. Un protocolo es pues, un conjunto de procedimientos normalizados o estandarizados que gobiernan el intercambio de comunicaciones, acuerdos o convenios que se adoptan para poder establecer una comunicación correcta, afectan a las frecuencias de las señales, reconocimiento de la conexión, código de recepción y emisión, control de errores, control de la sincronía, inicio de las operaciones, establecimiento de los caminos por los que irán los mensajes, asegurar que los datos han sido recibidos, etc

1.2.3 Tipos de Computadoras

Las computadoras que forman parte de una red pueden desarrollar dos tipos de funciones.

- ❑ Servidor
- ❑ Estación de trabajo

El servidor es aquella o aquellas computadoras que van a compartir sus recursos hardware y software con los demás equipos de la red Es empleado tanto por su potencia de cálculo, como por la información que gestiona, y los recursos que comparte Las computadoras que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red, así como los servicios que proporcionan los servidores a los cuales pueden acceder. También se puede pensar en computadoras híbridas, que hacen a la vez de servidores y de estaciones de trabajo Existen dos tipos de servidores:

- **Servidores dedicados** son aquellas computadoras que están exclusivamente a disposición de la red
- **Servidores no dedicados** además de tomar el papel de servidores también pueden utilizarse como estaciones de trabajo

El diseño de la infraestructura de una red de computadoras es una de las labores más importantes que debe llevar a cabo el ingeniero que la esté montando para una empresa. La red más pequeña puede constar de un único servidor y unas cuantas estaciones de trabajo conectadas mediante tarjetas y cables de red; redes más grandes pueden estar constituidas por varios servidores y una gran cantidad de estaciones de trabajo con sedes distribuidas alrededor de todo el mundo, lo cual conlleva el empleo de redes de comunicación (la red telefónica, Internet, etc.) para interconectar entre sí los equipos de todas las sedes

Una vez diseñada la infraestructura que va a tener una red de comunicación de computadoras hay que implementarla. Para ello es necesario instalar en cada computadora la tarjeta o circuito integrado necesario para la comunicación y establecer el camino físico que una todas las computadoras de la red.

1.3 CLASIFICACION DE REDES

❑ De acuerdo a su extensión geográfica las redes se clasifican:

◗ **Redes de Area local (LAN).** La red de área local (LAN, Local Area Network) nos va a permitir compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia software) y periféricos como puede ser un módem, una impresora, un digitalizador, etc. (se elimina la redundancia hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el chat. Además una red de área local conlleva un importante ahorro, tanto de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar sólo una conexión telefónica compartida por varias computadoras conectadas en red, como de tiempo, ya que se logra control de la información y del trabajo

Las redes locales permiten interconectar computadoras que estén dentro de un mismo edificio o en edificios colindantes, pero siempre teniendo en cuenta que el medio físico que los une no puede tener más de unos miles de metros

Los beneficios del uso de una red de computadoras de área local, se resumen en los siguientes:

- Se pueden compartir periféricos costosos, como son impresoras, plotters, módems, y digitalizadores.
- Se pueden compartir grandes cantidades de información mediante el empleo de administradores de bases de datos en red. Con ello se evita la redundancia de datos y se facilita su acceso y actualización
- La red se convierte en un mecanismo de comunicación entre los usuarios conectados a ella, ya que permite el envío de mensajes mediante el empleo del correo electrónico, ya sea entre usuarios de la red local o entre usuarios de otras redes o sistemas informáticos, programando reuniones o intercambiando archivos de todo tipo
- Se aumenta la eficiencia de las computadoras, poniendo a disposición del usuario todo un sistema que hace que las consultas sean más rápidas y cómodas.
- Se trata de un sistema completamente seguro, pudiendo impedirse que determinados usuarios accedan a áreas de información concretas, o que puedan leer la información pero no modificarla. El acceso a la red está controlado mediante nombres de usuario y claves de acceso. El control de los usuarios que acceden a la red lo lleva a cabo el sistema operativo El control de los usuarios que acceden a la información lo lleva a cabo el software de administración de bases de datos que se esté empleando.

Una red de área local está formada por computadoras con sus periféricos y por elementos que conectan entre sí dichas computadoras. Los dispositivos de conexión son tarjetas de red, cables o cualquier medio físico que permita a las computadoras intercambiar bytes de información (como puede ser un repetidor) necesarios para conectar las computadoras entre sí, de modo que quede formada la red local. Las grandes empresas suelen hacer uso de otras redes de comunicaciones, como puede ser la red telefónica, para interconectar sus redes locales entre sí

Las computadoras que forman parte de una red pueden estar formadas por distinto hardware (procesadores RISC, CISC, computadoras MAC, computadoras SUN, etc) y rodar bajo distintos sistemas operativos (Windows, Amiga WorkBench MacOS, Linux, Unix, etc.), para que se puedan comunicar entre ellas, sólo es necesario que exista un camino físico y que empleen el mismo protocolo de comunicaciones (TCP/IP, NETBEUI, IPX/SPX, etc.).

◗ **Redes de Area Amplia (WAN).** Son aquellas en las que es necesario conectar equipos de comunicación remota a las computadoras que integran la red Estas computadoras pueden ser "mainframes", minicomputadoras o computadoras personales. La extensión geográfica que abarca una red de este tipo puede ir desde una ciudad, un país o la comunicación intercontinental

◗ **Redes de Area Metropolitana (MAN).** Estas redes son denominadas híbridas, ya que pueden conectar los mismos tipos de computadoras que el arreglo anterior, pero se diferencian de las WAN, en que los equipos de comunicación no son tan complejos, pues no se transmite a distancia muy grande. Su extensión geográfica abarca desde una ciudad hasta una región especifica de un país.

❑ De acuerdo a los Medios de Transmisión las redes se clasifican:

◗ **Red Telefónica**. En una comunicación telefónica se utilizan con frecuencia los términos *pares* y *cuadretes* para describir al circuito que compone el canal. Los circuitos de pares se conocen como circuitos "semi-duplex" = Rj-11, en el cual uno de los hilos sirve para transmitir los datos y el otro es la línea de retorno eléctrico. Los circuitos de cuatro hilos se conocen como circuitos "full-duplex" = Rj-45 (estos arreglos incluyen un par de hilos para la transmisión de datos y los otros dos cierran el circuito eléctrico). Para las compañías telefónicas un enlace de 2 hilos corresponde a un circuito telefónico conmutado "normal", mientras que un circuito de cuatro hilos será una línea privada no conmutada

◗ **Redes de Microondas.** En una red de microondas, se utilizan antenas de transmisión y de recepción, repetidores y el espacio atmosférico como medio físico de transmisión La información se transmite en forma digital, a través de ondas de radio de muy alta frecuencia, y por lo tanto, de una longitud de onda mínima (microondas) Las estaciones consisten de una antena tipo parábola y de circuitos

que interconectan la antena con la terminal del usuario. El alcance promedio entre las antenas es de 40 Kmts., y una de las ventajas más importantes de utilizar los enlaces de microondas, es la capacidad de poder transportar miles de canales de voz a grandes distancias a través de repetidores, a la vez que permite la transmisión de datos en su forma digital.

◗ **Red Satelital** Actualmente es muy común el uso de satélites en redes de procesamiento y transmisión de datos y se espera, que con este tipo de dispositivos de comunicación se pueda establecer una cobertura de comunicación virtualmente en todo el planeta, eliminando de forma definitiva el obstáculo que desde el punto de vista de las comunicaciones representan los océanos y las montañas El satélite de comunicaciones es un dispositivo que actúa como "reflector" de las emisiones terrenas. Se puede decir, que el enlace de satélites es la extensión al espacio del concepto de torres de microondas, ya que al igual que éstas, los satélites reflejan un haz de microondas que transporta información codificada.

1.3.1 Medios de Transmisión de la Red

Para transferir señales entre computadoras se necesitan: un medio de transmisión para portar las señales y dispositivos para enviar y recibir las señales.

Las señales eléctricas se generan como ondas electromagnéticas (señales analógicas) o como una secuencia de pulsos de voltajes (señales digitales). Para propagarse, una señal debe viajar a través de un medio físico, el llamado medio de transmisión Hay dos medios de transmisión, guiados y no guiados.

Los medios guiados se fabrican de forma que las señales se confinan a un canal de transmisión estrecho y que se puede predecir su comportamiento. Son habituales, los cables de par trenzado (como los telefónicos), cables coaxiales (como los de las antenas de televisión) y cables de fibra óptica

Los medios no guiados son partes del entorno natural, a través de los que se transmiten las señales bajo forma de ondas Las frecuencias habituales corresponden con el espectro de radioondas (VHF y microondas) u ondas de luz (infrarrojo o visible)

Para planificar una red de computadoras, se exige un medio de transmisión, o combinación de ellos, en base a las circunstancias físicas, a la construcción de la red y las prestaciones que se requieren de ella Un objetivo habitual es guardar el costo al mínimo, basándose en las necesidades planteadas.

1.3.1.1 Dispositivos de Transmisión y Recepción

Una vez que se tiene un medio de transmisión, se necesitan los dispositivos que propaguen y reciban las señales a través del medio elegido. Estos pueden ser, adaptadores de red, repetidores, concentradores, transmisores diversos y receptores

❑ Adaptadores de red

Se fabrican de diversas formas, la más habitual es una placa de circuito impreso que se instala directamente en un zócalo de expansión de la computadora. Otros están diseñados para microcomputadoras portátiles, por lo que consisten en un dispositivo pequeño, que se conecta a la salida de impresora o a una ranura PCMCIA. Estos adaptadores se fabrican en diversas versiones, de forma que se puedan conectar a cualquier tipo de medio guiado. También se pueden conectar a dispositivos que puedan transmitir mediante medios no guiados.

❑ Repetidores

Se usan para incrementar las distancias a las que se puede propagar una señal de red. Cuando una señal viaja a través de un medio encuentra resistencia y gradualmente se hace más débil y distorsionada. Técnicamente este proceso se denomina atenuación.

❑ Puentes (Bridges)

Permiten conectar una LAN a otra red con diferentes protocolos en los niveles físico y de enlace, pero siempre que en los niveles superiores usen los mismos protocolos Es un hardware y software que permite que se conecten dos redes locales entre si Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Generalmente, se usa un puente externo con una estación dedicada para incrementar de esa forma el rendimiento de la interconexión. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, o la red de conmutación de paquetes

❑ Pasarelas (Gateways)

Se usan para conectar una LAN a otra red que utilice otros protocolos. Se emplean para conexión entre diferentes redes locales, o entre locales y amplias (WAN)

❑ Concentradores (HUB)

Se usan en redes de microcomputadoras para proporcionar un punto común de conexión para dispositivos de computación. Todos los concentradores tienen repetidores, además de otras funciones propias

❑ Transmisores de microondas

Transmisores y receptores de microondas, especialmente satélites, se usan para transmitir señales a grandes distancias. El medio de transmisión es la atmósfera.

❑ Transmisores infrarrojos y láser

Son análogos a los de microondas También usan la atmósfera como medio, sin embargo sólo son válidos para distancias cortas, ya que la humedad, niebla, obstáculos y otros fenómenos ambientales pueden causar problemas de transmisión.

❑ Módem

Un módem convierte señales digitales a analógicas (audio) y al revés, mediante la modulación y demodulación de una frecuencia portadora Se usan para transmitir las señales a través de líneas telefónicas. Es un periférico que permite que dos computadoras se puedan comunicar entre si, vía red telefónica conmutada. En este caso, uno de esas computadoras formará parte de la red, mientras que la otra será remota.

1.3.2 Topología de Redes

La topología de una red de computadoras hace referencia a como se distribuye u organiza el conjunto de computadoras dentro de la red A continuación se describen las topologías más comunes

❑ Topología en Estrella

La topología en estrella es una de las más antiguas, en ella, todas las estaciones están conectadas a una computadora central que actúa a modo de servidor. Todas las comunicaciones entre las estaciones se realizan a través de la computadora central, que es lo que controla la prioridad, procedencia y distribución de los mensajes La computadora central será normalmente el servidor de la red, aunque puede ser un dispositivo especial de conexión. Esta configuración presenta una buena flexibilidad a la hora de incrementar el número de equipos; además, la caída de una de las computadoras periféricas no repercute en el comportamiento

general de la red. Sin embargo, si el fallo se produce en la computadora central, el resultado afecta a todas las estaciones.

El diagnóstico de problemas en la red es simple, debido a que todas las computadoras están conectados a un equipo central. No es una topología adecuada para grandes instalaciones, ya que al agruparse los cables en la unidad central crea situaciones propensas a errores de administración, precisando además, grandes cantidades de costosos cables.

En algunos casos a este tipo de topología también se le conoce como Topología de Estrella/Bus, porque físicamente esta configurada como estrella, pero lógicamente funciona como un bus

❑ Topología en Anillo

Todas las estaciones están conectadas entre sí formando un anillo, de modo que cada estación tiene conexión directa con otras dos Los datos viajan por el anillo de estación en estación siguiendo una única dirección, de manera que toda la información pasa por todas las estaciones hasta llegar a la estación destino, en donde se queda. Cada estación se queda con la información que va dirigida a ella y retransmite al nodo siguiente las que tienen otra dirección

La velocidad de respuesta de este tipo de redes irá decreciendo conforme el flujo de información sea mayor; cuantas más estaciones intenten hacer uso de la red, más lenta irá esta, pero en todo caso siempre se puede averiguar el tiempo máximo de respuesta.

En una estructura en anillo, un fallo en cualquier parte de la vía de comunicación deja bloqueada a la red en su totalidad, mientras que un fallo en cualquiera de sus estaciones no necesariamente implica la caída de la totalidad de la red El coste total del cableado será menor que en una configuración en estrella.

❑ Topología en Bus

Todas las estaciones están conectadas a un único canal de comunicaciones, toda la información circula por ese canal y cada estación se queda solamente con la información que va dirigida a ella

Estas redes son sencillas de instalar y poseen una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones. La cantidad de cable que utilizan es mínima, sobre todo si la comparamos con la cantidad necesaria para la topología en estrella, ya que el cable no tiene que ir desde el servidor a cada una de las estaciones de trabajo. El fallo de una estación aislada no repercute en la red, aunque la ruptura del bus dejará la red totalmente inutilizada. Esta es la topología de red mas extendida

El inconveniente de esta red es el control del flujo, ya que aunque varias estaciones intenten transmitir a la vez, como sólo existe un bus, únicamente una de ellas podrá hacerlo, por lo que el control de flujo será más complicado cuantas más estaciones tenga la red, ya que se pueden producir más intentos simultáneos (colisiones). Además, es difícil aislar los problemas de cableado y determinar que estaciones o segmentos del cableado lo producen, ya que todas las estaciones pasan su información por el mismo cable

1.3.3 Tipos de Redes

Al hablar de "hardware" de red no hay más remedio que hablar de las implementaciones que existen en el mercado de ciertas normas creadas por el IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos). Cada una de estas normas engloba toda una serie de características entre las que destacan la topología, velocidad de transferencia y tipos de cable. Se describen tres tipos de redes: Arcnet, Ethernet y Token Ring.

❑ Ethernet

La redes Ethernet emplean una topología en bus con el método CSMA/CD (Carrier Sense Multiple Access with Collision Detection - Sensor de Portadora de Accesos Múltiples con Detección de Colisiones) para acceder al medio. Eso significa que cualquier estación puede intentar transmitir datos en cualquier momento, pero como todas ellas están conectadas a un único cable común, sólo una estación puede estar transmitiendo por el cable (bus) en un momento dado. Para solucionar los problemas de colisiones en la transmisión existen una serie de normas como son, antes de transmitir comprobar que no haya otra estación transmitiendo, o que en caso de colisión la estación causante espere un margen de tiempo aleatorio antes de volver a intentar el envío de datos Todas estas tareas son realizadas automáticamente por el software de red a unas velocidades tan elevadas que el usuario no se da cuenta de las colisiones.

❑ Token Ring

Es una red en anillo con paso de testigo. Eso significa que las computadoras conectadas a la red se van pasando un testigo de unas a otras de forma secuencial y cíclica, de modo que sólo puede transmitir información aquella computadora que posea el testigo en un momento dado Como la velocidad de transmisión de este tipo de redes puede ser hasta 16 Mbps, el usuario no se da cuenta del tiempo que tiene que esperar su computadora antes de recibir el nuevo testigo para poder empezar a transmitir. Las distintas computadoras de la red se conectan a las unidades de acceso multiestación, MAU (Multistation Acces Unit), dentro de las cuales está formado el anillo.

❑ Arcnet

Es una red en banda base que transmite a una velocidad de 2.5 Mbps, con una topología híbrida estrella/bus Este sistema fue desarrollado en 1978 por la empresa Datapoint[1], aunque fue potenciado en el mundo de las microcomputadoras por la empresa Standard Microsystems. Todas las computadoras de la red se conectan en estrella a un distribuidor central denominado *HUB activo*.

[1] DONALD H. Sanders, *Informática, Presente y Futuro*, México, 1990, McGRAW HILL

1.4 SEGURIDAD EN REDES

Actualmente por la complejidad a la cual suelen tender las estructuras físicas de las redes de computadoras se necesitan herramientas capaces de detectar fallas dentro de los sistemas de cómputo de diferentes niveles. Uno de los niveles dentro de los cuales se presta mayor importancia es el medio físico y monitoreo de dispositivos, cableado, tramas transmitidas, etc.

El tema de la seguridad de las redes está definitivamente sobre el tapete y requiere soluciones de corto plazo. Cualquier medida de seguridad corporativa, inclusive la utilización de complejos dispositivos de avanzadas tecnologías, podría ser inconducente si no se enmarca dentro de una estrategia organizacional que establezca las políticas de seguridad, las que deben considerar aspectos tales como autentificación, encripción, control de acceso físico y lógico y protecciones contra virus, sobre las redes corporativas El acceso no autorizado, daño o mal uso de la información de las empresas se puede traducir en pérdidas financieras inmediatas y, a mediano plazo, afectar su posición competitiva en el mercado con todos los perjuicios que ello podría significar. Para enfrentar este desafío, la empresa debe establecer sus propias políticas de seguridad, basadas en medidas tecnológicas y administrativas, cimentadas en la identificación de los riesgos, vulnerabilidades e impactos organizacionales a la que se expone a través de sus redes de comunicaciones.

La elaboración de una estrategia de seguridad corporativa debe considerar la identificación de amenazas, riesgos, vulnerabilidades y una evaluación de los costos organizacionales

Un aspecto importante que muchas veces se olvida es que más del 75% de los problemas inherentes a la seguridad se producen principalmente por fallas de los equipos y/o mal uso que hace el personal de la propia organización[2]. Esto quiere decir que un plan de seguridad debe contemplar no solo los ataques provenientes del mundo exterior ajeno a nuestra empresa sino también los procedimientos de uso interno También es importante saber que el mal funcionamiento de un componente en una red (disco duro, CPU, equipo de comunicaciones,etc) es la principal causa de los problemas de seguridad que se presentan en una organización.

Existen por otro lado dos aspectos contradictorios en las redes; por un lado su razón de ser es facilitar la comunicación y el acceso a la información, y por otro asegurar que no accesen a la misma aquellos elementos que no se desea que lo hagan. Esta contradicción está presente continuamente, ya que aquello que mejora la seguridad dificulta el uso, alentiza los accesos, exigiendo un compromiso entre ambos aspectos.

[2] http://www.iurix.es/biblio/libro/cm96_p14.htm

En un plan típico de seguridad se deben considerar los siguientes aspectos:

- Seguridad física de los accesos donde se encuentran los sistemas.
- Asegurarse contra todos los riesgos posibles, esto requiere un periodo de observación y una clasificación de los recursos y sistemas que están en los edificios de la organización, los que están fuera, los puntos de acceso remoto, las costumbres y hábitos del personal y el uso de la microinformática estática y portátil.
- Asegurarse que es una integración por encima de los sistemas, plataformas y elementos que constituyen las redes.
- La administración de la seguridad debe de ser centralizada

1.4.1 Sistema de Seguridad

La implementación de un Sistema de Seguridad en Redes debe contemplar los siguientes aspectos:

- Posibilidad de negar todos los servicios, excepto aquellos específicamente permitidos por el administrador de sistemas.
- Una administración flexible, para que los nuevos servicios o necesidades se puedan implementar fácilmente.
- Soporte de técnicas líderes de autenticación.
- El filtro de IP debe ser flexible, fácil de programar y debe poder filtrar tantos atributos como sea posible, incluyendo dirección IP destino y fuente
- Uso de Proxies en servicios como FTP y Telnet.
- Tener la posibilidad de filtrar y centralizar los accesos remotos.
- Contener mecanismos para guardar registros de tráfico y de actividad sospechosa.
- Generar alarmas o mecanismos para detectar.
- Que se ejecute en un host dedicado.
- Que se base en un sistema operativo seguro.
- Que sea simple en el diseño, por lo que puede ser comprendido y mantenido fácilmente
- Que pueda ser actualizado.

Podemos definir un *ataque* o *amenaza* como la potencial violación de un sistema de seguridad Las amenazas pueden producirse a partir de alguno de estos hechos:

- Modificación ilegal de los programas (virus, caballos de troya, borrado de información, etc)
- Deducción de información a partir de datos estadísticos o de uso, que se utilizan para reconstruir datos sensibles.
- Destrucción y modificación de datos controlada o incontroladamente.
- Cambio en la secuencia de los mensajes.
- Análisis del tráfico observando los protocolos y las líneas de comunicación o los discos de las computadoras
- Pérdida del anonimato o de la confidencialidad.
- Uso de una identidad falsa para hacer transacciones o enviar operaciones.
- Violación de los sistemas de control de acceso.

1.4.2 Seguridad de una Computadora

Hay tres formas principales de atacar la seguridad de una computadora

- Obtención no autorizada de información.
- Modificación no autorizada de información.
- Acceso no autorizado de servicio a los usuarios.

Estos ataques se clasifican en *pasivos* y *activos*, que se describen a continuación.

❑ Ataques pasivos

Son aquellos que no producen daño físico a las computadoras, a la información, o a cualquier componente de la red. Se refieren más bien, a la obtención fraudulenta de los datos, la cual puede tener lugar en cualquier punto del enlace de comunicaciones o de la red

Los enlaces por microondas y satélite se pueden interceptar mediante receptores de radio de alta sensibilidad Los lóbulos laterales de las antenas de microondas permiten monitorear las señales en las proximidades de las torres repetidoras, sin estar en la ruta directa del haz principal. Los enlaces por satélite son accesibles en una zona bastante amplia alrededor de la estación receptora de tierra. También son posibles los ataques activos a enlaces de datos vía satélite y microondas, pero son fáciles de detectar.

El cable coaxial de alta calidad y correctamente instalado emite una cantidad despreciable de energía electromagnética, pero si el cable se dobla más de lo que permite su radio de curvatura máximo, se incrementan las fugas Un equipo de radio sería capaz de intervenir de forma no invasiva en el enlace

Cualquier equipo electrónico para transmisión de datos, puede radiar emisión electromagnética a partir de la cual se pueden obtener los datos. Un receptor sensible localizado cerca del equipo o conectado a sus líneas de alimentación o a otros conductores cercanos, se puede utilizar para filtrar y grabar las emisiones Los teléfonos sirven de receptores excelentes para la radiación de campo cercano procedente de una computadora

❑ Ataques activos

Son aquellos que producen daño físico a las computadoras, a la información, o a cualquier componente de la red

1.4.3 Esquemas de Seguridad en Redes de Datos

Es indudable el valor que tiene la información en nuestra sociedad. Es mediante flujos de información que hacemos transferencias de dinero (Bancos, cajeros automáticos o teleservicios), nuestra información está almacenada en registros médicos, registros de pagos de impuestos, registros bancarios de historia de crédito y en el caso de la medicina pre-pagada es la información de nuestros estados de cuenta la que nos permite o no, acceder a los servicios; igual sucede con los servicios públicos, servicios de telefonía celular, la cuenta de Internet o el T V. cable.

En el mercado corporativo la información que posee una compañía le permite diferenciarse de la competencia y le da ventajas competitivas En el mundo empresarial conocemos la importancia de mantener la información de contactos actualizada, de modo que la información pueda fluir a los canales adecuados en el tiempo adecuado.

En pocas palabras, la información que posee hoy en día una compañía, tiene un precio y normalmente es alto, comparable incluso a los activos de las compañías. Sin embargo, muchas compañías en nuestro país toman pocas o ninguna precaución a la hora de cuidar sus datos

"El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias armados muy bien pagados Aún así, no apostaría mi vida por él".[3] Todo esto realmente no la hace muy funcional y tal vez sería más fácil no tener computadora. Pensar en aislar una red completamente es algo así como no tener carro, porque existe la posibilidad de que lo roben; al igual que existen alarmas para autos de distinta complejidad, existen varios esquemas de seguridad para redes de datos que se pueden utilizar

1.4.3.1 Acceso Físico a los Equipos

Uno de los primeros puntos a proteger es el acceso físico a los equipos, se requiere diseñar estrategias que mantengan los puntos más sensibles de un sistema fuera del acceso de los usuarios que no tienen nada que hacer allí, ya que según las estadísticas, muchos de los ataques a la red son internos. Es entonces recomendable que los centros de cableado, los concentradores, los armarios de distribución de pares, los servidores, enrutadores, switches, multiplexores, equipos de Frame Relay, Equipos de X.25, Equipos de ATM, módem y demás equipos neurálgicos se encuentren fuera del alcance de los operarios que no tienen que ver con ellos. Para los sitios que tienen alto tráfico en los que una cerradura permanente no resulta funcional, es conveniente instalar cerraduras automáticas.

[3] Eugene Spafford

1.4.3.2 Control de Acceso

El control de acceso es uno de los caballos de batalla más importantes en la cadena de la seguridad. El control de acceso se puede realizar con sistemas que combinan hardware y software. Una opción utilizada habitualmente son sistemas (módem, software, etc.) que generan una llamada a un puesto o teléfono de control preprogramado, que devuelve al punto de acceso la identificación a comprobar. Estos dispositivos se suelen localizar en los centros de administración de red o en las computadoras centrales.

Se pueden emplear controles de auditoría, en los cuales se registre la actividad en general de los usuarios dentro de su computadora También es importante que los sistemas permitan desconectar a los usuarios por inactividad, con el fin de evitar que alguien se encuentre una computadora ya conectada a otra y con todos los derechos activados

Los sistemas más sofisticados incluyen lectores de tarjetas de crédito, tarjetas inteligentes, detectores de huella digital o simplemente generadores de clave que son únicas para cada sesión.

1.4.3.3 Uso de Contraseñas (Passwords)

Una vez protegidos los equipos físicamente, el acceso a los servidores y estaciones de trabajo normalmente se maneja con contraseñas. Aunque resulta común, que muchos de los usuarios y operadores utilizan las mismas contraseñas durante toda la vida en la empresa, y frecuentemente éstas son sencillas de adivinar con el empleo de programas capaces de encontrarlas. Las principales contraseñas utilizadas, que deben evitarse, son: placa del auto, apodo o nombre familiar, nombre de usuario (login), fecha de cumpleaños o del matrimonio, nombre del perro, o combinaciones de nombre y apellido como primera letra del nombre seguida del apellido.

Una estrategia es configurar los servidores de forma de que estas contraseñas tengan un tiempo determinado de validez y se renueven automáticamente. El problema de esta estrategia, es que los usuarios terminan olvidando sus contraseñas o las anotan en un hoja de papel, que en el mejor de los casos, estará colocado debajo de la computadora y, el operador de la red termina atendiendo periódicamente a los usuarios que han olvidado sus contraseñas; por lo que se recomienda entonces un esquema de autenticación centralizado para todos los servicios Existen sistemas de autenticación centrales como el User Manager for Domains de Windows NT, SecurID de Security Dinamics o el Trust Me de Racal Guardata, los cuales utilizan un esquema de Token (una tarjeta o Software) que tiene el usuario y que periódicamente cambia la contraseña

Las contraseñas (password) han de ser secretas para el resto de los usuarios, por lo que se requiere que la persona tome en cuenta

- No elegir palabras como su nombre, número identificación del Seguro Social, fecha de nacimiento, etc., pues aunque son fáciles de recordar, son también fáciles de indagar.
- Si se ha elegido uno difícil de recordar, no se debe escribir en sitios próximos a la computadora.
- No poner la clave en programas para acceso automático a la red.
- Cambiar frecuentemente la contraseña
- No elegir palabras comunes que puedan estar en los diccionarios.

En el año 1993 un 20 % de los accesos fraudulentos se debían al uso de diccionarios para buscar contraseñas Un 86% de códigos de acceso estaban dentro de uno de estos conjuntos, palabras en un diccionario, palabras de un diccionario pero al revés, nombres comunes, números de matrículas del coche y otros números como el de identificación del Seguro Social[4].

1.4.3.4 Encripción o Cifrado

Los sistemas de autenticación dicen que la persona que está utilizando los servicios si es quien dice ser, esto protege la red interna; pero para protegerla una vez que ésta deja el perímetro seguro (la puerta de una oficina) se recomienda utilizar esquemas de encripción Para las conexiones dedicadas se utilizan entonces encriptores de línea como los Datacryptor 64 de RACAL[5], los cuales alteran los datos de la red, de modo que no sea posible entenderlos a menos que se posea un encriptor igual, y lo que realmente importa más, una llave de encripción igual a la del equipo que originalmente se utilizó para alterar los datos (estas llaves de software deben de ser generadas, guardadas y distribuidas por una persona de confianza de la organización).

En la primera guerra mundial surgió la necesidad de proteger los mensajes que se enviaban entre teletipos. Gilvert S. Vernam[6] desarrolló en 1917 un sistema de cifrado adecuado utilizando una clave secreta que se combinaba con los caracteres del texto original, utilizando una función exclusiva para formar los caracteres cifrados que se transmitían En el receptor se recuperaba el texto original mediante un proceso análogo.

La encripción o cifrado es un proceso que transforma texto legible por cualquiera en una forma incomprensible conocida como texto cifrado, mediante el uso de algoritmos matemáticos Sólo los usuarios con una clave digital, un

[4] http://arrakis.dif.um.es/~rafa/8trab.htm
[5] http://arrakis.dif.um.es/~rafa/8trab.htm
[6] http://arrakis.dif.um.es/~rafa/8trab.htm

programa codificador y decodificador basado en el algoritmo correspondiente, pueden leer el mensaje.

Existen dos métodos básicos de cifrado:

- **Cifrado de datos por transposición**, que toma los caracteres del texto y los codifica para formar el texto cifrado. Sólo se cambia la posición de los caracteres en el mensaje, y no los caracteres en sí.
- **Cifrado de datos por sustitución**, que cambia cada carácter del texto por otro diferente de acuerdo con un algoritmo determinado

Actualmente hay varios sistemas de cifrado, que se indican a continuación

❑ Clave de encripción privada

Este procedimiento usa una clave única para encriptar y desencriptar los datos La clave debe ser poseída tanto por el emisor de los datos como por el receptor. Este sistema es válido para enviar información desde un punto a un conjunto, o para transferirla entre dos puntos, siempre que sea en poca cantidad.

Hay un estándar para este sistema, conocido como DES (Data Encryption Standard - Estándar de Cifrado de Datos) DES es un esquema adoptado y mantenido por el Instituto para las Ciencias de la Computación y Tecnologia, en el National Bureau of Standard (EE UU.). DES especifica un algoritmo para encriptar y desencriptar información digital, basado en una clave binaria. La clave consta de 64 bit, 56 se usan en la operación correspondiente y los 8 restantes se emplean para corrección de errores. La clave se genera de forma que los 56 bit son aleatorios. Al ser cada clave única, los resultados después de aplicar el algoritmo son únicos Con este sistema hay 72*1015 combinaciones posibles[7].

Este sistema es habitual en la comunidad financiera y en industrias que necesitan elevados niveles de seguridad.

❑ Clave de encripción pública

Este sistema usa pares de claves, una privada y otra pública. La privada se emplea a nivel personal y no se distribuye, mientras que la otra, se difunde al ser necesaria para decodificar los mensajes. Cada clave pública sólo decodifica los mensajes emitidos por el propietario de la clave correspondiente privada

[7] http://arcaque.dif.um.es/~rafa/Rtrab.htm

1.4.3.5 Firewall

Para el caso de conexiones a Internet se utilizan otros esquemas llamados Firewalls (paredes de fuego), estos son computadoras especializadas con dos tarjetas de red local y un software especial. Estas máquinas tienen esquemas programables que filtran y repelen los ataques que provengan de la Internet, impiden que se utilicen algunos servicios (a quien le está permitido hacer qué), direcciones electrónicas (a quien le está permitido ir a donde) y otras funciones de acuerdo a las políticas que se programen. Pueden además manejar algo que se conoce como túneles encriptados, estos son canales de comunicación IP (Internet Protocol – Protocolo de Internet) encriptados a través de la Internet, esto permite utilizar la Internet como backbone (columna vertebral) de comunicaciones y al mismo tiempo mantener privacidad Además, también existe un túnel cliente para usuario final, de esta forma alguien puede comunicarse haciendo una llamada en cualquier punto del mundo con cualquier proveedor de acceso a Internet, y sus datos viajarán encriptados por la Internet hasta llegar a la organización.

1.4.3.6 Crackers

En la actualidad las comunicaciones y la información, incluyendo voz, imágenes, textos y números, se crean, almacenan, transfieren y se accede a ellas mediante tecnología digital. Desafortunadamente, los "crackers" (actualmente se estima la existencia de 35000 en EE.UU, y se prevé que aumente esta cifra hasta los 56000 en el año 2000) suelen acceder a los recursos de las redes y obtener información confidencial[8]; lo cual ha llevado a que grandes empresas estén sufriendo pérdidas considerables como resultado del acceso a las redes por parte de personas no autorizadas.

No se debe confundir el término cracker con el de *hacker*, ya que este último es una persona que se deleita aprendiendo los detalles de la programación de sistemas y cómo extender sus capacidades (contrario de la mayoría de los usuarios que prefieren aprender solo lo necesariamente mínimo).[9] Los "crackers" pertenecen a organizaciones bien estructuradas; estas organizaciones intercambian información al menos mensualmente y celebran reuniones anualmente La misma tecnología que ha revolucionado muchas empresas, también ha revolucionado el crimen electrónico, usando puntos de entrada no autorizados a la red Internet, accediendo a comunicaciones a larga distancia.

La seguridad en redes de comunicaciones es una protección contra las pérdidas debidas al vandalismo y al robo, cuyo origen puede deberse a causas variadas, como por ejemplo revanchas, retos intelectuales, o planes preconcebidos

[8] http://arrakis.dif.um.es/~raf/8trab.htm

[9] The Hacker's Dictionary 1988

con alguna finalidad. Independientemente del motivo, siempre hay un daño a la víctima.

El robo incluye la copia de documentos confidenciales (tales como el estado financiero de una empresa), y el uso sin autorización de recursos como por ejemplo sistemas telefónicos o redes de datos El vandalismo comprende la destrucción o corrupción de archivos de datos, introducción de virus informáticos y reconfiguración de las redes para hacerlas inaccesibles a los usuarios autorizados

Usualmente las grandes empresas y organismos oficiales protegen los puntos de acceso a sus instalaciones; vigilantes de empresas de seguridad son habituales en las entradas donde normalmente cualquier persona que acceda, ha de estar completamente identificada, y en algunos casos, sólo puede desplazarse a algunas partes del edificio. De forma análoga, en las redes de comunicaciones hay sistemas de seguridad respecto a los accesos y diversas posibilidades para llegar hasta distintas informaciones en función del tipo de usuario que se sea

1.4.3.7 Medidas Antivirus

La instalación de un programa antivirus es la medida más empleada por las empresas para protegerse de la "plaga" de virus, consiguiendo estabilizar las pérdidas que estos infringían a las empresas Los antivirus pueden ser preventivos o detectores.

La mayor parte de los virus son una combinación de las siguientes formas de actuar:

- Añaden código al final de un programa ejecutable.
- Insertan código en el interior de un programa ejecutable
- Emplean técnicas de redirección
- Sobreescriben archivos.
- Bloquean las funciones de consulta de directorio, presentando en pantalla una información que no corresponde con los verdaderos tamaños y fechas del sistema, enmascarando la existencia del virus.

Se enlistan a continuación algunas medidas para protegerse de los virus

- Utilizar computadoras aisladas para probar el software que viene de fuera.
- Utilizar siempre disquetes protegidos contra escritura.
- Hacer backups (respaldo de información) de forma regular
- No cargar software de ocio en las computadoras de la empresa

La seguridad se ve comprometida frente a los ataques de los virus por estas actividades

- Compartir disquetes con programas entre usuarios.
- Utilizar programas precompilados.
- Dejar disquetes sin protección de escritura en las disqueteras.
- Usar software pirata o software que se obtiene directamente de las redes como Internet
- Permitir el acceso a las computadoras a personal no autorizado.

Es importante comprender que un virus se introduce en una red a través de cualquier puerto que permite leer programas o que permite leer archivos que luego se pueden renombrar como programas. El número de puertos que hay en las redes hacen que éstas sean especialmente vulnerables y además es imposible monitorear la actividad de todos y cada uno de los usuarios que acceden a éstas.

1.4.3.8 Copias de Seguridad

Las copias de seguridad se manejan y administran mucho mejor en un sistema centralizado, que si se deja esta responsabilidad a los diferentes departamentos.

Algunos aspectos importantes relativos a las copias de seguridad, son:

- Los sistemas de backup (respaldos de información) para las redes, cada vez incorporan más funciones (por ejemplo, software independiente del hardware sobre el que se hacen las copias).
- Es muy importante automatizar los procesos, evitando siempre que sea posible, la intervención manual.
- Los nuevos estándares permiten operar las funciones de archivo y backup sobre distintas redes y plataformas
- En general es más económico pensar en un sistema de backup centralizado que uno distribuido. Se están imponiendo las librerías o juke-boxes que suministran elevadas capacidades de almacenamiento (100 - 1000 Gigas).

1.5 SITUACION INICIAL DE SICORI

A lo largo de este capítulo se ha presentado un panorama general sobre redes de computadoras y su seguridad, lo cual nos introduce a la metodología utilizada para el desarrollo de está Tesis. A continuación se describen las características básicas del departamento de SICORI (Unidad Corporativa de Sistemas de Información Geográfica)

En SICORI se tiene una red LAN tipo Ethernet que utiliza topología Estrella. Los enlaces físicos entre nodos son a través de cable UTP, que van conectados a varios concentradores (se tienen 5 concentradores, con 12 entradas cada uno), suficientes para mantener en red las 40 estaciones de trabajo y 10 servidores existentes en el departamento (figura 1.1). Los equipos son de alto rendimiento (procesadores RISC, Intel y Pentium), con velocidad superior a 100 Mhz, capacidad en disco duro de 2 GB en adelante y con memoria RAM mayor a 32 MB También se cuenta con un router y un gateway para mantener comunicación con otras redes dentro de la empresa. El protocolo utilizado es TCP/IP, porque las necesidades del departamento así lo requieren.

SICORI cuenta con las siguientes áreas de trabajo: Jefatura, Administración de Recursos Tecnológicos, Calidad, Mercadotecnia, Soporte Técnico, Finanzas y Producción; las cuales requieren de integridad, seguridad e independencia de su propia información

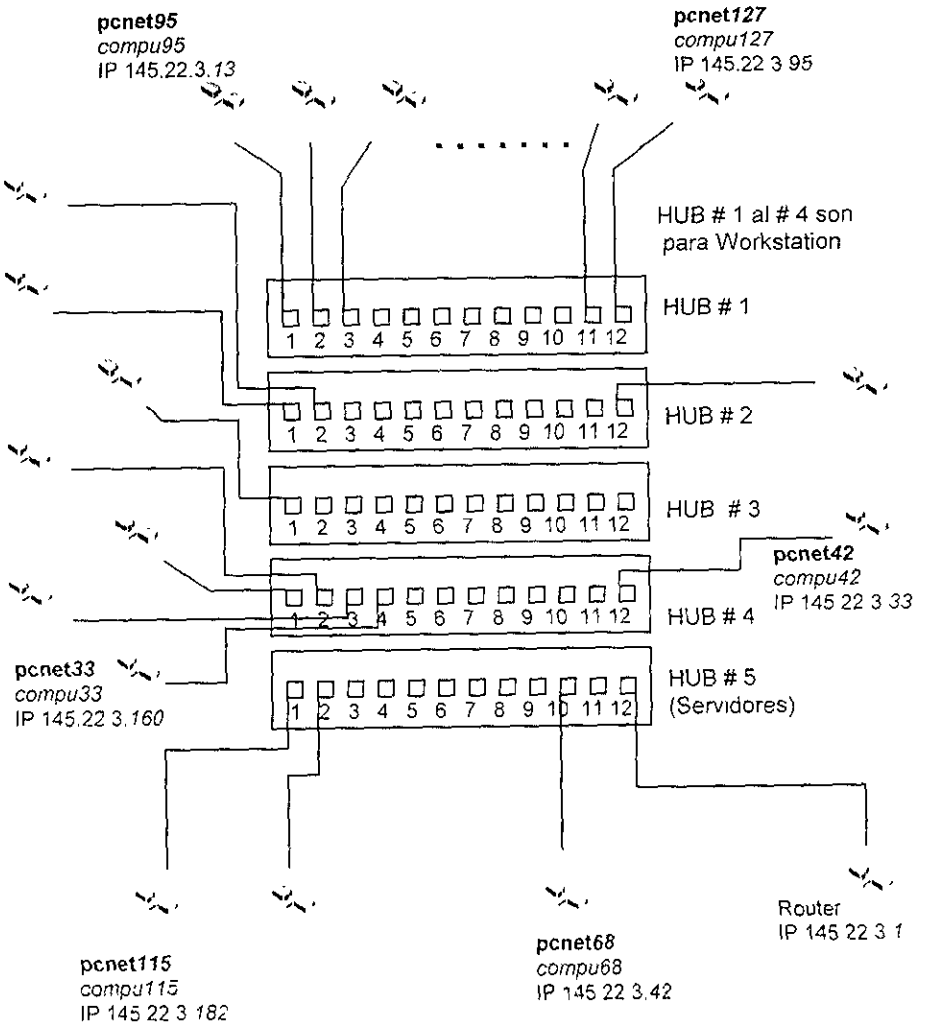
El área de Soporte Técnico es la encargada de implantar técnicas de seguridad en la red, equipos e información de los usuarios; es la que administra y soluciona los problemas involucrados con la computación (base de datos, impresión, soporte técnico a equipos, instalación de software, y otros). En esta área se encuentran los servidores, impresoras, plotters, consumibles (rollos y hojas de papel, tintas, cartuchos, acetatos, etc), cintas de respaldo de información, licencias de software, discos ópticos e información confidencial; por lo que el acceso está restringido mediante un sistema de alta seguridad (tarjetas sensoras de acceso, cámaras de video, vigilante) Como se puede apreciar, en SICORI existe bastante seguridad en los equipos, en cuanto acceso físico se refiere, pero, su seguridad en la red es muy pobre.

SICORI se dedica a la captura, digitalización, modificación, impresión y venta de planos, mapas e imágenes, que involucran a zonas petroleras principalmente; así como también sirve de apoyo a otras áreas y empresas que requieran de sus servicios (por ejemplo la Defensa Nacional Militar) Por lo que la información que se maneja es de estricto control confidencial, y el mal uso o pérdida de ésta provoca enormes problemas para la organización entera. Estos problemas se traducen en pérdida de dinero, prestigio, e incluso, seguridad nacional

En algunas ocaciones se ha llegado a detectar pérdida de información confidencial. Por ejemplo, hace algún tiempo se perdió toda la información contenida en una cinta de respaldo de la Defensa Nacional Militar. Afortunadamente, se pudó demostrar que la cinta había sido dañada físicamente, y que no había sido robada la información como se había pensado inicialmente. A partir de entoncés, se tiene más cuidado con la información que se maneja (se respalda en dos cintas la misma información, por ejemplo).

Como cada área requiere independencia de su información, y a la vez comunicación con otras áreas, resulta necesario el uso de un sistema operativo que brinde un ambiente amigable y de gran seguridad para los usuarios; como es Windows NT. En SICORI, se encuentra implantado este sistema operativo (Advanced Server y Workstation); pero desafortunadamente, los administradores de sistemas y los usuarios no tienen los conocimientos necesarios para la eficiente explotación de recursos con que éste cuenta. Esto implica una administración descentralizada de las cuentas y passwords de los usuarios, no se tienen adecuadas políticas de seguridad y se tiene un deficiente control de los recursos de la red y de la información. Todo esto se traduce a pérdida de tiempo, dinero y esfuerzo.

Aunque se tenga Windows NT, la administración de usuarios se realiza localmente Esto provoca gran carga de trabajo para los administradores de sistemas, ya que continuamente las cuentas requieren ser actualizadas (porque los usuarios olvidan su password, lo dan a conocer a otros usuarios, etc); por lo que se hace necesario ampliar los conocimientos sobre un uso adecuado de dicho sistema operativo (como se ve en el siguiente capítulo)



nombre	**pcnet x**
alias	*cumpu x*
dirección IP	IP x

Figura 1.1 Diagrama inicial de la red en SICORI.[10]

[10] Por razones de seguridad, los verdaderos nombres y direcciones de los equipos no se dan en esta Tesis.

SISTEMA OPERATIVO WINDOWS NT

En este capítulo se desarrollan las principales características y funciones del sistema operativo Windows NT. El estudio de su funcionamiento, arquitectura, y compatibilidad con otros sistemas operativos es fundamental, para explotar eficientemente todos los recursos que éste brinda a sus usuarios.

Se exponen de forma general los diferentes modelos de sistema operativos que existen.

2.1 SISTEMA OPERATIVO

Un Sistema Operativo es un grupo de programas que permite comunicación con una computadora para trabajar con ella, es decir, funciona como un traductor o puente entre el ser humano y la máquina. Es aquel que permite administrar todos los recursos de la máquina, tanto de software como de hardware

Existe gran variedad de Sistemas Operativos, que van de acuerdo a.

- Determinada familia de computadoras. Por ejemplo, las compatibles con IBM que pueden usar el MS-DOS, el DR-DOS, el OS/2, etc., o las compatibles con Macintosh que usan Mac OS, System 7, etc
- Determinado modelo dentro de una misma marca de computadoras. Por ejemplo el MPE para la HP-3000, el Level-6 de Honeywell.
- Aquellos que manejan ambiente multiusuario como el Unix (usado en la mayoría de los servidores de Internet), el Xenix, Windows NT, etc.

2.1.1 Modelos de Sistemas Operativos

❑ En Serie

Son aquellos que ejecutan un proceso a la vez También se les conoce como sistemas en línea (on-line)

❑ Por Lotes

- Permite poca interacción con el usuario.
- Tiene un potencial mayor de utilización de recursos.

- Son utilizados para procesos largos, donde se tenga muy poca interacción con el usuario.
- Los trabajos son procesados en el orden de admisión.

❑ Multiprocesamiento

Es el procesamiento simultáneo con dos o más procesadores en una computadora, o dos o más computadoras que están procesando juntas.

❑ Multiprogramación o Multitarea

Es la ejecución de dos o más programas en una computadora al mismo tiempo.

❑ Multiusuario o Multiacceso

Permite mantener a uno o más usuarios trabajando a la vez

❑ Tiempo Compartido

Permite atender alternadamente a varios procesos a la vez. Esto se hace mediante asignación de tiempos para el uso del procesador a cada uno de los procesos

❑ Tiempo Real

Es aquel que cuando cierto usuario solicita servicio, el sistema operativo lo atiende inmediatamente sin ninguna demora

2.1.2 Sistemas Operativos de Red

Un Sistema Operativo para Red de computadoras, es un programa que permite trabajar en un ambiente en el cual dos o más computadoras están comunicadas entre sí, de una forma "transparente" para los usuarios.

Existen varios tipos de Sistemas Operativos para Redes de computadoras, cada uno de ellos con sus correspondientes ventajas y desventajas. Entre estos están:

- Peer-to-Peer (Punto-a-Punto o Puerto-a-Puerto).
- Server-Client (Cliente – Servidor)

En el primer tipo, como su nombre indica, la comunicación se realiza de una computadora a otra, esto es, los recursos de cualquier computadora que se encuentre conectada a la red pueden ser compartidos por cualquier otra computadora que también se encuentre conectada a la red

En el segundo tipo, una computadora llamada *servidor* se encarga de suministrar programas y archivos a otra u otras computadoras conectadas a ella y que reciben el nombre de *clientes*. Dentro de este tipo, el de mayor preferencia en el ámbito mundial, es el desarrollado por Novell, llamado NetWare Operating System. También está Windows NT Advance Server (Servidor Avanzado) y Workstation (Estación de Trabajo), los cuales son de los más empleados por las ventajas de utilización, administración y seguridad que suministran

Hay una complejidad elevada en las tareas de control de las comunicaciones en una red. El programa que realiza esta tarea se denomina **Sistema Operativo de Red**, y ha de cumplir los siguientes requerimientos.

❑ Multitarea

Para atender las peticiones de muchos usuarios a la vez deben ser capaces de realizar varias tareas simultáneamente. De esta forma pueden realizar una lectura en disco al mismo tiempo que reciben otra petición a través de la red o imprimen un texto enviado por una estación de trabajo.

❑ Direccionamiento

Deben ser capaces de controlar grandes capacidades de disco, ya que éstos van a ser utilizados por más de un usuario. Para controlar gran capacidad de disco duro, necesitan gran cantidad de memoria que deben direccionar

❑ Control de acceso

Si se desea que los datos de todos los usuarios no sean dañados por error de alguno de ellos, el sistema operativo de red deberá incorporar un sistema que permita a los usuarios acceder sólo a los datos imprescindibles para su trabajo en la red

❑ Seguridad de datos

El disco duro de un servidor de archivos almacena muchos datos, más que el de una computadora personal aislada. Preservarlos justifica tener un sistema de seguridad que evite que un fallo de los componentes cause su pérdida. Por ello los sistemas operativos de red tienen sistema de tolerancia de fallos que funcionan de forma automática y transparente para los usuarios.

❑ Interfaz de usuario

Los usuarios deben seguir teniendo en su pantalla la misma apariencia que les ofrecía el entorno local El acceso a los periféricos de la red debe ser transparente y de la misma forma que si estuviera conectado en su estación. Sólo con ello se conseguirá facilidad de uso en la red

En el mercado existen varios sistemas operativos para red. Entre ellos destacan por su implantación.

- **DOS** Usan mucha memoria RAM y limita el tipo de aplicaciones a ejecutar en las terminales. A veces es insuficiente o difícil de manejar si se requieren varios servidores. En la realidad no se usa por que es prácticamente imposible que opere bien.

- **OS/2.** Se adapta un poco más que el anterior.

- **NETWARE** (de Novell). Dispone de diversas modalidades, basadas en DOS y dirigidas a entornos eminentemente locales.

- **VINES** (de Banyan). Se utiliza en los servidores del sistema operativo UNIX y de ahí le viene su compatibilidad casi total. Se puede considerar como el de mejores prestaciones, aunque está poco difundido.

- **Windows NT.** Los privilegios de agregar o eliminar aplicaciones e incluso de volver a formatear el disco duro, están reservados para los administradores de los sistemas

2.2 *SISTEMA OPERATIVO WINDOWS NT*

Windows NT desde su planteamiento inicial consideró su integración en ambiente de red de manera seria. NT tomó en cuenta aspectos tales como implementar nivel C2[1] de seguridad, crear los API's (Interfaz de Programa de Aplicación) necesarios para interactuar con programas desarrollados por terceros; e implementar una plataforma que permitiera un pronto acceso a proceso distribuido, etcétera.

Con MS-LAN Manager (LM) se agregan servicios de sistema operativo de red a OS/2, lo que se puede llegar a considerar como una capa de software adicional Con Windows NT el software de red no se agrega sino que forma parte integral del diseño, ofreciendo servicios tales como· cuentas para usuarios, seguridad para recursos, mecanismos de comunicación entre computadoras, servicios para compartir recursos, etcétera.

Los servicios de red incluidos con Windows NT ofrecen servicios punto a punto, tales como correo electrónico, copia de archivos y compartición de impresoras sin necesidad de instalar ningún software adicional.

Windows NT se tienen dos tipos de sistema operativo, Windows NT Workstation y Windows NT Advanced Server. NT Workstation contiene los servicios de red punto a punto y pretende ser el Windows NT para estación sencilla de trabajo, sin decir con esto monousuario Ya que, una sola estación de trabajo puede tener configuraciones para varios usuarios y cada uno utilizar diferentes recursos (paquetes, áreas de disco, etcétera), no al mismo tiempo en la misma máquina por supuesto.

Windows NT Advanced Server provee extensiones para entrar a un ambiente de redes controlado por dominios (redes grandes orientadas a manejar muchos servidores en un solo ambiente), la plataforma necesaria para interactuar con otros ambientes y mejorar la tolerancia a fallas

Windows NT es un sistema operativo completo que corre en toda una gama de computadoras de 32 bits, esto significa, que la transferencia de datos a los diversos sistemas de almacenaje, así como las instrucciones, se ejecutan más rápido La característica más importante de Windows NT es que cuenta con multitareas sustituibles. Por esto, el usuario puede correr varias aplicaciones al mismo tiempo Este proceso se lleva a cabo sin que haya interrupciones frecuentes ni pérdidas de información. Además, cuenta con procesamiento en recorridos múltiples, lo que ayuda a aumentar la respuesta de las aplicaciones que están

[1] Windows NT ha sido certificado como clase C2(requiere el ingreso del usuario individual con contraseña y un mecanismo de auditoria) del Libro Naranja (Trusted Computer Systems Evaluation Criteris, DOD Estandar 5200 28 – Criterios de evaluación de sistemas informáticos fiables), por el National Computer Security Center (NCSC – Centro Nacional de Seguridad para Computacion) de los Estados Unidos *(En el punto 2 2 3.6 se ve con más detalle)*

diseñadas para aprovechar el procesamiento múltiple NT es capaz de manejar hasta 4 gigabytes con seguridad integrada para proteger el sistema y, multiprocesamiento simétrico, características que sirven para aprovechar al máximo las computadoras con CPU múltiples

NT también estrena un nuevo sistema de archivos. NTFS (NT File System – Sistema de Archivos de NT), que reemplaza el sistema de FAT (File Allocation Table - Tabla de Asignación de Archivos) de DOS y provee algunos beneficios nuevos, tales como nombres largos de archivos (más de 8 caracteres).

NT es su propio sistema operativo para redes Funciona junto con varias de las redes para oficinas que hay en el mercado (como Novell NetWare), y presenta características como correo electrónico, planificador de grupos(controlador de dominio), etc.

2.2.1 Historia

Microsoft se introdujo por primera vez en el mundo de las redes, cuando DOS 3.1 agregó las extensiones al FAT necesarias para poder bloquear archivos, permitiendo de esta manera, que más de un usuario abriera el mismo archivo al mismo tiempo.

Conjuntamente a la liberación del DOS 3.1 se liberó un producto llamado Microsoft Networks, el cual informalmente se conoce como MS-NET. Producto que es la cuna de los actuales productos de red de Microsoft.

MS-NET implementaba llamadas a servicios remotos a través de lo que actualmente se conoce como redirector, este elemento detecta la llamada a la red (en vez de la llamada al sistema operativo local) y le pasa los componentes inherentes de MS-NET. El concepto de redirector continúa en Windows NT, evolucionado profundamente y de hecho soportando varios redirectores al mismo tiempo que permitan comunicarse a varios ambientes simultáneamente

Del MS-NET se toma el protocolo SMB (Server Message Block - Bloque de Mensajes de Servidor). SMB es una especificación para los niveles altos del modelo OSI (sesión, presentación y aplicación) permitiendo que las solicitudes a la red tengan un formato especial.

NetBIOS es otro elemento tradicional que se encuentra aún en Windows NT, pero como en versiones anteriores de LM utiliza la nueva implementación llamada NetBEUI. Está última implementación es una versión muy mejorada de NetBIOS

Después apareció "Windows for Workgroups" (Windows para Trabajo en Grupos) como solución para ambientes punto a punto Este producto con pretensiones de atacar un mercado hasta ahora ajeno a Microsoft, tiene características muy interesantes, que fueron tomadas en el nuevo Windows NT.

De estos productos, Windows NT toma lo mejor de cada uno y lo implementa en un mismo producto que a simple vista parece la integración de lo anterior en un solo paquete Windows NT Advanced Server es mucho más que la implementación de servicios conocidos en un ambiente familiar, es la maduración de conceptos tradicionales y la integración de algunos conceptos innovadores.

2.2.2 Arquitectura

Windows NT es un sistema operativo de Arquitectura abierta. Soporta el acceso a distintos sistemas de archivos a través de una librería llamada WNet API. Permite que diferentes protocolos de transporte sean cargados al mismo tiempo (por ejemplo, TCP/IP, NetBEUI, etcétera) y que estos llamen a la misma tarjeta de red.

El hecho de que el acceso a las tarjetas de red sea a través de driver NDIS (Network Driver Interface Speficication – Especificación de Interfaces para Controladores de Red) garantiza que las tarjetas podrán ser accesadas por varios protocolos (mencionados en el párrafo anterior), permitiendo a los fabricantes tener un estándar de referencia para crear sus drivers

Windows NT presenta una arquitectura del tipo cliente-servidor. Los programas de aplicación son contemplados por el sistema operativo como si fueran clientes a los que hay que servir, y para lo cual viene equipado con distintas entidades servidoras.

Uno de los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro-kernel.

Dentro de la arquitectura de NT se distingue un núcleo que se ejecuta en modo privilegiado, y se denomina **executive**; y unos módulos que se ejecutan en modo no privilegiado, llamados subsistemas protegidos

Los componentes que proporcionan la seguridad en Windows NT configuran el subsistema de seguridad. La figura 2.1 muestra cómo este sistema entra dentro de la arquitectura de Windows NT. Como la mayoría de otros modelos, encaja con la parte hardware en la base y con las aplicaciones de alto nivel en la cima. Todas las capas intermedias proporcionan servicios a las capas superiores e interactúan con las inferiores.

❑ Modo Núcleo

Se sabe que hay muchos tipos de procesadores distintos en el mercado, de modo que en vez de elegir una plataforma, se crea un módulo software pequeño (llamado núcleo) que se ejecuta para cada uno de estos procesadores. Para hacerlo más sencillo para los diseñadores, se crea una capa de abstracción de hardware (HAL), que oculta (abstrae) las diferencias del hardware a las capas superiores. Con esta aproximación, los diseñadores ven diferentes tipos de hardware del mismo modo, haciendo más fácil escribir programas

Ahora el sistema operativo va a ser utilizado en una gran variedad de entornos y no todo el mundo va a necesitar todos los servicios que un sistema operativo puede suministrar, entonces se crea un sistema modular en el que los componentes puedan ser añadidos y quitados. Estos módulos se unen al núcleo.

El núcleo planifica las actividades que debe ejecutar el procesador. Estos procesos se denominan hilos (threads) y el núcleo está encargado de que el procesador esté siempre ocupado ejecutándolas. Se asegura que las que tengan mayor prioridad se ejecuten antes de las que poseen prioridades menores.

El núcleo también sincroniza las actividades de los componentes unidos a él, como son.

◗ **Administrador de objetos.** Los archivos, puertos, carpetas, procesos e hilos se denominan usualmente objetos. El administrador de objetos está encargado de nombrar, proteger, situar y disponer de los objetos.

◗ **Administrador de procesos.** Un componente que crea y borra procesos.

◗ **Administrador de memoria virtual.** El componente que crea memoria simulada del espacio de disco.

◗ **Facilidad de llamada a procedimiento local.** Una facilidad que utilizan las aplicaciones para comunicarse con los niveles más bajos del sistema operativo gracias a la facilidad de paso de mensajes.

◗ **Administrador de E/S.** Un componente que administra la comunicación entre el sistema operativo y el mundo exterior Administra los dispositivos de las unidades, que son módulos software que ayudan al sistema operativo a acceder a dispositivos físicos como tarjetas de interfaz de red, unidades de disco y memoria cache.

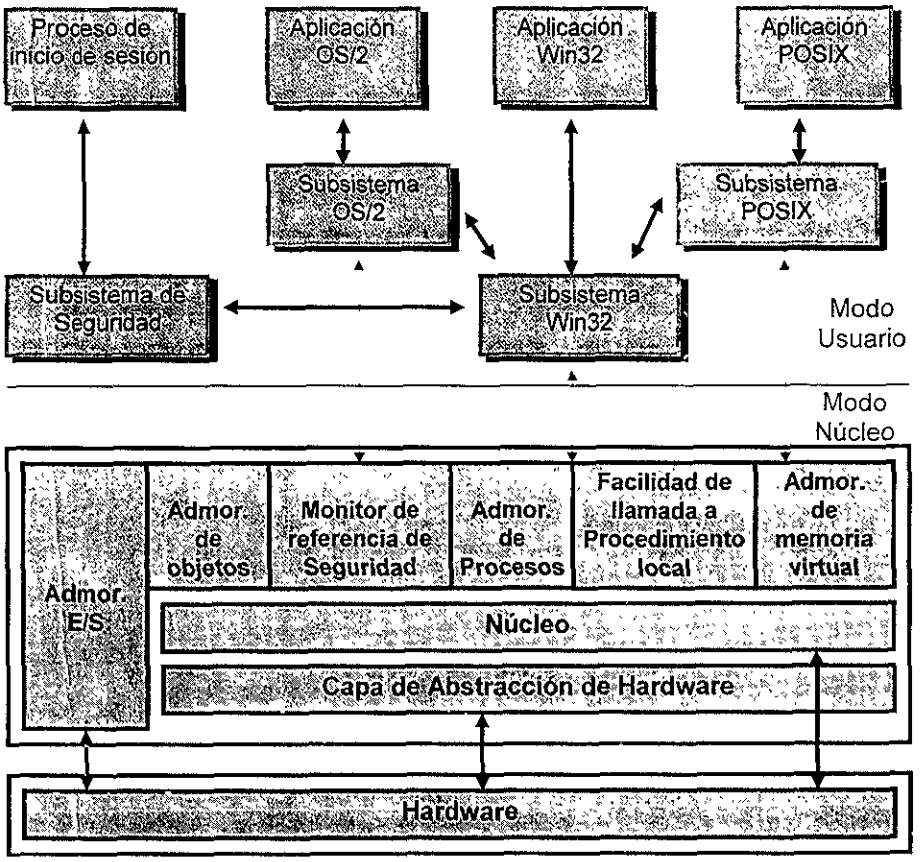


Figura 2.1 La arquitectura de Windows NT

❑ Modo Usuario

◗ **El subsistema Win32.** Es el principal, ya que proporciona la interfaz para aplicaciones específicamente construidas para Windows NT.

◗ **El subsistema POSIX.** La norma POSIX (Portable Operating System Interface for UNIX – Interfaz Portátil de Sistema Operativo para UNIX) fue elaborada por IEEE para conseguir la portabilidad de las aplicaciones entre distintos entornos UNIX

◗ **El subsistema OS/2.** Este subsistema da soporte a las aplicaciones del sistema operativo OS/2 Proporciona la interfaz gráfica y las llamadas al sistema.

◗ **El subsistema proceso de inicio.** El proceso de inicio (Logon Process) recibe las peticiones de conexión por parte de los usuarios. En realidad son dos procesos, cada uno encargándose de un tipo distinto de conexión. el proceso de inicio local, que administra la conexión de usuarios locales directamente a una máquina Windows NT; y el proceso de inicio remoto, el cual controla la conexión de usuarios remotos a servidores de NT.

◗ **El subsistema de seguridad.** Este subsistema interacciona con el proceso de inicio y el llamado monitor de referencias de seguridad, de esta forma se construye el modelo de seguridad en Windows NT. El subsistema de seguridad interactúa con el proceso de inicio, atendiendo las peticiones de acceso al sistema. Consta de dos subcomponentes: la autoridad de seguridad local y el administrador de cuentas. El primero es el corazón del subsistema de seguridad, en general administra la política de seguridad local, así, se encarga de generar los permisos de acceso, de comprobar que el usuario que solicita conexión, tiene acceso al sistema, de verificar todos los accesos sobre los objetos (para lo cual se ayuda del monitor de referencias a seguridad) y de controlar la política de auditorías, llevando la cuenta de los mensajes de auditoria generados por el monitor de referencias

El administrador de cuentas mantiene una base de datos con las cuentas de todos los usuarios (login, claves, identificaciones, etc.). Proporciona los servicios de validación de usuarios requeridos por el subcomponente anterior

Windows NT es un sistema operativo diseñado para ser exportable entre distintos procesadores, escalable a sistemas multiprocesadores, seguro según los estándares del gobierno de los EUA, y extensible permitiendo que se puedan añadir nuevos módulos.[2]

2.2.3 Características de Windows NT

El rango de opciones de Windows NT es abrumador, extendiéndose desde la simple compartición de recursos hasta las complejas caracteríticas que permiten crear un completo muro de fuego para la red. A continuación se presentan las caracteríticas esenciales de este sistema operativo.

2.2.3.1 Funcionamiento

Para poder entender la manera en que Windows NT implementa sus servicios de red, se analiza a continuación sus componentes y su ubicación dentro del modelo OSI (figura 2.2).

---

[2] SHELDON Tom *Manual de Seguridad de Windows NT*. McGRAW-HILL 1997 Pág 78

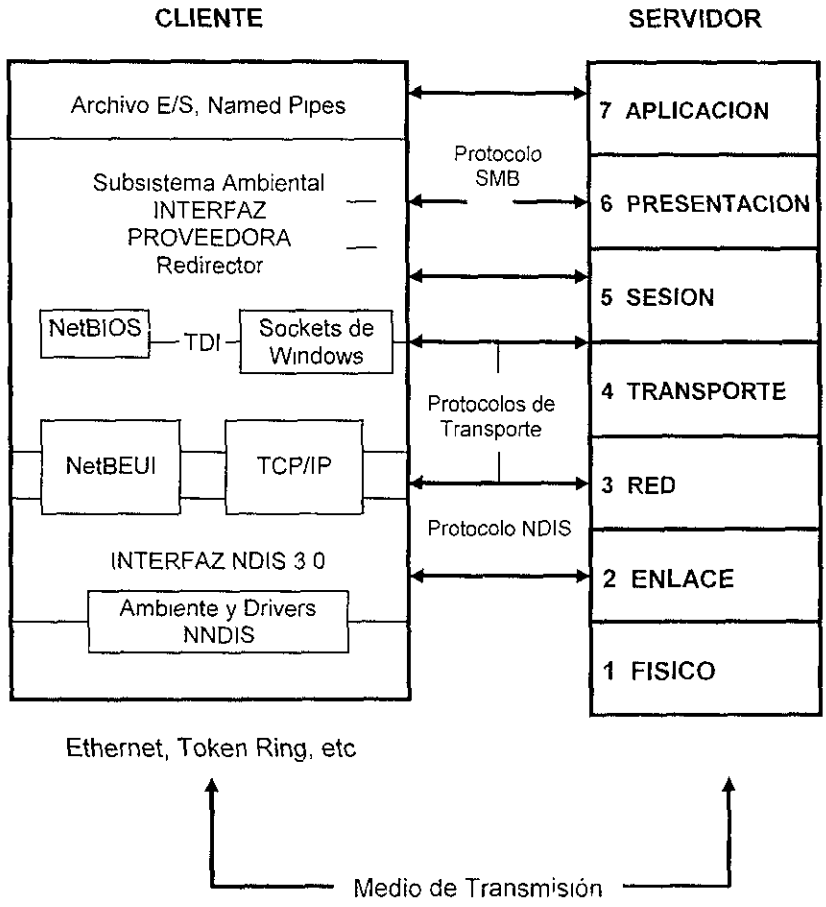


Figura 2.2 Componentes de Red de Windows NT y el Modelo OSI

Un software que se encuentra corriendo en modo usuario (user mode) hace una llamada de E/S remota a través de una llamada a los servicios de E/S nativos de Windows NT, el administrador de E/S de Windows NT crea un paquete de solicitud o IRP (I/O Request Packet) pasando la llamada a un driver de sistema de archivos registrado, que en el caso de Windows NT recibe el nombre de redirector. El redirector pasa el IRP a los drivers inferiores (de la capa de transporte) los cuales pondrán el paquete en la red finalmente. Cuando el paquete llega a otra máquina con Windows NT es recibido por los drivers de red localizados en el modo núcleo (kernel mode), de ahí ascenderán al sistema de archivos del servidor Este sistema de archivos servidor o simplemente el Server pasará el paquete al sistema de archivos local y finalmente al dispositivo físico, tal como se ve en la figura 2 3.

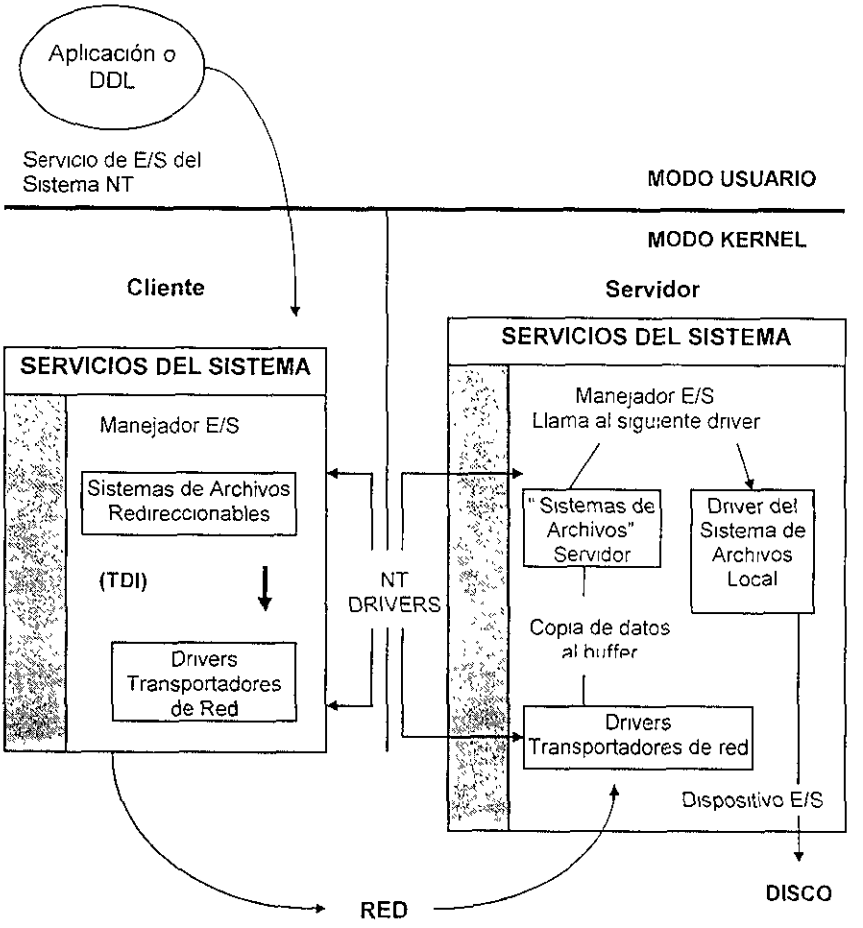


Figura 2.3 Sistema de Archivos Servidor.

Dentro del proceso anterior identificamos dos elementos importantes, el redirector y el *server*, mismos que dominan la actividad de la red. Estos elementos primarios del esquema de red de Windows NT, existen desde el antiguo MS-NET. Pero ahora, por supuesto, han sido mejorados y escritos en lenguaje C (y no en lenguaje máquina como se hacía antes) lo que permite que sean portables.

Estos elementos tienen ahora un esquema de drivers, lo que hace posible que sean cargados y descargados según se requiera.

La principal ventaja del Driver Server de Windows NT es que está dentro del Ejecutive de Windows NT[3] y que puede hacer llamadas al administrador de caché directamente, optimizando las transferencias de datos, lo que repercute en un mejor tiempo de acceso.

Tanto el redirector como el server utilizan una interfaz llamada TDI (Transport Driver Interface - Interfaz de Manejador de Transparte) para enviar y recibir los SMB ' s involucrados en una transacción. El TDI es un conjunto de rutinas colocadas como otro driver en el sistema, que a su vez puede *platicar* con los drivers de transporte cargados dentro de la máquina con Windows NT

2.2.3.2 Diseño Orientado a Objetos

Casi todo en el sistema operativo de Windows NT está representado como un objeto: archivos, memoria, dispositivos, procesos, hilos, e incluso las ventanas que aparecen en el escritorio. Los objetos son la clave para proporcionar un alto nivel de seguridad en Windows NT

Todos los objetos en Windows NT pueden ser accedidos sólo por el propio sistema operativo a través de estrictos controles El sistema de seguridad comprueba todos los accesos a los objetos, y el sistema de auditoría puede registrar estos sucesos.

Los objetos ocultan los datos al exterior y sólo suministran información de determinadas maneras, del modo que lo definen las funciones del objeto. Esto prohibe que los procesos externos puedan acceder a datos internos directamente. Esto tiene sentido cuando sé considera a un archivo de datos como un objeto al que se restringe el acceso, controlando quién puede leerlo. Es importante tener presente que todo en el sistema operativo Windows NT es un objeto.

Windows NT tiene altos niveles de seguridad no dejando nunca que los programas accedan directamente a los objetos. Cualquier acción sobre un objeto está autorizada y la realiza el sistema operativo Es relativamente fácil para Windows NT realizar estos chequeos sobre objetos ya que los objetos individuales poseen mucha de la información que se necesita para hacer una comprobación de seguridad.

[3] Ver glosario

2.2.3.3 Ambiente Distribuido

El proceso distribuido se lleva acabo cuando una serie de tareas son realizadas por varias computadoras comunicadas entre sí, de tal manera que juntas realizan un proceso determinado de forma transparente para el usuario. Windows NT provee la plataforma necesaria para crear y correr aplicaciones distribuidas.

Para la implementación de estas tecnologías, Windows NT incluye un servicio llamado RPC (Remote Procedure Call – Llamada a Procesos Remotos). Este servicio permite a los programadores desarrollar aplicaciones que tengan llamadas a procesos locales y a procesos remotos (localizados en otra computadora de la red). Un ejemplo de aplicación es, que se tuviera una workstation y una supercomputadora en la red, de tal manera que la workstation pudiera solicitar que la resolución de cálculos vectoriales o grandes matrices fueran resueltos en la supercomputadora y ella presentar los resultados en una gráfica tridimensional. De tal forma que la aplicación se vuelve mucho más rápida y el usuario ve resultados con mejor presentación y en menor tiempo

2.2.3.4 Comunicaciones Remotas

Para cuando se tiene la necesidad de comunicar una PC remota a la red, Windows NT Advanced Server provee un servicio incluido llamado RAS (Remote Access Server – Servidor de Acceso Remoto), por medio del cual se pueden utilizar enlaces X.25, líneas telefónicas conmutadas o privadas para comunicarse a red. La forma en la que este producto trabaja es la siguiente: se tiene un software para el cliente (DOS y Windows), el producto requiere preferentemente de un módem de 9600 bps (como mínimo) y en la parte de Windows NT Advanced Server se tiene que especificar (cuando se está instalando), que se desea instalar esta opción

Desde un programa de administración gráfico se configuran usuarios y conexiones de manera amigable Algo que es digno de mencionar es que el RAS puede controlar varios puertos a la vez. Windows NT Advanced Server permite hasta 64 usuarios conectados simultáneamente.

Una vez que se ha instalado el RAS, el usuario marca el número telefónico al cual se conectó el servidor, después de un pequeño proceso de verificación de claves de acceso el usuario remoto puede hacer uso de todos los recursos a los cuales se le haya dado acceso. Estos servicios incluyen impresoras, discos, acceso a bases de datos, etcétera

2.2.3.5 Tolerancia a Fallas

Windows NT soporta varios sistemas de archivos, entre estos están. el FAT (File Allocation Table) característico de DOS, el HPFS (High-Performance File System) característico de OS/2 1.3 y el nuevo llamado NTFS (NT File System). Entre las cualidades del nuevo NTFS, destaca la completa interoperabilidad con los anteriores, rápida recuperación de errores después de que el sistema ha fallado, capaz de controlar hasta 17 billones de gigabytes, cuando se graba un dato al disco se revisa que sea lo mismo que se tiene en memoria, en caso de no corresponder, se declara dañado el sector y se busca otro, a esto se le conoce como *Hot Fix.*

Como es común pensar, la tolerancia a fallas empieza en los discos duros, y Windows NT Advanced Server además de las características ya mencionadas del NTFS, agrega el llamado: Disk Mirroring (RAID 1)[4] permitiendo tener dos discos en *espejo.* Si un sector falla en el disco primario Windows NT Advanced Server marca el sector como dañado y lo toma del segundo disco, disminuyendo las probabilidades de error dramáticamente.

Otra característica nueva en Windows NT Advanced Server se llama *striping with parity* (datos e información con paridad, o RAID 5) Este proceso es aplicable a los casos donde se tienen de 3 a 32 discos, permite que los datos se graben en todo el arreglo de discos con paridad. En caso de que alguno de los discos falle, éste se puede retirar y el sistema continuará funcionando, ya que el resto de los discos contienen suficiente información para continuar la operación mientras el disco duro dañado se arregla.

Otro de los aspectos de tolerancia a fallas es el control de Windows NT sobre los UPS (Uninterruptible Power Supply - Fuente de Alimentación Ininterrumpible), esto es que Windows NT a través del puerto serial, puede conocer el estado del UPS y en caso de fallas en el suministro eléctrico, toma las medidas necesarias para mantener al máximo la integridad del sistema.

2.2.3.6 Seguridad

El modelo de seguridad de Windows NT ha sido diseñado para cumplir criterios de seguridad tanto nacionales como internacionales. En EUA es el criterio C2, como se define para el Departamento de Defensa de EUA en el documento llamado *Trusted Computer System Evaluation Criterio* (DOD 5200.28-STD, Diciembre de 1985). Este documento se conoce como el *libro naranja* El nivel C2

[4] RAID (Discos de Bajo Costo en Arreglo Redundante) Agrupamiento de discos en la que los datos se copian en muchas unidades Proporciona un caudal mas rapido, tolerancia de fallos (espejos) y corrección de errores (consultar Glosario)

es uno de los siete niveles de seguridad para sistemas de computadora del DOD Los siguientes son algunos de los requisitos importantes en C2.[5]

- Cada usuario debe ser identificado y autentificado usando un nombre de usuario y contraseña único, y todas las actividades de los usuarios deben ser trazadas usando esta identificación.
- Los recursos deben tener propietarios que puedan controlar el acceso a esos recursos
- Los objetos deben ser protegidos para que otros procesos no los puedan usar aleatoriamente. Esta protección se aplica a localizaciones de memoria, archivos y otros objetos.
- Todos los sucesos relacionados con la seguridad deben ser auditados, y los datos de la auditoría deben estar restringidos a los usuarios autorizados
- El sistema debe protegerse de interferencias y falsificaciones externas, tales como modificaciones del sistema operativo o de los sistemas de archivos almacenados en disco.

La implemetación de C2 de Windows NT Server está basada en software por completo, y por tanto no necesita componentes adicionales de hardware. Otros sistemas operativos necesitan dichos componentes para interceptar y encaminar todas las peticiones de seguridad de archivos y servidores Windows NT Server y Windows NT Workstation han sido diseñados para cumplir C2 desde el principio. Algunas de las propiedades de Windows NT Server son tan seguras (identificación y autenticación, y la habilidad de separar al usuario de sus funciones) que cumplen especificaciones de alto nivel tipo B2[6].

Propiedades adicionales de seguridad de Windows NT Server son:

- Los administradores controlan los derechos de acceso a los recursos, incluyendo archivos, carpetas, servidores, impresoras y aplicaciones.
- Administración de cuentas de usuario y bloqueo de cuentas.
- Propiedad de los recursos por parte de los usuarios y habilidad de definir el acceso a esos recursos.
- Expiración de contraseñas, reglas de complejidad de las contraseñas, y la encripción de contraseñas a nivel sistema para prevenir que los usuarios no autorizados descubran contraseñas mediante escuchas en las conexiones.

La seguridad en Windows NT puede ser bastante compleja, pero, a pesar de su aparente complejidad, realiza básicamente dos cosas muy simples:

---

[5] SHELDON, Tom *Manual de Seguridad de Windows NT*. McGRAW-HILL 1997 Pág 544

[6] B2 Garantiza una vía entre el usuario y el sistema de seguridad Provee la seguridad de que el sistema puede ser verificado y las franquicias no pueden ser degradadas

- Restringir el acceso a los objetos, tales como recursos del sistema, archivos y dispositivos.
- Proporcionar los servicios de auditoría que generen entradas en un registro para operar sobre un objeto.

El resto de la seguridad en Windows NT, se construye en estos conceptos. La idea es verificar que los usuarios son aquellos que dicen ser durante un inicio de sesión, y posteriormente autorizarles a acceder a los recursos. Esto necesita una cuenta de usuario qué defina qué usuarios están y qué pueden hacer en el sistema.

El inicio de sesión es una de las consideraciones de seguridad más importantes de cualquier sistema operativo La obtención de contraseñas de cuentas válidas es el mayor de los objetivos de los piratas informáticos. La protección de esas contraseñas es lo que mejor hace Windows NT

Windows NT es un sistema operativo orientado a objetos, y su seguridad se construye desde el nivel más bajo de la estructura de objetos. Esto hace que Windows NT sea mucho más fácil de proteger que otros sistemas operativos.

2.2.3.7 La Integración de las Aplicaciones

La ejecución de una aplicación individual de Windows no es tan útil como ejecutar múltiples aplicaciones. Con Windows NT se pueden operar múltiples aplicaciones simultáneamente (mediante su característica de multitareas), y hacer que cada aplicación utilice múltiples vías de ejecución en el procesador. Esto elimina el temido símbolo de reloj de arena cuando realiza tareas como una recalculación o una impresión. En cambio, se recobra el control de su aplicación casi inmediatamente.

2.2.3.8 Perfiles de Usuario

NT soporta *Perfiles de Usuario*, permitiendo a los usuarios seleccionar las configuraciones que desean para su computadora (escritorio, protector de pantalla, barra de acceso directo a MS-Office, etc.). Las variables de perfil podrían incluir resolución de vídeo, tarjetas para red y servicios para el cliente.

2.2.3.9 Inconvenientes

Se puede instalar Windows 95 y Windows NT 4.0 (ediciones para estación de trabajo o servidor) en la misma computadora y elegir cualquiera de los dos sistemas operativos al momento de iniciar, pero esto ocasionará algunas restricciones muy severas. Si se utiliza el sistema de archivos NTFS en el lado de NT, no se podrán visualizar los archivos cuando se inicie con Windows 95. De la misma forma, si se utiliza la compresión DriveSpace o el nuevo software de

partición de discos FAT32 en Windows 95, ese volumen no será visible cuando se utilice Windows NT.

Las aplicaciones de DOS y Windows 95 podrán ejecutarse en NT, aunque se notará una disminución en su rendimiento. Para que NT tenga éxito en plataformas que no se basen en procesadores de Intel, será necesario dar incentivos en cuanto a precio y rendimiento

2.2.3.10 Características Técnicas[7]

Desarrollado sobre el rendimiento superior y arquitectura de Windows NT 3 51, la versión de NT 4 0, mejora la facilidad de uso, instalación y administración, integrando la interfaz de usuario de Windows 95. Los administradores ahora pueden tener la misma interfaz de usuario en todas sus plataformas Windows de 32 bits, resultando esto en menores requerimientos de capacitación y facilidad de migración de usuarios dentro de la familia Windows de sistemas operativos.

Windows NT 4.0 integra todas las características de escalabilidad, portabilidad y seguridad, sin sacrificar la velocidad o el tiempo de respuesta. Las mejoras en velocidad y rendimiento en compartición de impresoras y archivos, procesamientos de aplicaciones, Internet y acceso remoto, lo hacen la plataforma más poderosa y completa que existe. En la Tabla 2 1 se muestran las características técnicas de Windows NT

TABLA 2.1 Características Técnicas de Windows NT

Interfaz Windows 95	La interfaz Windows 95 está integrada con Windows NT Server 4.0, haciendo al servidor más fácil de usar y consistente con las otras plataformas de Windows 32-bits.
Asistentes para Administración	Los Asistentes para Administración agrupan las herramientas más comunes de administración del servidor en un sólo lugar y lo guían por los pasos necesarios para realizar cada tarea.
Administrador de Tareas	Proporciona información detallada sobre cada aplicación y proceso corriendo en el sistema. También muestra gráficamente el estado del servidor en uso de recursos

[7] Microsoft Windows NT Server versión 4 0 (Folleto de información pag 4)

Monitor de Red	Examina el tráfico de red que entra y sale del servidor, hasta nivel paquete, y captura esa información para análisis posterior
Microsoft Internet Information Server (IIS) Versión 2.0	IIS está integrado con Windows NT Server 4.0 y ofrece. El más rápido servidor Web sobre Windows NT Server, hasta 40% más rápido que IIS 1.0 Servidor World Wide Web Servidor Gopher Servidor FTP Administrador de Servicios Internet Conector Internet para Bases de Datos
Microsoft Internet Explorer 2.0	Integra los estándares HTML existentes con mejoras como vídeo en línea, gráficas de fondo, soporte a Secure Sockets Layer (SSL) y soporte a compras a través de Internet
Microsoft FrontPage 1.1	Permite tanto a no-programadores y desarrolladores experimentados crear y administrar sitios Web de calidad profesional.
Microsoft Index Server	Ayuda a los usuarios a encontrar información en servidores distribuidos en su Intranet corporativa.
Distributed Component Object Model (DCOM)	Permite a las aplicaciones compartir componentes a través de redes incluyendo la Internet.
Servicio de Acceso Remoto Multilink Channel Aggregation	Permite a los clientes que accesan remotamente Windows NT Server 4.0 combinar todas las líneas disponibles para incrementar el ancho de banda.
Point-to-Point Tunneling Protocol (PPTP)	PPTP permiten a los usuarios extender la seguridad de las redes privadas a través de la Internet.
Multi-Protocol Router (MPR)	Elimina la necesidad de utilizar ruteadores dedicados en redes pequeñas y medianas utilizando Windows NT Server 4 0 como una solución de bajo costo para ruteo entre redes Proporciona ruteo de IPX/SPX, TCP/IP, y AppleTalk.
Telephony Application Programming Interface (TAPI) y Unimodem	Proporciona las tecnología requeridas por las aplicaciones de fax, el subsistema de mensajería de Windows (Cliente Microsoft Exchange), MSN™, El servicio de información en línea del Microsoft Network y el Microsoft Internet Explorer

Integración del Servidor Domain Name System (DNS) con el Windows Internet Name Service (WINS)	Permite el acceso a recursos en la red o sobre Internet utilizando nombres DNS. Las características DNS incluyen: Una utilería gráfica de administración. Inter-operabilidad con el protocolo de notificación
Escalabilidad	Soporta hasta 5,000 clientes de bases de datos concurrentes y bases de datos de 100 GB o más. Soporta más de 2,000 aplicaciones.
"Boot" remoto de Windows 95	Permite iniciar remotamente sistemas basados en Windows 95 desde el servidor de la red
Configuración de Políticas para Estaciones de Trabajo	Controla configuraciones y ambientes en las estaciones de trabajo, proporcionando un ambiente común en la organización
Cryptography APIs	Permite a los desarrolladores crear soluciones de encripción propias.

2.2.4 Requerimientos

Windows NT 4.0 ha sido creado como sistema operativo para computadoras de gran rendimiento, su facilidad de uso, flexibilidad, y servicios avanzados de Internet/Intranet y comunicaciones, satisfacen hasta las necesidades más avanzadas de cómputo. Por ello, las exigencias de NT respecto a la computadora en la que se instala son claramente más altas que en el caso de otros sistemas operativos.

2.2.4.1 Hardware[6]

En este apartado se describen las configuraciones mínimas para utilizar adecuadamente NT, cuáles son razonables y cuáles son las más convenientes para un óptimo desempeño En la siguiente tabla se muestran estas configuraciones

[6] B. Kretschmer C. Schneider *Todo sobre Winsows NT 4.0* Editorial Marcombo Barcelona 1996

TABLA 2.2 Requerimientos de Hardware para Windows NT

	Windows NT Workstation	Windows NT Server (equipamiento mínimo)	Windows NT Server (equipamiento razonable)
Procesador	- Intel 486 DX mejor: - Pentium 90 - Aplha - MIPS - Power PC	Pentium 90	Pentium PRO o Dual Pentium
Memoria RAM	A partir de 12 MB (Intel), o 16 MB (RISC)	A partir de 12 MB (Intel) o 16 MB (RISC)	64 MB o más
Disco Duro	A partir de 117 MB (Intel), o 124 MB (RISC)	A pertir de 148 MB (Intel) o 158 MB (RISC)	Dos discos duros reflejados de 4 GB
Controladora	E-IDE o SCSI	E-IDE o SCSI	SCSI
Tarjeta gráfica	Tarjeta VGA Accelerator con un mínimo de 2 MB de memoria.	Tarjeta S-VGA; o algo mejor	Tarjeta S-VGA; o algo mejor
Unidad de CD	ATAPI; mejor: SCSI	ATAPI; mejor: SCSI	ATAPI; mejor: SCSI

Windows NT Server 4.0 soporta hasta cuatro microprocesadoresa la vez[9].

2.2.4.2 Software

Otro de los atractivos de Windows NT son las aplicaciones de software Se pueden ejecutar las aplicaciones de 16 y 32 bits; sin embargo, la capacidad de recorrido múltiple por la cual las aplicaciones realizan distintas tareas simultáneamente, sólo se podrá aprovechar en aplicaciones de 32 bits que estén escritas para NT Además, las aplicaciones de 16 bits se ejecutan con mayor lentitud en NT que en DOS o Windows. Esto significa que el software tiene sus limitaciones

[9] Microsoft Windows NT Server 4 0 (Folleto de información pág .5)

Entre los primeros programas que se cambiaron a NT se encuentra los de CAD (Diseño Asistido por Computadora) y ello se debe a que en esta área hay aplicaciones de alto nivel en que se requiere de mucha memoria y hardware Puesto que NT es una arquitectura de 32 bits y cuenta con una memoria amplia, programas como AutoCAD podrán almacenar dibujos más grandes que con DOS o Windows. Además, los usuarios de AutoCAD podrán desarrollar, diversas aplicaciones al mismo tiempo La productividad aumentará considerablemente, puesto que una computadora trazará un dibujo y trabajará en otro simultáneamente

Otro punto que debe resaltarse respecto al software para NT, es que aparece con mucha mayor lentitud que el software para las plataformas tradicionales Esto se debe en parte a que Microsoft afirma que las aplicaciones requieren únicamente de un compilador simple y son totalmente transferibles. Los fabricantes necesitan tiempo para probar la recompilación en busca de fallas y esto exige un compromiso serio para cambiar a NT. Ellos, al igual que las compañías que elaboran periféricos, prefieren esperar para ver cómo evoluciona el mercado.

2.3 *WINDOWS NT WORKSTATION*

Una workstation (estación de trabajo) es una micro o minicomputadora para un único usuario, de alto rendimiento, que ha sido especializada para gráficos, diseño asistido por computadora, ingeniería asistida por computadora o aplicaciones científicas.

Windows NT Workstation es un sistema operativo de red, pero puede funcionar como un sistema operativo de escritorio. Puede formar parte de un ambiente de red workgroup (trabajo en grupo), o de un ambiente de dominios de Windows NT Server. La siguiente tabla lista las características de Windows NT Workstation.

Tabla 2.3 Características y beneficios de Windows NT Workstation.[10]

CARACTERISTICA	BENEFICIO
Función de Escritorio	Soporta múltiples procesadores para una verdadera ejecución multitarea.
Perfiles de Hardware	Crea y mantiene una lista de configuraciones de hardware para mantener las necesidades especificas de la computadora.
Microsoft Internet Explorer	Proporciona navegación más simple y rápida
Mensajería de Windows	Recibe y guarda correos electrónicos, incluyendo archivos y objetos creados en otras aplicaciones.
Servicios Web de Igual a Igual (Peer Web Services)	Permite que cualquier usuario publique páginas Web personales sobre una Intranet corporativa.
Seguridad	Proporciona seguridad local para archivos, carpetas, impresoras, y otros recursos. Los usuarios deben ser identificados por la computadora local o por el controlador de dominio, para poder accesar a los recursos de la máquina o de la red.
Estabilidad del Sistema Operativo	Soporta cada aplicación en espacios reservados de memoria. Una aplicación de mal comportamiento no afectará a otras aplicaciones ni al sistema operativo.

[10] Microsoft *Education and certification* Supporting Microsoft Windows NT 4.0 Core Technologies 1997

Una Windows NT Workstation mantiene su propia base de datos de cuentas de usuarios. Los grupos y las cuentas locales de estaciones de trabajo están localizadas en la base de datos de Usuarios en Windows NT Workstation o en servidores de dominio. Iniciar una sesión en una de estas cuentas permite el acceso a recursos en la computadora local, no en otras.[11]

2.3.1 Interfaz y Administración

La administración del equipo de escritorio deberá volverse más fácil también para los administradores del sistema. Las *Políticas de Sistema* y *Perfiles de Usuario* de NT, proporcionan un medio conveniente de controlar el acceso a los recursos de la red y del equipo de escritorio. Las políticas del sistema ayudan a los administradores a estandarizar las configuraciones de los equipos de escritorio y a reforzar el comportamiento. Se pueden almacenar perfiles ambulantes de usuario en un servidor NT, de manera que los usuarios siempre reciben el mismo escritorio, sin importar su ubicación.

2.3.2 Mejoras para Trabajo en Red

NT Workstation 4.0 cuenta con Servicios de Cliente para NetWare, que soporta el Servicio de Directorio NetWare (NDS: NetWare Directory Service). Esto permite a los usuarios NT conectarse en los servidores NetWare 4.x que ejecutan NDS y tener acceso a archivos y a recursos de impresión.

El Protocolo de Túnel Punto a Punto (PPTP por las siglas en inglés de: Point-to-Point Tunneling Protocol), es un estándar abierto que le permite usar Internet u otros proveedores públicos, para proporcionar conectividad segura entre clientes remotos y redes públicas. También proporciona la base para la tecnología de Red Privada Virtual (VPN: Virtual Private Network) de Microsoft. Al usar PPTP, los usuarios remotos pueden marcar a un proveedor Internet local y dirigirse a su red corporativa, encontrando la misma seguridad y características que se encuentran en su red privada. Desde la perspectiva del usuario, la ruta de conexión física es irrelevante, el túnel VPN encapsula todos los datos en paquetes IP (Internet Protocol - Protocolo de Internet). VPN soporta los protocolos para red más importantes, incluyendo TCP/ IP, IPX/SPX y NetBEUI

NT Workstation 4 0 soporta Mensajería Windows, una bandeja de entrada universal para correo electrónico que incluye controladores para Internet y Microsoft Mail El soporte Internet incluye la habilidad para intercambiar correo sobre cualquier red con servicios SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correspondencia) o de Protocolo 3 para Oficina Postal

---

[11] SHELDON Tom *Manual de Seguridad de Windows NT* McGRAW HILL 1997 Pag 156

(POP3: Postal Office Protocol 3). La Mensajería incluye soporte completo MAPI 1.0, permitiéndole enviar, recibir, organizar y almacenar correo electrónico, y objetos de sistema de archivos.

DCOM (Distributed Component Object Model – Componentes Distribuidos de Modelos de Objetos), un sistema de objetos de software diseñado para volverse a usar y para reemplazarse, en teoría permite distribuir procesos a través de computadoras múltiples proporcionando la infraestructura de comunicaciones basada en objetos NT Workstation 4.0 soporta DCOM escondiendo los detalles de señaladores de aplicaciones tanto de la aplicación como del objeto

2.4 *WINDOWS NT ADVANCED SERVER*

Advanced Server (Servidor Avanzado) incluye herramientas de administración que no tiene Windows NT Workstation, ya que incluye un usuario para el manejo de dominios, un programa de interfaz para administrador del servidor local, y los remotos, si se desea Se pueden configurar cuentas de operador que permiten a una persona agregar y reconfigurar cuentas de usuarios, pero no cambiar las configuraciones de los servidores, operadores de respaldos y de impresoras, que como su nombre lo indica controlan los dispositivos pertinentes Operadores del servidor pueden manejar impresoras, respaldos, archivos, formatear un disco del servidor y cambiar la fecha del sistema

Advanced Server permite la creación de grupos globales y locales para controlar a los usuarios y sus características.

Los servicios del Advanced Server se clasifican en cuatro amplias categorías: la administración y manejo de red, la seguridad y control de acceso, la confiabilidad, y el apoyo al cliente De forma significativa, el Advanced Server presenta el concepto de *dominios* al entorno de Windows. Un dominio es un grupo de servidores Bajo el Advanced Server, varios servidores pueden agruparse en un dominio y administrarse desde una misma computadora. Esta centralización le permite a los usuarios guardar configuraciones en una localización, y por tanto conectarse a la red desde cualquier dominio.

Dos servicios de servidor NT, el Servicio de Nombres Internet Windows (WINS: Windows Internet Name Service) y el Sistema de Nombres de Dominio (DNS. Domain Name System), se han combinado para proporcionar una forma de DNS dinámico. Los usuarios pueden introducir nombres de dominio DNS totalmente calificados, facilitando la conexión a recursos del sistema

El software también ofrece algunas características claves para empresas. El Advanced Server aumenta la confiabilidad del sistema con su apoyo para el RAID (Discos de Bajo Costo en Arreglo Redundante): Tanto el RAID 1, que refleja los datos de un disco a otro, y el RAID 5, que aumenta el rendimiento y la confiabilidad al esparcir los datos por un conjunto de discos y protegerlos con un chequeo de paridad [12]

---

[12] RAID: Agrupamiento de discos en la que los datos se copian en muchas unidades Proporciona un caudal más rápido, tolerancia de fallos (espejos) y corrección de errores Niveles de configuración

0 Solo separación de disco
1 Espejos (duplicación 100%)
2 Corrección compleja de errores
3 Transferencia en paralelo unidad de paridad
4 Transferencia independiente, no unidad de paridad
5 Transferencia independiente, unidad de paridad

El Advanced Server facilita la configuración de los clientes mediante la repetición de directorios, una característica que originalmente se ofreció en el LAN Manager basado en Microsoft OS/2 Esta característica deja que un servidor automáticamente cargue archivos, desde un directorio particular del servidor, para clientes designados. Se apoyan los usuarios remotos mediante los Servicios de Acceso Remoto (RAS); estos servicios se expanden desde un usuario único en NT a 64 usuarios en el Advanced Server.

NT soporta clientes de DOS, Windows, Unix y OS/2. El Advanced Server añade apoyo para la Macintosh

2.4.1 NT: Servidor de aplicaciones

Microsoft enfatiza los beneficios de usar NT como un servidor de aplicaciones. Según Microsoft, NetWare es suficiente como un servidor de archivos e impresoras, pero las aplicaciones de cliente/servidor demandan una arquitectura diferente, una como la que provee Windows NT

Una de las aplicaciones más populares para el servidor de una red es que funcione como el servidor de la base de datos, y esta característica la posee NT.

2.4.2 Operabilidad Internet

NT Server 4.0 es un sistema operativo para redes muy poderoso. Su facilidad de uso, flexibilidad, y servicios avanzados de Internet/Intranet y comunicaciones, satisfacen hasta las necesidades más avanzadas de computo para negocios

Para los desarrolladores "Webmasters"[13], la conectividad es la clave para producir aplicaciones que puedan integrarse tanto a través de redes locales como de Internet. La integración total del Microsoft Internet Information Server (IIS), así como la adición del Index Server, Microsoft Internet Explorer, y Microsot Frontpage para la creación y administración de Webs, se combinan para hacer de Windows NT Server una plataforma Internet/Intranet aún más poderosa que las versiones anteriores.[14]

Los Servicios Web de Igual a Igual (PWS. Peer Web Services), un subconjunto de IIS Workstation, permite que cualquier usuario publique páginas Web personales sobre una intranet corporativa. PWS también ofrece una plataforma en la cual se pueden desarrollar y probar aplicaciones Web. Aunque es mucho más modesto que IIS en cuanto a requerimientos de recursos, PWS proporciona todas las extensiones y filtros ISAPI y está integrado en el modelo de seguridad NT.

---

[13] Administrador y desarrollador de Intranet/Internet

[14] Microsoft Windows NT Server Folleto de información México, 1996 Pag 1

2.5 SISTEMA OPERATIVO DE SICORI

En este capítulo se ha ofrecido un resumen de las características y ventajas más importantes de Windows NT, las cuales sirven de apoyo para que SICORI lleve la implantación de este sistema operativo para trabajar en red

Windows NT es un sistema operativo de 32 bits, esto significa que las instrucciones, gráficas y transferencia de datos a los diversos sistemas de almacenaje se ejecutan más rápido. Es un sistema multitareas, multiusuario, trabaja en serie, y es del tipo cliente servidor (aunque también tiene características con las que se le puede considerar como del tipo peer-to-peer)

Desde sus inicios, SICORI ha utilizado Windows NT como su sistema operativo por las facilidades de uso que éste brinda. Todas las máquinas tienen instalado Windows NT 4 0 Server o Workstation, según se requiera (ver tabla 2.4); ya que la organización trabaja con aplicaciones de 32 bits y requiere de un ambiente de trabajo con alto desempeño y seguridad, y NT ofrece estas opciones. Además de que agrega una atractiva combinación de estabilidad y confiabilidad en los recursos de red y en la administración de usuarios, y éstos obtienen un incremento en su desempeño, un amplio rango de nuevas y mejores características de conectividad en accesos remotos; lo que implica el desarrollo de una estrategia administrativa eficiente, como se verá en el capítulo III.

Tabla 2.4 Distribución de software en los equipos de SICORI.

# Equipos	Tipo de Equipo	Software Instalado
40	Estación de Trabajo	Windows NT Workstation 4.0
4	Servidor de Impresión	Windows NT Workstation 4.0
2	Servidor de Base de Datos	Windows NT Advanced Server 4.0
2	Servidor de Documentos	Windows NT Advanced Server 4.0
1	Destinado para Servidor de PDC (Controlador Primario de Dominio)	Windows NT Advanced Server 4.0
1	Destinado para Servidor de BDC (Controlador de Copia de Seguridad del Dominio)	Windows NT Advanced Server 4.0

ADMINISTRACION DE WINDOWS NT

La administración del sistema es un tema de gran trascendencia en cuanto a la seguridad. Si no se entiende totalmente el sistema de seguridad, y como resultado, se configuran opciones inadecuadamente, los intrusos podrían aprovecharse de el sistema. Permisos inadecuados de el sistema de archivos permitirán a los invasores y a los usuarios legítimos a acceder a los archivos que no deberían poder acceder.

Si no es posible administrar todos los servidores, se recomienda Windows NT Workstation sólo para las tareas administrativas. De preferencia la red debe ser administrada desde una sola estación o desde un servidor como el controlador de dominio primario[1].

Hay *un determinado número de cosas que podrían proteger al sistema* durante la fase de instalación y configuración. Se requiere utilizar equipo de alta calidad para evitar pérdida de tiempo, y si se están actualizando equipos antiguos, es necesario comprobar que el disco duro no este dañado

No se deben crear sistemas de arranque dual para Windows NT Server. Un sistema de arranque dual es aquel que contiene dos o más particiones de disco, cada una de las cuales tienen sistemas operativos distintos. Un problema con los sistemas de arranque dual es que un intruso que tenga acceso físico al servidor *podría arrancar desde otra partición y usarla para ejecutar programas que puedan* explorar las particiones de disco de Windows NT. Es recomendable desactivar también la unidad de disco flexible y bloquear la cubierta para evitar este mismo tipo de ataque

Existen básicamente dos modelos de red en el entorno Windows. el modelo de trabajo en grupos y el modelo de dominios

❑ Modelo de trabajo en grupos.

Es un modelo simple de red en el que los usuarios en sus propias estaciones de trabajo participan con un grupo de usuarios en la compartición de recursos. El usuario local puede ser responsable de garantizar el acceso a los recursos de su computadora para los demás usuarios del grupo Todas las versiones actuales de Windows permiten este tipo de trabajo en grupo. Los nombres de las computadoras son importantes para este modelo.

---

[1] *En el capítulo cuatro se hablará detalladamente sobre controladores de dominio*

❑ Modelo de dominio

En el modelo de dominio, el acceso a los recursos está fuertemente controlado por un administrador central que controla una computadora Windows NT Server (el cual está ejecutando un servicio de administración de dominios). Este modelo implementa cuentas de usuarios válidos que son requeridas para validar los permisos de uso de recursos compartidos

El modelo de dominio es realmente un avance sobre el modelo de trabajo en grupos. La colección de computadoras para trabajo en grupo simplemente se convierten en un dominio, en el cual, la seguridad en la cuenta de los usuarios la administra un controlador de dominio. Sin embargo, cuando se utiliza el modelo de dominio, cualquier cliente puede todavía elegir compartir un recurso de su computadora con cualquier otra de la red

Un administrador de alto nivel único, puede estar a cargo de la configuración de políticas en toda la organización, mientras que los administradores de dominio individuales pueden implementar esas políticas en sus propios dominios Alternativamente, los dominios pueden ser instalados para ser configurados individualmente. Los administradores de dominio pueden asignar a un subadministrador para tratar varias tareas administrativas Windows NT incluye grupos de administración especiales que hacen más fácil crear una jerarquía de administración Añadiendo usuarios a estos grupos, se da a los primeros los derechos y permisos de los segundos para administrar varias partes del dominio.

3.1 CUENTAS DE USUARIOS Y DE GRUPOS

Cualquier usuario que quiera acceder a un sistema Windows NT seguro, debe tener una cuenta de usuario en ese sistema Un nombre de usuario identifica a un usuario y una contraseña le franquea el camino Los grupos son colecciones de usuarios Es más fácil para un administrador asignar derechos y permisos a grupos de usuarios que a cada usuario individual. Los grupos pueden ser también destino de listas de correo electrónico y de actividades planificadas.

En computadoras Windows NT aisladas, las cuentas de usuarios son sólo para la computadora y se administran con la utilidad de Administración de usuarios que se ejecuta en la máquina. En un entorno de dominios de red consistente en computadoras Windows NT, las cuentas de usuarios se administran para todo el dominio aunque las computadoras Windows NT puedan tener cuentas propias de usuarios. En el entorno de dominios, las cuentas son administradas por la utilidad de Administración de usuarios para dominios del Windows NT Server.

3.1.1 Cuentas de usuarios

Las cuentas de usuarios contienen información sobre los usuarios, tales como su nombre completo, su nombre de usuario, su contraseña, la localización de su directorio de inicio de sesión, la información sobre cuándo y cómo ha iniciado su sesión, y las configuraciones personales de su escritorio

Cuando se crea la cuenta de un nuevo usuario, Windows NT le asigna un *identificador de seguridad único (SID)*[2]. *Todos los procesos internos utilizan ese* SID para identificar al usuario en vez de utilizar el nombre de usuario de la cuenta. Este identificador (ID)[3] es único para cada cuenta. Si se crea una cuenta, la borra y la vuelve a crear con el mismo nombre de usuario, el SID es nuevo y distinto

Cuando se instala por primera vez un Windows NT Server o Workstation, se crean por default dos cuentas:

- *Administrador*

Esta es la cuenta con mayores niveles de privilegios porque proporciona acceso completo al sistema o al dominio. Se suelen instalar dominios y cuentas administrativas alternas. La cuenta no puede ser borrada o deshabilitada, pero se recomienda que se cambie de nombre y se le asigne una contraseña para que permanezca oculta a los ataques.

---

[2] SHELDON, Tom ***Manual de Seguridad de Windows NT.*** McGRAW-HILL pág 76, 96
[3] SHELDON Tom ***Manual de Seguridad de Windows NT.*** McGRAW-HILL pág 76 , 96

El Administrador puede hacer lo siguiente:

- Crear y administrar cuentas de usuarios y grupos
- Crear directorios compartidos y conectarse a directorios compartidos.
- Establecer relaciones de confianza
- Administrar todos los aspectos de los discos duros
- Administrar todos los aspectos de impresoras y de la compartición de impresoras.
- Administrar políticas de seguridad.
- Administrar registros de auditoria y de seguridad.
- Modificar el sistema operativo e instalar nuevos controladores.
- Adueñarse de archivos y otros objetos
- Bloquear e iniciar sesiones y apagar servidores.

❑ Invitado (Guest)

Esta cuenta permite muy pocos accesos al sistema y se emplea para dar servicio a gente que no tiene cuentas. Por default, no se activa en el servidor Windows NT 4.0; sin embargo, si se activa en estaciones de trabajo Windows NT 4 0. Los usuarios que inician la sesión como *invitado* no necesitan especificar un nombre de usuario, por lo que no se puede saber quién está utilizando la computadora y no se podrán auditar las actividades de un usuario especifico.

Un administrador de sistemas es responsable de la administración de la red y del equipo del servidor, de planificar el sistema, las cuentas de usuarios, los datos almacenados, y una gran variedad de otras cosas. Si otra gente tuviese que administrar el sistema utilizando la cuenta del administrador, se deben crear cuentas alternativas de administrador por una buena razón· cada cuenta puede ser rastreada por separado y así seguir actividades maliciosas.

Por razones de seguridad, no se debe permitir que *invitados* tenga permisos de escritura o borrado en cualquier archivo o directorio; deben sólo poder leer archivos en directorios especificos. Si necesitan guardar archivos, entonces se debe crear un directorio, en donde tengan privilegios de escritura. Así podrán escribir en él, pero nunca podrán leer los archivos almacenados, ni siquiera el que ellos dejen.

3.1.2 Políticas de cuentas

Las politicas de cuentas controlan las restricciones de contraseñas y los bloqueos de cuentas. Se activan las políticas para todas las cuentas de usuarios, ya sea en computadoras individuales o en dominios. La figura 3.1 muestra la caja de diálogo de las politicas de cuentas.

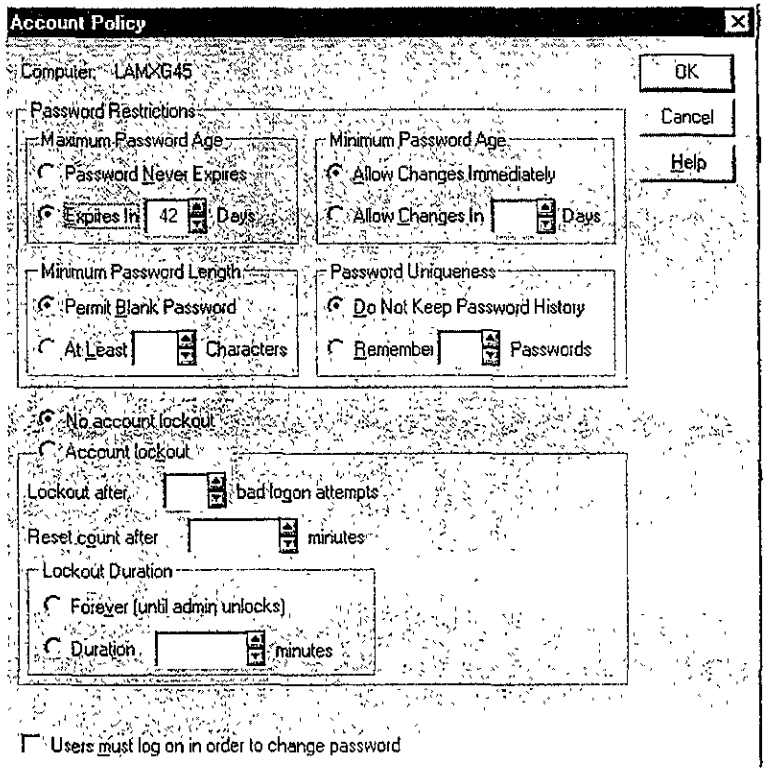


FIGURA 3.1 Políticas de Cuentas.

Todas las configuraciones del cuadro de diálogo de políticas de cuentas son críticas si se desea activar una seguridad consistente. Todas ellas aseguran que las contraseñas se han implementado cuidadosamente por los usuarios, y que son difíciles de adivinar. Se pueden configurar las siguientes opciones

- Finalización de la vida de las contraseñas después de un número de días.
- Obligar a los usuarios a crear contraseñas de un determinado número mínimo de caracteres.
- Asegurar que los usuarios no reutilizan contraseñas que han usado recientemente.
- Bloqueo de cuenta. Si un intruso intenta entrar en la cuenta de un usuario adivinando la contraseña, se puede bloquear la cuenta si éste intenta acceder y falla más de un determinado número de veces.

Otras opciones para evitar el uso indebido de cuentas que aparece en las propiedades de la cuenta de cada usuario en el servidor de dominio, son las siguientes: [4]

- Limitar el horario de uso de la cuenta.
- Permitir al usuario iniciar sesión sólo desde ciertas máquinas.
- Poner fecha de caducidad a las cuentas.

3.1.2 Grupos

Los grupos son conjuntos de cuentas de usuarios. Es más fácil garantizar derechos y permisos a grupos que a usuarios individuales. Después de crear un grupo, se añaden cuentas de usuarios a él, asignándole los derechos y permisos adecuados.

Windows NT tiene un número de grupos predeterminados. Pertenecen a dos categorías distintas: *grupos locales y grupos globales.*

❑ Grupos locales

Este tipo de grupos define permisos y derechos para usuarios sobre máquinas locales dentro de un dominio, pero se pueden añadir cuentas de usuarios y de grupos de otros dominios a este grupo

Los grupos locales en Windows NT Workstation y en Windows NT Server que no son controladores de dominio incluyen las cuentas de *Administradores, Operadores de copia de seguridad, Usuarios, Invitados y Todos.* Las computadoras Windows NT aisladas no conectadas a la red, sólo necesitan y crean usuarios locales.

❑ Grupos globales

Un grupo global consiste en cuentas de usuarios sólo del dominio donde se ha creado el grupo global, pero los grupos globales pueden ser miembros de grupos locales que sean parte del mismo dominio o de otros dominios. Hecho esto, los primeros obtienen los permisos de los segundos. Los grupos globales existen sólo si un controlador de dominio está presente en la red

[4] http //enete fie us es

3.1.3 Derechos de usuario

Los *derechos de usuario* definen qué pueden hacer los usuarios en los servidores y las estaciones de trabajo de una red Windows NT No se deben confundir éstos con permisos, que son los controles de acceso que definen qué usuarios pueden acceder a los objetos (archivos, directorios, dispositivos) y qué pueden hacer con ellos Los derechos de los usuarios están otorgados directamente al usuario. Algunos de los derechos más comunes son.

- El derecho a iniciar la sesión directamente en la computadora (inicio de sesión local)
- El derecho a iniciar una sesión en una computadora sobre la red (inicio de sesión remota)
- Derechos de administración, tales como la posibilidad de crear nuevas cuentas de usuarios.

3.1.4 Grupos de Programas

Al instalar una nueva aplicación dentro de Windows NT 4 0, su ejecución depende del tipo de usuario que se sea. Si se tienen los permisos de un usuario ordinario, esa aplicación sólo estará disponible para el mismo usuario. Cualquier grupo de programas creado por el programa de instalación sólo aparecerá en su menú particular de Inicio Por otro lado, si se conecta con privilegios de administrador, la instalación aparecerá por omisión en los *grupos Comunes* que sé encuentran en la parte inferior de la lista de Programas para todos los usuarios del sistema. En *\Winnt\Profiles\All Users\Start Menu* se pueden eliminar o añadir manualmente elementos a la lista. Por supuesto, también se necesitan derechos de administrador para poder hacerlo.

3.1.5 Perfiles de usuario

Cuando un usuario inicia la sesión en una computadora, puede tener varios entornos de trabajo configurados y cargados en el sistema Estas configuraciones incluyen esquemas de escritorio, colores, conexiones de red e impresoras, teclas abreviadas y otras configuraciones. Cada usuario puede tener su propio perfil profesional que se usa independientemente desde dónde acceda, porque los perfiles se almacenan en servidores centrales. Esto significa que un usuario puede viajar de una computadora a otra de la red y mantener sus propias configuraciones de escritorio de Windows

Todo lo que necesita el administrador es especificar la dirección del perfil dentro de la cuenta del usuario. Luego cuando el usuario inicia la sesión, se carga su perfil actual. La primera vez que el usuario accede, el perfil está vacío, pero cualquier cambio que se haga en la configuración del escritorio se almacenan en el perfil cuando acaba su sesión, y se vuelve a cargar la próxima vez que vuelva a iniciar la sesión.

También hay perfiles de usuario obligatorios impuestos por el administrador que no pueden ser cambiados por los usuarios Estos son importantes en cuanto a la seguridad, ya que pueden prevenir a los usuarios de hacer cosas que no estén permitidas .

Debido a que NT está diseñado para permitir que múltiples usuarios se conecten sin interferir con la información de los demás, cada usuario obtiene una carpeta *Escritorio* independiente que se encuentra almacenada junto con una gran cantidad de otras carpetas especificas del usuario (menú Inicio, Favoritos, etc) entre la jerarquía de carpetas *\Winnt\Profiles\Nombre de usuario*

3.2 EL SISTEMA DE ARCHIVOS DE WINDOWS NT (NTFS)

NTFS es un sistema de archivos que permite más seguridad que los sistemas de archivos tales como el FAT (File Allocation Table - Tabla de asignación de archivos) de DOS[5]. Durante la instalación de Windows NT, se elige entre el FAT de DOS y el NTFS, pero si se está interesado en la seguridad, se debe elegir NTFS. NTFS permite un número de protecciones sobre archivos y directorios que permiten especificar qué usuarios y grupos pueden acceder a qué información y exactamente cómo pueden hacerlo. La conversión de FAT a NTFS puede realizarse en cualquier momento usando el comando *convert* :

convert unidad: /fs:ntfs

NTFS tiene características de seguridad, las cuales se mencionan a continuación.[6]

- Windows NT no utiliza para nada los servicios del sistema DOS. Arranca por su cuenta y utiliza sus propios servicios.
- Todas las funciones de accesos a disco de bajo nivel las realizan controladores software específicos de Windows NT, no controladores de disco almacenados en la BIOS de la computadora.
- Si se ejecuta un programa DOS desde Windows NT, el sistema operativo no permitirá que el programa escriba directamente en los discos duros

NTFS proporciona un modo de controlar el acceso a los archivos y directorios con permisos. Los permisos son una parte de la seguridad en Windows NT, controlan el acceso a todo tipo de objetos, no sólo a los objetos del sistema de archivos. Se pueden instalar permisos en directorios que serán heredados por todos sus archivos y subdirectorios. Se puede también configurar permisos individuales en archivos dentro de directorios.

3.2.1 Compartición de recursos

Hay dos aspectos en la seguridad del sistema de archivos el primero, es la restricción del acceso a la información de una computadora local a la gente que inicia la sesión en esa computadora El segundo, es la restricción del acceso a la información que se comparte en la red. Cuando un directorio está compartido, los usuarios pueden acceder a él desde las estaciones de trabajo unidas a la red basados en permisos.

---

[5] SHELDON, Tom *Manual de Seguridad de Windows NT* McGRAW HILL pág 101
[6] SHELDON, Tom *Manual de Seguridad de Windows NT*, McGRAW-HILL pág 101

Durante la instalación de NT se asignan por defecto permisos de control total a todos los usuarios sobre todos los archivos, esta peligrosa situación debe ser modificada por el administrador antes de que alguien cause un desastre en el sistema. Estos cambios sólo deben realizarse inmediatamente después de haber instalado el sistema, si ya sé tienen aplicaciones instaladas, podrían dejar de funcionar correctamente

Para hacer accesible la información en un sistema Windows a otros usuarios en la red, se comparten carpetas. Cuando se comparte una carpeta, todos los archivos y todas las subcarpetas de ella se comparten también. Se puede entonces cambiar los permisos de acceso de cualquier archivo o carpeta en la carpeta compartida si necesita bloquear el acceso.

3.2.2 Configuración de permisos

El acceso a carpetas y archivos está controlado por permisos, y los permisos están configurados por el administrador o por el propietario del recurso. Hay permisos estándar y permisos individuales. Los permisos individuales de la siguiente lista se usan combinados para crear permisos estándar como se describirá a continuación:

- **Lectura (R).** Abrir y ver los contenidos de un archivo.
- **Escritura (W).** Cambiar los contenidos de un archivo o crear un nuevo archivo.
- **Ejecución (X).** Ejecución de un programa o archivo ejecutable.
- **Borrado (D).** Borrado de archivos.
- **Cambio de permisos (P).** Alteración de los permisos de un directorio o archivo.
- **Toma de posesión (O).** Hace que uno mismo sea el propietario de un archivo o directorio.

Los permisos estándar son una combinación de estos permisos individuales y están diseñados para conseguir un conjunto de permisos apropiados para la mayoría de los usuarios. Los permisos estándar para carpetas se listan en la Tabla 3 1. La segunda columna lista los permisos individuales que forman los permisos estándar, y la tercera columna indica los permisos que los nuevos archivos obtienen cuando se añaden a la carpeta

Tabla 3.1 Permisos para carpetas[7].

Permisos estándar para carpetas	Permisos Individuales	Permisos para nuevos archivos
Sin acceso	Ninguno	Ninguno
Listar	Lectura, ejecución	Sin especificar
Lectura	Lectura, ejecución	Lectura, ejecución
Añadir	Lectura, ejecución	Sin especificar
Añadir y Lectura	Lectura, escritura y ejecución	Lectura, ejecución
Cambio	Lectura, escritura, ejecución y borrado	Lectura, escritura, ejecución y borrado
Control Total	Todo	Todo

La Tabla 3.2 lista los permisos individuales que forman los permisos estándar para archivos. Desde luego, se pueden crear permisos de acceso especiales en cualquier momento que se necesite.

Los usuarios pueden conseguir los permisos para acceder a las carpetas y archivos de diferentes maneras. Por ejemplo, podrían tener permisos de *Lectura* a través de su propia cuenta de usuario y permisos de *Cambio* debido a que pertenecen a un grupo. Se aplican los más altos niveles de permisos, los permisos son acumulativos por lo que la asignación de permisos de distintas fuentes se combina. Sin embargo, un permiso de *No acceso* de cualquier fuente niega el acceso a un archivo o directorio, sin importarle que otros permisos lo concedan.

Tabla 3.2 Permisos para archivos[8].

Permisos estándar para archivos	Permisos Individuales
Sin acceso	Ninguno
Lectura	Lectura, ejecución
Cambio	Lectura, escritura,ejecución y borrado
Control Total	Todos

[7] SHELDON Tom *Manual de Seguridad de Windows NT*. McGRAW HILL pág 103
[8] SHELDON, Tom *Manual de Seguridad de Windows NT* McGRAW-HILL pág 103

3.2.3 Compresión de carpetas y archivos

Si se configuró NT para que empleará el sistema de archivos FAT compatible con Windows 95, no se tiene ninguna opción de compresión. Los viejos volúmenes[9] comprimidos con cualquier versión de DriveSpace no estarán disponibles para NT. En cambio, con Windows NT como sistema operativo único en el equipo, con NTFS (System File NT – Sistemas de Archivos de NT), se pueden comprimir archivos, carpetas o unidades completas. Cuando se comprime toda una carpeta, cualquier archivo añadido a esa carpeta será comprimido automáticamente.[10]

Los usuarios individuales no pueden editar los permisos para otros usuanos y grupos, pero pueden establecer permisos para archivos que les pertenecen, lo cual les permite mantener la seguridad de sus archivos individuales. Los usuarios pueden escandalizarse cuando sepan que los administradores pueden adquirir la propiedad de un archivo y transgredir la seguridad, pero existen buenas razones para ese diseño; por ejemplo, si un empleado es despedido los administradores pueden necesitar tener acceso a los archivos de trabajo de un proyecto crucial.

---

[9] Volumen, se define como:
1) Una unidad de almacenamiento físico, como un disco duro, disco flexible, cartucho de discos o carrete de cinta
2) Una unidad de almacenamiento lógico que abarca una cantidad de unidades físicas

[10] PAYRO OGARIO, Pablo PC Computing. ***Supergula de Windows 95/NT Supergula Anual de Windows.*** México 1996 Pág. 54

3.3 ADMINISTRADOR DE TAREAS

Para eliminar una aplicación de mal comportamiento que esté trabajando bajo Windows NT, Windows NT 4.0 marcó el debut del Administrador de Tareas actualizado de NT Responde a las teclas ***Ctrl-Alt-Del*** mostrando una lista de los programas que se están ejecutando y ofreciendo la opción de eliminar cualquiera de ellos con un sólo clic. Gracias a la poderosa protección de memoria de NT, el Administrador de Tareas casi siempre puede prevalecer frente a una aplicación que cause problemas. Un nuevo separador del Administrador de Tareas permite ejercer ese mismo control sobre procesos en segundo plano que normalmente no aparecen como aplicaciones que se están ejecutando. Un tercer separador brinda una vista del uso del CPU y de la memoria. Lo mejor de todo es que el Administrador de Tareas sé reduce a una pequeña bandeja cuando se minimiza Se debe hacer clic con el botón derecho del mouse sobre la Barra de Tareas para que aparezca un menú contextual con opciones para el Administrador de Tareas. También se puede buscar el archivo *Taskmgr exe* en la carpeta *Winnt\System32* y arrastrarlo hacia el botón de Inicio.

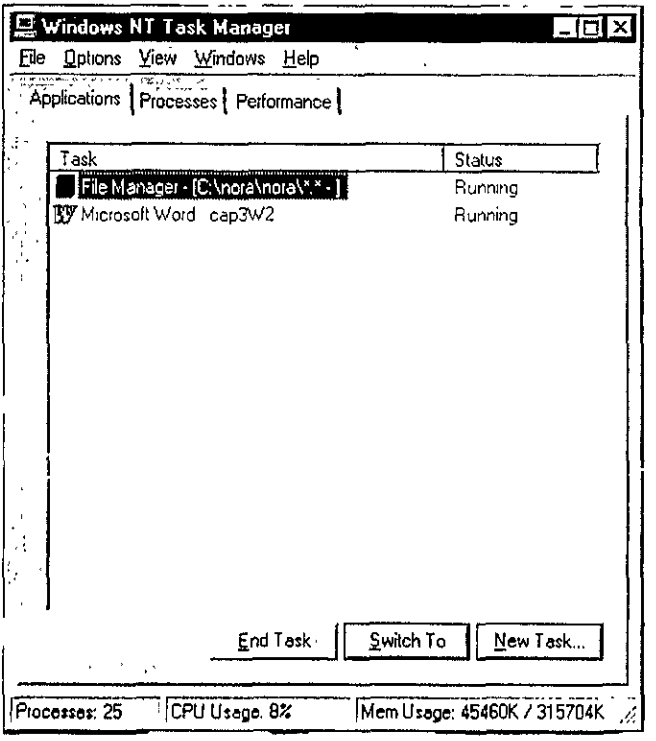


Figura 3.2 a) Programas que se están ejecutando

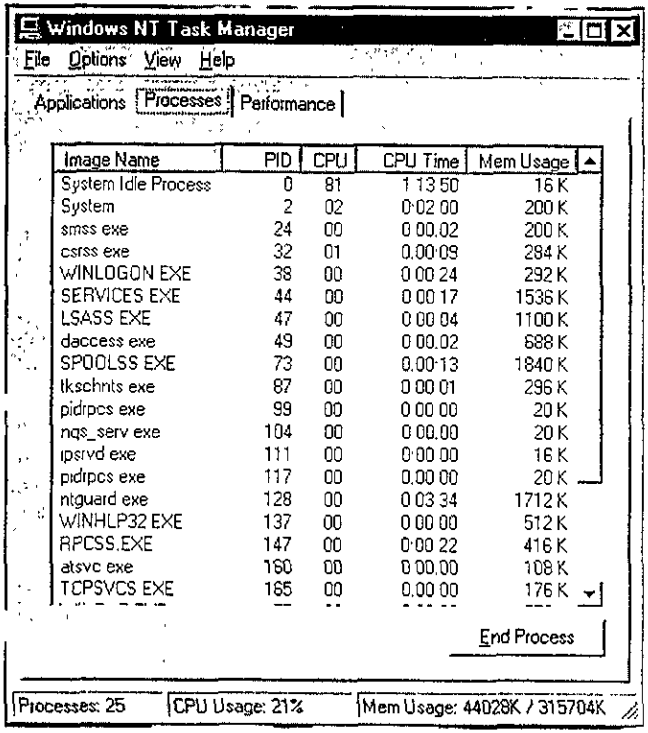


Figura 3.2 b) Procesos que se están ejecutando

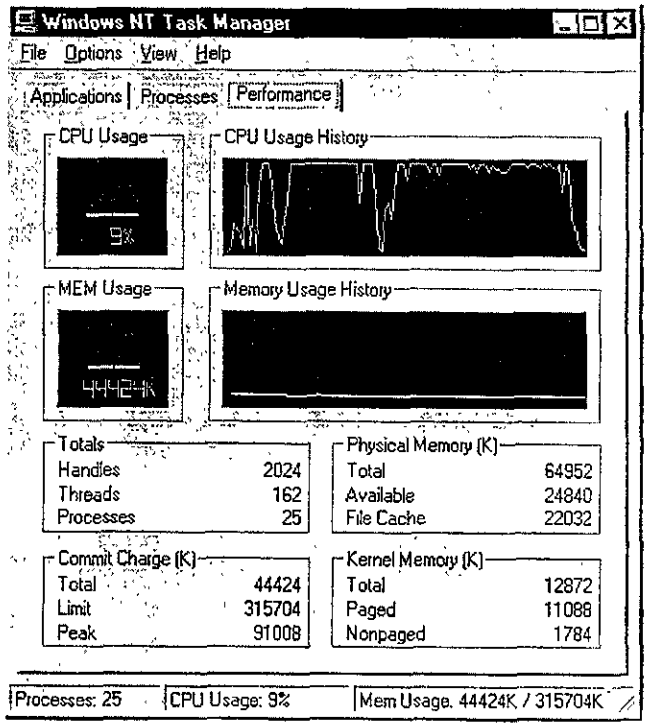


Figura 3.2 c) Uso de CPU y de la Memoria.

Figura 3.2 Administrador de Tareas de Windows NT

En la figura 3.2 (a,b y c) se muestran las pantallas del Administrador de Tareas de Windows NT

3.4 IMPRESIÓN CON WINDOWS NT

Debido a que NT es más rico en opciones de seguridad, se tiene un mejor control sobre las impresoras compartidas.

Cualquier usuario autorizado puede conectarse a una impresora remota dentro de un servidor NT o dentro de una estación de trabajo, al igual que lo haría con una impresora compartida en Windows 95. Sin embargo, en las redes NT, también es posible administrar la impresora en forma remota, si es que se cuenta con los permisos de acceso de Control total.

El administrador del sistema, puede remotamente liberar o dar priviledios de impresión a cualquier archivo que se encuentre en la cola de impresión. En la figura 3.3 se muestra una pantalla de las propiedades de un archivo "encolado", al cual se le otorgarán privilegios de impresión.

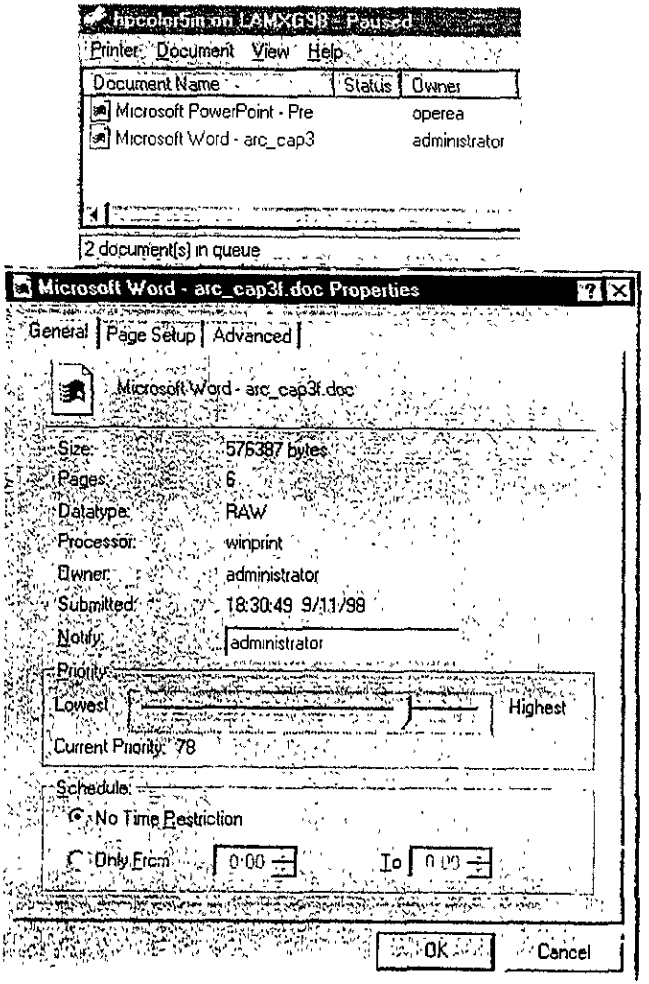


Figura 3.3 Privilegios de impresión

3.5 EL ADMINISTRADOR DE DISCOS

El administrador de disco es la herramienta gráfica que emplea NT para la administración de discos duros, con dicha herramienta podemos:

- Administrar particiones de disco y unidades lógicas.
- Dar formato a volúmenes y asignarles nombres.
- Leer la información del estado de los discos.
- Leer la información del estado de los volúmenes, la etiqueta y la letra del volumen, el sistema de archivos y su tamaño.
- Crear y modificar las asignaciones de letras
- Ampliar un volumen o un conjunto de volúmenes
- Crear y eliminar conjuntos de volúmes.
- Establecer o romper conjuntos de espejos.(Ver niveles raid en el glosario).

En la figura 3.4 se presenta un ejemplo de lo que se puede hacer con el Administrador de Discos:

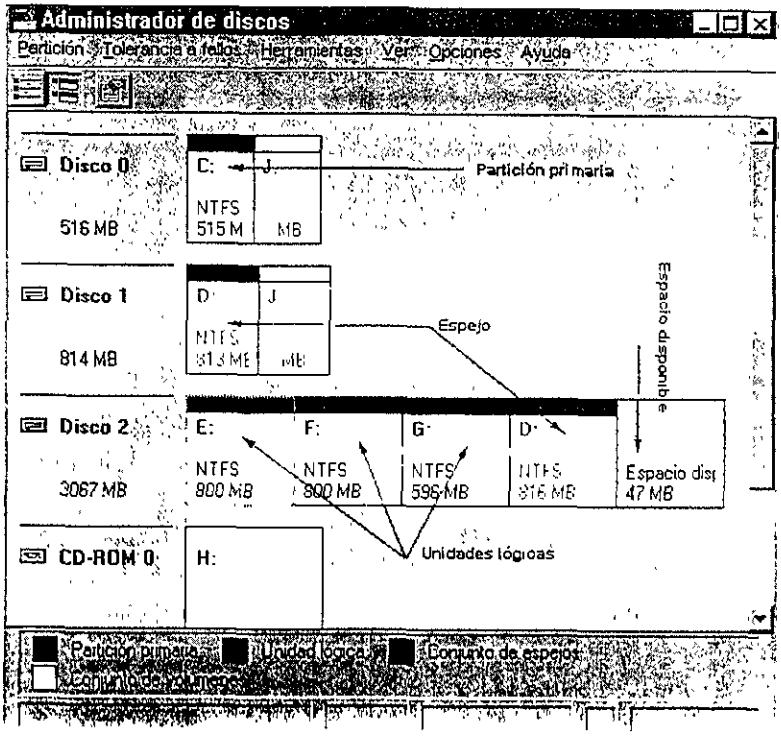


Figura 3.4 Administrador de discos

En este gráfico se puede ver al administrador de discos trabajando sobre un sistema con tres discos físicos (0,1 y 2), y un lector de cdrom. Aquí se puede apreciar:

- Una partición primaria y activa de 515 MB que contiene la unidad lógica **C:** en el disco duro 0.
- Un conjunto de espejos para integridad de datos (unidad **D:**) en el disco duro 1.
- Una unidad lógica repartida en dos particiones de dos discos distintos, el 0 y el 1,(conjunto de volumenes **J:**, aún sin formatear).
- Un disco duro con cinco particiones: tres de unidades lógicas **E:**, **F:**, **G:** y un espejo de la unidad **D:** del disco 1.
- Espacio disponible sin particionar en el disco 2.

El modo de vista "Volúmenes", resalta más las unidades lógicas, y es más completo en cuanto a datos numéricos se refiere, como la capacidad, el espacio disponible, y el porcentaje de espacio disponible en relación a la capacidad total. Estos datos son importantes, porque permiten ver que volúmenes se estan quedando pequeños, y como se tiene repartido el espacio de almacenamiento. (Ver figura 3 5).

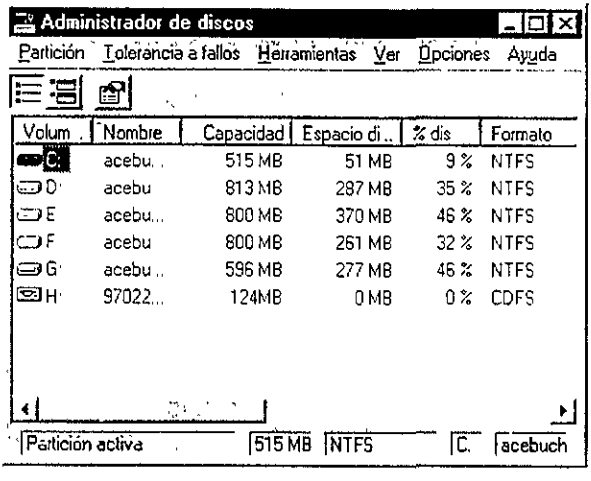


Figura 3.5 Modo de vista "Volúmenes".

Los administradores pueden utilizar la herramienta *Administrador de disco* para asignar permanentemente una letra de unidad a un disco duro específico, o a una partición. Cuando se añada un nuevo disco duro, estas letras de unidad asignadas estáticamente no cambiarán. En los discos duros, aunque no en las unidades de CD-ROM, se puede optar por no asignar una letra de unidad, a pesar de que sé podría obtener un mensaje de error si esa unidad está en uso Este

cambio no requiere que se vuelva a inicializar el sistema; tan pronto como se haga *clic* en Aceptar, la asignación de la letra de la unidad surtirá efecto.[11]

Windows NT incluye un programa de diagnóstico de disco· es posible acceder a él utilizando la opción de verificación de disco que se encuentra en la hoja de propiedades para cada disco duro local (También puede ejecutar CHKDSK desde la línea de comandos o utilizar la herramienta de Administrador de disco.) Naturalmente, no podrá ejecutar la herramienta de verificación de disco a menos que haya iniciado con privilegios de Administrador.

No se recomienda tener una sola unidad de disco duro en un servidor, es más aconsejable tener dos o tres discos, si sé tiene un disco de gran capacidad, es mejor crear varias particiones. Tener más de un disco puede ayudar en el momento en que uno de ellos decida fallar, sé perderá menos información, y siempre sé podrá mover ésta a otro disco, antes de un desastre total En caso de particionar el disco duro, es recomendable tres particiones (unidades distintas), como se muestra a continuación: [12]

- **Unidad de sistema**· será la unidad de arranque (C:), contendrá el directorio raiz de Windows, las aplicaciones de sistema y archivos críticos para el administrador (registro de actividades, información de usuarios, utilidades de diagnóstico, etc.). Por esto, es muy importante restringir al máximo los permisos en esta unidad
- **Unidad de usuarios**: incluye las carpetas personales, los datos comunes y los archivos para instalar aplicaciones.
- **Unidad de uso público**: contendrá todos los archivos accesibles desde el exterior: ftp público, páginas html del servidor web, etc Todo el mundo tendrá acceso aquí, pero es importante que los permisos sean de sólo lectura

[11] **NOTA:** El administrador de discos no permite trabajar sobre la partición de sistema (normalmente C:) ya que contiene los archivos necesarios para que NT se ejecute. El resto de las particiones son totalmente maldeables, pero se deberá tener cuidado con lo que se hace en aquellas que contengan datos, ya que se podrían perder.

[12] Esto es sólo una sugerencia de los autores de este trabajo

3.6 ADMINISTRACION CON WINDOWS NT EN SICORI

Hasta ahora, se ha mencionado lo que implica llevar una administración en un ambiente Windows NT, lo cual brinda una visión de las ventajas que ofrece éste sobre otros sistemas operativos de red; al igual, se ha detallado que NT tiene la ventaja de restringir todo tipo de privilegios a los administradores. Un administrador es quien tiene el control de todas las opciones de seguridad que implica el trabajo en red, él puede asignar un extenso arreglo de permisos de acceso para grupos individuales y predefinidos, incluyendo por ejemplo. *Usuarios de Dominio, Grupos Globales y Locales*, etc.; con lo que se puede desarrollar una administración centralizada de usuarios.

Como se ha mencionado en los capítulos anteriores, el potencial de Windows NT no era explotado en SICORI, porque no se contaba con la capacitación necesaria para su eficiente utilización. El porcentaje de seguridad era mínimo; y esto obstruía el desarrollo de una administración totalmente fuerte y segura. Se utilizaban los recursos de NT más básicos, como son monitoreo de red, partición de disco duro (en casi todos los equipos), respaldo de información (cada 3 meses), etc

Se tenía una administración descentralizada, es decir, no existía un *Dominio* ni *Grupos Globales* concentrados en un servidor. Las cuentas de usuario se administran localmente, esto implica que el administrador vaya directamente a la computadora de cada usuario para crearle su cuenta. Si el usuario olvida su *password o necesita trabajar en alguna otra máquina, el administrador debe de ir a* crearle su cuenta otra vez. Además, a la hora de crear una cuenta no existe estandarización en el *Nombre de Usuario* (login), al igual que un usuario puede pedirle a un administrador que le cambie su login y su contraseña cuando él lo desee

Lo anterior, implica un desajuste en la administración de usuarios, ya que el control de cuentas de éstos se tiene que realizar manualmente por los administradores de sistemas; lo cual ocasiona una pérdida de tiempo en el trabajo para ambos. Por ejemplo, si un usuario pide su cambio de login, o simplemente es un usuario nuevo, es necesario dar de alta su cuenta en todos los servidores de impresión, de lo contrario, no podrá mandar a imprimir. Otro incoveniente en el trabajo cotidiano de los usuarios, es que gente de otras áreas tenga acceso a sus recursos compartidos en red; lo cual provoca inseguridad en el manejo de la información

Esta falta de control en la administración dentro de la organización, ha llevado a la necesidad de implantar técnicas de seguridad en los recursos de la red, utilizando un *Controlador de Dominio* para poder proporcionar un ambiente seguro a cada uno de los miembros del sistema (como se ve en el capítulo IV). Los administradores de sistemas tendrán a cargo la creación y modificación de cuentas

de usuarios, permisiones requeridas para cada usuario y el control total de recursos de red, de una forma automática y centralizada.

CAPITULO IV

CONTROLADORES DE DOMINIO: CONSTRUCCION Y SEGURIDAD

CONTROLADORES DE DOMINIO: CONSTRUCCION Y SEGURIDAD

La administración de una red local bajo Windows NT se basa en los dominios y relaciones de confianza

Los dominios son conjuntos de computadoras y usuarios de computadora que están administrados por una autoridad central Los dominios pueden reunir a departamentos, divisiones, y/o grupos de trabajo, así como a otros tipos de grupos de computadoras. También se emplean para hacer que los grupos de computadoras sean más manejables y para aplicar políticas de seguridad en áreas específicas de la red.

Debido a que los dominios son grupos de computadoras, comparten algunas de las propiedades de los grupos. Por ejemplo, se pueden utilizar dominios para dividir lógicamente redes grandes en grupos de recursos, que hagan más sencillo a los usuarios encontrar otros recursos También, los usuarios pueden compartir recursos de sus propias computadoras cuando se establece un dominio con el modelo al nivel de usuario. Es una manera útil para los administradores de una organización, crear servidores de seguridad de la red, con estrictos controles de acceso, basados en las cuentas de los usuarios.

Los dominios sirven principalmente como herramienta de administración, con la cual se simplifica el control de las cuentas de los usuarios; pueden proporcionar:

- Una cuenta de usuario única para cada usuario, incluso cuando la red consista en distintas redes interconectadas.
- Un inicio de sesión único para acceder a los recursos de cualquier parte de la red.
- Una administración centralizada de la red, en cuanto a usuarios, grupos y recursos.

En un entorno de dominio de Windows NT, los usuarios de la red tienen cuentas de usuarios que son administradas en un *Controlador de Dominio* de un Windows NT Server en una *Base de Datos del Directorio*[1] Cada domino tiene un PDC (Primary Domain Controller - Controlador de Dominio Primario) y uno o más BDC (Backup Domain Controller - Controladores de Dominio para Copias de Seguridad) también. La Base de Datos del Directorio contiene todas las cuentas y la información de seguridad del dominio Todos los cambios en la base de datos de

[1] En el punto 4.1 se habla de la Base de Datos de Directorio

un PDC se replican en los BDC inmediatamente La sincronización de los relojes de ambos controladores es parte de este esquema. Así se asegura una ordenación adecuada de las actualizaciones y de las copias de seguridad.

Una tercena designación, es el servidor miembro, que se utiliza con los servidores que usan servicios de los dominios PDC y BDC, pero que no pertenecen a ningún dominio. Estos no tienen copias de la Base de Datos del Directorio; se pueden ejecutar aplicaciones críticas y otros servicios, que no interfieran con las tareas de administración de la Base de Datos del Directorio y en los de inicio de sesión. (Por ejemplo, un servidor miembro se puede utilizar como servidor Proxy).[2]

Los usuarios pueden iniciar la sesión en cualquier dominio escribiendo el nombre de éste en el campo "*dominio*" del cuadro de diálogo de *inicio de sesión* Esto se llama *inicio de sesión remoto* y tiene lugar sobre la red Sin embargo, si el usuario escribe el nombre de una computadora local en este campo (*dominio*), se inicia la sesión en la computadora local, y no en el dominio

Un dominio permite funciones muy importantes como las siguientes:

❑ Política de seguridad

Consiste en políticas de contraseñas (restricciones, tamaño, etc.), y políticas de bloqueos de cuentas (que determinan cuándo una cuenta se ha de bloquear si existen demasiados intentos de acceder fallidos). Se instalan estas políticas en el *administrador de usuarios para dominios*[3] eligiendo *cuenta* del menú de *políticas*. (Ver figura 3 1 del capítulo 3)

❑ Base de datos de cuentas de usuarios (Base de Datos del Directorio)

Mantiene información de las cuentas de todos los usuarios que pueden entrar en el dominio. Se puede crear una base de datos *maestra* (Dominio Maestro)[4] que contenga las cuentas de los usuarios que pertenecen a otros dominios. Haciendo esto se simplifica la administración guardando todas las cuentas de usuarios en una base de datos única.

---

[2] SHELDON, Tom *Manual de Seguridad de Windows NT*. McGRAW-HILL pág 132

[3] El ***administrador de usuarios para dominios*** es una herramienta administrativa de Windows NT Avanced Server, la cual se usa para administrar cuentas de usuarios, relaciones de confianza, políticas y otras propiedades de dominios

[4] En este capítulo, se explica que es un *Dominio Maestro*

4.1 LA BASE DE DATOS DEL DIRECTORIO

El nombre oficial para base de datos de cuentas de usuarios, es el de Base de Datos del Directorio. Mantiene toda la información de cuentas de usuarios y de seguridad del dominio; su localización principal es el PDC, pero podría estar duplicada en otros controladores de dominio. La principal función de los controladores de dominio, es almacenar y mantener la Base de Datos del Directorio.

La Base de Datos del Directorio suministra sólo uno de los pilares de la seguridad en Windows NT, describe qué pueden hacer los usuarios, y la Lista de Control de Acceso de los objetos (ACL) [5] describe qué usuarios tienen permisos para acceder a los objetos.

La Base de Datos del Directorio contiene información sobre los objetos del entorno, como cuentas de usuarios, de grupos y computadoras sobre Windows NT Workstation y Windows NT Server.[6] Su tamaño máximo recomendado es de 40 MB.

Una estación de trabajo aislada Windows NT tendrá su propia base de datos de cuentas de usuarios, que incluye los nombres de los usuarios que inician sesiones físicamente (localmente) en la computadora. Este esquema permite que muchas personas utilicen una sola computadora Si la Windows NT Workstation está unida a una red, puede participar en un grupo de trabajo y otras computadoras de ese grupo (como un sistema Windows 95) podrían usar su base de datos de cuentas de usuarios para identificar a los usuarios de la red. Esto permite que la Windows NT Workstation comparta sus propiedades de seguridad con clientes menos seguros, para mejorar la seguridad en el acceso a los recursos de la red.

Básicamente, hay dos tipos de bases de datos de cuentas de usuarios:

- La base de datos de Windows NT Workstation (o de Windows NT Server que no sea controlador de dominio) para usuarios que acceden localmente.
- La Base de Datos del Directorio para PDC's, para los usuarios de dominio.

---

[5] Una *ACL* (Lista de control de Accesos) es básicamente una lista de usuarios y de grupos que tienen permisos para acceder a un objeto Todo objeto tiene su propio ACL En el glosario de hablara mas sobre la ACL

[6] SHELDON Tom ***Manual de Seguridad de Windows NT*** McGRAW-HILL pág 134

4.2 RELACIONES DE CONFIANZA

Los dominios de una red se relacionan mediante el concepto de *Relación de Confianza* (Trust).

En el entorno de dominios, existe casi siempre la necesidad de que los usuarios accedan a los recursos de otro dominio. Para permitir este cruce de actividades, los administradores de dominios instalan las relaciones de confianza. Estas son seguras, si están bien implementadas; pero es importante, que los administradores de un dominio no confíen demasiado en otros dominios.

Si una organización tiene sólo un dominio, no se necesitan relaciones de confianza, pero en organizaciones grandes es normal la existencia de distintos dominios, con lo que las relaciones de confianza son necesarias para intercambiar información Un sólo administrador puede administrar todos los dominios, o cada dominio ser administrado por su propio equipo de seguridad.

Esta es la terminología para las relaciones de confianza:

- **Dominio confiado**. Permite que otros dominios accedan a sus recursos.
- **Dominio fiable**. Puede acceder a los recursos del domino confiado.

Hay relaciones de confianza de un sentido y de doble sentido. En las primeras, un dominio confía en los usuarios del otro dominio y les permite utilizar sus recursos, pero no viceversa. En las las segundas, hay compartición de recursos de ambos dominios. Desde luego, después de instalar estas relaciones de confianza, el siguiente paso es garantizar a usuarios y grupos específicos de un dominio que tengan acceso a los recursos del otro dominio[7].

Aquí hay algunos puntos de interés sobre las relaciones de confianza:

- Por razones de seguridad, deberían configurarse en una sola dirección, así se puede llevar un mejor control de acceso a los recursos
- Los administradores deberían explícitamente crearlas. No hay relaciones de confianza transitivas. Por ejemplo,si el dominio "A" confía en el "B" y el "B" confía en el "C", "A" no confía automáticamente en el "C".
- El acceso de un usuario a los recursos está todavía limitado por los derechos y privilegios que haya dado el administrador del dominio. Una relación de confianza en sí misma, no da a los usuarios acceso a los recursos de otro dominio
- El dominio fiable permite una relación de confianza, y el administrador del dominio confiado necesita escribir una contraseña para completar la relación.
- Se crea una cuenta de usuario oculta para la relación de confianza.

[7] http//enete.fie.us.es

- La contraseña de esa cuenta de confianza la cambia periódicamente el PDC del dominio confiado.
- Ya que todos los controladores del dominio confiado reciben la cuenta de la relación de confianza, cualquiera de estos puede instalar un canal seguro con el dominio fiable.

Es importante considerar que un usuario de un dominio puede acceder a los recursos de otro dominio como "*invitado*"[8], asumiendo que la cuenta *invitado* está activa. Esto resulta peligroso, ya que esta cuenta permite inicios de sesión anónimos en un dominio desde otro dominio, estén o no establecidas relaciones de confianza.

[8] En el capítulo 3 se mencionan las características de la cuenta *invitado*. Por default, la cuenta de *invitado* no se activa en el servidor Windows NT 4.0 , sin embargo está activada en estaciones de trabajo Windows NT 4.0 y en Windows NT 3.1

4.3 CONSTRUCCIÓN DE DOMINIOS

Una organización puede tener uno o múltiples dominios con relaciones de confianza, las cuales pueden ser de uno o doble sentido, por lo que hay relativamente pocas opciones para elegir un modelo de dominio.

Los modelos potenciales son:

- **Modelo de dominio único**. Un dominio y un administrador.
- **Modelo de dominio maestro único**. Conjunto de dominios con un sólo administrador.
- **Modelo de dominio maestro múltiple** Conjunto de dominios con administradores en cada conjunto

Cada dominio puede tener hasta 26 000 usuarios con estaciones de trabajo individuales, además, pueden tener hasta 250 grupos. Mientras estos números permiten a la mayoría de las organizaciones cumplir con sus requisitos en un sólo dominio, todavía se podría considerar la posibilidad de las ventajas que aportaría la seguridad y la administración teniendo múltiples dominios.

4.3.1 Administrador de Servidores

Es la herramienta primaria para controlar dominios. Se arranca abriendo el grupo de *herramientas administrativas* y eligiendo el *administrador de servidores.* Una ventana como la de la Figura 4.1 es la que aparece. El administrador de servidores puede ejecutarse desde una estación de trabajo, si se instalan las herramientas del servidor de Windows NT que se incluyen en el CD-ROM del NT Server.

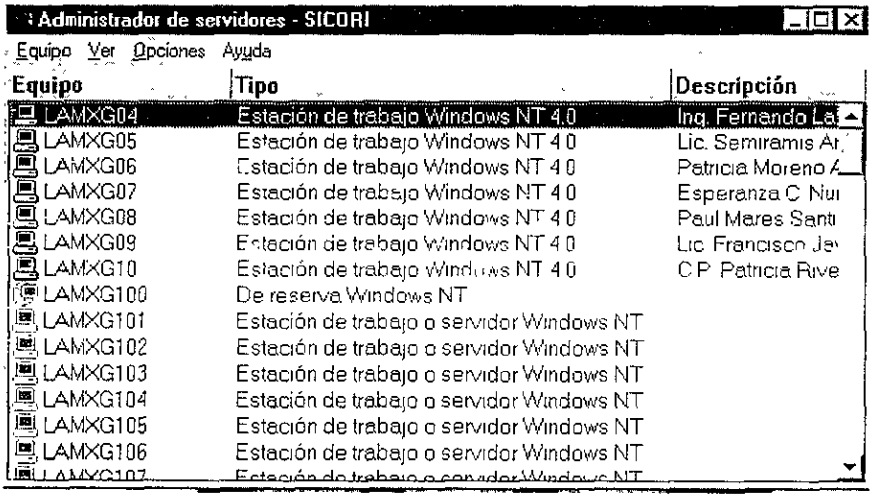


Figura 4.1. Uso del Administrador de servidores para administrar los controladores de dominios.

Se pueden realizar las siguientes tareas en el administrador de servidores:

- Administrar los roles y la comunicación entre los PDC's y BDC's
- Administrar las propiedades de servidores individuales en dominios.
- Administrar los recursos compartidos en servidores individuales en dominios.

Para controlar dominios con el administrador de servidores, se debe iniciar una sesión como miembro de los grupos locales de Administradores u Operadores del servidor, o del grupo global de Administración de dominios. Las opciones para configuraciones específicas del dominio están localizadas en el menú *equipo*, se muestran a continuación:

❑ Promoción a controlador primario de dominio

Si el PDC falla o necesita ser apagado, se selecciona el Windows NT Server que está trabajando como BDC, y se elige esta opción para promocionarlo a un estado de controlador primario de dominio. Al restaurarse el PDC original, se cambia su estado automáticamente a controlador de copia de seguridad del dominio.

❑ Sincronización de todo el dominio

Esta orden duplica la base de datos de seguridad del PDC a todos los BDC's. Se puede elegir sólo después de seleccionar el controlador primario de dominio.

❑ Añadir al dominio

Se elige esta orden para añadir computadoras al dominio, y a los usuarios de éstas se les asignan cuentas en la base de datos de seguridad del dominio, para que puedan accesar a los equipos.

❑ Quitar del dominio

Se elige esta orden para quitar una computadora del dominio Se selecciona la computadora que se quiere quitar.

❑ Selección del dominio

Sirve para escoger un dominio diferente.

4.3.2 Modelo de dominio único

Es una configuración de servidores y estaciones de trabajo Windows NT que, como indica su nombre, forma un sólo dominio. Dentro de éste hay un PDC, uno o más BDC's y servidores miembros. El dominio contiene una sola base de datos de cuentas de usuarios administrada centralizadamente. Este modelo es bueno para organizaciones pequeñas y de tamaño medio, que prefieren centralizar la administración y utilizar un modelo de dominio simple, que es más fácil de controlar. No hay relaciones de confianza que configurar porque sólo hay un dominio.

4.3.3 El dominio maestro

Es donde se almacenan todas las cuentas de los usuarios de la red; en él se definen varios grupos globales. Se crean, tanto dominios como grupos globales se requieran, y se hace que todos ellos confíen en el maestro Se configura una relación de confianza, de tal modo, que el Dominio "x" <<confía>> en el Dominio maestro. Esto da lugar a una administración centralizada Desde luego, el dominio "x" puede todavía mantener su propia base de datos de cuentas de usuarios. Un administrador local del dominio podría necesitar crear cuentas de usuarios para gente que accede a recursos sólo en el dominio "x". Al mismo tiempo, el administrador local podría utilizar una lista de cuentas de usuarios y grupos de la

base de datos maestra, para garantizar a usuarios y grupos de esa base el acceso a recursos del dominio "x".

4.3.4 Modelo de dominio maestro único

En este modelo se designa un dominio maestro, desde el cual se administran los demás dominios. Esto se hace creando relaciones de confianza que designa al maestro como el dominio fiable, y a los demás como dominios confiados. Este modelo tiene muy buena seguridad porque uno o varios administradores en una localización central, pueden controlar la red entera. Todavía es posible delegar la administración de recursos en dominios individuales a administradores locales, pero los administradores del dominio maestro tienen el control más alto en esta configuración.

Los dominios restantes se llaman dominios secundarios en este modelo. Todas las cuentas se almacenan en una base de datos de cuentas de usuarios única en el dominio maestro, y todos los usuarios inician las sesiones siendo verificados en esta base de datos. Los secundarios establecen una relación de confianza de un sólo sentido con el maestro Al mismo tiempo, los administradores del sistema local pueden controlar recursos en sus propios departamentos o divisiones, basados en privilegios administrativos que tengan asignados. Una desventaja de este modelo es que, a medida que crece la red, la base de datos de cuentas de usuarios única podría llegar a ser inmanejable.

4.3.5 Modelo de dominio maestro múltiple

Consiste en dos o más dominios maestros únicos y es adecuado para organizaciones internacionales muy grandes. Cada dominio maestro tiene sus propios dominios secundarios que se enlazan con relaciones de confianza de sentido único. Las cuentas de los usuarios se duplican entre los dominios maestros, así que se crea una red de relaciones de confianza y los administradores pueden dar permiso a los usuarios de toda la red Este modelo es especialmente adecuado para organizaciones que tienen más de 40 000 usuarios; también permite usuarios móviles que pueden iniciar las sesiones desde cualquier punto de la red.

En cualquiera de las configuraciones anteriores, es importante considerar los BDC. Los usuarios pueden acceder a éstos para identificarse; y si los usuarios están localizados en un sitio remoto, se coloca un BDC en esta localización para que los usuarios accedan. El PDC y el BDC realizan duplicación automáticamente para mantener actualizadas las bases de datos de cuentas de usuarios en las localizaciones remotas [9]

[9] SHELDON, Tom *Manual de Seguridad de Windows NT.* McGRAW HILL Pag 141

4.3.6 Elección de un modelo de dominio[10]

En la Tabla 4.1 se muestran criterios que ayudan a decidir qué modelo de dominio es adecuado para la red. Se puede utilizar para relacionar las características y las ventajas de cada modelo con sus necesidades.

Tabla 4.1 Criterio para elegir un modelo de Dominio de Red.[11]

Atributo del dominio	Dominio Único	Dominio Maestro Único	Dominio Maestro Múltiple	Dominio Independiente Único con relaciones de confianza
Menos de 40,000 usuarios por dominio	X	X		
Mas de 40,000 usuarios por dominio			X	
Administración de Cuentas Centralizada	X	X	X	
Administración de Recursos Centralizada	X			
Administración de Cuentas Desentralizada			X	X
Administración de Recursos Desentralizada		X	X	X

[10] SHELDON, Tom *Manual de Seguridad de Windows NT* McGRAW HILL Pag 144

[11] Microsoft Corporation.

4.4 INICIO DE SESIÓN EN DOMINIOS

Una computadora Windows NT puede estar en alguno de los estados siguientes:

- **Estado de fuera de sesión**. En este estado, no se permite el acceso a recursos locales o de red hasta que se inicie la sesión Se teclea ***CTRL-ALT-DEL*** para iniciar la identificación de usuario y del sistema. Después de un inicio de sesión correcto, se puede trabajar con el programa de interfaz de órdenes de usuario (Explorador o Administrador de programas) en el sistema.
- **Estado de inicio de sesión**. En este estado el sistema está dentro de una sesión, y se puede bloquear la estación, cerrar los trabajos y abandonar la sesión. Si se está en una computadora que tiene una sesión abierta, se teclea ***CTRL-ALT-DEL*** para iniciar una nueva sesión.
- **Estado de estación de trabajo bloqueada**. En este estado la estación está bloqueada por el usuario y se muestra un escritorio seguro. Se requiere una contraseña válida para desbloquear la computadora Cuando está bloqueada, una computadora todavía puede estar dentro de una sesión, pero sólo el usuario de la máquina o un administrador pueden obligarla a salir de la sesión.

En la pantalla de inicio de sesión aparecen tres campos para llenarse, en el primero y segundo se teclea el nombre de usuario (login) y su contraseña, respectivamente En el tercer campo· *dominio*, se teclea el nombre de una computadora local, o de un dominio, dependiendo del tipo de inicio de sesión que se quiera hacer (local o de dominio)

Para ejecutar la Secuencia de Atención de Seguridad (SAS)[12] se teclea ***CTRL-ALT-DEL***. SAS suministra un inicio de sesión seguro para obligar al sistema a cambiar a un entorno seguro que no deje ejecutar programas de tipo caballo de Troya.[13]

Los pasos para el proceso de inicio de sesión suministran un inicio de sesión muy seguro, que protege de ataques en los que alguien intenta reproducir información capturada para acceder o engañar al sistema Todas las contraseñas se encriptan antes de transmitirse. A continuación se mencionan estos pasos (suponiendo que se está dentro de una sesión en una Windows NT Workstation):[14]

- Tecleando ***CTRL-ALT-DEL*** se muestra el cuadro de diálogo de *Inicio de sesión*, se rellena y un proceso llamado *Winlogon* pasa las credenciales de usuario (nombre de usuario y contraseña) a la Autoridad de Seguridad Local (LSA) de la misma estación de trabajo.

---

[12] Ver el glosario

[13] Un *caballo de troya* es un programa que puede aparentar ser otro, es similar a un virus Ver el glosario

[14] SHELDON Tom ***Manual de Seguridad de Windows NT***. McGRAW-HILL pág 145

- La LSA envía las credenciales a un paquete de identificación de la misma estación.
- El Administrador de Cuentas de Seguridad (SAM) en la computadora local o de dominio se ejecuta para proporcionar el SID[15] (ID de seguridad) y el SID global. Un proceso llamado *Netlogon* pasa las credenciales entre computadoras de la red.
- El LSA de la computadora mira en la Base de Datos del Directorio las políticas, para obtener los derechos del usuario y otra información asociada con el SID, y crea un testigo de acceso
- Winlogon usa el testigo de acceso para arrancar el entorno local (una interfaz de órdenes de usuario como el Administrador de programas o el escritorio) para que se pueda acceder al sistema y a sus recursos [16]

Ahora se tiene un testigo de acceso que se puede usar para ejecutar procesos y acceder a objetos. Si se accede a un objeto como un archivo, los SID del testigo se comparan con los SID de la Lista de Control de Accesos

Lo siguiente podría ocurrir durante un inicio de sesión·

- Si el nombre del usuario no es válido y si una cuenta de *invitados* está activada, el usuario accede al dominio o al dominio fiable como invitado
- Si la cuenta *invitados* no está activada, o si el nombre de usuario es válido pero la contraseña no lo es, aparece un mensaje denegando el acceso y falla el inicio de sesión.
- Si un usuario intenta iniciar una sesión en un dominio y falla, la computadora cliente (se supone que es una Windows NT Workstation) comprobará en su propia base de datos de cuentas el nombre de usuario y la contraseña escritos. Si estas credenciales no son válidas en el sistema local, el cliente entra como invitado local si la cuenta *invitados* está activada en la computadora local

Una vez que el servicio Netlogon ha localizado a la computadora que va a identificar, primero se necesita asegurar que la computadora es un sistema válido para el dominio. Los servicios Netlogon localizados en cada sistema inician un proceso de verificación desafío/respuesta. Cuando la identificación ha tenido éxito, un canal seguro se establece entre las computadoras. Luego, una sesión de comunicación tiene lugar entre las dos computadoras para que el usuario acceda. El canal se mantiene abierto para que llamadas subsecuentes en la red puedan pasarse entre los sistemas.

---

[15] SID (Identificador de Seguridad). Ver el glosario

[16] Consultar el glosario para obtener información de los términos mostrados en estos pasos

4.5 PLANES DE SEGURIDAD

Una parte del control de la seguridad en un dominio es establecer políticas de seguridad. Se inicia el *administrador de usuarios para dominios* y se elige *cuentas* en el menú de *políticas*. Aparece el cuadro de diálogo de la Figura 3.2 (capítulo 3), en el cual se pueden configurar políticas que afecten a todas las cuentas del dominio. Se pueden establecer políticas y propiedades individuales para los usuarios, accediendo a las propias cuentas. Estas propiedades de cuentas de usuarios individuales incluyen perfiles especiales, horas de inicio de sesión, estaciones de trabajo para inicios de sesión, finalizaciones de cuentas y otras.

4.5.1 Restricciones de contraseñas

En la sección de restricciones de contraseñas, en el cuadro de diálogo de *políticas de cuentas*, es donde se establecen las políticas que controlan cómo se tratan las contraseñas en el dominio. Las configuraciones que se hacen aquí son críticas para proteger contraseñas y el sistema de seguridad de contraseñas.

Las políticas de contraseñas protegen la red de ataques de piratas informáticos, y definen las responsabilidades de los usuarios que tienen acceso al sistema de información de la organización

- Duración máxima de la contraseña

Es el periodo de tiempo que se permite a un usuario usar una contraseña antes de que Windows NT le pida cambiarla Se puede configurar este valor para que nunca acabe, o se puede controlar el tiempo de expiración entre I y 999 días.

- Duración mínima de la contraseña

Permite que un usuario pueda cambiar su contraseña en un determinado número de días. Por defecto, éstos pueden cambiar las contraseñas cuando quieran, pero con ésta opción, se puede configurar un valor entre I y 999 días para evitar que cambien su contraseña en ese periodo.

- Longitud mínima de la contraseña

Está opción permite configurar la contraseña del usuario entre 1 y 14 caracteres.

❑ Historia de contraseña

Esta opción puede evitar que los usuarios puedan hacer pequeñas variaciones en sus contraseñas preferidas y reduzca la posibilidad de que sean violadas. Si se activa esta opción a *no guardar historia de contraseñas*, ellos pueden repetir una contraseña que hayan utilizado Configurando la opción *recordar* a un valor entre 1 y 24, se puede evitar que los usuarios repitan las últimas 24 contraseñas que hayan utilizado.

4.5.2 Bloqueo de cuentas

La propiedad de bloqueo de cuentas es la clave para evitar ataques repetidos sobre las contraseñas; ya que después de varios intentos fallidos de tratar de adivinar una contraseña, se bloqueará la máquina y el único que puede desbloquearla es un administrador.

Nota: La cuenta del administrador no se puede bloquear. Esto evita un bloqueo total del sistema, en el caso de que el administrador olvide su contraseña o situación similar.

Si una cuenta llegase a bloquearse por un ataque de un asaltante o por otras razones, el administrador puede reconfigurarlo, abriendo el *administrador de usuarios para dominios* y abriendo el cuadro de *propiedades de la cuenta bloqueada* (pulsando dos veces sobre el nombre de la cuenta). La opción *cuenta bloqueada* estará activada Desactivar esta opción permite el acceso a la cuenta bloqueada.

Cuando se activa la opción *cuenta bloqueada*, se pueden configurar las opciones siguientes.

❑ Bloquear después de x inicios de sesión incorrectos

El valor de x determina cuántas veces un usuario puede intentar iniciar una sesión en una cuenta, antes de que ésta sea bloqueada El elemento temporal de este valor se configura con la opción *restablecer la cuenta*, después de x minutos. Un valor realista sería 2 intentos o más, para permitir la identificación de los usuarios que se hubiesen equivocado escribiendo por error su contraseña El rango para esta opción es de 1 a 999 intentos de inicio de sesión.

❑ Restablecer cuenta despues de x minutos

Sirve para determinar el número de minutos que se desea que transcurran entre cada intento de inicio de sesión fallidos (antes de que la máquina quede bloqueada); el rango es de l a 99999 minutos

❑ Duración del bloqueo

Tiene dos opciones, que el bloqueo de una cuenta dure hasta que el administrador la desbloquee; o que automáticamente se restablesca después de un determinado número de minutos (1 a 99999).

❑ Desconectar del servidor a los usuarios remotos cuando termine la hora de inicio de sesión

Cuando esta opción se activa, los usuarios se desconectan del servidor donde sus horas de trabajo han expirado Las horas de sesión pueden configurarse para cada usuario individual utilizando el *administrador de usuarios de dominios*. En entornos seguros, se podría habilitar esta opción para apagar las cuentas que hayan sido dejadas abiertas por accidente por usuarios, para que otros empleados no puedan acceder a la cuenta

4.5.3 Administración de la seguridad para grupos y usuarios

Al hablar de bases de datos de cuentas de usuarios, es importante considerar lo siguiente:[17]

- Un Windows NT Server trabajando como controlador de dominio, mantiene la base de datos de las cuentas de usuarios del dominio.
- Un servidor miembro es un Windows NT Server que no es un controlador de dominio. Puede mantener su propia base de datos de cuentas de usuarios y dar acceso a usuarios de la red también. No almacena la base de datos de cuentas de usuarios del dominio y consecuentemente no puede iniciar a usuarios en él
- Una Windows NT Workstation mantiene su propia base de datos de cuentas de usuarios y puede proporcionar el acceso a usuarios de la red. También puede participar en un dominio.
- Los grupos y las cuentas locales de estaciones de trabajo están localizadas en la base de datos de usuarios en Windows NT Workstation o en servidores miembros. Iniciar una sesión en una de estas cuentas permite el acceso a recursos en la computadora local, no en otras
- Los grupos y las cuentas locales de dominios están definidas en controladores de dominio primarios, y están duplicadas en los controladores de copias de seguridad del dominio El grupo puede ser usado sólo en el dominio
- Los grupos globales son colecciones de cuentas de usuarios y grupos que pueden ser hechos miembros de otros grupos.

---

[17] Las referencias que aquí se hacen son para Windows NT Server y Windows NT Workstation, debido a que estas computadoras mantienen sus propias bases de datos de cuentas de usuarios. Windows 95 y otras versiones de Windows no mantienen sus propias bases de datos pero pueden participar en grupos de trabajo o dominios Windows NT

4.6 EL ADMINISTRADOR DE USUARIOS

Se utiliza el *administrador de usuarios*, como se muestra en la Figura 4.2, para crear y administrar cuentas de usuarios, configurar derechos de usuarios, establecer planes de cuentas para el dominio, activar relaciones de confianza y establecer planes de auditoria. Si se está trabajando con una Windows NT Workstation, la utilidad simplemente se llama *administrador de usuarios*, y lo utiliza para administrar cuentas locales en la estación de trabajo. Si está trabajando con un controlador de dominio Windows NT Server, la herramienta se llama *el administrador de usuarios para dominios* y lo utiliza para administrar cuentas para el dominio entero, o para permitir el acceso a cuentas en otros dominios de confianza.

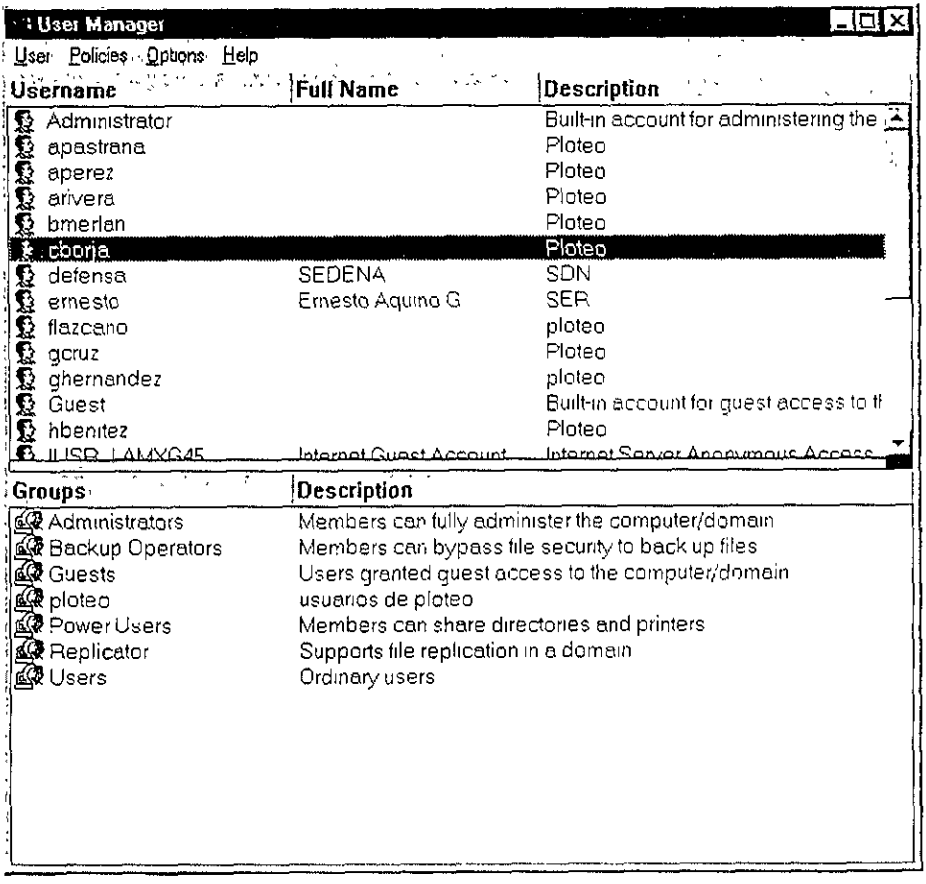


FIGURA 4.2 Administrador de Usuarios.

Las cuentas de usuarios individuales se muestran en la ventana superior, y los grupos en la inferior. Por razones de seguridad, los propietarios de las cuentas administrativas también tienen sus propias cuentas personales para usar cuando acceden a la red para tareas no administrativas. Estas cuentas tienen menos derechos y privilegios para protegerlas de invasiones.

Para configurar derechos de usuarios se elige *derechos de usuarios* del menú *políticas*. Aparece un cuadro de diálogo como el de la figura 4.3.

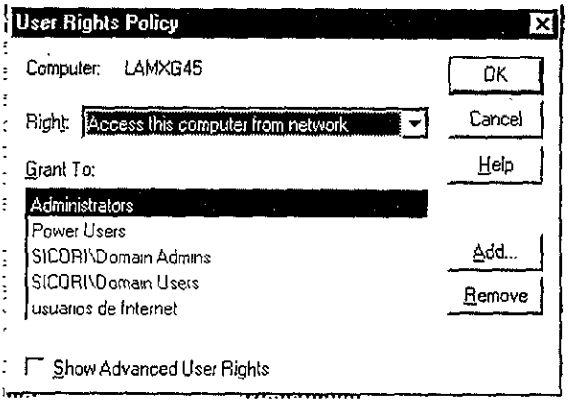


FIGURA 4.3 Políticas de Derechos de Usuarios.

Un derecho es una autorización para realizar alguna acción en el sistema. Estas acciones están con frecuencia relacionadas con tareas que los administradores del sistema tienen que hacer, pero hay algunos derechos básicos que todos los usuarios necesitan para acceder al sistema. Los derechos se aplican a un dominio, mientras que los permisos determinan cómo los usuarios individuales o los grupos pueden acceder a objetos específicos como archivos y directorios.

4.6.1 Cuentas de Usuarios

Para crear una cuenta, se elige *usuario nuevo* del menú *Usuario* que se encuentra *Administrador de usuarios*, aparece un cuadro de diálogo como el de la figura 4.4, en este se asignan las propiedades de la cuenta, luego se pulsa el botón *agregar* para crear otra cuenta o *cancelar* para no añadir más. Para cambiar las propiedades de una cuenta existente, se pulsa dos veces ésta en la lista Un cuadro de diálogo con los mismos campos aparecerá.

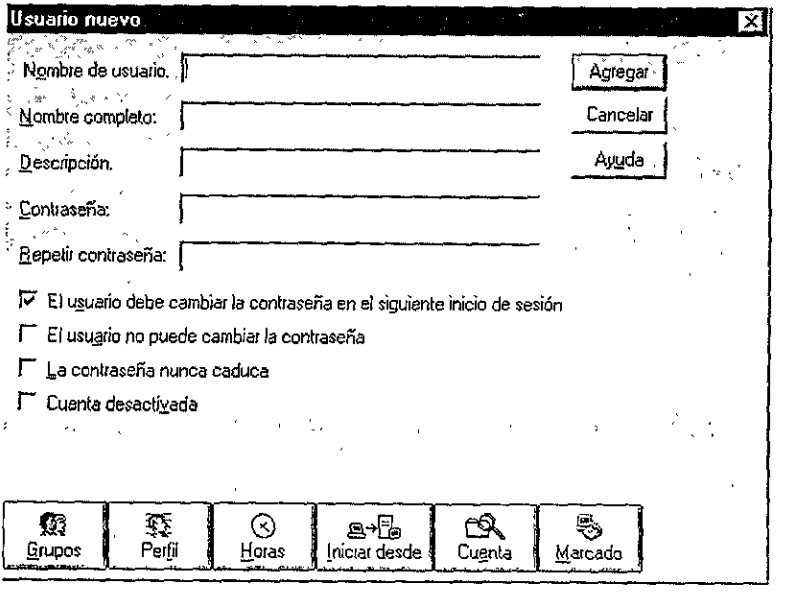


Figura 4.4 Propiedades de las cuentas de usuarios.

A continuación se describen cada uno de los botones de la figura 4.4, los cuales describen las propiedades de las cuentas de los usuarios:

- Perfil

Aparece el cuadro de diálogo *Perfil del entorno del usuario* de la figura 4.5 se puede especificar un archivo de órdenes de inicio de sesión y un directorio raíz para el usuario, así como un perfil que incluya las configuraciones del entorno del usuario. Los perfiles permiten a los usuarios, iniciar una sesión en un entorno familiar desde otras computadoras en el dominio. Un directorio raíz del usuario, es donde se almacenan archivos personales y programas

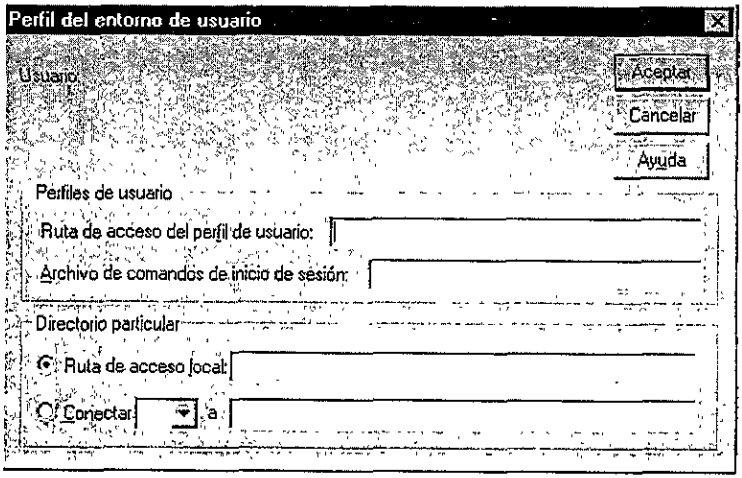


Figura 4.5 Perfil del entorno de usuario.

❑ Horas

El cuadro de diálogo *Horas de inicio de sesión* de la figura 4.6, sirve para restringir las horas de inicio de sesión, en que el usuario puede acceder al dominio y conectarse al controlador del dominio. *Horas* es una opción importante de la seguridad, porque se puede evitar que los usuarios inicien una sesión en el sistema fuera de horas permitidas, cuando sus actividades son probablemente menos vigiladas. Esta opción puede evitar también, que los piratas informáticos puedan violar una cuenta, después de que los usuarios hayan salido

Para cambiar las horas se pulsa y desplaza el marcador sobre un conjunto específico de horas, luego se pulsa *Permitir* o *Denegar.* Si un usuario no tiene privilegios para un periodo de tiempo particular, las barras negras de marca no aparecen en ese periodo.

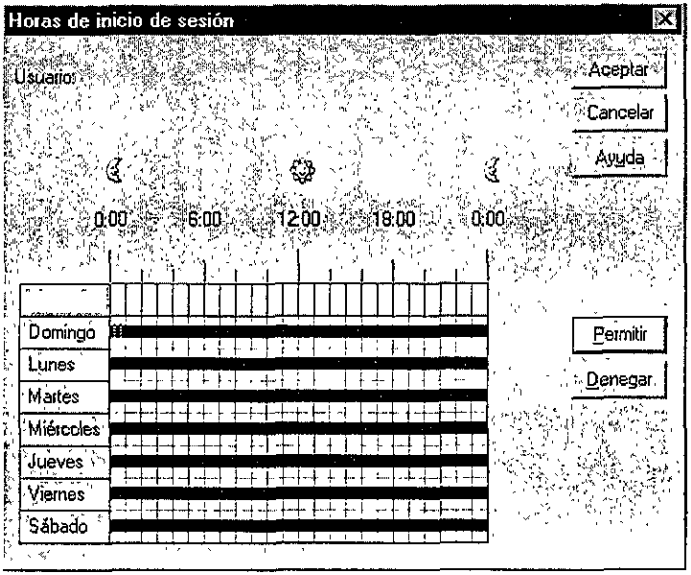


Figura 4.6 Horas de inicio de sesión

❑ Iniciar desde (acceder a)

La figura 4 7 muestra la pantalla en la que se especifican los nombres de las computadoras a las que el usuario puede acceder

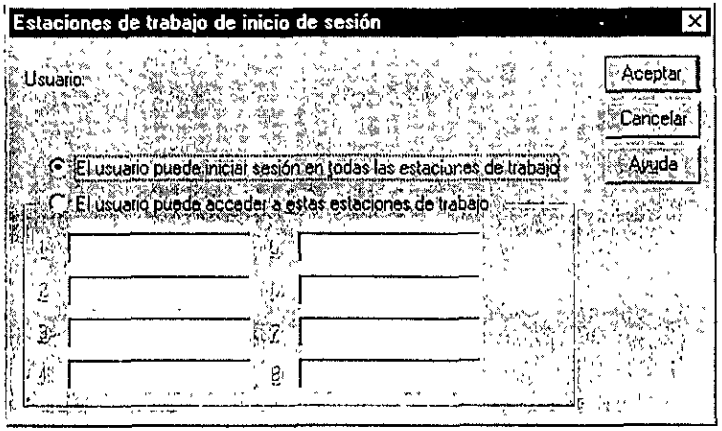


Figura 4.7 Iniciar desde

❑ Cuenta

El cuadro de diálogo de *Información de la cuenta* (figura 4.8), permite especificar cuándo una cuenta estará inactiva, si se trata de una cuenta para un usuario temporal, lo que es una opción de seguridad crítica si se tienen consultores o trabajadores a tiempo parcial en los sistemas Las cuentas ya finalizadas no se borran, por lo que se pueden reutilizar si vuelve un usuario temporal. Si un usuario está dentro de una sesión, la cuenta finaliza cuando salga de ella. Hay diferentes tipos de cuenta en el campo *Tipo de cuenta*, que se describen a continuación:

- **Cuentas globales**. Están disponibles en todo el dominio y a través de relaciones de confianza.
- **Cuentas locales**. Permite a los usuarios de dominios peligrosos, que accedan a recursos locales, pero no permite acceso a dominios de Windows NT Server.

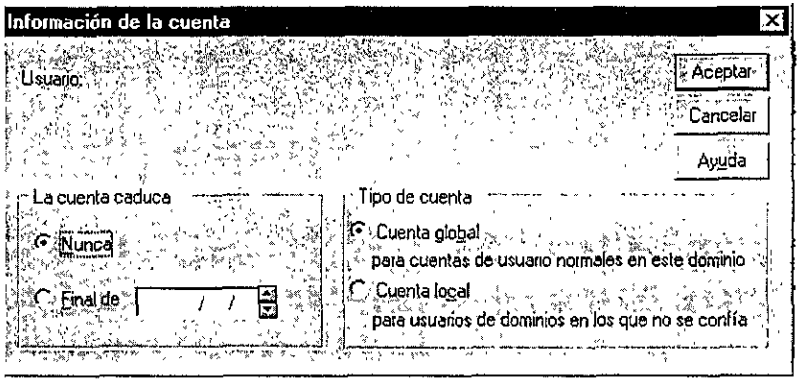


Figura 4.8 Cuadro de diálogo de Información de la cuenta de usuario.

❑ Marcado

La opción de *Marcado* (figura 4 9), se utiliza para garantizar permisos para realizar llamadas telefónicas y poder conectarse a la red. Esta opción está disponible sólo si los componentes de *Servicio de acceso remoto* están instalados.

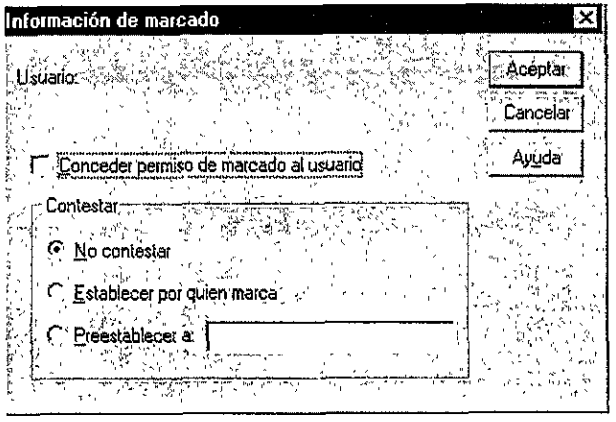


Figura 4.9 Opción Dialup (marcado)

4.6.2 Administración de entornos de usuario

Se pueden administrar el entorno de usuario y establecer una serie de propiedades de seguridad utilizando perfiles y políticas Los perfiles de usuario son importantes cuando más de una persona utiliza la misma computadora o cuando un usuario se mueve de una computadora a otra en distintas localizaciones. Los perfiles contienen ajustes definibles por el usuario para el entorno de trabajo de las computadoras Windows NT, como

- La disposición del escritorio que el usuario dejó la última vez que accedió.
- Un escritorio personalizado que sea diferente del de otra persona que utilice la misma computadora.
- Perfiles personales que vayan con el usuario a otras computadoras. Estos son los perfiles móviles

Una importante característica de seguridad es que se pueden hacer obligatorios para evitar que los usuarios los cambien Las configuraciones del perfil se almacenan en archivos del sistema Las configuraciones incluyen el esquema del escritorio y las características del escritorio que pueden modificar o no los usuarios. Por ejemplo, se puede restringir el acceso a las opciones del *Panel de control*.

4.7 PROPIEDADES DE LOS GRUPOS EN EL DOMINIO

Desde el punto de vista de la administración, es mucho más fácil administrar los derechos y los permisos de grupos que de usuarios individuales. Es fácil añadir usuarios a grupos y luego borrarlos cuando se quiera revocar sus derechos en ese grupo. Desde el punto de vista de la seguridad, no es bueno asignar derechos y permisos a cuentas de usuarios individuales ya que es demasiado difícil rastrearlos a todos. Por ejemplo, se puede observar a los grupos que tienen permisos en un directorio[18] mirando en el cuadro de diálogo *Permisos de Directorio*, como se muestra en la figura 4.10.

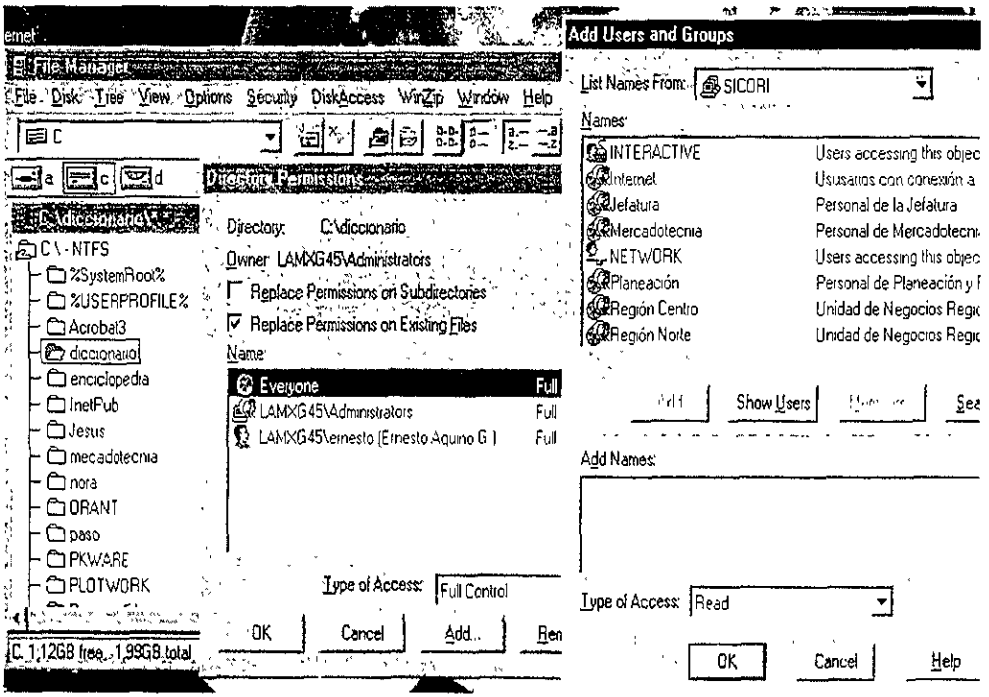


Figura 4.10 Permisos de Directorio.

Para averiguar qué cuentas de usuarios son miembros de un grupo particular, en el *Administrador de usuarios* se pulsa dos veces sobre el grupo. Aparece un cuadro de diálogo, como el de la figura 4 11, que describe el grupo y lista sus miembros actuales

[18] Esto se hace desde el *Administrador de Archivos* usando NTFS (System File NT - Sistema de Archivos de NT)

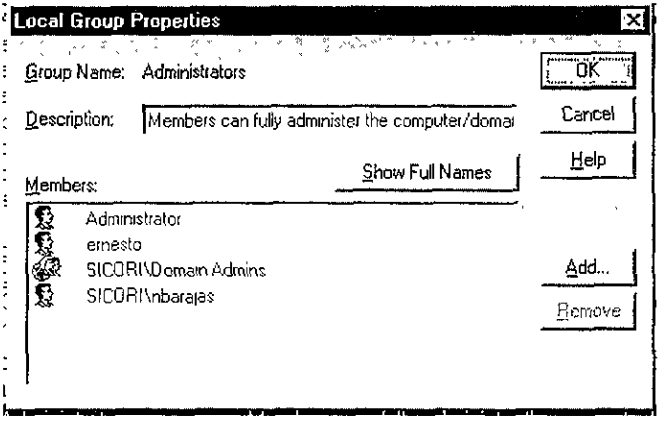


Figura 4.11 Propiedades de un grupo.

Se puede pulsar el botón *Agregar* para añadir un nuevo miembro, o seleccionar cualquier miembro y apretar el botón *Quitar.*

Para crear nuevos grupos, se elige *Nuevo* Grupo global o *Nuevo* grupo local del menú *Usuarios* en el *Administrador de usuarios.*

4.7.1 Grupos Locales y Globales en el Dominio

Hay dos tipos de grupos en el entorno Windows NT: grupos locales y grupos globales. Los grupos locales de dominio tienen derechos y permisos en un dominio único. Los servidores miembros (Windows NT Server que no son controladores de dominio) y Windows NT Workstation tienen sus propios grupos locales que tienen derechos y permisos sólo en esas computadoras.

Los grupos globales son importantes en entornos multidominio (varios dominios). Se usan para crear una estructura jerárquica de administración o para dar acceso a los recursos a usuarios regulares en otros dominios Son especialmente útiles cuando la base de datos de cuentas de usuarios está centralizada en el dominio maestro

Puede resultar algo confuso si un usuario tiene una cuenta en una base de datos de cuentas de usuarios local y en la de un dominio, cada una con una contraseña distinta La cuenta local puede usarse para acceder a recursos de la máquina local, pero si se intenta utilizar los recursos del dominio, se pedirá la contraseña de usuario o se impedirá el acceso. En este último caso, algunas aplicaciones pueden negar el acceso en vez de pedir la contraseña. La solución

sería asegurarse de que los usuarios tienen una contraseña que puedan utilizar en toda la red.

Se puede añadir un grupo global (y a sus miembros) a un grupo local para dar al primero los derechos y permisos del segundo. Cuando se habla de grupos locales se debe tener en cuenta lo siguiente

- Los grupos locales en los controladores de dominio tienen derechos sólo en el dominio donde se han creado.
- Los grupos locales en Windows NT Workstation y servidores miembros tienen derechos en la computadora donde se han creado.
- Los grupos en Windows NT Workstation y servidores miembros no son parte de la seguridad aplicable en los grupos de dominio.
- Un grupo local no puede contener otros grupos locales del mismo dominio. Sólo puede contener cuentas de usuarios o grupos globales del mismo u otros dominios.

Por razones de seguridad, los miembros de grupos globales deben ser revisados regularmente. Como los grupos globales pueden añadirse a grupos locales y además obtienen sus derechos y permisos, algunos miembros de estos grupos podrían conseguir permisos de acceso inapropiados. En la figura 4 12 se muestra la pantalla de configuración de grupos de dominio para un usuario; la cual se localiza en el *administrador de usuarios para dominios*, en la pantalla de propiedades de cada usuario

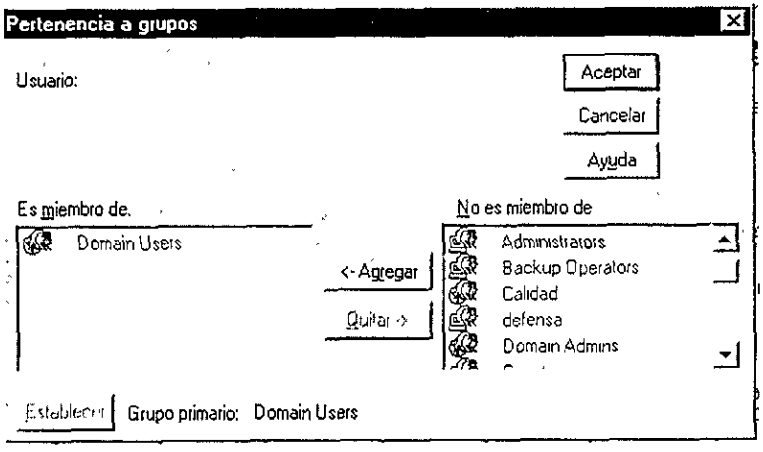


Figura 4.12 Configuración de Grupos para un usuario.

4.7.1.1 Grupos locales

Los controladores de dominio Windows NT tienen los siguientes grupos locales:

- **Grupo Administradores**. Sus miembros pueden administrar el dominio entero.
- **Grupo Operadores de copia de seguridad**. Sus miembros pueden realizar copias de seguridad y restauración.
- **Grupo Invitados**. Sus miembros pueden acceder al servidor desde la red pero no pueden iniciar sesiones localmente en éste.
- **Grupo Operadores de impresión** Sus miembros pueden administrar las impresoras.
- **Grupo Duplicadores**. Sus miembros pueden administrar la duplicación de servicios.
- **Grupos Operadores de servidor** Sus miembros pueden administrar servidores.
- **Grupo Usuarios** Sus miembros pueden acceder al servidor desde la red, pero no pueden iniciar sesiones localmente en éste

Las Windows NT Workstation y los servidores miembros (Windows NT Server que no sean Controladores de dominio) tienen los siguientes grupos.

- **Grupo Administradores**. Sus miembros pueden administrar el sistema local.
- **Grupo Operadores de copia de seguridad**. Sus miembros pueden realizar copias de seguridad y restauración en el sistema local
- **Grupo Invitados** Sus miembros pueden acceder al sistema local.
- **Grupo Usuarios Avanzados**. Sus miembros pueden administrar las cuentas de usuarios en el sistema local.
- **Grupo Duplicadores** Sus miembros pueden administrar la duplicación de servicios.
- **Grupo Usuarios**. Sus miembros pueden acceder a la estación de trabajo local y usarla para acceder a la red, también pueden apagar el sistema

❑ Grupo Administradores

El grupo *Administradores*, que existe en todas las computadoras Windows NT, tiene control total de la computadora. Ningún otro grupo tiene tales capacidades. La cuenta del usuario *Administrador* tiene estos derechos por ser miembro de este grupo y no puede ser quitada de aquí (lo que evita riesgos de accidentes). En el entorno de dominios, los administradores administran la configuración del dominio entero.

Aunque los administradores tienen acceso total al sistema, sólo tienen acceso a cada archivo del servidor al principio. A medida que los usuarios comienzan a crear archivos, ellos empiezan a ser poseedores de esos archivos. La propiedad de los objetos permite al propietario configurar todos los permisos y

tener acceso completo del objeto. Un usuario que cree un archivo o directorio lo posee. Por contra, si un miembro del grupo *Administradores* crea un archivo o directorio, todos los miembros del grupo *Administradores* lo poseen, y el resto de los usuarios no.

❑ Grupo Operadores de copias de seguridad

Los miembros de este grupo tienen la habilidad de hacer copias de seguridad y restaurar archivos en cualquier directorio del sistema, incluso, si no tienen permiso para acceder a archivos Los usuarios que tienen derechos de Copia de seguridad y de Restauración pueden leer, cambiar y escribir cualquier archivo. Los permisos de este grupo sobreescriben otros permisos. Normalmente, un usuario que crea un directorio o un archivo es el propietario de esa entidad y puede configurar permisos, pero el grupo *Operadores de copias de seguridad* puede saltárselos para hacer copias de seguridad del servidor en cinta u otro medio.

Obviamente, la pertenencia a este grupo debe ser fuertemente controlada. Un usuario sin escrúpulos podria robar información del servidor o un espía industrial podría convencer al operador de copias de seguridad de robar archivos o permitirle el acceso a la cuenta. Un pirata informático que viole esa cuenta, puede aprovecharse de los derechos para robar información valiosa, incluyendo archivos que contengan contraseñas e información de cuentas de usuarios.

❑ Grupo Operadores de cuentas

Miembros del grupo *Operadores de cuentas*, pueden usar la utilidad *Administrador de usuarios* para crear cuentas de usuarios y grupos Sin embargo, sólo pueden cambiar y borrar las cuentas y grupos que creen. Los operadores de cuentas también pueden iniciar una sesión en servidores, apagarlos y añadir computadoras al dominio. Este grupo tiene bastante poder para crear una amenaza de seguridad seria; sus miembros deben ser controlados. Una persona no autorizada que obtenga el estado *Operador de cuentas* puede crear y cambiar cuentas de usuarios

Los operadores de cuentas no pueden modificar el grupo global *Administradores del dominio*, *el grupo de Administradores*, el de *Operadores de cuentas*, el de *Operadores de copias de seguridad*, el grupo de *Operadores de impresión* o el grupo de *Operadores de servidores*.

❑ Grupo Invitados

El grupo *Invitados* es muy parecido a la cuenta de *Invitados* con respecto a sus derechos y permisos de acceso al sistema. Ya que una Windows NT Workstation podria estar instalado en un entorno donde muchas personas podrian acceder al teclado, la cuenta de *Invitados* tiene el derecho de iniciar una sesión local Los servidores miembros se han configurado del mismo modo, lo que podria

causar un problema de seguridad si se almacena información sensible en el servidor. Los controladores de dominios no permiten que la cuenta *Invitados* acceda localmente, pero permite que los invitados accedan por la red, si la cuenta está activada

❑ Grupo Usuarios avanzados

Este grupo existe en estaciones de trabajo Windows NT o en servidores miembros Los miembros del grupo tienen un conjunto de derechos extendidos y privilegios que podrían ser considerados subordinados a los derechos del Administrador. Pueden realizar tareas de administración del sistema como

- Compartición de directorios por la red
- Instalación de impresoras y compartirlas por la red.
- Creación, modificación y borrado de cuentas de usuarios (pero no de cuentas administrativas).
- Adición de cuentas de usuarios a los grupos de *Usuarios avanzados, Usuarios* e *Invitados.*
- Realización de otras tareas como configuración del reloj del sistema y del monitor del sistema

El procedimiento típico de administración para tratar cuentas de usuarios en estaciones de trabajos Windows NT que participan en dominios, es añadir la cuenta de dominio del usuario al grupo de *Usuarios avanzados.* Luego, los usuarios tienen los derechos normales en el dominio y los derechos del grupo *Usuarios avanzados* en su estación de trabajo. Usando esta técnica, los administradores de dominio pueden decidir qué usuarios deberían tener el estado Usuarios avanzados en una estación particular.

❑ Grupo Operadores de impresión

Los miembros de este grupo pueden administrar impresoras. Tienen la posibilidad de crear, cambiar, borrar, y compartir las impresoras en el dominio. Los *operadores de impresión* también pueden acceder a servidores y apagarlos.

❑ Grupo Duplicadores

Los Windows NT Server pueden duplicar (copiar) información entre sí. Los contenidos de un directorio pueden ser copiados automáticamente a un directorio parecido en otro servidor para que esta información sea guardada como medida de seguridad y actualizada en tiempo real Este grupo debe incluir cuentas de usuarios de dominio que tengan permiso para iniciar sesiones en los servicios de duplicación en el controlador primario de dominio y en los controladores de copias de seguridad del dominio.

❑ Grupo Operadores de servidores

Los miembros de este grupo pueden crear, cambiar y borrar impresoras, directorios y archivos compartidos. También pueden hacer copias de seguridad y restaurar archivos, dar formato a discos duros, cambiar la hora del sistema, bloquear la computadora y apagar el sistema. El Operador de servidores no puede desbloquear una estación de trabajo que haya sido bloqueada por otro usuario Sólo el Administrador o el usuario que la ha bloqueado pueden hacerlo

Para crear subadministradores en servidores de dominios, se añaden usuarios al grupo *Operadores de servidores*. Como miembros del grupo pueden apagar servidores, compartir o no directorios, hacer copias de seguridad y restaurar archivos. Sin embargo, no pueden cambiar atributos del usuario, añadir controladores o hacerse dueños de archivos.

❑ Grupo Usuarios

Los miembros del grupo *Usuarios* (no confundirlos con los usuarios de dominios) no tienen derechos de acceso locales o de red en servidores, pero pueden acceder localmente a Windows NT Workstation. Los derechos en estaciones de trabajo incluyen la posibilidad de acceso local, apagar el sistema, crear grupos locales y administrar los grupos que creen. Los usuarios de la red pueden iniciar sesiones en servidores siendo miembros del grupo *Todos*, no por ser miembros del grupo *Usuarios*. Todo el mundo tiene el derecho de acceder a esta computadora de la red por default en los servidores. Si se ha borrado a *Todos* de este derecho, se necesita asignar a un nuevo grupo de usuarios de la red este derecho.

❑ Otros grupos

Los grupos siguientes no tienen miembros en el mismo sentido que los grupos hasta ahora discutidos En su lugar, cualquier cuenta que use la computadora de una manera especifica será automáticamente miembro del grupo Estos grupos reflejan el acceso a recursos, pero no se refieren al nivel de privilegios del usuario.

- **Usuarios interactivos** Cualquier usuario que inicie una sesión en la computadora con un acceso interactivo.
- **Usuarios de la red** Cualquier usuario que se conecta a la computadora por la red.
- **Todos** Cualquier usuario que acceda a la computadora, incluyendo a los interactivos y de la red.
- **Creador/Propietario**. Cualquier usuario que cree o se adueñe de un recurso.

❑ El grupo Todos

Este grupo incluye a todo el mundo que acceda a una computadora incluyendo a usuarios locales y de la red. Los administradores deben prestar especial atención a éste;ya que por omisión, tiene permisos que pueden no ser adecuados en entornos seguros. En particular, los usuarios *Invitados* tienen acceso a todos los directorios disponibles para *Todos.*

El grupo *Todos* tiene los permisos siguientes, que pueden ser considerados un riesgo de seguridad·

- Control total cuando se crea o comparte una carpeta, aunque esto se cambia fácilmente
- Cambiar permisos en los directorios *Raíz* de todas las unidades NTFS (Lectura, Escritura, Ejecución y Borrado)
- Cambiar permisos en el directorio System32.
- Cambiar permisos en el directorio Win32App

4.7.1 2 Los Grupos globales

Cuando se añade una computadora Windows NT a un dominio, se crean automáticamente una serie de grupos a los grupos locales de estas computadoras. Estos grupos globales se describen en las siguientes secciones.

❑ Administradores del dominio

- Cuando se instala Windows NT, la cuenta *Administrador* se crea y se hace miembro del grupo local *Administradores* Esto da control total sobre el sistema local. La cuenta de *Administrador* no puede ser borrada de este grupo
- Cuando se designa una computadora Windows NT como controlador primario de dominio, la cuenta del *Administrador* se añade al grupo global *Administradores del dominio.*
- El grupo global *Administradores del dominio,* se añade automáticamente al grupo local de *Administradores* en cada computadora Windows NT del dominio.

Consecuentemente, cualquiera que acceda a la cuenta Administrador tiene derechos administrativos en el dominio local. Si se quiere dar a otro usuario administrativo derechos en el dominio, sólo se debe añadir su cuenta de usuario al grupo global *Administradores del dominio.* También se puede poner el grupo *Administradores del dominio* en el grupo local de *Administradores* en sistemas de otros dominios para permitir a los miembros del grupo los derechos administrativos de esos dominios; sin embargo, se necesita una relación de confianza entre esos dominios. Para permitir a un usuario derechos administrativos en una computadora

Windows NT que no sea controlador de dominio, se añade al grupo local *Administradores.*

❑ Usuarios del dominio

La cuenta *Administrador* y todas las cuentas de nuevos usuarios se añaden automáticamente al grupo global *Usuarios del dominio.* En Windows NT Workstation, este grupo tene el derecho de iniciar sesiones localmente, apagar el equipo, crear y administrar grupos locales

❑ Invitados de dominio

El grupo global *Invitados de dominio* inicialmente contiene la cuenta de usuario *Invitado del dominio.*

4.7.2 Creación de Grupos

Se pueden crear grupos locales y globales eligiendo *Grupo local nuevo* o *Grupo global nuevo* del menú *Usuario* del *Administrador de usuarios.* Cuando se configuran cuentas y grupos, se deben identificar todos los requisitos que los usuarios necesiten tener en el sistema y crear las cuentas de acuerdo a eso El procedimiento general de creación de grupo es

- El grupo global *Administradores del dominio* se añade automáticamente al grupo local de *Administradores* en cada computadora Windows NT del dominio.
- Crear grupos locales con accesos a objetos del dominio, como directorios de programas o dispositivos (impresoras, etc.)
- Otorgar los derechos del grupo.
- Crear uno o más grupos globales que deban tener acceso a los objetos.
- Añadir usuarios a los grupos globales.
- Añadir los grupos globales a los grupos locales de cualquiera de los dominios o computadoras, donde los usuarios del grupo global deban tener acceso a los recursos.

Si no se desea que un usuario continúe teniendo acceso a un recurso, se borra su cuenta del grupo global Si no se quiere que todos los miembros de un grupo global tengan acceso a los recursos asignados a un grupo local, se borra el grupo global del local.

Cuando se crea un grupo, se puede copiar un grupo existente y cambiar sus propiedades, o se puede crear un nuevo grupo por completo desde el principio Copiar un grupo asegura que el nuevo grupo tendrá todos los derechos y permisos que había asignado al existente Luego, se puede mejorar o restringir esos derechos y permisos del nuevo grupo

Cuando se diseña y crea una jerarquía de grupos, se debe pensar en los grupos globales en términos de departamentos, grupos de trabajo y/o divisiones de la compañía. Esto ayudará a crear grupos inteligibles que se correspondan adecuadamente con los recursos de la red

4.7.3 Derechos de los Grupos

Los derechos están relacionados directamente con los grupos. Dan a los miembros de éstos, el permiso que necesitan para realizar tareas administrativas o de simple acceso a un sistema

Para cambiar o permitir derechos de un grupo existente, se elige *Derechos de usuarios* del menú *Políticas* del *Administrador de usuarios*. Aparece el cuadro de diálogo de *Políticas de derechos de usuarios* (figura 4.3); se elige un derecho del campo *Derecho*, luego se añade o se borra un grupo del campo *Conceder a*.

La Tabla 4.2 describe los derechos de usuario estándar de Windows NT. La Tabla 4.3 describe cómo estos derechos se implementan en un Windows NT Server y en una Windows NT Workstation.

Tabla 4.2 Derechos predefinidos para Windows NT.[19]

DERECHOS	DESCRIPCION
Acceso a esta computadora desde la red.	Permite a los usuarios acceder a la computadora desde otra cuenta de la red.
Añadir Windows NT y servidores miembros al dominio	Permite al usuario que no sea miembro del grupo de Administradores de un dominio, añadir Windows NT Workstation y servidores miembros al dominio.
Copia de seguridad de archivos y directorios.	Permite a los usuarios administrar copias de seguridad de datos.
Cambio de la hora del sistema.	Permite a los usuarios cambiar la hora del sistema.
Forzar el apagado desde un sistema remoto.	Permite a los usuarios apagar un equipo remoto.
Instalación y desinstalación de controladores de dispositivos.	Permite a los usuarios administrar los controladores de dispositivos del sistema.
Inicio de sesión localmente.	Permite a los usuarios iniciar sesiones localmente, como contraposición al inicio de sesión en la red
Administración de auditorías y registro de seguridad.	Permite a los usuarios administrar el sistema de auditorías y los registros.
Restauración de archivos y directorios.	Permite a los usuarios administrar la restauración de datos.
Apagado del sistema	Permite a los usuarios parar el sistema operativo.
Apropiación de archivos y otros objetos.	Permite a los usuarios cambiar el nombre del usuario que crea o posee directorios o archivos y poner el suyo propio.

[19] SHELDON Tom *Manual de Seguridad de Windows NT* McGRAW-HILL pág 181

También hay derechos llamados *posibilidades predefinidas* que pasan a ciertos grupos sus derechos especiales para administrar el sistema Estas posibilidades se definen en la Tabla 4 4

Los derechos y las posibilidades son ligeramente diferentes en estaciones de trabajo Windows NT Los derechos se aplican a todo el sistema, o bien dominio o bien computadora local. Los permisos, por otra parte, se aplican a objetos específicos. Los derechos con frecuencia se imponen a los permisos de los objetos. Esto es cierto en el caso del *Operador de copia de seguridad*, que tiene el derecho de hacer copias de seguridad incluso de archivos a los que el propietario haya negado el acceso a todos los usuarios.

Tabla 4.3. Derechos por default en Windows NT 4 0.[20]

DERECHOS	GRUPOS CON ESTE DERECHO, EN WINDOWS NT SERVER	GRUPOS CON ESTE DERECHO, EN WINDOWS NT WORKSTATION
Acceso a esta computadora desde la red.	Administradores, Todos.	Administradores, Usuarios avanzados.
Copia de seguridad de archivos y directorios.	Administradores, Operadores de copias de seguridad, Operadores de servidores.	Administradores, Operadores de copias de seguridad.
Cambio de la hora del sistema.	Administradores, Operadores de servidores.	Administradores, Usuarios avanzados.
Forzar el apagado desde un sistema remoto.	Administradores, Usuarios avanzados desde estaciones de trabajo Windows NT, Operadores de servidores.	Administradores, Usuarios avanzados.
Instalación y desinstalación de controladores de dispositivos.	Administradores.	Administradores.

[20] SHELDON, Tom *Manual de Seguridad de Windows NT* McGRAW HILL Pag 183

Inicio de sesión localmente.	Administradores, Operadores de servidores, Operadores de copias de seguridad, Operadores de cuentas, Operadores de Impresión, cuenta Invitados de Internet.	Administradores, Usuarios avanzados, Usuarios, Invitados, Todos y Operadores de copias de seguridad.
Administración de auditorías y registro de seguridad.	Administradores.	Administradores.
Restauración de archivos y directorio.	Administradores, Operadores de servidores, Operadores de copias de seguridad, Operadores de cuentas, Operadores de Impresión.	Usuarios avanzados, Usuarios, Todos y Operadores de copias de seguridad.
Apagado del sistema.	Administradores, Operadores de servidores, Operadores de copias de seguridad, Operadores de cuentas, Operadores de Impresión.	Usuarios avanzados, Usuarios, Todos y Operadores de copias de seguridad.
Apropiación de archivos y otros objetos.	Administradores	Administradores.

Tabla 4.4. Posibilidades predefinidas para el Windows NT[21].

POSIBILIDADES PREDEFINIDAS	GRUPOS CON ESTE DERECHO EN WINDOWS NT SERVER	GRUPOS CON ESTE DERECHO EN WINDOWS NT WORKSTATION
Añadir Workstation al dominio.	Operadores de cuenta.	
Creación y administración de cuentas de usuarios.	Administradores, Operadores de cuentas.	Administradores, Usuarios avanzados.
Creación y administración de grupos locales.	Administradores, Operadores de cuentas, Usuarios.	Administradores, Usuarios avanzados.
Creación y administración de grupos globales.	Administradores, Operadores de cuentas	
Asignación de derechos de usuarios.	Administradores	Administradores
Bloqueo del servidor (o computadora).	Administradores, Operadores de servidores, Todos.	Administradores, Usuarios avanzados, Todos.
Administración de la auditoría de sucesos del sistema.	Administradores.	Administradores.
Bloqueo del servidor (o estación de trabajo).	Administradores, Operadores de servidores.	Administradores, Usuarios avanzados, Todos.
Desbloqueo del servidor (o estación de trabajo).	Administradores, Operadores de servidores.	Administradores.
Dar formato al disco duro de servidores (o estación de trabajo).	Administradores, Operadores de servidores	Administradores.

[21] SHELDON Tom *Manual de Seguridad de Windows NT.* McGRAW-HILL Pág 184

Creación de grupos comunes.	Administradores, Operadores de servidores.	Administradores, Usuarios avanzados.
Compartición o no directorios compartidos.	Administradores, Operadores de servidores.	Windows NT Workstation: Administradores, Usuarios avanzados.
Compartición o no de impresoras compartidas.	Administradores, Operadores de servidores, Operadores de impresión.	Administradores, Usuarios avanzados.

Para asegurar un entorno seguro, el grupo *Todos* e *Invitados* no deben tener los derechos de *inicio de sesión* local y *apagado del sistema*. La primera opción podría permitir a cualquiera acceder a la máquina, y hacer uso de más recursos para actividades delictivas. La última opción permitiría que alguien apagase el servidor y negase el servicio al resto

4.8 CONSTRUCCION DEL DOMINIO DE SICORI

En este capítulo se han proporcionado los conocimientos necesarios para poder implantar un *Controlador de Dominio*, que sirve de base para la construcción del Dominio de SICORI. Para llevar esto a cabo, fue nenesario la capacitación de los administradores de sistemas (con cursos, pláticas, conferencias, manuales, etc). Se realizó un análisis de las áreas de trabajo para elegir el tipo de dominio adecuado, llegando a la conclusión que era el *modelo de dominio único.*[22] A partir de aquí, se crearon Grupos Globales, cuentas de usuarios, prioridades, políticas de seguridad.

El encargado de la implantación del Controlador de Dominio fue el Jefe del Area de Soporte Técnico; quién también fue el responsable de la capacitación de otros dos administradores de sistemas Entre los tres desarrollaron las siguientes etapas:

❑ Construcción del Dominio

Se destinaron dos de los servidores que tienen instalado Windows NT Server; uno funciona como PDC (Controlador Primario de Dominio) y el otro como BDC (Controlador de Dominio para Copias de Seguridad). Todas las configuraciones siguientes, necesitan ser realizadas sólo en el PDC

El nombre del dominio creado es **SISTEMA**, y el DNS (Servidor de Nombres de Dominio) es ***sistema.admin.pemex.com*** La dirección IP del PDC es *145.22.3* **93** y su nombre de equipo *pcnet***93**, su alias *compu***93**, los cuales servirán de estándar para las demás computadoras del departamento. Se utiliza un rango de 1 a 100 en el último número de la dirección IP, el cual deberá ser igual al del nombre y alias. Por ejemplo, si una computadora tiene la dirección IP *145.22.3.***168**, nombre *pcnet***25** y alias *compu***25**, entonces se cambia a *145.22.3.***25**, *pcnet***25** y *compu***25**

❑ Creación de Grupos

Una vez configurados los servidores de dominio (PDC y BDC), se realiza la configuración de *Grupos Globales y Cuentas de Usuarios*, se crean en una pantalla similar como la que aparece en la figura 4 2. SICORI tiene como grupos globales los siguientes:

- Administradores de Dominio (para el personal del área de Soporte Técnico).
- Administrativos (personal del área de Administración de Recursos Técnológicos).
- Calidad.

[22] Ver punto 4 3 de este capítulo

- Finanzas.
- Mercadotecnia.
- Producción.
- Usuarios de Dominio (instalado por default para todos los usuarios).

Las cuentas de usuarios se estandarizan de acuerdo al siguiente patrón:

inicial del (los) nombres + apellido paterno

Se realiza un análisis de necesidades para estructurar las políticas de seguridad de las cuentas de usuarios. se otrogan en un cuadro similar al de la figura 3.1.[23]

❑ Estructuración de Cuentas

Se elabora una lista que incluye nombre completo del usuario, dirección IP, nombre y alias del equipo, área a la que pertenece, y se marca *SI/NO* si tiene instalado *Internet Explorer* ó *Netscape* (tabla 4.5).

Tabla 4.5 Lista para la estructuración de cuentas de usuarios

Nombre de usuario	Dirección IP	Nombre de equipo	Alias de equipo	Área	Internet ó Nestcape Instalado (SI/NO)
Silvia Arteaga Osorio	*145.22.3.***16**	*pcnet***25**	*compu***25**	Calidad	NO
.....	.....	.....	..	.....	. .
.....	.....	.. ..	.....	.	... .

Se determina que las primeras máquinas a las que se realizará algún cambio (nombre, alias o dirección IP), son las que tengan instalado *Internet Explorer* ó *Netscape*. Esto con la finalidad, de que si lo que se requiere es un cambio de dirección IP (es decir, si el último número de ésta excede a 100), le sea comunicado este cambio al área de *Telecomunicaciones* (de PEMEX) encargada de otorgar dichas direcciones.

❑ Implantación

Se comienza hacer el cambio de nombre, alias ó dirección IP en los equipos, según se requiera; y se va introduciendo cada uno de ellos al dominio El proceso que se lleva a cabo para realizar esto, es el siguiente

- En el equipo de cada usuario se inicia la sesión con cuenta de administrador. Se entra al icono de *Propiedades de Red*, ubicado en el escritorio de NT.

[23] Por razones de seguridad las políticas de seguridad de SICORI no se indican en este proyecto

- Se cambia el nombre del equipo (si es necesario).
- Se declara el dominio (*SISTEMA*), para que esto tenga efecto, se introduce el login y contraseña del administrador.
- Se cambia el último número de la dirección IP (si es necesario).
- Se da el nombre de DNS (*sistema.admin.pemex.com*), y se pone la dirección IP del servidor de dominio (*145 22.3.93*).

Se apaga el equipo; y antes de reiniciarlo se va al PDC para hacer los siguientes cambios

- En el *Administrador de Servidores* (figura 4 1) se da de alta el equipo y el nombre completo del usuario.
- En el *Administrador del DNS* (el cual se encuentra *en Herramientas Administrativas*, igual que el anterior), se da de alta la dirección IP, nombre y alias del equipo [24]

El administrador vuelve a iniciar la sesión en la máquina del usuario para comprobar que los cambios se realizaron satisfactoriamente.

Para que el usuario pueda iniciar la sesión con su cuenta en el dominio; el administrador tuvo que haber introducido anteriormente un password *base* (común a todos los usuarios) en el PDC, en la pantalla similar al de la figura 4.4. Así, el administrador tecleará el nombre del dominio (SISTEMA), login del usuario y el password base en la computadora del usuario, y éste podrá introducir su contraseña en un nuevo cuadro de diálogo que aparecerá. Cada mes reaparecerá este cuadro para pedirle que cambie su contraseña [25]

Este mismo procedimiento se hace para todos los miembros del dominio.

Cuando se da de alta un nuevo usuario o se requiere hacer algún cambio en su password, el administrador lo realiza desde el PDC, sin necesidad de ir al equipo de éste, como se hacia anteriormente

❑ Actualización de datos y etiquetado

En la lista mencionada en la etapa 3, se añaden los campos de *Nuevo* nombre, alias y dirección IP. Con ayuda de esta lista se puede tener un mejor control de los cambios que se realicen en los equipos.

También se realiza la identificación de los nodos de la red Se etiqueta con el nombre del equipo la parte del cable que se conecta a la entrada del concentrador, y se etiqueta la parte posterior del mismo cable (el que se conecta a la computadora del usuario), con el número de concentrador y de entrada.

---

[24] La pantalla de *Administrador de DNS* no se presenta aquí por políticas de seguridad de la organización

[25] Las políticas de seguridad de las cuentas de usuarios se configuran según las necesidades de la empresa

❑ Seguridad en Archivos

En el PDC se configuran permisos de accesos de un equipo con otro(s), ver figura 4.7 Estas configuraciones se hacen por área de trabajo, es decir, alguien que pertecece a Mercadotecnia puede ver sólo las carpetas o directorios de máquinas de su misma área. Pero, para poder abrir, copiar, modificar, borrar archivos, etc., el usuario en su cuenta da las permisiones a sus archivos compartidos, en una pantalla similar a la de la figura 4.10.

❑ Problemas Técnicos

Aquí se corrigen algunos problemas presentados durante la implantación del Controlador de Dominio.

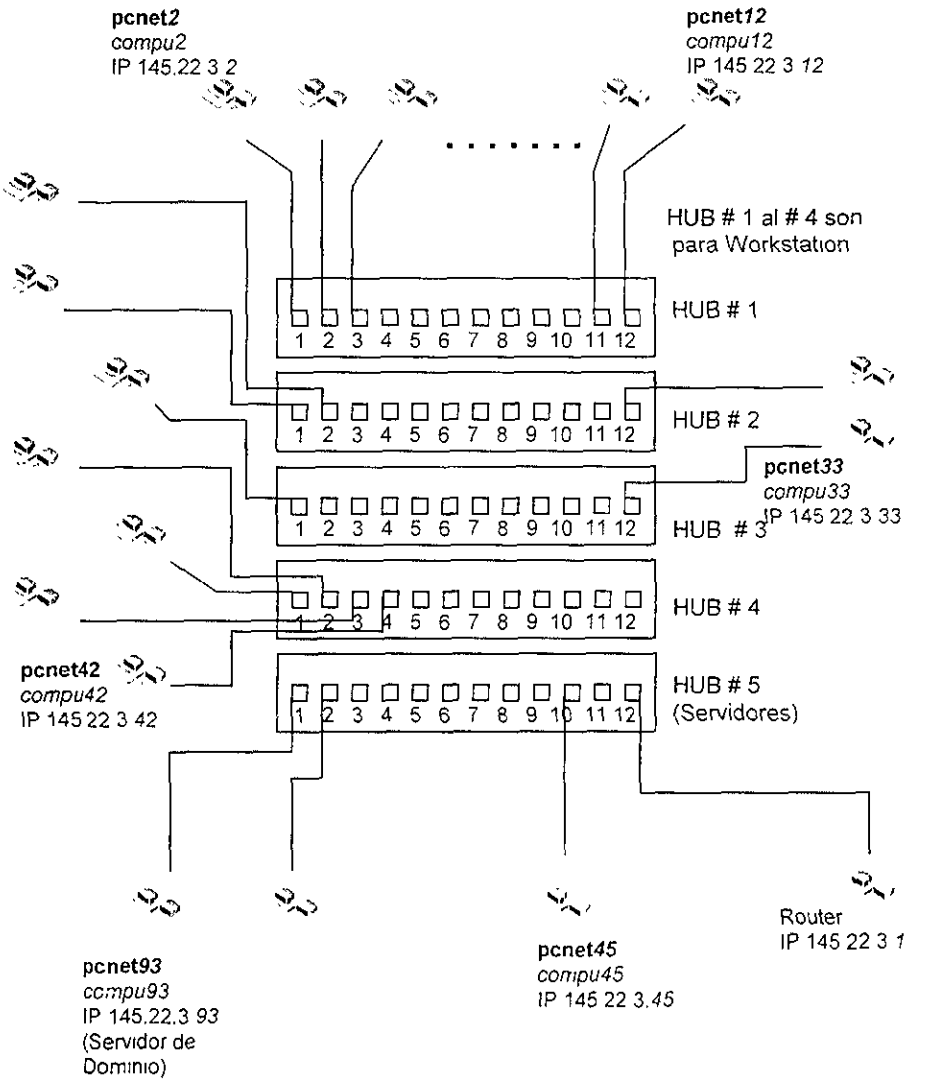
- No se podían dar de alta en el dominio algunos equipos con fallas en la tarjeta de red. Por lo que el proveedor tuvo que cambiar dichas tarjetas, y las máquinas entraron al dominio sin problemas.

- Pocas veces sucedió que el software de Windows NT era el que estaba dañado en el equipo, y no se podía introducir éste al dominio. Se reinstaló el software y en algunos casos se le tuvo que dar formato y volver a instalar el software para solucionar el problema

- Se detectó en algunas máquinas que el servicio *Server* (ver cuadro de diálogo de la figura 5.3) estaba detenido; esto lo ocacionaba la falta de recursos hardware (memoria, disco duro, etc) que antes no había sido detectado. Lo cual provocaba que no fueran vistas en el dominio dichas máquinas La solución al problema fué la adquisición de los recursos faltantes

Actualmente el sistema implantado ya está en operación, y hasta el momento los resultados han sido óptimos. En la figura 4.13 se muestra la configuración final de la red de SICORI.

En el capítulo V, se presentan algunas herramientas de Windows NT, para monitorear fallas, errores y accesos remotos, que garanticen el buen funcionamiento de los recursos de la red.



nombre	**pcnet x**
alias	*compu x*
dirección IP	IP x

Figura 4.13 Digrama final de la red de SICORI

CAPITULO V

PRUEBAS DE DESEMPEÑO DE LA SEGURIDAD EN WINDOWS NT

PRUEBAS DE DESEMPEÑO DE LA SEGURIDAD EN WINDOWS NT

Este capítulo presenta las herramientas de administración Windows NT para monitorear las fallas,errores, rendimiento y actividades de los servidores y la red; también se enlistan algunas utilidades que se pueden ejecutar desde la línea de comandos de DOS, como son las órdenes NET y TCP/IP.

A continuación se presentan algunas de las herramientas para monitorear actividades en una red Windows NT:

- **Diagnósticos Windows NT.** Es útil para configurar y encontrar los problemas de hardware del sistema y componentes añadidos.
- **Administrador de servidores.** Se emplea para administrar servidores individuales en dominios, conexiones de usuarios y las propiedades de servidores.
- **Monitor del sistema.** Muestra estadísticas de rendimiento sobre cómo funcionan los servidores con las cargas actuales. Se puede utilizar esta información para justificar mejoras del equipo o para contabilizar las actividades en servidores Web
- **Monitor de la red.** Permite capturar o visualizar paquetes en la red. Se puede utilizar no sólo para encontrar problemas en la red, sino para monitorear las actividades de piratas informáticos.
- **El visor de sucesos.** Se utiliza para visualizar los contenidos de los registros de auditorías.

A lo largo del capítulo se desarrollaran cada uno de estos servicios

5.1 DIAGNÓSTICOS DE WINDOWS NT

Windows NT suministra una nueva y mejorada utilidad que se puede abrir eligiendo *Diagnósticos de Windows NT* del grupo *Herramientas administrativas*; aparece un cuadro de diálogo similar al que se muestra en la figura 5 1. Es una poderosa herramienta para evaluar y encontrar problemas en el hardware del sistema y en las configuraciones del entorno.

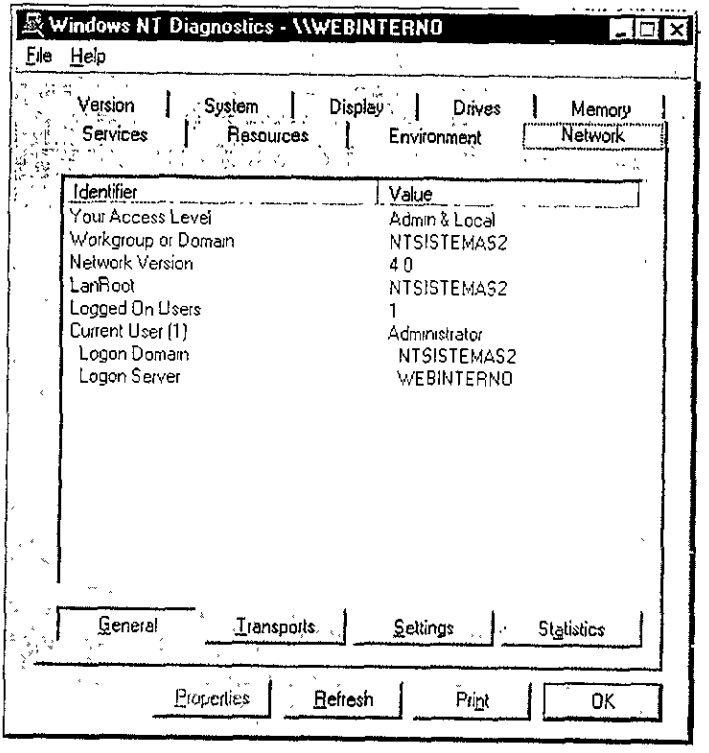


Figura 5.1 Diagnósticos Windows NT

Cada separador del cuadro *Diagnósticos de Windows NT* visualiza información sobre un servidor, sus versiones y el hardware instalado en el sistema. Se puede utilizar la información contenida en cada separador para obtener un resumen sobre el servidor, con propósitos de auditoría de seguridad.

A continuación se describen los registros de cada separador del cuadro *Diagnósticos de Windows NT*[1]:

[1] B Kretshmer, C Schneider *Todo sobre Windows NT 4.0* Editorial Marcombo Barcelona 1996 pag 179

- **Versión.** Visualización de la versión actual y el número de sistema operativo
- **Sistema.** Información sobre el Hardware Abstraction Layer (HAL)[2] utilizado, la interfaz entre el hardware y los componentes que soportan la plataforma, el tipo de procesador, así como la versión y la fecha del BIOS de la tarjeta madre del sistema.
- **Monitor.** Muestra la resolución y frecuencia (en Hertz) de la tarjeta gráfica
- **Controladores.** Visualización de información sobre unidades de disco.
- **Memoria.** Presenta la información sobre el tamaño y ocupación de la memoria principal física y del archivo de intercambio (pagefile.sys).
- **Servicios.** Visualización de qué servicios se están ejecutando o están detenidos.
- **Recursos.** Muestra las configuraciones de los dispositivos hardware del sistema.
- **Entorno.** Informa sobre las variables del sistema actuales o sobre las variables de entorno locales de Windows NT 4.0.
- **Red.** Visualización de la información crítica sobre la red. Hay cuatro botones en la página Red:
  - *General.* Muestra las configuraciones actuales de la red, como grupo de trabajo o dominio, versión de la red, dominio de inicio de sesión, servidor de inicio de sesión y el nombre de usuario actual.
  - *Transportes.* Muestra una lista de protocolos de transporte de red actuales y las direcciones de los adaptadores de red unidos a ella.
  - *Configuración.* Muestra el valor actual de los parámetros de la red como tiempos de finalización de la sesión, búfers, cache y encriptación.
  - *Estadística* Muestra las estadísticas actuales de la red, como los bytes recibidos, perdidos y transmitidos, así como muchos otros parámetros

Cuando se piensa que el sistema está siendo atacado, es recomendable vigilar las siguientes estadísticas:

❑ Errores de contraseñas en servidores

Esta estadística rastrea los intentos fallidos de inicio de sesión en el servidor; puede indicar si alguien está ejecutando un programa para adivinar contraseñas en un intento de violación del sistema.

❑ Errores de permisos en servidores

Este es el número de veces que a los clientes se les ha negado el acceso a archivos que han intentado abrir. Este valor podría indicar que alguien está intentando aleatoriamente acceder a archivos con la esperanza de conseguir algo que no esté protegido adecuadamente.

---

[2] Ver *Modo Nucleo* de la página 8 del capítulo II. Consultar el glosario

5.2 LA UTILIDAD SERVIDOR Y EL ADMINISTRADOR DE SERVIDORES

La utilidad *Servidor* y el *Administrador de servidores*[3] tienen la misma funcionalidad. Permiten administrar los servidores y las conexiones a otros servidores. El *Administrador de servidores*, localizado en el grupo *Herramientas administrativas*, muestra una lista de servidores en el dominio actual (o en otros dominios elegidos) que puede administrar. La utilidad *Servidor* está localizada en el *Panel de control* y suministra la misma funcionalidad que el *Administrador de servidores* para administrar las propiedades de un servidor local.

5.2.1 Administración de propiedades del servidor

Para administrar las propiedades de un servidor, se elige uno de la lista del *Administrador de servidores*, luego se elige *Propiedades* del menú *Equipo*; o se pulsa dos veces sobre el nombre de la computadora. Aparece un cuadro de diálogo *Propiedades* similar al de la figura 5.2.

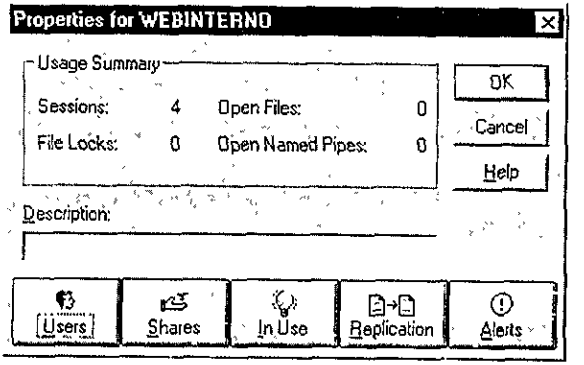


Figura 5.2 Cuadro de diálogo *Propiedades* del servidor.

El cuadro Resumen suministra la siguiente información:

- **Sesiones**. El número de usuarios conectados a la computadora
- **Archivos abiertos**. El número de archivos compartidos por el servidor
- **Bloqueos de archivos**. El número de archivos bloqueados actualmente. (Un bloqueo protege al archivo de que pueda ser accedido por otro usuario mientras esta siendo utilizado).
- **Canalizaciones con nombre abiertos**. El número de pipes[4] actualmente abiertos.

[3] El *Administrador de servidores* se menciona en el punto 4.3.1 del capítulo IV

[4] *Pipe* es el espacio compartido que acepta la salida de un programa para la entrada en otro. Ver el glosario

CAPITULO V

PRUEBAS DE DESEMPEÑO DE LA SEGURIDAD EN WINDOWS NT

PRUEBAS DE DESEMPEÑO DE LA SEGURIDAD EN WINDOWS NT

Este capítulo presenta las herramientas de administración Windows NT para monitorear las fallas,errores, rendimiento y actividades de los servidores y la red; también se enlistan algunas utilidades que se pueden ejecutar desde la línea de comandos de DOS, como son las órdenes NET y TCP/IP.

A continuación se presentan algunas de las herramientas para monitorear actividades en una red Windows NT:

- **Diagnósticos Windows NT.** Es útil para configurar y encontrar los problemas de hardware del sistema y componentes añadidos.
- **Administrador de servidores.** Se emplea para administrar servidores individuales en dominios, conexiones de usuarios y las propiedades de servidores.
- **Monitor del sistema.** Muestra estadísticas de rendimiento sobre cómo funcionan los servidores con las cargas actuales. Se puede utilizar esta información para justificar mejoras del equipo o para contabilizar las actividades en servidores Web.
- **Monitor de la red.** Permite capturar o visualizar paquetes en la red. Se puede utilizar no sólo para encontrar problemas en la red, sino para monitorear las actividades de piratas informáticos.
- **El visor de sucesos.** Se utiliza para visualizar los contenidos de los registros de auditorías

A lo largo del capítulo se desarrollaran cada uno de estos servicios.

5.1 DIAGNÓSTICOS DE WINDOWS NT

Windows NT suministra una nueva y mejorada utilidad que se puede abrir eligiendo *Diagnósticos de Windows NT* del grupo *Herramientas administrativas*; aparece un cuadro de diálogo similar al que se muestra en la figura 5 1. Es una poderosa herramienta para evaluar y encontrar problemas en el hardware del sistema y en las configuraciones del entorno.

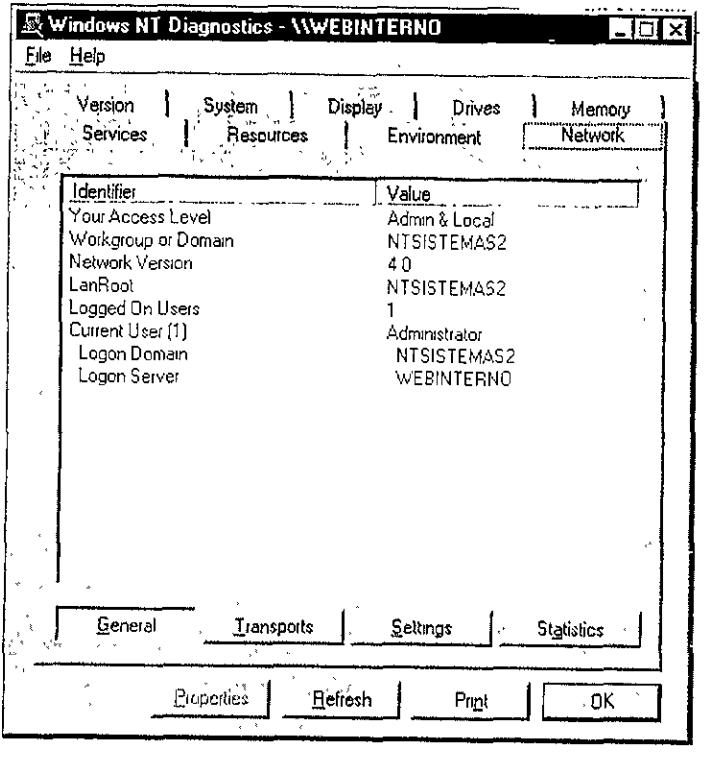


Figura 5.1 Diagnósticos Windows NT

Cada separador del cuadro *Diagnósticos de Windows NT* visualiza información sobre un servidor, sus versiones y el hardware instalado en el sistema. Se puede utilizar la información contenida en cada separador para obtener un resumen sobre el servidor, con propósitos de auditoría de seguridad.

A continuación se describen los registros de cada separador del cuadro *Diagnósticos de Windows NT*[1]:

[1] B Kretshmer, C Schneider *Todo sobre Windows NT 4.0* Editorial Marcombo Barcelona 1996 pág 179

- **Versión.** Visualización de la versión actual y el número de sistema operativo.
- **Sistema.** Información sobre el Hardware Abstraction Layer (HAL)[2] utilizado, la interfaz entre el hardware y los componentes que soportan la plataforma, el tipo de procesador, así como la versión y la fecha del BIOS de la tarjeta madre del sistema.
- **Monitor.** Muestra la resolución y frecuencia (en Hertz) de la tarjeta gráfica
- **Controladores.** Visualización de información sobre unidades de disco
- **Memoria.** Presenta la información sobre el tamaño y ocupación de la memoria principal física y del archivo de intercambio (pagefile sys).
- **Servicios.** Visualización de qué servicios se están ejecutando o están detenidos.
- **Recursos.** Muestra las configuraciones de los dispositivos hardware del sistema.
- **Entorno.** Informa sobre las variables del sistema actuales o sobre las variables de entorno locales de Windows NT 4.0
- **Red.** Visualización de la información crítica sobre la red Hay cuatro botones en la página Red.
  - *General.* Muestra las configuraciones actuales de la red, como grupo de trabajo o dominio, versión de la red, dominio de inicio de sesión, servidor de inicio de sesión y el nombre de usuario actual.
  - *Transportes* Muestra una lista de protocolos de transporte de red actuales y las direcciones de los adaptadores de red unidos a ella
  - *Configuración.* Muestra el valor actual de los parámetros de la red como tiempos de finalización de la sesión, búfers, cache y encriptación.
  - *Estadística.* Muestra las estadísticas actuales de la red, como los bytes recibidos, perdidos y transmitidos, así como muchos otros parámetros

Cuando se piensa que el sistema está siendo atacado, es recomendable vigilar las siguientes estadísticas:

❑ Errores de contraseñas en servidores

Esta estadística rastrea los intentos fallidos de inicio de sesión en el servidor; puede indicar si alguien está ejecutando un programa para adivinar contraseñas en un intento de violación del sistema

❑ Errores de permisos en servidores

Este es el número de veces que a los clientes se les ha negado el acceso a archivos que han intentado abrir Este valor podría indicar que alguien está intentando aleatoriamente acceder a archivos con la esperanza de conseguir algo que no esté protegido adecuadamente.

---

[2] Ver *Modo Nucleo* de la página 8 del capítulo II Consultar el glosario

5.2 LA UTILIDAD SERVIDOR Y EL ADMINISTRADOR DE SERVIDORES

La utilidad *Servidor* y el *Administrador de servidores*[3] tienen la misma funcionalidad. Permiten administrar los servidores y las conexiones a otros servidores. El *Administrador de servidores*, localizado en el grupo *Herramientas administrativas*, muestra una lista de servidores en el dominio actual (o en otros dominios elegidos) que puede administrar. La utilidad *Servidor* está localizada en el *Panel de control* y suministra la misma funcionalidad que el *Administrador de servidores* para administrar las propiedades de un servidor local

5.2.1 Administración de propiedades del servidor

Para administrar las propiedades de un servidor, se elige uno de la lista del *Administrador de servidores*, luego se elige *Propiedades* del menú *Equipo*; o se pulsa dos veces sobre el nombre de la computadora Aparece un cuadro de diálogo *Propiedades* similar al de la figura 5 2.

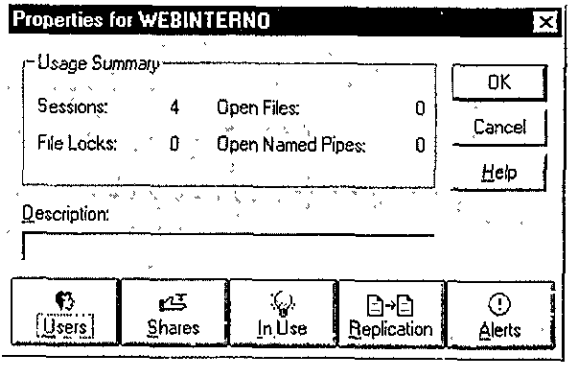


Figura 5.2 Cuadro de diálogo *Propiedades* del servidor.

El cuadro Resumen suministra la siguiente información

- **Sesiones**. El número de usuarios conectados a la computadora.
- **Archivos abiertos**. El número de archivos compartidos por el servidor
- **Bloqueos de archivos**. El número de archivos bloqueados actualmente (Un bloqueo protege al archivo de que pueda ser accedido por otro usuario mientras esta siendo utilizado).
- **Canalizaciones con nombre abiertos**. El número de pipes[4] actualmente abiertos.

[3] El *Administrador de servidores* se menciona en el punto 4 3 1 del capitulo IV

[4] *Pipe* es el espacio compartido que acepata la salida de un programa para la entrada en otro Ver el glosario

Los botones en la parte inferior del cuadro de diálogo *Propiedades del servidor* (figura 5.2), abren otros cuadros que permiten visualizar los usuarios que están conectados a la red actualmente y una lista de recursos en uso de cada uno. A continuación se describe cada botón:

❑ Usuarios

Abre un cuadro en el cual se puede desconectar del sistema a uno o varios usuarios. Se debe desconectar a usuarios si se sospecha que están envueltos en actividades no autorizadas, o si sus cuentas han sido utilizadas por alguien que haya conseguido acceso no autorizado

❑ Recursos compartidos

Sirve para visualizar una lista de los recursos compartidos disponibles en el sistema y los usuarios que los están utilizando. Se puede seleccionar cualquier usuario que esté compartiendo un recurso y hacer que deje de compartirlo.

❑ En uso

En este cuadro se puede visualizar la lista de recursos actualmente en uso, ordenados por el usuario que los está utilizando Se puede desconectar a cualquier usuario del recurso al que está accediendo

❑ Alertas

Las alertas son una parte crítica de la estrategia de seguridad. Son generadas por un sistema donde hay problemas en procesos de seguridad, de acceso, de sesiones, de alimentación eléctrica y del sistema; por ejemplo, un usuario puede ser avisado cuando una duplicación de directorio no ocurra (en un backup), o cuando un disco esté cerca del agotamiento.

En el cuadro *Alertas* se especifica qué computadoras o usuarios deberían ser avisados cuando ocurre una alerta. Se puede teclear un nombre de usuario o un nombre de computadora en el cuadro de texto y pulsar el botón *Agregar* para añadirlo a la lista de usuarios o computadoras que serán avisados. Si un usuario está dentro de una sesión en varias estaciones de trabajo, las alertas sólo aparecen en una de ellas, así que el usuario podría no verla.

5.3 ADMINISTRACIÓN DE SERVICIOS

Los *servicios* son configurados durante la instalación de Windows NT, o cuando se instalan componentes usando utilidades del *Panel de control*. Se puede elegir *Servicios* en el *Panel de control* para visualizar y administrar los servicios que están ejecutándose en la computadora. Aparece un cuadro de diálogo similar al de la figura 5 3

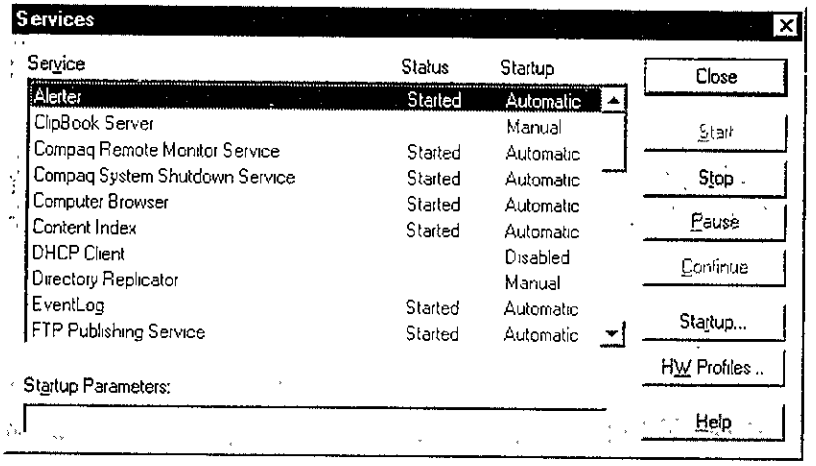


Figura 5.3 Cuadro de diálogo *Servicios*

Para trabajar con el cuadro de diálogo de Servicios, se debe tener en cuenta lo siguiente.

- Se debe iniciar la sesión en una cuenta que sea miembro del grupo local de *Administradores* para configurar servicios.
- Se pueden detener o pausar algunos servicios no esenciales para mejorar el rendimiento del servidor.
- Se recomienda ejecutar sólo los servicios más esenciales, ya que algunos de servicios podrían amenazar la seguridad
- Muchos servicios se inician en la cuenta *Sistema* que, por default, tiene acceso total a unidades enteras. Este nivel de acceso es inadecuado para muchos servicios; se deberá elegir iniciarlos en una cuenta de bajo nivel, por ejemplo, la de *usuarios*.
- Si se pausa un servicio como el del *Servidor*, todavía está disponible para el grupo de *Administradores y Operadores del servidor*, pero todos los demás usuarios no pueden utilizarlo. Si se detiene el servicio, los usuarios existentes no pueden utilizarlo hasta que se reinicie el equipo Se recomienda que antes de detener un servicio, se envíe un mensaje a los usuarios para que puedan salir correctamente

Los siguientes servicios se instalan por omisión en Windows NT 4.0. [5] El servidor puede incluir servicios adicionales dependiendo de las selecciones durante la instalación o del hardware y software instalado. Es importante evaluar cuidadosamente cuáles de estos servicios se necesitan ejecutar y cuáles puede ser detenidos. Algunos servicios dependen de otros y no pueden ser detnidos sin parar estos otros.

❑ Alertas

Este servicio envía alertas generadas en máquinas locales a computadoras o usuarios remotos. Lo utiliza el servicio *Servidor* y otros servicios; y necesita el servicio *Mensajes*.

❑ Visor del Portafolio

Permite que las páginas en el *Portafolio del servidor* (comúnmente llamado *mi maletín*) puedan ser vistas por los usuarios de otras estaciones de trabajo que ejecutan *Portafolio*.

❑ Examinador de Computadora

Se ocupa de buscar y mostrar listas de computadoras que suministran servicios en un dominio. Por razones de seguridad, se podría querer desactivar la búsqueda, pero hacerlo podría ser inconveniente para los usuarios. Los usuarios necesitarán teclear el nombre de la computadora a la que quieran acceder o crear teclas de acceso abreviado a estos sistemas.

❑ Duplicador de directorios

Este servicio duplica directorios y los archivos en los directorios entre servidores. Si no se utiliza la duplicación, se recomienda desactivarlo.

❑ Registro de sucesos

Este servicio registra actividades del servidor en el registro de sucesos No se puede pausar o detener este servicio.

[5] SHELDON, Tom ***Manual de Seguridad de Windows NT*** McGRAW-HILL pág 237

❑ Mensaje

Este servicio envía y recibe mensajes y alertas enviados por administradores o por servicios que generan alertas, y las muestra en la pantalla como cuadro de mensajes Este servicio se para cuando el servicio *Estación de trabajo* es detenido.

❑ Inicio de sesión en red

En estaciones de trabajo Windows NT este servicio permite la identificación de inicios de sesión, y se utiliza para inicios de sesión cuando la estación de trabajo participa en un dominio En servidores Windows NT, este servicio identifica el inicio de sesión de usuarios y sincroniza las bases de datos de seguridad del servidor entre el controlador primario de dominio y los controladores de copias de seguridad del dominio

❑ DDE red

Este servicio suministra un transporte de red así como seguridad para conversaciones DDE (Intercambio Dinámico de Datos).

❑ Proveedor LAN Manager (LM) de soporte de seguridad NT

Suministra seguridad Windows NT para aplicaciones RPC (Llamada a Procedimiento Remoto) que utilizan transportes que no son canales identificativos.

❑ Localizador de llamada a procedimiento remoto (RPC)

Permite que las aplicaciones distribuidas utilicen el servicio RPC de Microsoft y administra la base de datos *Servicio de nombres RPC*. La parte del servidor de las aplicaciones distribuidas registra la disponibilidad de este servicio y la parte del cliente de una aplicación distribuida pide a este servicio que encuentre aplicaciones disponibles en el servidor. Se puede detener este servicio en computadoras aisladas que suministran servicios mínimos como un servidor Web conectado a Internet, pero en servidores conectados a un dominio o grupo de trabajo se necesitará para la mayoría de las aplicaciones administrativas y de usuario.

❑ Servicio de llamada a procedimiento remoto (RPC)

Este es el subsistema RPC para Windows NT; incluye el asignador de punto final y otros servicios relacionados. Detener o pausar este servicio en servidores conectados a la red producirá resultados impredecibles y bloqueos.

❑ Servidor

Este es el servicio SMB (Bloque de Mensajes de Servidor) que permite a una computadora Windows NT compartir sus recursos por la red. Puede conectarse con otras computadoras, pero permite que las otras lo hagan con ella El intercambio de mensajes entre cliente y servidor es tratado por el protocolo SMB Si se detiene esté servicio, otros como *Examinador de computadora*, *Duplicador de directorio*, *Inicio de sesión en red*, y *Servicios de acceso remoto* también se detendrán.

❑ Ayuda TCP/IP NetBIOS

Suministra NetBIOS a servicios sobre TCP/IP y sólo está disponible si éste protocolo está instalado. Se puede detener si no se quiere utilizar NetBIOS por razones de seguridad; desactivarlo detiene también el servicio *Examinador de computadora* y el *inicio de sesión en la red* Detener este servicio en el controlador primario de dominio cuando TCP/IP es el único protocolo en uso, se tendrán resultados impredecibles. En la mayoría de los casos, se recomienda dejarlo que se siga ejecutando.

❑ SAI

Esta suministra servicios para la conexión de fuentes de alimentación que no pueden ser interrumpidas.

❑ Estación de trabajo

permite a una computadora Windows NT acceder a recursos en una red de grupos de trabajo y a un dominio; con frecuencia, se le llama reexpedidor. Todas las peticiones de usuarios de servicios de red pasan por este servicio, las peticiones de conectar, abrir, leer o escribir en una unidad reexpedida (una unidad que hace referencia a un directorio compartido en otra computadora de la red) son enviados al reexpedidor y empaquetados para ser enviados por la red al servidor. Los servidores Windows NT, funcionando como controladores primarios del dominio también lo ejecutan, por lo que pueden conectarse como clientes con otros controladores de dominio e intercambiar información.

Existen otros servicios que se pueden instalar opcionalmente, o que tienen que ser iniciados manualmente; por ejemplo, se pueden instalar los servicios *FTP, Gopher, Web y RAS* en las computadoras Windows NT Otros servicios no necesarios al principio, pueden ser instalados cuando se configuran nuevas aplicaciones.

Hay varios casos donde se podría querer desactivar algunos servicios por razones de rendimiento y de seguridad. Supongamos que se quiere configurar un

servidor Web conectado internamente al de los usuarios dentro de una compañía. Se instala el software *Servidor de Información Internet de Microsoft* en una computadora Windows NT, y se detienen los servicios *Servidor*, *Estación de trabajo* y *Examinador de computadora*; ahora los usuarios internos pueden acceder sólo a páginas Web. Sólo los directorios que estén disponibles en el *Administrador de Servicios Internet* pueden ser accedidos por los examinadores. Debido a que el servicio *Examinador* está desactivado, los usuarios no verán el nombre de esta computadora en la lista del examinador, no podrán teclear su nombre NetBIOS en su examinador Web; tienen que teclear la dirección IP del servidor Web al que quieren acceder. Sin embargo, después de conectarse a la página por primera vez, pueden crear una tecla abreviada de acceso a ella en sus escritorios para hacer más fáciles las conexiones futuras

5.4 ORDENES NET Y TCP/IP

NET y TCP/IP son órdenes que los administradores pueden ejecutar en la ventana del *comandos de DOS* (ventana de MS-DOS), para mostrar información sobre redes, servidores, sesiones de conexión y directorios compartidos.

5.4.1 El Comando Net

El comando NET tiene varias opciones que se pueden utilizar para añadir cuentas de usuarios y grupos cambiar configuraciones de dominios y trabajar con recursos compartidos [6]

Se pueden hacer muchas de las mismas cosas que se pueden hacer en el *Administrador de usuarios* y en el *Administrador de servidores,* ejecutando órdenes NT desde una línea de comandos. Se puede incluso, crear archivos de procesamiento en lotes que incluyan órdenes para crear múltiples cuentas de usuarios y grupos. Sin embargo, algunas cosas todavía se tienen que hacer desde el *Administrador de usuarios*, como garantizar derechos.

La siguiente es una lista de órdenes NET para Windows NT. Las comandos de interés especial para administradores de la seguridad son *NET ACCOUNTS*, que indica cuáles son las configuraciones actuales para las restricciones de inicios de sesión y contraseñas; *NET FILE*, que dice qué archivos están siendo utilizados, si se está rastreando a un pirata informático; *NET PAUSE* y *NET STOP*, que suministran un modo rápido para detener o parar un servicio en caso de emergencia (por ejemplo, que el sistema esté siendo atacado) y *NET SESSION*, que lista las sesiones actuales y permite borrar una sesión de un intruso. Estas órdenes no se ejecutan en contra de las computadoras que tienen el servicio *Servidor* desactivado.[7]

- **NET ACCOUNTS** Muestra las configuraciones actuales sobre las contraseñas, las limitaciones en el inicio de sesión e información sobre dominios. También tiene opciones para actualizar la base de datos de cuentas de usuarios y modificar las contraseñas e inicios de sesión para todas las cuentas.
- **NET COMPUTER** Añade o borra computadoras de una base de datos del dominio y está disponible en servidores Windows NT
- **NET CONFIG SERVER (o NET CONFIG WORKSTATION).** Despliega la información de configuración sobre el servicio *Servidor (o Estación de trabajo).* Cuando se utiliza sin el conmutador *SERVER o WORKSTATION*, la orden muestra la lista de servicios configurables. Los usuarios de computadoras de

---

[6] Si el servicio *Servidor* está desactivado en el PDC, no se pueden utilizar órdenes NET

[7] Se recomienda utilizar la opción *MORE* para desplegar en forma de página la información de ayuda en la pantalla. Por ejemplo, se puede teclear *NET ACCOUNT | MORE* para desplegar la ayuda sobre *Cuentas*

cliente Windows pueden teclear *NET CONFIG* para visualizar el nombre de la computadora, del usuario que ha accedido, y del dominio o el del grupo de trabajo.

- **NET CONTINUE** Reactiva un servicio Windows NT que ha sido detenido por *NET PAUSE*.
- **NET FILE**. Lista los archivos abiertos en el servidor, tiene opciones para cerrar los que están compartidos, y para desbloquearlos. Las listas incluyen el número de identificación asignado a un archivo abierto, su ruta, el número de bloqueos y el nombre del usuario. Esta orden sólo funciona en computadoras que ejecutan el servicio *Servidor*
- **NET GROUP**. Muestra información sobre los nombres de grupos, y tiene opciones que se pueden utilizar para añadir o modificar los grupos globales en servidores. Se puede utilizar en un archivo de procesamiento por lotes para añadir o modificar los grupos enteros.
- **NET HELP**. Para conseguir ayuda de órdenes *NET*, se escribe *NET HELP orden* o *NET orden /HELP*.
- **NET HELPMSG mensaje#.** Para conseguir ayuda sobre mensajes de la red, se escribe esta orden, reemplazando *mensaje#* con el número del mensaje de error.
- **NET LOCALGROUP**. Se utiliza para ver los grupos locales en servidores. También tiene opciones para modificar los grupos.
- **NET NAME** Despliega los nombres de las computadoras y usuarios a los cuales los mensajes son enviados. También tiene opciones para añadir y borrar un nombre de mensaje (alias)
- **NET PAUSE** Detiene servicios Windows NT. Al parar un servicio, permanece así hasta que se utilice la orden *NET CONTINUE* para hacer que continúe.
- **NET PRINT**. Muestra los trabajos de impresión y las colas compartidas.
- **NET SEND.** Envía mensajes a otros usuarios o computadoras en la red. Para recibir mensajes, el servicio *Mensaje* tiene que estar funcionando.
- **NET SESSION**. Despliega información sobre sesiones actuales, y tiene opciones para borrar sesiones entre computadoras. Se puede utilizar para desconectar una conexión no deseada.
- **NET SHARE**. Muestra información sobre todos los recursos compartidos en una computadora También se usa para crear comparticiones en la red
- **NET STATISTICS SERVERS (o WORKSTATION).** Presenta el registro de estadísticas para el servicio *Workstation* o *Server*.
- **NET STOP**. Se usa en servicios Windows NT, cancelando todas las conexiones que el servicio utiliza. Es importante considerar que al detener un servicio se podrían parar otros dependientes de él. Por razones de seguridad, se podría querer utilizar la orden *NET STOP* para detener rápidamente un servicio. El servicio *Registro de sucesos* no puede ser detenido nunca.
- **NET TIME**. Se utiliza para mostrar o configurar *la hora* en una computadora o dominio.

- **NET USE**. Despliega una lista de computadoras conectadas a la red y tiene opciones para conectar y desconectar recursos compartidos en otras computadoras.
- **NET USER**. Muestra una lista de cuentas de usuarios de la computadora y tiene opciones para crear y modificar estas cuentas. Se utiliza sólo con servidores Windows NT. Hay opciones extendidas para crear cuentas de usuarios; se pueden escribir varias órdenes en un archivo de procesamiento por lotes para crear un grupo de cuentas de usuarios.
- **NET VIEW** Presenta una lista de recursos compartidos en una computadora. Se pueden especificar opciones para mostrar recursos en otros dominios o en servidores NetWare.

5.4.2 Órdenes TCP/IP

A continuación se muestran varios comandos que se pueden utilizar para monitorear, encontrar problemas y mantener las redes TCP/IP. En la mayoría de los casos, éstas órdenes están diseñadas para redes internas, pero se pueden utilizar algunas de ellas a través de Internet.[8]

- **ARP**. Permite administrar la asignación entre direcciones IP y direcciones físicas de la red.
- **IPCONFIG.** Muestra la información diagnóstica y los valores de configuración actuales de la red TCP/IP.
- **NBTSTAT.** Produce información sobre las conexiones NetBIOS sobre TCP/IP.
- **NETSTAT.** Muestra estadísticas sobre protocolos y conexiones actuales de TCP/IP.
- **PING.** Prueba conexiones en redes TCP/IP.
- **TRACERT**. Rastrea cómo los paquetes se envían por la red interna o por Internet

[8] Para más información sobre las órdenes listadas, refiérase a la ayuda Windows NT o al libro *TCP/IP: Architecture, Protocols and Implementation* de Sidnie Feit (McGraw Hill, 1996)

5.5 VISUALIZACIÓN DE ACTIVIDADES CON EL MONITOR DEL SISTEMA

El *Monitor del sistema* es una herramienta para presentaciones gráficas y generación de estadísticas que puede utilizarse para ver la información del rendimiento sobre los servidores, y puede avisar cuando ocurren ciertos sucesos Se pueden utilizar propiedades de monitoreo, representación y registro del *Monitor del Sistema* para ayudar en la localización de problemas de rendimiento inicial y planificar la capacidad del servidor local o de otros servidores de la red.

El Monitor del Sistema se muestra en la figura 5 4; se inicia pulsando dos veces la opción *Monitor del sistema* del grupo *Herramientas Administrativas*. Se muestran cuatro procesos en esta gráfica; están nombrados en la parte inferior de la ventana. Se puede elegir qué rastrear y luego almacenar la información recogida en archivos para un estudio posterior.

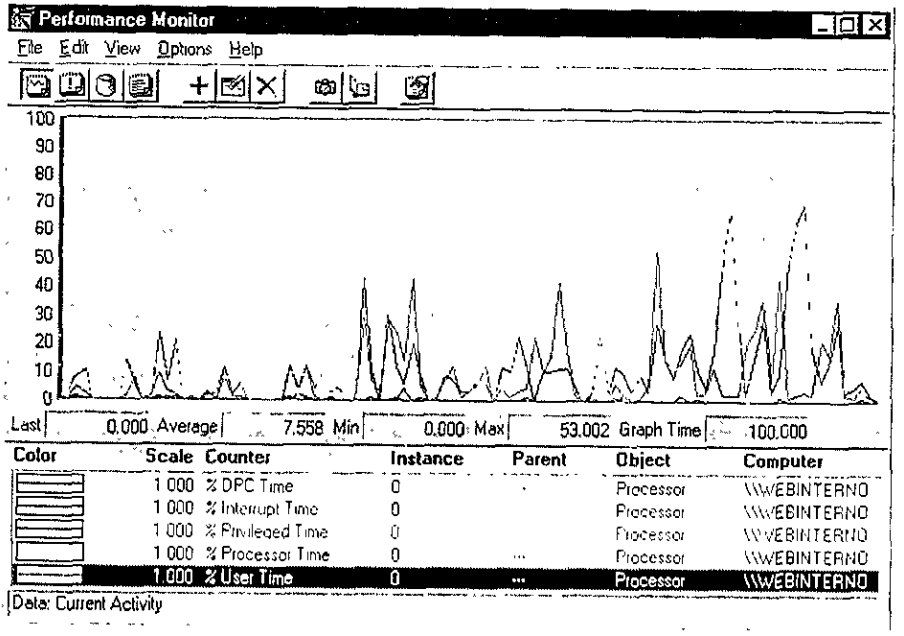


Figura 5.4 Monitor del Sistema

Se presenta a continuación una lista de lo que se puede hacer con el *Monitor del Sistema*:

- Configurar alertas para que avisen de actividades de intrusos, o accesos intentados a archivos no autorizados

- Visualizar información sobre computadoras múltiples al mismo tiempo. Se pueden abrir múltiples copias del *Monitor del sistema* y rastrear múltiples sucesos en cada copia.
- Recolección de información de modo gráfico, registros de alerta e informes.
- Visualizar los gráficos y cambiar dinámicamente las configuraciones según las necesidades.
- Exportar la información recolectada a programas de hojas de cálculo o bases de datos para análisis e impresiones futuras.
- Configurar alertas para rastrear y comparar valores *contador* frente a valores de *referencia*
- Salvar las configuraciones y los valores actuales para sesiones gráficas.

El *Monitor del Sistema* rastrea objetos, que son procesos y servicios que se ejecutan en servidores Windows NT. Cada objeto tiene contadores que rastrean sucesos o actividades específicas. Enseguida se presenta una lista de objetos a monitorear:

- Examinador.
- Cache.
- Servidor FTP (Protocolo de transferencia de archivos).
- Servicio Gopher.
- Servicio HTTP.
- Memoria
- NetBEUI y sus recursos.
- Interfaz y segmento de red.
- NWLink IPX, NWLink NetBIOS y NWLink SPX.
- Discos físicos.
- Procesador.
- Servicios de acceso remoto.
- Servidor
- Sistema
- TCP/IP.

Los contadores para objetos están rastreados y representados en la ventana de la figura 5.4. Se puede visualizar una lista de objetos para rastrearlos y obtener una descripción de lo que son, pulsando el botón *Explicar*. La ventana *explicación* se abre en la parte inferior del cuadro de diálogo.

5.5.1 Alertas de seguridad

Las siguientes opciones de seguridad son importantes para proteger la información contra piratas informáticos, y es mejor hacer que *el Monitor del Sistema* alerte cuando estos sucesos ocurran. Estas opciones se añaden en el menu *Ver* en la opción *Alerta*.

- **Errores de permiso en los accesos**. El número de veces que un cliente intenta, pero falla, al abrir un archivo y recibe un mensaje de *STATUS_ ACCESS_DENIED.* Esta alerta puede indicar si alguien está intentando aleatoriamente acceder a archivos esperando encontrar alguno desprotegido .
- **Errores de accesos concedidos** El número de veces que los accesos a archivos abiertos con éxito fueron negados. Esto puede indicar los intentos de acceder a archivos sin accesos de autorización adecuados
- **Errores de inicios de sesión**. El número de intentos de inicios de sesión fallidos en el servidor. Puede indicar si existen programas para adivinar contraseñas que alguien este utilizando para violar la seguridad en el servidor

5.6 MONITOREO DE LA RED

La utilidad de *Monitor de Red* permite rastrear el tráfico de red de una computadora; sólo puede utilizarse para monitorear paquetes de información que son enviados o recibidos por la computadora donde se está ejecutando el programa. Es una herramienta de diagnóstico para visualizar redes de área local, localizar un servidor apagado o localizar cuellos de botella en la red. Suministra una presentación gráfica de estadísticas de la red, como se muestra en la Figura 5.5.

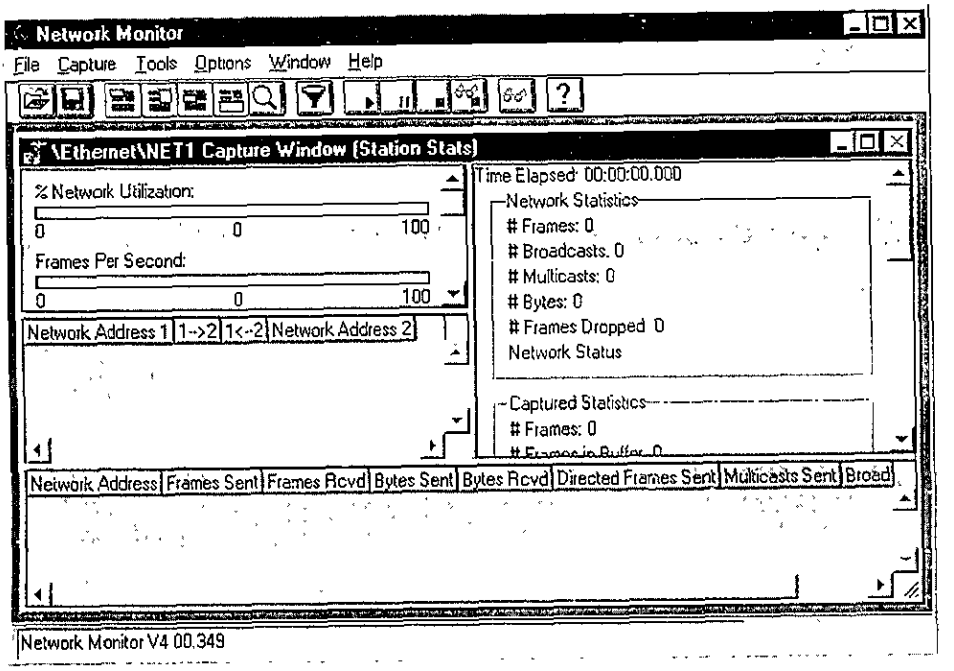


Figura 5.5 Monitor de Red.

La presentación del *Monitor de Red* contiene cuatro ventanas distintas, cada una con la siguiente información.

- Información sobre el host que ha enviado una trama[9] por la red.
- Información sobre el host que ha recibido la trama.
- Los protocolos utilizados para enviar la trama.
- Los datos o una porción del mensaje enviado.

[9] Consultar el glosario

La dirección de red es un número hexadecimal único (base 16) que identifica a una computadora en la red, es la dirección hardware predefinida asignada a cada tarjeta de interfaz de red. Para descubrir la dirección hexadecimal de un sistema, se teclea una de las órdenes mostradas a continuación, reemplazando *dirección IP* con la dirección IP de la computadora en cuestión, o *nombre de la computadora* con el nombre *NetBIOS* de ésta.

NBTSTAT - A *dirección IP*
NBTSTAT - a *nombre de la computadora*

El *Monitor de red* recoge información sobre la red durante un periodo de tiempo. Durante ese periodo, la información sobre todas las tramas transmitidas por la red, es registrada y está disponible en la ventana del *Monitor de Red*. Se puede visualizar la información en una presentación gráfica a medida que sucede, y puede guardarse en archivos para verla más tarde.

Cuando se captura información, se pueden configurar filtros para ver sólo la información esencial para detectar intrusos u otros problemas. Por ejemplo, se puede filtrar por:

- **Protocolo,** para ver tramas relacionadas con una orden particular que un pirata podría estar usando;
- **Por dirección de red,** para capturar tramas de computadoras específicas en la red; y
- **Por patrones de datos** que permite capturar sólo las tramas con un patrón específico ASCII o hexadecimal. Se puede especificar cuántos bytes de datos debe contener la trama para encajar con el patrón.

5.7 AUDITORÍAS

El *Sistema de auditorías* Windows NT permite rastrear sucesos relacionados con las políticas de seguridad, del sistema y de las aplicaciones El sistema de auditorías produce registros que se pueden visualizar con el *Visor de Sucesos, ubicado* en el grupo *Herramientas administrativas* Con este sistema se pueden rastrear las actividades realizadas por usuarios autorizados y no autorizados

Hay dos tipos de auditorías que pueden ser rastreadas.

- **Auditoría de cuentas de usuarios**. Rastrea los sucesos de seguridad y los escribe en el registro de seguridad. Esta opción se activa en la utilidad *Administrador de usuarios en dominios.*
- **Auditoría del sistema de archivos**. Rastrea sucesos del sistema de archivos Se activa esta opción en el *Administrador de Archivos*

Se deben tener derechos de *administrador* para configurar propiedades de auditoría. Una vez que se activa una auditoría, se utiliza el *Visor de Sucesos* para examinar qué eventos han sido auditados La auditoria puede consumir una gran cantidad de tiempo de procesamiento y espacio de disco; cuantos más usuarios sean rastreados, mayor cantidad de disco consume. Para mantener la sobrecarga en medidas razonables, se recomienda activar la auditoria sólo cuando se sospeche de actividades maliciosas. Es importante asegurarse que los usuarios no autorizados, no tengan accesos al directorio *servername\System32* donde se almacena la información sobre auditorias

5.7.1 Configuración de auditoríás de cuentas de usuarios

Para activar la auditoría de cuentas de usuarios, se elige *Auditoría* del menú *Directivas* de la utilidad *Administración de usuarios en dominios*; y aparece el cuadro de diálogo *Políticas de auditoría*, como se muestra en la figura 5 6 Se usa el botón *Auditar estos sucesos* para activar el sistema de auditorías, el cual rastrea el exito o fracaso de los sucesos; y éstos se determinan dependiendo de las necesidades de la empresa.

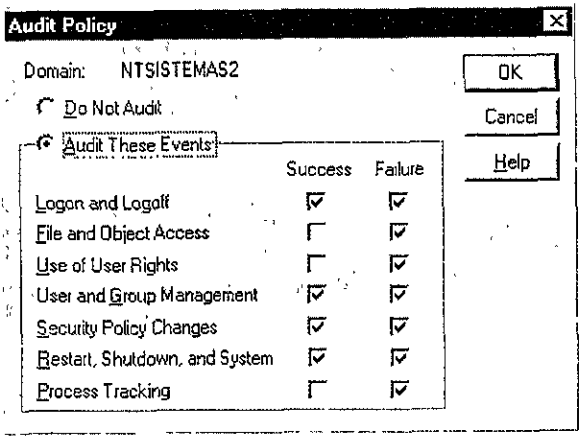


Figura 5.6 Políticas de auditoría

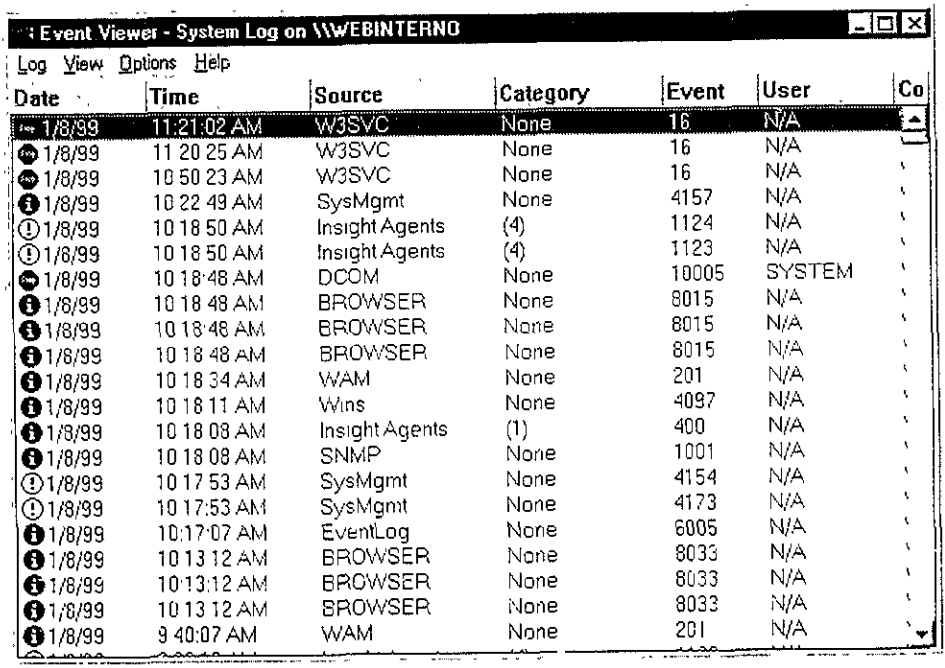
A continuación se presenta una lista de los sucesos que se recomienda que sean auditados:

- **Inicio y cierre de sesión**. Rastrea si un usuario ha iniciado o salido de una sesión, o se ha conectado a la red.
- **Acceso a archivos y objetos**. Rastrea si un usuario ha accedido a un directorio, un archivo o a una impresora que está siendo auditada.
- **Uso de los derechos de usuario**. Avisa si un usuario ha utilizado un derecho de usuario.
- **Administración de usuarios y grupos**. Rastrea si una cuenta de usuario ha sido creada, cambiada o borrada.
- **Cambios en el plan de seguridad**. Registra si se ha hecho un cambio en los *derechos de Usuarios*, *Auditoría* o *Relaciones de confianza*.
- **Reinicio, apagado y sistema**. Rastrea si un usuario ha reiniciado o apagado la computadora, si un suceso ha ocurrido afectando a la seguridad del sistema o al registro de seguridad.
- **Seguimiento de procesos**. Registra información detallada sobre el rastreo de procesos, como la activación y cierre de programas.

El sistema de auditoria sólo registra las cuentas de usuarios que fueron utilizadas para los sucesos auditados Si alguien se ha apropiado de una cuenta sin autorización, se podria pensar erróneamente que el propietario legal es el responsable de las actividades no autorizadas. Es importante aclarar que sólo los archivos y los directorios en particiones **NTFS** pueden ser auditados.

5.7.2 Visor de Sucesos

El *Visor de Sucesos* es la herramienta que se utiliza para ver eventos del sistema y de auditoría de seguridad. Se localiza en el grupo *Herramientas administrativas* (como se muestra en la figura 5.7), se puede elegir *Sistema*, *Seguridad* o *Aplicación* del menú *Registro* para ver tres conjuntos distintos de sucesos.



Date	Time	Source	Category	Event	User	Co
1/8/99	11:21:02 AM	W3SVC	None	16	N/A	
1/8/99	11 20 25 AM	W3SVC	None	16	N/A	
1/8/99	10 50 23 AM	W3SVC	None	16	N/A	
1/8/99	10 22 49 AM	SysMgmt	None	4157	N/A	
1/8/99	10 18 50 AM	Insight Agents	(4)	1124	N/A	
1/8/99	10 18 50 AM	Insight Agents	(4)	1123	N/A	
1/8/99	10 18 48 AM	DCOM	None	10005	SYSTEM	
1/8/99	10 18 48 AM	BROWSER	None	8015	N/A	
1/8/99	10 18 48 AM	BROWSER	None	8015	N/A	
1/8/99	10 18 48 AM	BROWSER	None	8015	N/A	
1/8/99	10 18 34 AM	WAM	None	201	N/A	
1/8/99	10 18 11 AM	Wins	None	4097	N/A	
1/8/99	10 18 08 AM	Insight Agents	(1)	400	N/A	
1/8/99	10 18 08 AM	SNMP	None	1001	N/A	
1/8/99	10 17 53 AM	SysMgmt	None	4154	N/A	
1/8/99	10 17:53 AM	SysMgmt	None	4173	N/A	
1/8/99	10:17:07 AM	EventLog	None	6005	N/A	
1/8/99	10 13 12 AM	BROWSER	None	8033	N/A	
1/8/99	10:13:12 AM	BROWSER	None	8033	N/A	
1/8/99	10 13 12 AM	BROWSER	None	8033	N/A	
1/8/99	9 40:07 AM	WAM	None	201	N/A	

Figura 5.7 Visor de Sucesos.

Se pueden elegir las siguientes opciones del menú *Ver*

- **Todos los sucesos**. Muestra todos los sucesos.
- **Filtrar sucesos** Se eligen los sucesos que se quieren ver por fechas, horas, tipos de suceso, categorías, etc.
- **Nuevos**. Muestra los sucesos más recientes en la parte superior de la lista.
- **Antiguos**. Muestra los sucesos más antiguos en la parte superior de la lista.
- **Buscar**. Busca un suceso específico.

Para ver información detallada sobre cualquier suceso, se pulsa dos veces sobre éste. Se pueden guardar en archivos externos, eligiendo *Guardar como* del menú *Registro*. Por otra parte, dentro del menú *Registro*, hay una opción para

borrar el *Registro de sucesos*; antes de hacerlo, es importante asegúrarse de que se han guardado los registros para referencias futuras

Visualizar periódicamente el *Visor de Sucesos* es importante, ya que puede alertar de intrusos u otras actividades no autorizadas.

Si se pulsa dos veces en cualquier suceso del *Registro de sucesos*, aparecerá un cuadro de diálogo similar al de la figura 5 8

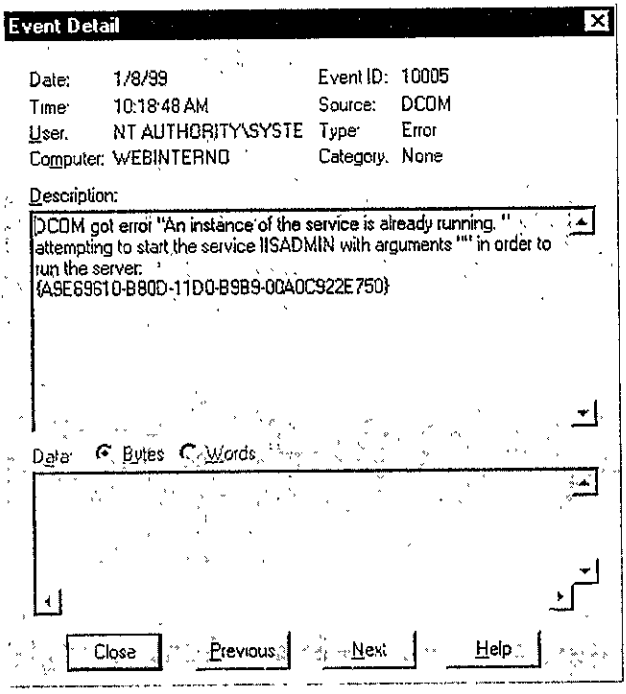


Figura 5.8 Detalles de un suceso

El cuadro anterior, suministra información sobre los eventos Por ejemplo, la hora en que se efectúo, el usuario que lo realizó, el éxito o fracaso, categoría, el ID del propio suceso, etc.

Los sucesos se clasifican según la siguiente lista.

- **Suceso Sistema**. Afecta a todo el sistema o al *Registro de auditoría*.
- **Inicio/salida de sesión**. Inicios y salidas de sesión con o sin éxito y el tipo de inicio de sesión pedido (por ejemplo, interactivo, red o servicio)
- **Acceso a objetos** Accesos con o sin éxito a objetos protegidos.

- **Uso de privilegios**. Intentos con o sin éxito de usar privilegios, incluyendo un caso especial cuando éstos se asignan.
- **La administración de cuentas** Describen cambios de alto nivel en la base de datos *cuenta de seguridad* (crear un nuevo usuario o cambiar una cuenta de usuario)
- **Cambio de plan** Describen cambios de alto nivel en un plan de seguridad, como la asignación de privilegios o cambios en la política de auditoría
- **Rastreo detallado**. Los sucesos que suministran rastreo detallado de las actividades del sujeto (usuario o proceso).

5.7.3 Protección del sistema de auditorías

Se debe tener cuidado y proteger los archivos de auditoría que están almacenados en el directorio *systemroot\System32\CONFIG*; sus nombres se muestran a continuación.

- **APPEVENT.EVT** Registro de sucesos en aplicaciones.
- **SECEVENT.EVT**. Registro de sucesos de seguridad.
- **SYSEVENT.EVT** Registro de sucesos del sistema.

Un administrador tramposo podría realizar actividades y luego borrar los archivos para cubrir sus huellas. También es posible, pero muy difícil, que cambie apuntes en los archivos. Un escenario más probable es que alguien simplemente los borre

5.7.4 La cuenta del auditor ficticio

En algunos sistemas operativos como *Novell NetWare*, existe una cuenta de *Auditor* separada de la cuenta del *Administrador*. Una vez que se asigna un auditor, esa persona puede registrar todas las actividades del Administrador y tiene control total sobre los registros de auditorías. El Administrador no puede tocar la cuenta del auditor ni los registros de auditorías. Por tanto, todas las actividades del Administrador pueden ser rastreadas por un Auditor independiente

Windows NT no tiene tal cuenta de *Auditor*, y para crear una, se necesita tratar la cuenta *Administrador* como cuenta de *Auditor*. Todos los demás administradores deben ser asignados a grupos administrativos de menor nivel, tales como *Operadores de cuentas* y *Operadores de impresión*. No se recomienda utilizar los grupos *Administradores u Operadores de servidores* porque cualquiera que sea miembro de estos grupos puede cambiar o borrar los registros de auditoría. Sólo el Administrador, que será ahora el Auditor, tendrá estos derechos y

permisos permitidos a esos grupos. Los pasos básicos recomendados para crear un auditor son los siguientes:[10]

- Designar dos o tres personas como Auditores.
- Renombrar la cuenta *Administrador* a *Auditor* o algún nombre difícil para evitar su detección
- Quitar a todos los miembros de los grupos *Administradores* y *Operadores de servidores* y reasignarlos a grupos de administración personalizados para que no puedan borrar o cambiar *Registros de auditorías.*
- Incluir a los nuevos Auditores en el servidor.
- En el campo *Contraseña*, hacer que el Auditor 1 introduzca su contraseña, luego se escribirá en una tarjeta marcada con un 1 y se cerrará en un sobre El sobre irá eventualmente a una persona de confianza
- Repetir lo anterior con los otros Auditores.
- Una vez que la nueva contraseña esté introducida, iniciar la sesión bajo una nueva cuenta y comprobar la configuración.

[10] SHELDON, Tom *Manual de Seguridad de Windows NT* McGRAW-HILL pag 266

5.8 DESEMPEÑO DE LA RED EN SICORI

Se ha llegado al final del desarrollo de esta investigación. En este capítulo se dieron las herramientas necesarias para monitorear fallas, errores y accesos remotos que garantizan el buen funcionamiento de una administración centralizada, empleando Windows NT. Todas estas herramientas son empleadas actualmente por SICORI, y éstas le permiten generar estadísticas para la toma de decisiones.

Inicialmente, la información que viajaba a través de la red era lenta, muchas veces no llegaba a su destino, y continuamente había caídas en la red porque ésta se saturaba demasiado. Esto se debía principalmente a la falta de control en los accesos y compartición de los recursos; llevando a la necesidad de crear un plan de seguridad, el cual implicó un aumento en la velocidad en tiempo de respuesta, disminución del tráfico en la red, y transmisión de información más rápida y segura

Para corroborar el buen funcionamiento de la red, continuamente se hacen monitoreos en cuanto a rendimiento de los recursos que utiliza NT, acceso de los usuarios, manejo de información, tráfico en la red, etc. Esto comprueba, que los accesos indebidos y pérdida de información han disminuido notablemente, y que el cambio en la administración de los recursos de la red implementando controladores de dominio resultó funcional para SICORI

Apróximadamente, la seguridad inicial en SICORI era de 45 %; actualmente ha incrementado a un 85%. Esto se ve reflejado en mejores condiciones de trabajo para el departamento; obteniendo mayor rápidez, calidad y eficacia en la elaboración y venta de sus productos.

CONCLUSIONES

Al final de cada uno de los capítulos, se han ido planteando las necesidades que orillaron a SICORI a contemplar la elaboración de una estrategia de seguridad corporativa, la cual debia de considerar la identificación de amenazas, riesgos, vulnerabilidades, y una evaluación de los impactos y costos organizacionales.

Con la elaboración de este proyecto, fue posible la evaluación de los diferentes servicios de red que se determinaron los índices de integridad, confiabilidad, seguridad, manejo y organización de la información y de los usuarios, que Windows NT Server y Workstation ofrecen. Al igual que se estudiaron las necesidades de los diferentes grupos de trabajo del departamento, para poder otorgar privilegios en el uso de los recursos del sistema.

Gracias al desarrollo de este proyecto, se han reducido al máximo los accesos indebidos a la red, pérdida de información, mal uso de recursos compartidos; y así se ha elevado la calidad en la administración de usuarios e información en SICORI.

La construcción de Grupos Globales de trabajo administrados por un controlador de dominio en una plataforma Windows NT, ha ayudado al departamento para:

- Llevar una administración de usuarios centralizada.
- Proporcionar los requerimientos en accesos remotos.
- Dar permisiones en cuentas de usuarios, para lograr seguridad de los recursos en la red.
- Lograr que el manejo de la información sea integro y seguro
- Realizar monitoreos de auditorias para detectar fallas, errores, intrusos en la red, etc., que permitirán rastrearlos, detectarlos, así como generar estadísticas reales

En la implantación del controlador de dominio, no se encontraron problemas criticos, más bien se presentaron algunas deficiencias en equipos, en cableado de la red, en configuraciones de software, etc., que fueron solucionados muy fácilmente Gracias a que el controlador de dominio configurado fué el adecuado, se pudieron desarrollar técnicas de seguridad para todos los usuarios de SICORI; entre estas técnicas se encuentran: estandarización del login de usuario, permisos

y privilegios para el manejo de cierta información, independencia de los recursos de cada área de trabajo, políticas en las cuentas de usuarios, etc.; y con el monotoreo de estas técnicas se garantiza un eficiente desempeño de los recursos de la red.

Se puede apreciar que no sólo basta con tener herramientas administrativas de seguridad; sino que es necesario saberlas utilizar para aprovechar su máximo rendimiento. Y por más políticas y sistemas de seguridad se tengan, si no son respetadas de nada sirven

Finalmente, se considera que la realización de este proyecto, garantiza un ambiente seguro, amigable, rápido, de fácil manejo, y eficiente para todos los usuarios que existen en SICORI. Al igual que puede servir de base a otras empresas u organizaciones que quieran obtener un efecto similar en su administración.

GLOSARIO

Adaptador de Interfaz. En comunicaciones, un dispositivo que conecta la computadora a la terminal de una red

API (Application Program Interface) Interfaz de programa de aplicación. Lenguaje y formato utilizados por un programa para comunicarse con otro. También puede incluir los comandos utilizados para interrumpir a la computadora con el fin de llamar la atención a otro programa Un API utilizado en comunicaciones se llama protocolo.

ASCII (American Standard Code for Information Interchange) Código Americano Estandard para Intercambio de Información. Código binario de datos que se usa en comunicaciones, en la mayor parte de las minicomputadoras y en todas las computadoras personales. ASCII es un código de 7 bits que permite 128 combinaciones posibles de caracteres, de las cuales las primeras 32 se usan para control de impresión y transmisión.

ATM (Asynchronous Transfer Mode) Modo de Transferencia Asíncrona. Red estándar para transmitir a alta velocidad por medio de fibras ópticas Utiliza un paquete de 53 bytes de longitud fija para datos

Backup. Hacer una copia de seguridad, respaldar. Hacer una copia de datos importantes para su seguridad en un medio de almacenamiento diferente al que se encuentran.

BIOS (Basic Input Output System) Sistema Básico de Entrada y Salida. Conjunto de rutinas de software que contienen las instrucciones detalladas para activar los periféricos conectados al computador. En las computadoras personales IBM, el BIOS reside en el chip de memoria de sólo lectura (ROM) y acepta requerimientos de entrada y salida desde el sistema operativo y desde los programas de aplicación.

Bit (BInary digiT) Dígito Binario. Es la unidad más pequeña de información, puede tomar el valor binario (1 ó 0) En la computadora, un bit es físicamente una celda de memoria (constituida por transistores o un transistor y un condensador), un punto magnético en un disco o una cinta, o un pulso de alto o bajo voltaje viajando a través de un circuito

Byte. La unidad común de almacenamiento en computación, desde computadoras personales hasta macrocomputadoras. Se compone de ocho dígitos binarios (bits). Puede agregarse un noveno como bit de paridad, para comprobación de errores. Un byte contiene el equivalente de un solo carácter, tal como la letra A, el signo $,

o el punto decimal En cuanto a los números, un byte puede contener un solo dígito de 0 a 9 (decimal), dos dígitos numéricos (decimal empaquetado) o un número entre 0 y 255 (números binarios).

Caballo de Troya. Es similar a un virus pero contamina un sistema simulando ser algún otro programa.

Cable Coaxial. Un cable de alta capacidad utilizando en comunicaciones y video, generalmente llamado *co-ax*. Contiene un alambre aislado, sólido o multifilamento, que está rodeado por una pantalla sólida o de malla trenzada, bajo una cubierta exterior. El revestimiento exterior de teflón para protección contra incendios es opcional.

Cache. Una sección reservada de la memoria que se utiliza para mejorar el rendimiento. Un cache de disco es una porción reservada de la memoria normal, o memorias adicionales en la tarjeta controladora del disco. Cuando el disco es leído, se copia un gran bloque de datos en el cache. Si los requerimientos de datos subsiguientes pueden ser satisfechos por el cache, no se necesita el empleo de un acceso a disco, el cual es más lento. Si el cache es utilizado para escritura, los datos se alinean en memoria y se graban en el disco en bloques más grandes.

CD ROM (Compact Disc Read Only Memory) Memoria de Solo Lectura en Disco Compacto. Un formato de disco compacto que se utiliza para almacenar texto, gráficos y sonido estereofónico de alta fidelidad. Es prácticamente el mismo disco que un CD de música, pero usa pistas distintas para los datos Un reproductor musical de CD no puede reproducir discos CD ROM, pero un reproductor de CD ROM puede reproducir discos CD, y tiene enchufes para conectarlo a un amplificador y/o auriculares. Un lector de CD ROM está cableado y controlado por una tarjeta que se enchufa en una de las ranuras de expansión de la computadora. Los CD ROM pueden almacenar más de 600 MB de datos, lo que equivale a aproximadamente 250 000 páginas de texto o 20 000 imágenes de resolución media.

CISC (Complex Instruction Set Computer) Computadora de Conjunto de Instrucciones Complejas. Computadoras que poseen un conjunto de instrucciones muy extenso. Las máquinas CISC tienen de doscientas a trescientas instrucciones que están grabadas en microcódigo.

Chat Mode - Modo Charla. Opción en comunicaciones que permite teclear mensajes de un usuario a otro usuario (remoto) . Cada pulsación de tecla se transmite a medida que se va tecleando el mensaje.

Cliente/Servidor. En una red de comunicaciones, el cliente es la máquina solicitante y el servidor es la máquina proveedora Esto implica que existe un software especializado en ambos extremos. Por ejemplo, en un sistema de base

de datos para trabajar en red, la interfaz de usuario reside en la estación de trabajo y las funciones de almacenamiento y recuperación residen en el servidor.

Compilador. Software que traduce lenguajes de programación de alto nivel, como COBOL y C, en lenguaje máquina. Un compilador habitualmente genera en primer lugar lenguaje ensamblador y a continuación traduce este lenguaje a lenguaje máquina. Convierte un lenguaje de alto nivel a un juego de órdenes y un texto en una representación de muy bajo nivel que pueda ejecutarse.

Computadora Híbrida. Es una computadora digital que procesa señales analógicas que han sido convertidas a forma digital. Se utiliza en control de procesos y en robótica

Conmutador. Trueque, cambio o permuta que se hace de una cosa por otra.

Corporativo. Perteneciente o relativo a una corporación (cuerpo, comunidad).

CPU (Control Processing Unit) Unidad Central de Procesamiento. También llamada el procesador, está constituída por la Unidad de Control y la Unidad de Almacenamiento. Es el cerebro de la computadora, organiza y administra todos sus recursos e información. La CPU de una computadora personal está contenida en un microprocesador único La CPU de una minicomputadora está contenida en una o varias tarjetas de circuito impreso. La CPU de una macrocomputadora está contenida en muchas tarjetas de circuito impreso.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Sensor de Portadora de Accesos Múltiples / Detección de Colisiones. Es un método de acceso en las comunicaciones de banda base que emplea una técnica de detección de colisiones. Cuando un dispositivo trata de ganar acceso a la red, verifica si la misma está libre; si no lo está, espera una cantidad aleatoria de tiempo antes de intentarlo nuevamente. Si la red está libre y dos dispositivos tratan de ganar acceso exactamente al mismo tiempo, ambos se retractan para evitar una colisión y luego cada uno de ellos espera una cantidad aleatoria de tiempo antes de reintentarlo.

DARPA (Defense Advanced Research Projects Agency) Agencia de Proyectos Avanzados de Investigación para la Defensa. Se trata de una Agencia de Investigación del Departamento de Defensa de Estados Unidos de America.

DCOM (Distributed Component Object Model) Componentes Distribuidos de Modelos de Objetos. Es un sistema de objetos de software diseñado para volverse a usar y para reemplazarse, en teoria permite distribuir procesos a través de computadoras múltiples proporcionando la infraestructura de comunicaciones basada en objetos.

DDE (Dynamic Data Exchange) Intercambio Dinámico de Datos. El protocolo de mensajes de Microsoft Windows que permite que los programas de aplicación pidan e intercambien los datos automáticamente. Un programa en una ventana puede interrogar a un programa en otra ventana utilizando el protocolo DDE.

Dedicado. Es un servicio que no es compartido por otros usuarios y organizaciones.

Demodulación. Reconvertir una señal modulada a su forma original, extrayendo los datos de la frecuencia portadora.

DES (Data Encryption Standard) Estándar de Cifrado de Datos. Es una técnica de cifrado estándar de NIST que embrolla los datos en un código impenetrable para la transmisión en una red pública. Usa un número binario como clave de cifrado que ofrece más de 72 000 000 000 000 000 de combinaciones. El número, que puede ser elegido al azar para cada transmisión, es usado como un patrón para convertir los bits en ambos extremos de la transmisión.

Dirección IP. Cada dirección IP define el ID de la red y el ID del Host. Cada host TCP/IP está identificado por una dirección IP lógica Una dirección IP única es requerida por cada host y componente de la red que se comunica a través de TCP/IP. Tienen 32 bits formados por 4 campos de 8 bits separados por comas; cada campo puede tener un valor comprendido entre 0 y 255.

Disco Duro. Es un disco magnético hecho de metal y cubierto con una superficie de grabación magnética. Los discos duros vienen en variedades removibles y fijas que contienen desde 10 hasta cientos de megabytes. Es un medio masivo de almacenamiento de información.

DNS (Domain Naming System) Sistema de Nombres de Dominios. Sistema de direccionamiento de correo electrónico utilizado en redes como Internet y Bitnet.

Dominio. Es un grupo lógico de recursos de redes diseñado para facilitar la administración centralizada Este puede contener servidores, estaciones de trabajo, gateways, cuentas de usuarios en cada server, etc.

DOS (Disk Operating System) Sistema Operativo en Disco. (1) La denominación genérica de un sistema operativo **(2)** Un sistema operativo monousuario para las series PC, PS/1 y PS/2 de IBM Desarrollado por Microsoft. El DOS es a veces denominado PC-DOS, para diferenciarlo del MS-DOS, la versión de Microsoft para las PC no IBM Ambos productos son prácticamente idénticos y a ambos se les llama DOS.

DR DOS. Sistema operativo compatible con DOS de Digital Research, que destaca por sus características avanzadas y facilidad de uso La versión 5.0 incluye un programa pequeño de instalación, ayuda incorporada, protección de palabras

reservadas (de paso), caché de disco, transferencia automática de archivos en serie, capacidad de almacenaje, controladores en memoria alta y una opción de interfaz gráfica opcional. La versión 6 0 incluye compresión automática de archivos que dobla la capacidad del disco duro

Driver (controlador, conductor). También llamado *device driver* (controlador de dispositivos), es una rutina de programa que contiene las instrucciones necesarias para controlar la operación de un dispositivo periférico. Los controladores contienen información detallada acerca de los dispositivos que manejan; por ejemplo, la cantidad de sectores por pistas o el número de líneas de resolución en pantalla. Contienen el código de máquina preciso para activar todas las funciones de cada dispositivo

DriveSpace. Es un programa que proporciona una interfaz de usuario fácil de usar, basada en menús para configurar y trabajar con unidades comprimidas.

ELS NetWare (Entry Level System) Sistema a Nivel de Entrada. Fue el primer sistema de igual a igual (peer-to-peer) de Novell que soporta hasta ocho estaciones de trabajo y ha sido reemplazada por *NetWare Lite*.

Executive (Ejecutivo). Es un núcleo que se ejecuta en modo privilegiado (kernel) dentro de la arquitectura de Windows NT.

FAT (File Allocation Table) Tabla de Asignación (distribución) de Archivos. La parte del sistema de archivos del DOS y OS/2 que lleva la cuenta de dónde están almacenados los datos en un disco. Es una tabla con una entrada para cada "cluster " (cúmulo) en el disco, y la tabla completa está duplicada. El directorio, el cual contiene identificación del archivo (nombre, extensión, fecha de última actualización, etc.) apunta a las entradas de la FAT donde comienzan en los archivos. Si un archivo ocupa más de un "cluster", esa entrada apunta a otra entrada y así sucesivamente Si un "cluster" se daña, su entrada correspondiente en la FAT se marca y no se usa nuevamente.

Fibra Optica. Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz Las fibras ópticas poseen capacidades de transmisión enormes, del orden de miles de millones de bits por segundo Además, a diferencia de los pulsos eléctricos, los impulsos luminosos no son afectados por interferencias causadas por la radiación aleatoria del ambiente

Frame Relay. Protocolo de conmutación de paquetes de alta velocidad que proporciona una transmisión más rápida que X.25. Es más adecuada para la transferencia de datos y de imágenes que para la voz

FTP (File Transfer Protocol) Protocolo de Transferencia de Archivos. Es una aplicación de Internet que permite transferir archivos de una computadora a otra. Es usado para conectarse a la red, listar directorios y copiar archivos.

Gopher. Es un sistema que permite utilizar la mayoría de los recursos de Internet mediante menús, sin tener que preocuparse del uso de direcciones IP, nombres de dominio o qué programas hay que utilizar en cada caso.

Hacker. Ver Pirata Informático

HAL (Hardware Abstraction Layer) Capa de Abstración Hardware. Es una capa de abstracción de hardware que oculta "abstrae" las diferencias del hardware a las capas superiores en el modo núcleo del sistema operativo Windows NT. Con esta aproximación, los diseñadores ven diferentes tipos de hardware del mismo modo, haciendo más fácil escribir programas

Hardware. Son todos los circuitos electrónicos y dispositivos electromecánicos que constituyen el sistema de computación. Cualquiera de las partes físicas del sistema, incluyendo circuitos integrados, terminales de video, impresora, mandos de juego, y dispositivos auxiliares de memoria

Hexadecimal (hexa). Significa dieciséis, es un sistema numérico de base 16 usado como una forma abreviada de representar todos los valores posibles de un byte. El hexadecimal se utiliza para representar bytes por su uniformidad en la impresión y en la presentación por pantalla. Dos dígitos hexadecimales siempre constituyen un byte, mientras que el valor decimal de un byte puede ser un número desde uno hasta tres dígitos de longitud (0 a 255).

Host. Es la computadora central o la computadora controladora en un entorno de procesamiento en tiempo compartido o distribuido Indica el nombre y la dirección IP de una estación de trabajo determinada.

HPFS (High Performance File System) Sistema de Archivos de Alto Rendimiento. Un sistema de archivos, presentado con OS/2 versión 1.2, que maneja discos más grandes (volúmenes de 2TB; archivos de 2GB), nombres largos de archivos (256 bytes) y puede lanzar el programa por referencia a los datos como en la Macintosh. Coexiste con el sistema FAT existente.

HTML (HyperText Markup Language) Lenguaje de Marcado de Hipertexto. Se trata de un formato especial de archivos sobre el que está basada la estructura de la aplicación WWW (World Wide Web)

HTTP (HyperText Transfer Protocol) Protocolo de Transferencia de Hipertexto. Es un protocolo de Internet que suministra servicios cliente-servidor sobre redes TCP/IP Permite hiperenlaces en los documentos

IBM (International Business Machines Corporation) Corporación Internacional de Máquinas para Negocios. La compañía informática más grande del mundo. Comenzó en 1911 en la ciudad de Nueva York cuando se creó la Computing-

Tabulating-Recording Corporation (CTR) gracias a la fusión de The Tabulating Machine Corporation (la compañía de tarjetas perforadas de Hollerith en Washington), la International Time Recording Corporation (fabricante de relojes marcadores de tiempo en el estado de Nueva York), la Computing Scale Corporation (fabricante de balanzas y cortadoras de alimentos en Dayton, Ohio), y la Bundy Manufacturing (fabricante de relojes marcadores de tiempo en Poughkeepsie, N.Y). La CTR comenzó con 1200 empleados y un capital evaluado en 17 5 millones de dólares.

ID. Identificador único

IEEE (Institute of Electrical and Electronic Engineers) Instituto de Ingenieros Electricistas y Electrónicos. Es una organización de asociados que incluye ingenieros, científicos y estudiantes en electrónica y disciplinas afines. Fué fundada en 1963, y está involucrada en el establecimiento de estándares en informática y comunicaciones

Interfaz. Es una conexión e interacción entre hardware, software y usuario. Las interfaces de hardware son los conectores, zócalos y cables que transportan las señales eléctricas en un orden prescrito. Las interfaces de software son los lenguajes, códigos y mensajes que utilizan los programas para comunicarse unos con otros, tal como entre un programa de aplicación y el sistema operativo. Las interfaces de usuario son los teclados, ratones, diálogos, lenguajes de comando y menús empleados para la comunicación entre el usuario y la computadora.

Internet. Es un conjunto de redes de ámbito mundial conectadas entre sí mediante el protocolo IP.

IP (Internet Protocol) Protocolo de Internet. Parte del protocolo TCP/IP, que envía un mensaje por medio de redes.

IPX (Internet Packet EXchange) intercambio de Paquetes entre Redes. Es un protocolo de comunicaciones del NetWare de Novell que se utiliza para encaminar mensajes de un nodo a otro Los programas de aplicación que manipulan sus propias comunicaciones cliente-servidor o de igual a igual en una red Novell pueden acceder directamente al IPX o al protocolo SPX de NetWare. El IPX no garantiza la entrega del mensaje como lo hace el SPX

ISO (International Standards Organization) Organización Internacional de Estándares. Es una organización que establece estándares (normas) internacionales, fundada en 1946 en Ginebra, Suiza Se ocupa de todos los campos, excepto la electricidad y la electrónica, las cuales están ya desde antes bajo la jurisdicción de la IEC (International Electrotechnical Commission - Comisión Electrotécnica Internacional), también radicada en Ginebra. Con respecto a los estándares de procesamiento de la información, la ISO y la IEC crearon

recientemente la JTC1 (Joint Technical Committee - Comité de Conjunto Técnico) para la tecnología informática

Juke-box. Robot que controla información a través de varios discos ópticos y cintas magnéticas.

Kernel (núcleo). Es la parte fundamental de un programa, tal como un sistema operativo, que reside en memoria todo el tiempo

LAN Manager. Un sistema operativo de red de área local de Microsoft que se ejecuta como una aplicación bajo OS/2 en un servidor de archivos y soporta las estaciones de trabajo DOS y OS/2 Utiliza el protocolo Microsoft File Sharing (SMB) para archivos compartidos, el protocolo NetBIOS para su mecanismo de transporte y usa Named Pipes para comunicación interprocesos (IPC).

MBps, Mbps (MegaBytes Per Second, MegaBits Per Second). Megabytes por segundo, megabits por segundo. Es una unidad de medida utilizada en Redes de Computadoras.

MAC Y MAC PLUS. En 1984, la Macintosh fue presentada con un diseño de gabinete exclusivo: una unidad semi-portátil, como una caja, autónoma, con una pantalla incorporada de 9 pulgadas Tenía 128 K de memoria, un disco flexible, dos puertos seriales y un generador de sonido de cuatro voces.

Macintosh. Serie de computadoras de 32 bits de Apple Computer, presentada en 1984. Usa la familia de procesadores Motorola 68000, y un sistema operativo propio que simula el escritorio del usuario en la pantalla. Esta interfaz , combinada con su lenguaje de gráficos QuickDraw incorporado, ha provisto una medida de consistencia y uniformidad que es única

Mainframe - macrocomputadora. Es una computadora grande. A mediados de los años 60, las épocas antiguas de las computadoras, todas las computadoras eran mainframes (literalmente "bastidor principal"), ya que el término se refería al gabinete que contenía la CPU Aunque mainframe aún significa gabinete principal, usualmente se refiere a un gran sistema de computación y toda la experiencia asociada que va con él

MAU (Multi-station Access Unit) Unidad de Acceso a Múltiples Estaciones. Núcleo central en una red de área local de tipo anillo

Memoria. Almacenamiento de trabajo de la computadora, que físicamente es una colección de chips RAM. Es un recurso importante de la computadora, ya que determina el tamaño y el número de programas que pueden ejecutarse al mismo tiempo, como también la cantidad de datos que pueden ser procesados instantáneamente. Toda la ejecución de programas y procesamiento de datos se realiza en la memoria

Memoria Caché. Ver Caché

Memoria RAM. Ver RAM.

Microprocesador. Es una CPU en un solo chip Para funcionar como una computadora, requiere suministro de potencia, reloj y memoria. La primera generación de microprocesadores fueron los 8080 de Intel, Z80 de Zilog, 6800 de Motorola y 6502 de Rockwell Internacional; el primer microprocesador fue creado por Intel.

Minicomputadora. Es una computadora de pequeña a mediana escala que funciona como una sola estación de trabajo, o como un sistema multiusuario con cientos de terminales.

Modelo OSI (Open System Interconnection) Interconexión de Sistemas Abiertos. Un modelo de referencia que fue definido por la ISO (International Standards Organization) como un estandard para las comunicaciones mundiales. Define una estructura para implementación de protocolos en siete estratos o capas.

Modulación. Mezclar una voz o señal de datos con una portadora para transmisión en una red de comunicaciones. Los datos se modulan sobre la portadora por varios métodos, que se menciona a continuación: modulación de amplitud, en la cual la altura de la onda se cambia; modulación de frecuencia, en lo cual la frecuencia se cambia y; modulación de fase, en la cual la fase (polaridad) de la onda se cambia.

MS. Microsoft

MS-DOS (MicroSoft - Disk Operating System) Sistema Operativo en Disco de Microsoft. Sistema operativo de un solo usuario para PC, de Microsoft. Es casi idéntico a la versión de IBM, que se llama DOS, y ambas versiones se llaman DOS genéricamente.

MS-LAN Manager. Ver LAN Manager.

MS-Net. Versión de Microsoft de PC-Network, presentada en 1985.

NDIS (Network Driver Interface Specification) Especificación de Interfaces para Controladores de Red. Es una especificación de Microsoft para describir controladores independientes del hardware en el estrato de enlaces de datos (método de acceso a los medios). Cuando los protocolos de transporte se comunican con la especificación NDIS, las tarjetas de red con controladores MAC que responden al NDIS pueden ser libremente intercambiadas.

NDS (Netware Directory Service) Servicios de Directorio Netware. Se implemeta en los servidores Netware 4.x. Es un directorio en forma de árbol que define organizaciones, departamentos, usuarios y recursos en un árbol jerárquico

NFS (Network File System) Sistema de Archivos de Red. Es un sistema de archivos distribuido diseñado principalmente para ambientes UNIX

NetBEUI (NETBIOS Extended User Interface) Interfaz de Usuario Extendido de NetBIOS. Es la realización del protocolo de transporte NetBIOS en LAN Manager y LAN Server. Se comunica con las tarjetas de interfaz de red (NICs) vía NDIS (Network Driver Interface Specification - Especificación de Interfaces para Controladores de Red).

NetBIOS (Network Basic Imput/Output System) Sistema Básico de Red de Entrada y Salida. Es un protocolo de transporte para enlazar el sistema operativo de red con hardware específico. Los programas de aplicación usan NetBIOS para comunicaciones cliente/servidor.

NetWare. Es una familia de sistemas operativos de redes de Novell, que se ejecuta en PCs 286 y superiores y soporta DOS, OS/2 y estaciones de trabajo Mac, y una variedad de métodos de acceso de LANs, incluyendo Token Ring, Ethernet y Arcnet Es el programa de control de redes más usado.

NetWare 2.x (el primer NetWare 286 Avanzado). Se ejecuta en un servidor de achivos dedicado y soporta hasta 100 usuarios. Es el único programa de control en el servidor.

Novell Network. Es una red de área local que es controlada por alguno de los sistemas operativos *NetWare de Novell.*

OS/2. Sistema operativo multitarea monousuario para PCs 286 y superiores. Las versiones de 16 bits se han desarrollado conjuntamente por IBM y Microsoft. Las versiones de 32 bits se han desarrollado independientemente.

Paridad. Suma de las cifras de un byte, cuyo resultado puede ser 1 ó 0. La paridad se utiliza como patrón para el reconocimiento de fallos en los procesos de transmisión de datos.

Partición. Una parte reservada del disco o memoria que se guarda para algún propósito.

PC (Personal Computer) Computadora Personal. Son todas las máquinas que se ajustan a los estándares de IBM PC y PS/2, colectivamente, son la mayor base de computadoras instalada en el mundo. Cualquier computadora personal

PCMCIA (Personal Computer Memory Card International Association) Asociación Internacional de Tarjetas de Memoria para Computadoras Personales. Organización de compañías japonesas y de E.U.A. para estandarizar tarjetas de memoria.

Periférico. Cualquier dispositivo de hardware conectado a una computadora, como el monitor, teclado, impresora, trazador, unidad de disco o cinta, tableta gráfica, explorador, palanca de juegos, paleta y ratón

Pipe. Espacio compartido que acepta la salida de un programa para la entrada de otro En DOS o en OS/2, la orden pipe es una línea vertical (|).

Pirata Informático, Intruso Informático (Hacker). Un programador que realiza programas en lenguaje ensamblador o en lenguajes a nivel de sistemas, como C, para violar algún sistema. Persona que viola un código y obtiene ingreso ilegal a un sistema.

Plataforma. La arquitectura del hardware de un modelo particular o familia de computadoras. La plataforma es el estándar con que los diseñadores de software escriben sus programas. El término a menudo se refiere al sistema operativo incluido con el hardware

PPTP (Protocolo Punto a Punto Canalizado). Permite redes privadas virtuales multiprotocolo seguras a través de Internet. Con PPTP, los clientes pueden acceder a sus redes corporativas a través de conexiones seguras de Internet

Procesador. Igual a CPU

Procesamiento por Lotes. Ejecuta una orden o una serie de órdenes una por una.

Programa. Colección de instrucciones que indican a la computadora que debe hacer.

Protocolo. En comunicaciones, un conjunto de normas y regulaciones que gobiernan la transmisión y recepción de datos

Protocolo Punto a Punto. Es un protocolo utilizado para acceder a Internet mediante una línea telefónica y un módem de alta velocidad.

Proxy. Es un servidor de cortafuegos que controla cómo los usuarios internos acceden al mundo exterior (Internet) y cómo los usuarios de Internet acceden a la red interna

Puerto Paralelo. Un conector externo en una computadora que se usa para conectar una impresora u otro dispositivo paralelo En PCs, el puerto paralelo usa

un conector DB-25 del lado de la computadora y un conector Centronics de 36 clavijas del lado de la impresora

Puerto Serial. Conector externo de una computadora que se emplea para conectar un modem u otro dispositivo en serie El puerto serial típico usa un conector DB-25 o DB- 9

RAID (Redundance Array of Inexpensive Disk). Es una tecnología popular para preparar técnicas de discos tolerantes a fallas

RAID 1. Todos los datos de un disco son suplicados, o espejeados en otro disco (si se utilizan dos duplicadoras de disco se conoce como disk duplexing)

RAID 5. Datos e información de paridad es distribuida en varios discos, accesándolos en paralelo

RAM (Random Access Memory) Memoria de Acceso Aleatorio. Es una memoria en la que los datos pueden almacenarse temporalmente. Sobre la RAM se puede escribir y leer sin limitaciones. El contenido de la RAM desaparece cuando la computadora se apaga

RAS (Remote Acces Service) Servicio de Acceso Remoto. Es un servicio de llamadas telefónicas en red incluido en Windows NT y opcional para Windows 95. Consta de clientes y servidores.

Remoto. Distante o apartado

RISC (Reduced Instruction Set Computer) Computadora de Conjunto de Instrucciones Reducidas. Arquitectura de computadoras que ejecuta un número limitado de instrucciones El concepto es que la mayoría de los programas usan generalmente unas pocas instrucciones, y si se acelera la ejecución de esas instrucciones básicas, se mejora el rendimiento. La arquitectura RISC elimina una capa de carga operativa llamada "microcódigo", que se emplea normalmente para facilitar la agregación de nuevas y complejas instrucciones a una computadora. Las computadoras RISC poseen un pequeño número de instrucciones montadas en los circuitos de nivel inferior, que trabajan a máxima velocidad.

RPC (Remote Procedure Call) Llamada a Procedimiento Remoto. Interfaz que permite a un programa llamar a otro en una ubicación remota. Una RPC normal permite que un programa de aplicación sea utilizado sin cambios en una variedad de redes.

SAI (Sistema de Alimentación Ininterrumpida). Ver UPS.

Scanner (Digitalizador). Dispositivo que lee texto, imágenes y código de barras Los digitalizadores de texto y de código de barras reconocen las letras impresas y

los códigos de barras y los convierten en código digital, tal como el ASCII. Los digitalizadores gráficos convierten una imagen impresa en una de video (gráficos por trama) sin reconocer el contenido real del texto o las figuras.

Server (Servidor). Es una computadora compartida por múltiples usuarios, la cual constituye la central de datos en las redes locales; para ese fin, dispone de un medio grande de almacenamiento masivo, generalmente un disco duro rápido, en el cual se encuentran todos los archivos importantes para la red.

Shell. Capa exterior de un programa, que proporciona la interfaz del usuario, o medio para gobernar la computadora. Son programas agregados, creados para sistemas operativos manejados por comandos, tales como UNIX y DOS. El Shell brinda al sistema una interfaz gráfica (orientada a iconos) o manejada por menús, con el fin de facilitar su uso.

SID. Identificador de Seguridad Único

Sistema Operativo (Operating System). Software mínimo requerido para la operación básica de una computadora, el cual permite la utilización de programas de aplicación y asegura su funcionamiento. Es el primer programa que se carga (copia) en la memoria de la computadora después de que ésta sea encendida, y el núcleo central ("kernel") del mismo debe estar siempre residente en memoria.

SMB (Server Message Block) Bloque de Mensajes de Servidor. Formato de mensajes usado en el protocolo de archivos compartido Microsoft/3Com para PC Network, MS-Net y LAN Manager. Se usa para transferir solicitudes de archivos entre estaciones de trabajo y servidores, y también dentro de un servidor para operaciones internas. Cuando se transfieren a través de la red, los SMB son transportados dentro del paquete "NetBIOS network control block" (NCB - bloque de control de red).

SMTP (Simple Mail Transfer Protocol) Protocolo Simple de Transferencia de Correspondencia. Protocolo de correo electrónico empleado en las redes TCP/IP.

Software. Instrucciones para una computadora. Una serie de instrucciones que realizan una tarea en particular se llama programa o programa de software. Las dos categorías principales son software de sistemas y de aplicaciones. El software de sistemas se compone de programas de control, incluyendo el sistema operativo, software de comunicaciones y administrador de bases de datos. El software de aplicaciones es cualquier programa que procesa datos para el usuario (inventario, nómina, hoja de cálculo, procesador de texto, etc)

SPX (Sequenced Packet eXchange) Intercambio Secuencial de Paquetes. Protocolo de comunicaciones de Novell NetWare que se utiliza para comunicaciones entre procesos (interprocess communications - IPC). Garantiza

que un mensaje completo llegue intacto, y emplea el protocolo NetWare IPX como mecanismo de distribución

SSL (Socket Security Layer) Capa de Conectores Seguros. Es un protocolo que suministra un canal seguro, que sirve para reforzar la seguridad en las conexiones Web cliente-servidor.

Sun Microsystems (Sun Microsystems, Inc.). Fabricante de estaciones de trabajo de alto rendimiento, basadas en redes, fundado en 1982. Las líneas de productos Sun-3, Sun-4 y Sun 386 incluyen sistemas independientes y en red, estaciones de trabajo sin discos y servidores de archivos. Sun se ajusta a un modelo de computación informático de sistemas abiertos a lo largo de toda su línea de productos, lo cual le permite interactuar en redes de sistemas de computación de otros fabricantes. Su software Open Network Computing (cálculo de red abierta) es utilizado por más de 100 fabricantes, incluidos Apple, Digital y HP. El software Network File System (NFS - Sistema de archivo en red) de Sun, que permite la utilización común de datos a través de la red, se ha convertido en un estándar industrial.

Tarjeta Interfaz. En comunicaciones, un dispositivo que conecta la computadora a una red.

Tarjeta Madre. Placa principal de circuito impreso en un dispositivo electrónico, que contiene conectores que aceptan placas adicionales En una computadora personal, la placa base contiene el bus, los conectores (zócalos) de la CPU y del coprocesador, los conectores de la memoria, el controlador del teclado y los chips de soporte. Los chips que controlan la visualización de video, los puertos en serie y en paralelo, las unidades del ratón y de disco se pueden encontrar o no presentes en la placa base. Si no lo están, son controladores independientes que se conectan en una ranura de expansión en la placa base

TCP/IP (Transmission Control Protocol/Internet Protocol) Protocolo de Control de Transmisiones / Protocolo de Internet. Conjunto de protocolos de comunicaciones desarrollado por la Defense Advanced Research Projects Agency (DARPA - Agencia de Proyectos Avanzados de Investigación para la Defensa) para intercomunicar sistemas diferentes. Se ejecuta en un gran número de computadoras basadas en UNIX, y es utilizado por muchos fabricantes de hardware, desde los de computadoras personales hasta los de macrocomputadoras. Es empleado por numerosas corporaciones y por casi todas las universidades y organizaciones federales de los Estados Unidos. El protocolo TCP controla la transferencia de los datos, y el IP brinda el mecanismo para encaminarla.

TELNET. El protocolo TELNET proporciona una capacidad de emulación de terminal que permite al usuario interactuar con cualquier otro tipo de computadora de la red

Thread (hilo, camino). Es una transacción o mensaje en un sistema.

Trama. (1) En gráficos por computadora, es el contenido de una pantalla de datos a su espacio equivalente de almacenamiento. **(2)** En comunicaciones, es un grupo de bits que conforman un bloque elemental de datos para su transmisión por ciertos protocolos. **(3)** En inteligencia artificial, es una estructura de datos que contiene una descripción general de un objeto. La descripción proviene de conceptos básicos y de la experiencia

UNIX. Es un sistema operativo multiusuario y multitarea de AT&T que se ejecuta en una amplia variedad de sistemas de computación de micro a macrocomputadoras. UNIX está escrito en C (también desarrollado por AT&T) que es un lenguaje diseñado para programación a nivel de sistemas; y es la transportabilidad inherente al C lo que permite que UNIX pueda ejecutarse en tal cantidad de computadoras diferentes.

UPS (Uninterruptible Power Supply) Sistema de Alimentación Ininterrumpida. Energía de seguridad para un sistema de computación cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos; los necesarios para apagar la computadora de manera ordenada. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros.

VINES (Virtual Networking System) Sistema de Redes Virtuales. Un sistema operativo de red basado en el System V de UNIX, de Banyan Systems, que se ejecuta en servidores basados en DOS y OS/2 Proporciona una interconexión por red de PCs, minis, macrocomputadoras y otros recursos de computación, proporcionando información compartida a través de organizaciones de tamaño ilimitado.

Volumen. (1) Una unidad de almacenamiento físico, como un disco duro, disco flexible, cartucho de discos o carrete de cinta. **(2)** Una unidad de almacenamiento lógico que abarca una cantidad de unidades físicas.

VPN (Virtual Private Network - Redes Virtuales Privadas). Son túneles encriptados a través de Internet para transmitir información privada entre localizaciones de la red.

Web. Ver WWW.

Windows. Entorno operativo para gráficos de Microsoft que se integra con DOS. Proporciona un entorno de sobremesa similar al Macintosh, en el cual cada aplicación activa se visualiza en una pantalla movible y redimensionable sobre la pantalla Con objeto de usar todas las funciones del Windows, las aplicaciones

deben escribirse específicamente para él. Sin embargo, Windows también ejecuta aplicaciones de DOS y se puede usar como el entorno operativo desde el que se lanzan todos los programas

Workstation - Estación de Trabajo. (1) Micro o minicomputadora para un único usuario, de alto rendimiento, que ha sido especializada para gráficos, diseño asistido por computadora, ingeniería asistida por computadora o aplicaciones científicas **(2)** En una red de área local, una computadora personal que sirve a un único usuario, a diferencia de un servidor de archivos, que sirve a todos los usuarios de la red **(3)** Cualquier terminal o computadora personal

WWW (World Wide Web). Red de Área Mundial. Es un potente sistema utilizado para localizar y acceder a las fuentes de información de Internet. Es un protocolo que permite a los usuarios hacer que su información sea fácilmente accesible para los otros usuarios.

X.25. Estándar CCITT (1976) para los protocolos y formatos de mensajes que definen la interfaz entre una terminal y una red de conmutación de paquetes.

BIBLIOGRAFIA

LIBROS

- AMPLIAR Y REPARAR SU PC
  Schüller Ulrich, Veddeler Hands-Georg.
  Editorial Computec-Marcombo.
  Grupo Editor Alfaomega, Barcelona, España, 1996.
  Segunda edición.

- FUNDAMENTOS DE PROGRAMACION
  Peñaloza Romero Ernesto.
  UNAM Campus ARAGON, Primera Edición México 1994.

- HANDBOOK OF INFORMATION SECURITY MANAGEMENT
  Zella G. Ruthberg, Harold F Tipton.
  Editorial Auerbach, EUA 1994.

- INFORMÁTICA: PRESENTE Y FUTURO.
  Donald H Sanders, Roberto Luis Escalona.
  Traducción México 1992.
  McGRAW-HILL Interamericana de México.

- INTERNET FIREWALLS AND NETWORK SECURITY
  Siyan, Karanjit.
  Editorial New Riders Publishing Indianapolis, Ind, 1995.

- INTERNET SECURITY WITH WINDOWS NT
  Mark Joseph Edwards.
  Editorial Duke Press, EUA agosto 1997

- LA DIRECCIÓN Y LA SEGURIDAD DEL ORDENADOR
  Tarbot, J.R.
  Editorial Hispano Europea, Barcelona, 1983.

- MANUAL DE SEGURIDAD PARA PC Y REDES LOCALES
  Cobb, Stephen
  Editorial McGraw-Hill Madrid, 1994.

- MICROSOFT EDUCACION Y CERTIFICACION.
  Administering Microsoft Windows NT 4.0.
  Student Lab.
  Manual Microsoft.

- MICROSOFT EDUCACION Y CERTIFICACION.
  Administering Microsoft Windows NT 4.0
  Student Workbook
  Manual Microsoft.

- MICRSOFT WINDOWS NT 3.5: GUIDELINES FOR SECURITY, AUDIT, AND CONTROL
  (Microsoft Professional Editions).
  Editorial Microsoft Press, EUA febrero 1, 1995

- PCWEEK MICROSOFT WINDOWS NT SECURITY: SYSTEM ADMINISTRATOR'S GUIDE
  Nevin Lambert, Manish Patel, Steve Sutton.
  Editorial Ziff Davis Pr, EUA junio 1997.

- REDES LOCALES Y TCPI/IP
  Raya Cabera José Luis, Raya Pérez Cristina.
  Computec ra-ma.
  Grupo Editor Alfaomega, Madrid España 1995.

- WINDOWS NT ADVANCED SERVER.
  Remote Access Service
  Manual Microsoft.

- WINDOWS NT NETWORK SECURITY
  Matthew Strebe, Charles Perkins, and Michael Moncur
  Editorial Sybex Network Press, EUA

- WINDOWS NT SECURITY
  Nik Okuntseff, Nikolaio Okountsev.
  Editorial Miller Freeman Books, EUA septiembre 1997.

- WINDOWS NT SECURITY: A PRACTICAL GUIDE TO SECURING WINDOWS NT SERVERS AND WORKSTATIONS (MCGRAW-HILL NCSA GUIDES)
  Charles B. Rutstein
  Editorial Computing McGraw-Hill, EUA abril 1997

- WINDOWS NT SECURITY GUIDE
  Stephen A. Sutton.
  Editorial Addison-Wesley Pub Co, EUA diciembre 1,1996.

- WINDOWS NT SECURITY HANDBOOK
  Thomas Sheldon.
  Editorial Osborne McGraw-Hill, EUA noviembre 1,1996

- WINDOWS NT SERVER 4 SECURITY HANDBOOK
  Lee Hadfield, Dave Hatter, Dave Bixler, David Hatter.
  Editorial Que, EUA julio 1997.

- WINDOWS NT SERVER 4· SECURITY, TROUBLESHOOTING, AND OPTIMIZATION
  Wayne Dalton, Scott Fuller, Bob Kolosky, Joel Millecan, Nachenberg, Chris Goggans.
  Editorial New Riders Publishing, EUA enero 1997.

- WINDOWS 95 AND NT 4.0 REGISTRY & CUSTOMIZATION HANDBOOK
  Jerry Honeycutt, Bernard Farrell, Rich Kennelly, Jerry Millsaps.
  Editorial Que Corp, EUA enero 1997.

REVISTAS

- BYTE México, Como Dominar las Grandes Redes
  Velocidad Sobre NT
  Monroy Niebla, Quina
  México 1996, pag. 40-50

- Noti Comper, Conectividad y Sistemas Abiertos
  Windows NT Su Soporte a Red
  Castillo, Ulises
  México 1993, pag. 32-38

- PC Computing, Superguía de Windows 95/NT
  Superguía Anual de Windows
  Payró Ogarrio, Pablo
  México 1996, pag. 46-75

- ¿SERÁ WINDOWS NT EL SISTEMA OPERATIVO DEL FUTURO?
  PC MAGAZINE en español.
  Rick Ayre y Robin Raskin.
  Enero de 1994

- WINDOWS NT EN LA CUENTA REGRESIVA.
  PC/TIPS BYTE.
  Areli Gaona Castillo.
  septiembre de 1992.

- WINDOWS NT: ¿TRANSFORMARA EL MERCADO?
  Revista PERSONAL
  Computing México.
  Gina Pfeffer.
  Febrero de 1994

DIRECCIONES DE INTERNET

http://netecsa.com/bwfs/introseguridad/default html
http://www rediris.es/rediris/boletin/35/enfoque2 html
http://www aicrag cl/articulos/arti_001 htm http //www aicrag cl/articulos/arti_001 htm
http://www aui.es/biblio/libros/mi96/p14.htm
http.//www sistecol com@coldatos/esquema.htm
http //arraquis.dif.um.es/~rafa/8trab htm
http://www magenta cl/Servicios/presentaciones_powerpoint_de_mag.htm
http://www rgb co uk/wpg/firewall html
http //all.net/journal/netsec/top html
http.//www.rotativo.com/timagazine/cfm/secciones/seguridad cfm
http://tiny uasnet mx/prof/cln/ccu/mario/REDES/Lan.html
http //www.dcc.uchile cl/~osalazar/clase2/node2.html
http://www.uady.mx/~educacio/servicios/ceprosed/rcnos html
http //www tlogic com/double.html
http.//www.lesley.edu/faculty/;seaman/security html
http.//enete fie.us.es