UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

LICENCIATURA EN SISTEMAS COMPUTACIONALES

"ADMINISTRACIÓN DE REDES BAJO EL ENTORNO DE WINDOWS XP"

M O N O G R A F Í A

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTACIONALES

P R E S E N T A:

P.L.S.C. JENNY HERNÁNDEZ ESCOBAR.

ASESOR: I.S.C. EDGAR OLGUÍN GUZMÁN.

PACHUCA DE SOTO, HGO., OCTUBRE 2006.

INDICE TEMÁTICO

CAPÍTULO II

ADMINISTRACIÓN DE REDES CON WINDOWS XP PROFESIONAL.

ÍNDICE DE FIGURAS

I N T R O D U C C I Ó N

Las redes fueron creadas para fomentar la autodependencia, intercambiar información, cambiar la sociedad, mejorar la productividad, la situación laboral y así compartir recursos.

La administración de redes se esta convirtiendo en una creciente y compleja tarea debido a la variedad de tipos de red y a la integridad de diferentes medios de comunicación, a medida que las redes se vuelven mas grandes y mas complejas, el costo de la administración aumenta, para ello son necesarias herramientas automáticas para dar el soporte requerido por el administrador, recolectando información acerca del estatus y el comportamiento de los elementos de la red.

Con la administración de redes bajo el entorno de Windows XP, se pretende dar a conocer a la administración de redes desde un panorama de forma general; así como también describir la administración de redes en el sistema operativo Windows XP Profesional (SP2), sus utilerías administrativas, sus formas de seguridad y la configuración de una red dentro del mismo sistema operativo.

J U S T I F I C A C I Ó N

Es indiscutible la importancia que tienen las redes de computadoras en las empresas modernas. Se aprende a instalar, configurar y administrar una red. Hoy en día las empresas trabajan conectadas en red, esto se debe a la rapidez que se necesita para transmitir información, una red posee muchos beneficios como realizar un trabajo en una máquina y abrirlo en otra, pasar información de una a otra máquina sin utilizar ningún tipo de periférico externo, etc.

Actualmente, las redes son utilizadas por muchas personas, lo cual determina que han crecido mucho. Estas redes pueden ser empleadas para varios propósitos por personas con intereses diferentes. Es por eso que se crea la necesidad de tener una mejor seguridad en los sistemas que dan acceso a la información flexible en estas redes y sobre la información que se transmite a través de las redes de comunicación.

Esto hace que el área de administración de redes tenga una importancia que anteriormente no tenia y justifica ampliamente que se desarrollen metodologías para la implementación de sistemas de administración en redes, e inclusive que se desarrolle investigación en estas áreas.

La administración de la red o redes es la forma de aprovechar al máximo los recursos tanto físicos como internos de la red, manteniéndola operativa y segura para los usuarios y que mejor que utilizar Windows XP Profesional SP2, para que ayude a proporcionar una base confiable que cumpla las necesidades de seguridad y confidencialidad en redes, al mismo tiempo ofrece un mejor rendimiento y facilidad de uso.

Para el Centro de Cómputo Académico del Campus Tlahuelilpan es primordial e indispensable una planeación adecuada para la administración de la red, ya que en base a una administración de red que incluya un monitoreo constante,

es posible establecer un modelo de seguridad que sirva de apoyo para satisfacer con calidad las necesidades de los usuarios del CECA.

O B J E T I V O S

OBJETIVO GENERAL:

El objetivo general de este trabajo profesional es describir la importancia de la administración de redes a través de las diferentes utilerías que nos ofrece el sistema operativo Windows XP Profesional; empleando los conocimientos en un caso de estudio, basado en las funciones del Centro de Cómputo Académico del Campus Tlahuelilpan de la UAEH.

OBJETIVOS ESPECIFICOS:

- Describir las principales funciones de la administración de redes.
- Describir como utilizar y administrar las utilerías administrativas de Windows XP Profesional.
- Identificar las posibilidades de gestión de redes que tiene el sistema operativo Windows XP Profesional.
- Establecer una fuente de consulta para tomar decisiones con respecto a la administración de redes en Windows XP Profesional (SP2).

CAPITULO 1

MARCO REFERENCIAL DE LA ADMINISTRACIÓN DE REDES.

En este capítulo se presenta una introducción a la administración de redes, dando a conocer en primer término los conceptos básicos y las operaciones que se realizan en una administración de redes.

1.1 Concepto de Administración de Redes.

Es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. [R1]

Proceso que consiste en la planeación, organización y control de las actividades que envuelven el funcionamiento de los datos dentro de una organización. [R2]

Es un servicio que utiliza una gran variedad de herramientas, aplicaciones y dispositivos, para ayudar a los administradores de la red a supervisar y mantener las redes. [B1]

1.1.1 Concepto de Administrador de Red.

Es la persona responsable de la configuración y administración de la red. El administrador generalmente configura la red, asigna contraseñas, permisos y ayuda a los usuarios. [B3]

Es la persona responsable de supervisar y controlar el hardware y software de una red; incluye el control del esquema de seguridad y administración de procesos y aplicaciones en red.

Las responsabilidades del administrador de la red se dividen en siete áreas:

1. Responder a las necesidades de los usuarios.
2. Diseñar la instalación, incluyendo el cableado, el lugar donde se van a instalar las estaciones, los derechos de acceso, los interfaces de los usuarios, y la seguridad.
3. Configurar la red al ponerla en marcha y siempre que se haga algún cambio.
4. Mantener y administrar la red.
5. Diagnosticar problemas y efectuar reparaciones sencillas.
6. Evaluar el rendimiento de la red.
7. Planificar los cambios a corto y largo plazo. [B3]

1.2 Objetivos de la Administración de Redes.

- ✓ Mantener operativa la red satisfaciendo las necesidades de los usuarios.
- ✓ Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- ✓ Hacer uso eficiente de la red y utilizar mejor los recursos.
- ✓ Asegurar el funcionamiento de la red, protegiéndola contra el acceso no autorizado, impidiendo que personas ajenas puedan entender la información que circula en ella.
- ✓ Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios. [B1]

1.2.1 Razones por las cuales la administración de redes es importante y difícil.

- ✓ Se mezclan diversas señales como voz, datos, imágenes y graficas.
- ✓ Se interconectan varios tipos de redes de acuerdo a su cobertura: LAN, MAN y WAN.
- ✓ El empleo de varios sistemas operativos.
- ✓ Se utilizan diversas arquitecturas de red.

1.3 Principales Operaciones de la Administración de Red:

- ✓ **Administración de fallas.** Maneja las condiciones de error en todos los componentes de la red, bajo las siguientes fases:
  - Detección de fallas.
  - Diagnostico del problema.
  - Solución de problemas y mecanismos de recuperación.
  - Seguimiento y control.
- ✓ **Control de fallas.** Esta operación tiene que ver con la configuración de la red, así como el monitoreo continuo de todos sus elementos.
- ✓ **Administración de cambios.** Comprende la planeación, la programación de eventos e instalación.

- ✓ **Administración del comportamiento.** Asegura el funcionamiento óptimo de la red, lo que incluye: el número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.
- ✓ **Servicios de contabilidad**. Este servicio provee datos que van a la cargo por uso de la red, como:

    - Tiempo de conexión y terminación.
    - Número de mensajes transmitidos y recibidos.
    - Nombre de mensajes transmitidos y recibidos.
    - Razón por la que termino la conexión.

- ✓ **Control de Inventarios.** Debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.
- ✓ **Seguridad.** La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados:

    - Identificación y autentificación del usuario.
    - Autorización de acceso a los recursos.

- ✓ **Confidencialidad.** Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía.

1.4 Arquitectura de la Administración de Redes.

Las arquitecturas para la administración de redes utilizan la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de red, utilizan un software que les permite enviar mensajes de alerta cuando se detecta algún problema. Al recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, el cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red, pero los agentes en los dispositivos que se están administrando responden a todas las verificaciones.
Los agentes son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por ultimo la ponen a disposición (de manera preactiva o reactiva) de las entidades que forman parte de los sistemas de administración de la red vía un protocolo de administración de red, como por ejemplo, SNMP (Protocolo Simple de Administración de Redes) y CMIP (Protocolo de Información de Administración Común). [B1]

Los proxies de administración son entidades que proporcionan información de parte de otras entidades.
La figura 1.1 muestra una arquitectura habitual de administración de redes.

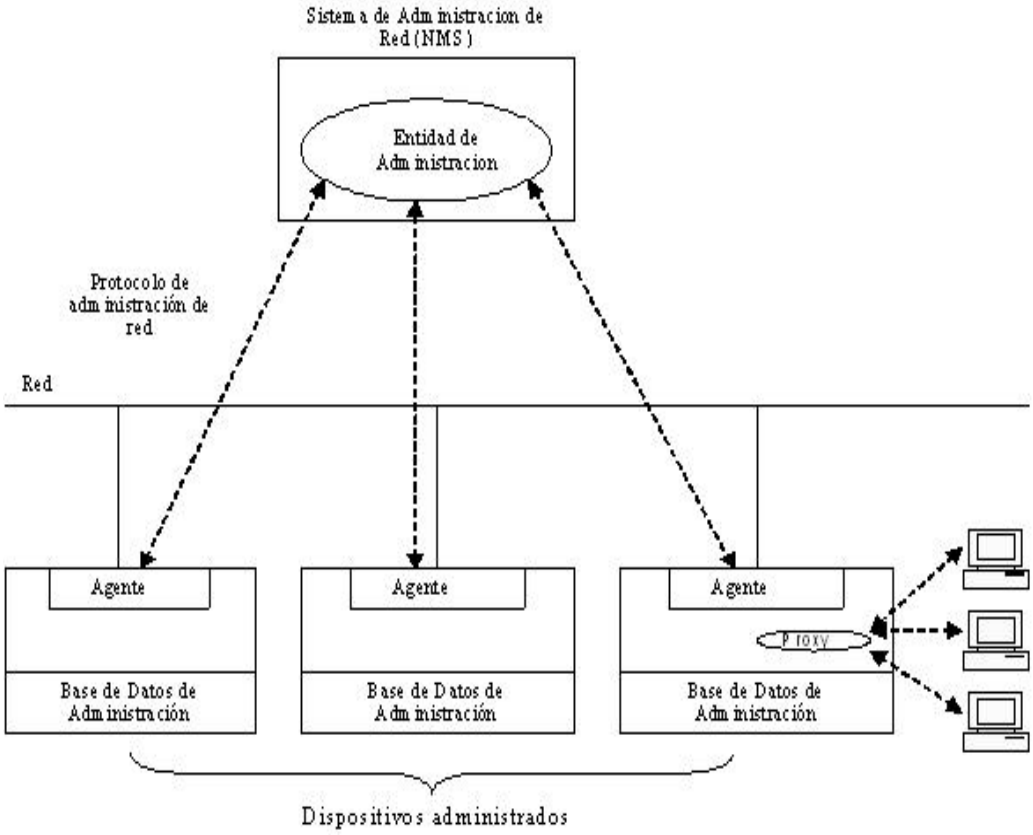


Figura 1.1 Arquitectura de la administración de Redes

1.4.1 Funciones de administración definidas por OSI.

OSI define 5 funciones de administración:

- ✓ Configuración.
- ✓ Fallas.
- ✓ Contabilidad.
- ✓ Comportamiento.
- ✓ Seguridad.

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.

La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.

La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.

La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

1.4.2 Modelo de Administración de Red de la ISO. [B1]

ISO ha contribuido en gran medida a la estandarización de las redes. Su modelo de administración de redes es de los principales para entender las funciones fundamentales de los sistemas de administración de redes. Este modelo consiste en cinco áreas conceptuales:

- Administración del desempeño.
- Administración de la configuración.
- Administración de la contabilidad.
- Administración de fallas.
- Administración de la seguridad.

1.- Administración del Desempeño. Su objetivo es medir y proveer la información disponible del desempeño de la red para mantener el funcionamiento de la red interna en un nivel aceptable.

2.-Administración de la Configuración. Su objetivo es supervisar la información de la configuración de la red y de los sistemas para rastrear y

manejar los efectos sobre el desempeño de las versiones del software y hardware de la red.

3.- Administración de la Contabilidad. Su objetivo es medir los parámetros de utilización en la red para regular apropiadamente las aplicaciones de un usuario o grupo en la red.

4.- Administración de Fallas. Su objetivo es detectar, registrar y notificar los problemas que existen en la red, para después ejecutar un proceso de corrección automática y lograr el funcionamiento óptimo de la red.

La Administración de Fallas implica:

- Primero se determinan los síntomas y se aísla el problema.
- Entonces el problema es fijo, y la solución se prueba en todos los subsistemas importantes.
- Finalmente la detección y la resolución del problema son registradas.

5.- Administración de la Seguridad . Su objetivo es controlar el acceso a los recursos de la red con respecto a las normas de consulta locales, de modo que la red no pueda ser saboteada (intencionalmente o involuntariamente) y que la información que es vulnerable no pueda ser utilizada por aquellos sin una autorización apropiada.

Los subsistemas de seguridad trabajan dividiendo los recursos de la red en áreas autorizadas y en áreas no autorizadas.

Los subsistemas de seguridad realizan varias funciones. Estos subsistemas identifican los recursos de la red que son vulnerables (incluso los sistemas, archivos y otras entidades), determinan la relación entre estos recursos y su utilización. También supervisan los puntos en los recursos de la red que son vulnerables y registran los accesos sin autorización a estos recursos. [B1]

1.5 Protocolo de Administración de Red TCP/IP.

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Protocolo Simple de Administración de Redes), que ha llegado a ser un estándar de ISO en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red.

Para hacer más eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- ✓ Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- ✓ Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas. [B6]

1.6 SNMP (Protocolo Simple de Administración de Red).

SNMP surge para resolver los problemas de administración de redes TCP/IP, debido a que el crecimiento apresurado y desmesurado de este tipo de redes ha hecho que la administración y gestión de las mismas se convierta en una labor intensa. Un caso muy particular es el de Internet, debido a su complejidad y gran tamaño. La arquitectura de este protocolo se diseñó tomando en cuenta el modelo OSI. [B1]

El protocolo sencillo de administración de red (SNMP) es el protocolo de administración de redes estándar usado en Internet. Este protocolo, define la comunicación de un administrador con un agente.

Es un protocolo de gestión de red muy utilizado.
Permite obtener: información de dispositivos de la red, memoria libre, uso de CPU, detección de errores, establecer alarmas, estado de funcionamiento.

SNMP está formado por cuatro componentes básicos:

1. **Base de datos lógica:** SNMP sigue el modelo de una base de datos lógica, en la misma se almacena información referente a la configuración, estado, error y rendimiento.
2. **Agentes:** El agente es un software, que permite el acceso a la información. Dicho agente responde a peticiones, realiza actualizaciones e informa los problemas.
3. **Administradores:** La estación de administración, contiene un software de administrador, el cual se encarga de enviar y recibir los mensajes SNMP. Además de esto existen otra serie de aplicaciones de administración que se comunican con los sistemas de red mediante el administrador.
4. **Base de información de administración:** La base de información de administración, denominada MIB, constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración. [B1]

SNMP es muy utilizado en redes TCP/IP y de intercambio de paquetes de Internet, para transportar información administrativa y comandos entre los programas de administración ejecutados por un administrador y el agente de administración de red que se ejecuta en un sistema principal o host; es decir SNMP funciona bajo TCP/IP, lo cual significa que desde un sistema central se puede gestionar cualquier computadora de una red LAN, WAN o Internet.

El SNMP define el formato y el significado de los mensajes que intercambian el administrador y el agente. En lugar de definir muchas operaciones, el SNMP utiliza el paradigma de obtención y almacenamiento. En el cual el administrador manda solicitudes de obtención y almacenamiento de valores en variables. Todas las operaciones se definen como efectos colaterales de las operaciones de almacenamiento.

1.6.1 Tipos de datos de SNMP.

SNMP maneja los siguientes tipos de datos:

- **Dirección IP***:* Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.
- **Dirección física***:* Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.
- **Contador:** Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.
- **Tabla:** es una secuencia de listas.
- **Cadena de Octetos:** Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

1.6.2 Base de datos de administración.

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto. Una variable u objeto MIB se define especificando la sintaxis, el acceso, el estado y la descripción de la misma

- Sintaxis: Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc.
- Acceso: Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.
- Estado: Define si la variable es obligatoria u opcional.
- Descripción: Describe textualmente a la variable.

1.6.3 Objetos de administración de MIB.

Grupo de Sistemas. Se usa para registrar información del sistema el cual corre la familia de protocolos.

Grupo de Interfaces. Registra la información genérica acerca de cada interfase de red, como el número de mensajes erróneos en la entrada y salida,

el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados.

Grupo de traducción de dirección. Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar.

Grupo IP. Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc.

Grupo TCP. Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual.

Grupo EGP. En este grupo se requieren sistemas (ruteadores) que soporten EGP.

1.7 Agentes y Consolas.

Los agentes y consolas son los conceptos claves en la administración de redes.

Consola: es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.

Agentes: son programas especiales que están diseñados para recoger información específica de la red. [R1]

1.7.1 Características de los agentes:

- Están basados en software frente a monitores y analizadores basados en hardware.
- Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar al rendimiento de los mismos.
- La información que recogen la almacenan en bases de datos relacionales que después son explotadas a través de las consolas.

- Los agentes son configurados de forma remota a través de la consola para su correcta operación.

1.7.2 Funciones que soportan los agentes.

- Visualizar y manipular información de la red.
- Automatizar la distribución de ficheros.
- Mantener el inventario del hardware.
- Gestión y configuración del software remoto.
- Recibir notificación de alarmas de red.
- Automatizar tareas como copias de seguridad y detección de virus.
- Monitorizar la utilización de discos y de ficheros.
- Establecer y gestionar la seguridad en la red.

1.7.3 Gestión de usuarios.

La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recursos y mantenimiento de la seguridad en los accesos a la red.

Tareas principales en la gestión de usuarios:

1. Altas, bajas y modificaciones de usuarios en la red.
2. Establecimiento de políticas de passwords (contraseñas) como su longitud, tiempo de vida, seguridad de la base de datos de passwords, etc.
3. Asignación de permisos para la utilización de recursos de red.
4. Monitorización de la actividad de los usuarios.
5. Establecimiento de políticas generales y de grupo que faciliten la configuración de usuarios.

1.7.4 Gestión del hardware.

La gestión del hardware es una actividad esencial para el control del equipamiento y sus costes asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Para evitar visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota.

Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

1. Añadir información relativa a puestos de trabajo no instalados en red.
2. Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.
3. Establecimiento de parámetros de configuración en los ficheros de configuración del Sistema Operativo.
4. Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.
5. Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc.).

En los servidores, se realiza un seguimiento de los parámetros de funcionamiento como pueden ser actividad del CPU, de los discos, espacios disponibles, número de conexiones, etc.

Este seguimiento permite analizar el comportamiento y, en su caso, detectar nuevas necesidades y adaptar las características hardware de los servidores.

1.7.5 Gestión del software.

El software de administración de red permite al administrador supervisar y controlar los componentes de una red; permite que el administrador investigue dispositivos como hosts, ruteadores, conmutadores y puentes para determinar su estado y obtener estadísticas sobre las redes a las que se conectan. El software también permite controlar tales dispositivos cambiando las rutas y configurando interfaces de red.

Las actividades relativas a la gestión de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten

el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.

De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red. Sus características particulares son:

- Obtienen su información revisando todos los discos de los puestos de trabajo en la red.
- Normalmente son capaces de identificar cientos de paquetes comerciales y se les puede añadir nuevos paquetes particulares de la empresa.
- Realizan mediciones del número de copias de un paquete que se están usando en la red de forma simultánea con objeto de comprobar su adecuación al número de licencias adquiridas.

Las tareas que se realizan en la administración de red en esta área son:

- Creación y mantenimiento del inventario de software instalado.
- Especificación y requerimiento del número de copias disponibles de los distintos paquetes.
- Seguimiento de la instalación no autorizada de software y de otros ficheros en prevención de introducción de virus.
- Autorización a los usuarios para la utilización de los paquetes de software.

La información que se suele extraer es la siguiente:

- Información general del paquete: fabricante, versión, No de licencias.
- Disponibilidad: quién usa el software, quién lo puede usar.
- Archivos que componen el paquete.
- Información adicional establecida por el administrador.

1.7.6 Distribución de archivos.

Debido a la enorme dispersión de puestos en red, la distribución de software y otros archivos se realiza mediante la utilización de agentes de distribución de archivos.

Las características de los agentes de distribución de archivos son:

- Las funciones que realizan son instalación y actualización de software, descargas y eliminación de archivos.
- Pueden aplicarse a puestos individuales o a grupos de estaciones simultáneamente.
- Tienen en cuenta los permisos de accesos de los usuarios a más de una máquina para instalar el software en cada una de las máquinas a las que se accede.

1.7.7 Monitorización de la actividad de red.

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red.

Los eventos típicos que son monitorizados suelen ser:

- Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de los cambios que se producen en el inventario de hardware.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.
- Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.

Además de los eventos, otra característica importante es la monitorización del tráfico de red:

- Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.
- Se almacenan para su posterior análisis.
- Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red. [R1]

1.7.8 Planificación de procesos.

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realice las tareas programadas en los momentos previstos.

Los agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador. Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.

1 .7.9 Protección contra virus.

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo.

La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador,

comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y archivos de los propios servidores, etc.

Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

1.7.10 Soporte de impresoras.

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red.

Las actividades relacionadas con el soporte de impresoras son dos:

1. Las relacionadas con el manejo de las impresoras por parte del administrador.
2. Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.

El modo de operar suele ser el siguiente:

1. El administrador da de alta las impresoras en la red.
2. Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.
3. El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.
4. Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.
5. El administrador a través de los agentes de impresión monitorea la actividad de las impresoras y soluciona problemas que puedan surgir.

1.7.11 Gestión del espacio de almacenamiento.

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos.

La extracción de información que realiza el agente suele ser a nivel de:

- ✓ Partición: utilización del espacio de la partición (poco nivel de detalle)
- ✓ Directorios: grado de utilización del espacio para los directorios.
- ✓ Ficheros: tamaño que ocupan los ficheros.

1.7.12 Seguridad.

La seguridad es un aspecto que afecta a todas las áreas de administración.

Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos.

Todas estas tareas son muy complejas por lo que se utiliza actualmente son políticas de seguridad. Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

1.7.13 RMON (Monitoreo Remoto).

RMON es un estándar que define objetos actuales e históricos de control, permitiendo que usted capture la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet.

Puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite que usted detecte, aísle, diagnostique, y señale problemas potenciales y reales de la red antes de que se extiendan a las situaciones de crisis.

RMON permite que usted instale las historias automáticas, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica tal como la utilización, colisiones.

CAPITUO 2

ADMINISTRACIÓN DE REDES CON WINDOWS XP PROFESIONAL.

En el presente capítulo se presenta una introducción sobre la importancia que tiene la administración de redes bajo un sistema operativo como lo es Windows XP Profesional, tratando como primer término una pequeña introducción a Windows XP.

2.1 Introducción a Windows XP.

Windows XP (cuyo nombre en clave inicial fue Whistler), fué hecho público el 25 de Octubre de 2001 por Microsoft, en Seatle, Estados Unidos. Las letras “XP” provienen de la palabra inglesa Experience (“Experiencia “, en español). [B5]

2.2 Detalles de Windows XP.

Windows XP esta basado en el código de Windows 2000 con un nuevo interfaz grafico (llamado Luna), el cual incluye características ligeramente rediseñadas. Así como también admite la especificación de la interfaz de configuración y emergía, que proporciona una administración de energía y una configuración del sistema seguras.

2.3 Historia.

Antes de XP, Microsoft producía dos líneas separadas de sistemas operativos. Una línea estaba dirigida a los ordenadores domésticos representada por Windows 95, Windows 98 y Windows Me, mientras que la otra, representada por Windows NT y Windows 2000, estaba pensada para el mercado corporativo y empresarial e incluía versiones especiales para servidores. Windows XP es el intento por parte de Microsoft de ofrecer un único sistema operativo multiuso, con el inconveniente de eliminar definitivamente el soporte para los programas basados en MS-DOS del sistema operativo. [R2]

2.4 Versiones.

Microsoft inicialmente sacó a la venta dos versiones:

- ✓ Windows XP **Home** está destinada al mercado doméstico, esta versión no tiene originalmente soporte para SMP, aunque con los Service Pack se utiliza dicha función, gracias a esto los procesadores con HT se pueden utilizar con esta versión.

- ✓ Windows XP **Professional** dispone de características adicionales diseñadas para entornos empresariales, como la autenticación por red y el soporte multiprocesador.

En Noviembre de 2002, Microsoft sacó a la venta dos nuevas versiones de Windows XP para hardware específico:

- ✓ Windows XP **Media Center Edition** para PCs especiales.

Actualmente, dichos PCs son los "HP Media Center Computer" y la serie "Alienware Navigator". "Windows XP Media Center Edition" debe ser vendido con uno de estos ordenadores y no puede encontrarse en tiendas.

- ✓ Windows XP **Tablet PC Edition** para ordenadores portátiles especiales diseñados con una pantalla táctil que admiten escritura a mano y pantallas tamaño portarretratos.

Adicionalmente, el 28 de Marzo de 2003, Microsoft hizo pública otra versión:

- ✓ Windows XP 64 Bit Edition para fabricantes cuyo destino son los procesadores AMD 64 e Intel con extensiones de 64 bits.

Tiempo después, en Junio de 2005, Microsoft hizo pública otra versión:

- ✓ Microsoft Windows XP **Starter Edition** destinado a países con habitantes con pocos recursos (donde Sistemas operativos como GNU/Linux comienzan a hacerse con un hueco del mercado) o con altos niveles de copia ilegal. Se puede considerar un Windows XP normal, con características limitadas.

Debido a una sentencia judicial de la Unión Europea, Microsoft lanzó otra versión:

- ✓ Windows XP **N Edition**: Versión Home de **Windows XP** pero sin Windows Media Player, esta versión se distribuye únicamente en la Unión Europea por problemas legales. [R3]

2.5 Actualizaciones.

Cada cierto tiempo, Microsoft libera unos paquetes denominados Service Packs (Paquetes de servicio), en el que están todos los parches de los errores aparecidos hasta la fecha, y con los que dotan al Sistema operativo de nuevas funcionalidades.

Un Service Pack es un grupo de actualizaciones publicadas previamente. Los Service Packs también pueden contener un número limitado de características o cambios de diseño solicitados por los clientes. El último Service Pack incluye todas las actualizaciones y cambios incluidos en los Service Packs anteriores.

2.5.1 Service Pack 1 (SP1).

El SP1 para Windows XP fué lanzado el 9 de Noviembre de 2002. La novedad más visible fue la incorporación de la utilidad Configurar acceso y programas predeterminados, para poder elegir de forma más sencilla que programas se desea utilizar para las tareas más comunes. Otras novedades que introdujo fueron el soporte para USB 2.0, por lo que Windows XP podría soportar discos duros de más de 137 GB.

Como consecuencia de un pleito con Sun Microsystems, Microsoft se vio forzada a sacar una revisión a este SP, llamada Service Pack 1a (SP1a), en la que se eliminaba la Máquina virtual Java de Microsoft.

2.5.2 Service Pack 2 (SP2).

El 6 de agosto de 2004, Microsoft lanzó el **SP2**, que incluía el **SP1**, además de varias novedades, centradas sobre todo, en dar mayor seguridad al sistema operativo. Dichas novedades son:

- ✓ Un centro de seguridad, para comprobar el riesgo al que está sometido Windows XP.

- ✓ Nueva interfaz del Cortafuegos de Windows XP, además de ser activado por defecto.
- ✓ Incorporación a Internet Explorer de un bloqueador, la capacidad de bloquear controles ActiveX, el bloqueo de las descargas automáticas y un administrador de complementos.
- ✓ Uso de la tecnología DEP (Data Execution Prevention o Prevención de ejecución de datos) por Hardware o Software (Según si el Procesador tenga o no soporte para ello).
- ✓ Las actualizaciones automáticas están activadas por defecto.
- ✓ El servicio Windows Messenger se desactiva por defecto.
- ✓ Outlook Express bloquea los archivos adjuntos potencialmente peligrosos (.exe).
- ✓ La ventana de Agregar o quitar programas permite mostrar u ocultar las actualizaciones.
- ✓ Mejoras multimedia como la inclusión del Reproductor de Windows Media 9, DirectX 9.0c, y Windows Movie Maker 2.1.

2.5.3 Futuros Service Packs.

Para futuros Service Packs, Microsoft ha anunciado que incorporará algunas de las novedades de Windows Vista a Windows XP. Dichas novedades podrían ser Windows Presentation Foundation, WinFS, Internet Explorer 7 y Windows Media Player 11.

Microsoft sacará un SP3 (Service Pack 3) para Windows, posiblemente en 2007, tras lanzar de manera oficial el nuevo Windows Vista, con el fin de crear un Windows XP más seguro.

La nueva versión del sistema operativo Windows es Windows XP esta construidos sobre la plataforma Windows más fiable. Windows XP es un gran paso adelante hacia el proyecto de Microsoft de hacer que la información esté disponible en cualquier momento, lugar o dispositivo.

Windows XP Profesional contiene una administración de la configuración de directivas mejorada, para que los administradores puedan ajustar, administrar o simplemente desactivar las características que no deseen utilizar.

2.6 Para utilizar Windows XP Professional (SP2), es necesario:

- ✓ Unidad de CD ROM.
- ✓ Procesador a 300 MHz o superior (2.0, 2.4 GHz).
- ✓ 128 MB de RAM o superior (256, 512 MB).
- ✓ 2 GB de espacio de disco disponible durante la instalación.[R3]

2.7 Principales razones para utilizar Windows XP Profesional.

- ❖ **Intercambio rápido de usuarios**. Permite que entre familiares o amigos se pueda compartir una sola computadora para acceder a sus propias cuentas, sin que se tenga que cerrar cada una de las aplicaciones o que se tenga que reiniciar el sistema.
- ❖ **Nuevo diseño visual simplificado**. Permite simplificar el manejo de la PC, ya que gracias a su diseño limpio y fácil de usar que muestra las funciones que se utilizan con más frecuencia.
- ❖ **Windows Media Player para Windows XP**. Integra las actividades de medios digitales más comunes en un solo lugar y es fácil de usar.
- ❖ **Windows Messenger**. Es la manera más fácil de comunicarnos con cualquier persona en tiempo real. Los usuarios pueden seleccionar texto, voz y video, a la que disfrutan de excelente rendimiento.
- ❖ **Windows Movie Maker**. Permite que se pueda captar editar, organizar y compartir fácilmente películas que se elaboran en casa, esto se logra conectando una cámara digital a la PC; la otra opción es con el hardware adecuado (cámara analógica).
- ❖ **My pictures**. Permite que uno como usuario pueda realizar tareas de administración básica, tales como agregar, clasificar y eliminar archivos.

- **Internet Explorer 6**. Incluye muchas funciones nuevas y mejoradas, las cuales simplifican las tareas, incrementan la confiabilidad y contribuyen a mantener la privacidad de información personal en la Web.
- **Asistencia Remota**. Permite que un profesional de informática, que este utilizando Windows XP, controle de manera remota su PC para mostrar un proceso o ayudarle a resolver un problema.
- **Restablecimiento del Sistema.** Permite monitorear cambios en los archivos del sistema, de manera que, en caso de que ocurra algún problema, el usuario pueda restablecer su ordenador al estado en el que se encontraba sin perder los archivos de datos personales.
- **Asistencia de configuración de red.** Permite crear con facilidad una red en casa, de manera que varias PCS puedan compartir impresoras, dispositivos, archivos y conexiones de Internet.
- **Remote Destop (Escritorio Remoto).** Proporciona acceso a un escritorio que ejecute Windows XP desde una ubicación remota, dando a los usuarios la capacidad de trabajar mientras se esta fuera de casa u oficina. Cuando se activa el escritorio remoto en una computadora, los usuarios pueden conectarla desde una PC basada en Windows 95 o posterior y acceder a todos sus archivos, aplicaciones y recursos de la red, como si estuvieran sentados frente a ala computadora misma.
- **Soporte inalámbrico para redes.** Proporciona acceso seguro, así como rendimiento y mejoras para redes inalámbricas
- **Soporte para múltiples idiomas.** Permite a los usuarios crear, leer y editar fácilmente documentos en distintos idiomas.
- **Sistema de encriptación de archivos.** Permite proteger los datos confidenciales en los archivos que están almacenados en sus discos. Para Windows XP, la encriptación del sistema de archivos ahora funciona como archivos y carpetas fuera de línea.[R4]

2.8 Servicios de Windows XP Profesional.

2.8.1 Concepto de Servicio.

Son programas o aplicaciones cargadas por el sistema operativo.

Programa, rutina o proceso que realiza una determinada función del sistema para ofrecer compatibilidad con otros programas.

2.8.2 Como acceder a los servicios:

- Hacer clic en el botón de inicio.
- Hacer clic en panel de control.
- Hacer clic en herramientas administrativas.
- Administración de equipos, aparecerá una ventana con una serie de opciones que lleva por nombre Administración de equipos.
- Servicios y aplicaciones (Servicios), del lado derecho de la ventana se mostrará una serie de procesos y aplicaciones que usa Windows.

2.8.3 Servicios con los que cuenta Windows XP Profesional (Panel de control).

- **Actualizaciones automáticas.** Su función es habilitar la descarga e instalación de actualizaciones de Windows. Si este servicio esta deshabilitado, Windows se puede actualizar manual mente en el sitio Web de Windows Update, Windows se da cuenta de la aparición de una nueva actualización después de que esta aparezca. [R9]

  Es mejor deshabilitar este servicio, ya que perdemos control de la información que entra y sale de la computadora.

- **Administración de aplicaciones.** Ofrece servicios de instalación de software como asignar, publicar y quitar. Si éste servicio las nuevas aplicaciones continúan almacenándose en agregar y quitar programas.

- **Administrador de carga.** Este servicio se encarga de administrar transferencias sincronas y asíncronas de archivos entre clientes y servidores en la red.

- **Administrador de conexión automática de acceso remoto.** Este servicio crea una conexión a una red remota siempre que un programa hace referencia a un nombre o dirección DNS.

- **Administrador de cuentas de seguridad.** Almacena información de seguridad de cuentas de usuarios locales. Controla todo tipo de información de seguridad.

- **Administrador de discos lógicos.** Este servicio se encarga de detectar y supervisar unidades de disco duro y nuevas y envía información del volumen de disco al servicio de administración de discos lógicos para su configuración. Si se detiene este servicio, la información y configuración de discos dinámicos pueden quedar desactualizada.

- **Administrador de sesión de ayuda de escritorio remoto.** Este servicio se encarga de administrar y controlar la asistencia remota. Nunca llegamos a utilizar este servicio, éste es uno de los 'peligrosos' ya que puede llegar a aceptar una petición de conexión de alguien no deseado, recomiendo deshabilitarla.

- **Almacenamiento protegido.** Este servicio nos ofrece almacenamiento protegido para datos importantes, como lo son claves privadas, para impedir el acceso de servicios, procesos o usuarios no autorizados. Si queremos una máxima seguridad y podemos prescindir de la utilización de recordar contraseña, podemos deshabilitar este servicio y ningún dato importante será almacenado en la computadora.

- **Ayuda de NetBios sobre TCP/IP.** Este servicio permite habilitar la compatibilidad con NetBios.

- **Cliente de seguimiento de vínculos distribuidos.** Mantiene vínculos entre archivos NTFS dentro de un equipo o entre equipos en un dominio de red.

- **Cliente DHCP.** Administra la configuración de la red registrando y actualizando direcciones IP y nombre DNS.

- **Cliente DNS.** Este servicio resuelve y almacena en cache los nombres del sistema de nombres de dominio (DNS) para el equipo. Si se detiene este servicio, el equipo no podrá resolver nombres DNS, ni ubicar controladores de dominio en Active Directory, si se desactiva este servicio, no se podrá iniciar ninguno de los servicios.

- **Cliente Web.** Este servicio habilita los programas basados en Windows para que creen, tengan acceso y modifiquen archivos basados en Internet, si este servicio se detiene estas funciones no estarán disponibles.

- **Compatibilidad con cambio rápido de usuario.** Este servicio proporciona administración para aplicaciones que necesitan asistencia en un entorno de usuarios múltiples.

- **Conexión de seguridad a Internet (ICF) / Conexión compartida a Internet (ICS).** Ofrece servicios de traducción de direcciones, direccionamiento, resolución de nombres y servicios de prevención de intrusión para una red domestica.

- **Conexiones de Red.** Este servicio administra objetos en la carpeta Conexiones de red y acceso telefónico, donde se pueden ver conexiones de red de área local remota.

- **DDE de red (Network DDE).** Este servicio ofrece transporte y seguridad en la red para el intercambio dinámico de datos (DDE) para los programas que se ejecutan en el mismo equipo o en diferentes equipos.

- **Estación de trabajo.** Este servicio crea y mantiene conexiones de cliente de red a servidores remotos, si se detiene el servicio, estas conexiones no estarán disponibles.

- **Examinador de equipos.** Mantiene una lista actualizada de equipos en la red y proporciona esta lista a los equipos designados como exploradores.

- **Horario de Windows.** Mantiene la sincronización de fecha y hora en todos los clientes y servidores de la red.

- **Host de dispositivo Plug and Play universal.** Proporciona compatibilidad para dispositivos Plug and Play universales.

- **Inicio de sesión en red.** Admite la autenticación de pasos de sucesos de inicio de sesión de cuenta para los equipos en un dominio.

- **Instantáneas de volumen.** Administra e implementa Instantáneas de volumen usadas para copias de seguridad y otros propósitos.

- **Llamada a procedimientos remoto.** Este servicio es fundamental para el funcionamiento del sistema, lo dejaremos en automático.

- **Mensajero.** Transmite mensajes del servicio de alertas y el comando net send entre clientes y servidores, si se detiene este servicio, no se transmitirán los mensajes de alerta.

- **Plug and Play.** Habilita un equipo para que reconozca y adapte los cambios de hardware con el menor esfuerzo por parte del usuario. Si se detiene o deshabilita este servicio, el sistema se volverá inestable. Este servicio se encarga de detectar los cambios de dispositivos Plug and Play.

- **Servicio de alerta (Alerter).** Este servicio notifica a usuarios y equipos seleccionados de alertas administrativas. Si se detiene el servicio, los programas que utilizan alertas administrativas no las recibirán.

- **Servicio de Index Server (Indexing service).** Indexa el contenido y las propiedades de archivos en equipos locales y remotos.

- **Servicio de puerta de enlace de capa de aplicación (Application Layer Gateway Service).** Proporciona soporte a otros complementos de protocolo para Conexión compartida a Internet y servidor de seguridad de conexión a Internet. Si no usamos "Conexión compartida a Internet" o el firewall de Windows XP lo deshabilitamos.

- **Transfer Service.** Usa el ancho de banda de la red inactiva para transferir datos.

- **Servidor.** Ofrece compatibilidad con uso compartido de archivos, impresoras y canalizaciones con nombre de red, para este equipo. Si se detiene el servicio, esta funciones no estarán disponibles.[R5]

2.9 Seguridad.

En una red, protección de un sistema informático y sus datos contra daños o pérdidas, que se implementa especialmente para que sólo los usuarios autorizados puedan tener acceso a los archivos compartidos.

2.9.1 Introducción a Servidor de seguridad de conexión a Internet.

Servidor de seguridad es un sistema de seguridad que actúa como límite de protección entre una red y el mundo exterior. Servidor de seguridad de conexión a Internet (ICF, Internet Connection Firewall) es el software de servidor de seguridad que se utiliza para establecer restricciones acerca de qué información se comunica desde una red doméstica o de oficina pequeña a Internet, y viceversa.

Si la red utiliza Conexión compartida a Internet (ICS), para proporcionar acceso a Internet a varios equipos, ICF debería estar habilitado en la conexión compartida a

Internet. Sin embargo, ICS e ICF se pueden habilitar de forma independiente. Debe habilitar ICF en la conexión a Internet de cualquier equipo que esté conectado directamente a Internet. Para comprobar si ICF está habilitado o para habilitar el servidor de seguridad.

ICF protege también un único equipo conectado a Internet. Si sólo hay un equipo conectado a Internet con un módem por cable, un módem DSL o un módem de acceso telefónico, ICF protege la conexión a Internet. [R6]

2.9.1.1 Cómo funciona Servidor de seguridad de conexión a Internet (ICF).

ICF se considera un servidor de seguridad "con estado". Un servidor de seguridad con estado es el que supervisa todos los aspectos de las comunicaciones que pasan por él e inspecciona las direcciones de origen y destino de cada mensaje que administra. Para impedir que el tráfico no solicitado de la parte pública de la conexión entre en la parte privada, ICF mantiene una tabla de todas las comunicaciones que tienen origen en el equipo ICF. En el caso de un único equipo, ICF hace un seguimiento del tráfico originado en el equipo. Si se utiliza en combinación con ICS, ICF hace un seguimiento de todo el tráfico cuyo origen es el equipo ICF o ICS, y todo el tráfico cuyo origen son los equipos de la red privada. Todo el tráfico entrante de Internet se compara con las entradas de la tabla. Sólo se permite que el tráfico entrante de Internet llegue a los equipos de la red cuando hay una entrada en la tabla que muestra que el intercambio de comunicación se inició en el equipo o en la red privada.

Windows XP Profesional tiene funciones que evitan el acceso de intrusos por Internet, protegen los archivos confidenciales y restauran la estabilidad del sistema en caso de una falla.

2.9.1.2 Protección contra intrusos.

Uno de los peligros de Internet es que permite que un hacker ingrese a una computadora de forma remota, este riesgo es mayor cuando se utilizan conexiones de alta velocidad, como los cables de modem o DSL.

La protección de intrusos se puede realizar a través de:

2.9.1.2.1 Firewall.

Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de la red privada e Internet.

Bloquean el acceso de intrusos por la red. Para que el firewall sea efectivo todo tráfico de información a través de Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

Un firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Como se muestra en la figura 2.1.

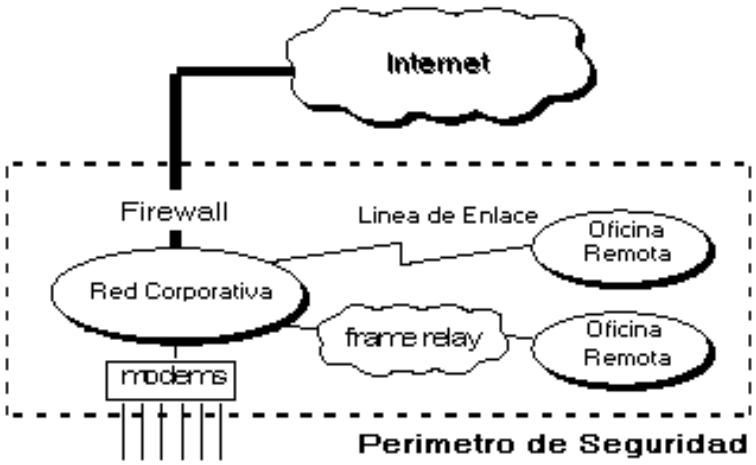


Figura 2.1 La Política de Seguridad crea un perímetro de defensa.

La figura 2.2 muestra los beneficios de un firewall:

- ✓ Administran los accesos posibles de Internet a la red privada
- ✓ Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en Internet.
- ✓ El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este genera una alarma ante la posibilidad de que ocurre un ataque o suceda algún problema en el transito de los datos.

Concentra la seguridad Centraliza los accesos

Genera alarmas de seguridad Traduce direcciones (NAT)

Monitorea y registra el uso de servicios de WWW y FTP.

Figura 2.2 Monitoreo de seguridad de un firewall.

Windows XP Profesional incluye un firewall muy oportuno para los usuarios que tengan dispositivos con conexiones de banda ancha. No es un firewall avanzado, pero ofrece la protección básica.

2.10 Sistema de Encriptación de Archivos.

La encriptación es un proceso que codifica los archivos de manera que sean ilegibles para las personas que no poseen la contraseña.

La creciente funcionalidad del Sistema de Encriptación de Archivos (EFS), aumenta significativamente el poder de Windows XP proporcionando flexibilidad adicional para usuarios corporativos cuando éstos implementan soluciones de seguridad basadas en archivos de datos encriptados.

El Sistema de Encriptación de archivos:

- ✓ Protege los datos confidenciales en los archivos que están almacenados en sus discos y que utilizan el sistema de archivo NTFS.
- ✓ La encriptación del sistema de archivo es la tecnología básica para encriptar y desencriptar archivos almacenados en volúmenes NTFS.
- ✓ Solo el usuario que encripta un archivo protegido puede abrir el archivo y trabajar con el.

Para encriptar un archivo o una carpeta simplemente se escoge esa opción en el menú de propiedades del elemento, de la misma forma que se otorgan otros atributos como ocultos o solo lectura. [R7]

2.11 Administración Corporativa.

Las configuraciones de políticas de grupo simplifican la administración de los usuarios y objetos, permitiendo a los administradores organizarlos en grupos como departamentos o ubicaciones y después asignar mismas autorizaciones de seguridad.

2.11.1 Nombres de usuarios y contraseñas almacenados.

Al iniciar una sesión en un equipo que ejecuta Windows XP, puede facilitar un nombre de usuario y una contraseña. Éste se convierte en el contexto de seguridad predeterminado para conectar con otros equipos en redes y a través de Internet. Sin embargo, es posible que este nombre de usuario y esta contraseña no proporcionen acceso a todos los recursos deseados.

Casos en los que desee utilizar nombres y contraseñas diferentes para conectarse a recursos distintos:

- ✓ Cuando el usuario desea iniciar una sesión en su equipo con una cuenta estándar y conectarse a algunos equipos como administrador por cuestiones de mantenimiento y solución de problemas.
- ✓ Cuando se está trabajando en casa y se desea utilizar el nombre de usuario y la contraseña de la oficina para conectarse a servidores relacionados con ésta.
- ✓ Cuando la cuenta está en un dominio y necesita acceso a equipos de un dominio que no es de confianza.
- ✓ Cuando se desea obtener acceso a sitios Web con nombres de usuario y contraseñas específicos de cada sitio.

Los administradores pueden iniciar una sesión en la red utilizando su nombre de usuario y su contraseña estándar, pero deben conectarse a un servidor remoto con acceso administrativo para realizar funciones específicas. En este caso, el usuario debe poder facilitar un nombre de usuario y una contraseña diferentes para esta conexión. También es posible que el usuario desee almacenar este nombre de usuario y esta contraseña para volver a utilizarlos posteriormente. Ésta es la función de los nombres de usuario y contraseñas almacenados. Si un usuario necesita conectarse con servidores Web seguros mediante un nombre de usuario y una contraseña específicos. Los nombres de usuarios y contraseñas almacenados permiten a los usuarios conectar con diferentes servidores Web utilizando los nombres y las contraseñas facilitados y almacenarlos para su posterior reutilización. Los nombres de usuario y las contraseñas pueden ser

específicos de un único servidor Web o también pueden ser genéricos para que se faciliten cuando el usuario intente iniciar una sesión en un servidor Web seguro.

Los nombres de usuarios y contraseñas almacenados también almacenan la información guardada como parte integrante de un perfil de usuario. Esto significa que dichos nombres de usuario y contraseñas viajarán con el usuario de equipo en equipo por toda la red.

2.12 Administración de equipos.

Administración de equipos es un conjunto de herramientas administrativas que se pueden utilizar para administrar un solo equipo local o remoto. Combina diversos programas de administración en un árbol de consola proporciona un fácil acceso a las propiedades y herramientas administrativas. [B4]

2.12.1 Administración de equipos se puede utilizar para:

- ✓ Supervisar sucesos del sistema, como la hora de inicio de sesión y los errores de programa.
- ✓ Crear y administrar recursos compartidos.
- ✓ Ver una lista de usuarios conectados a un equipo local o remoto.
- ✓ Iniciar y detener servicios del sistema, tales como Tareas programadas y los Servicios de Index Server.
- ✓ Establecer las propiedades para los dispositivos de almacenamiento.
- ✓ Ver la configuración de dispositivos y agregar controladores de dispositivo nuevos.
- ✓ Administrar aplicaciones y servicios.

Administración de equipos contiene tres elementos:

- ✓ Herramientas del sistema.
- ✓ Almacenamiento.
- ✓ Servicios.

Pasos para abrir Administración de equipo (Utilizando vista de categorías).

1.- Hacer clic en inicio.

2.- Panel de control.

3.- Rendimiento y mantenimiento, herramientas administrativas.

4.- Doble clic en Administración de equipos.

Al conectar con otro equipo, el nombre de dicho equipo aparece entre paréntesis junto a Administración de equipos en el árbol de la consola

Para conectar con otro equipo

- Abrir Administración del equipo.
- En el árbol de la consola, hacer clic con el botón secundario del mouse en Administración de equipos.
- Hacer clic en conectar con otro equipo.
- En el cuadro de dialogo seleccionar equipo, hacer clic en otro equipo y seleccionar el equipo que desee administrar.

2.13 Operación en red.

Una de las muchas tareas importantes que corresponden a un administrador de red es la monitorización del sistema, es indispensable conocer todo en todo momento que esta ocurriendo en la red y resolver así cualquier problema que pueda surgir, esto se puede resolver a través de el protocolo sencillo de administración de red (SNMP) y otras herramientas que permitan obtener información en tiempo real.

2.14 Monitor de Red.

Permite detectar y resolver problemas en redes LANs y WANs, incluyendo enlaces de direccionamiento y acceso remoto. Se puede utilizar para identificar los patrones de tráfico de la red y los problemas de la red**.**

La monitorización de red permite solucionar y prevenir muchos de los problemas que pueden presentarse en la administración de la misma: cuellos de botella, sobrecarga de usuarios, intrusiones, etc. Por lo tanto, es importante estar siempre informado de los datos que circulan por el sistema. [B5]

CAPITULO

3

UTILERÍAS ADMINISTRATIVAS DE WINDOWS XP PROFESIONAL.

En el presente capítulo se describen las utilerías de Windows XP Profesional, así como su configuración y utilización, con la finalidad de ofrecer mayor nivel de experiencia y lograr una mejor aplicación en el caso de estudio.

3.1 Introducción.

Windows XP Profesional proporciona las herramientas avanzadas de administración, instalación y soporte que facilitan su trabajo. Windows XP Profesional se integrará sin fallas a los ambientes Windows 2000 Active Directory existentes, al tiempo que se ofrece cientos de nuevas políticas del sistema. Para facilitar la implementación y la migración, Windows XP cuenta con varias correcciones importantes para las tecnologías existentes, además de introducir características innovadoras y esenciales.

3.2 Herramientas de productividad de Windows XP Profesional.

3.2.1 Escritorio Remoto.

El Escritorio Remoto permite a un usuario crear una sesión virtual en su computadora de escritorio utilizando el Protocolo de escritorio remoto (RDP) de Microsoft.

El escritorio remoto permite a un cliente acceder a todos los datos y aplicaciones alojados en la computadora de escritorio a partir de otra computadora que ejecute Windows 95 ó posterior, la cual está conectada al sistema a través de la red. [B8]

3.2.2 Administrador de credenciales.

Un administrador de credenciales es un depósito seguro para información de claves de acceso. Esta función permite ingresar el nombre de usuario y las claves de varios recursos y aplicaciones en la red (como correo electrónico) una vez y luego hacer que el sistema proporcione automáticamente esa información cuando vuelva a utilizar esos recursos.

Los usuarios que no están conectados a un dominio, o que necesitan acceder a recursos en varios dominios, podrán acceder fácilmente a los recursos de la red.

3.2.3 Archivos y carpetas fuera de línea.

Los usuarios pueden especificar los archivos y carpetas en red que desean tener disponibles cuando se desconecten de la red. De manera adicional, con Windows XP Profesional, las carpetas fuera de línea pueden ahora encriptarse para proporcionar el máximo nivel de seguridad.

Los usuarios pueden trabajar con documentos mientras están desconectados de la red, de la misma manera que lo hacen cuando están conectados.

3.2.4 Asistencia Remota.

Asistencia remota es una tecnología de Windows XP Profesional que permite a los usuarios de Windows XP Profesional prestarse asistencia mutua a través de Internet.

La asistencia remota permite al usuario compartir el control de su equipo a través de una red o de Internet.
Un administrador o un amigo pueden ver la pantalla del usuario y controlar el puntero y el teclado para ayudar a solucionar un problema técnico.

Reduce el tiempo que los administradores de sistemas pasan en los escritorios de los usuarios. Muchas tareas administrativas y de solución de problemas se pueden realizar ahora desde los escritorios de los administradores. [B8]

3.2.5 Restauración del Sistema.

La función de Restauración del Sistema de Windows XP permite a los usuarios y a los administradores de informática restaurar una PC, en el caso de que haya algún problema, a un estado previo sin perder archivos con datos personales. Restauración del Sistema monitorea activamente los cambios a los archivos del sistema para registrar o almacenar versiones previas antes de que ocurrieran los cambios. Con Restauración del Sistema los usuarios nunca tienen que pensar

acerca de tomas instantáneas del sistema, ya que crea automáticamente puntos de restauración fácilmente identificables, que permiten al usuario restaurar el sistema a un momento previo.

Si los usuarios experimentan fallas en el sistema u otro problema importante, pueden utilizar la Restauración del Sistema a partir de la modalidad “Safe” o normal, para regresar a un estado del sistema anterior, restaurando así la funcionalidad óptima del sistema. La Restauración del Sistema no revertirá los datos o los archivos de documentos del usuario, por lo que restaurar no provocará que los usuarios pierdan su trabajo, correo o incluso su historial de navegación y favoritos.

3.2.6 Windows Messenger.

Windows Messenger es la manera más fácil de comunicarse con sus clientes, socios, amigos y la familia, en tiempo real. Le permitirá saber si sus contactos están o no en línea. Colabore con sus contactos, transfiera archivos, comparta aplicaciones y dibujos.

Windows XP proporcionará a los usuarios una gran plataforma para conferencias y colaboración en línea.

3.2.7 Asistente de Instalación de Redes.

El Asistente de Instalación de Redes le facilita al propietario de una pequeña empresa la instalación y gestión de su red. El asistente los guía a través de los pasos principales, incluyendo el uso compartido de archivos e impresoras, así como de su conexión a Internet y la configuración del firewall de conexión a Internet.

3.3 Conexiones de red.

Conexiones de red permite que su equipo se conecte a Internet, a una red o a otro equipo. En Conexiones de red, puede tener acceso a recursos y funciones de redes, ya se encuentre físicamente en la ubicación de la red o en una ubicación remota. Las conexiones se crean, configuran, almacenan y supervisan desde la carpeta Conexiones de red.

3.3.1 Requisitos de hardware para las conexiones de red.

Dependiendo de la configuración, quizá necesite el hardware siguiente:

- ✓ Tarjeta adaptadora de red con un controlador certificado para Especificación de interfaz de controlador de red (NDIS), para la conectividad de LAN.
- ✓ Uno o varios módems compatibles y un puerto COM disponible.
- ✓ Un módem de 28,8 K o 56 K, o un adaptador ISDN (RDSI) (si va a utilizar una línea ISDN (RDSI)).
- ✓ Módem DSL. Un módem DSL externo suele estar conectado a un adaptador de red Ethernet.
- ✓ Módem por cable. Un módem por cable externo suele estar conectado a un adaptador de red Ethernet.
- ✓ Línea telefónica analógica.
- ✓ Si el equipo está configurado para aceptar conexiones entrantes, un adaptador de múltiples puertos puede aumentar el rendimiento cuando haya varias conexiones.

3.3.2 Tipos de conexión de red.

Hay cinco tipos de conexión de red y de acceso telefónico. La figura 3.1 muestra cada tipo de conexión, los métodos de comunicación que utilizan para establecer la conexión y un ejemplo de la conexión.

Tipo de conexión	Método de comunicación	Ejemplo
Conexiones de acceso telefónico	Módem, ISDN, X.25	Conecta con una red corporativa o con Internet mediante acceso remoto.
Conexiones de área local	Ethernet, Token Ring, módem por cable, DSL, FDDI, IP sobre ATM, IrDA, comunicaciones inalámbricas, tecnologías WAN (T1, Frame Relay)	Usuario corporativo típico. Conecta a Internet mediante módem por cable o DSL. Puede utilizar Ethernet, IrDA, conexión inalámbrica o adaptadores de red de línea telefónica doméstica (HPNA) para configurar la red doméstica o de pequeña oficina.
Conexiones de red privada virtual (VPN)	VPN sobre PPTP o L2TP a redes corporativas o Internet	Conectan de forma protegida con una red corporativa a través de Internet.
Conexiones directas	Cable serie, vínculo de infrarrojos, cable DirectParallel	Sincronizan la información entre un PC de mano Windows CE y un equipo de escritorio.
Conexiones entrantes	Conexiones VPN, directas o de acceso telefónico	Llaman a un servidor de acceso remoto de la red doméstica o de pequeña oficina.

Figura 3.1 Tabla de tipos de conexión.

3.3.2.1 Conexiones de acceso telefónico.

Una conexión de acceso telefónico le conecta a una red o a Internet mediante un dispositivo que utiliza la red telefónica. Este dispositivo puede ser un módem que utilice una línea telefónica estándar, una tarjeta ISDN (RDSI) con una línea ISDN (RDSI) de alta velocidad

Los usuarios típicos suelen tener una o dos conexiones de acceso telefónico a Internet y quizás a la red empresarial. En una situación de servidor más compleja, se pueden utilizar varias conexiones de acceso telefónico para implementar el enrutamiento avanzado.

3.3.2.2 Conexiones de área local.

Al crear una red doméstica o de pequeña oficina, los equipos que ejecutan Windows XP Professional, quedan conectados a una red de área local (LAN, Local Área Network). Al instalar Windows XP Profesional se detecta el adaptador de red y se crea una conexión de área local. Al igual que todos los demás tipos de conexión, se muestra en la carpeta Conexiones de red. De forma predeterminada, la conexión de área local está siempre activada. La conexión de área local es el único tipo de conexión que se crea y se activa de forma automática.

Si el equipo tiene varios adaptadores de red, en la carpeta Conexiones de red se presenta un icono de conexión de área local para cada adaptador.

Se puede crear redes de área local que utilicen Ethernet, inalámbricas, de línea telefónica doméstica (HPNA), módems por cable, DSL o redes LAN IrDA (infrarrojos), Token Ring, FDDI, IP sobre ATM.

Si se efectúan cambios en la red, puede modificar la configuración de las conexiones de área local existentes para adaptarlas a esos cambios. Con la opción de menú **Estado** de Conexiones de red, se puede ver información de la conexión como la duración, la velocidad, la cantidad de datos transmitidos y recibidos, y las herramientas de diagnóstico disponibles para una conexión específica.

Si se instala un nuevo adaptador de red en el equipo, la próxima vez que lo inicie aparecerá un nuevo icono de conexión de área local en la carpeta Conexiones de red. La funcionalidad de Plug and Play encuentra el adaptador y crea una conexión de área local para él. Puede agregar una tarjeta PC mientras el equipo está en funcionamiento sin reiniciar el equipo. El icono de la conexión de área local se agrega inmediatamente a la carpeta. No se pueden agregar manualmente conexiones de área local a la carpeta Conexiones de red.

Puede configurar varios adaptadores de red mediante la opción de menú **Configuración avanzada**. Puede modificar el orden en el que una conexión utiliza los adaptadores, así como los clientes, servicios y protocolos asociados con el adaptador. Se puede modificar el orden en el que la conexión tiene acceso a los proveedores para obtener información de la red, como redes e impresoras.

Puede configurar el dispositivo que una conexión utiliza y todos los clientes, servicios y protocolos asociados con la conexión, mediante la opción de menú **Propiedades**. Los clientes definen el acceso de la conexión a los equipos y archivos de la red. Los servicios proporcionan características como Compartir

impresoras y archivos. Los protocolos, como TCP/IP, definen el lenguaje que el equipo utiliza para comunicarse con otros equipos.

Según el estado de su conexión de área local, la apariencia del icono cambiará en la carpeta Conexiones de red o aparecerá un icono distinto en el área de notificación. Si el equipo no detecta un adaptador de red, no aparecerá ningún icono de conexión de área local en la carpeta Conexiones de red. En figura 3.2 describen los distintos iconos de conexión de área local.

Icono	Descripción	Ubicación
 Conexión de área local	La conexión de área local está activa.	Carpeta Conexiones de red
 Conexión de área local	El medio está desconectado.	Carpeta Conexiones de red
	El medio está desconectado.	Área de notificación
 Conexión de área local	El controlador está deshabilitado.	Carpeta Conexiones de red

Figura 3.2 Iconos de conexión de área local.

3.3.3 Configuraciones de Red.

Existen varias formas diferentes de instalar una red doméstica o de pequeña oficina. Puede utilizar Conexión compartida a Internet (ICS), conectar sus equipos y módems DSL o por cable directamente a un concentrador Ethernet, o bien, utilizar una puerta de enlace residencial.[B1]

3.3.3.1 Conexión compartida a Internet.

En esta configuración de red, un equipo es el host de ICS y comparte su conexión a Internet. La comunicación a Internet desde y hacia los equipos de la red pasa a través del equipo host de ICS. La figura 3.3 muestra el modelo de una conexión compartida a Internet.

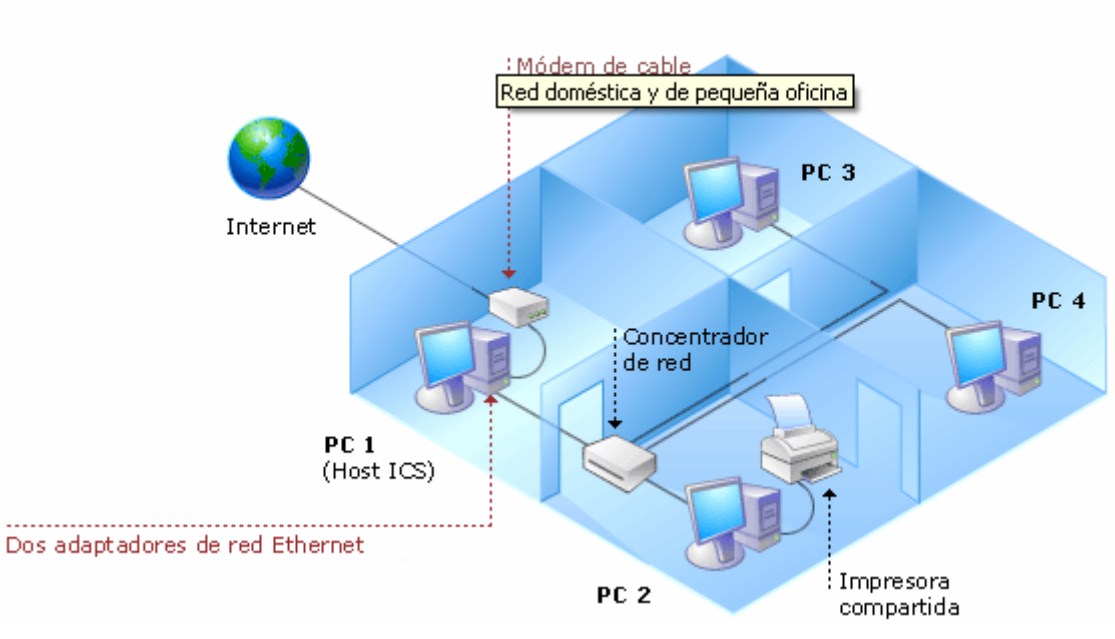


Figura 3.3 Modelo de una conexión compartida a Internet

Las ventajas de este tipo de configuración de red son:

- ✓ Compartir una conexión de Internet con todos los equipos de la red puede reducir el coste de conexión a Internet y permite que todos los equipos de la red estén conectados al mismo tiempo.
- ✓ Conexión compartida a Internet de Windows XP Profesional proporciona un punto de seguridad para la red. La red doméstica o de pequeña oficina está protegida contra intrusiones de Internet.
- ✓ Si el equipo Windows XP Profesional tiene diferentes tipos de adaptadores de red, puede utilizar Puente de red para proporcionar la configuración automática de la red sin tener que configurar manualmente los adaptadores de red para comunicarse entre sí.

- ✓ Utilizar Plug and Play Universal (UPnP) en su casa o pequeña oficina. Con UPnP puede controlar la conexión a Internet desde cualquier lugar de su casa o pequeña oficina.

La instalación de la red doméstica o de pequeña oficina con esta configuración le permite crear una red segura mediante una combinación de Conexión compartida a Internet y Seguridad de conexión a Internet de Windows XP Profesional y disponiendo de conexiones de red públicas y privadas. Además, puede utilizar compartir archivos e impresoras sin preocuparse de si pueden verse sus archivos privados en Internet.

3.3.3.1.1 Configuración de equipo para conexión a Internet.

La forma mas común de conectarse a Internet es mediante un módem y una cuenta con un proveedor de servicios Internet (ISP).

Para compartir una conexión a Internet con otros equipos de una red de pequeña oficina. Se debe ejecutar el Asistente para configuración de red, que configura Conexión compartida a Internet (ICS).

1. En la barra de tareas hacer clic en el botón de inicio. Como se muestra en la figura 3.4.

Figura 3.4 Botón de inicio.

2. Hacer clic en panel de control.

3.-Dentro del selector de categorías, hacer clic en el icono Conexiones de Red e Internet. Como se muestra en la figura 3.5.

Figura 3.5 Panel de control (Categorías).

4. En el selector de tareas, hacer clic en el icono Conexiones de Red. Como se muestra en la figura 3.6.

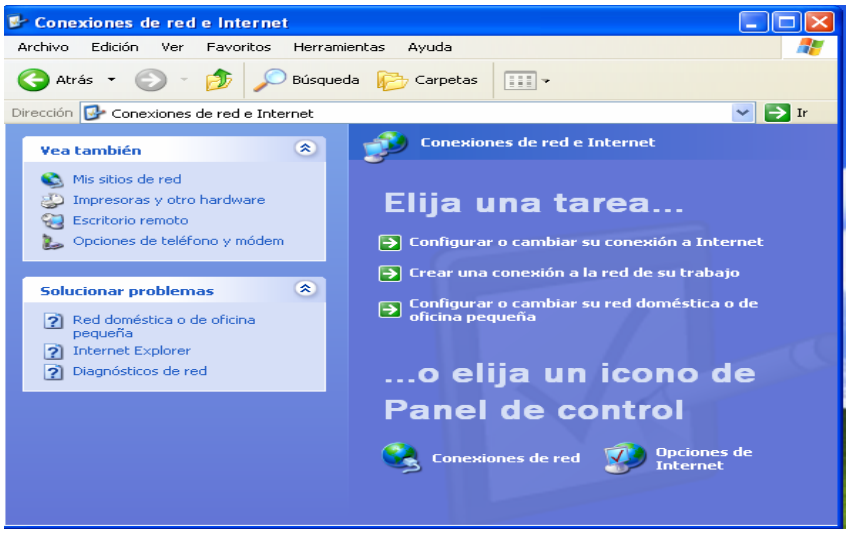


Figura 3.6 Conexiones de red e Internet.

5.- Hacer un clic con el botón derecho del mouse sobre el icono de conexión de área local y hacer clic en la opción Propiedades. Como se muestra en la figura 3.7

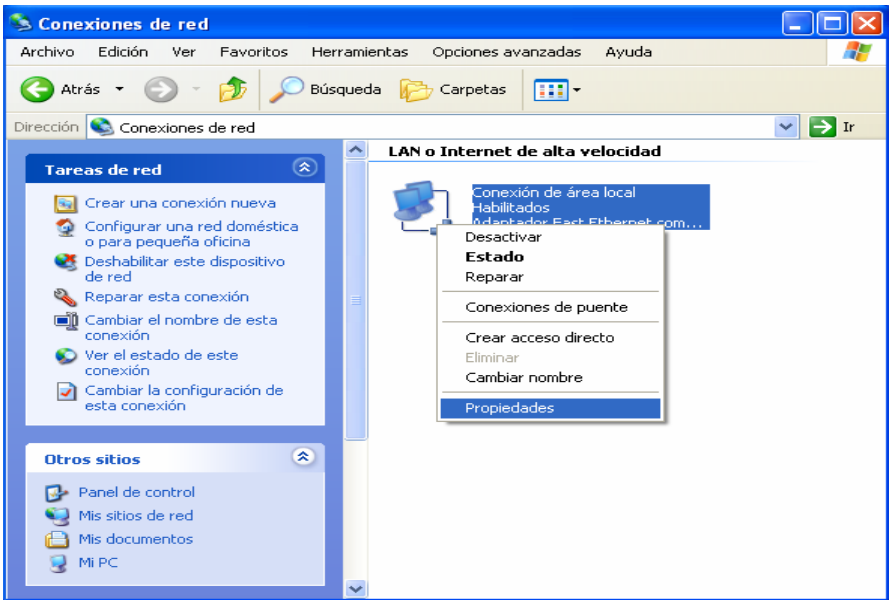


Figura 3.7 Conexiones de Red.

6.- Ubicar el protocolo Internet TCP/IP definido para este dispositivo, hacer clic sobre él para seleccionarlo y presionar el botón Propiedades. Como se muestra en la figura 3.8. En caso de no hallarse en esta ventana el protocolo Internet TCP/IP, se debe de instalar presionando el botón Instalar, opción Protocolo.

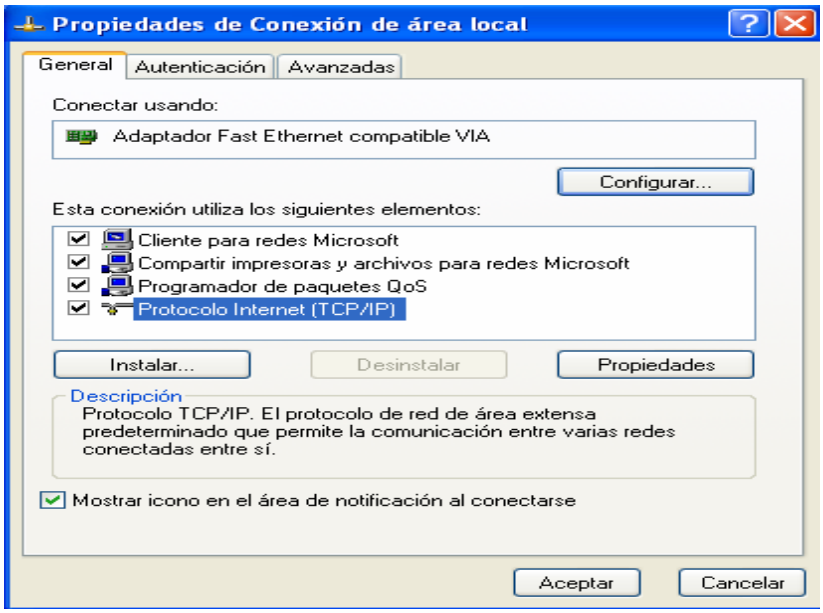


Figura 3.8 Propiedades de conexión de área local.

En las propiedades del Protocolo TCP/IP se especifican 5 parámetros: Como se muestra en la figura 3.9.

- Dirección IP: Este es el único parámetro que podemos elegir de un rango de posibilidades. Para cada una de las PCs de una red local. Es muy importante que no haya en la misma red local dos PCs con la misma IP, ya que esto provocaría inestabilidad de la misma, es recomendable mantener un orden lógico de las IP.
- La mascara de subred. Este parámetro será para todas las PCs.
- Puerta de enlace predeterminada. Es la dirección IP del módem.

Direcciones de Servidor DNS:

Servidor DNS preferido. Se especifica el servidor DNS primario del ISP Servidor DNS alternativo. Se especifica el servidor DNS alternativo del ISP, luego presionamos el botón aceptar. [B4]

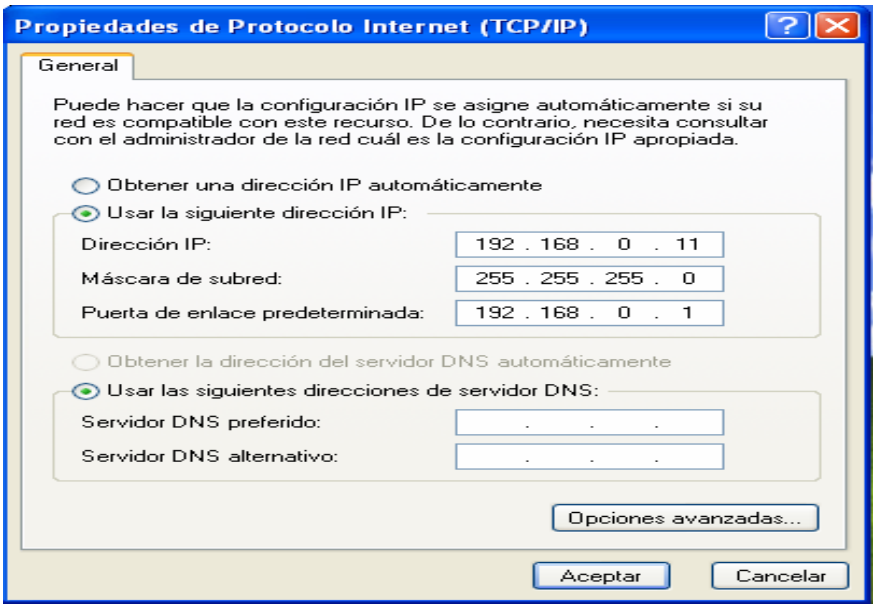


Figura 3.9 Propiedades de Protocolo Internet (TCP/IP)

3.3.3.2 Puerta de enlace residencial.

Una puerta de enlace residencial es un dispositivo de hardware que conecta la red doméstica o de pequeña oficina a Internet. Similar a Conexión compartida a Internet de Windows XP Profesional, la puerta de enlace le permite compartir una conexión a Internet DSL o por módem por cable con el resto de equipos de la red doméstica o de pequeña oficina. La puerta de enlace residencial se sitúa entre el módem DSL o por cable y la red doméstica o de pequeña oficina. La figura 3.10 muestra el modelo de una conexión de puerta de enlace.

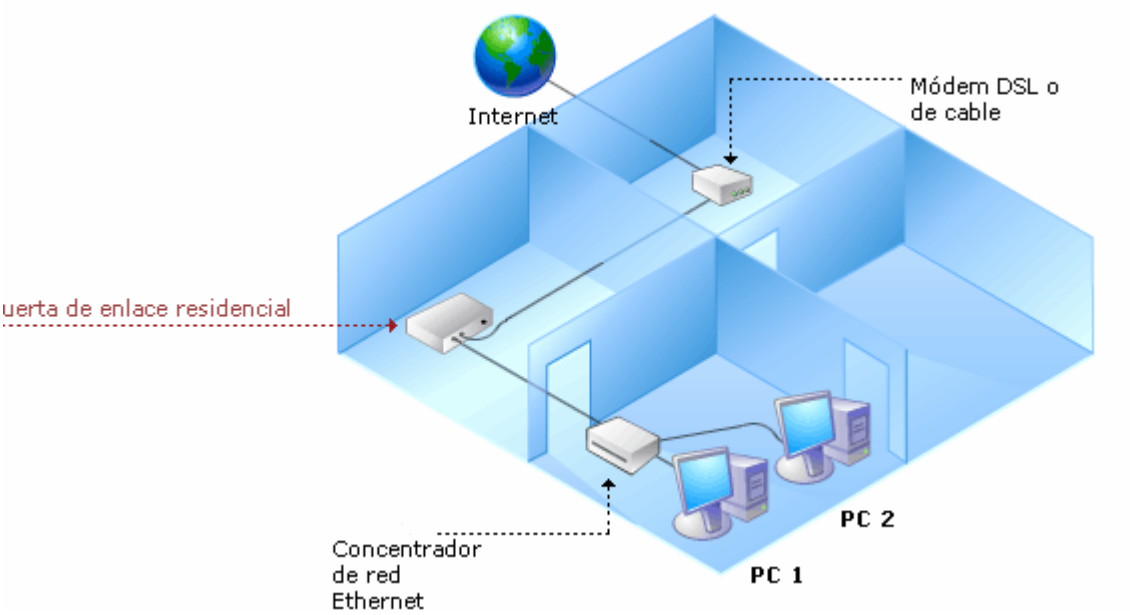


Figura 3.10 Modelo de una conexión de puerta de enlace.

Las ventajas de utilizar una puerta de enlace residencial son las siguientes:

- ✓ Aparece como un equipo en Internet, ocultando los equipos de la red doméstica o de pequeña oficina.
- ✓ Compartir una conexión a Internet con todos los equipos de la red.
- ✓ No necesita tener un equipo conectado todo el tiempo para proporcionar conexión a Internet.
- ✓ Utilizar Plug and Play Universal (UPnP) en su casa o pequeña oficina. Con UPnP puede controlar la conexión a Internet desde cualquier lugar de su casa o pequeña oficina.

3.3.3.3 Conexiones con Internet individuales.

Si se tiene un módem externo DSL o por cable, se puede conectar a un concentrador de red Ethernet y también conectar los equipos al concentrador Ethernet, tal como se muestra en la figura 3.11. Cada equipo de la red se conecta a Internet directamente o mediante un concentrador de red.

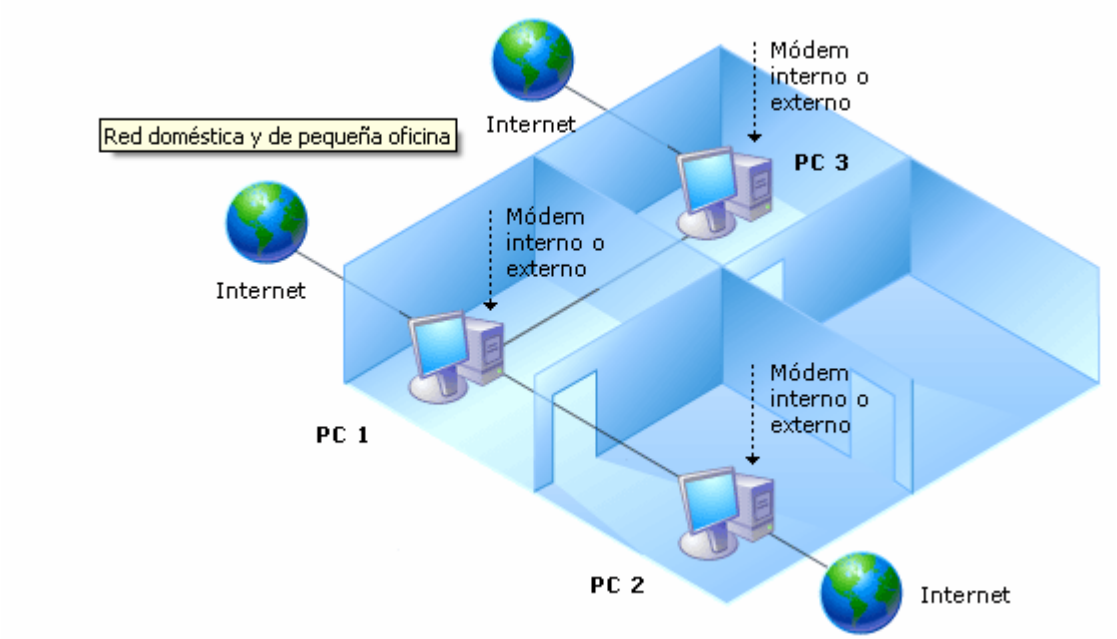


Figura 3.11 Modelo de una conexión con Internet Individual.

Las ventajas de configurar la red con este tipo de configuración son:

- ✓ No necesita tener un equipo conectado todo el tiempo para acceder a Internet.

Las desventajas de configurar la red con este tipo de configuración son:

- ✓ Debe mantenerse la seguridad de cada equipo de la red. Los equipos de la red que utilizan Windows XP Profesional pueden activar la seguridad de conexión a Internet en cada conexión al concentrador de red. Para equipos que utilicen versiones anteriores de Windows, se recomienda otro servidor de seguridad.
- ✓ Si no se activa Seguridad de conexión a Internet u otro servidor de seguridad en cada conexión a Internet, los archivos y carpetas compartidos pueden verse en Internet.
- ✓ Si utiliza Seguridad de conexión a Internet de Windows XP u otro servidor de seguridad en cada conexión a Internet, puede bloquearse la característica de compartir archivos e impresoras entre equipos de la red.

- ✓ Otros equipos y dispositivos que utilizan Plug and Play Universal (UPnP) no pueden utilizarse en la red.
- ✓ Ciertas configuraciones de red pueden evitar el funcionamiento de compartir archivos e impresoras en la red.

3.4 Compartir archivos en una red local.

3.4.1 Acceso de Usuarios

En Windows XP Profesional cuando se comparte un recurso, se hace para todos. Ese Todos, es todo el conjunto de los usuarios dados de alta en el ordenador que comparte. Por tanto si se ve el recurso, se puede acceder a él sin mas limitación que la impuesta en las restricciones. Es por ello que se debe eliminar el usuario Todos y añadir el nombre de los usuarios que se quiera que accedan al recurso y no todo el conjunto de usuarios que estén dados de alta en el equipo.

La gestión de usuarios es un proceso sencillo que cada propietario de equipo con Windows XP Profesional puede realizar a través del Panel de Control del Equipo. Como se muestra en la figura 3.12. El Servicio de Informática recomienda que cada equipo disponga de una cuenta principal y de otra opcional a través de la que se realicen los compartimentos de recursos. Debe quedar claro, que todos los usuarios dados de alta deben tener clave, ya que de lo contrario, se está comprometiendo la seguridad del equipo. Asimismo, se aconseja que las cuentas opcionales sean del tipo "Cuenta limitada" para evitar riesgos de posibles administraciones remotas.

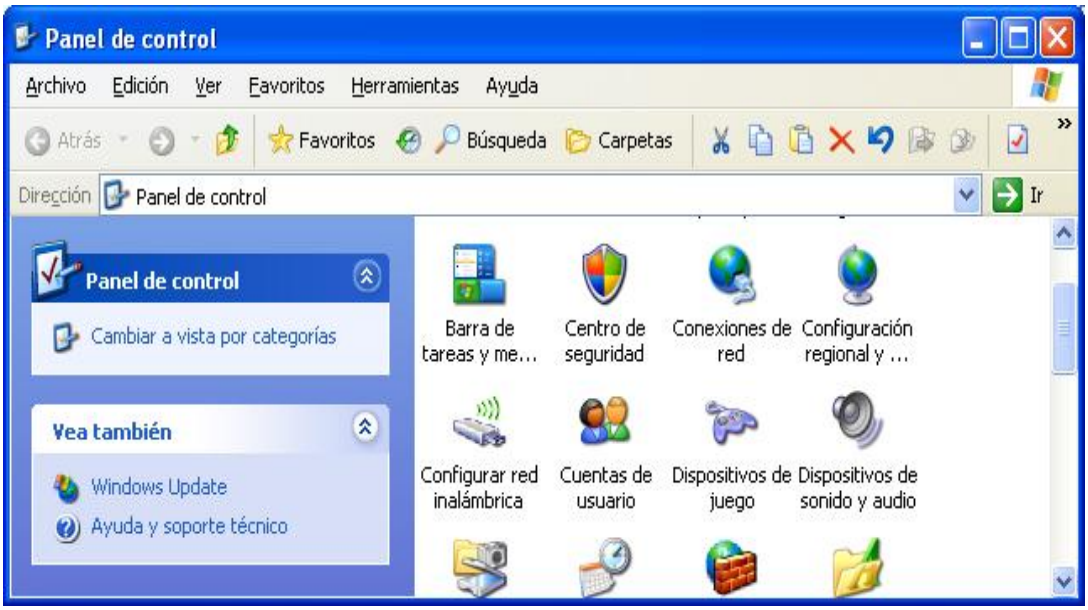


Figura 3.12 Panel de control.

Por tanto, a partir del instante en que se comparte, el recurso puede ser usado por todos los ordenadores que estén en red. Al definir usuarios concretos, sólo podrán utilizar los recursos aquellos usuarios a los que se les haya dado de alta y autorizado.

3.4.2 Compartir Carpetas.

La forma de compartir una carpeta en Windows XP Profesional es muy simple. Si se quiere compartir la carpeta pública del disco duro (nunca se debe compartir el disco duro completo). Para cualquier otra carpeta el proceso es el mismo.

- ✓ Se selecciona la carpeta a compartir pulsando el botón izquierdo del ratón, (Mi PC, Disco Duro C: y la carpeta.
- ✓ Se pulsa el botón derecho del ratón sobre el icono y se elige “Compartir”:
- ✓ Aparece la pantalla que indica que el recurso no está compartido:
- ✓ Se selecciona la opción Compartir esta carpeta y se le asigna el nombre que se desee.

- **Recurso compartido:** Es el nombre que se le quiere dar al recurso. Se asigna por defecto pudiendo ser cambiado. Hay que tener en cuenta que el nombre no debe contener espacios ni símbolos de puntuación y no debe de exceder de 8 caracteres (aunque lo admite, no es conveniente).
- **Comentario:** Se indica alguna reseña que identifique al recurso al resto de usuarios.

Pulsar el botón **Permisos** que da varias posibilidades a la lista de usuarios a los que se permita el acceso.

- **Control Total:** Todos los usuarios de la red podrán leer el contenido de la carpeta, copiarla a su ordenador, borrarla, modificarla, y crear nuevos archivos o carpetas dentro. Es decir, el acceso completo permite usar la carpeta ajena como si estuviera en su propio ordenador.
- **Leer:** Sólo se pueden consultar archivos del recurso compartido. No admite modificaciones, es decir, los demás usuarios de la red podrán leer el contenido del recurso, e incluso copiarlo a su ordenador, pero no borrarlo ni modificarlo, ni crear nuevos archivos o carpetas dentro.
- **Cambiar:** Permite la modificación de los elementos que contiene la carpeta pero impide su borrado.

Desde el botón Agregar de la pestaña de Permisos de los recursos compartidos, obtenida en el paso anterior, se pueden añadir los usuarios que, dados de alta previamente, podrán acceder al recurso. Sólo hay que escribir el nombre del usuario y pulsar el botón Comprobar nombres para que el sistema valide al usuario.

Se pulsa Aplicar y después Aceptar y ya se tiene el recurso compartido para los usuarios concretos. Las carpetas o recursos compartidos se muestran por debajo, para dar a entender que las ofrecen a otros usuarios. Se puede compartir no sólo carpetas, sino el disco duro entero, o la unidad de CD ROM/DVD, e incluso una impresora.

Si se desea dejar de compartir una carpeta o recurso, basta con volver a seleccionarla con el botón derecho y elegir No Compartir esta carpeta. [R8]

3.4.2.1 Carpetas Compartidas.

Windows XP Profesional dispone de una herramienta que muestra la lista de carpetas compartidas, su ubicación y el tipo de acceso, con el objeto de que podamos gestionarlas cómodamente. Además, indica una lista de usuarios conectados al equipo, desde el equipo donde se conectan y los ficheros que mantienen abiertos en cada instante.

Todo esto se obtiene haciendo:

- ✓ Un clic con el botón derecho del mouse sobre el icono MI PC en el escritorio.
- ✓ Seleccionando la opción Administrar. Con esto se abre la herramienta Administración de Equipos (que también es accesible a través del Panel de Control / Herramientas Administrativas). Como se observa en la figura 3.13.

Figura 3.13 Administración de equipos.

Carpetas compartidas se puede utilizar para ver un resumen de las conexiones y el uso de los recursos en equipos locales y remotos. Mediante esta herramienta, puede:

- ✓ Crear, ver y establecer permisos en recursos compartidos.
- ✓ Ver una lista de todos los usuarios conectados al equipo a través de una red y desconectar alguno de ellos o todos.
- ✓ Ver una lista de los archivos abiertos por usuarios remotos y cerrar alguno de ellos o todos.

Las **subcarpetas de Carpetas compartidas** contienen información, ordenada en columnas, acerca de todos los recursos compartidos, sesiones y archivos abiertos en el equipo. Los encabezados de las columnas de estas carpetas se definen de la siguiente manera:

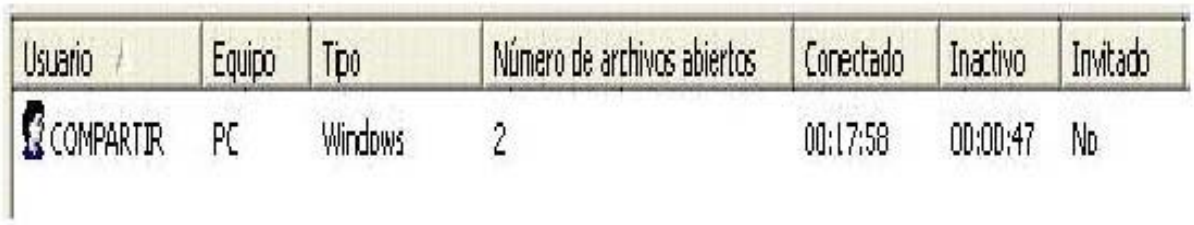
- ❖ **Recursos compartidos:** Contiene la información siguiente acerca de los recursos compartidos disponibles en el equipo. La figura 3.14 muestra información sobre recursos compartidos.
  - ✔ **Carpeta compartida:** Enumera los recursos compartidos disponibles en el equipo. Un recurso compartido puede ser una carpeta compartida, una impresora compartida etc.
  - ✔ **Ruta de acceso compartida:** Muestra la ruta del recurso compartido.
  - ✔ **Tipo:** Muestra el tipo de conexión de red: Windows
  - ✔ **Conexiones de cliente:** Muestra el número de usuarios que están conectados al recurso compartido.
  - ✔ **Comentario:** Describe el recurso compartido.

Carpeta compartida	Ruta de acceso compartida	Tipo	# Conexiones de cliente	Comentario
ADMIN$	C:\WINDOWS	Windows	0	Admin remota
Archivos de programa	C:\Archivos de programa	Windows	0	
C$	C:\	Windows	0	Recurso predeterminado
D$	D:\	Windows	0	Recurso predeterminado
IPC$		Windows	1	IPC remota
Mis documentos	D:\Documents and Settings\bd\Mis documentos	Windows	1	
print$	C:\WINDOWS\System32\SPOOL\DRIVERS	Windows	0	Controladores de impresora

Figura 3.14 Recursos compartidos.

- **Sesiones:** Contiene la información siguiente acerca de todos los usuarios de la red conectados al equipo: Como se muestra en la figura 3.15

  - **Usuario:** Enumera los usuarios de la red conectados al equipo.
  - **Equipo:** Muestra el nombre del equipo del usuario conectado.
  - **Tipo:** Muestra el tipo de conexión de red: Windows, Macintosh.
  - **Número de archivos abiertos:** Muestra el número de recursos abiertos por el usuario en este equipo.
  - **Tiempo conectado:** Muestra las horas y los minutos transcurridos desde que se estableció la sesión.
  - **Tiempo de inactividad:** Muestra las horas y los minutos transcurridos desde que este usuario inició una acción por última vez.
  - **Invitado:** Especifica si este usuario está conectado al equipo como invitado (se muestra Sí o No).



Usuario	Equipo	Tipo	Número de archivos abiertos	Conectado	Inactivo	Invitado
COMPARTIR	PC	Windows	2	00:17:58	00:00:47	No

Figura 3.15 Información de un recurso compartido.

Archivos Abiertos: Contiene la información siguiente acerca de todos los archivos abiertos en el equipo. Como se observa en la figura 3.16.

- **Archivo abierto:** Enumera los nombres de los archivos abiertos. Un archivo abierto puede ser un archivo, un trabajo de impresión en una cola de impresión, etc.
- **Abierto por:** El nombre del usuario que abrió el archivo o tuvo acceso al recurso.
- **Tipo:** El tipo de conexión de red: Windows, Macintosh.

- **No. de bloqueos:** Muestra el número de bloqueos del recurso.
- **Modo de apertura:** Muestra el permiso concedido cuando se abrió el recurso.

Figura 3.16 Abrir un archivo.

Para utilizar carpetas compartidas, debe de ser miembro del grupo Administradores o usuarios avanzados.

3.5 Seguridad en Windows XP Profesional.

Significado de los iconos de seguridad de Windows XP Profesional. [R9]

El icono de seguridad principal indica información y configuración de seguridad importante.

Cuestión de seguridad: riesgo potencial para la seguridad.

La Situación es más segura. El equipo usa la configuración de seguridad recomendada.

Aviso: La situación es posiblemente dañina. Considere ajustar la configuración de seguridad para mejorar la seguridad del equipo.

La configuración de seguridad actual del equipo no se recomienda.

3.6 Centro de Seguridad de Windows XP Profesional.

El Centro de seguridad supervisa la configuración de seguridad esencial y le advierte cuando el equipo puede estar en peligro. Como se muestra en la figura 3.17.

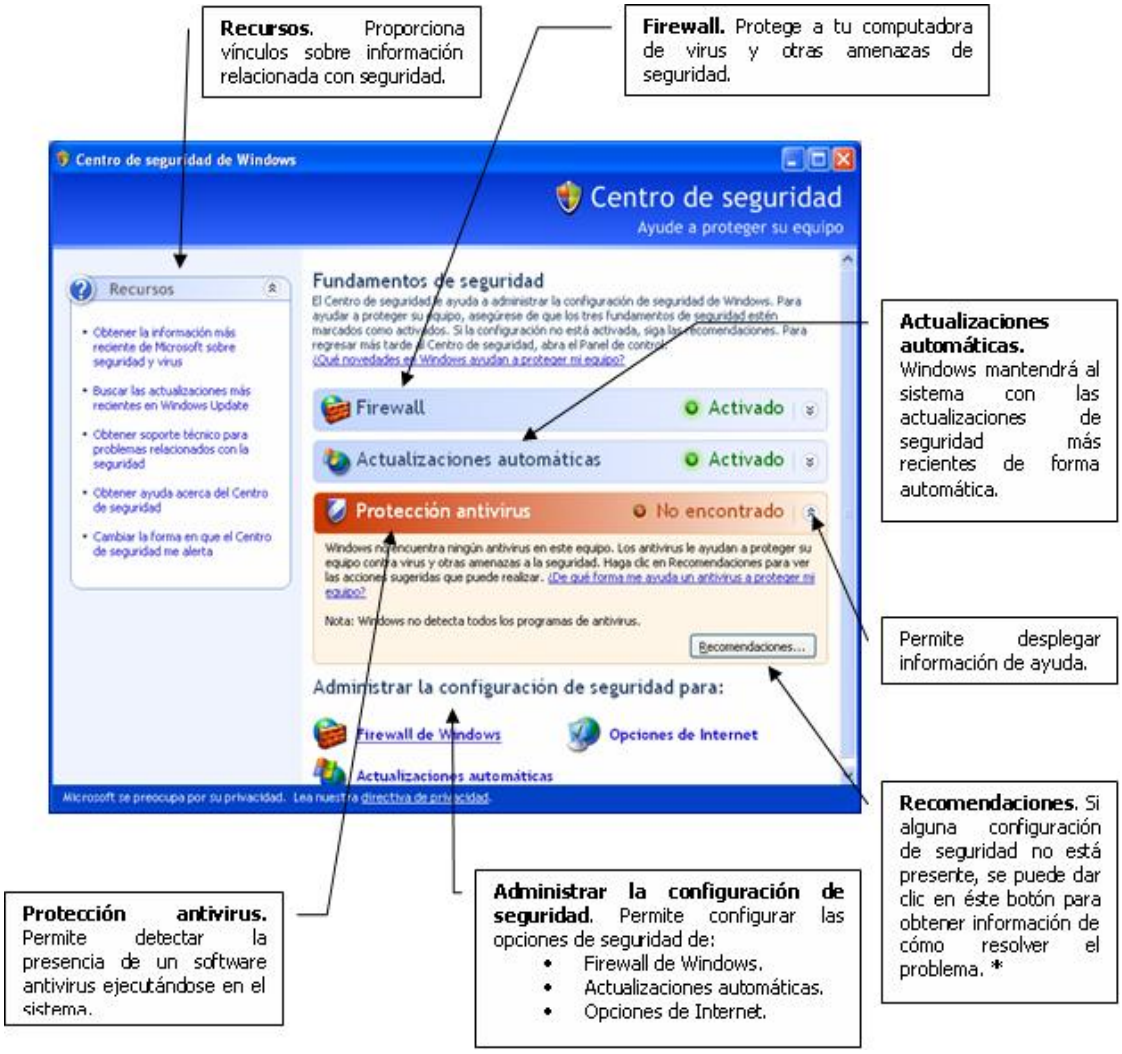


Figura 3.17 Centro de Seguridad de Windows.

El servicio del centro de seguridad se ejecuta como un proceso en segundo plano y comprueba el estado de los siguientes puntos esenciales de seguridad del equipo del usuario:

- ✓ Firewall de Windows.
- ✓ Actualizaciones automáticas.
- ✓ Protección antivirus.

- ❖ **Firewall.** El centro de seguridad comprueba si el Firewall de Windows esta activado o no, también puede comprobar la presencia de servidores de seguridad de terceros.
- ❖ **Actualizaciones automáticas.** El centro de seguridad comprueba y se asegura de que las actualizaciones automáticas estén configuradas de acuerdo con las opciones recomendadas para descargar e instalar automáticamente actualizaciones importantes en el equipo del usuario. Si las actualizaciones automáticas se desactivan o si no están configuradas según las opciones recomendadas, el centro de seguridad proporciona las recomendaciones apropiadas.
- ❖ **Protección contra virus** El Centro de seguridad comprueba la presencia de software antivirus mediante la búsqueda de proveedores específicos de Instrumental de administración de Windows (WMI), que los fabricantes participantes han proporcionado. Si la información está disponible, el servicio del Centro de seguridad informa si el software está actualizado y si cuenta con la exploración en tiempo real activada.

Si se encuentra que un componente importante esta en un estado no seguro o indetectable, el Centro de seguridad coloca un escudo rojo en el área de notificación de la barra de tareas del equipo así como también proporciona un mensaje de alerta al iniciar la sesión, este mensaje contiene vínculos al centro de seguridad que muestra un mensaje acerca del problema y le ofrece recomendaciones para solucionarlo. Como se muestra en la figura 3.18.

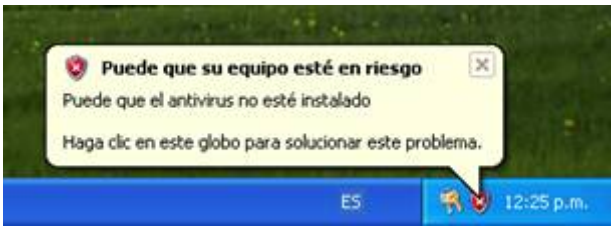


Figura 3.18 Área de notificación (icono del centro de seguridad).

Procedimientos que llevan al utilizar el Centro de seguridad:

- ✓ Modificaciones de las alertas del centro de seguridad.
- ✓ Configuración de las opciones de Firewall de Windows.
- ✓ Configuración de actualizaciones automáticas. [R9]

3.6.1 Firewall de Windows.

Un Firewall ayuda a mantener al equipo más seguro. Restringe la información que llega al equipo desde otros equipos, proporcionando un mejor control sobre los datos en el equipo y también proporciona una línea de defensa contra gente o programas que intentan conectarse al equipo sin autorización.

Un firewall es un barrera que verifica la información (llamado tráfico de red) proveniente de Internet o de una red y después bloquea o permite el paso de dicha información al equipo, dependiendo de las configuraciones del firewall.

En el Service Pack 2 de Windows XP Profesional la característica Firewall de Windows está habilitada de forma predeterminada, puede ser deshabilitado. [R10]

3.6.1.1 Nuevas características.

- ✓ Habilitado de forma predeterminada en todas las conexiones del equipo.
- ✓ Nuevas opciones de configuraciones globales que aplican a todas las conexiones.
- ✓ Nuevo conjunto de cuadros de diálogo para configuración local.
- ✓ Nuevo modo de operación.
- ✓ Seguridad en inicio del sistema.
- ✓ Puede ser exento tráfico específico por ámbito o alcance.
- ✓ Puede ser exento tráfico específico por el nombre de archivo de aplicación.
- ✓ Soporte incorporado para tráfico IP (Protocolo de Internet).

3.6.1.2 Funcionamiento del Firewall de Windows XP Profesional.

Cuando alguien en el Internet o en una red intenta conectarse a una computadora, intenta un "requerimiento no solicitado". Cuando el equipo obtiene un requerimiento no solicitado, el Firewall de Windows bloquea la conexión. Si está ejecutando un programa como lo es un programa de mensajería instantánea o un juego de red multiusuario que necesita recibir información desde Internet o desde una red, el firewall pregunta desea bloquear o permitir la conexión. Si escoge permitir la conexión, Firewall de Windows crea una excepción para que el firewall no pregunte nuevamente cuando este programa necesite recibir información en el futuro.

Por ejemplo, si se esta intercambiando mensajes instantáneos con alguien al cual se le desea enviar un archivo (una foto, por ejemplo), el Firewall de Windows preguntará si se desea permitir la conexión y permitir que la foto llegue al equipo.

Aunque puede deshabilitar la característica de Firewall de Windows para conexiones específicas de Internet y de red, hacer esto incrementa el riesgo que la seguridad de que su equipo pueda ser comprometido.

La figura 3.19 muestra lo que hace y no hace un firewall.

+	Ayuda a bloquear que virus y gusanos accedan al equipo.
+	Pide permiso al usuario para bloquear o permitir ciertos requerimientos de conexión.
+	Crea un registro de seguridad, dependiendo de lo que se configure (registro de intentos de conexiones satisfactorias o fallidas al equipo). El registro no está habilitado de forma predeterminada.
-	Detecta o deshabilita virus o gusanos si ya existen en el equipo.
-	Evita abrir correos electrónicos con archivos adjuntos maliciosos.
-	Bloquea spam o correo electrónico no solicitado.

Figura 3.19 Tabla de lo que hace y no hace un firewall.

3.6.1.3 Estructura del Firewall de Windows.

El nuevo cuadro de diálogo Firewall de Windows contiene las siguientes pestañas: como se muestra en la figura 3.20.

- ✓ General.
- ✓ Excepciones.
- ✓ Opciones avanzadas.

❖ **Pestaña General.** La pestaña General contiene las siguientes opciones de configuración predeterminadas:

Figura 3.20 Firewall de Windows

- ✓ **Activado (recomendado)**. Si se selecciona, permite habilitar el Firewall de Windows para todas las conexiones de red que están seleccionadas en la pestaña Opciones avanzadas. El Firewall de Windows está habilitado de forma predeterminada para permitir solo el tráfico entrante solicitado y exento. El tráfico exento es configurado en la pestaña Excepciones.

- ✓ **No permitir excepciones**. Si se selecciona solo se permitirá el tráfico entrante solicitado. El tráfico entrante exento no está permitido. Las configuraciones en la pestaña Excepciones son ignoradas y todas las conexiones de red son protegidas, independientemente de las configuraciones en la pestaña Opciones Avanzadas.

- ✓ **Desactivado (no se recomienda)**. Si se selecciona, la característica de Firewall de Windows será deshabilitada. Esto no es recomendado, especialmente si las conexiones de red son accesibles directamente desde el Internet, al menos que ya se este utilizando un producto de Firewall de terceros.

Es importante hacer notar que la opción predeterminada para el Firewall de Windows *es* Activado (recomendado) para todas las conexiones de un equipo ejecutando Windows XP Profesional y para nuevas conexiones creadas. Esto puede impactar las comunicaciones con programas o servicios que confían en tráfico entrante no solicitado. En este caso se deberían identificar estos programas que no funcionan y agregarlos o en su defecto su trafico como tráfico exento. Muchos programas, como los navegadores de Internet y clientes de correo electrónico (como Outlook Express), no confían en tráfico entrante no solicitado y operan adecuadamente con Firewall de Windows habilitado.

- **Pestaña Excepciones.** Contiene las siguientes opciones de configuración predeterminada. Como se muestra en la figura 3.21.

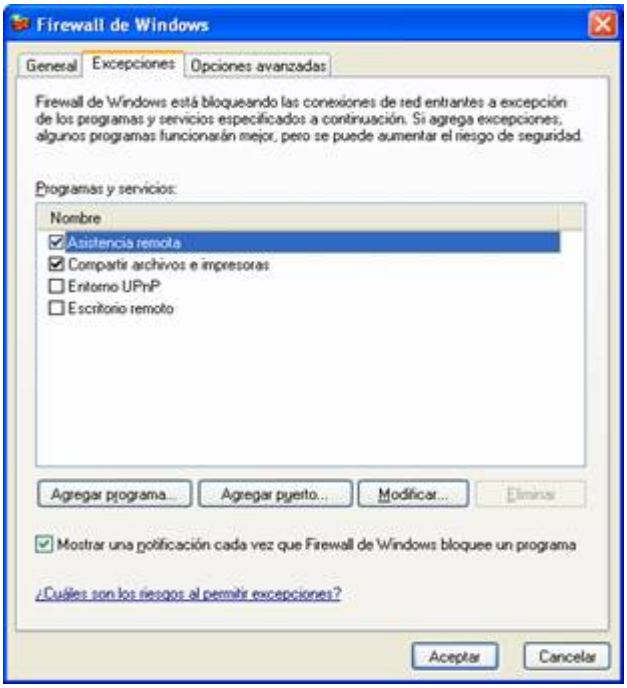


Figura 3.21 Firewall de Windows (Pestaña de Excepciones).

Mediante la pestaña Excepciones es posible habilitar o deshabilitar un programa o servicio existente o mantener una lista de programas y servicios que definen el

tráfico exento. El tráfico exento no está permitido cuando la opción No permitir excepciones esta seleccionada en la pestaña General.

Existe un conjunto de programas y servicios preconfigurados:

- ✓ Asistencia remota (habilitada de forma predeterminada).
- ✓ Compartir archivos e impresoras.
- ✓ Entorno UpnP.
- ✓ Escritorio remoto.

Estos programas y servicios no pueden ser eliminados.

Si es permitido por las Directivas de Grupo, es posible crear excepciones adicionales en base a un nombre de programa específico dando clic en Agregar programa y excepciones en base a un puerto TCP o UDP específico dando clic en Agregar puerto.

Agregar programa. Cuando se da clic en Agregar programa, es mostrado el cuadro de diálogo Agregar un programa desde el cual es posible seleccionar un programa o navegador para un nombre de archivo de programa. Como se muestra en la figura 3.22.

Figura 3.22 Agregar un programa

Agregar puerto. Cuando se da clic en Agregar puerto, es mostrado el cuadro de diálogo Agregar un puerto desde el cual es posible configurar un puerto TCP o UDP. Como se muestra en la figura 3.23.

Figura 3.23 Agregar un puerto.

El Firewall de Windows permite especificar el rango del tráfico exento. El ámbito define la porción del a red desde la cual el tráfico exento tiene permitido originarse. Para definir el ámbito para un programa o puerto, de clic en el botón Cambiar ámbito. Como se muestra en la figura 3.24.

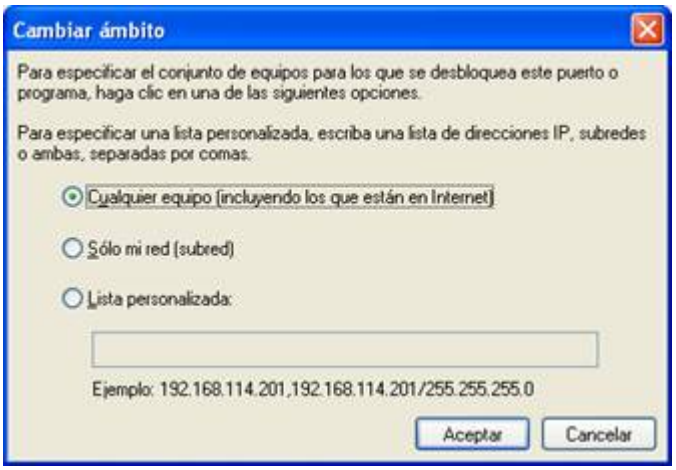


Figura 3.24 Cambiar ámbito.

Se tienen tres opciones para definir el ámbito para un puerto o programa:

- ✓ **Cualquier equipo (incluyendo los que están en Internet)**. El tráfico exento es permitido desde cualquier dirección de IP. Esta configuración podría hacer al equipo vulnerable a ataques provenientes de usuarios o programas maliciosos en Internet.
- ✓ **Sólo mi red (subred)**. El tráfico exento es permitido solo desde direcciones IP que cumplen con el mismo segmento de red local (subred) a la cual la conexión de red que recibe el tráfico esta conectada.
- ✓ **Lista personalizada**. Es posible especificar una o más direcciones IP o rangos de direcciones IP separadas por comas. Los rangos de direcciones IP corresponden típicamente a subredes. Para direcciones IP, se deben escribir las direcciones IP en notación de punto decimal. Para rangos de direcciones IP, se debe especificar el rango utilizando una mascara de subred con punto decimal o un prefijo de longitud.

El ámbito **Sólo mi red (subred)** es utilizado cuando se desea permitir el acceso a un programa o servicio para las computadoras en una red casera local que están todas conectadas a la misma subred, pero no para usuarios de Internet potencialmente maliciosos.

Una vez que un programa o puerto es agregado, éste es deshabilitado de forma predeterminada en la lista Servicios y programas.

Todos los programas o servicios habilitados en la pestaña Excepciones son habilitados para todas las conexiones que están seleccionadas en la pestaña Opciones Avanzadas. Como se muestra en la figura 3.25.

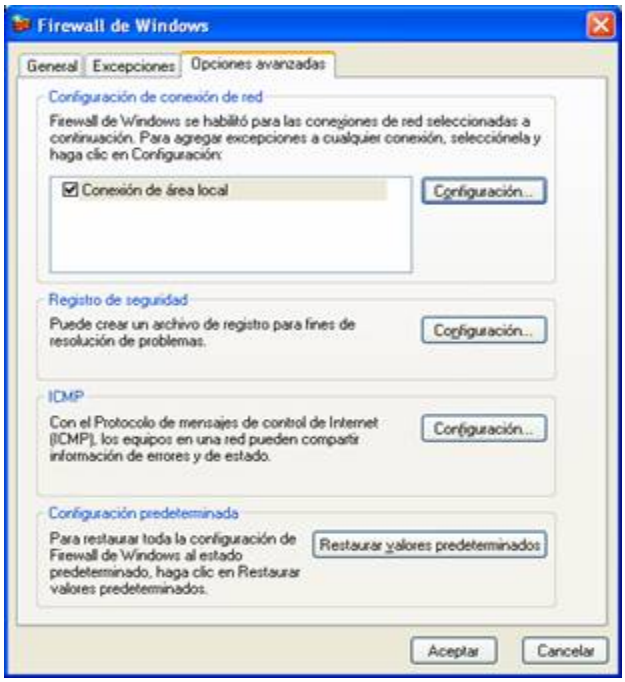


Figura 3.25 Firewall de Windows (Pestaña opciones avanzadas).

❖ **La pestaña Opciones avanzadas** contiene las siguientes secciones:

- ✓ Configuración de conexión de red.
- ✓ Registro de seguridad.
- ✓ ICMP.
- ✓ Configuración predeterminada.

- ✓ **Configuración de conexión de red**. Mediante esta opción de configuración es posible:

Especificar el conjunto de interfaces en las cuales el Firewall de Windows está habilitado. Para habilitar una interfaz, se debe seleccionar el cuadro de verificación que esta situado junto al nombre de la conexión a Internet. Para deshabilitarla, se debe limpiar el cuadro de verificación. De forma predeterminada, todas las conexiones de red tienen habilitadas el Firewall de Windows. Si una conexión de red no aparece en la lista, significa que no es una conexión de red estándar.

Configurar opciones avanzadas de una conexión Configurar opciones avanzadas de una conexión de red individual seleccionando el nombre de la conexión de red y después dando clic en el botón **Configuración.**

Si se deseleccionan todos los cuadros de verificación en la opción Configuración de conexión de red*,* entonces el Firewall de Windows no está protegiendo el equipo, independientemente si se ha seleccionado la opción Activado (recomendado*)* en la pestaña General*.* Las opciones de configuración en Configuración de conexión de red son ignoradas si se ha seleccionado no permitir excepciones en la pestaña General*,* en éste caso, todas las interfaces están protegidas.

Cuando se da clic en el botón **Configuración**, el cuadro de diálogo **Configuración avanzada***,* es desplegado (ver figura 3.26). En este cuadro de diálogo, es posible configurar servicios específicos desde la pestaña Servicios (solo por puerto TCP o UDP) o habilitar tipos específicos de tráfico ICMP desde la pestaña ICMP. Estas dos pestañas son equivalentes a las pestañas de configuración del Servidor de seguridad de conexión a Internet en Windows XP Profesional anterior al Service Pack 2.

Figura 3.26 configuración avanzada.

- ✓ **Registro de seguridad.** Dentro de esta pestaña se debe dar clic en el botón Configuración para especificar la configuración del registro de Firewall de Windows en el cuadro de diálogo Configuración de registro. Como se muestra en la figura 3.27.

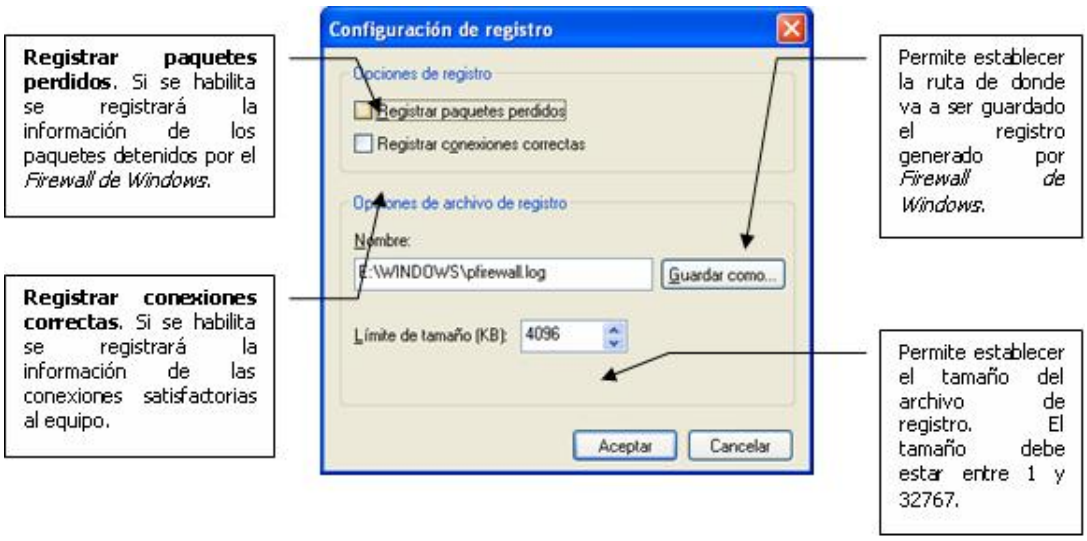


Figura 3.27 Configuración de registro.

Mediante el cuadro de diálogo Configuración del registro, es posible configurar si en el registro se escribirán los paquetes bloqueados por el firewall *(*Registrar paquetes perdidos*)* o las conexiones satisfactorias *(*Registrar conexiones correctas*)* o ambas. También a través de este cuadro de diálogo es posible especificar el nombre y localización del archivo de registro y su tamaño máximo.

- ✓ **ICMP.** Dentro de esta pestaña se debe dar clic en el botón Configuración para especificar los tipos de tráfico ICMP (como se muestra en la figura 3.28), que serán permitidos en el cuadro de diálogo Configuración de ICMP.

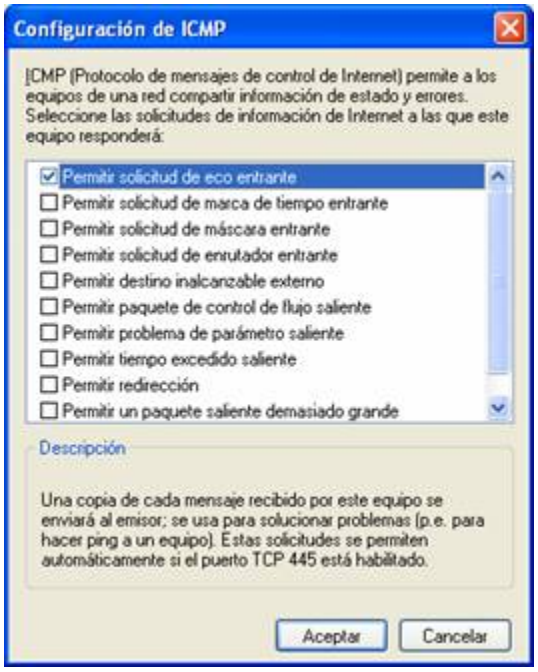


Figura 3.28 Configuración de ICMP.

Mediante el cuadro de diálogo Configuración de ICMP es posible habilitar y deshabilitar los tipos de mensajes ICMP entrantes que el Firewall de Windows permitirá para las conexiones seleccionadas en la pestaña Opciones avanzadas. Los mensajes ICMP son utilizados para diagnostico, condiciones de reportes de error y para configuración. De forma predeterminada ningún tipo de mensaje ICMP en la lista es permitido.

Una técnica común en la resolución de problemas de conectividad es utilizar la herramienta Ping contra la dirección del equipo al cual se está tratando de conectarse. Cuando se realiza un ping, se envía un mensaje de eco ICMP y se obtiene un mensaje de Respuesta de Eco ICMP.

De forma predeterminada, el Firewall de Windows no permite mensajes de Eco ICMP entrantes y por lo tanto el equipo no puede enviar una Respuesta de Eco ICMP como respuesta. Para configurar el Firewall de Windows para permitir mensajes de Eco ICMP entrantes se debe habilitar la opción de configuración Permitir solicitud de eco entrante.

- ✓ **Configuración predeterminada.** Si se da clic en el botón Restaurar valores predeterminados es posible reestablecer el Firewall de Windows a su estado original de instalación. Cuando se da clic en el botón Restaurar valores predeterminados aparece un cuadro de diálogo para verificar la decisión antes de que las configuraciones del Firewall de Windows sean cambiadas.

3.6.1.4 Configuración de Firewall de Windows XP Profesional.

Habilitación de Firewall de Windows en una conexión basada en red:

- ✓ Desde centro de seguridad, en administrar la configuración de seguridad, hacer clic en Firewall de Windows.
- ✓ En Firewall de Windows hacer clic en la ficha opciones avanzadas
- ✓ En la ficha opciones avanzadas, en el área configuración de conexiones de red, quitar las conexiones que no necesita que proteja Firewall de Windows.
- ✓ En la ficha opciones avanzadas, en el área configuración de conexión de red, hacer clic para resaltar la conexión especifica para la que desea configurar opciones del servidor de seguridad diferentes de las predeterminadas y hacer clic en Configuración.

- ✓ Seleccione o quite el servicio específico que desea habilitar o deshabilitar para esta conexión.
- ✓ Si no se muestra el servicio que desea habilitar para esta conexión, hacer clic en Agregar.
- ✓ En la página Configuración del servicio, escriba los detalles del servicio que desea habilitar y hacer clic en Aceptar.
- ✓ Hacer clic en Aceptar para cerrar la página Configuración avanzada. [R10]

3.6.2 Actualizaciones Automáticas.

Actualizaciones Automáticas es un sitio Web de Microsoft que facilita actualizaciones para las diversas ediciones del sistema operativo Windows. Estas actualizaciones solucionan problemas conocidos y ayudan a protegerse de amenazas contra la seguridad. La figura 3.29 muestra la ventana principal de actualizaciones automáticas.

Las actualizaciones se dividen en las categorías siguientes:

- **Máxima prioridad**: incluye actualizaciones críticas, actualizaciones de seguridad y Service Packs. Se recomiendan que se instalen**,** ya que, por ejemplo, algunos virus que se aprovechan de los puntos débiles de Windows pueden ser neutralizados por las actualizaciones de seguridad.
- **Software (opcional)**: se trata de actualizaciones no críticas para programas de Windows como Windows Media(r) Player. Sólo deberá instalar estas actualizaciones si las necesita.
- **Hardware (opcional)**: se trata de actualizaciones no críticas para controladores (software que permite que dispositivos como impresoras o tarjetas gráficas se comuniquen con Windows).

La pantalla de configuración *de* Actualizaciones automáticas accesible a través de Sistema*,* en el Panel de Control también ha sido considerablemente cambiada con

texto claro y un vínculo al sitio Web Windows Update para los usuarios que deseen realizar una actualización manual. Éste cuadro de diálogo de configuración también es accesible desde la opción Actualizaciones automáticas del Centro de Seguridad de Windows.

Las configuraciones predeterminadas del cuadro de diálogo Actualizaciones automáticas son las siguientes:

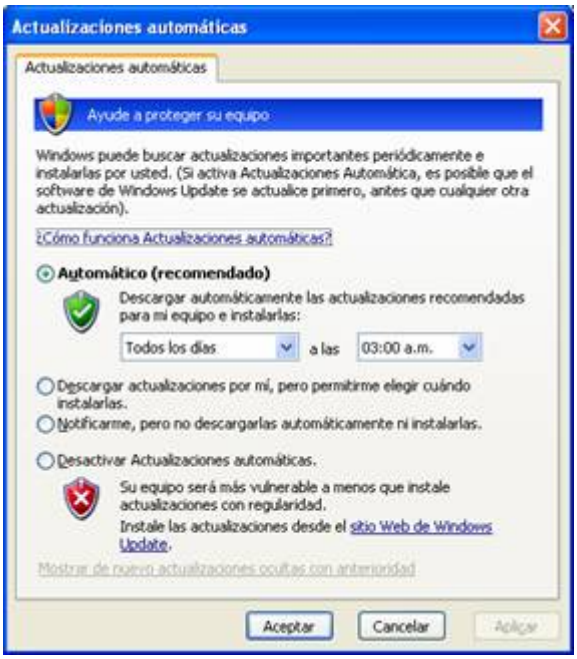


Figura 3.29 Ventana de actualizaciones automáticas.

Dentro del cuadro de diálogo Actualizaciones automáticas es posible configurar alguna de las siguientes opciones:

- ✓ **Automático (recomendado)**. Descarga automáticamente las actualizaciones recomendadas para el equipo y las instalas de acuerdo a lo programado. La programación predeterminada es descargarlas todos los días e instalarlas a las 3:00 a.m. La programación puede ser cambiada de acuerdo a lo deseado.

- ✓ **Descargar actualizaciones por mí, pero permitirme elegir cuándo instalarlas**. Permite descargar las actualizaciones disponibles pero pedirá al usuario permiso para la instalación.
- ✓ **Notificarme, pero no descargarlas automáticamente ni instalarlas**. Esta opción solo notifica al usuario la existencia de actualizaciones disponibles, pero el usuario decidirá si las descarga y las instala.
- ✓ **Desactivar actualizaciones automáticas**. Deshabilita la descarga automática de actualizaciones, esto puede dejar al equipo vulnerable en el caso de que sea liberada una actualización de seguridad crítica, al menos que se instale manualmente. Esta opción proporciona un vínculo al sitio Web de Windows Update.

3.6.2.1 Para instalar las últimas actualizaciones de Windows del sitio Web Windows Update:

1. Iniciar sesión con derechos de administrador.
2. Conectarse a Internet y entrar en el sitio Web Windows Update.
3. Hacer clic en el botón de inicio.
4. Seleccionar la opción de todos los programas.
5. Dar un clic en la opción de Windows Update (situado en la parte superior del menú de inicio). También se puede actualizar desde:

    - ✓ Hacer clic en el botón de Inicio.
    - ✓ Seleccionar la opción de ayuda y soporte técnico.
    - ✓ Hacer clic en la opción de mantener actualizado su equipo con Windows Update (en elegir una tarea).

6. Aparecerá la siguiente pantalla: Como se muestra en la figura 3.30.

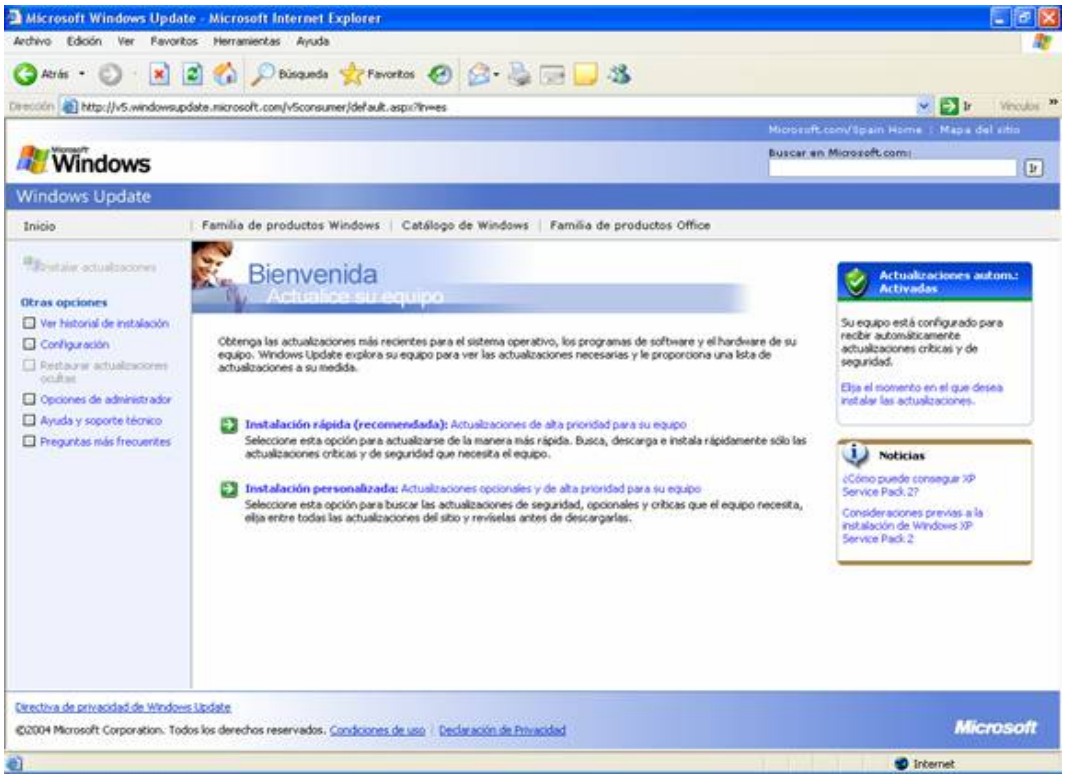


Figura 3.30 Bienvenida de Windows Update.

7.- Seleccionar **Instalación rápida (recomendada)** para instalar sólo actualizaciones críticas y de seguridad. Seleccionar **Instalación personalizada** si desea instalar otras actualizaciones opcionales además de las actualizaciones críticas y de seguridad.

Windows Update buscará las actualizaciones disponibles.

Si se ha elegido la **Instalación rápida**, hacer clic en **Instalar** para instalarlo todo de una vez.

Si se ha elegido **Instalación personalizada**, se puede ver y seleccionar cada actualización antes de instalarla. Utilizar el panel de navegación situado a la izquierda para cambiar entre las distintas categorías. Cuando se esté de acuerdo, hacer clic en el botón para **descargar e instalar ahora.**

8.- Seguir las instrucciones de la pantalla y reiniciar el equipo cuando se solicite. Se recomienda que se reinicie siempre el equipo inmediatamente después de instalar programas nuevos. De lo contrario el equipo podría comportarse de forma impredecible.

CAPITULO 4

CASO DE ESTUDIO:

"ADMINISTRACIÓN DE LA RED DEL CENTRO DE CÓMPUTO ACADÉMICO CAMPUS TLAHUELILPAN DE LA UAEH".

En este capítulo se muestra la administración de red que se lleva en el Centro de Cómputo Académico Campus Tlahuelilpan de la Universidad Autónoma del Estado de Hidalgo, así como las medidas de seguridad que se llevan dentro del Centro de Cómputo Académico.

Así mismo en este capítulo se ofrece un panorama de forma general de la administración de redes utilizando el sistema operativo Windows XP Profesional SP2 en el CECA del Campus Tlahuelilpan.
La administración de red que se lleva en el CECA es con respecto a hardware, software, configuración y seguridad de red.

La seguridad de los equipos de la red cuenta con varias políticas. La intención de estas políticas de la red es establecer un marco de referencia que asegure la protección adecuada para los equipos.
El personal del CECA debe involucrarse en la coordinación y cooperación para satisfacer las necesidades de la red. Los usuarios deben estar estrictamente limitados a las áreas no autorizadas.

4.1 Antecedentes del Campus Tlahuelilpan de la UAEH.

La Universidad Autónoma del Estado de Hidalgo en su afán por formar más profesionistas y ante los requerimientos de la sociedad hidalguense se da a la tarea de abrir Campus, como lo es actualmente el Campus Tlahuelilpan.

El Campus Tlahuelilpan representa un paso adelante en el programa de descentralización de la educación superior en la entidad, como expresión de la pertinencia de esta casa de estudios. Fué inaugurado por el expresidente Dr. Ernesto Zedillo Ponce de León, acompañado del exgobernador Lic. Manuel Ángel Núñez Soto y del Rector Lic. Juan Manuel Camacho Beltrán.

El Campus Tlahuelilpan comenzó su funcionamiento con la impartición de dos licenciaturas que son las que los sectores públicos, privados y sociales requieren para incidir positivamente en su desarrollo armónico.

Este espacio universitario vino a favorecer a los jóvenes de los municipios de: Tlahuelilpan, Tlaxcoapan, Tetepango, Progreso, Mixquiahuala, Tula, Chapantongo, Tepetitlan, entre otros que se ubican en esta región.
Este proyecto fué posible gracias al apoyo brindado por la Secretaría de Educación Pública, el gobierno del estado, la presidencia municipal y los sectores empresariales y sociales de la región.

4.2 Antecedentes del Centro de Cómputo Académico Campus Tlahuelilpan de la UAEH. [E2]

El Centro de Cómputo Académico Campus Tlahuelilpan inició con 5 equipos conectados a la red, fueron distribuidos de la siguiente manera:

- ✓ 4 equipos en laboratorio.
- ✓ 1 equipo (servidor), se conecta a un modem.

Posteriormente se implementó a 14 equipos:

- ✓ 4 equipos para laboratorio.
- ✓ 10 equipos en aula de cómputo.
- ✓ 1 equipo en administración de cómputo.
- ✓ 1 equipo en dirección.
- ✓ 1 equipo en control escolar.
- ✓ 2 líneas de voz.

En el período de Julio-Diciembre de 2004 se autorizó el proyecto de red del Campus Tlahuelilpan. Se inició con 20 equipos de red en laboratorio, 26 equipos en aula de cómputo, 14 equipos distribuidos en áreas como: biblioteca, autoacceso, educación continua, servicio social, coordinación de carreras.

Posteriormente en el período Enero-Junio de 2004, se inició la conexión de aula virtual. Así como también se autorizó la ampliación de la red.

4.3 Objetivo del CECA.

Apoyar con criterios de calidad, eficiencia y seguridad las actividades de cómputo en las áreas académicas, de investigación y administrativas del Campus.

4.4 Visión.

La Dirección General de Servicios Académicos proporciona servicios sistematizados y automatizados de calidad acordes a las necesidades de los programas Educativos y a las nuevas formas de aprendizaje; con tecnología de vanguardia y el respaldo de una evaluación permanente a fin de contribuir a la aceptación de sus egresados y a la vinculación de los sectores productivo y social.

4.5 Misión.

Coordinar los servicios de apoyo académico del Centro de autoacceso, Vinculación, Biblioteca, Centros de Información, Laboratorios y Talleres, conforme a los programas académicos y proyectos de investigación institucionales que refuercen los conocimientos teóricos-metodológicos, el desarrollo de habilidades, destrezas y aptitudes de los usuarios.

4.6 Función.

El centro de cómputo académico tiene como función esencial brindar servicios de calidad a los usuarios del Campus Tlahuelilpan, integrando personal capacitado, equipos actuales, así como herramientas y material que satisfagan las necesidades de Mantenimiento Preventivo y Correctivo de equipos de cómputo, Soporte Técnico y Servicios de Internet.

4.7 Formación del Centro de Cómputo Académico.

Actualmente el Centro de Cómputo Académico cuenta con:

- ✓ Área de SITE.
- ✓ Área de Control.
- ✓ 1 Laboratorio.
- ✓ 2 Aulas de cómputo.

4.7.1 Área de SITE.

En esta área solo puede entrar personal autorizado (sólo entra la encargada y auxiliar del Centro de Cómputo Académico), es una área restringida, debido a que en esta área se encuentra el RAC de comunicaciones, el modem y el concentrador, partes importantes de la red. Actualmente se cuenta con un ancho de banda de 512 kbps.

4.7.2 Área de Control.

La función de esta área es la atención a usuarios. Desde esta área el usuario (alumno) realiza su reservación para que pueda tener derecho a la utilización de un equipo (después de clases).

4.7.3 Laboratorio (Sala de Cómputo).

Es el área en donde los usuarios tienen derecho a utilizar un equipo después de haber reservado, para realizar alguna investigación o trabajo.

Actualmente este laboratorio cuenta con 18 equipos, todos tienen conexión a Internet y tienen instalado el sistema operativo Windows XP Profesional (SP2), el antivirus Hauri y el AntiSpyware Windows Defender.

4.7.3.1 Características de los equipos del laboratorio:

- ✓ Pentium 4 a 2.0 Ghz.
- ✓ Disco duro de 40 GB.
- ✓ 256 de memoria RAM.
- ✓ Unidad de 3 ½.
- ✓ Tarjeta de Red.
- ✓ Monitor de 15 Pulgadas.

4.7.4 Aulas de Cómputo.

Son las aulas es donde todos los alumnos del Campus se les imparten sus clases de computación. El Centro de Cómputo Académico cuenta con dos aulas de cómputo y cada aula cuenta con 24 equipos de cómputo. Todos los equipos cuentan con conexión a Internet y tienen instalado el sistema operativo Windows XP Profesional (SP2), el antivirus Hauri y el AntiSpyware Windows Defender.

4.7.4.1 Características de los equipos de las aulas.

Aula número uno:

- ✓ Pentium 4 a 3.0 Ghz.
- ✓ 512 de memoria RAM.
- ✓ 2 discos duros de 40 GB (cada disco).
- ✓ Unidad de 3 ½.
- ✓ Grabador CD.
- ✓ Tarjeta de Red.
- ✓ Monitor de 17 pulgadas.

Aula número dos:

- ✓ Pentium 4, a 2.4 Ghz.
- ✓ 256 de memoria RAM.
- ✓ 2 discos duros de 40 GB (cada disco).
- ✓ Unidad de 3 1/2.

- ✓ Unidad de CD.
- ✓ Tarjeta de Red.
- ✓ Monitor de 15 pulgadas.

4.8 Tipos de Servicios.

Los principales servicios informáticos que ofrece el Centro de Cómputo son:

- ✓ Administración del Área de Control.
- ✓ Administración del SITE.
- ✓ Administración de 2 aulas de cómputo.
- ✓ Administración del laboratorio (Sala de cómputo).
- ✓ Administración del segmento de la red del Campus.
- ✓ Mantenimiento preventivo y correctivo del equipo de cómputo.
- ✓ Instalación y mantenimiento de Software.
- ✓ Cursos de capacitación.
- ✓ Asesorías a los usuarios.

4.9 Usuarios.

Se consideran usuarios a todos los catedráticos (de tiempo parcial y tiempo completo), alumnos y personal administrativo del Campus Tlahuelilpan, que se encuentren en activo en la universidad.

Para estar debidamente registrado como usuario, los usuarios (alumnos) deben, cuando el personal del centro de cómputo se los requiera, acreditar su relación con la institución mediante presentación de credencial o tira de materias vigente.

4.10 Dirección de Telecomunicaciones de la UAEH.

La administración de la Red del Campus Tlahuelilpan, así como la de los demás campus, se lleva en Red Universidad en el área de Telecomunicaciones.

La Dirección de Telecomunicaciones proporciona los servicios de datos, voz y video a través de la red universitaria en los diferentes institutos, campus y escuelas remotas de la Universidad Autónoma del Estado de Hidalgo, para ello cuenta con tecnología de punta y personal capacitado.

El área de Telecomunicaciones es el área que se encarga de administrar toda la infraestructura de la red. Como se muestra en la figura 4.1 [R11]

Figura 4.1 Dirección de Telecomunicaciones.

Uno de los nodos de la red universitaria es para el Campus Tlahuelilpan, la comunicación con el campus se realiza desde el nodo central a través de dos enlaces S0 (digital Signal 0, Señal Digital 0) de Telmex de 512 Kbps de ancho de banda cada uno, uno de los cuales se utiliza para la transmisión de datos y el otro para la transmisión de voz. Es necesario para establecer dicha comunicación un enrutador que maneje voz y datos sobre IP tanto en el nodo remoto (Campus Tlahuelilpan) como en el nodo principal. Este nodo remoto tiene 23 servicios de datos y 2 de voz.

De acuerdo a la entrevista (ver anexo 1), que se le realizó al Lic. Computación David Rivero Borja, administrador de red, de Telecomunicaciones UAEH, menciona las actividades que se realizan para llevar una buena administración de la red de este nodo y son: [E4]

4.10.1 Administración del rendimiento.

Tiene como objetivo recolectar y analizar, el tráfico que circula por la red para determinar su comportamiento en diversos aspectos.

La administración del rendimiento se puede dividir en dos etapas:

Monitoreo. Consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como:

- ✓ Utilización de enlaces. Se refiere a las cantidades ancho de banda utilizado por cada uno de los enlaces.
- ✓ Caracterización de tráfico. Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red.

Análisis. Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a su mejor desempeño

Durante el proceso de análisis se pueden detectar comportamientos como por ejemplo:

- ✓ Tráfico inusual. El haber encontrado mediante el monitoreo, las aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual, aportando elementos importantes en la solución de problemas que afecten al rendimiento de la red.
- ✓ Elementos principales de la red. Algo muy importante es conocer cuales son los elementos a los cuales establecer un monitoreo más constante. Si se detecta un elemento que no se encuentra dentro de los equipos con más actividad, puede ayudar a la detección de ataque contra la seguridad de dicho equipo.
- ✓ El servicio, garantiza mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, Voz sobre IP (VoIP).
- ✓ Control del tráfico. Puede ser enrutado por otro.

Todo esto se debe estar revisando y actualizando constantemente, preferentemente a diario.

4.10.2 Administración de Fallas.

Su objetivo es detectar y solucionar oportunamente situaciones anormales en la red. Consiste en varias etapas, primero una falla debe ser detectada y reportada de manera inmediata, una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son algunas veces la manera de localizar el origen de una falla, una vez que el origen ha sido detectado se debe de tomar las medidas correctivas para reestablecer la situación de la falla.

Cuando se detecta una falla en algún equipo del campus Tlahuelilpan lo que hacen es desactivarlo para que de esta forma no afecte a los demás equipos y de inmediato hay que localizar el origen de la falla.

Localización de fallas. Es importante para identificar las causas que han originado la falla. La alarma indica el lugar del problema pero las pruebas son las que ayudan a determinar el origen de la misma, una vez identificado el origen se tiene que tomar las acciones suficientes para reparar el daño.

4.10.3 Corrección de Fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En este trabajo profesional sólo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos de una red basada en interruptores que pueden aplicarse, se encuentran los siguientes.

- ✓ Reemplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- ✓ Aislamiento del problema. Aislar el recurso que se encuentra dañado además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- ✓ Redundancia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.

- ✓ Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- ✓ Instalación de software. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- ✓ Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

4.11 ADMINISTRACIÓN DE LA RED DEL CENTRO DE CÓMPUTO ACADÉMICO CAMPUS TLAHUELILPAN DE LA UAEH, BAJO EL ENTORNO DE WINDOWS XP PROFESIONAL (SP2).

Aparte de la Administración que se lleva del Centro de Cómputo Académico Campus Tlahuelilpan en Telecomunicaciones también se lleva una administración de manera interna.

Dentro del centro de cómputo académico de este campus se lleva una administración de red adecuada con respecto a hardware, software, configuración y seguridad, haciendo uso del sistema operativo Windows XP Profesional.

El concepto administrador de acuerdo con Microsoft Windows XP Profesional persona responsable de configurar y administrar controladores de dominio o equipos locales, y sus cuentas de usuario y de grupo correspondientes, asignar contraseñas y permisos, así mismo ayudar a los usuarios a solucionar problemas de red. Los administradores son miembros del grupo Administradores y tienen control total del dominio o el equipo.

4.11.1 Administración de la Configuración. [E2]

Dentro del proceso de la administración de la configuración de la red, se lleva a cabo las siguientes actividades como son la instalación y administración correcta del software; administración de hardware, así como los procedimientos y políticas que son de ayuda para el desarrollo de esta área.

4.11.2 Instalación y Administración del Hardware y Software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red. Para ello se propone el formato de Administración de Hardware y Software. Ver anexo 2.

4.11.3 Instalaciones de Hardware.

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento y abarcan un dispositivo completo como un ruteador o solo una parte de los mismos, como una tarjeta de red, etc.

Proceso de instalación:

- ✓ Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- ✓ Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- ✓ Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- ✓ Coordinar la configuración del hardware con la de software.

4.11.4 Administración del Software.

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además de mantener un control sobre los programas que serán utilizados.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente:

- ✓ Que las cantidades de memoria de almacenamiento sean suficientes para el nuevo software.
- ✓ Asegurar que no existan conflicto alguno, entre las versiones actuales y las que se pretenden instalar.
- ✓ Respaldo de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado.

En el centro de Cómputo se lleva una tarea especial que tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Esta tarea es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables,

tarjetas, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar los recursos de la red, tanto de software como de hardware:

- ✓ Algunos elementos de hardware más importantes como son: tarjetas, fuentes de poder, equipos para sustitución.
- ✓ Instalación de aplicaciones más utilizadas
- ✓ Respaldo de configuraciones
- ✓ Procedimiento de instalación de una nueva versión de sistema operativo

4.11.5 Seguridad en los equipos de la Red.

El objetivo primordial es proporcionar una mejor seguridad a cada unos de los equipos así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques. La prevención de ataques tiene como objetivo el mantener los recursos de red fuera del alcance de usuarios maliciosos, algo que no hay que olvidar es que los ataques solamente se reducen pero nunca se eliminan del todo.

4.11.5.1 Administración del equipo de cómputo.

En el Ceca para llevar a cabo una buena administración de los equipos, las responsables llevan a cabo las siguientes reglas.

- ✓ Cambiar la cuenta de administrador por otra menos obvia.
- ✓ Deshabilitar las cuentas de invitados.
- ✓ Asignar el nombre del equipo acorde con su uso.
- ✓ No compartir carpetas ni archivos, en caso de ser necesario, protegerlas con una contraseña, de ocho caracteres o más.
- ✓ No instalar aplicaciones que necesiten de una conexión permanente (kazaa).
- ✓ Memorizar las contraseñas y no compartirlas.
- ✓ Restringir el acceso físico al equipo.
- ✓ Hacer respaldos de la información para evitar pérdidas.

Ningún equipo o recurso de cómputo puede usar y/o tener instaladas herramientas de software que no haya sido previamente autorizados por la responsable del centro de cómputo académico.

4.11.6 Políticas de Seguridad.

Algo importante que se debe de tener en cuenta son los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. La Lic. Mónica García Murguía, encargada y la Lic. Norma Lilia Cornejo Reyna auxiliar del centro de cómputo académico, son las personas responsables de llevar a acabo todas las políticas después de haber realizado un análisis profundo de las necesidades de seguridad.

- ✓ Políticas de cuentas de usuarios.
- ✓ Políticas de contraseñas.
- ✓ Políticas de respaldo.
- ✓ Políticas de listas de acceso.

4.11.6.1 Políticas de Cuentas de Usuario.

Dentro del centro de cómputo académico se cuenta con la política de seguridad de cuentas de usuario. Con esta opción se pueden administrar cuentas de usuarios de manera fácil. Refuerza varias funciones, como la forma en que los usuarios inician una sesión en el sistema y utiliza un enfoque de administración orientado a tareas.

Los equipos del centro de cómputo cuentan con dos tipos de cuentas de usuario:

- ✓ **Cuenta de Administrador.**
- ✓ **Cuenta limitada (la cuenta de invitado es desactivada).**

A la cuenta de administrador solo podrán accesar las personas responsables del centro de cómputo académico, un usuario con una cuenta de administrador de equipo puede crear eliminar y modificar todas las cuentas de usuario del equipo. Puede hacer cambios en todo el sistema, instalar o desinstalar programas y tener acceso a todos los archivos.

La cuenta Limitada está reservada para los alumnos como una política de seguridad para los equipos del centro de cómputo.

La figura 4. 2 muestra el cuadro de dialogo de Cuentas de Usuario.

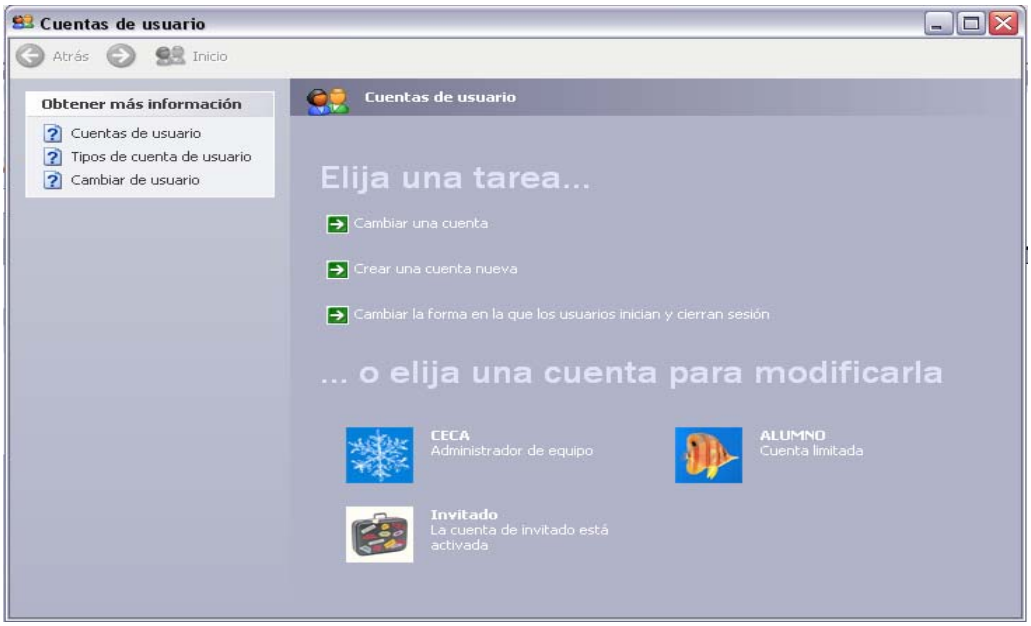


Figura 4.2 Cuadro de dialogo de cuentas de usuario.

Esta opción permite a los usuarios cambiar algunas características de su cuenta como la imagen que se despliega en la pantalla de bienvenida.

Se puede cambiar una cuenta, crear cuentas nuevas así como Cambiar la forma en la que los usuarios inician y cierran sesión.

Cambiar una cuenta: esta opción permite Cambiar nombre, cambiar contraseña, quitar contraseña, cambiar imagen, cambiar tipo de cuenta, etc.

Las cuentas de usuario proporcionan una vista personalizada de los archivos del usuario, una lista de sitios Web favoritos y una lista de páginas Web visitadas recientemente. Con una cuenta de usuario, los documentos que cree o guarde se almacenarán en su propia carpeta Mis documentos, separados de los documentos de otros usuarios que también utilizan el equipo.

Si tiene una cuenta de usuario y cambia la configuración de equipo, como el tipo, el tamaño o el protector de pantalla, esa configuración sólo se aplicará a su cuenta.

4.11.6.2 Políticas de Contraseña.

Otra política de seguridad que se aplica en centro de cómputo académico es la política de contraseñas.

Las contraseñas se cambian mensualmente. En la figura 4.3 se muestra cual es el procedimiento a seguir para cambiar una contraseña en Windows XP Profesional.

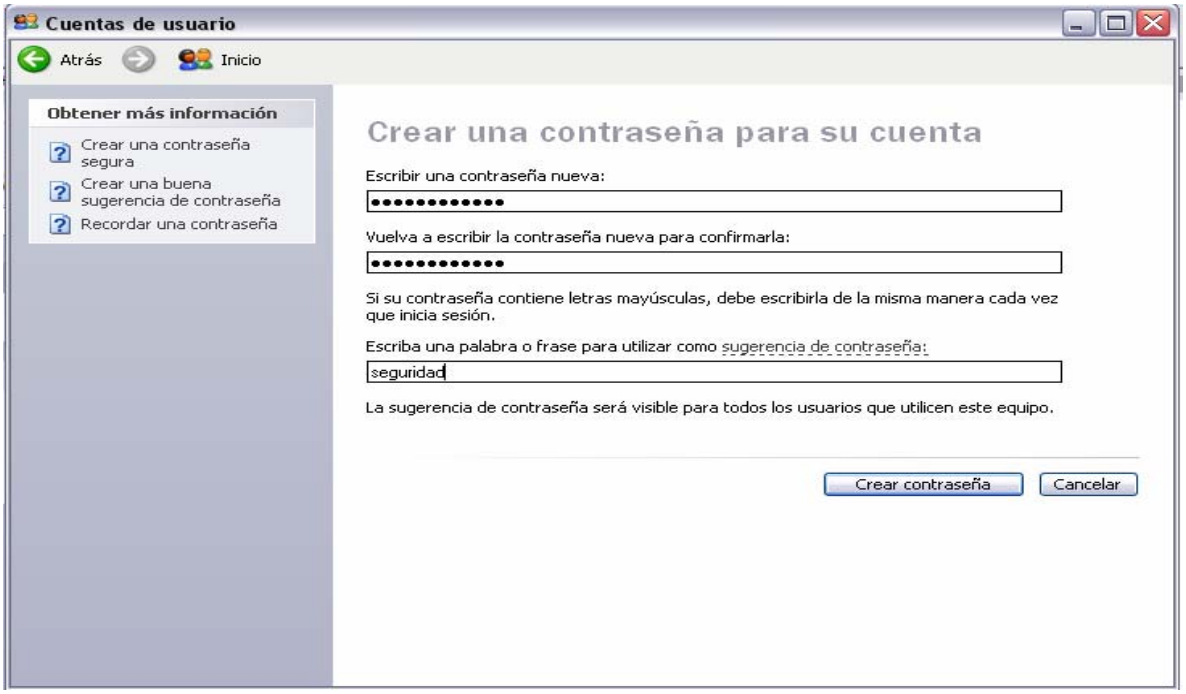


Figura 4.3 Contraseña para una cuenta.

4.11.6.3 Políticas de Respaldo.

Los procedimientos y frecuencia de respaldo de información o aplicaciones deberán considerar la calidad de la información a respaldar. La información se respalda cada semestre.

Para el registro y control de respaldo es necesario contar con una bitácora. Como la sugerida en la figura 4.4.

Universidad Autónoma del Estado de Hidalgo
Centro de Cómputo Académico
Registro y Control de Respaldos

Hora de inicio	Hora de conclusión	Fecha del respaldo	Contenido del respaldo	Número de equipo	Aulas		Laboratorio	Nombre y firma de la persona que lo realizo
					1	2		
				20	X			

Figura 4.4 Registro y Control de Respaldos.

4.11.6.4 Políticas de Lista de Acceso.

Cada profesor que ingrese a las aulas registra su entrada y salida.

Cada alumno al inicio de semestre registra su posición, por el día y la hora en que lo van a ocupar, haciéndose responsable del equipo en el momento en que lo utilizan y se utiliza el siguiente formato de lista de control de posiciones. Ver anexo No.3.

4.12 Configuración de la Red utilizando Windows XP Profesional.

El Centro de Computo Académico del Campus Tlahuelilpan cuenta con una Red de Área Local (LAN). Los equipos se conectan a un concentrador y se utiliza cable de red denominado par trenzado Ethernet RJ-45, el concentrador se conecta a un modem. Actualmente se cuenta con un ancho de banda de 512 kbps.

Al crear una red doméstica o de pequeña oficina, los equipos que ejecutan Windows XP Professional (SP2), quedan conectados a una red de área local (LAN). Al instalar Windows XP Profesional (SP2) se detecta el adaptador de red y se crea una conexión de área local. La conexión de área local es el único tipo de conexión que se crea y se activa de forma automática.

En el Centro de Computo Académico del Campus Tlahuelilpan, para la configuración de una red se siguen los siguientes pasos:

1. En la barra de tareas, hacer clic en el botón de inicio y, a continuación seleccionar todos los programas, accesorios, comunicaciones y dar un clic en Asistente para configuración de red.
2. Aparece la pantalla de asistente para configuración de red. Como se muestra en la figura 4.5.
3. Hacer clic en el botón siguiente.

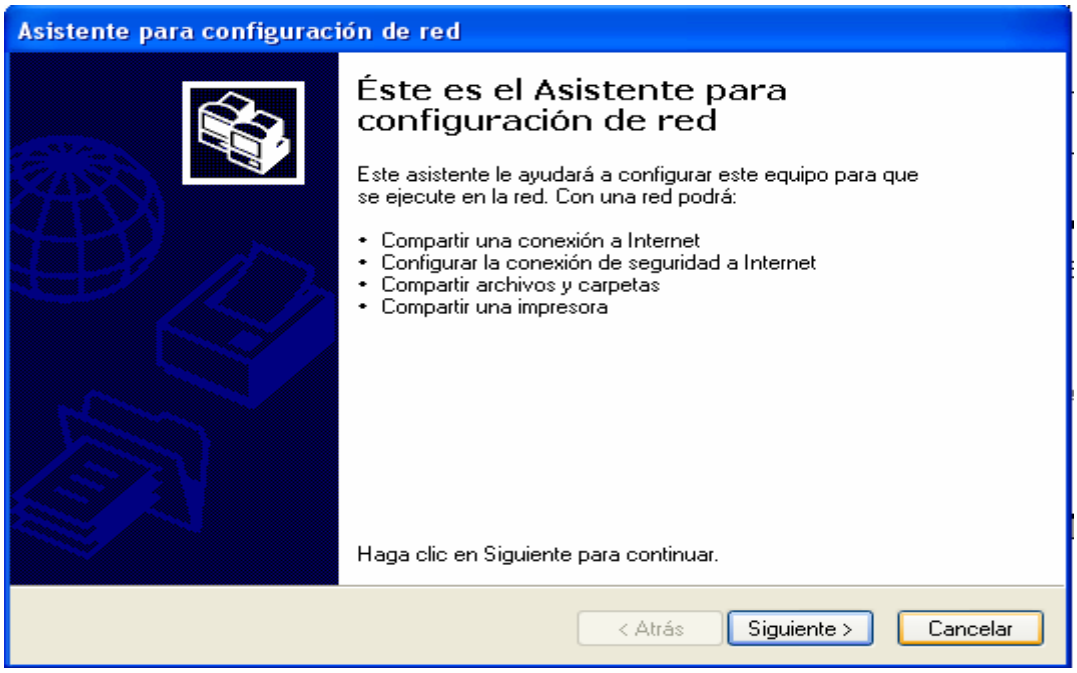


Figura 4.5 Asistente para configuración de red.

4. Aparece la ventana de lista de comprobación para crear una red. Clic en el botón siguiente. Como en la figura 4.6.

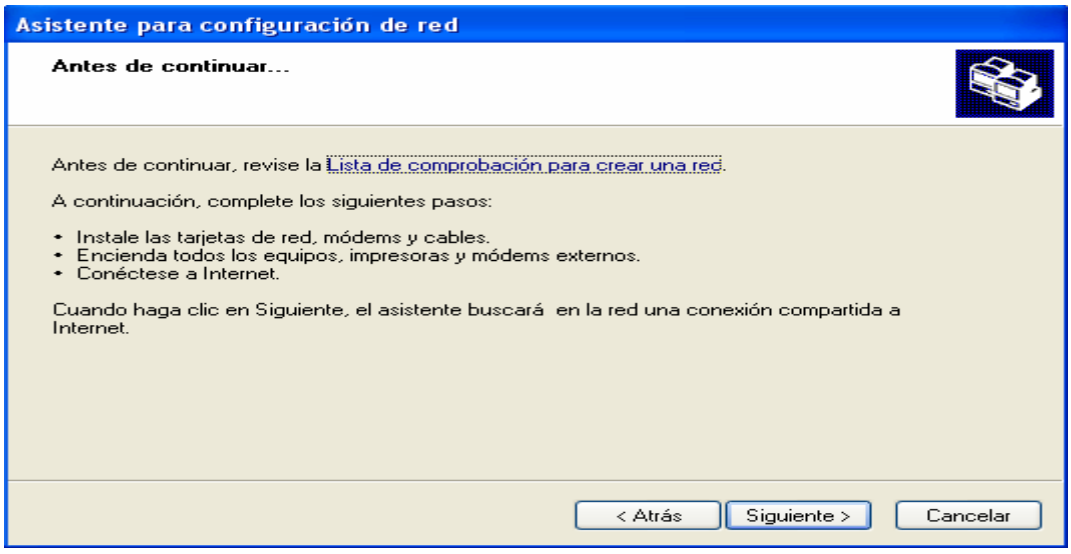


Figura 4.6 Lista de comprobación para crear una red.

5. Seleccionar un método de conexión (activar la opción de otros) y hacer clic en el botón de siguiente. Como se muestra en la figura 4.7.

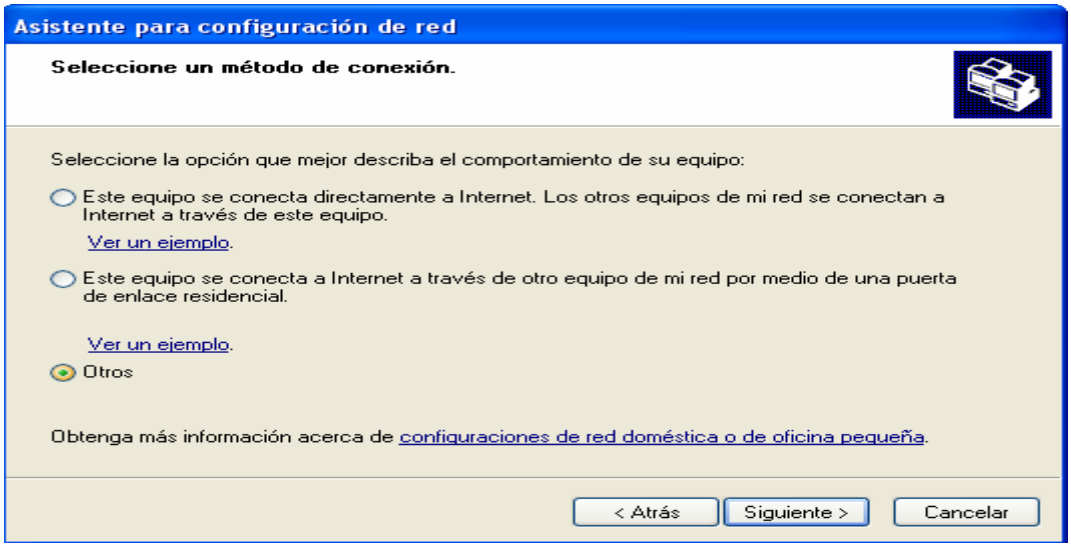


Figura 4.7 Método de conexión.

6. Seleccionar la opción de este equipo se conecta a Internet directamente o a través de un concentrador y a continuación hacer clic en el botón de siguiente. Como en la figura 4.8.

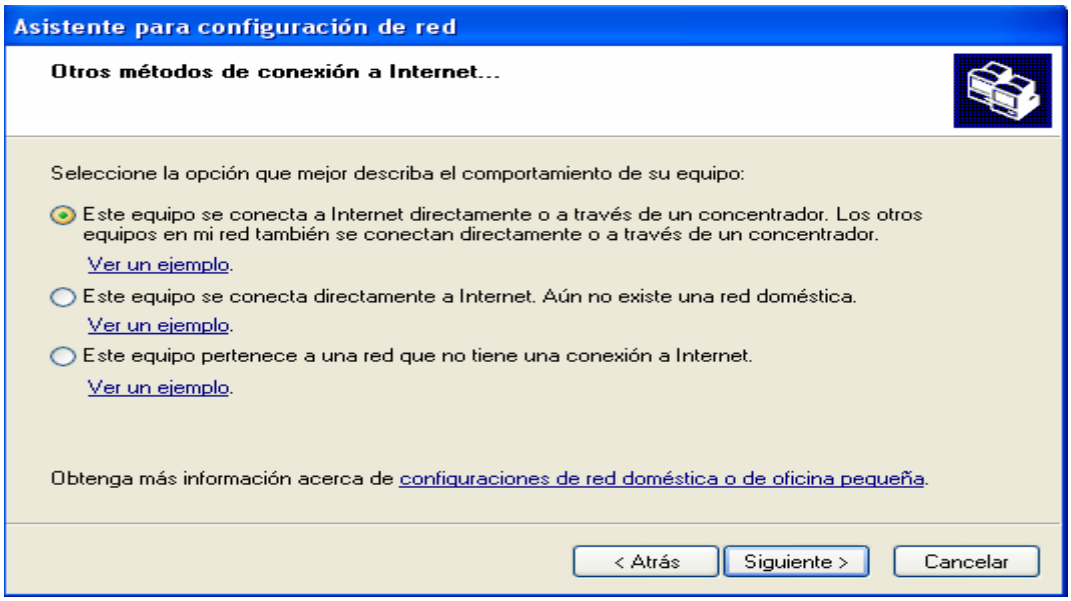


Figura 4.8 Otros métodos de conexión a Internet.

7. Asignar la descripción del equipo y el nombre de equipo y a continuación hacer clic en el botón de siguiente. Como se muestra en la figura 4.9.

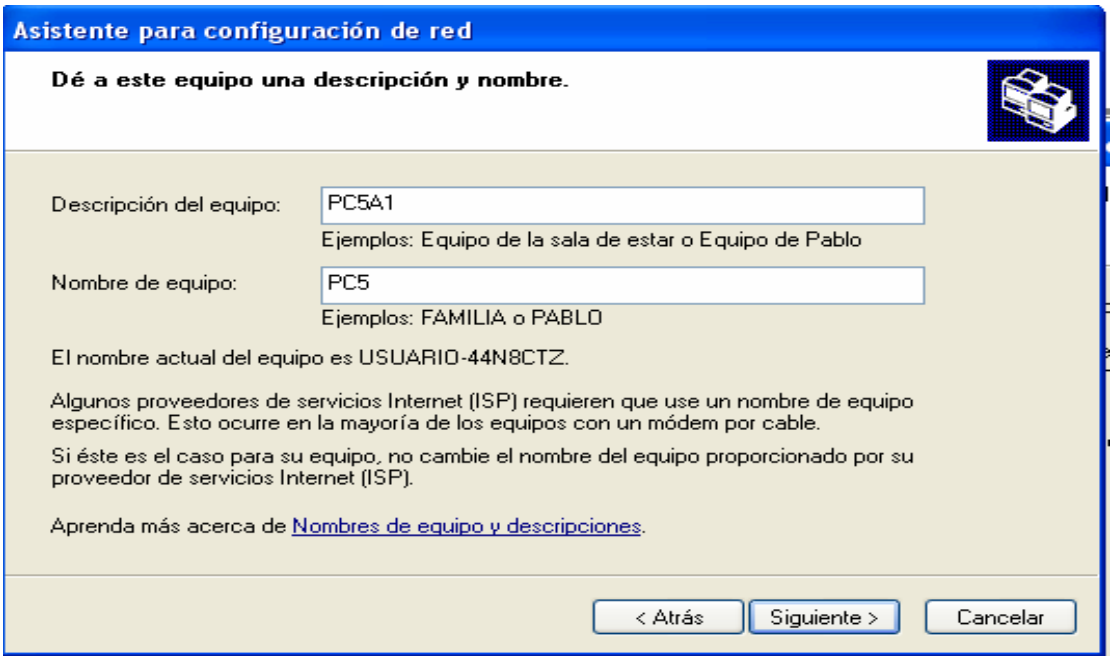


Figura 4.9 Descripción y nombre del equipo.

8. Asignar el nombre del grupo de trabajo (en este caso CECA) y hacer clic en botón siguiente. Como se muestra en la figura 4.10.

Figura 5.10 Nombre a la red (nombre del grupo de trabajo).

9. Revisar si los datos para la configuración de la red son correctos, y a continuación hacer clic en el botón siguiente. Como se muestra en la figura 4.11.

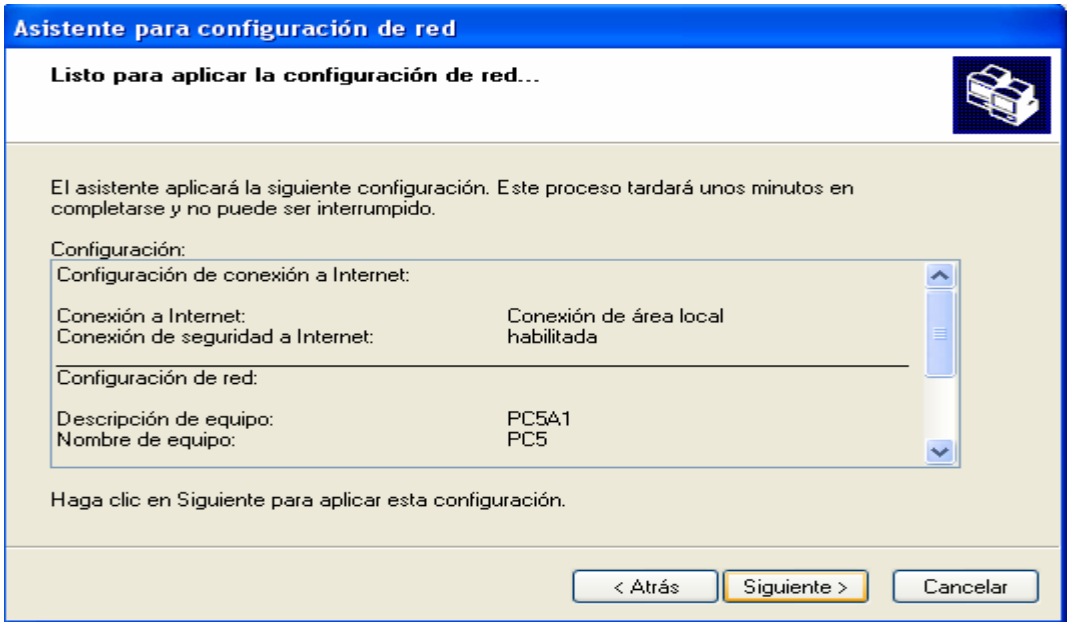
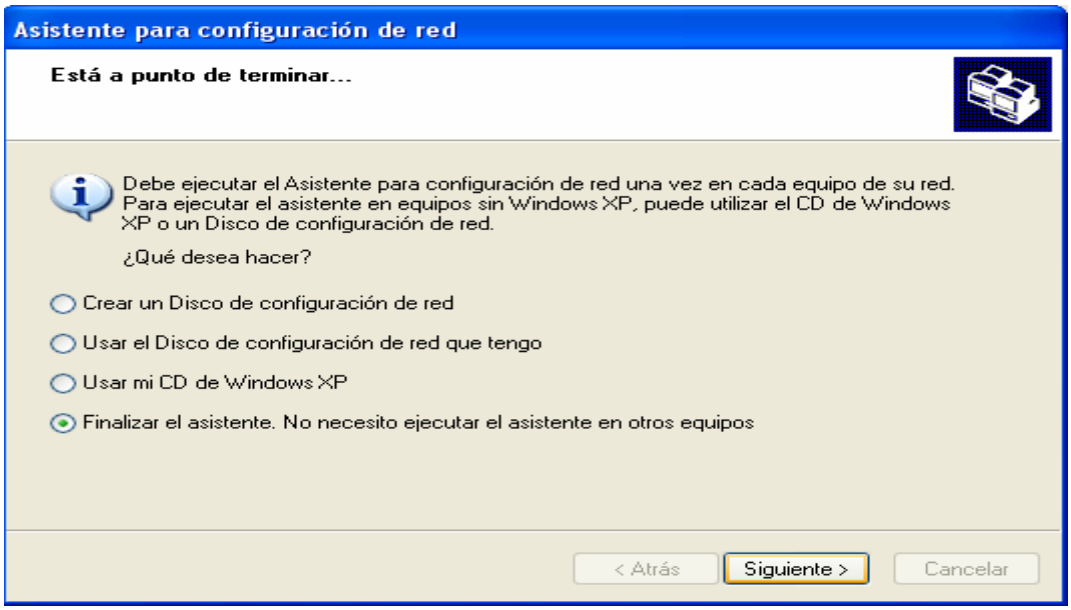


Figura 4.11 Aplicación de la configuración de la red.

10. Configuración de la red. Figura 4.12.

Figura 4.12 Configuración de la red.

11. Ya que se termino de configurar, activar la opción de finalizar y hacer clic en el botón de siguiente. Como se muestra en la figura 4.13.



4.13 Activación de la opción de finalizar el asistente.

12. Finalización del Asistente para configuración de la red. Hacer clic en el botón de finalizar. Como se muestra en la figura 4.14.

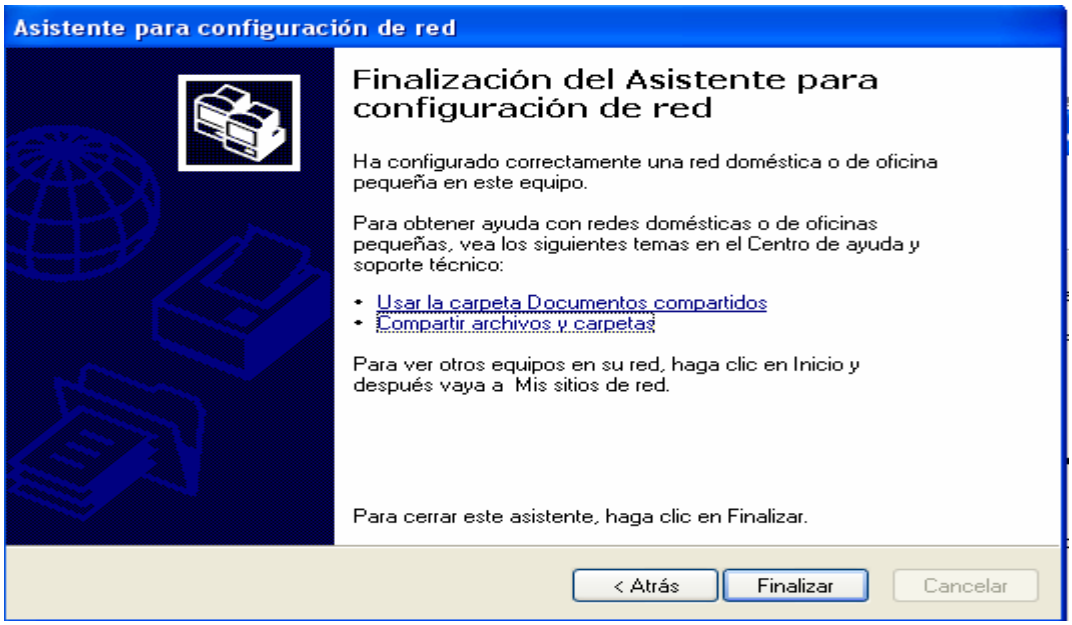


Figura 4.14 Finalización del asistente para configuración de la red.

4.12.1 Configuración de un equipo cliente para que se conecte a Internet, utilizando Windows XP Profesional (SP2).

En el Centro de Cómputo se utiliza el tipo de conexión compartida

1. Iniciar sesión en el equipo.
2. En la barra de tareas, hacer clic en inicio y a continuación, en panel de control. Como se muestra en la figura 4.15.

Figura 4.15 Botón de inicio.

3. Dentro del selector de categorías, hacer clic en el icono de conexiones de Red e Internet. Como se muestra en la figura 4.16.

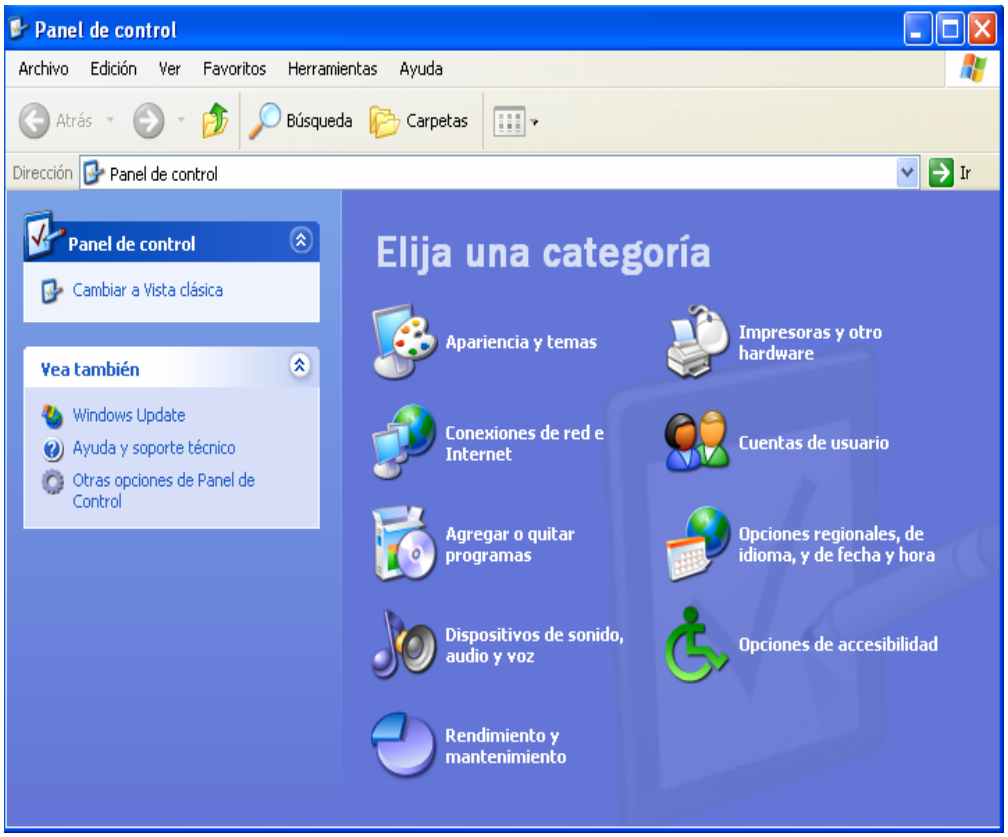
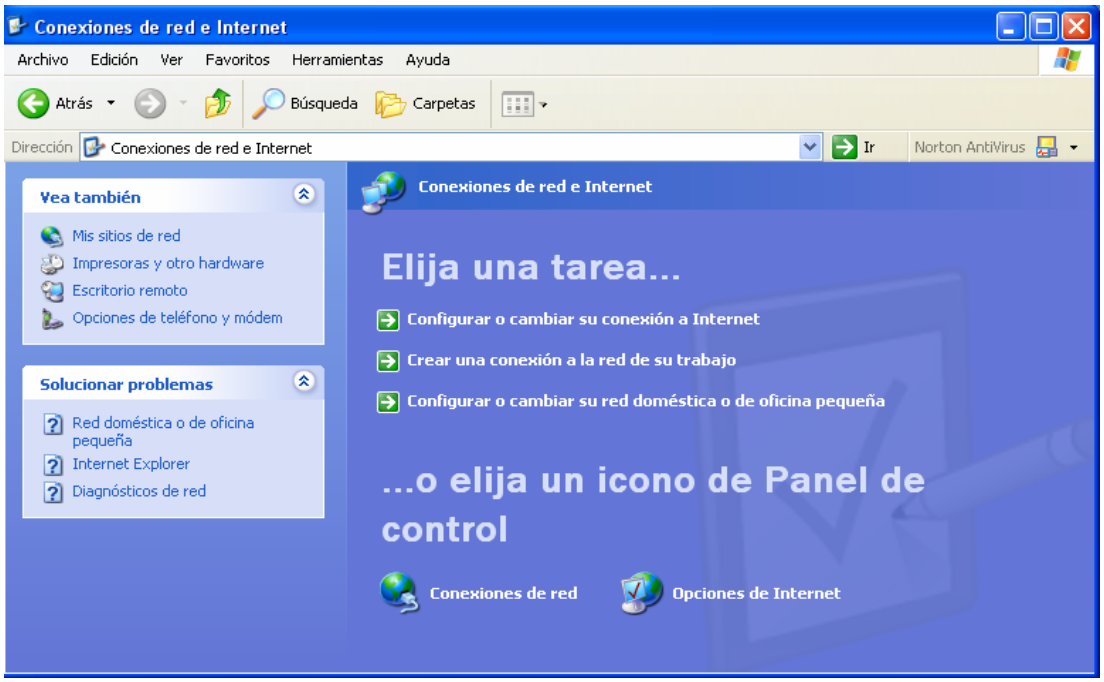


Figura 4.16 Panel de control.

4. En el selector de tareas, hacer clic en Conexiones de Red (En elija un icono del panel de control). Como se muestra en la figura 4.17.



4.17 Conexiones de red e Internet.

5. Hacer clic con el botón secundario del mouse (ratón) en conexiones de área local y después en el menú contextual que aparece, hacer clic en Propiedades. Como se muestra en la figura 4.18.

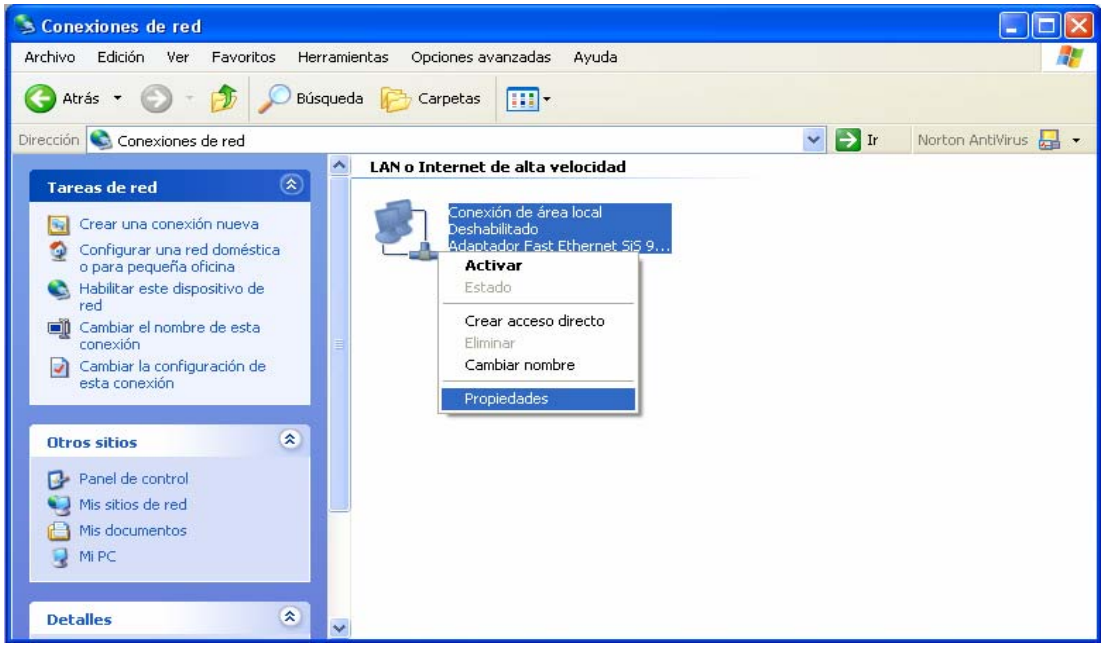


Figura 4.18 Conexiones de Red.

En la ficha General, en al lista. Esta conexión utiliza los siguientes elementos, hacer clic en Protocolo Internet (TCP/IP) y, a continuación en Propiedades. Como se muestra en la figura 4.19.

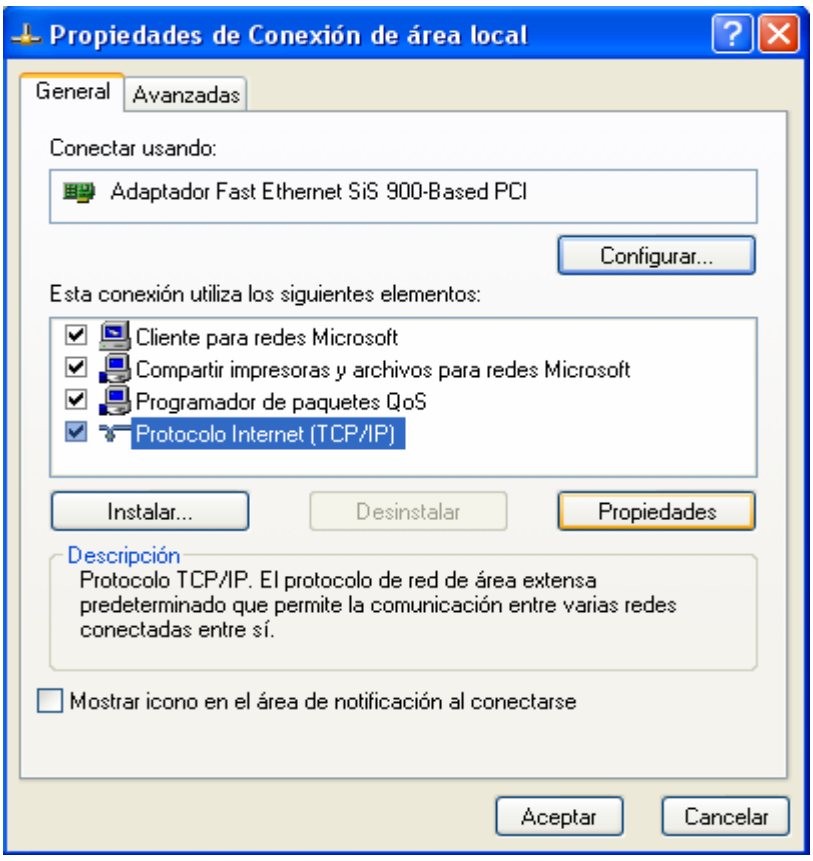


Figura 4.19 Propiedades de conexión de área local.

6. En el cuadro de dialogo Propiedades de Protocolo Internet (TCP/IP), hacer clic en usar la siguiente dirección IP, y se asigna la dirección IP, mascara de subred, puerta de enlace. Después se activa la opción de usar las siguientes direcciones de servidor DNS, y se asigna el servidor DNS preferido. Como se muestra en la figura 4.20.

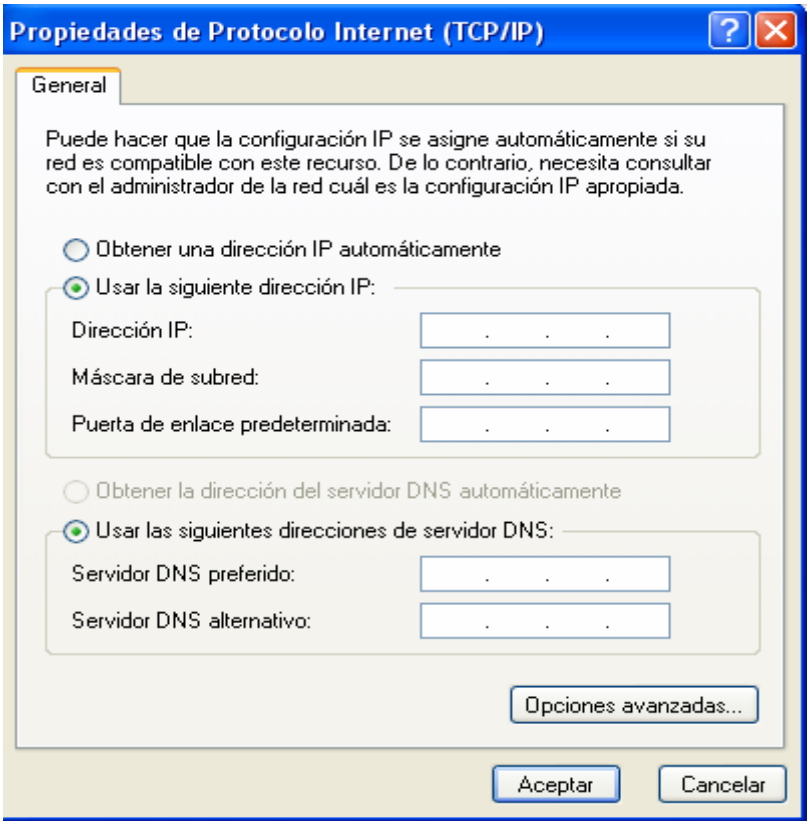


Figura 4.20 Propiedades de Protocolo de Internet (TCP/IP).

7. Hacer clic en el botón de aceptar.
8. En el cuadro de dialogo Propiedades de conexión de área local, hacer clic en aceptar.
9. Salir del panel de control.

4.13 Servicios de seguridad.

Esto servicios definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad.

Las medidas de seguridad que se llevan dentro del centro de cómputo son:

- ✓ En cuanto a software.
- ✓ En cuanto a hardware.

4.13.1 En cuanto a software:

- ✓ Antivirus HAURI.
- ✓ AntiSpayware Windows Defender.
- ✓ Firewall.
- ✓ Actualizaciones Automáticas.

4.13.1.1 Antivirus ViRobot Expert Ver 4.0 (HAURI).

HAURI es un programa antivirus poco conocido; pero que ha superado satisfactoriamente las pruebas que le han hecho. Es fácil de utilizar, y posee todas las opciones avanzadas que se podría esperar de un antivirus moderno, por ejemplo, una vacuna residente que revisa todos los archivos antes de abrirlos, un buen mecanismo erradicador de infecciones, la posibilidad de generar disquetes de rescate y de actualizaciones vía Internet.

El modo de operación de los antivirus tradicionales normalmente realizan sus funciones directamente en el disco duro y en algunas aplicaciones como el correo electrónico.

HAURI accede directamente a las carpetas compartidas: "Actúa desde la capa de comunicaciones para limpiar desde ahí la información y pasarla directamente a la vista del usuario". Como parte de las características de los productos de Hauri, el usuario dispone de herramientas gratuitas para matar, parchar y limpiar el virus y

la posibilidad de identificar de dónde proviene. Razones por la cual en el centro de cómputo académico del Campus Tlahuelilpan utiliza este antivirus.

En la figura 4.21 se muestra el antivirus utilizado en centro de cómputo como medida de seguridad.

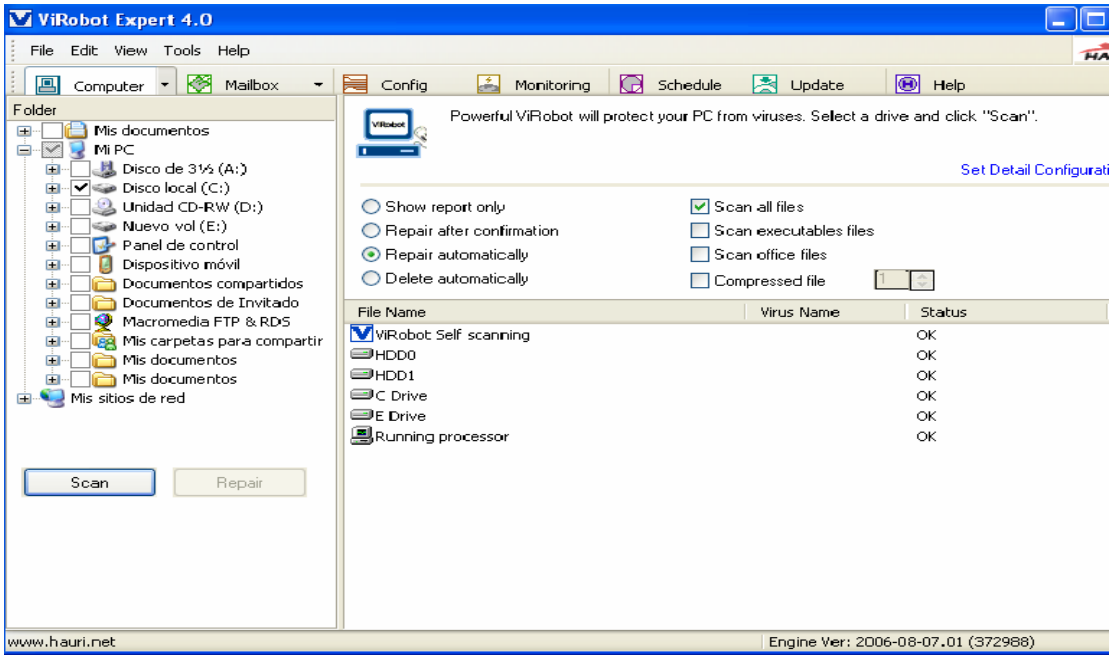


Figura 4.21 Antivirus Hauri.

4.13.1.2 Windows Defender (Beta 2).

Windows Defender (Beta 2) es el nuevo nombre para la tecnología de seguridad de Microsoft Windows AntiSpyware (Beta) que ayuda a proteger del software espía y otros programas no deseables.

Pasos para comprobar si esta actualizado Windows Defender (Beta 2)

1. Dar un clic en el botón de inicio
2. Seleccionar Todos los programas

3. Dar un clic en Windows Defender (mostrara entonces el cuadro de dialogo Estado).

En la figura 4.22 muestra la versión de Windows Defender (Beta 2) que ejecuta en los equipos del CECA.

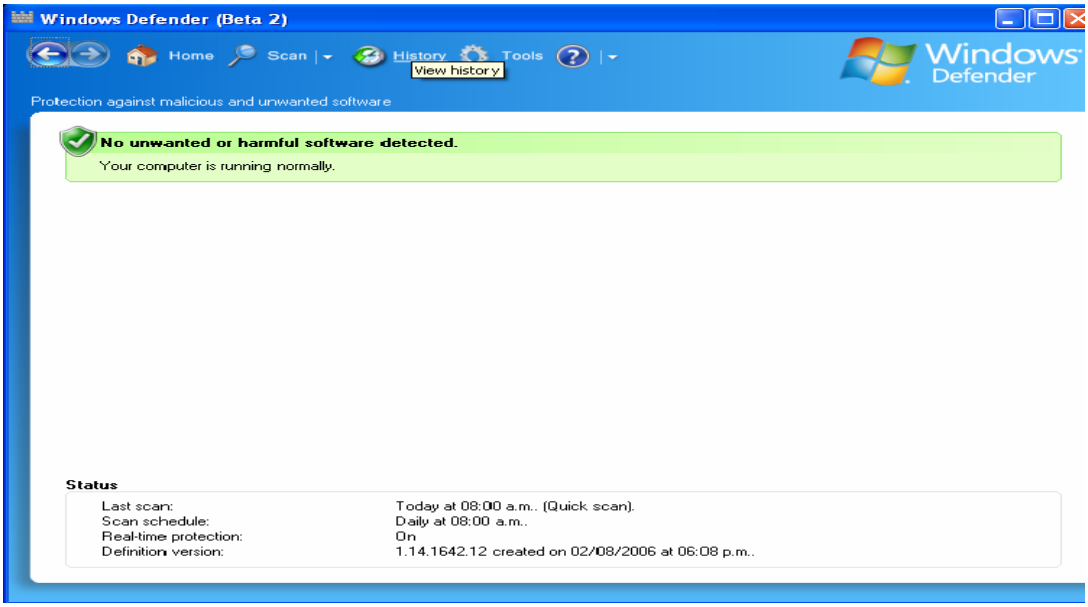


Figura 4.22 Cuadro de Dialogo de Estado de Windows Defender.

4.13.1.3 Firewall de Windows.

El objetivo principal de un Firewall es proteger a una red de otra El Firewall actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación.

Una forma para proteger a los equipos del centro de cómputo contra los ataques procedentes de Internet o de una red es a través de Firewall de Windows y esta activado de forma predeterminada. En Firewall se encuentra en el centro de seguridad. Como se muestra en las figuras 4.23 y 4.24.

Figura 4.23 Centro de Seguridad de Windows.

El cuadro de dialogo de Firewall de Windows en la pestaña **General** se activa la opción (Activado recomendado). Permite la activación del Firewall de Windows. Es la opción recomendada para proteger el equipo. Es importante hacer notar que la opción predeterminada para el Firewall de Windows *es* Activado (recomendado) para todas las conexiones de un equipo ejecutando Windows XP Profesional SP2. Como se muestra en la figura 4.24.

Figura 4.24 Firewall de Windows.

4.13.1.4 Actualizaciones Automáticas.

En el centro de cómputo académico utilizan las actualizaciones como una medida de seguridad. Estas actualizaciones ayudan a protegerse de amenazas contra la seguridad de los equipos.

4.13.1.4.1 Para instalar las últimas actualizaciones de Windows del sitio Web Windows Update (Actualizaciones Automáticas):

1 Iniciar sesión con derechos de administrador.

2 Conectarse a Internet y entrar en el sitio Web Windows Update.

3 Hacer clic en el botón de inicio.

4 Seleccionar la opción de todos los programas.

5 Hacer clic en la opción de Windows Update (situado en la parte superior del menú de inicio). También se puede actualizar desde:

- ✓ Hacer clic en el botón de Inicio.
- ✓ Seleccionar la opción de ayuda y soporte técnico.
- ✓ Dar un clic en la opción de mantener actualizado su equipo con Windows Update (en elegir una tarea).

6 Aparecerá la siguiente pantalla. Como se muestra en la figura 4.25

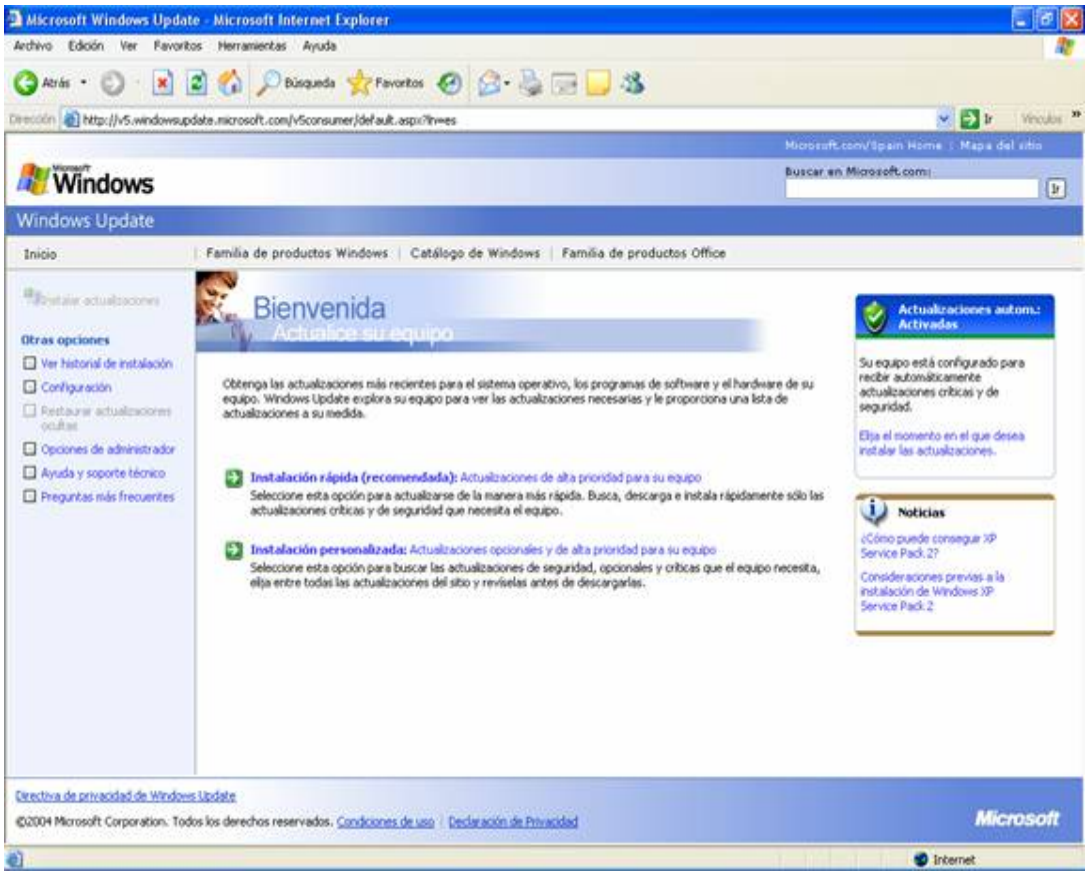


Figura 4.25 Bienvenida de Windows Update.

7.- Seleccionar **Instalación rápida (recomendada)** para instalar sólo actualizaciones críticas y de seguridad. Seleccionar **Instalación personalizada** si se desea instalar otras actualizaciones opcionales además de las actualizaciones críticas y de seguridad.

Windows Update buscará las actualizaciones disponibles.

Si se ha elegido la **Instalación rápida**, hacer clic en **Instalar** para instalarlo todo de una vez.

Si se ha elegido **Instalación personalizada**, se podrá ver y seleccionar cada actualización antes de instalarla. Utilizar el panel de navegación situado a la izquierda para cambiar entre las distintas categorías. Cuando se esté de acuerdo, hacer clic en el botón para **descargar e instalar ahora.**

8.- Seguir las instrucciones de la pantalla y reiniciar el equipo cuando se solicite. (Se recomienda que se reinicie siempre el equipo inmediatamente después de instalar programas nuevos. De lo contrario el equipo podría comportarse de forma impredecible).

4.13.2 En cuanto a Hardware:

Las responsables toman las medidas necesarias para entender sus roles y responsabilidades para administrar y proteger el hardware del centro de cómputo y de esta forma aplicar las medidas necesarias para la protección del hardware.

Las medidas de seguridad que se aplican para el hardware son:

- ✓ Los alumnos no entran con cosas, ni alimentos, ni bebidas.
- ✓ Al inicio y término de cada clase se revisan los laboratorios.
- ✓ Se lleva un control de inventario de hardware (control de altas y bajas de equipos). Como se muestra en los formatos de control de inventarios (Aviso de alta, ver anexo No. 4) y (Aviso de baja, ver anexo No.5).

CONCLUSIONES

- La administración de redes consiste en la planeación, organización y control de todas las actividades que envuelven el funcionamiento de los datos, enfocadas a mantener una red eficiente. Para que esto se lleve acabo es necesario realizar actividades fundamentales como el monitoreo, la atención a fallas, configuración y seguridad en la red.

- Es muy importante que en una red de computadoras se lleve una administración adecuada, aun cuando se considere que es pequeña o que no es necesario, cabe mencionar que entre más grande sea la red mas énfasis se debe de poner en esta tarea.

- Los resultados obtenidos después de aplicar el caso de estudio en el centro de cómputo académico del campus Tlahuelilpan de la UAEH ofrecen una visión global de los indicadores de equilibrio dentro de la administración de la red, basados en la utilización de funciones como el monitoreo, el control y la seguridad.

- Mediante la utilización del centro de seguridad que Windows XP Profesional SP2 se puede llevar un mejor control de la red de computadoras, haciendo uso del firewall, así como también de las actualizaciones automáticas que nos ofrece este sistema operativo.

- Una mala administración de la red trae como consecuencia desorganización general en la misma, es por ello que la persona encargada de revisarla, debe realizarlo constantemente para evitar daños en la red.

- A través del desarrollo del presente trabajo profesional, se aplicaron los conocimientos teóricos aprendidos en el aula, en el desarrollo de un caso de estudio, con la finalidad de vincular la teoría con la práctica.

G LO S A R I O

A

Acceso Remoto. Es la utilidad para que un usuario accese desde su propia PC a otro que esté ubicado remotamente y pueda operar sobre él.

Administrador. Es una persona responsable de la configuración y administración de la red. El administrador generalmente configura la red, asigna contraseñas y permisos y ayuda a los usuarios. Para usar las herramientas administrativas.

Agente. Software de ruteo en un dispositivo controlado por SNMP que responde para recibir y formular pedidos y envía mensajes de advertencia.

Ancho de Banda (BW). Cantidad de datos que puede ser enviada en un periodo de tiempo. Rango de frecuencias, definido por una frecuencia máxima y una mínima, que ocupa una determinada señal electrónica sin sobrepasar los dos limites definidos. El BW esta ligado a la capacidad del canal o medio de transmisión ya que a mayor ancho de banda, mayor capacidad. Se expresa en KB/s (Kilobytes por segundo), bps (bits por segundo) o baudios.

AntiSpyware. Es una tecnología de seguridad que ayuda a proteger a los usuarios de Windows del spyware y otro software no deseado. El spyware ya conocido puede ser detectado y removido del equipo

Ataque. Es un intento deliberado de omitir la seguridad del equipo o privarlo de su uso.

C

Cable RJ-45. Cable de teléfono de ocho hilos que se utiliza para enlazar equipos a una red de área local (LAN).

Concentrador. Dispositivo de hardware que conecta los componentes de la red en una ubicación central y transfiere los datos entre todos ellos.

Clave privada. Es la clave que tan sólo nosotros conocemos y que utilizamos para desencriptar el mensaje que nos envía encriptado con nuestra clave pública. Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

Clave pública. Es la clave que hacemos que esté al alcance de todo el mundo para que nos puedan enviar un mensaje encriptado. También con ella puede desencriptar lo que les enviemos encriptado con nuestra clave privada.

Clave secreta. Es el código básico utilizado para encriptar y desencriptar un mensaje. Cuando se utiliza la misma para las dos funciones, estamos ante un sistema simétrico.

Conexión de banda ancha. Conexión de alta velocidad. Las conexiones de banda ancha suelen alcanzar velocidades de 256 kilobytes por segundo o superiores. En la banda ancha se incluye DSL y el servicio de módem por cable.

Configurar. Adaptar una aplicación software o un elemento hardware al resto de los elementos del entorno y a las necesidades específicas del usuario. Es una tarea esencial antes de trabajar con cualquier nuevo elemento.

D

Dirección IP. Es un número binario de 32 bits que identifica de manera única y precisa la posición de una computadora particular en Internet. Las direcciones IP están formadas por cuatro enteros decimales separados por puntos, en donde cada entero proporciona el valor de un octeto de la dirección IP.

Dominio. Grupo de equipos y dispositivos de una red que se agrupan con reglas y procedimientos comunes.

DSL. Línea de subscriptor digital, una tecnología que aumenta enormemente la capacidad de los cables de teléfono normales para transportar información digital.

E

Encriptación. Es un proceso que codifica los archivos de manera que sean ilegibles para las personas que no poseen la contraseña.

Estación de Trabajo (workstation). Es una PC que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. En la mayor parte de los casos esta computadora ejecuta su propio sistema operativo y posteriormente se añade al ambiente dela red.

F

Firewall. Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de la red privada e Internet.

H

Hardware de Red. Dispositivos que se utilizan para interconectar a los componentes de la red. Encontramos a las tarjetas de red*; e*l cableado entre servidores y estaciones de trabajo, así como a los diferentes cables para conectar a los periféricos

I

IEEE Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicación y redes.

Impresora de red. Impresora conectada a la red de tal forma que más de un usuario pueda imprimir en ella.

K

Kbps (kilo bits por segundo). Es la unidad de velocidad de transmisión de datos.

M

Mascara de Subred. Indica cuantos bits de una dirección IP son utilizados para el direccionamiento de la subred.

Modem. Es un dispositivo que convierte la señal digital en señal analógica y viceversa para posibilitar que el mensaje enviado por un DTE (Date Terminal Equiment) puede llegar a otros DTE´s a través de líneas análogas

N

Nodo. Punto final de conexión de red o unión común para varias líneas de red. Los nodos pueden ser: procesadores, controladoras o estaciones de trabajo

P

Paquetes. Bloques de información para la transmisión en sistemas de conmutación de paquetes.

Ping. Sonda de paquetes Internet. Verifica si una dirección IP especifica esta disponible. Un paquete se envía a otra dirección IP y espera una respuesta.

Protocolo. Es como un lenguaje para la comunicación de información. Son las reglas y procedimientos que se utilizan en una red para comunicarse entre los nodos que tienen acceso al sistema de cable.

R

Recursos a compartir. Son aquellos dispositivos de hardware que tienen un alto costo y que son de alta tecnología, los más comunes son las impresoras.

Red. Es un conjunto de dispositivos físicos "hardware" y de programas "software", mediante el cual podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.).

S

Seguridad del protocolo Internet (IPSec). Es un conjunto de servicios y protocolos de seguridad basado en criptografía.

Servicio. Son programas o aplicaciones cargadas por le propio sistema operativo.

Sistema de nombres de dominio (DNS). Base de datos jerárquica y distribuida que contiene asignaciones de nombres de dominio DNS para varios tipos de datos, como direcciones IP. DNS permite la búsqueda de equipos y servicios mediante nombres descriptivos y el descubrimiento de otra información almacenada en la base de datos.

Sistema operativo de red. Conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados

SNMP Simple Network Management Protocol (Protocolo simple de administración de redes). Gestiona las LAN. El software basado en SNMP se comunica con los

dispositivos que disponen de agentes SNMP incorporados. Los agentes SNMP recopilan información de la actividad de la red y del estado del dispositivo y la envían de vuelta a una estación de trabajo.

Subred. Es un segmento de una red y es establecida por el administrador de la misma.

T

TCP/IP (Transmission Control Protocol/Internet Protocol). Protocolo que utiliza Internet para enviar y recibir la información en forma de paquetes

V

Virus. Es un fragmento de programa que se anexa a un programa legítimo con la intención de infectar otros programas.

SIGLARIO

CPU. Unidad central de procesamiento. La parte de un equipo que procesa la información.

DHCP.(Dynamic Host Configuration Protocol). Protocolo de Configuración Dinámica de Servidor.

ICF: Conexión de Seguridad a Internet.

ICS: Conexión compartida a Internet.

IEEE. (Intitute of Electrical and Electronics Engineers). Instituto de Ingenieros Eléctricos y Electrónicos.

IP.(Internet Protocol). Protocolo de Internet.

IPSec.- Seguridad del protocolo Internet.

ISO: Organización de Estándares Internacionales.

ISP: Proveedor de Servicio de Internet.

Kbps Kilo bits por segundo.

LAN. Red de are local.

MAC Control de acceso a medios.

MRN.- Monitoreo remoto.

NDS. (Novell Directory Services). Servicio de Directorios de Novell.

NetBEUI. (NetBIOS Extended User Interface). Interfaz Extendida de Usuario NetBIOS.

NetBIOS. (Network Basic Input/Output System). Sistema de Red Básico de Entrada / salida.

NFS. (Network File System). Sistema de Archivos de Red.

NIC. (Network Interface Card). Tarjeta de Interfaz de Red.

NOS. (Network Operating System). Sistema Operativo de Red.

NTFS. (NT File System). Sistema de Archivos de NT.

NT.- Nueva tecnología.

PC. (Personal Computer). Computadora Personal.

RDP.- Protocolo de escritorio remoto.

RPC.- Llamada a procedimientos remoto.

SHCP. Protocolo sencillo de administración.

SNMP.- Protocolo sencillo de administración de red

SMTP. (Simple Mail Transfer Protocol). Protocolo de Transferencia de Correo Simple.

S.O. Sistema Operativo.

TCP/IP. (Transmission Control Protocol/Internet Protocol). Protocolo de Control de Transmisión /protocolo de Internet.

TCP/IP. Protocolo de control de transmisión / protocolo de Internet

WAN. (Wide Area Network). Red de Área Amplia.

WMI: Instrumental de Administración de Windows.

VoIP.- Voz sobre IP.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
CAMPUS TLAHUELILPAN
CENTRO DE CÓMPUTO ACADÉMICO

PRIMERA REUNIÓN

- ✓ **Orden del día.**
- ✓ **Análisis de requerimientos.**
- ✓ **Entrevista.**
- ✓ **Comentarios generales.**

ENTREVISTA

1. ¿Qué funciones desempeña el CECA?.
2. En forma general que tipos de información procesa el CECA.
3. Existe relación entra las diversas áreas o cada una es independiente de las otras.
4. ¿Cómo se distribuyen las tareas dentro del CECA?
5. ¿Cuáles son los principales servicios informáticos que ofrece el CECA?

SEGUNDA REUNIÓN.

- ✓ **Orden del día.**
- ✓ **Análisis de requerimientos.**
- ✓ **Entrevista.**
- ✓ **Comentarios generales.**

ENTREVISTA

1. ¿Qué tipo de red se tiene en el CECA?.
2. ¿Con qué acho de banda se cuenta actualmente?.
3. ¿Por qué se utiliza el sistema operativo Windows XP (SP2) y no otro sistema operativo?.
4. ¿Cuáles son los procedimientos que se siguen para la administración de la red dentro del Centro de Cómputo Académico del Campus?.

TERCERA REUNIÓN.

- ✓ **Orden del día.**
- ✓ **Análisis de requerimientos.**
- ✓ **Entrevista.**
- ✓ **Cometarios generales.**

ENTREVISTA

1. ¿Quién esta autorizado para usar los recursos de la red?
2. ¿Quién esta autorizado para conceder acceso y aprobar el uso?
3. ¿Quién puede tener privilegios de administración del sistema?
4. ¿Cuáles son los derechos y responsabilidades del usuario?
5. ¿Qué hace con la información delicada?

CUARTA REUNIÓN.

- ✓ **Orden del día.**
- ✓ **Análisis de requerimientos.**
- ✓ **Entrevista.**
- ✓ **Cometarios generales.**

ENTREVISTA

1. ¿Cuál es el procedimiento a seguir cuando se presentan fallas en algún equipo?.
2. ¿Qué procedimientos siguen para la configuración de la red?
3. ¿Qué procedimientos utilizan para la configuración de un equipo (para que dicho equipo sea conectado a Internet?.
4. ¿Cuáles son las medidas de seguridad que se aplican para la red?

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

CAMPUS TLAHUELILPAN

CENTRO DE CÓMPUTO ACADÉMICO

ADMINISTRACION DE HARDWARE Y SOFTWARE

AULA _____ **FECHA**_____

	MONITOR	CPU	MOUSE	CD	3½1/2	INTERNET	Sistema Operativo	ASPEL	Adobe Acrobat 5.0	Cosmo Player 2.1.1(41451)	DesktopX	EasyClear	Forder Access 2.0.0 Free version	ForSer 3.1 Beta 1	J2SE Development Kit 5.0 Update 1	OBSERVACIONES
1AC							Windows XP Profesional (SP2)									
2AC																
3AC																
4AC																
5AC																
6AC																
7AC																
8AC																
9AC																
10AC																
11AC																
12AC																
13AC																
14AC																
15AC																
16AC																
17AC																
18AC																
19AC																
20AC																
21AC																
22AC																
23AC																
24AC																

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
CAMPUS TLAHUELILPAN
CENTRO DE CÓMPUTO ACADÉMICO

Centro de Cómputo Académico

	Java 2 SDK Standard Edition v1.3.1_06 jGRASP	LiveUpdate 2.6 (Symantec Corporation)	Logic	Macromedia	Microsoft AntiSpyware VRobot	Microsoft Office Profesional; FromtPage	Microsoft Visual Studio 6.0 Edition empresarial (Español)	MySQL Server 5.0	PHP 3.3.3	VMS SiteClient 2.0	WinZip		
1AC													
2AC													
3AC													
4AC													
5AC													
6AC													
7AC													
8AC													
9AC													
10AC													
11AC													
12AC													
13AC													
14AC													
15AC													
16AC													
17AC													
18AC													
19AC													
20AC													
21AC													
22AC													
23AC													
24AC													

Universidad Autónoma del Estado de Hidalgo
Centro de Cómputo Académico
Área de Control

Lista de Control de Posiciones

Centro de Cómputo Académico

Nombre del Catedrático:_____ Firma:_____
Escuela:_____ Materia:_____
Software que utilizará durante el semestre: _____
Semestre:_____ Grupo:_____ Fecha:_____
Horario 1:_____ Aula:_____ Horario 2:_____ Aula:_____

	No. Cta.	Nombre del alumno	Pos.1	Pos.2	Firma de Conformidad
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					

NOTA:
Con esta fecha los que suscriben Catedrático y Alumnos de la UAEH. Cuyos datos aparecen en la presente, recibimos de conformidad el aula, así como el equipo que la integra funcionando en su totalidad y quedando como responsables durante el día y hora de clases del mismo. En el semestre _____ de _____; detallando de la manera individual posición que ocupa en el equipo correspondiente.

FDCO8.4-009-01

UNIVERSIDAD AUTONOMA DEL ESTADO DE HIDALGO
Coordinación de administración y finanzas
Departamento de control de inventarios
AVISO DE ALTA

FOLIO

FECHA

DEPENDENCIA _____ CLAVE

CENTRO DE TRABAJO: _____ CLAVE

CLAVE				
A.- COMPRA DIRECTA	B.- DONATIVO	C.- TRANSFERENCIA	D.- REPOSICIÓN	E.- OTROS

No. DE INVENTARIO DEL BIEN	CAN TIDAD	DESCRIPCIÓN	CLAVE DEL MOVIMIENTO	GRUPO	SUB-GRUPO

OBSERVACIONES:

VERIFICADO POR		TITULAR O RESPONSABLE DEL INVENTARIO DEL C.C.	
NOMBRE	FIRMA	NOMBRE	FIRMA

NOTA: LA DESCRIPCIÓN DEL BIEN COMPRENDE LO SIGUIENTE: NOMBRE, MATERIAL, DIMENSIONES, SERIE, MODELO, TIPO Y MARCA

DAF-PO74-08 R01

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
Coordinación de Administración y Finanzas
Departamento de Control de Inventarios
AVISO DE BAJA

FOLIO

31/01/2005
FECHA

DEPENDENCIA **Campus Tlahuelilpan**

CLAVE

CENTRO DE TRABAJO **Centro de Cómputo Académico**

CLAVE

CLAVE				
01 DESUSO	02 EXTRAVÍO	03 DESTRUCCIÓN	04 TRANSFERENCIA	05 DONACIÓN

No. DE INVENTARIO DEL BIEN	CANTIDAD	DESCRIPCIÓN	CLAVE DEL MOV. BAJA	GRUPO	SUB-GRUPO	TPO.
S/N	1	Gabinete Pentium III a 500 MhZ **N/S 20000050203906**	2			
83674	1	Monitor SVGA de 15" **N/S DT15HCEN824872B**	4			
83619	1	Teclado en Español PS/2 **N/S 9K05409659B**	4			

OBSERVACIONES:

AUTORIZA LA BAJA TITULAR DEL CENTRO DE COSTOS	ENTREGA LOS BIENES DESCRITOS	RECIBE DE CONFORMIDAD
NOMBRE FIRMA	NOMBRE FIRMA	NOMBRE FIRMA

NOTA: LA DESCRIPCIÓN DEL BIEN COMPRENDE LO SIGUIENTE: NOMBRE, MATERIAL, DIMENSIONES, SERIE, MODELO, TIPO Y MARCA.

DAF-PO74-09 R01

Bibliografía

[B1] Ford, M. y Kim, Lew. (1998). *Tecnologías de Interconectividad de Redes.* México: Prentice Hall.

[B2] A, S. y Schuster, C. (1998). *Firewalls y la Seguridad en Internet*. México: Prentice Hall.

[B3] Rabago, J.F. (2000). *Introducción a las redes locales.* Madrid, España: Anaya.

[B4] Stanek, W. (2002). *Microsoft Windows XP Profesional. Manual del administrador.* España: Mc Graw Hill.

[B5] Goldberger, R. (2002). *Microsoft Windows XP.* México: Prentice-Hall.

[B6] Black, U. (2000). *Redes de Computadoras, Protocolos, normas e interfaces*. México, D.F: Alfaomega ra-ma.

[B7] Tanenbaum, A. y Woodhull, A. (1998). *Sistemas Operativos, Diseño e implementación.* México: Prentice-Hall.

[B8] Paul, M.J. (2004). *Aprendiendo Microsoft Windows XP*. España: Prentice-Hall.

Referencias Electrónicas

[R1] [en línea]. Disponible en: URL
http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php
[2004, 8 de Octubre].

[R2] Microsoft Corporation. [en línea]. Disponible en URL:
http://www.microsoft.com/windowsxp.

[R3] Microsoft Corporation. (2004). Service Pack 2 de Windows XP. [en línea] España. Disponible en URL:
http://www.microsoft.com/windowsxp/sp2/whattoknow/es/sp2_whattoknow.mspx

[R4] Microsoft Corporation. [2001]. Características de Windows XP Profesional. [en línea]. Disponible en: URL:
http://www.microsoft.com/latam/windowsxp/pro/evaluacion/caracteristicas.asp

[R5] Microsoft Corporation. [2001]. Redes domésticas. [en línea]. Disponible en URL:
http://www.microsoft.com/spain/windowsxp/home/using/howto/homenet/protect.asp

[R6] Microsoft Corporation. [en línea]. Disponible en URL:
http://www.microsoft.com/spain/empresas/seguridad/articulos/sec_winxp_pro_p2p.mspx

[R7] Microsoft Corporation. (2002) [en linea]. Disponible en URL:
http://www.microsoft.com/latam/windowsxp/pro/biblioteca/mobile/xpmobilesecurity05.asp

[R8] Universidad de Jaén. (2005). Compartir recursos en red bajo Windows XP [en línea]. Disponible en URL:
http://www.ujaen.es/sci/redes/conex/redmicrosoft/wxp/rmswxp.htm.
[2004, 14 de Mayo].

[R9] Microsoft Corporation. (2004).Administrar la configuración de seguridad del equipo en un solo lugar. [en línea]. Disponible en URL:
http://www.microsoft.com/latam/windowsxp/using/security/internet/sp2_wscintro.mspx

[R10] Jimenez, J.R. (2004). Microsoft Windows XP SP2, [en linea]. México: Departamento de Seguridad en Cómputo DGSCA-UNAM. Disponible en URL: http://www.seguridad.unam.mx/doc/?ap=tutorial&id=125. [2005, 20 de Enero].

[R11] Universidad Autónoma del Estado de Hidalgo. [en línea]. Disponible en http://www.uaeh.edu.mx

Entrevistas

[E1] Ing. Juan Francisco Valerio Islas (Comunicación personal, Mayo, 2005).
Director del Campus Tlahuelilpan.

[E2] Lic. Mónica García Murguía (Comunicación personal, Mayo, 2005).
Responsable del Centro de Cómputo Campus Tlahuelilpan.

[E3] Lic. Norma Lilia Cornejo Reyna (Comunicación personal, Mayo, 2005).
Auxiliar del Centro de Cómputo Campus Tlahuelilpan.

[E4] Lic. Comp. David Rivero Borja (Comunicación personal, Mayo, 2005).
Administrador de Red, Telecomunicaciones UAEH.