UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ACATLÁN

IMPLEMENTACIÓN DE UNA INTRANET BAJO WINDOWS 2000 CON INTERNET MEDIANTE EL SERVICIO DE ENRUTAMIENTO Y ACCESO REMOTO Y EL PROTOCOLO DE TRADUCCIÓN DE DIRECCIÓN DE RED (NAT): CASO PRÁCTICO

T E S I N A

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PRESENTA:

JOSÉ DAMIÁN VÁSQUEZ RAMIRO

ASESOR: OSCAR GABRIEL CABALLERO MARTINEZ

Julio del 2007

AGRADECIMIENTOS

A mis papás por darme su amor, su apoyo y por darme las bases para construir el profesionista y hombre que soy.

A mi hermana por su cariño incondicional, y por ese par de niños hermosos que tiene.

A mis amigos Benito y Juan por los momentos que compartimos juntos pero sobre todo por su amistad.

A la personas que encontré en mi camino por la universidad y que me hicieron mejor persona y mejor profesionista.

A la UNAM por todo lo que me brindo durante mi estancia en ella, como alumno y como trabajador, es para mí un orgullo ser Universitario.

A mi entrenadora de Básquetbol por enseñarme tantas cosas del deporte que amo y por apoyarme a seguir sin él.

Y muy en especial a Mary por todo el amor, cariño y apoyo. Gracias por compartir tu vida al lado mío, te amo.

Gracias

ÍNDICE

INTRODUCCIÓN

La historia de las redes se remonta a muchos años atrás, aquí no se pretende hacer más documentación sobre esa historia simplemente se quiere mostrar que en la actualidad ocupamos aquellos conceptos y que han evolucionado de manera asombrosa para el beneficio de toda la humanidad y no sólo de entidades militares o gubernamentales como originalmente fue pensado. Las redes nos facilitan el día a día ya que hoy no imaginamos la vida sin Internet o sin correo electrónico y mucho menos sin una computadora ya sea portátil o de escritorio.

El presente trabajo se desarrollo como una solución al problema que se presenta cuando no tenemos un área de trabajo con administración centralizada, sin control de los recursos que se tienen, es decir sin estar en un ambiente de red.

Se describirá brevemente el ambiente sobre el cual se implemento este trabajo:

Es un área de trabajo común con aproximadamente 45 equipos y estos dan servicio aproximadamente a 1000 usuarios.

Inicialmente los usuarios eran capaces de modificar a su gusto los programas instalados y la configuración del equipo asignado y no existía registro alguno de quien lo hacia y constantemente había que estar reconfigurando los programas y en el peor de los casos reinstalando completamente el equipo. Al mismo tiempo la calidad del servicio que se ofrecía no era el mejor por la situación antes descrita, además de esto el usuario tenía que transportar su información en discos flexibles 3 ½" lo cual no es práctico ni cuenta con capacidad muy grande, lo que ocasionaba que los discos se dañaran continuamente sufriendo perdidas de información.

El servicio de impresión que se ofrecía era en 4 impresoras de matriz conectadas cada una a una computadora por lo que resultaban insuficientes, debido a que se saturaban y los trabajos no tenían buena calidad.

Durante el proceso de configuración de los equipos los programas se instalaban equipo por equipo llegando a tardarse varias horas en este proceso y si algún archivo o disco estaba dañado se tenía que repetir el proceso, lo cual ocasionaba una pérdida de tiempo considerable y además un equipo menos disponible para su uso.

La actualización del antivirus se realizaba equipo por equipo portando la actualización correspondiente en discos flexibles por lo que a veces no todos los equipos estaban actualizados en las definiciones de antivirus.

Se tenía la necesidad de ofrecer el servicio de acceso a Internet, pero la limitante eran las direcciones IP homologadas, ya que no había disponibilidad de ellas; por lo que se

propone utilizar una solución basada en Windows 2000 Server y el servicio de NAT (Network Adress Translation) para satisfacer esta necesidad.

El objetivo del documento es demostrar que al tener nuestros equipos en red, con Windows 2000 Server y estaciones de trabajo Windows 2000 o Windows XP Profesional se logra tener un mejor control sobre los accesos a ellos y sobre los servicios que ofrecen que al estar de manera independiente aun con Windows 2000 o XP, además que reducimos el tiempo hombre que se dedica a la instalación y configuración de los equipos debido a que ya no requerimos instalar cada uno de manera independiente, ni tenemos que crear usuarios en cada equipo para que puedan usarse.

También gracias a que están en red podremos tener más y mejor control sobre los usuarios que los ocupan, ya que podremos aplicar restricciones mediante políticas por grupo o por usuario según se requiera, teniendo como consecuencia prohibir la modificación e instalación de programas no autorizados por el administrador, lo cual nos beneficiará en que la administración sea centralizada, más eficiente y segura.

Además de todo esto, nos permitirá ofrecer servicios que antes no se ofrecían como por ejemplo: el servicio de impresión vía red, es decir mandar a imprimir desde su equipo de trabajo y no pararse de su lugar con un disco u otro dispositivo de almacenamiento e ir a imprimir al equipo que tiene conectada físicamente la impresora.

Otro servicio que se podrá ofrecer es el de almacenamiento de información en el servidor (File Server), así el usuario contara con un espacio asignado para guardar información con la seguridad de que nadie mas tendrá acceso a ella y por ende no tendrán que estar transportando diariamente su información en discos o cualquier otro medio.

El servicio que resulta más llamativo para el usuario final es el de Internet, ya que actualmente es un medio necesario para consultar información, comunicarnos, tomar cursos, pago de servicios, etc.

El trabajo describe y explica paso a paso como hacer toda la instalación y configuración de nuestro servidor con Windows 2000 Server para que éste, nos brinde el servicio y seguridad que requerimos al momento de ofrecer acceso a Internet, así mismo sugiere el aplicar algunas medidas adicionales que nos ayudarán a que nuestra red sea más segura.

Aunque primordialmente el trabajo está enfocado a los administradores o encargados de una red también puede ayudar a que el usuario final este consciente de las obligaciones y derechos a los cuales esta sujeto al momento de convertirse en usuario de una red de datos corporativa, escolar u otra con o sin servicio de Internet.

El documento está dividido en cuatro capítulos, cada uno aborda un tema en particular que nos ayudarán a lograr el objetivo final que es: instalar, configurar y administrar nuestros equipos en red con Windows 2000 Server, brindando los servicios antes

mencionados, lo que no explica el trabajo es como hacer la conexión física de los equipos en red esa parte se podrá consultar en libros o manuales de redes.

Ojala que este trabajo sirva como referencia para administradores y usuarios que estén interesados en el tema de las redes y la administración de las mismas bajo ambientes Windows. También espero que con trabajos así logremos desmitificar la idea de que una red con Windows es una red insegura y vulnerable por el sólo hecho de ser Microsoft.

Una red con otro sistema operativo como por ejemplo “Unix” puede ser igual o más insegura que una con Windows, la seguridad no radica por si misma en el nombre de la compañía que fabrica el sistema operativo, la seguridad de una red es un trabajo conjunto de los administradores, usuarios, de la configuración correcta del software instalado y la seguridad física que se tenga del servidor y equipos.

Bienvenidos, esperando que sea interesante y de utilidad lo que se expone a continuación.

CAPÍTULO 1. ANTECEDENTES

1.1. Conceptos

Se empezará hablando brevemente de la historia de las redes y como fue su evolución.

1.1.1. Información general de TCP/IP

El Protocolo de Control de Transporte/Protocolo de Internet (TCP/IP, Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos estándar del sector diseñado para conjuntos de redes a gran escala que abarcan entornos de Red de Área Local (LAN, Local Área Network) y Red de Área Amplia (WAN, Wide Área Network)

Los orígenes de TCP/IP se remontan a 1969, cuando el Ministerio de defensa de EE.UU. encargó la creación de la Red de agencias para proyectos de investigación avanzados (ARPANET, Advanced Research Projects Agency Network).

ARPANET fue el resultado de un experimento de uso compartido de recursos. El propósito era proporcionar vínculos de comunicación a través de redes de alta velocidad entre diversos "súper equipos" ubicados en diferentes zonas de Estados Unidos.

Los primeros protocolos, como Telnet (para la emulación de terminales virtuales) y el Protocolo de transferencia de archivos (FTP, File Transfer Protocol), se desarrollaron para especificar utilidades básicas necesarias para compartir información a través de ARPANET. A medida que ARPANET crecía en tamaño y alcance, aparecieron otros dos protocolos importantes:

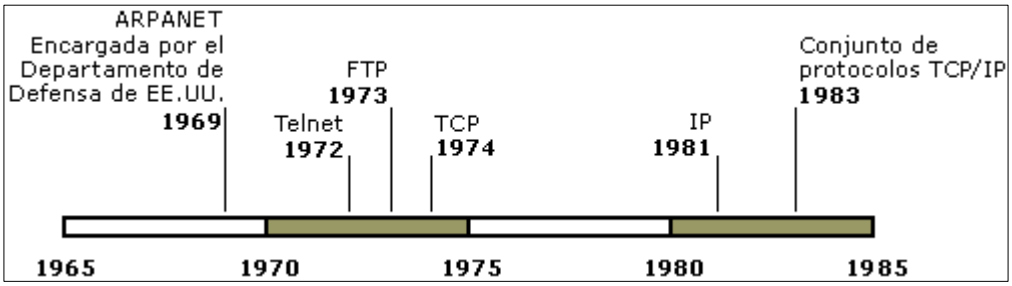
En 1974, se introdujo el Protocolo de control de transporte (TCP) como una especificación de borrador que describía cómo crear un servicio de transferencia de datos de host a host confiable a través de una red.

En 1981, se introdujo el Protocolo de Internet (IP) en forma de borrador que describía cómo implementar un estándar de direcciones y enrutar paquetes entre redes conectadas.

El 1 de enero de 1983, ARPANET comenzó a exigir el uso estándar de los protocolos TCP e IP para todo el tráfico de redes y comunicaciones fundamentales. A partir de esta fecha, ARPANET comenzó a ser más conocida como Internet y sus protocolos necesarios comenzaron a conocerse como el conjunto de protocolos TCP/IP.

El conjunto de protocolos TCP/IP está implementado en diversas ofertas de software de TCP/IP disponibles para muchas plataformas distintas. En la actualidad, el software TCP/IP sigue siendo de uso generalizado en Internet y se utiliza a menudo para crear

conjuntos de redes privadas enrutadas de gran tamaño. En la siguiente imagen podemos observar de manera grafica su evolución a través del tiempo.



Evolución de los protocolos

1.1.2. El modelo TCP/IP

TCP/IP está basado en un modelo de referencia de cuatro niveles. Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo.

Cada nivel del modelo TCP/IP corresponde a uno o más niveles del modelo de referencia Interconexión de Sistemas Abiertos (OSI, Open Systems Interconnection) de siete niveles o capas, propuesto por la Organización Internacional de Estándares (ISO, International Standards Organization).

Los tipos de servicios realizados y los protocolos utilizados en cada nivel del modelo TCP/IP se describen con más detalle en la Tabla 1.1

Nivel	Descripción	Protocolos
Aplicación	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
Transporte	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.	TCP, UDP, RTP

Internet	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.	IP, ICMP, ARP, RARP
Interfaz de red	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

TABLA 1.1

A continuación se definirán términos que se usarán a lo largo de todo el trabajo.

Dirección IP: Es una dirección de 32 bits utilizada para identificar a una computadora en una red, representada habitualmente mediante notación decimal, con puntos, separando el valor decimal de cada octeto con un punto. Ejemplo: “192.168.236.45”

IP Homologada: Es una dirección IP que es válida en Internet.

IP No-Homologada: Es una dirección IP que no se puede resolver públicamente, es decir que no es accesible desde Internet.

Dominio: Agrupación lógica de computadoras y otros recursos que comparten una misma base de datos bajo un mismo nombre de dominio.

Controlador de Dominio (DC): Es el servidor cuya función es la autentificación de los usuarios del dominio, mantiene las políticas de seguridad y una base de datos centralizada para todo el dominio.

Servidor de Nombres de Dominio (DNS): Es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa. Se conoce como zona Forward cuando es de nombre a IP y zona Reverse cuando es de IP a nombre. Y gracias a esto los usuarios podemos utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Protocolo de configuración dinámica de servidores (DHCP): Es un protocolo de red

en el que el servidor asigna los parámetros de configuración a las computadoras conectadas a la red que soliciten una dirección IP. Es decir sirve para administrar y asignar a los clientes una dirección IP, junto con la máscara de red, puerta de enlace, dns primario, wins primario, entre otros parámetros.

Servicio de enrutamiento y acceso remoto (RRAS): Es un servicio que permite las conexiones procedentes de clientes de acceso telefónico o VPN, y puede proporcionar enrutamiento IP o realizar ambas tareas a la vez.

Traducción de direcciones de Red (NAT): Oculta las direcciones IP administradas internamente a las redes externas, mediante la traducción de direcciones privadas a direcciones externas públicas. También oculta la estructura de la red interna, con lo que se reduce el riesgo de ataques contra los sistemas internos.

Protocolo: Un protocolo es una serie de normas y convenciones para enviar información a través de una red. Los protocolos pueden estar implementados en tarjetas de red, drivers o una combinación de ambas partes hardware y software.

Protocolo TCP/IP: Son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todas las computadoras en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes llegan a su destino final en el orden apropiado.

Protocolo de Internet (IP): Es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP se asegura de que los paquetes lleguen correctamente a su destino. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente.

Puerta de enlace (Gateway): Es un equipo que provee el acceso entre una intranet e Internet o entre dos redes de diferentes segmentos.

Directorio Activo (Active Directory): Agrupación lógica de objetos que comparten una base de datos en común (Active Directory Repository). El AD proporciona funcionalidad de servicio de directorio como medio para organizar, administrar y controlar centralmente el acceso a los recursos de red.

Red de computadoras: Conjunto de computadoras o equipos conectados entre sí para compartir recursos o servicios.

Unidad Organizacional (OU): Son contenedores de objetos que se usan para agrupar cuentas de usuario similares o equipos y que normalmente ayudan a representar la estructura física de la organización dentro del AD.

Group Policy Objet (GPO): Es un conjunto de una o más políticas del sistema. Cada

una de las políticas del sistema establece una configuración del objeto al que afecta. Por ejemplo, tenemos políticas para:

- Establecer el título del explorador de Internet
- Ocultar el panel de control
- Deshabilitar el uso de REGEDIT.EXE y REGEDT32.EXE
- Etc…

1.2. Requerimientos mínimos para instalar el sistema operativo Windows 2000® Server

Se requiere un equipo con al menos las siguientes características:

Procesador Pentium a 166 Mhz aunque se recomienda Pentium II y Pentium III, AMD K6, K6-2, K6 3 y Athlon o superior.

128 Mb de memoria RAM aunque se recomienda 256Mb.

Se necesita una partición con espacio suficiente de al menos 1 GB o más dependiendo de los componentes que se vayan a instalar entre más componentes mayor será el espacio requerido.

- ✓ Tarjeta de video VGA o resolución superior.
- ✓ Teclado.
- ✓ Mouse (opcional)
- ✓ Unidad de CD-ROM o de DVD.
- ✓ Unidad de 3 ½“ si el sistema no admite el inicio desde la unidad de CD-ROM.

1.3. Componentes a instalar

Antes de proceder a instalar el Sistema Operativo debemos saber qué componentes vamos a instalar, esto dependerá de las necesidades que tengamos, Windows 2000 incluye una gran variedad de componentes principales, incluidas numerosas herramientas administrativas, que el programa de instalación agrega automáticamente, pero no es necesario seleccionar todos los componentes en ese momento, se pueden instalar después (con agregar o quitar programas del *Panel de Control*).

Dependiendo del rol que va a desempeñar nuestro servidor podemos seleccionar que componentes necesitamos tener instalados, se recomienda que los Servidores tengan en lo posible bien definido su rol y no ejecuten muchos servicios en el mismo equipo, esto nos beneficiará en el desempeño y en la seguridad del mismo.

Algunas de las funciones o roles que puede desempeñar un servidor son:

- ➢ Servidor DHCP, Servidor DNS o Servidor WINS

- Servidor de Acceso a Archivos o Acceso a Impresión
- Servicios de Terminal Services
- Autenticación y comunicación segura. (IAS)
- Servicios de Internet (Web, Ftp, News)
- Servidor de Correo (Exchange, Lotus Notes)

1.4. Modalidad de Licencia

También es importante saber que modo de licencia utilizaremos, los dos tipos que admite Windows son: Por Puesto y Por Servidor

Por puesto.- Cada equipo que tenga acceso a un servidor que ejecuta Windows 2000® Server requiere una Licencia de acceso de cliente (CAL) independiente. Éste es el método de licencia utilizado con más frecuencia para compañías con más de un servidor que ejecuta Windows 2000 Server.

Por servidor.- Significa que cada conexión simultánea a este servidor requiere una CAL independiente. Es decir, en un momento dado, Windows 2000® Server puede admitir un número fijo de conexiones. Por ejemplo, si se selecciona el modo Por servidor y cinco conexiones simultáneas, este servidor que ejecuta Windows 2000® Server puede tener cinco equipos (clientes) conectados a la vez. Estos equipos no necesitarían licencias adicionales. El modo de licencia Por servidor suele preferirse para compañías pequeñas con un solo equipo que ejecuta Windows 2000® Server.

CAPÍTULO 2. INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO WINDOWS 2000® SERVER

Antes de empezar a describir a detalle el proceso de instalación mencionaremos cuales son las versiones de Windows 2000® Server que existen:

Microsoft Windows 2000® Server

Este es el sistema operativo de red para los negocios pequeños y medianos. Es la solución perfecta para servidores de archivos, impresión, intranet e infraestructura. Aunque no se recomienda para servicios de misión crítica. Soporta desde 1 a 4 procesadores y soporta hasta 4GB de RAM.

Microsoft Windows 2000® Advanced Server

Windows 2000® Advanced Server es un sistema operativo que ofrece mayor confiabilidad, disponibilidad y escalabilidad para ejecutar aplicaciones de comercio electrónico y de la línea de negocio. Las opciones de arreglo (RAID) ofrecen más confiabilidad y disponibilidad. Recomendado para servicios de misión crítica. Soporta desde 1 hasta 8 procesadores y puede soportar el doble de memoria que la versión Server es decir hasta 8GB de RAM.

Microsoft Windows 2000® Datacenter Server

Windows 2000® Datacenter Server es el sistema operativo de servidor más poderoso ofrecido por Microsoft. Windows 2000® Datacenter Server está diseñado para las empresas que demandan el más alto nivel de disponibilidad y escalabilidad. Proporciona máxima confiabilidad y disponibilidad con sus opciones de arreglos (clustering) de 4 nodos. Soporta desde 1 hasta 32 procesadores y puede soportar hasta 32 GB de RAM.

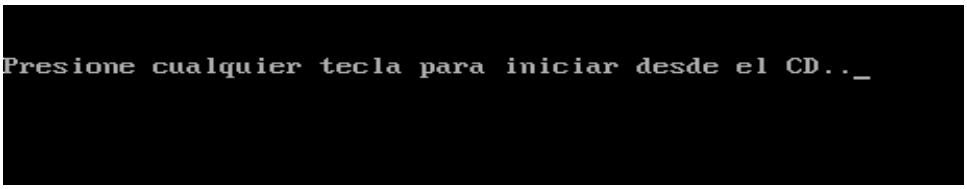
La instalación que describiremos en este documento será una instalación limpia desde el CD de Microsoft Windows 2000® Server, es decir borraremos el contenido del Disco Duro si es que tuviese algo, aunque no es la única manera de instalar Windows 2000® Server, existen otras opciones como la de actualizar la versión del sistema operativo o iniciar la instalación desde la red o iniciar la instalación desde el Open Manage del fabricante entre otras.

A continuación se describirá e ilustrará con detalle el proceso de instalación.

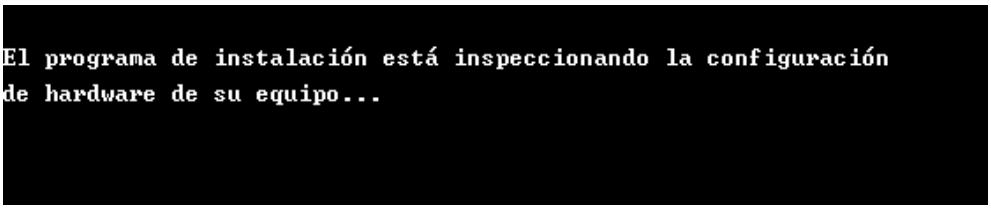
2.1. Procedimiento de instalación del sistema operativo

Insertar el CD de Windows 2000® Server en la unidad de CD-ROM y reiniciar el equipo.

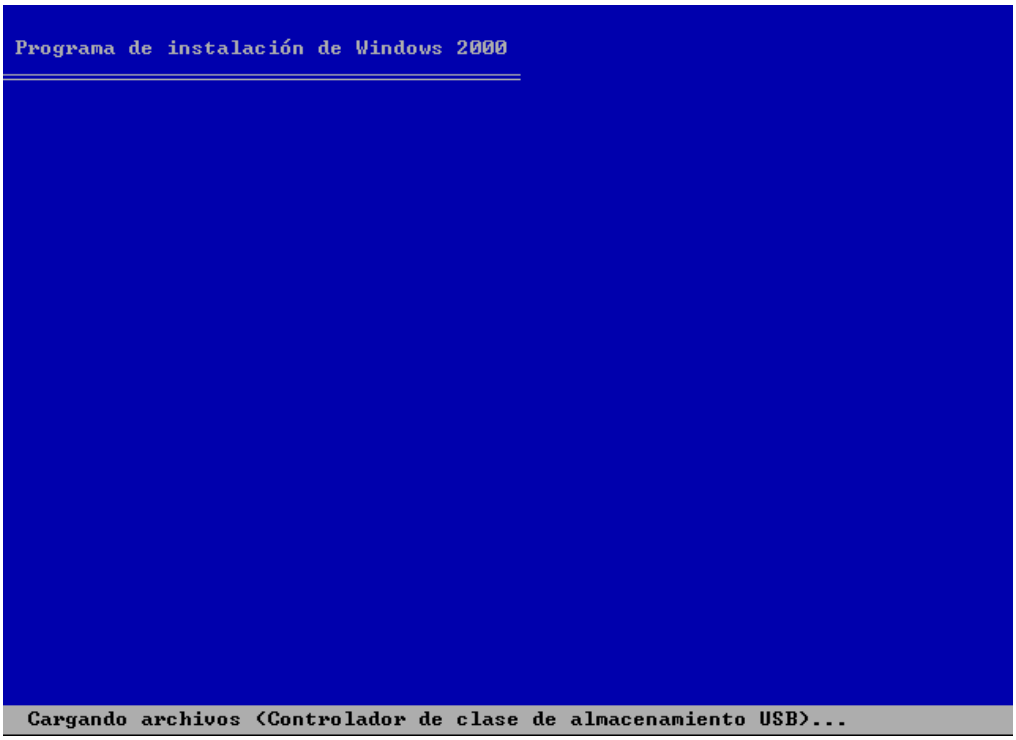
A continuación verá la siguiente pantalla.



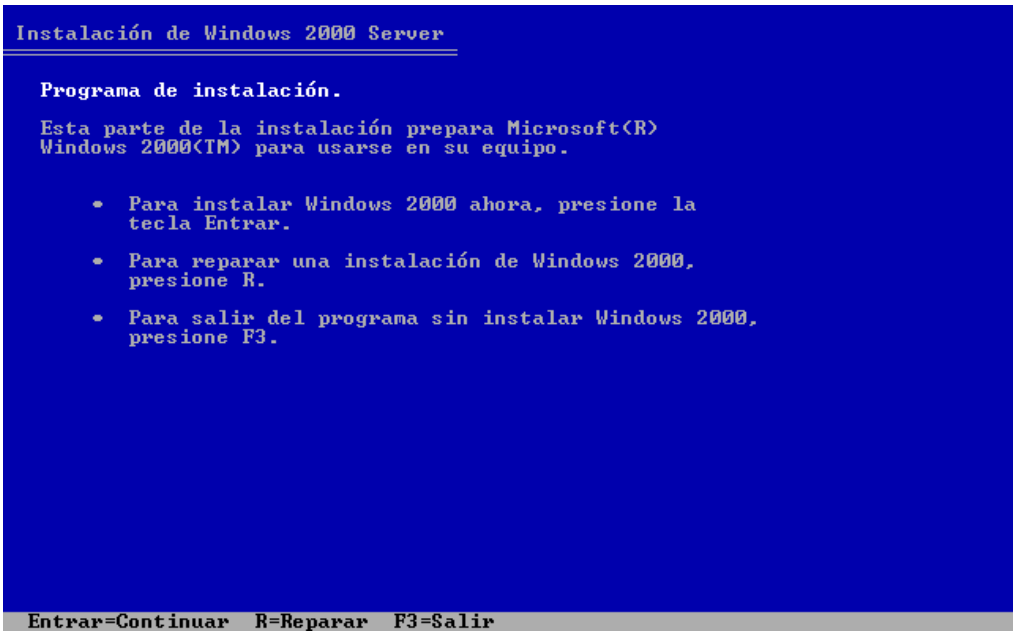
Aquí presionamos cualquier tecla para que inicie nuestro equipo desde el CD de Windows 2000® Server y posteriormente saldrá la siguiente pantalla.



Aquí se está reconociendo el hardware del equipo, al terminar mostrará la siguiente pantalla.

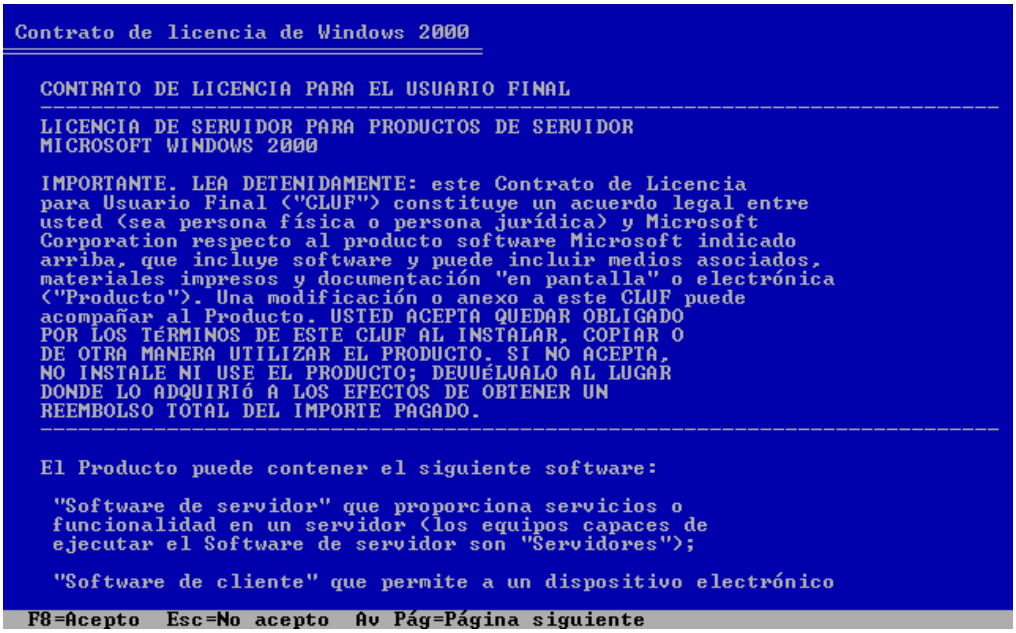


En la pantalla anterior, se muestra como carga los archivos necesarios para empezar la instalación es decir los controladores. Una vez terminado el proceso mostrará la siguiente pantalla.

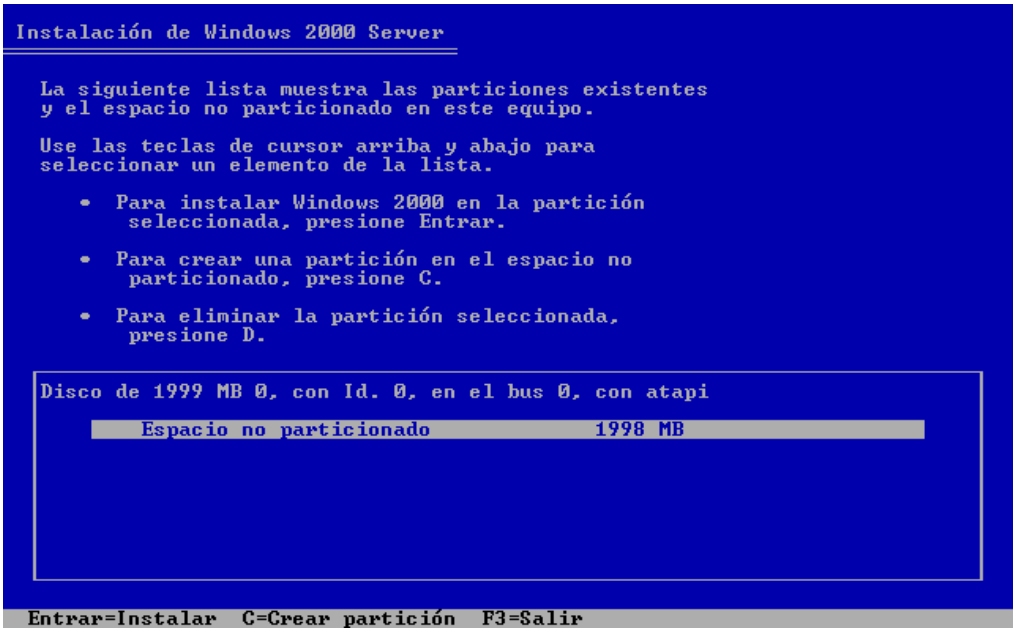


En esta pantalla aparecen tres opciones del tipo de instalación, seleccionaremos la

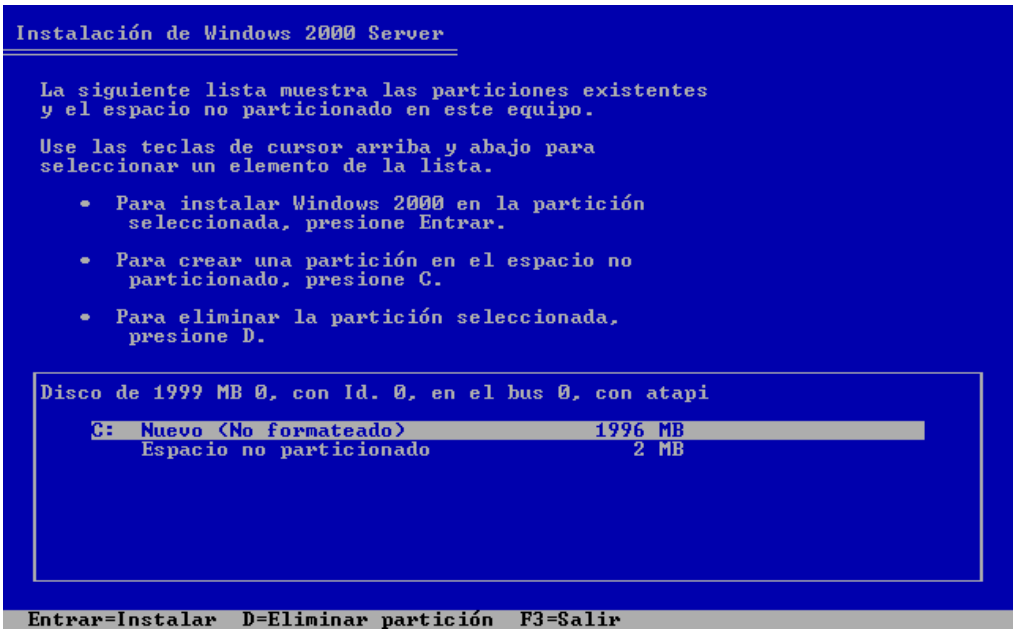
primera ya que haremos una nueva instalación. Así que pulsamos la tecla "*ENTER*" y mostrará la siguiente pantalla.



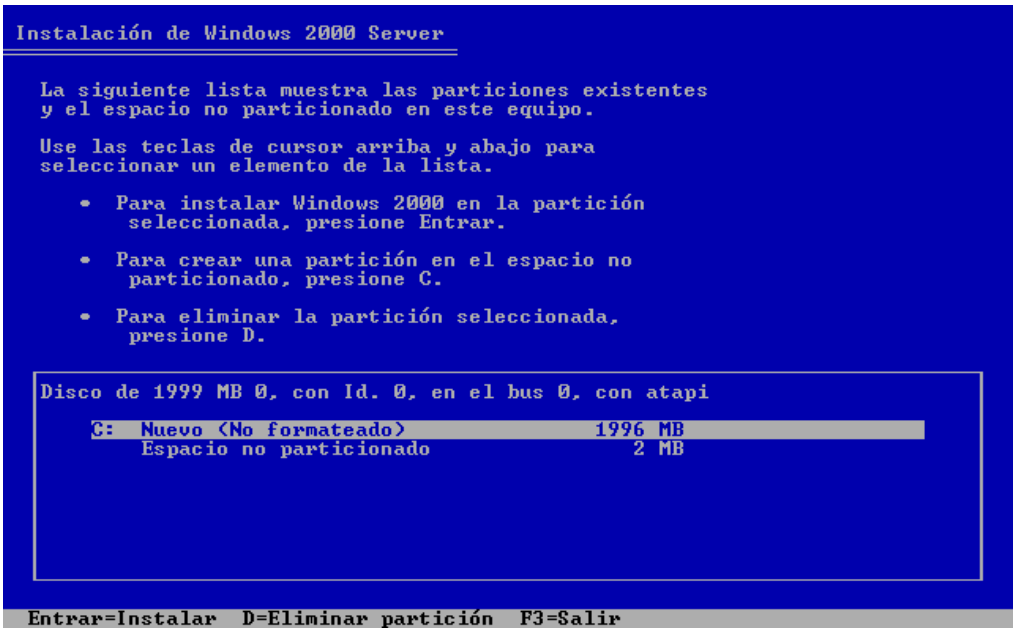
Aquí se observa la pantalla donde aparece el contrato de licencia de Windows 2000® Server. Con la tecla "*Av Pag*" nos desplazaremos a lo largo del documento para su lectura y posteriormente pulsaremos la tecla "*F8*" para aceptar este contrato y mostrará la siguiente pantalla.



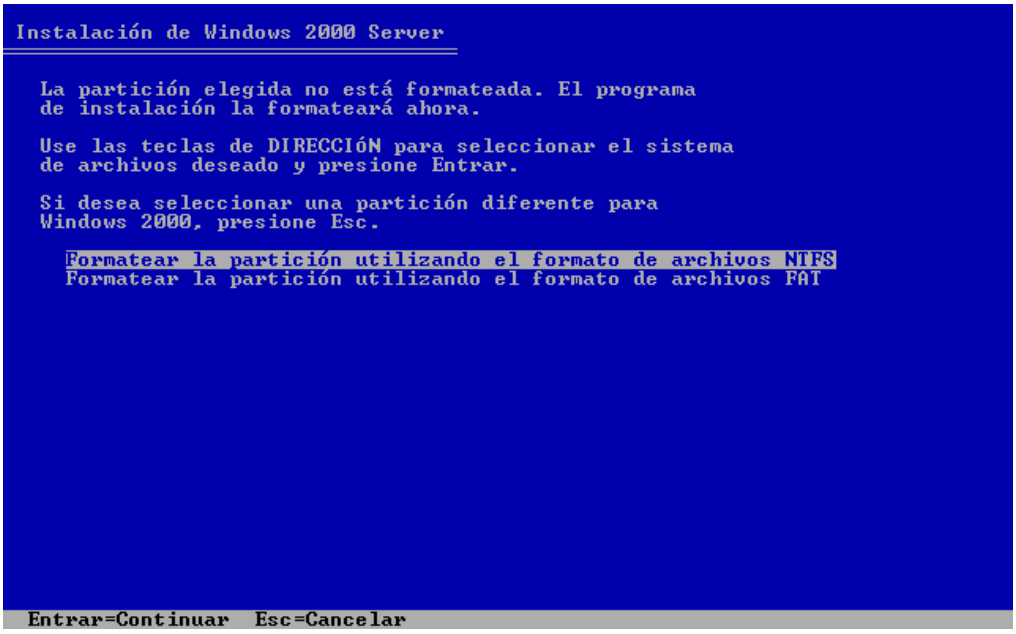
Esta pantalla nos muestra las particiones de nuestro equipo. En este caso no tenemos ninguna creada, así que pulsaremos la tecla "*C*" para crear una nueva partición y mostrará la siguiente pantalla.



Aquí estableceremos el tamaño en Mega Bytes para la partición primaria, en nuestro caso seleccionamos el total del tamaño y pulsaremos la tecla "ENTER" para continuar y aparecerá la siguiente pantalla.



Aquí podemos observar que se creo la partición C, para continuar con la instalación pulsamos la tecla "*ENTER*" y mostrará la siguiente pantalla.



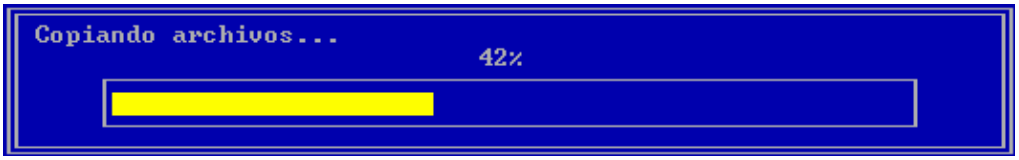
En esta pantalla nos informa que se necesita dar formato a nuestra nueva partición, seleccionamos la primera opción formato de archivos NTFS, presionamos "*ENTER*" y aparecerá la siguiente pantalla.

Aquí se aprecia cómo se está formateando nuestra partición. Sólo debemos esperar a que

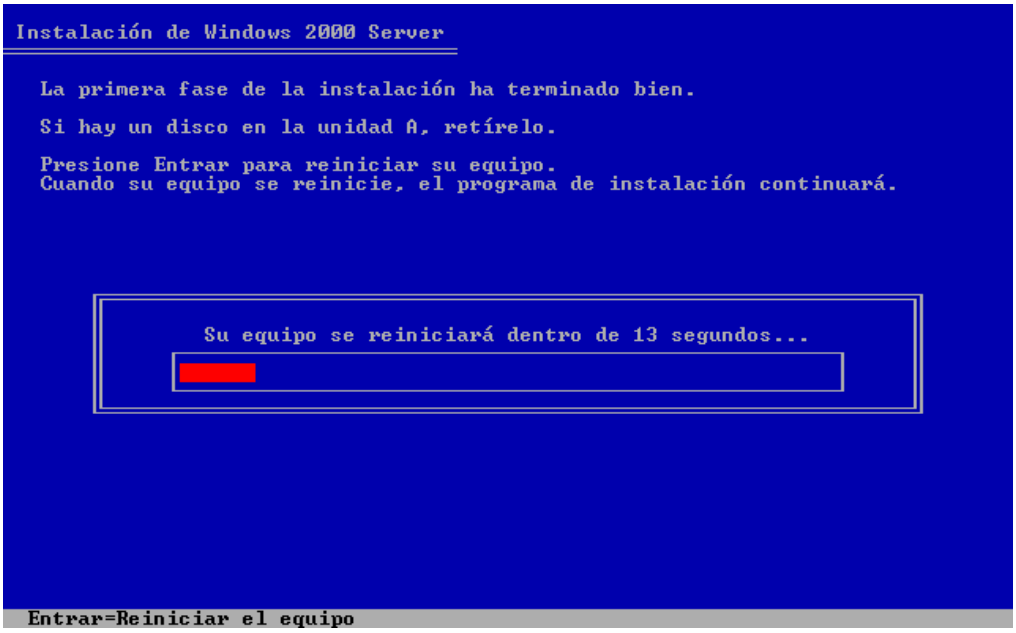
termine.

En esta pantalla se aprecia que el avance del proceso llegó al 100%, lo que indica que podemos seguir con la instalación.

Aquí se muestra que empieza la copia de archivos de instalación.



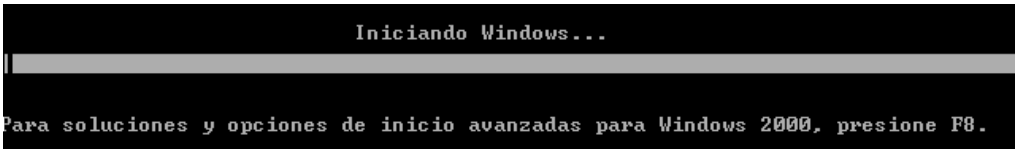
Al llegar al 100% de archivos copiados nos mostrará la siguiente pantalla.



Al llegar a esta pantalla significa que hemos realizado correctamente la primera fase de la instalación y que debemos reiniciar el equipo para continuar el proceso sin retirar el CD

de la unidad.

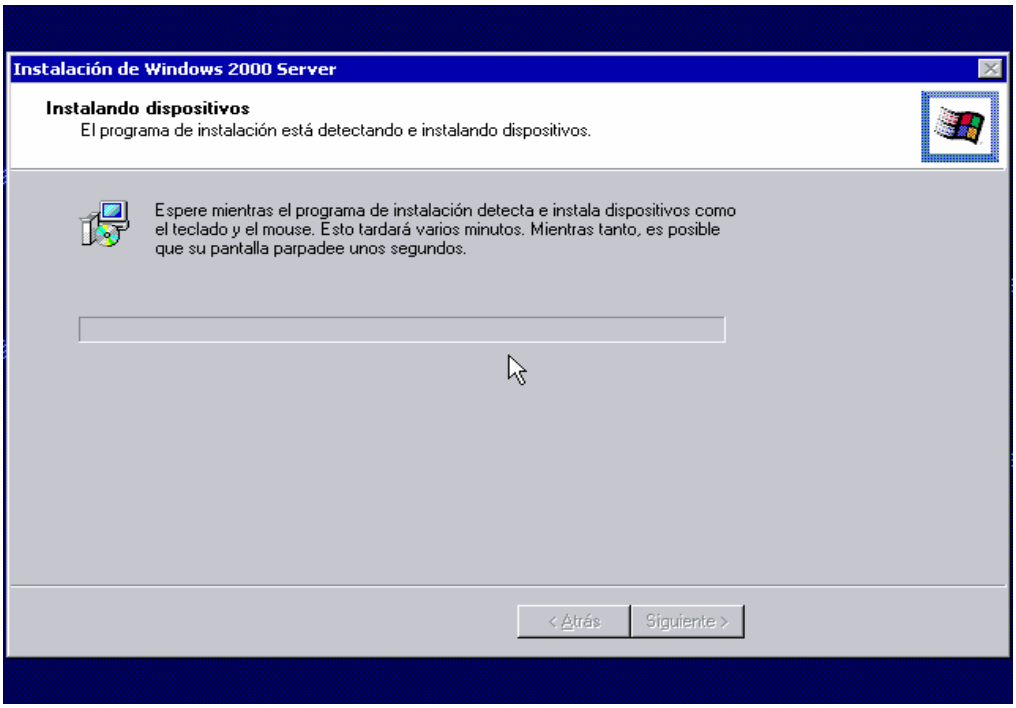
Al reiniciar el equipo ésta será la pantalla que veremos.



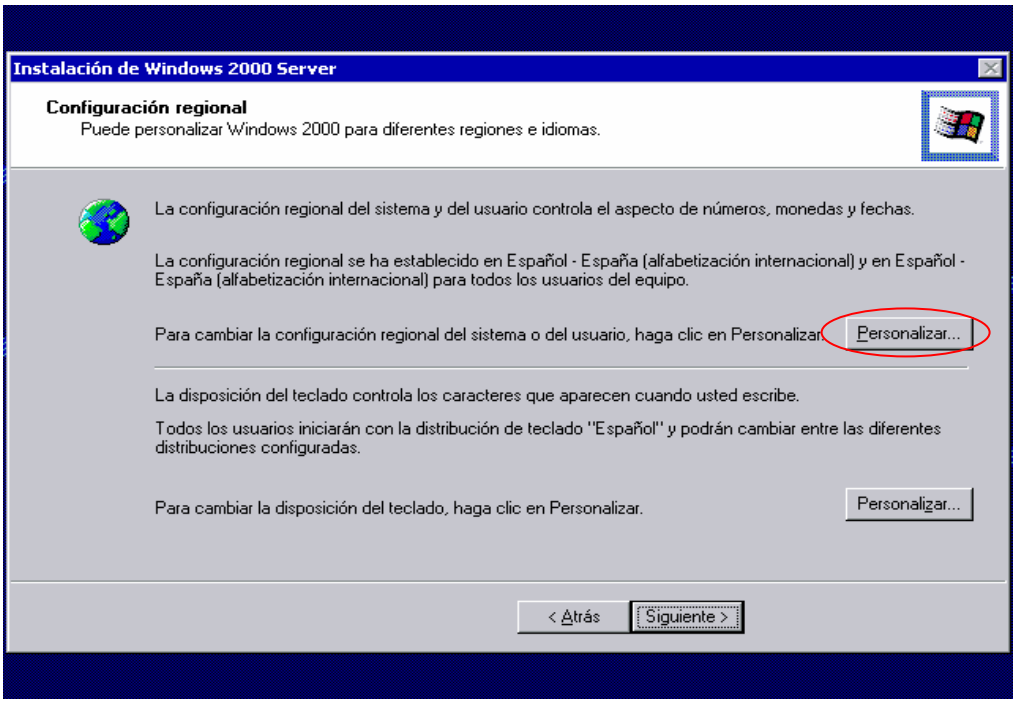
Después aparecerá esta pantalla donde esta cargando el programa de instalación.

Una vez terminado este proceso aparecerá la siguiente pantalla.

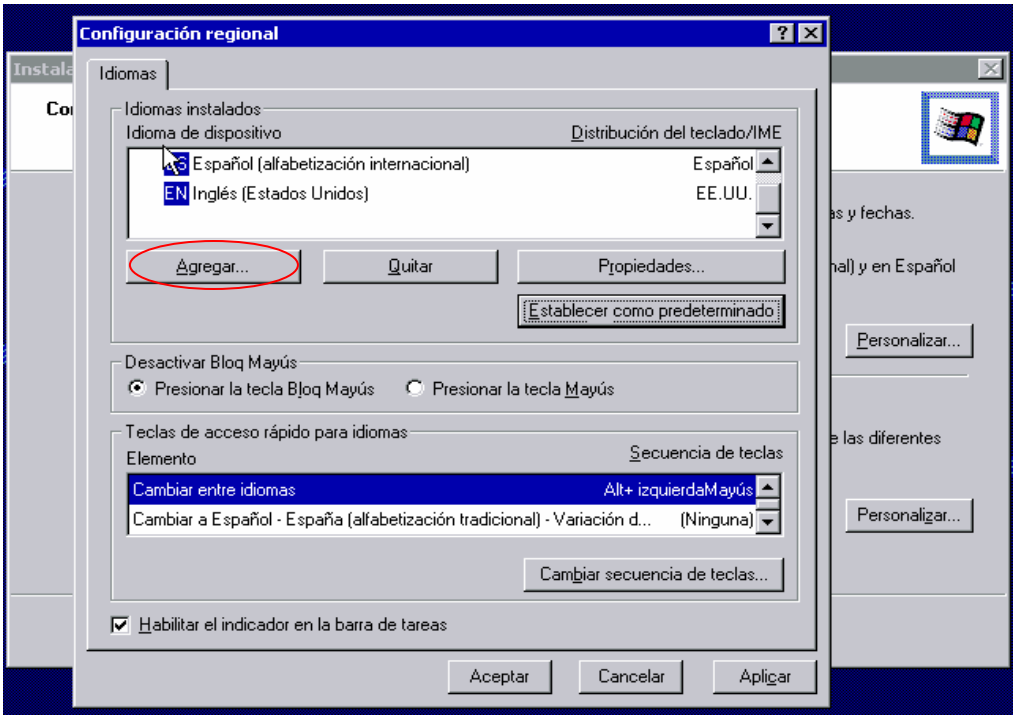
Aquí podemos observar el asistente que nos guiará con la instalación de Microsoft Windows 2000® Server damos clic en "***siguiente***" y aparecerá la siguiente pantalla.



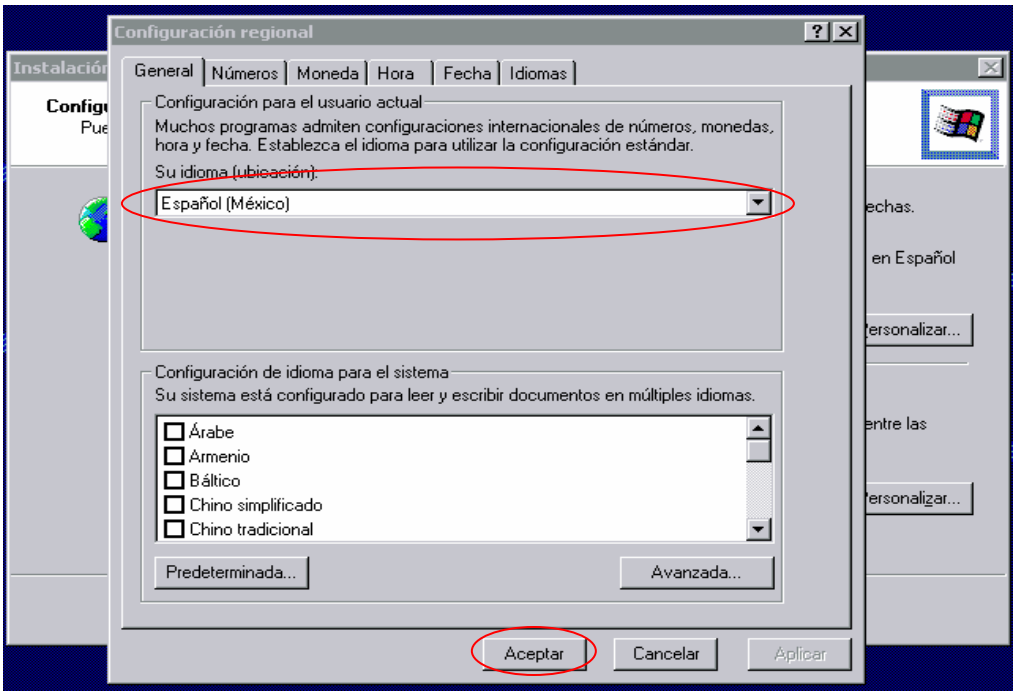
En la pantalla anterior se muestra como está detectando e instalando los dispositivos como son: Teclado, Mouse, Tarjeta de Video, etc. El proceso puede tardar algunos minutos dependiendo de cada equipo, una vez terminado aparecerá la siguiente pantalla.



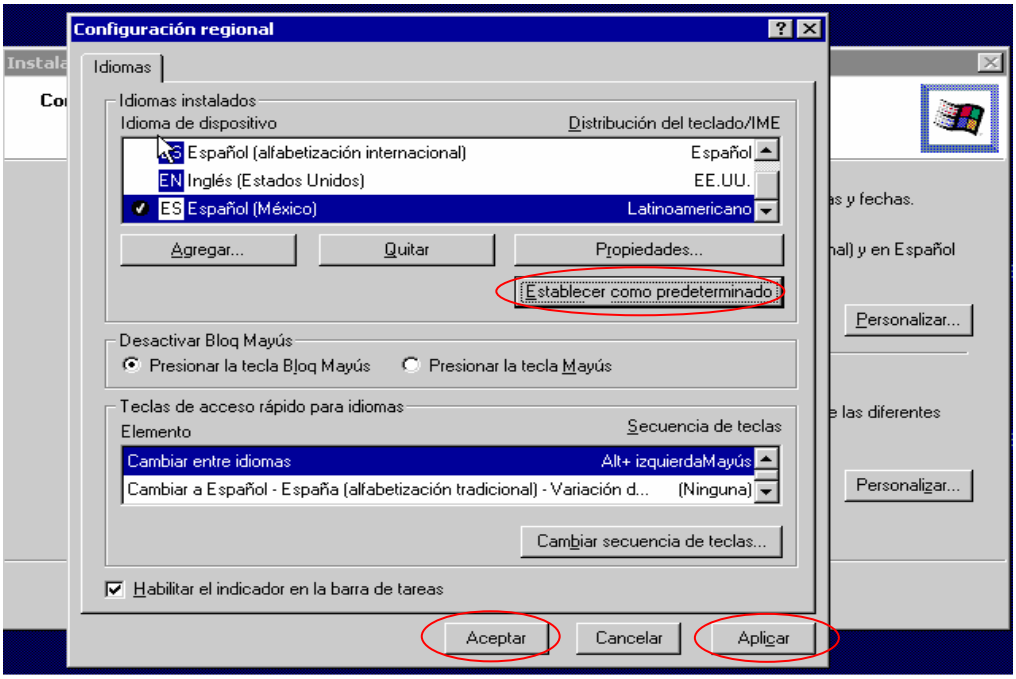
En la pantalla anterior podemos establecer la configuración regional del sistema y el idioma de nuestro teclado. Para ésto damos clic sobre el primer botón "***Personalizar***" con lo que aparecerá la siguiente pantalla de configuración regional.



En esta pantalla se muestra la configuración actual del sistema que está en Español Internacional, así que procederemos a personalizar nuestra configuración dando un "*clic*" en "***Agregar***" y nos mostrará la siguiente pantalla.

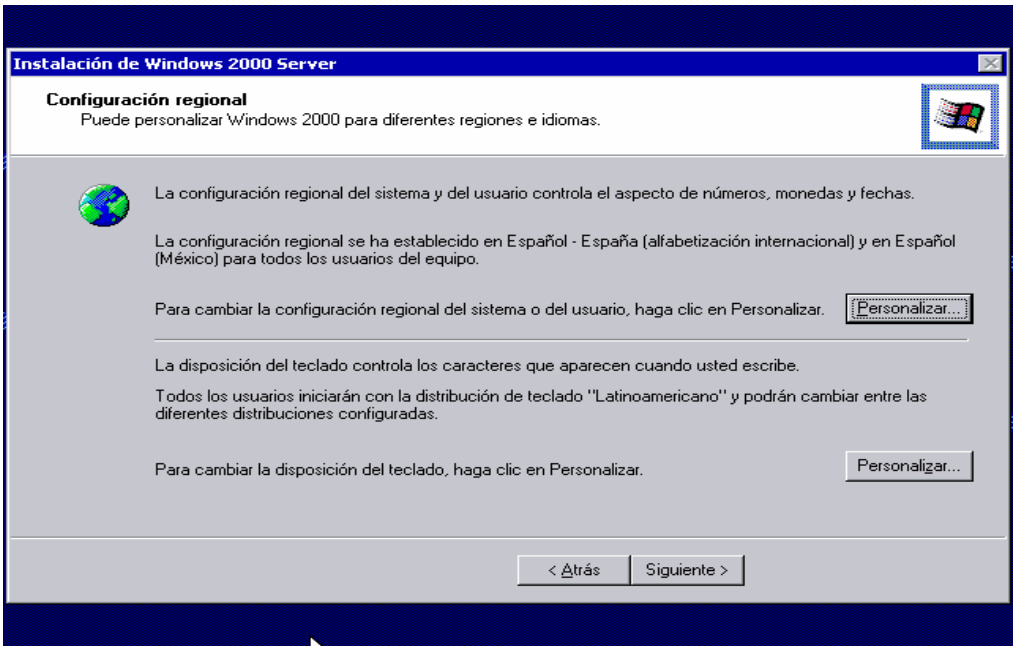


Seleccionamos Español (México) y damos "*clic*" en "***Aceptar***" con lo cual nos regresará a la pantalla anterior, pero ahora con la opción que agregamos.

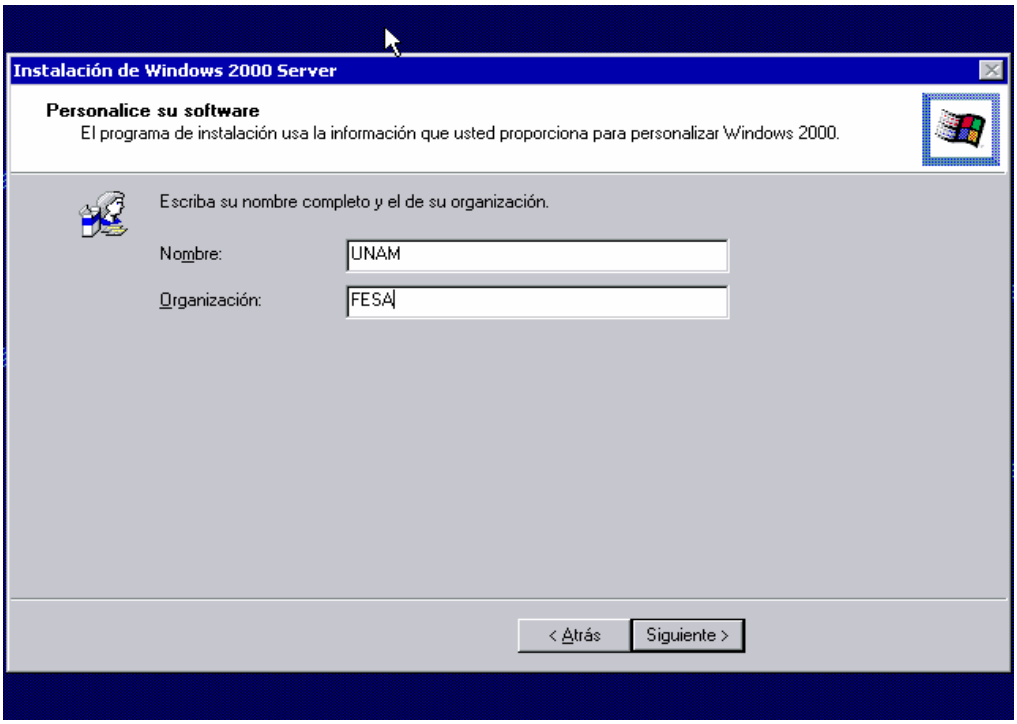


En la pantalla anterior definimos el idioma Español (México) como predeterminado para esto damos clic en "***Establecer como predeterminado***" y después damos clic en "***Aplicar***"

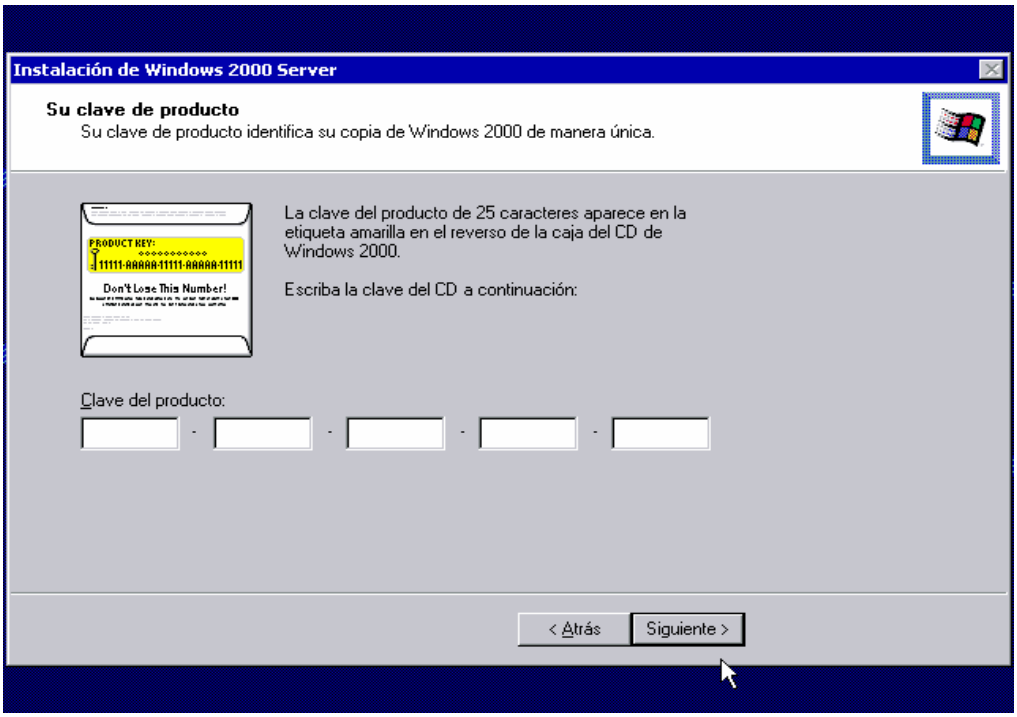
y por último en "***Aceptar***" con lo cual nos regresará a la primer pantalla pero con la opción que acabamos de definir.



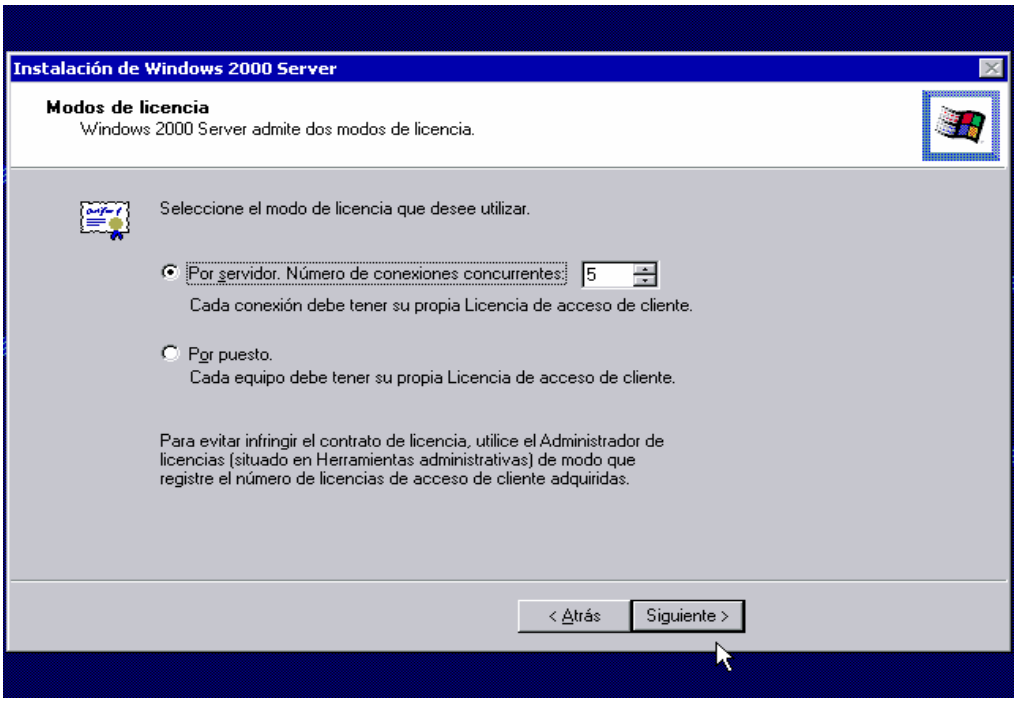
Ahora podríamos personalizar la distribución del teclado pero este está configurado con distribución "*Latinoamericano*" lo cual es correcto por lo que no realizaremos cambio alguno, así que damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



En la pantalla anterior nos pide nombre completo y el nombre de nuestra organización. Para nuestro ejemplo pondremos "UNAM" y "FESA" respectivamente, damos clic en "***siguiente***" y aparecerá la siguiente pantalla.

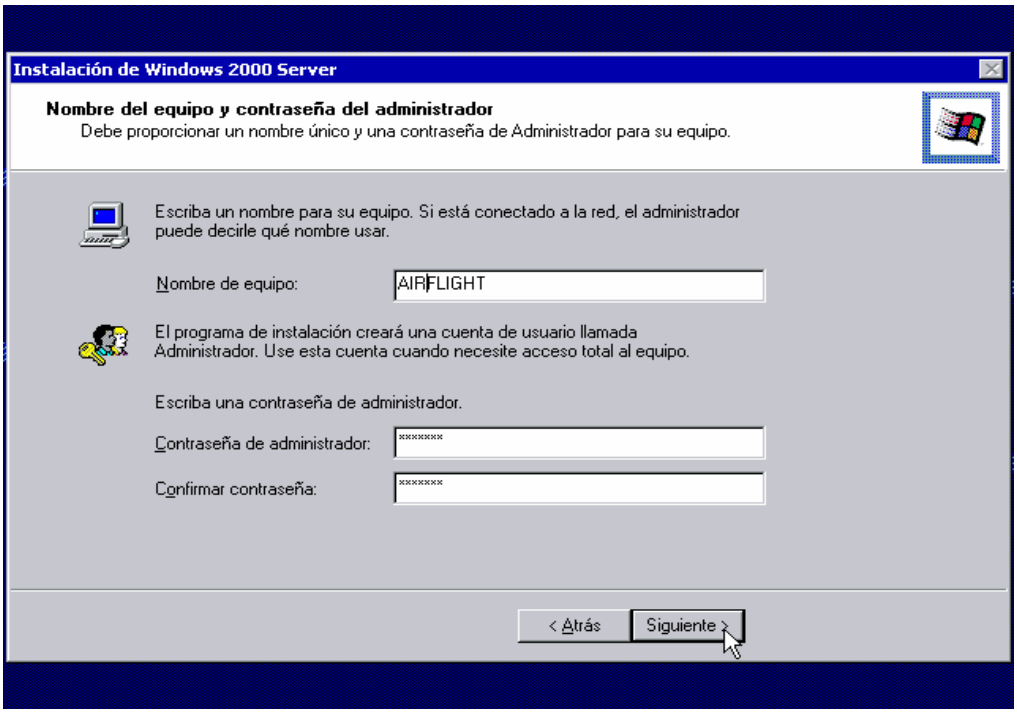


En esta pantalla debemos teclear la clave del producto, introducimos nuestra clave, damos clic en "***siguiente***" y aparecerá la siguiente pantalla.

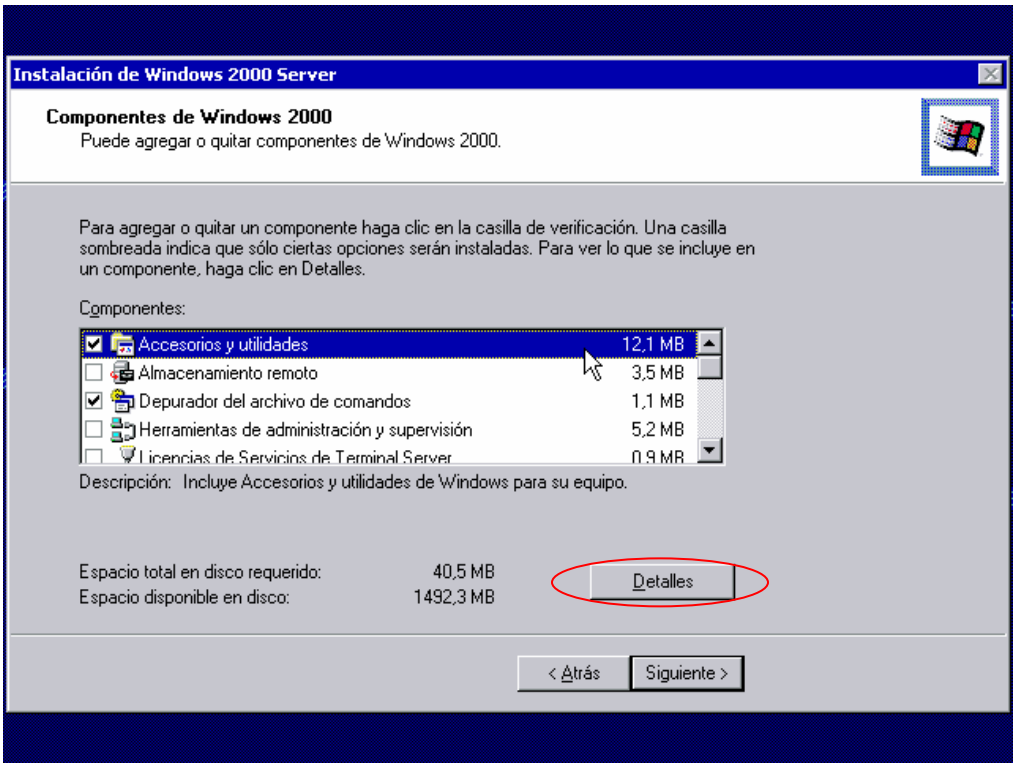


En la pantalla anterior definimos el modo de licencia que vamos a utilizar, para este

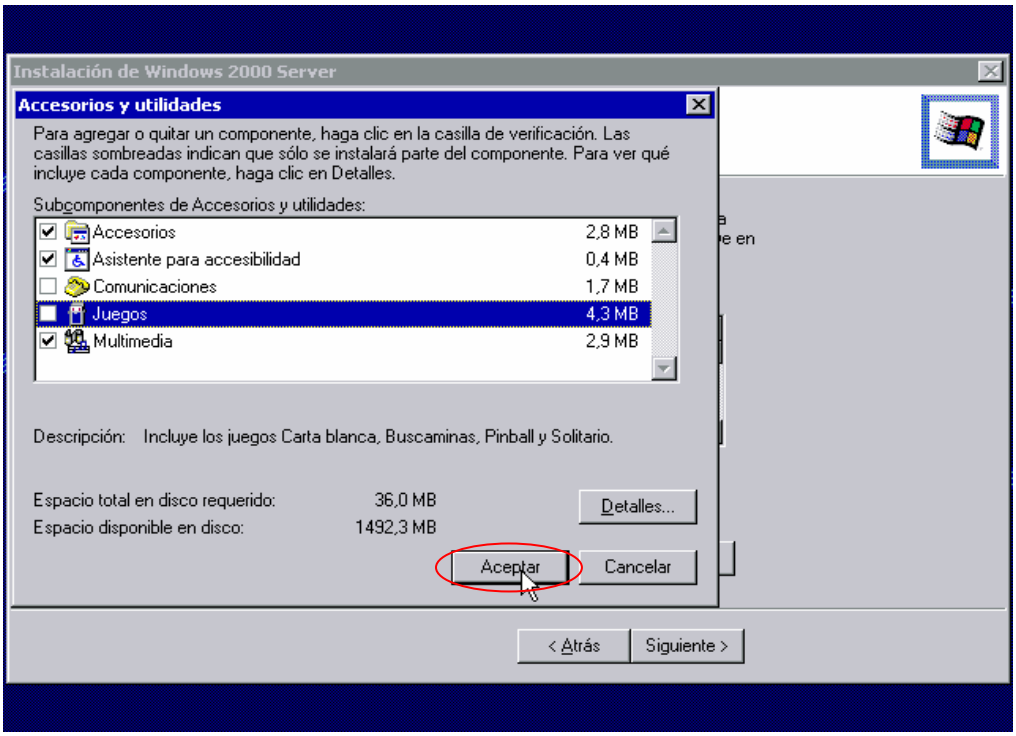
ejemplo utilizaremos "*Por servidor, número de conexiones concurrentes*" establecemos el número, damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



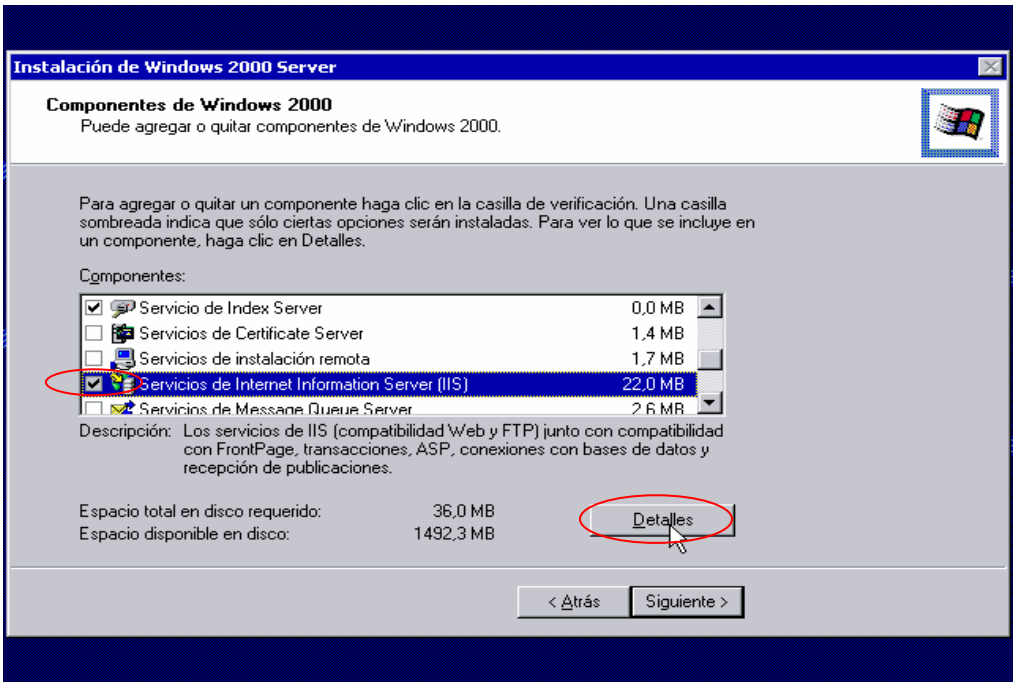
En esta pantalla nos pedirá el nombre del equipo y contraseña del administrador, proporcionamos los datos, damos clic en "***siguiente***" y aparecerá la siguiente pantalla.



En esta pantalla seleccionaremos los componentes que vamos a instalar, recordando que entre menos componentes agreguemos más seguro será nuestro servidor. Es decir quitaremos componentes que no necesitamos, ésto dependerá de cada caso en particular y del rol que desempeñara nuestro equipo. Para ejemplo quitaremos juegos y comunicaciones que se encuentran en "*Accesorios y utilidades*" para esto damos clic en ***detalles*** y aparecerá la siguiente pantalla.

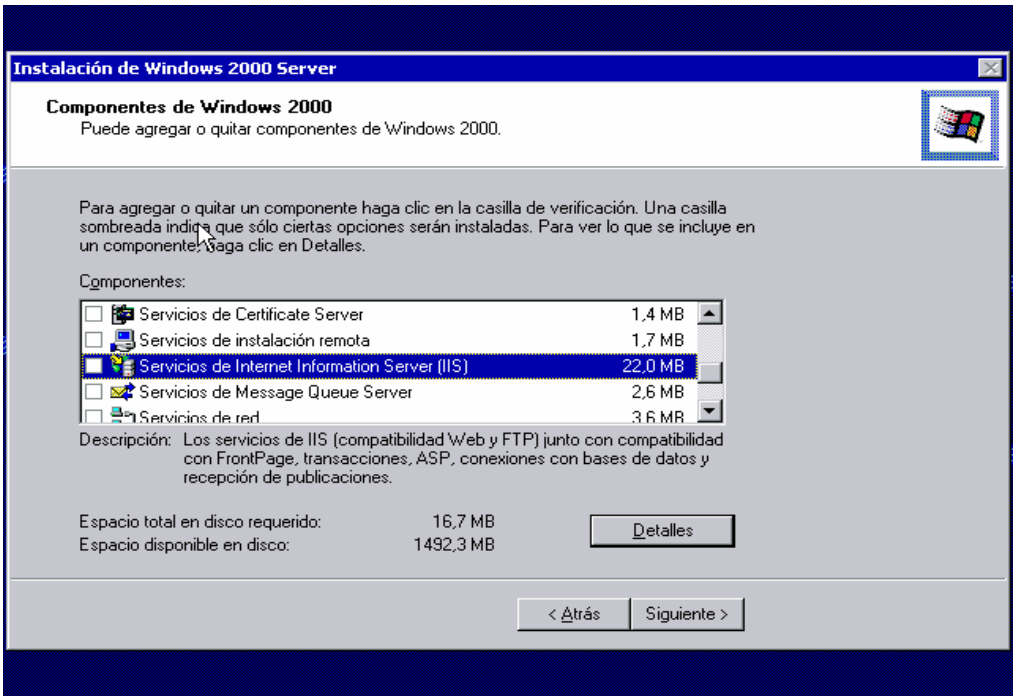


Aquí es donde se listan los subcomponentes, para quitarlo bastará con desmarcar la casilla del subcomponente que no requerimos damos clic en "***aceptar***" y nos regresará a la pantalla anterior.

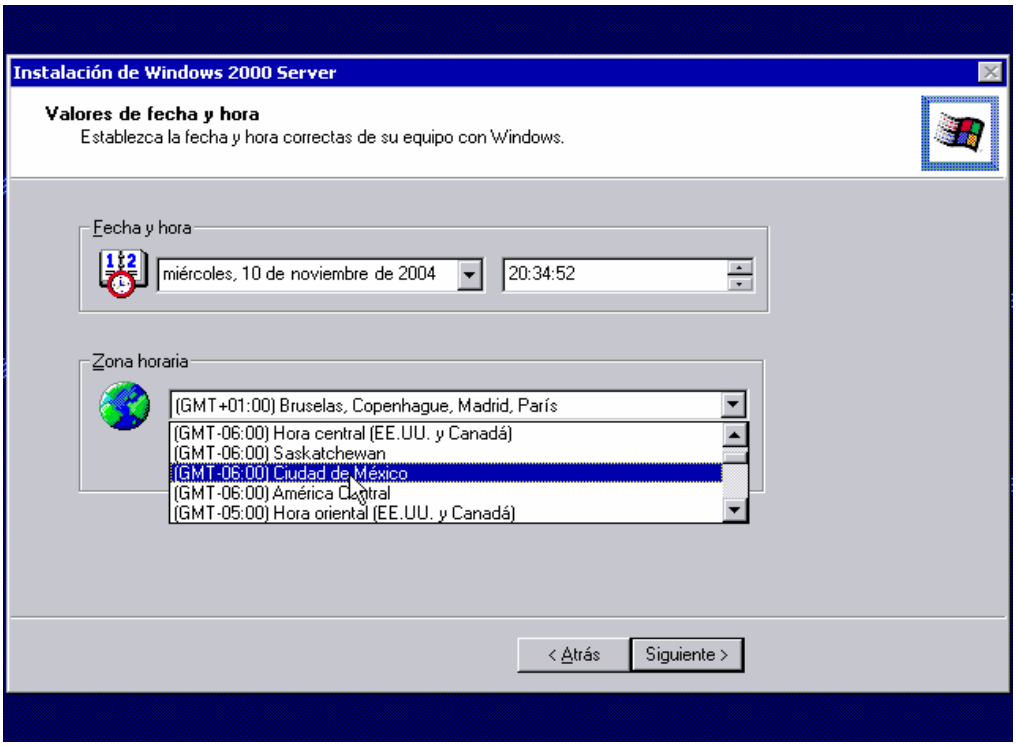


Aquí se observa como quitaremos los servicios de IIS[1] debido a que no requerimos brindar el servicio Web (WWW), para ésto seleccionamos el componente después damos clic sobre el check box con lo que ya no aparecerá seleccionado, al terminar mostrará una pantalla similar a ésta.

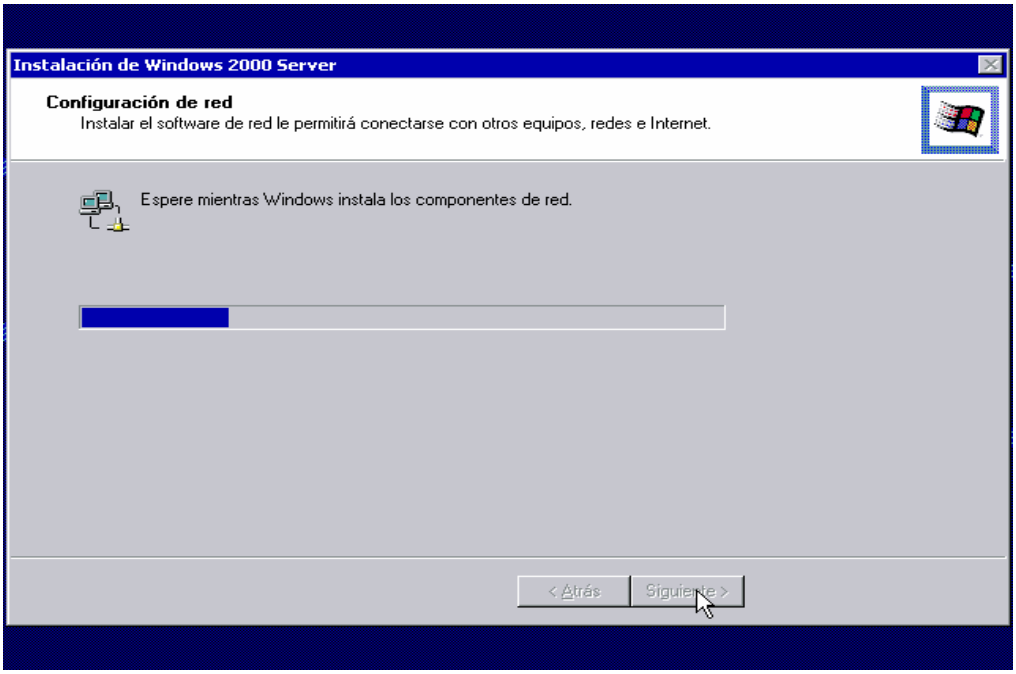
[1] IIS: Internet Information Services, es el servidor de páginas Web de la plataforma Windows. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.



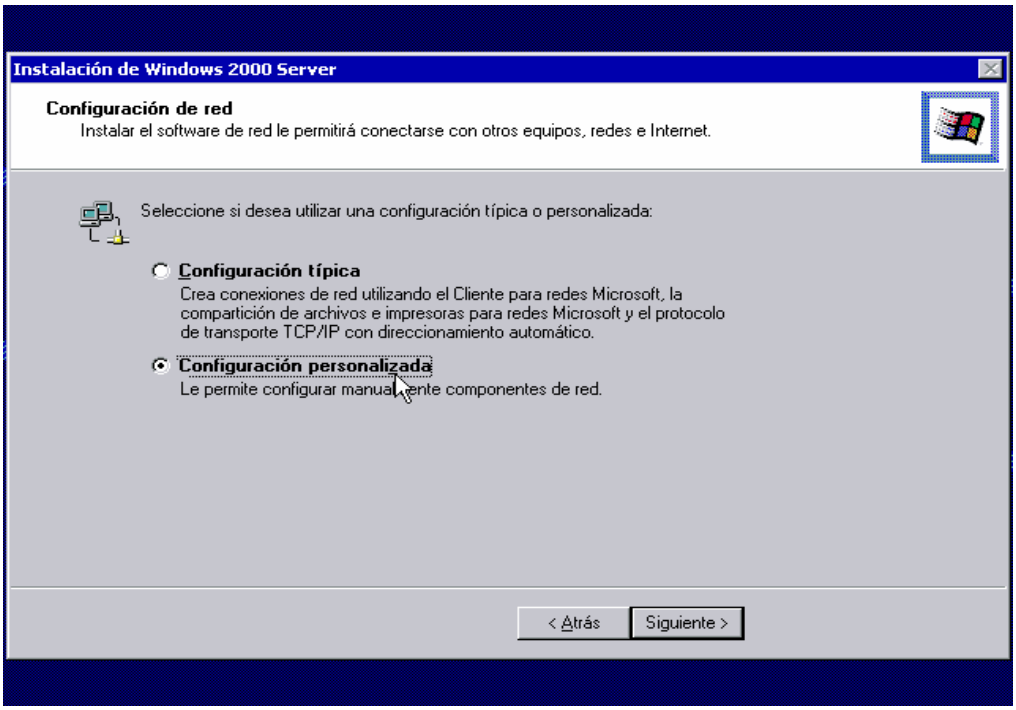
En esta pantalla podemos seguir quitando los componentes que no utilizaremos, para este ejemplo hemos terminado, damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



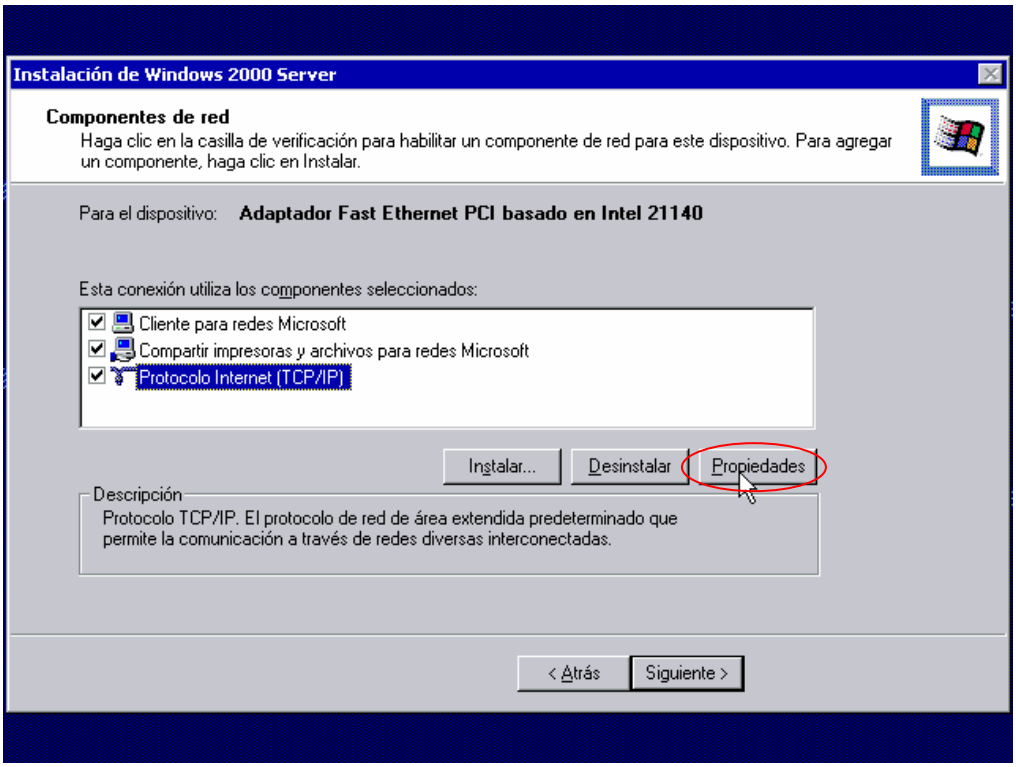
Seleccionamos los valores de fecha, hora y zona horaria respectivamente, para la zona horaria seleccionaremos "*Ciudad de México*", damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



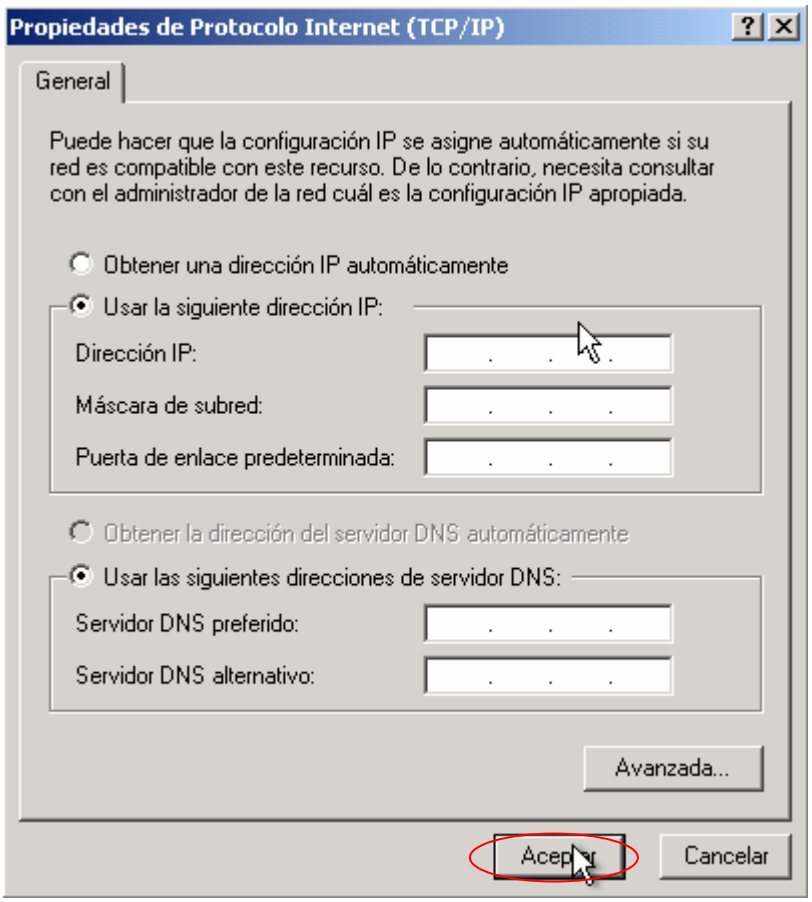
Aquí esta detectando e instalando los controladores de la tarjeta de red si es que existe o si es que los controladores son compatibles con el Sistema Operativo (de lo contrario se tendrá que instalar los controladores de forma manual) al terminar mostrará la siguiente pantalla.



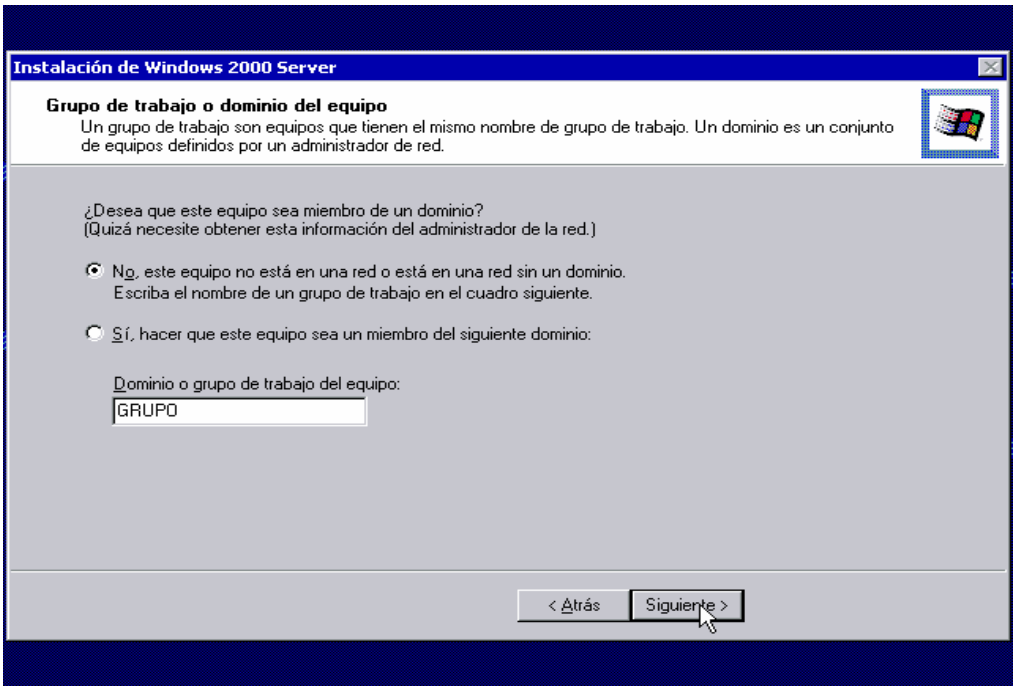
En esta pantalla seleccionaremos la segunda opción es decir nosotros configuraremos manualmente nuestra tarjeta de red, damos clic en "***siguiente***" y aparecerá la siguiente pantalla.



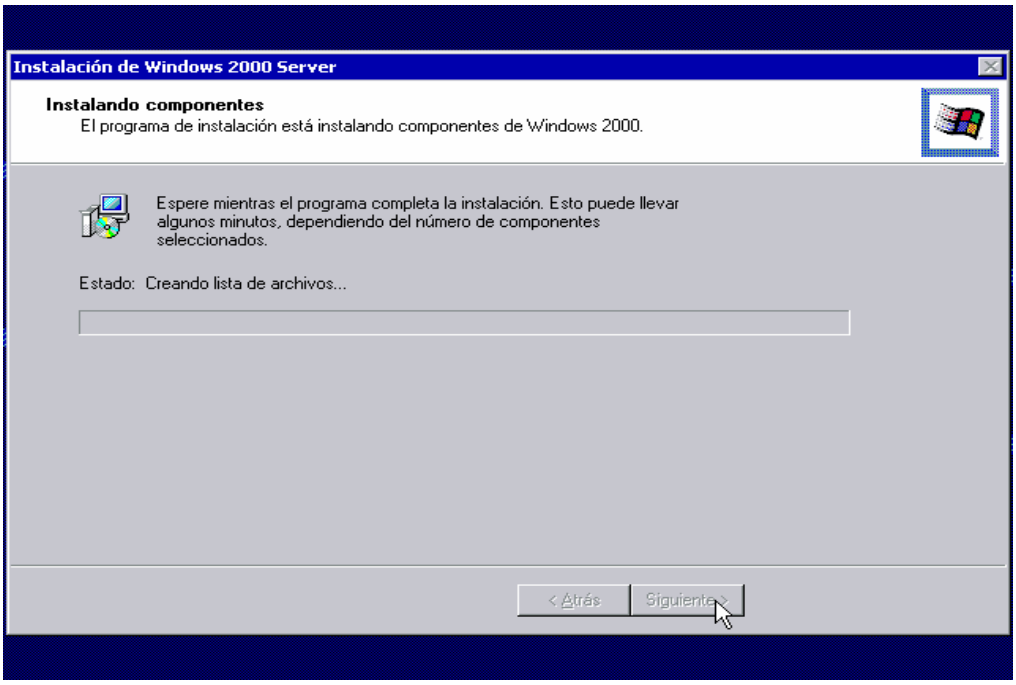
Antes de continuar con el procedimiento cabe hacer la aclaración que para poder configurar esta opción necesitamos contar con una dirección IP, un servidor DNS y una puerta de enlace o gateway. También se recomienda no conectar este servidor directamente a Internet ya que no cuenta con ninguna seguridad ni actualización y es vulnerable a un ataque de gusanos, virus u otro de cualquier índole, solo se recomienda conectarlo en una intranet que cuente con la seguridad necesaria para no poner en riesgo nuestra nueva instalación. Una vez hecho esta aclaración proseguiremos con este proceso, en esta pantalla seleccionaremos *Protocolo Internet* (TCP/IP) y damos clic en ***Propiedades*** con lo que aparecerá la siguiente pantalla.



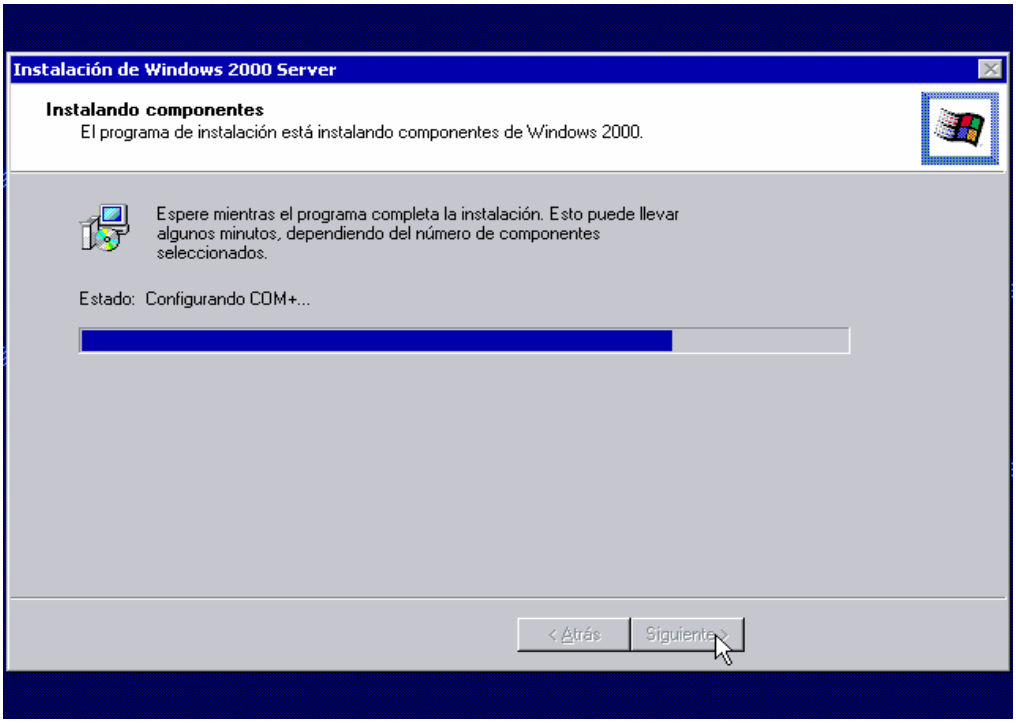
En esta pantalla introduciremos la dirección IP, la máscara de subred, la puerta de enlace predeterminada o gateway, el servidor DNS preferido y el alterno si fuera el caso. Al terminar damos clic en ***Aceptar*** y nos regresará a la pantalla anterior donde daremos clic en ***siguiente*** y aparecerá la siguiente pantalla.



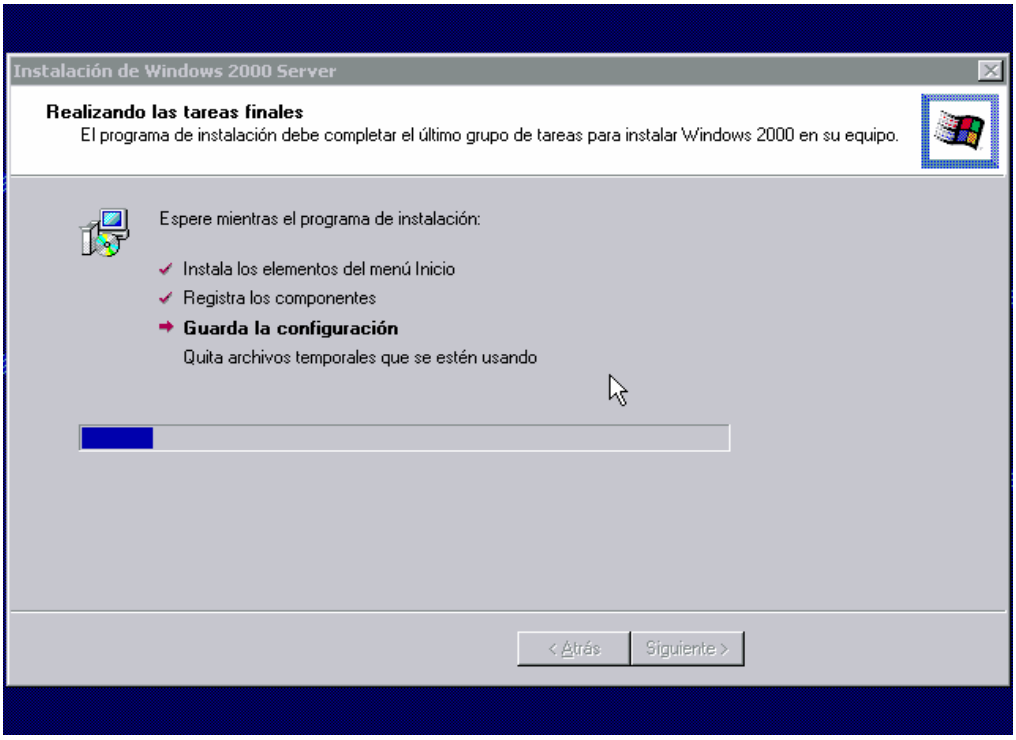
Esta pantalla nos pregunta si nuestro equipo formará parte de un dominio o no. En este caso escogeremos la primera opción es decir que forme parte de un Grupo de Trabajo ya que este será nuestro primer servidor en la organización y aún no tenemos ningún dominio, el nombre que le pondremos a nuestro Grupo de Trabajo es opcional, para este caso le dejaremos GRUPO daremos clic en "***siguiente***" y aparecerá la siguiente pantalla.



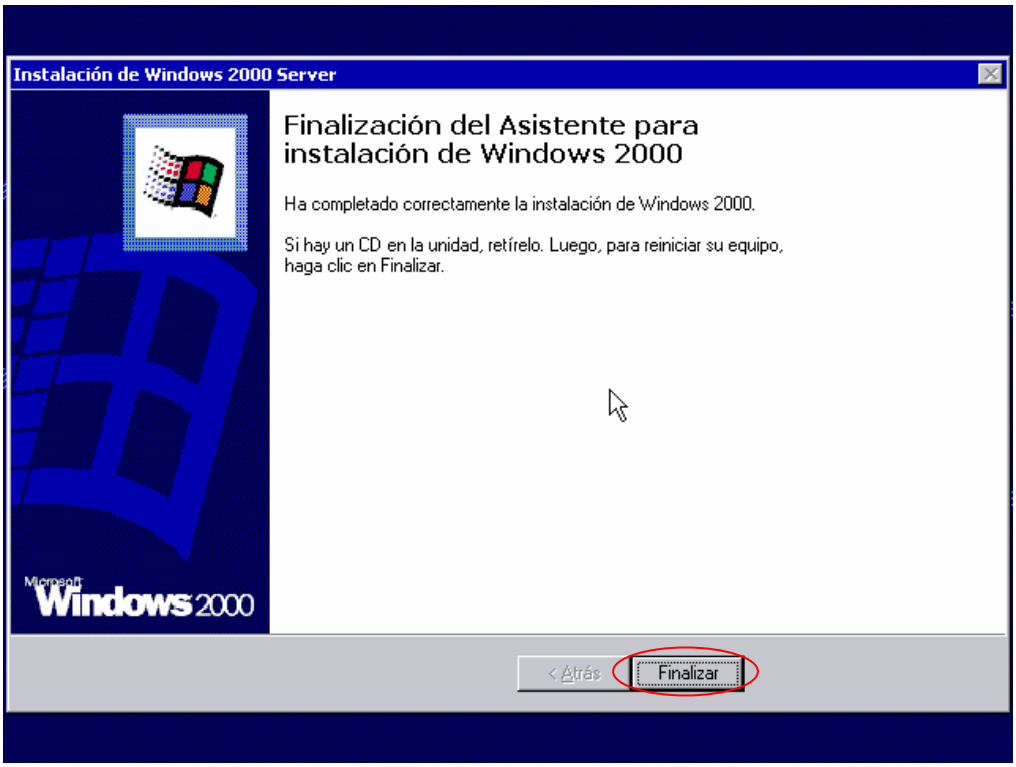
En la pantalla anterior muestra que esta instalando los componentes de Windows 2000® que elegimos, aquí esperaremos hasta que la barra se llene por completo, el tiempo variará dependiendo de las opciones seleccionadas y de nuestro hardware.



Al terminar aparecerá la siguiente pantalla.



En la pantalla anterior se realiza la última parte de la instalación y configuración, aquí también tendremos que esperar hasta que termine las tareas finales, es decir que instale los componentes del menú inicio, guarde la configuración y borre los archivos temporales de la instalación. Al terminar mostrará la siguiente pantalla.



Si hemos llegado a esta pantalla significa que hemos terminado correctamente la instalación de Windows 2000® Server. Quitamos el CD de la unidad damos clic en "***Finalizar***" y el equipo se reiniciará automáticamente.

Al reiniciar nuestro equipo deberá mostrar la siguiente pantalla que indica que está listo para iniciar sesión y seguir con el proceso de configuración de nuestro servidor.

2.2. Tareas previas antes de promover nuestro Servidor a Controlador de Dominio.

Antes de hacer la promoción de nuestro servidor se recomienda instalar el último Service Pack disponible así como los últimos hotfix, un antivirus para tener mayor seguridad ya que al promover nuestro servidor requerimos conectarlo a la red y puede ser muy vulnerable en ese momento. Para más información acerca de otras recomendaciones consultar el capítulo 4.

2.2.1. Verificando la versión del Service Pack.

Lo primero es iniciar sesión en nuestro servidor, para ésto presionamos ***CTRL+ALT+SUPR*** con lo que nos pedirá un usuario y su contraseña.

Una vez tecleados el usuario y contraseña damos clic en ***aceptar*** para iniciar sesión.

Una vez firmado en el Server podremos verificar que versión se tiene de service pack escribiendo en *Ejecutar* el comando "*winver*" y saldrá la siguiente ventana:

Como podemos observar en la parte donde aparece la versión también indica que tiene el Service Pack 4, que es el último disponible para Windows 2000®, si al hacer esta prueba encontramos que se tiene una versión anterior se debe proceder a actualizarla antes de continuar con el proceso. Se descarga del sitio de Microsoft y no tiene costo alguno. Para el caso de los hotfix se pueden verificar los instalados en el equipo en agregar o quitar programas.

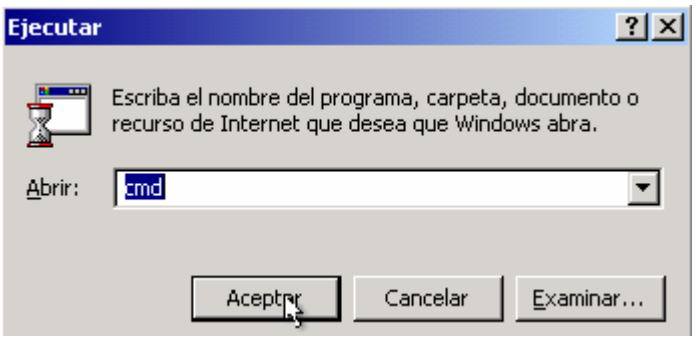
Se deberán instalar los hotfix disponibles para el sistema operativo ya sea que los descarguemos en otro equipo que cuente con conexión a Internet, antivirus, etc. Y posteriormente instalarlos en nuestro servidor o lo conectemos a una red segura. Al mismo tiempo es conveniente aplicar una plantilla de seguridad base, la cual nos ayudará a tener más seguridad sobre nuestro servidor, esta plantilla varía en cada organización y normalmente su finalidad es quitar servicios, renombrar o deshabilitar cuentas que no se requieren o configurar aquellos que serán requeridos.

2.3. Promoción de nuestro servidor a controlador de dominio y configuración del Servicio de nombres de dominio (DNS).

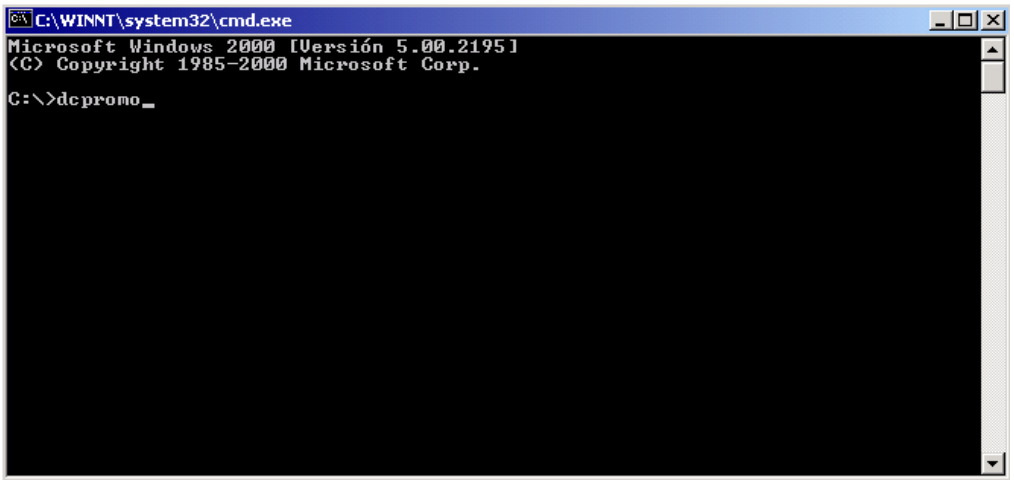
El siguiente paso es promover nuestro servidor a controlador de dominio (DC), el

procedimiento lo describiremos a continuación.

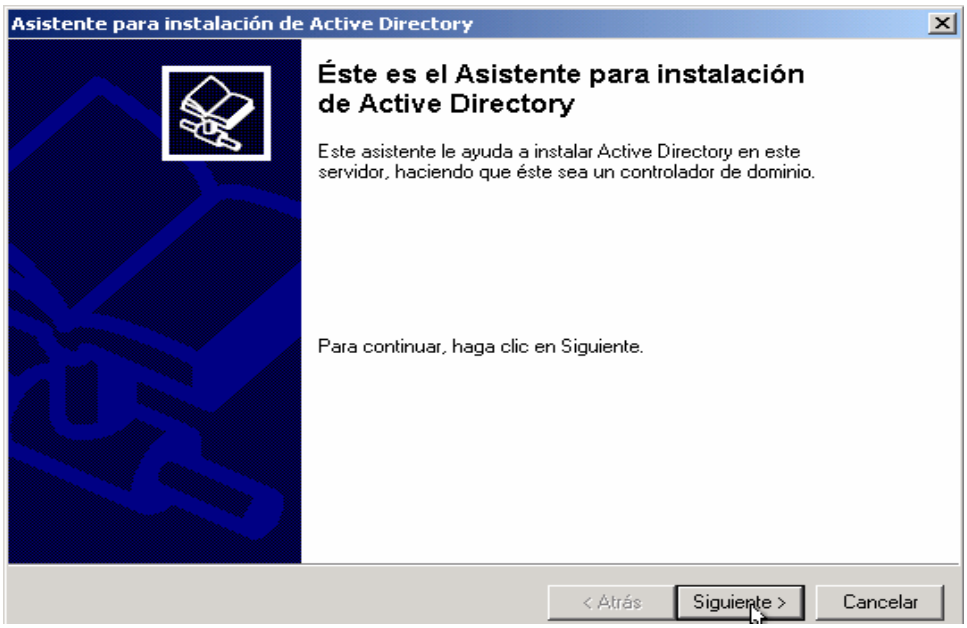
Lo primero es iniciar sesión en nuestro servidor con una cuenta con privilegios de administrador, después abrir una ventana de comandos, nos vamos a Inicio, Ejecutar, tecleamos "*cmd*" y damos clic en aceptar.



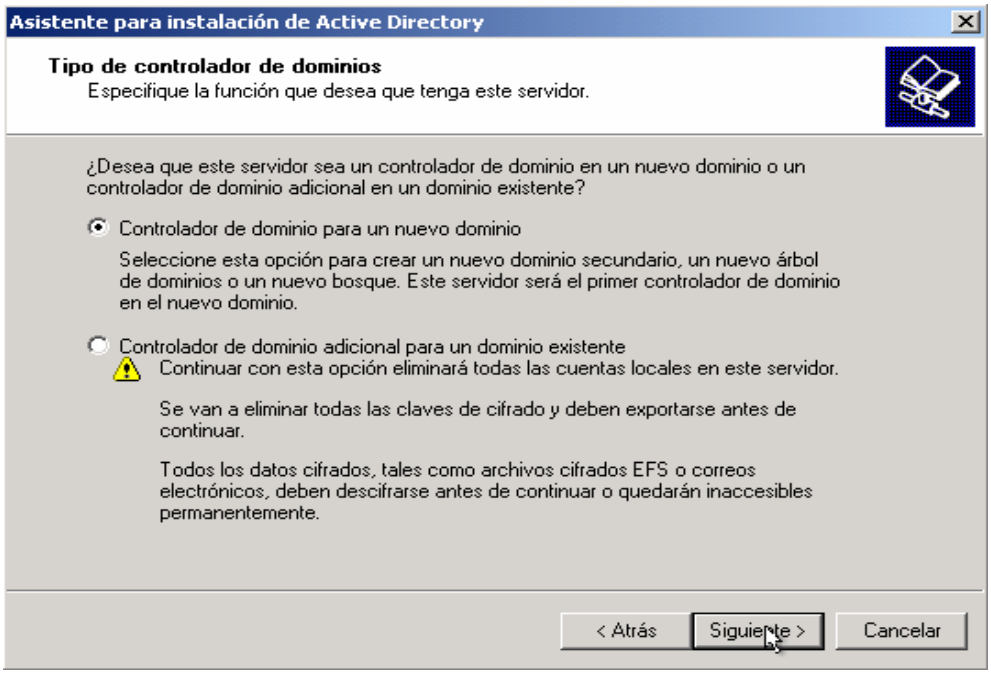
Posteriormente aparecerá una ventana similar a esta.



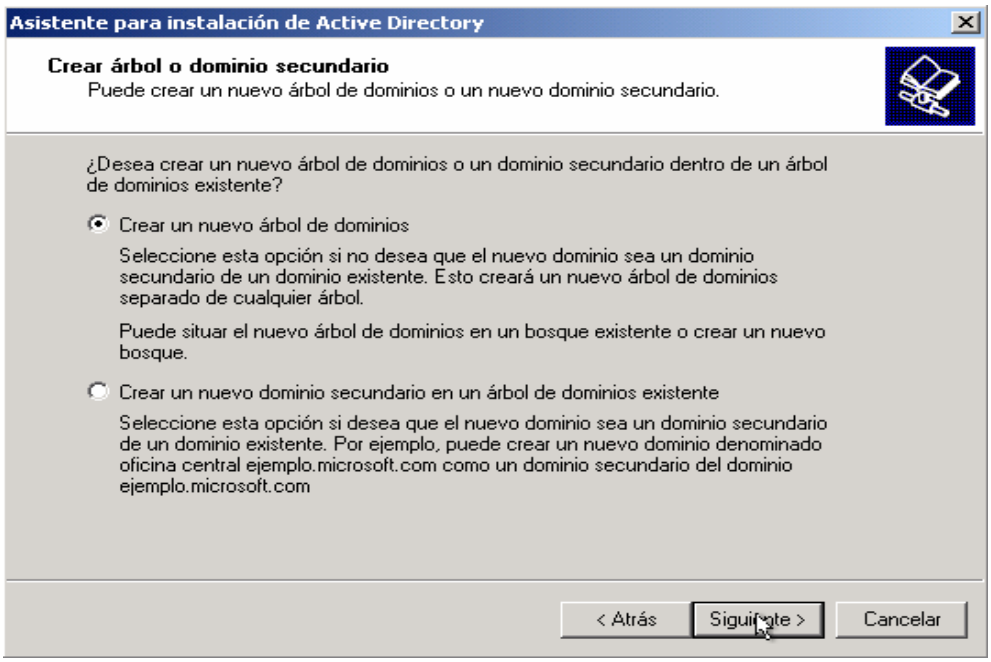
Ahí teclearemos el comando ***dcpromo*** y damos "*enter*". Aparecerá el asistente que nos guiará en el proceso de promoción de nuestro servidor a controlador de dominio (DC).



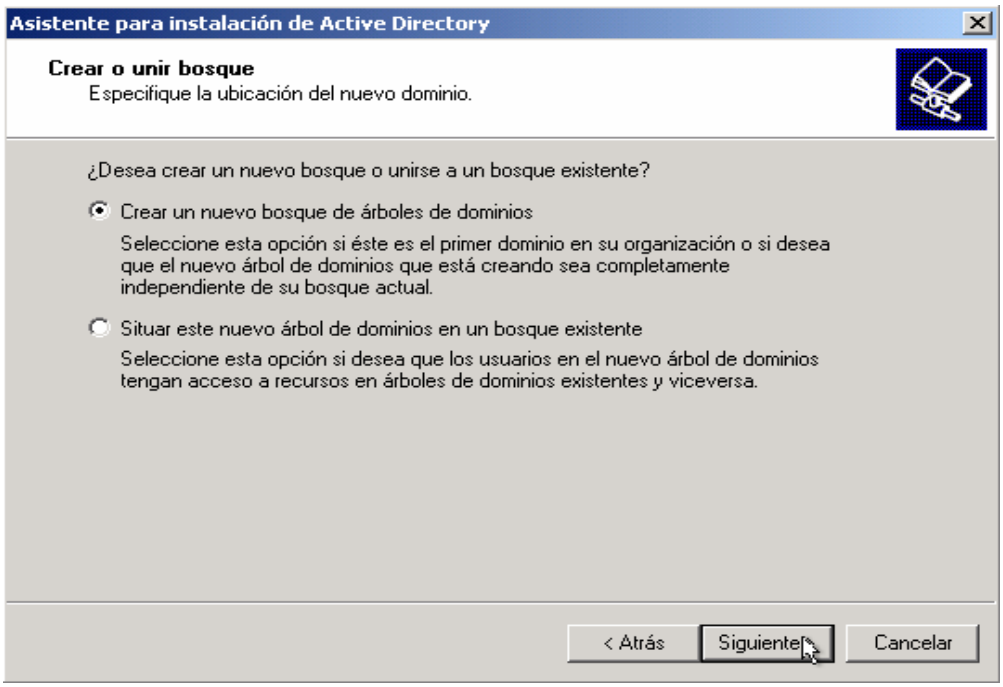
Damos clic en "***siguiente***" y aparecerá la siguiente ventana.



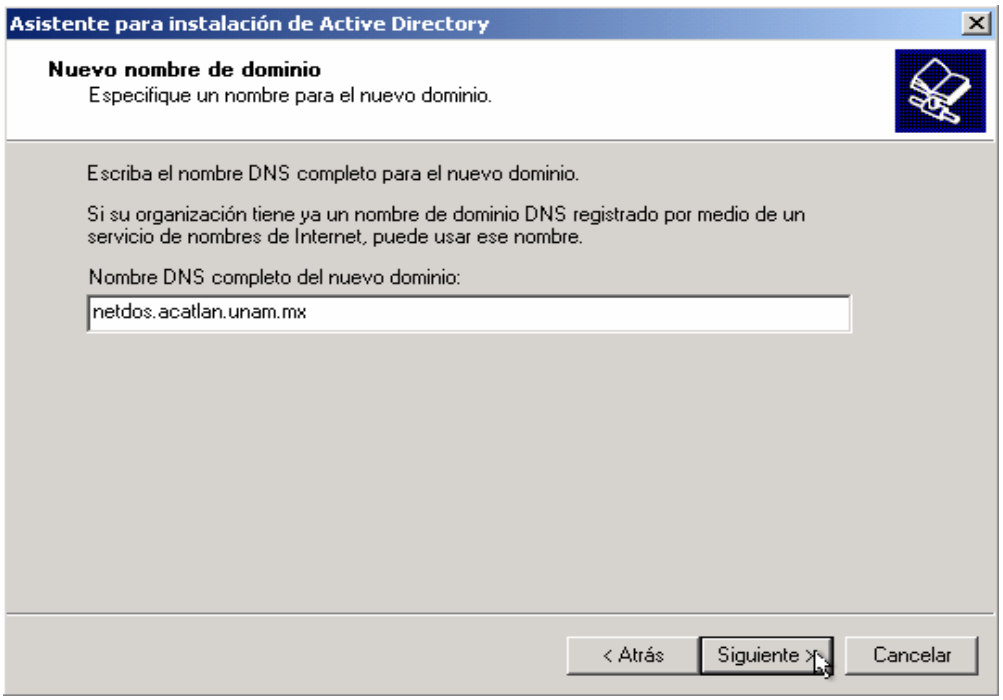
Aquí seleccionamos la primera opción "*controlador de dominio para un nuevo dominio*" y damos clic en ***siguiente*** y con lo cual aparecerá la siguiente ventana.



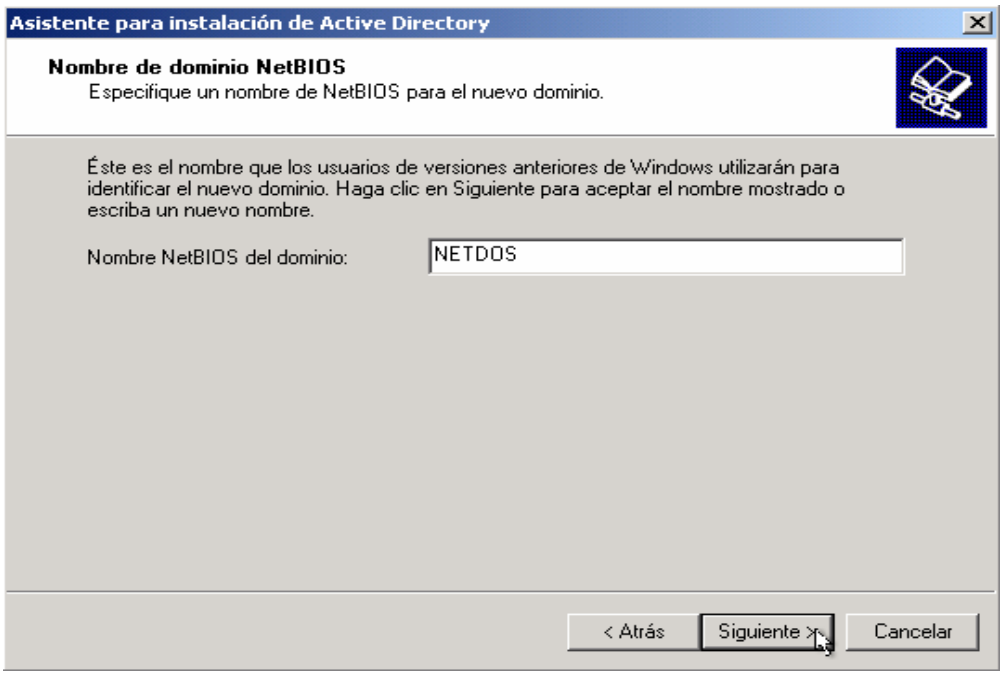
En esta ventana nuevamente seleccionamos la primera opción "*Crear un nuevo árbol de dominios*", damos clic en ***siguiente*** y aparecerá la siguiente ventana.



Nuevamente seleccionamos la primera opción "*Crear un nuevo bosque de árboles de dominio*", damos clic en ***siguiente*** y aparecerá la siguiente ventana.

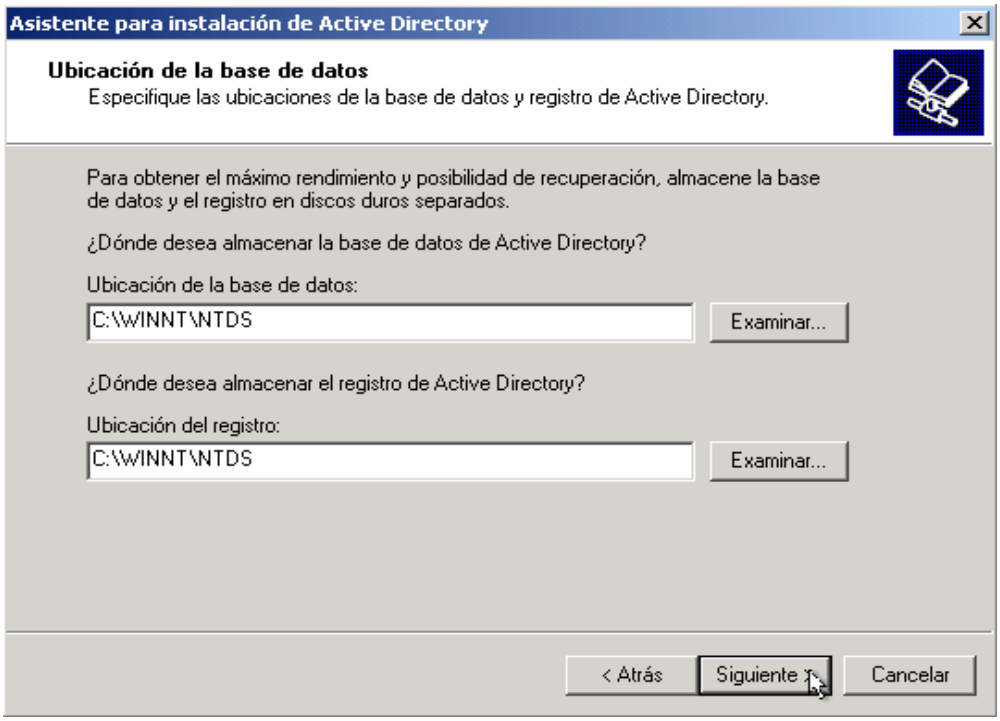


En esta pantalla escribiremos el nombre DNS completo del nuevo dominio, una vez escrito damos clic en "***siguiente***" y aparecerá la siguiente pantalla.

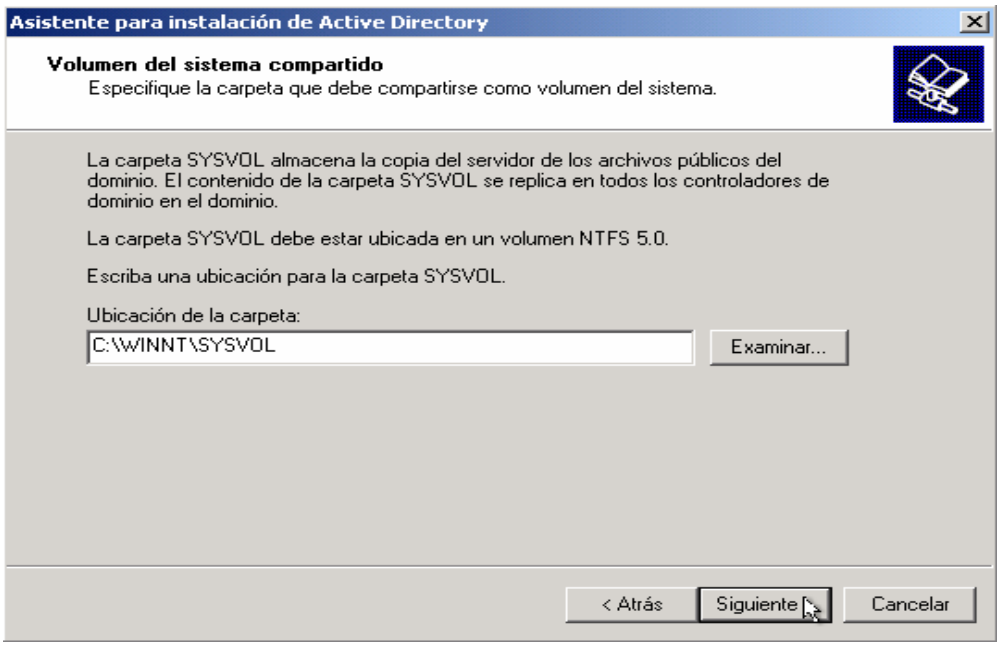


En esta pantalla nos pide el nombre NetBIOS del dominio, tecleamos el nombre y damos

clic en "***siguiente***" con lo que aparecerá la siguiente ventana.

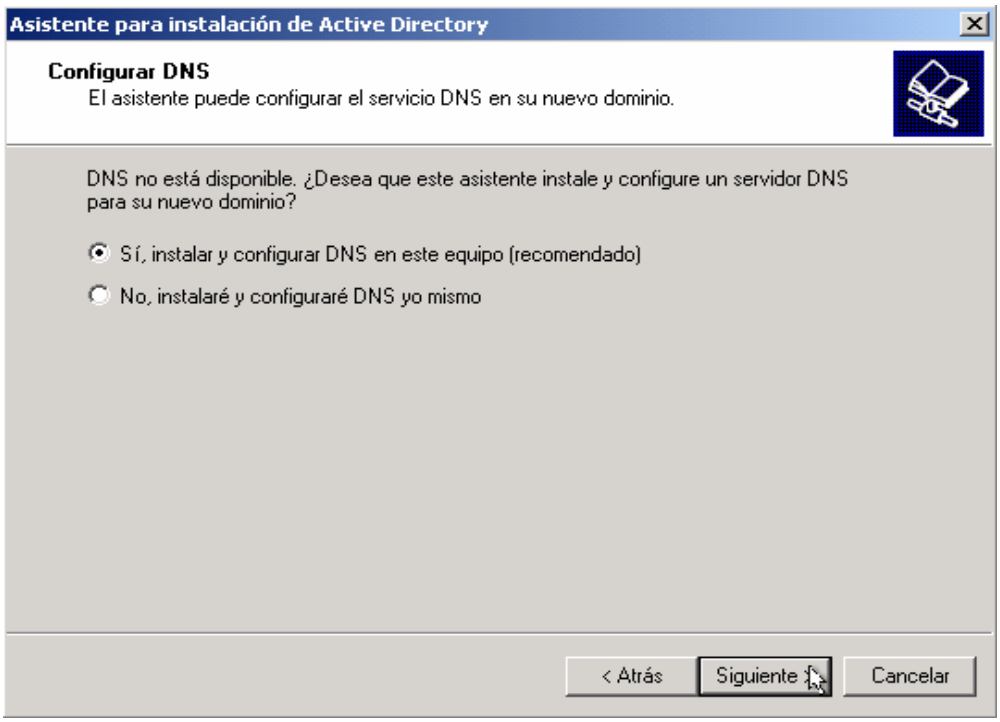


En esta pantalla podemos elegir la ruta donde guardará la base de datos del Directorio Activo, dejamos las rutas propuestas, damos clic en ***siguiente*** y aparecerá la siguiente ventana.

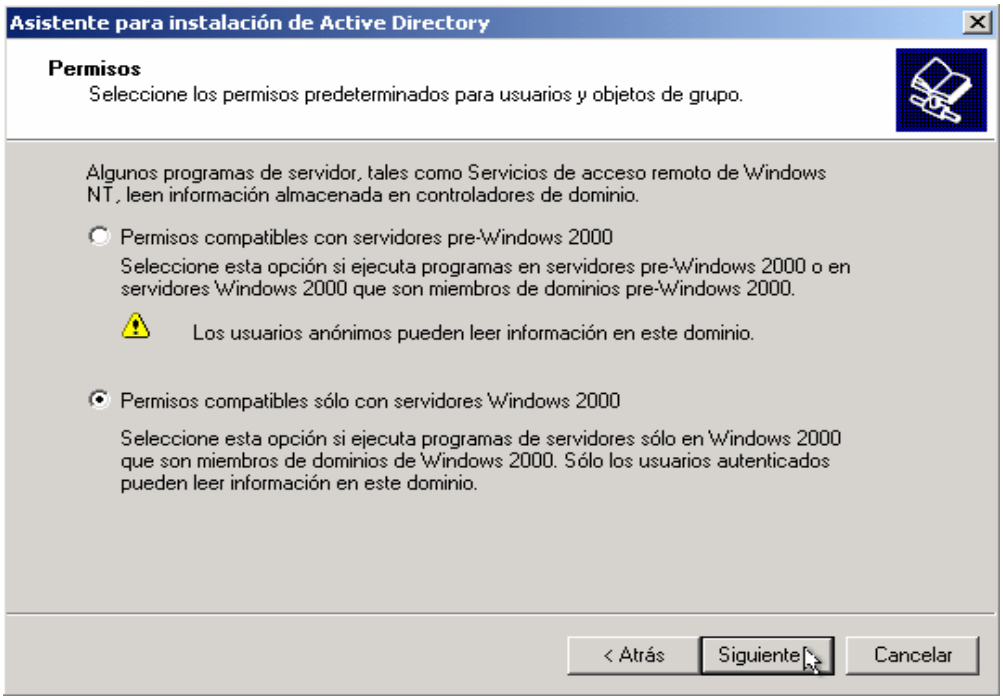


En esta ventana nos pide la ruta de la carpeta que se compartirá como volumen del sistema, dejamos la ruta propuesta, damos clic en "***siguiente***" y aparecerá esta ventana.

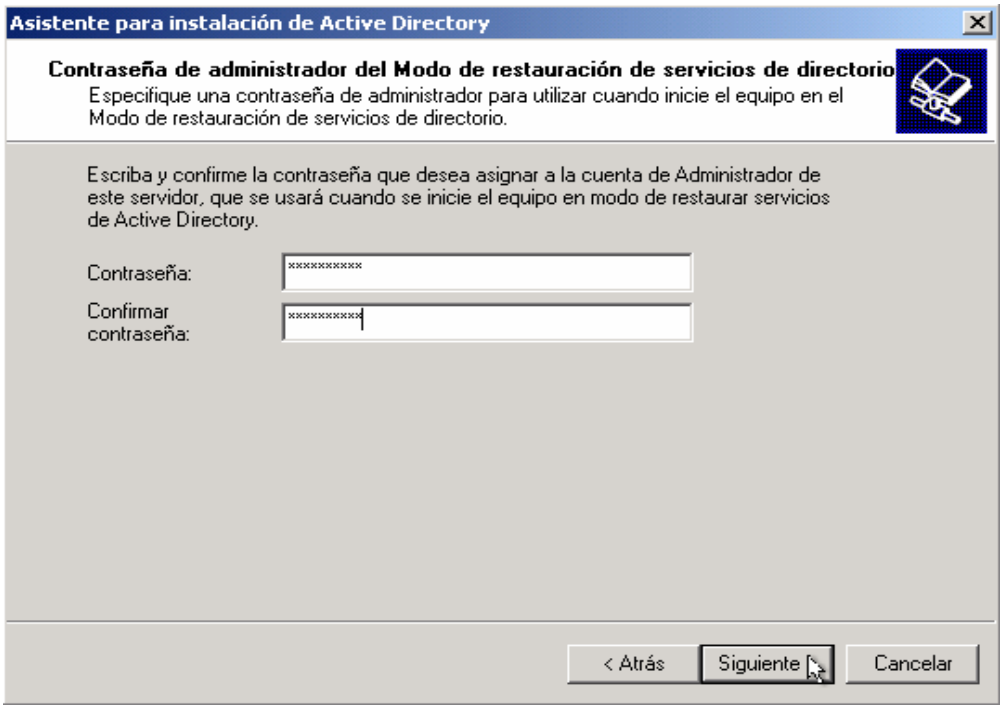
El mensaje que estamos viendo se debe a que aún no tenemos configurado nuestro Servidor de Nombres de Dominio (DNS). Damos clic en "***aceptar***" y aparecerá la siguiente ventana donde lo instalaremos y configuraremos.



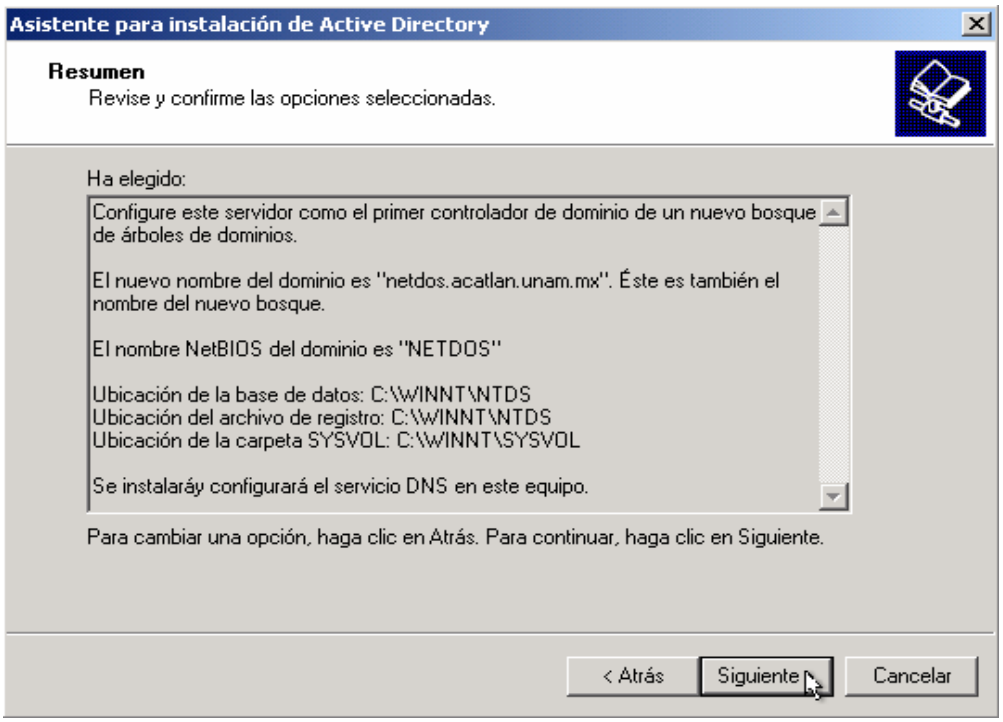
Aquí seleccionamos la primera opción *"instalar y configurar DNS en este equipo"*, damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



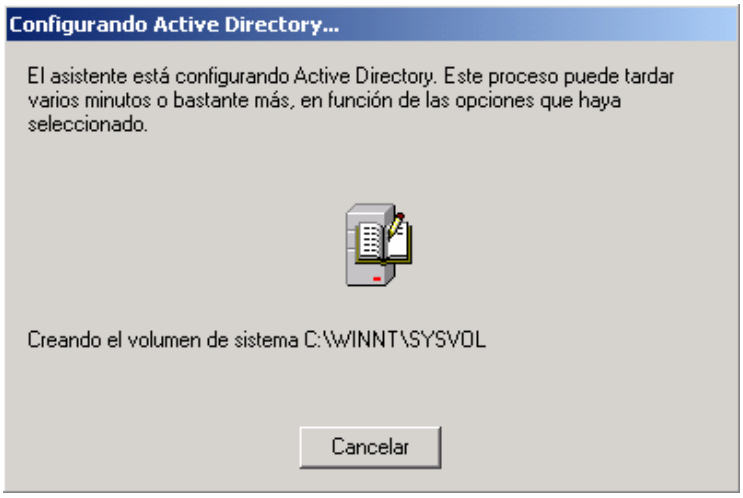
En esta ventana podemos seleccionar los permisos predeterminados, dado que nosotros no tenemos ningún Dominio en un ambiente anterior (NT), seleccionaremos la segunda opción *Permisos compatibles sólo con servidores Windows 2000.* Si requiriéramos compatibilidad con un Dominio que esté ejecutando Windows NT Server, tendríamos que seleccionar la primera opción. Damos clic en "***siguiente***" y aparecerá la siguiente ventana.



Aquí nos pide ingresar una contraseña para asignar a la cuenta de administrador del modo de restauración de servicios de Active Directory, esta sólo se pedirá cuando se entre en este modo. Se recomienda que sea una contraseña diferente a la del administrador. Damos clic en ***siguiente*** y aparecerá la esta pantalla.



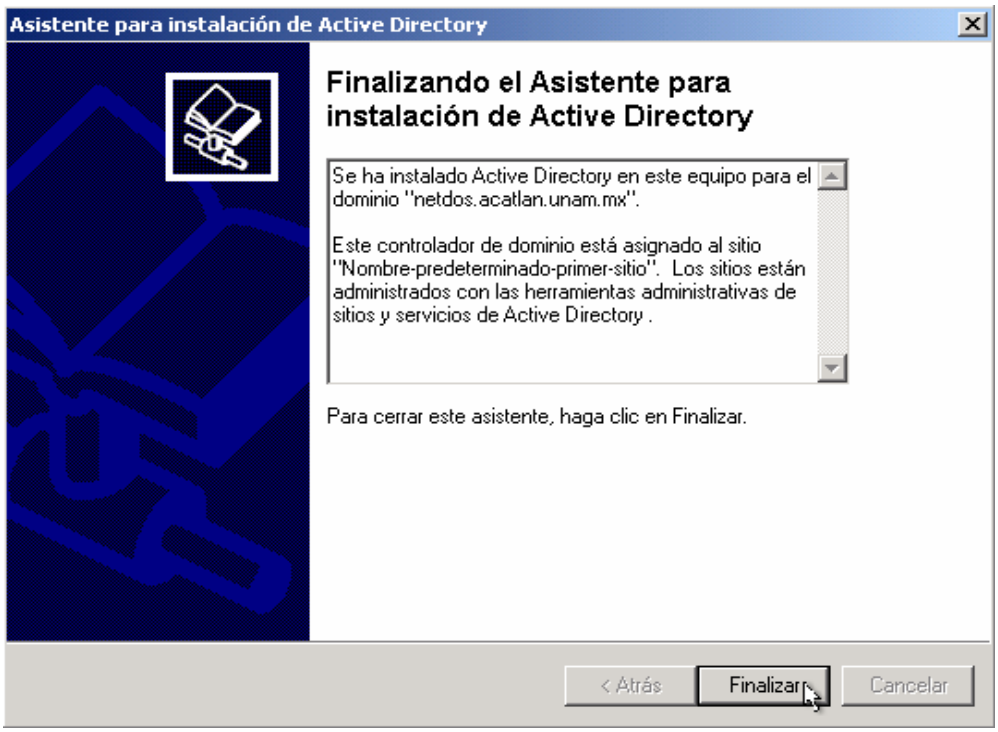
En esta ventana nos presenta un resumen de lo que hemos configurado anteriormente, revisamos para asegurarnos que éste todo correcto, si no lo estuviera, damos clic en **atrás** hasta la parte donde está el error lo corregimos y regresamos hasta esta ventana, damos clic en ***siguiente*** y observaremos la siguiente ventana.



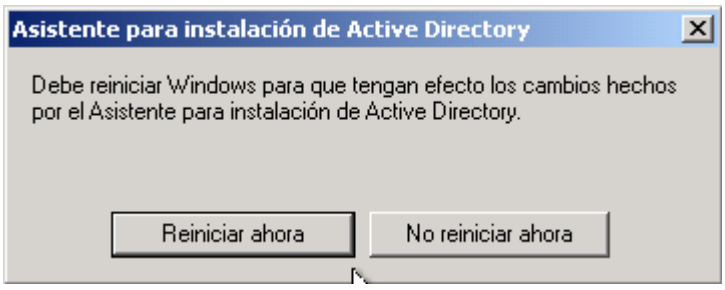
Aquí podemos observar que se está configurando el Active Directory tardará algún tiempo dependiendo de las opciones que se configuraron. Es necesario tener el CD de Windows 2000® Server para la instalación del DNS de lo contrario saldrá una ventana

requiriendo el CD.

Posteriormente aparecerá la siguiente pantalla.



Si podemos ver esta ventana indica que se ha finalizado correctamente la instalación del Active Directory, damos clic en ***Finalizar*** y aparecerá esta ventana.



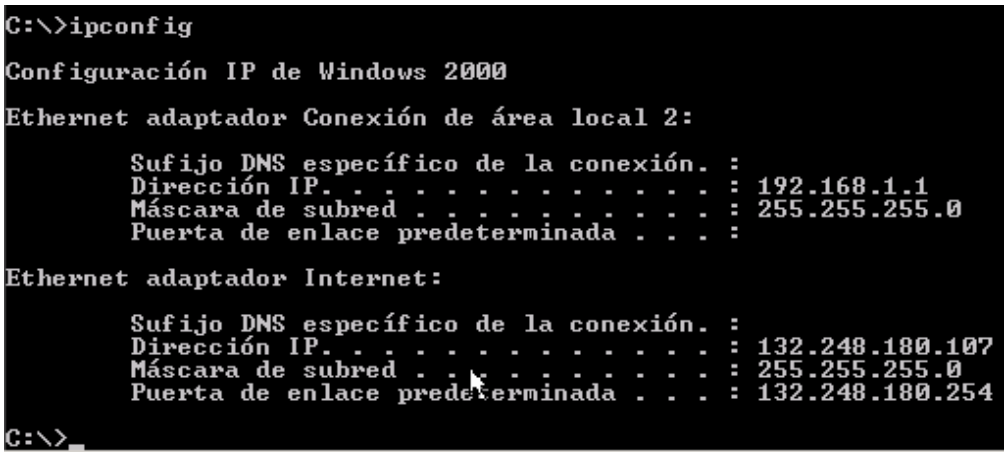
Damos clic en "***Reiniciar ahora***" y listo. Hemos terminado de promover nuestro servidor a Controlador de Dominio de forma satisfactoria.

El siguiente paso será empezar a configurar los servicios que necesitamos para el adecuado funcionamiento de la red.

CAPÍTULO 3. CONFIGURACIÓN DE DHCP Y NAT

Antes de proceder a describir las configuraciones del DHCP y NAT respectivamente se deberá instalar la segunda tarjeta de red en nuestro servidor que es necesaria para el servicio de NAT.

Una vez instalada la segunda tarjeta se le asignará una IP no homologada y como DNS primario tendrá la IP del DNS, el cual configuramos anteriormente. Podremos verificar esto ejecutando el comando *ipconfig* el cual mostrará los datos actuales en ambas tarjetas de red.

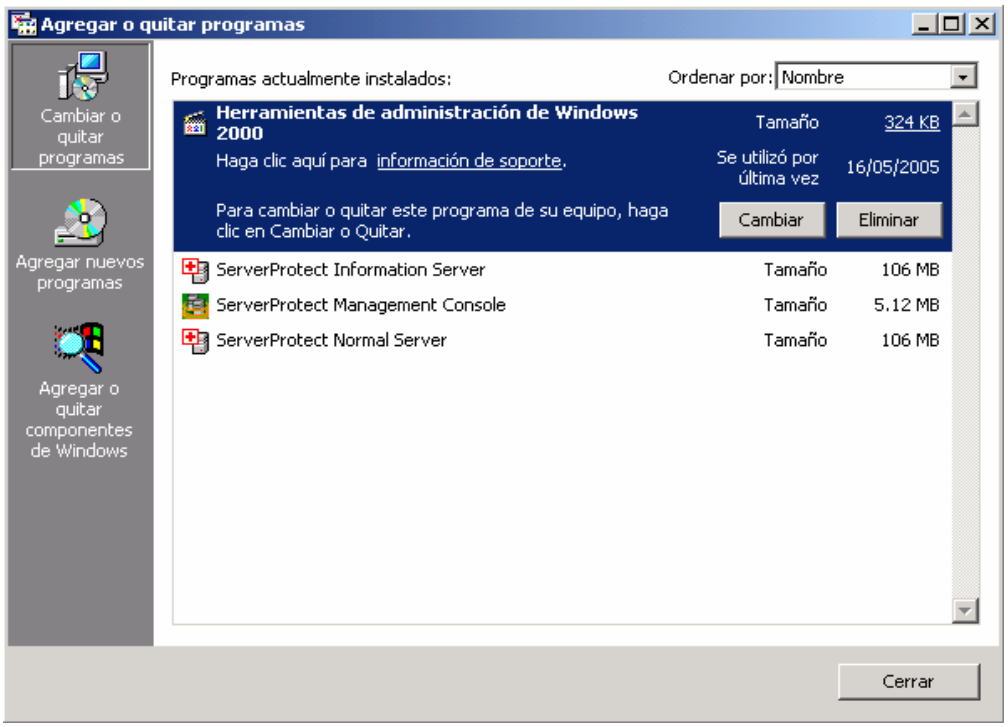


Como podemos ver en esta imagen se tiene dos tarjetas de red configuradas en el equipo.

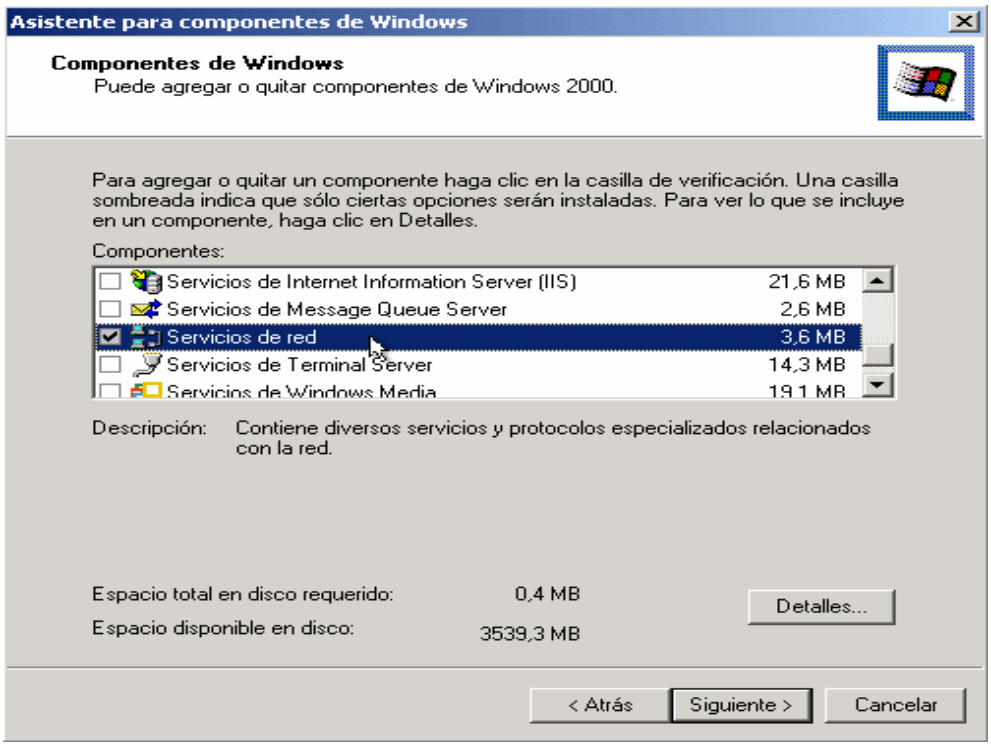
3.1. Instalación del servicio de DHCP

Describiremos los pasos necesarios para la instalación del servicio DHCP en nuestro servidor.

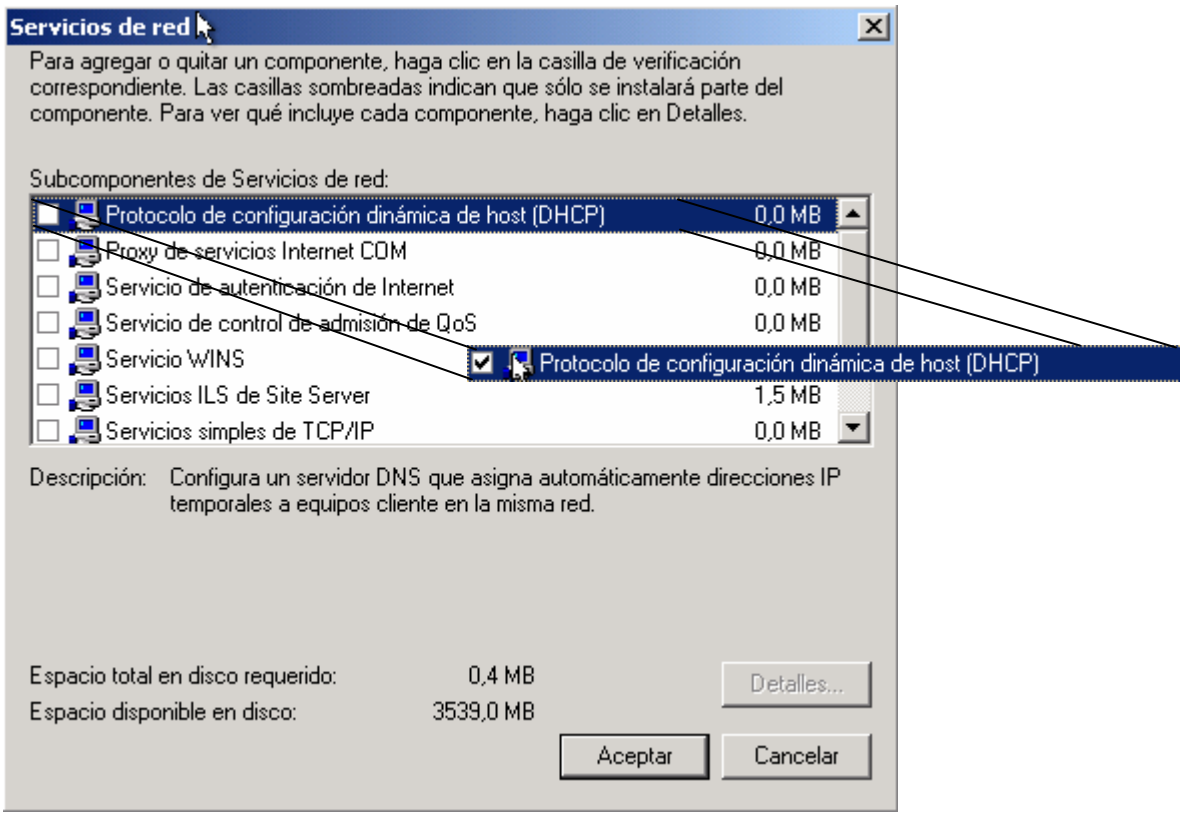
Primero iniciamos sesión con una cuenta con privilegios de administrador y abrimos *Panel de Control* damos clic en *Agregar o quitar programas* una vez hecho esto aparecerá la siguiente ventana.



En esta ventana damos clic en A*gregar o quitar componentes de Windows* con lo cual aparecerá la siguiente ventana:

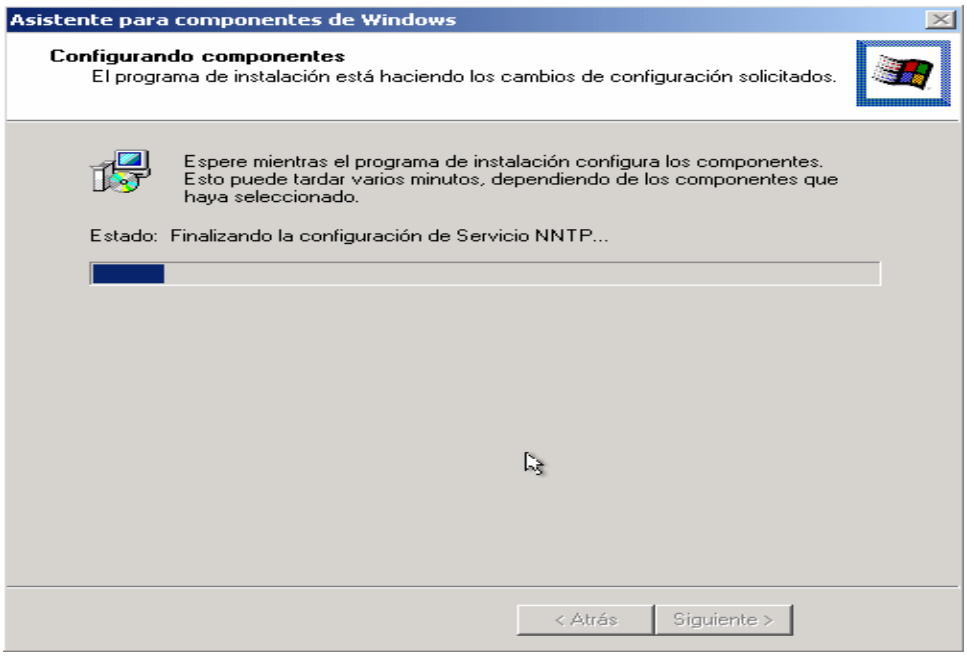


Una vez aquí nos desplazaremos hasta seleccionar "*Servicios de red*" damos clic en ***detalles***, con lo cual aparecerá una ventana similar a ésta.

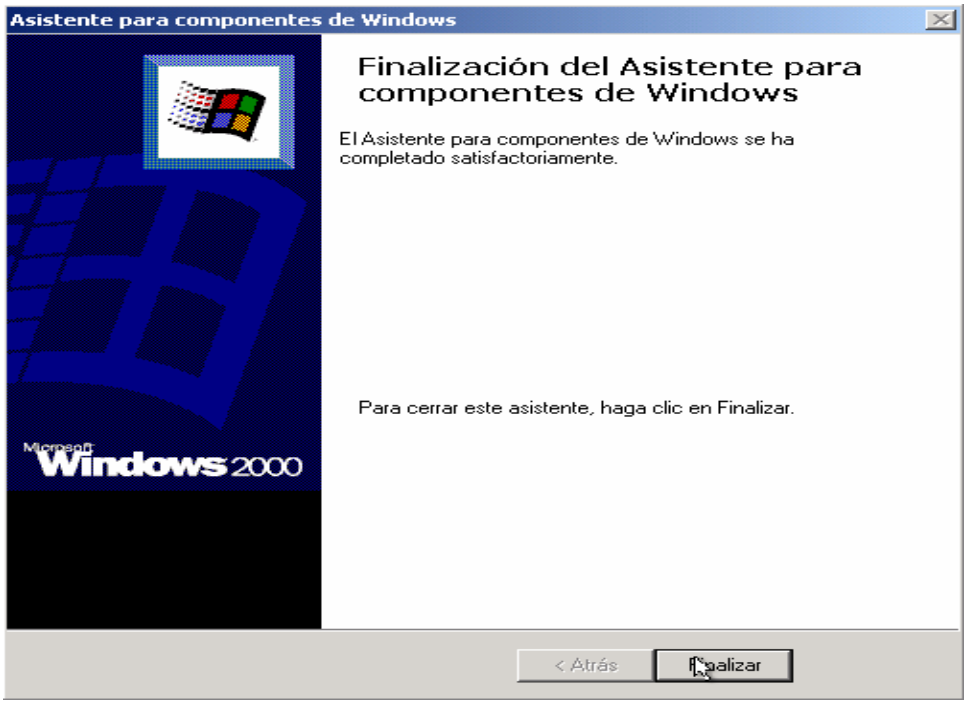


Aquí seleccionaremos la primera opción "*Protocolo de configuración dinámica de host (DHCP)*", marcamos el check box y damos clic en ***aceptar***.

Después de eso aparecerá la siguiente pantalla donde se está realizando la actualización de los componentes a instalar.



Al terminar aparecerá la siguiente pantalla.

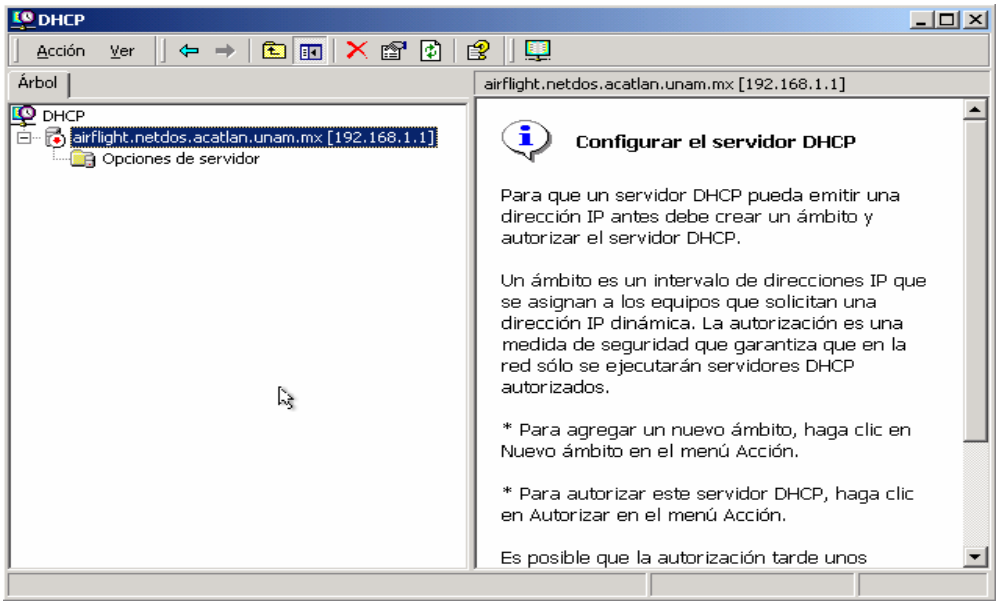


Esta pantalla indica que la instalación se ha finalizado exitosamente, damos clic en ***finalizar***.

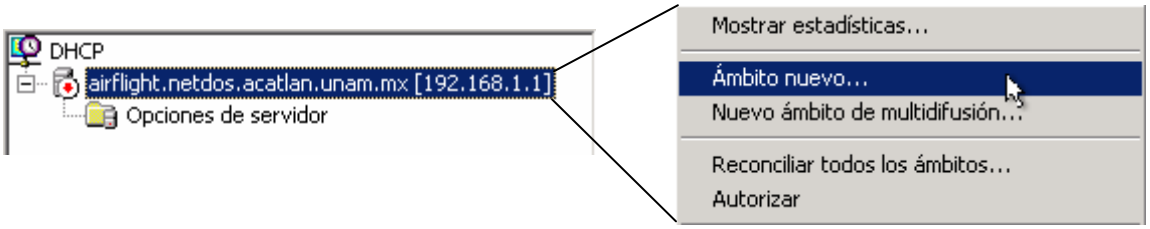
3.2. Configuración del Servicio de DHCP.

Ahora abrimos la consola del DHCP que se encuentra en *Inicio*, *Programas*, *Herramientas administrativas*, DHCP.

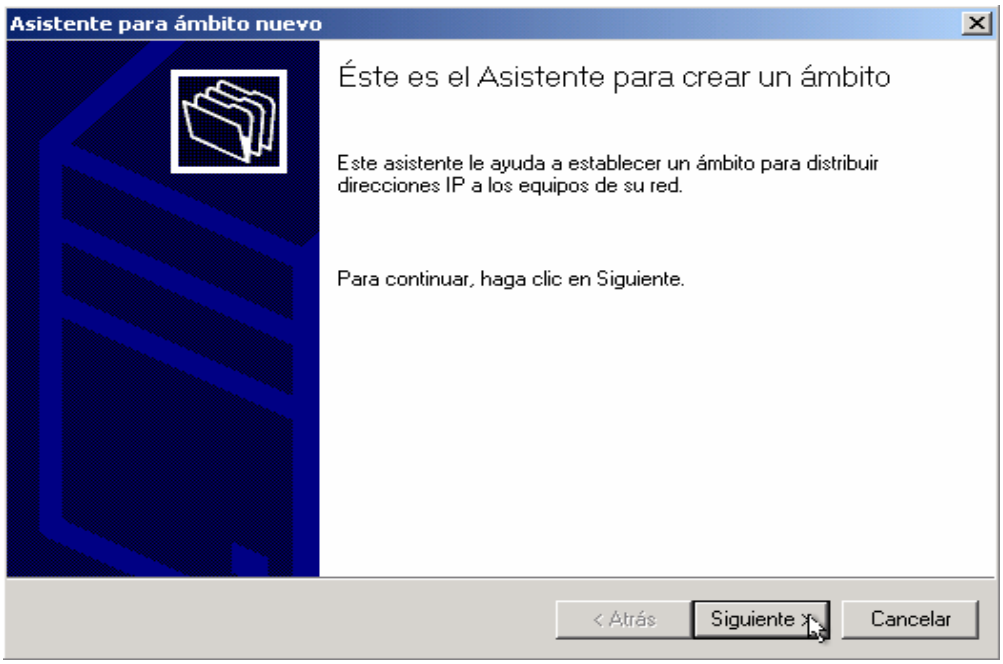
Y muestra la siguiente ventana que es la consola de administración del DHCP.



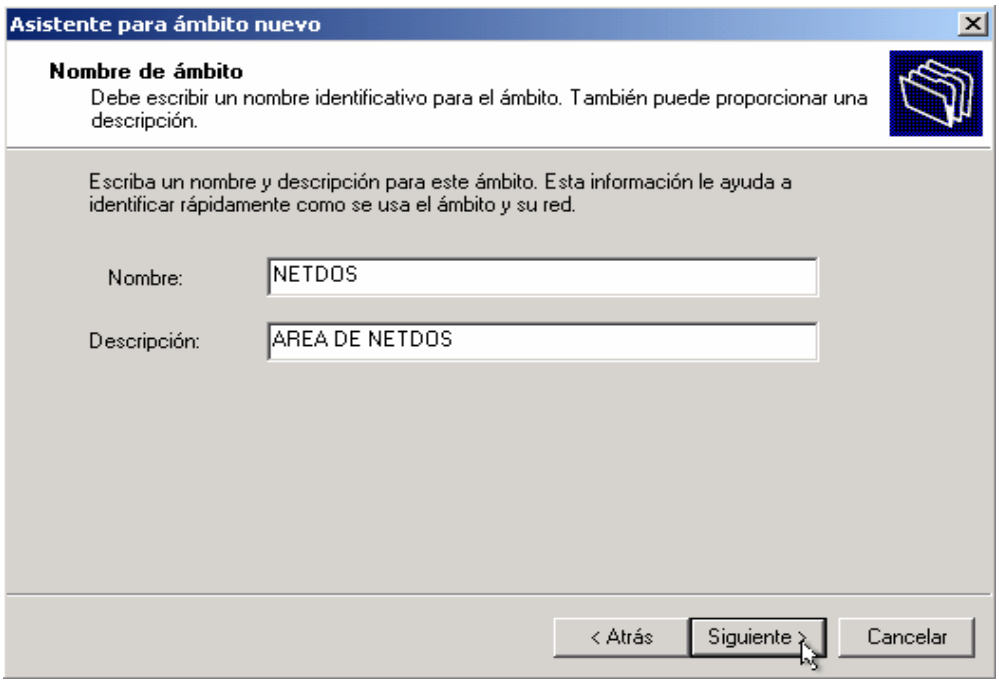
Una vez en la consola de administración crearemos un ámbito para asignar direcciones IP en nuestra red. En la consola seleccionamos el servidor y pulsamos botón derecho, saldrá un menú emergente y seleccionaremos *ámbito nuevo*.



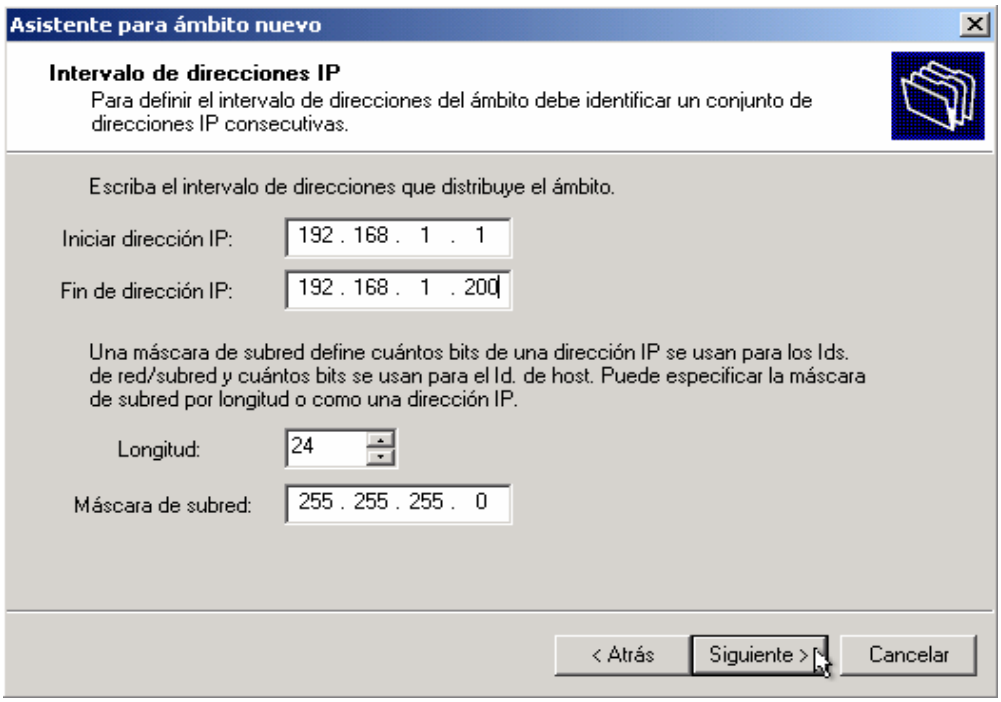
A continuación saldrá un asistente el cual nos guiara en el proceso de creación de nuestro ámbito.



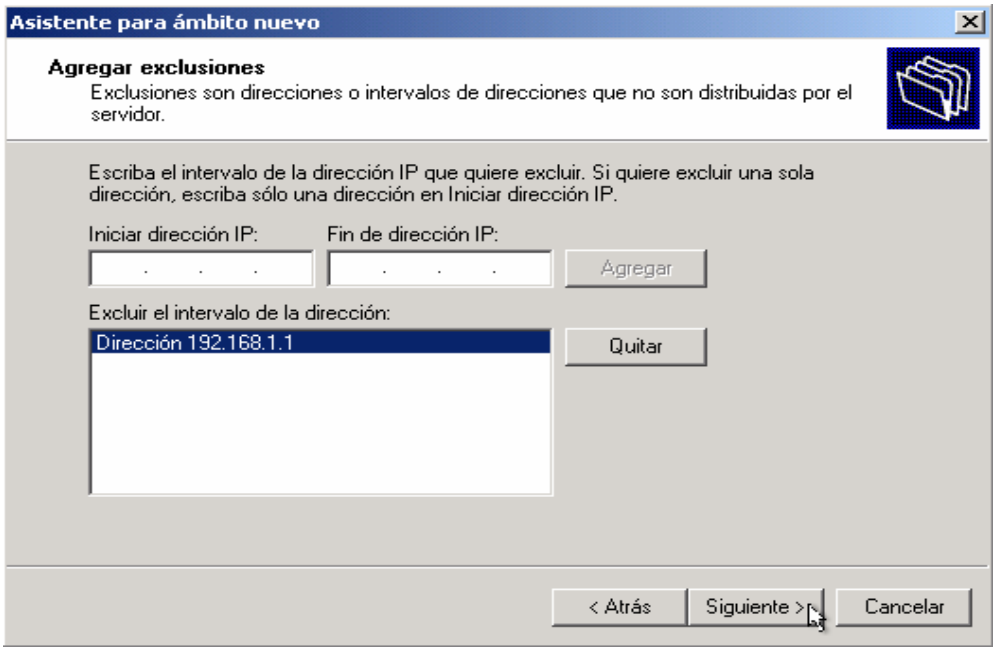
Una vez en el asistente damos clic en ***siguiente*** y aparecerá esta ventana.



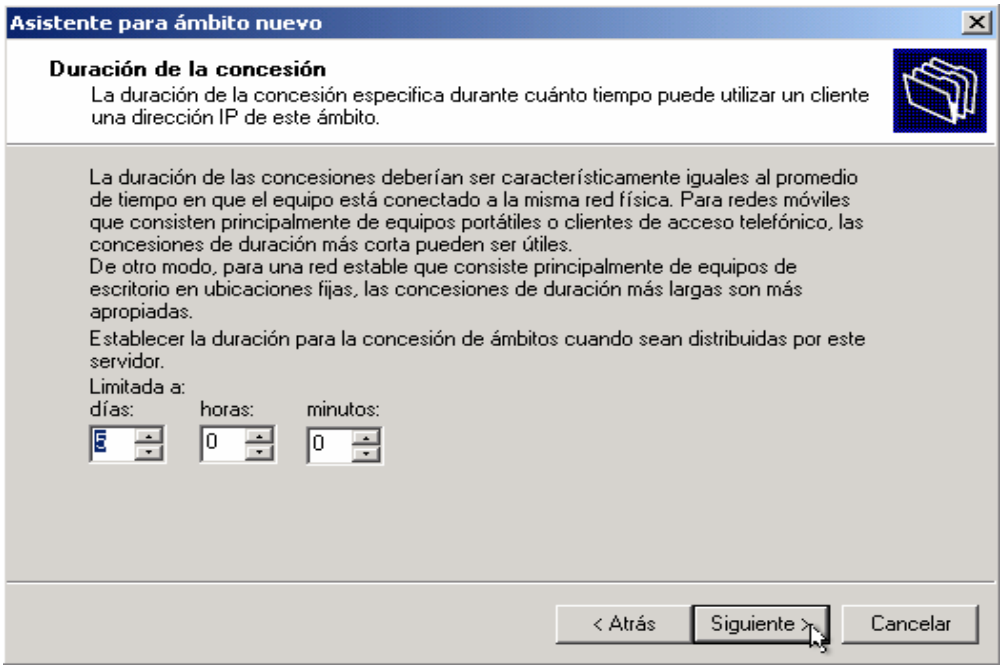
Aquí nos pedirá un nombre y una descripción de nuestro ámbito, esto es para identificarlo más rápido en caso de que sean más de uno los que creemos. Una vez llenado los campos requeridos damos clic en "***siguiente***" y aparecerá la siguiente ventana.



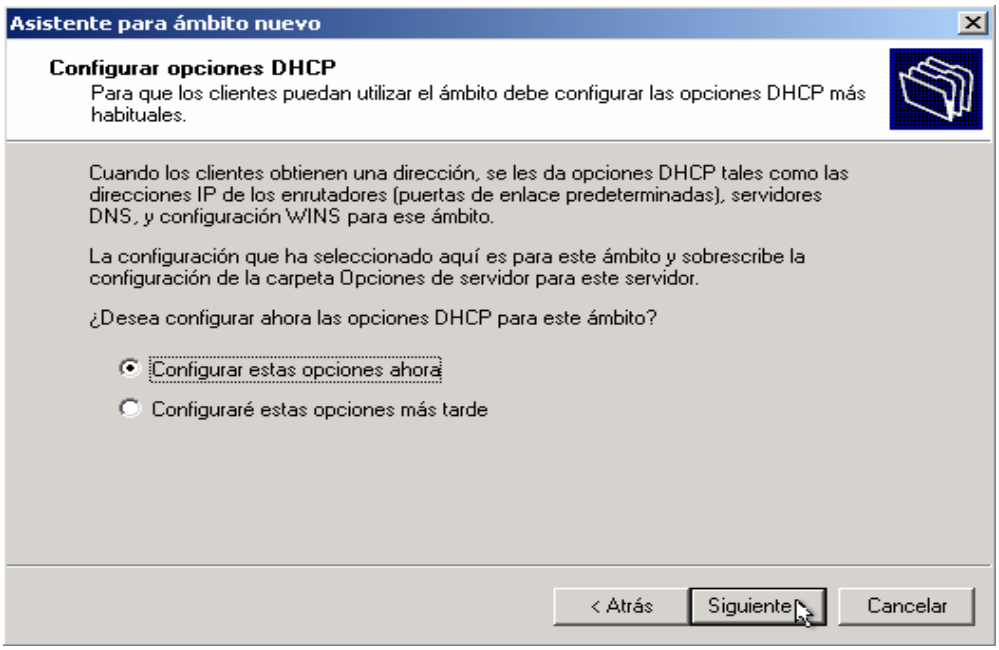
En esta pantalla nos pide definir el rango de direcciones IP que distribuirán en nuestro ámbito puede ser de cualquier clase sólo debe ser del mismo rango que la dirección IP no homologada actual de nuestro servidor. Al llenar el rango automáticamente asigna la máscara de red correspondiente, damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



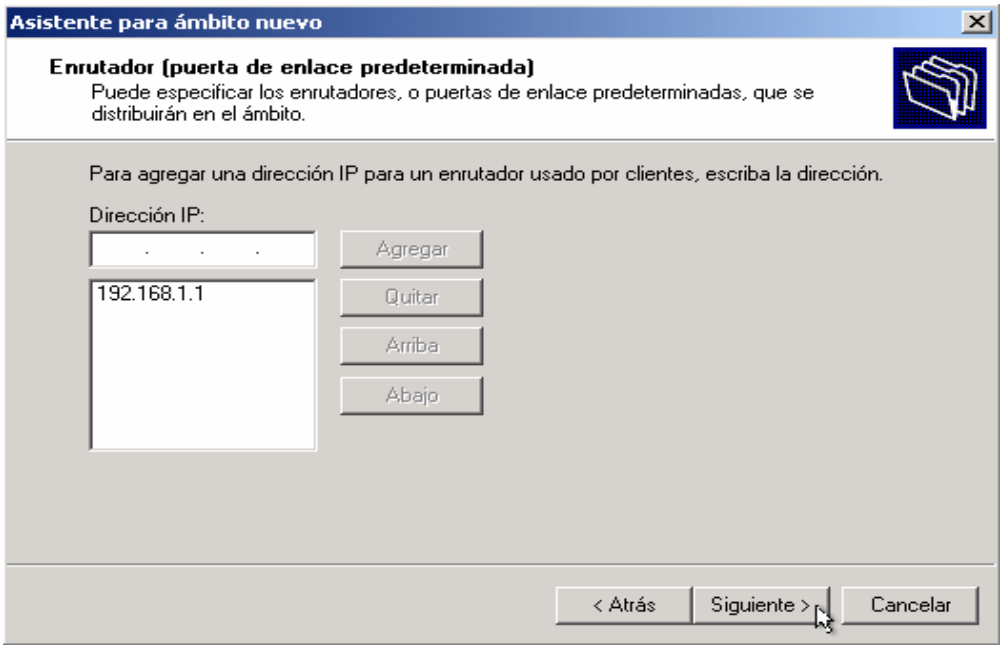
En esta pantalla ponemos las direcciones que queremos excluir o apartar a la hora de asignar las direcciones IP en los clientes, podemos poner una o un rango. En este caso sólo será una IP la que excluiremos, la agregamos, damos clic en ***siguiente*** y aparecerá la siguiente ventana.



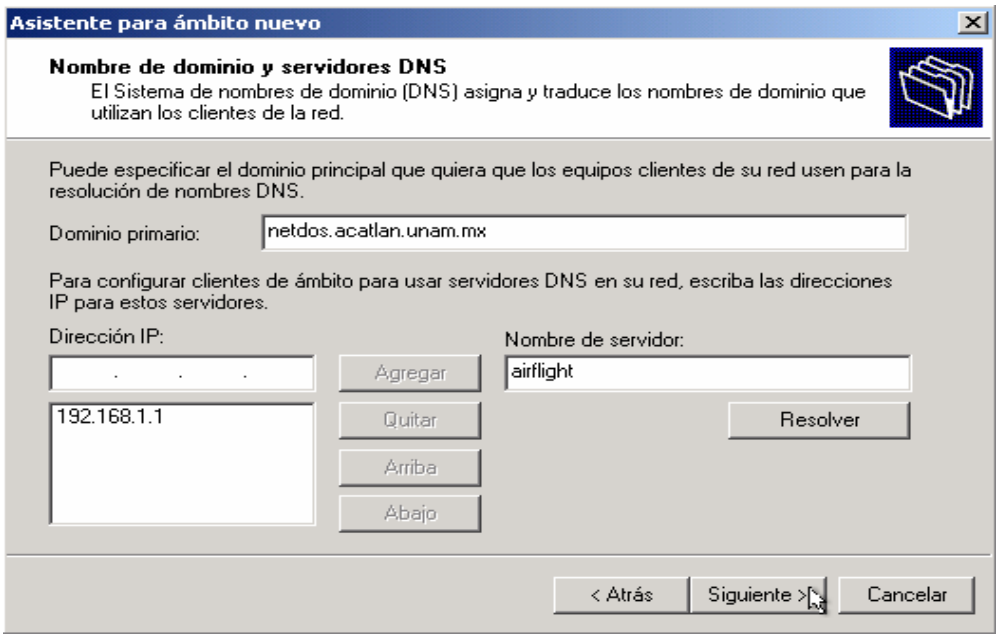
En esta pantalla se define el tiempo de vida que tendrá el préstamo de la dirección IP, el valor por *default* es de 8 días, para nuestro caso lo estableceremos en 5 días. Establecemos el valor, damos clic en ***siguiente*** y saldrá la siguiente ventana.



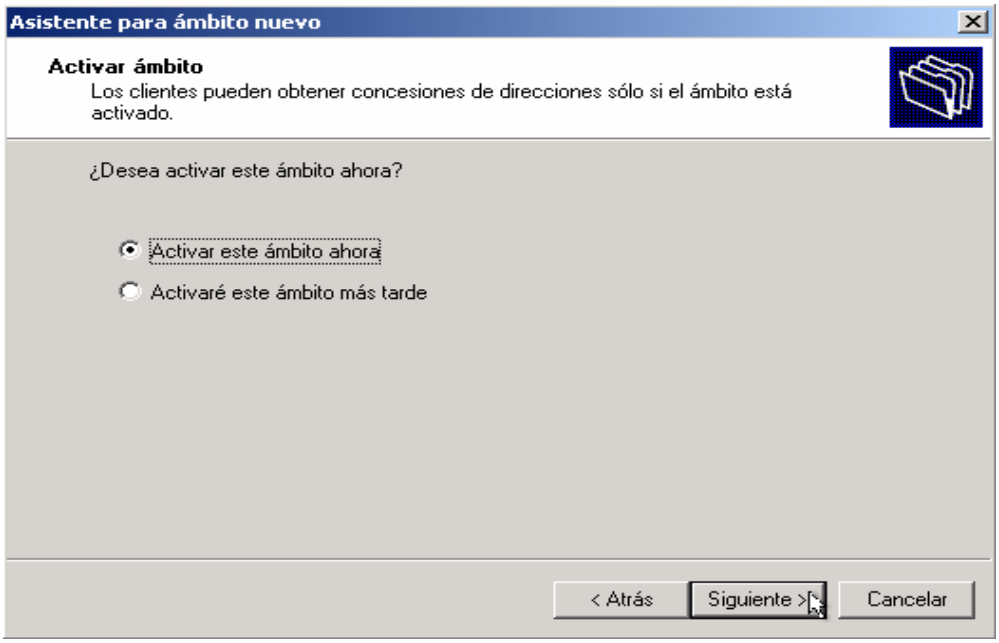
En esta pantalla nos pregunta si queremos configurar las opciones del DHCP como son DNS, puerta de enlace, etc. Para este caso seleccionamos la primera opción para definirlas, ahora mismo, presionamos ***siguiente*** y veremos la siguiente ventana.



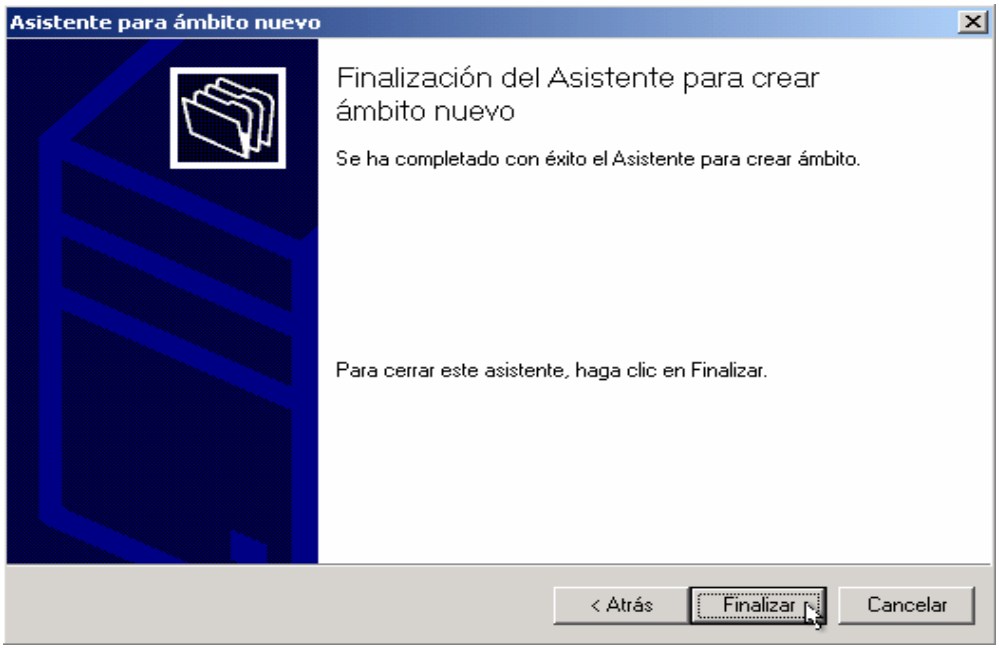
En esta pantalla estableceremos la puerta de enlace que va a tener nuestro ámbito, agregamos la IP, damos clic en ***siguiente*** y aparecerá la siguiente ventana.



En esta pantalla podemos establecer el dominio predeterminado que usen los clientes así como el servidor DNS que ocuparán para la resolución de nombres, agregamos los datos damos clic en "***siguiente***" y aparecerá la siguiente ventana.



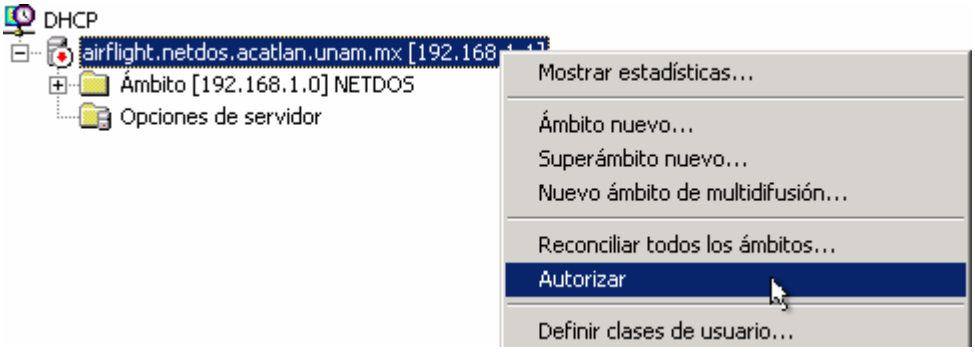
En esta pantalla nos pregunta si queremos activar nuestro ámbito ahora o después. Esto se aplica cuando no se van a usar de inmediato los ámbitos creados. Seleccionamos activar ahora, damos clic en ***siguiente*** y aparecerá la siguiente pantalla.



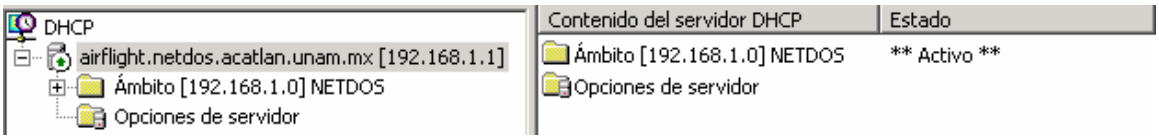
En esta pantalla nos indica que hemos terminado de configurar nuestro nuevo ámbito, en nuestro DHCP damos clic en ***finalizar*** para cerrar el asistente.

Hasta aquí hemos creado nuestro ámbito para que reparta direcciones IP a los clientes que lo soliciten, pero nos falta autorizar este servidor ya que de no hacerlo no podrá asignar las direcciones aunque esté bien configurado.

Para autorizar el servidor DHCP nos posicionamos sobre el servidor y pulsamos botón derecho y saldrá un menú emergente en el cual seleccionamos *Autorizar y listo.*

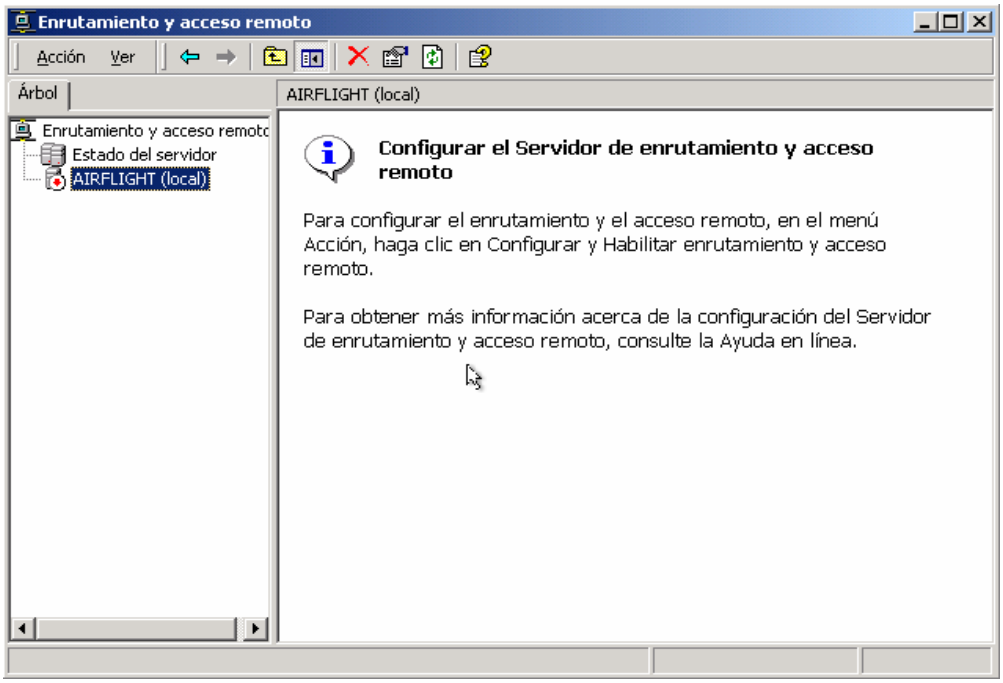


Una vez autorizado nuestro servidor DHCP se vera así y estará listo para asignar direcciones IP a los clientes que lo soliciten.



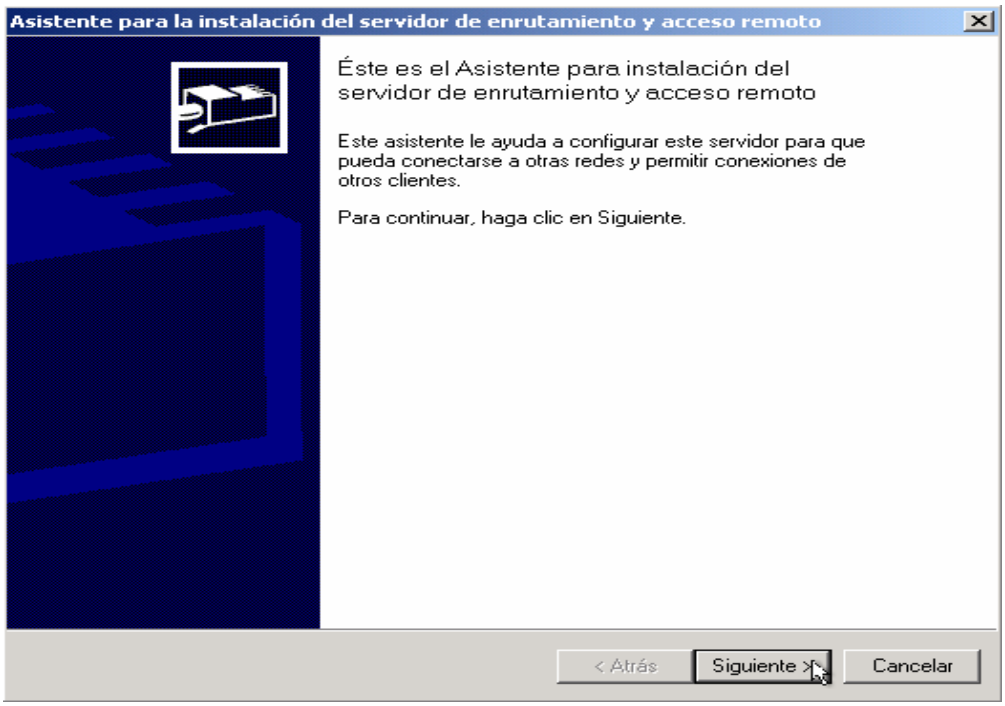
3.3. Configuración del Protocolo de enrutamiento Traducción de Direcciones de Red (NAT)

Primero abrimos la consola de Enrutamiento y Acceso Remoto (RRAS), esto desde Inicio, Programas, Herramientas Administrativas, Enrutamiento y Acceso Remoto.

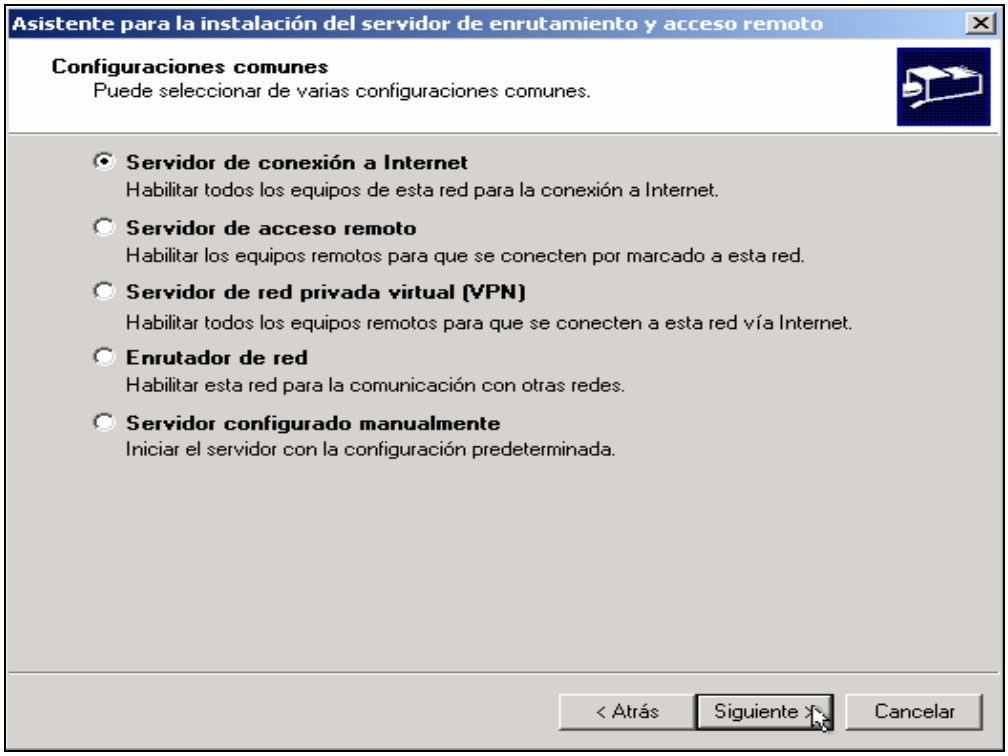


Una vez en la abierta la consola de administración nos posicionamos sobre el nombre del servidor damos clic con el botón secundario del Mouse, hecho esto aparecerá un menú emergente donde seleccionaremos la opción de *Configurar y habilitar el enrutamiento y acceso remoto*.

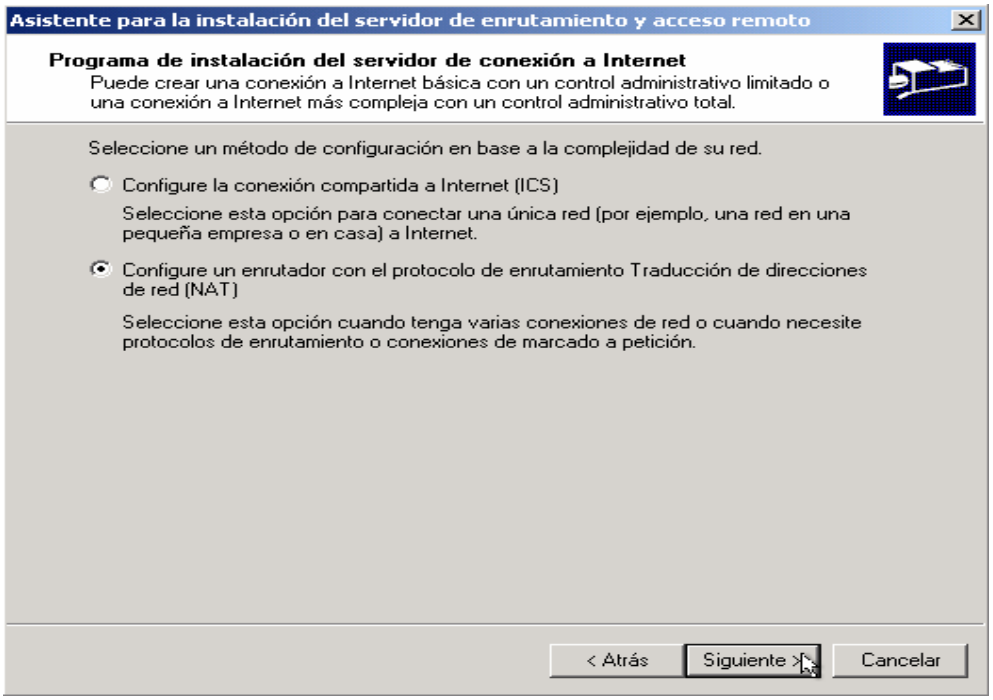
Una vez hecho esto, aparecerá el asistente que nos ayudará en el proceso de configuración.



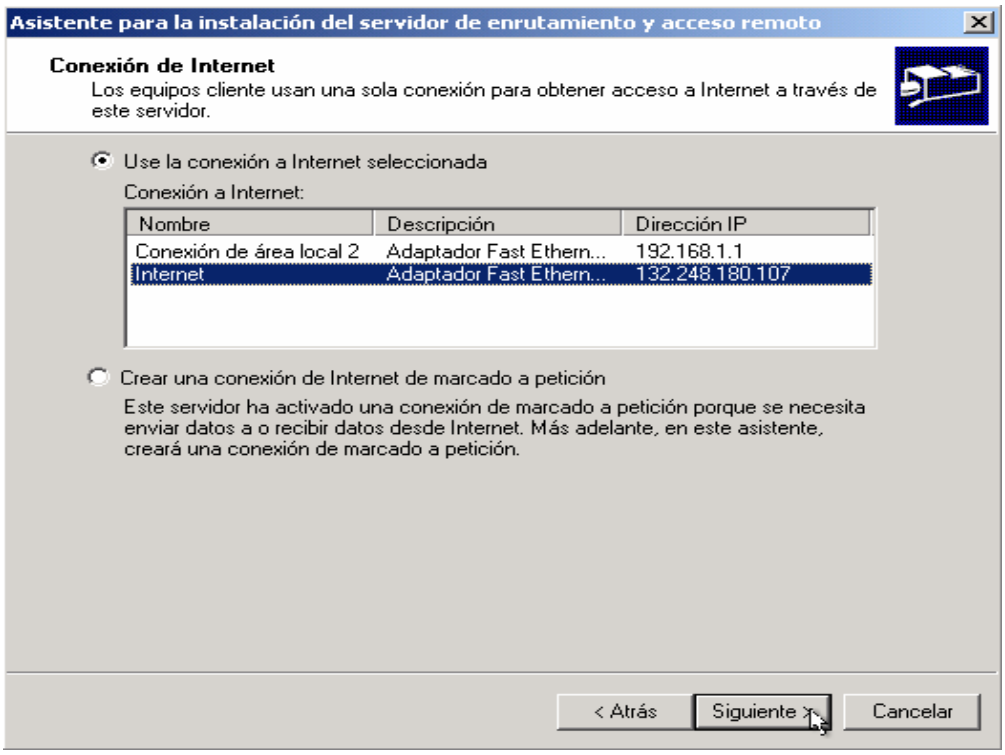
Esta pantalla observamos el asistente de configuración, damos clic en ***siguiente*** y aparecerá la siguiente ventana.



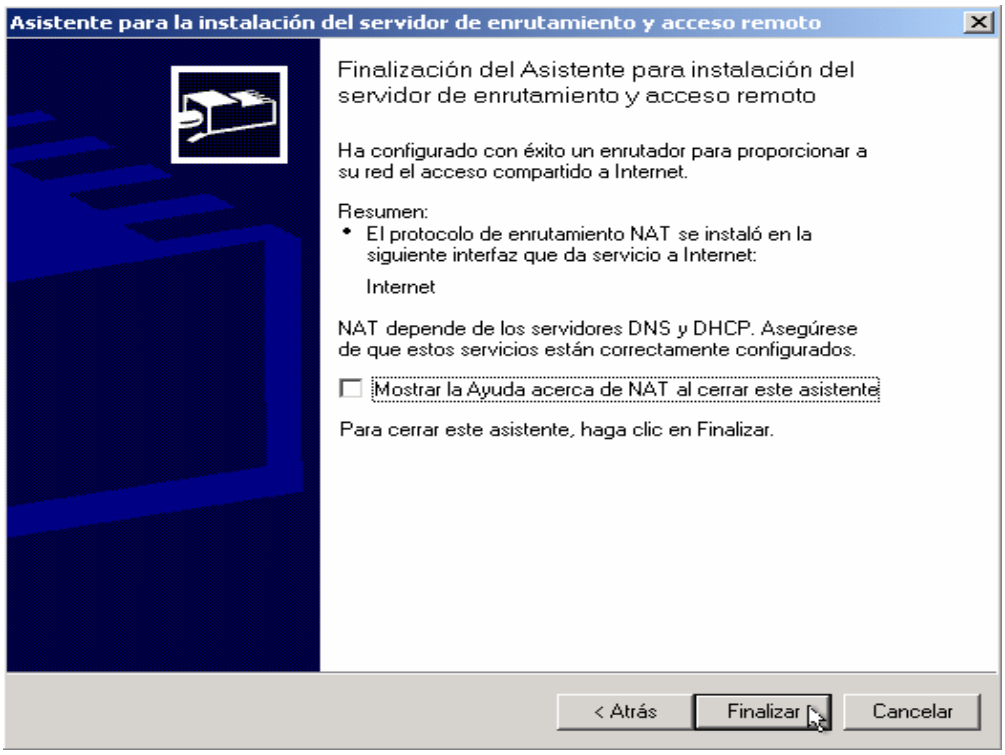
En esta pantalla seleccionamos la primera opción que necesitemos, para nuestro caso seleccionamos la primera *Servidor de conexión a Internet* damos clic en ***siguiente*** y aparecerá la siguiente ventana.



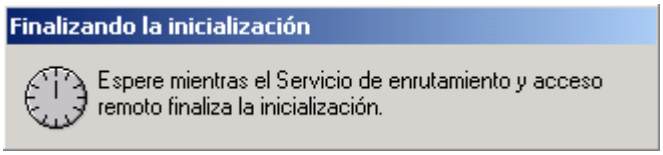
En esta pantalla seleccionamos la segunda opción (NAT), damos clic en ***siguiente*** y aparecerá la siguiente ventana.



Aquí seleccionamos la primera opción *Use la conexión a Internet Seleccionada* damos clic en ***siguiente*** y aparecerá la siguiente ventana.

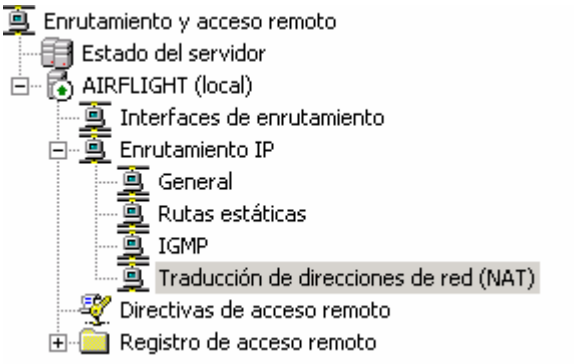


Esta pantalla indica que hemos finalizado con éxito la configuración del servidor de enrutamiento y acceso remoto con el protocolo de NAT, damos clic en **finalizar** y aparecerá esta ventana.



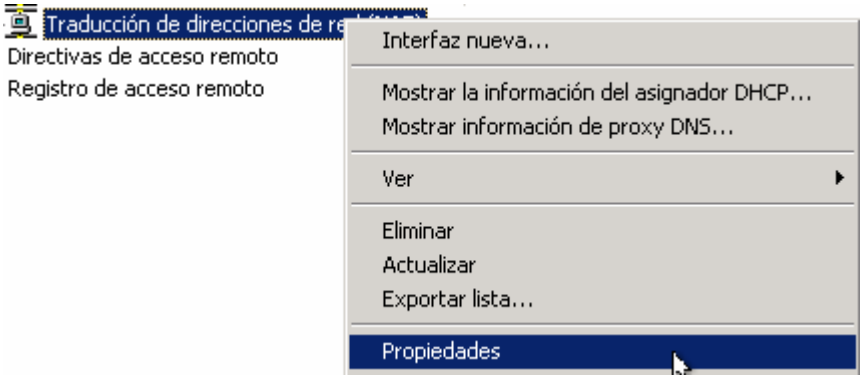
Esta ventana nos informa que se está inicializando el servicio de enrutamiento que hemos configurado previamente.

Una vez terminado este proceso regresamos a la consola de Enrutamiento y Acceso Remoto para terminar con la configuración.

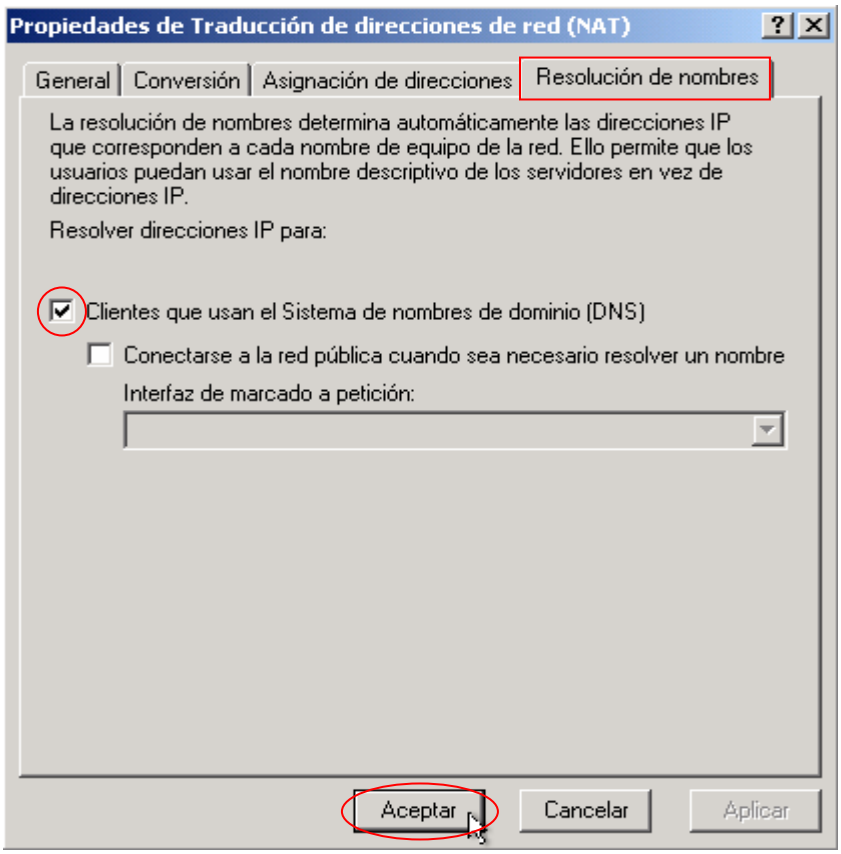


Como se observa en la imagen aparece NAT lo cual indica que se configuró e inicializó correctamente el servicio.

Ahora procederemos a configurar la resolución de nombres. Para ésto nos posicionamos sobre *Traducción de direcciones de red (NAT)* damos clic con el botón derecho para que aparezca el menú emergente y seleccionamos *"Propiedades"*, como se aprecia en la imagen siguiente.



Una vez hecho ésto aparecerá la siguiente pantalla.



Nos posicionamos en la pestaña de *Resolución de Nombres* marcaremos el check box *Clientes que usan el Sistema de nombres de dominio (DNS)*, damos clic en ***aceptar*** y nos regresará a la pantalla anterior. Con lo que hemos terminado de configurar nuestro servidor. Cerramos la consola de administración de de Enrutamiento y Acceso Remoto (RRAS) sólo falta configurar los clientes y a disfrutar de Internet.

Hasta ahora sólo hemos hablado y descrito la parte de las configuraciones del lado del servidor, pero también es necesario configurar nuestros clientes para que puedan usar lo que hemos hecho hasta ahora.

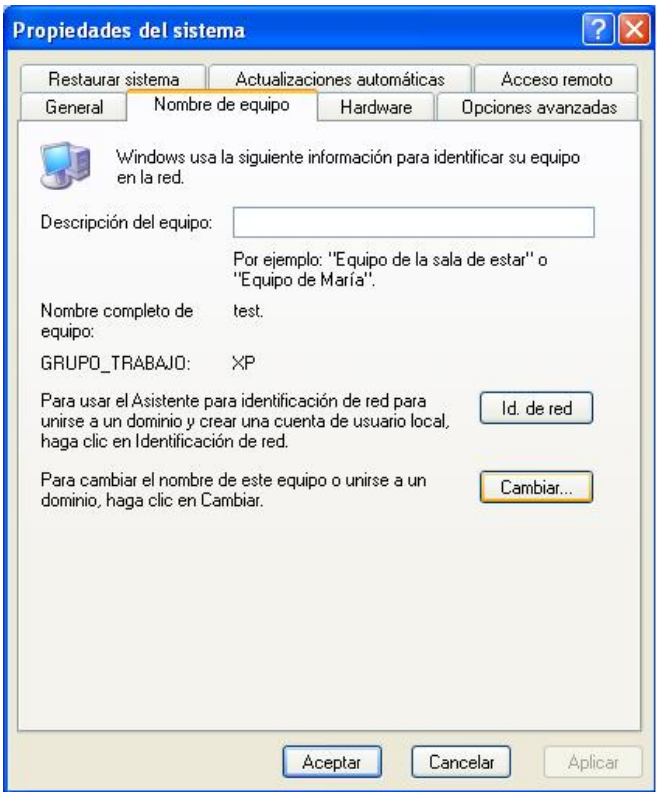
En este material no describiremos el procedimiento de instalación del Sistema Operativo Windows XP o 2000 Profesional en las estaciones de trabajo. Asumiremos que este proceso ya está realizado y sólo nos enfocaremos a la configuración de la tarjeta de red (NIC) para su correcto funcionamiento en nuestra red.

Así que una vez instalado el Sistema Operativo ya sea Microsoft Windows 2000® Profesional o Windows XP Profesional lo primero que se tiene que revisar es que este actualizado con el último Service Pack disponible, hotfixes, contar con un antivirus y tenerlo actualizado. Cabe insistir en que no se recomienda conectar un equipo a Internet

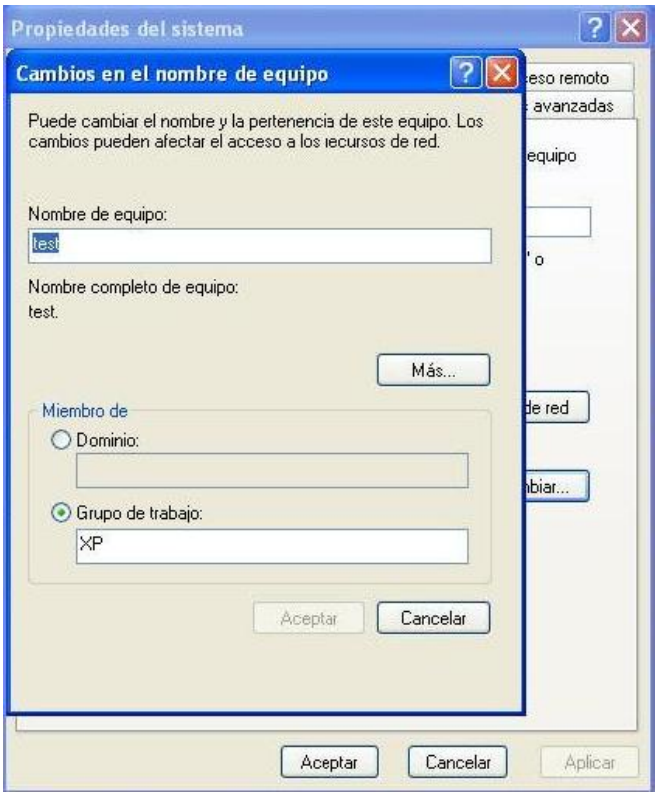
si no se encuentra actualizado y no tiene un antivirus por lo vulnerable que se encuentra.

Una vez revisado esto debemos proceder a agregar la computadora al dominio. Para lo cual es necesario ingresar al equipo cliente con una cuenta con privilegios de administrador local, una vez dentro de la sesión nos posicionamos sobre el icono de *Mi Pc*, damos clic derecho y seleccionamos Propiedades, como se muestra en la siguiente imagen.

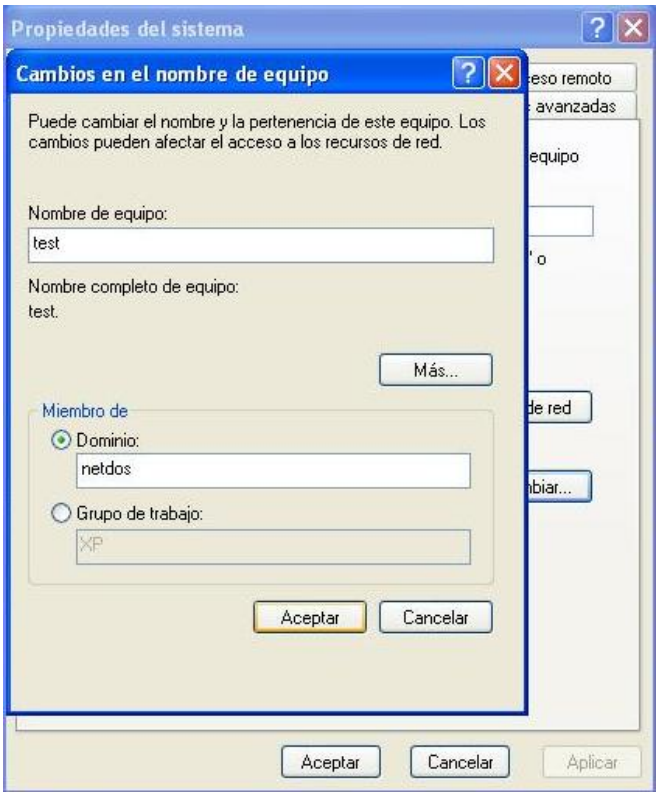
Con lo cual nos aparecerá una ventana similar a la que abajo vemos donde seleccionaremos la pestaña "*Nombre de Equipo*" en esa pestaña damos clic en el botón "*Cambiar*" lo que nos permitirá ingresar el equipo a un Dominio.



Una vez hecho esto aparecerá la ventana siguiente:



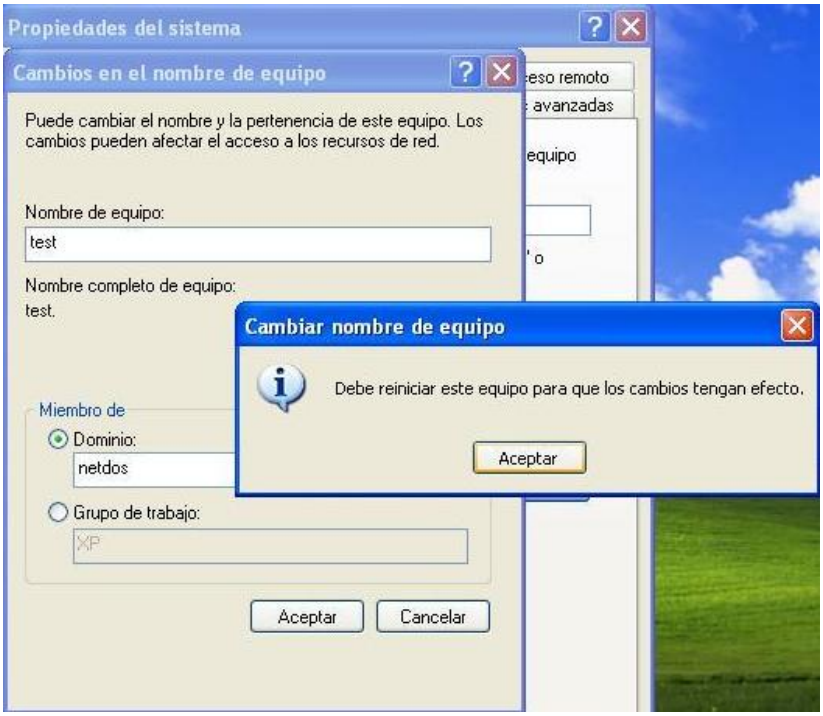
En la pantalla anterior seleccionamos la opción de dominio y escribimos el nombre de nuestro dominio, para este caso “netdos”.



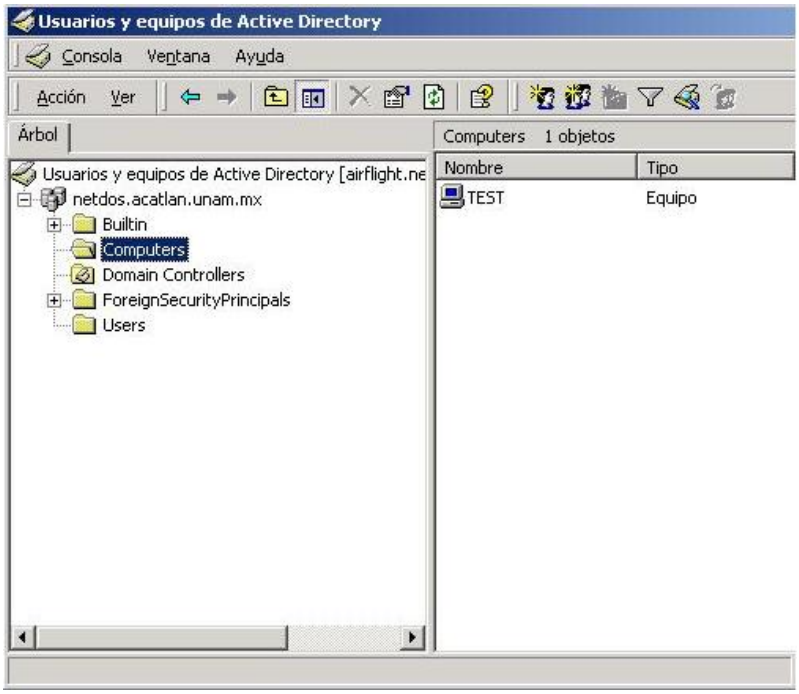
Una vez puesto el dominio damos clic en aceptar con lo que nos pedirá una cuenta que tenga permisos de administrador o que pueda agregar equipos al dominio como se observa en la siguiente figura.

Una vez validada la cuenta nos aparecerá una ventana con el mensaje de que hemos agregado correctamente la computadora al dominio, similar a la siguiente pantalla.

Después de dar clic en aceptar pedirá reiniciar el equipo para que los cambios se vean reflejados como se puede observar en la siguiente figura.



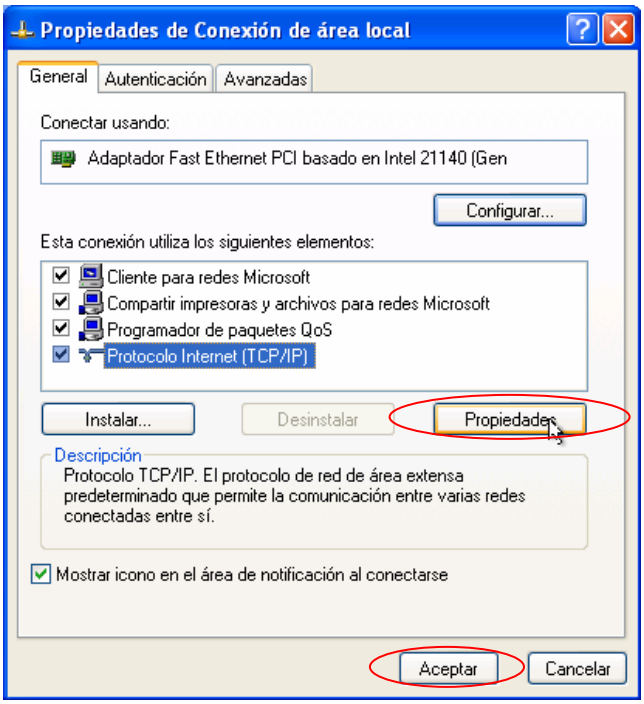
Ahora en nuestro DC con la herramienta "Usuarios y equipos de Active Directory" podemos verificar que el equipo se ha unido al Dominio, como se muestra en la siguiente pantalla.



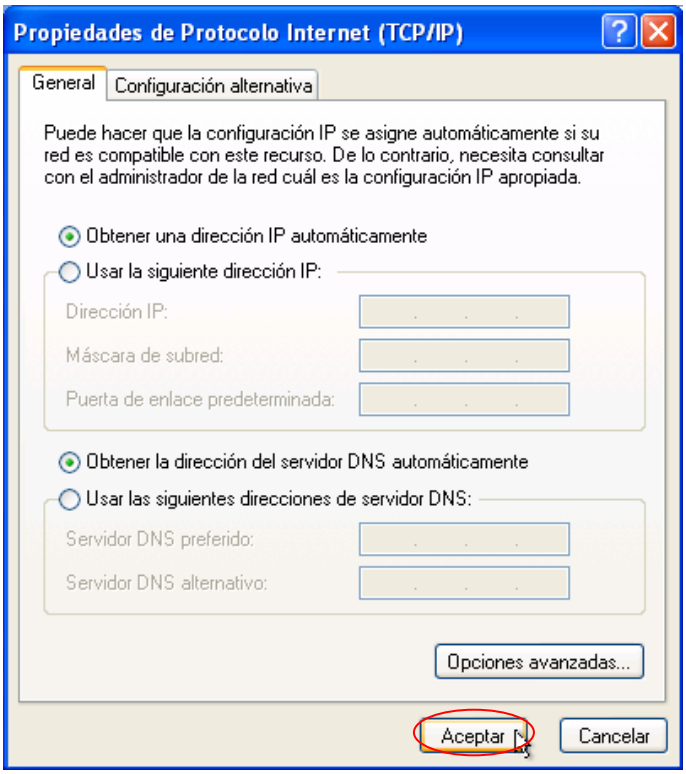
Bien, una vez verificado lo anterior podemos iniciar una sesión en el equipo y trabajar en él, pero antes debemos de configurar la NIC del equipo como se describe en la siguiente sección para el correcto funcionamiento del equipo y así pueda acceder a todos los recursos disponibles en la red incluyendo el acceso a Internet.

3.4. Configuración en los clientes para usar DHCP

Lo primero que realizaremos para este procedimiento será firmarnos con una cuenta que tenga sea miembro de los administradores locales del equipo o del dominio, una vez iniciado sesión abriremos las propiedades de la NIC que tengamos instalada y mostrará una pantalla similar a ésta.

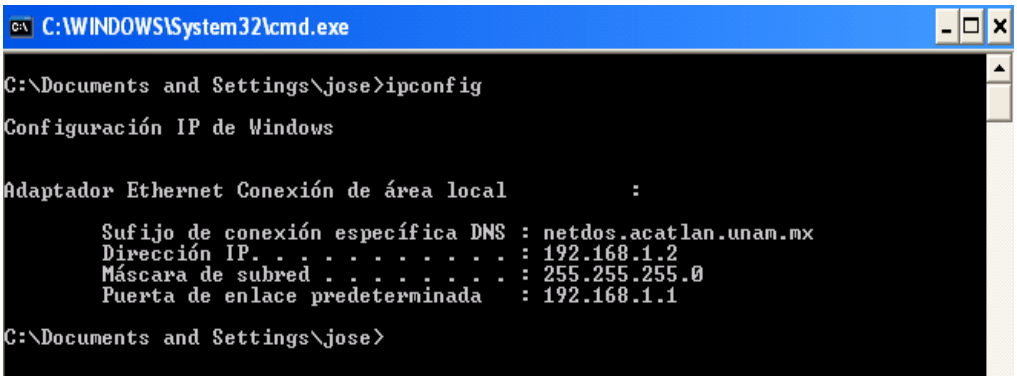


En esta pantalla seleccionamos *Protocolo Internet (TCP/IP)* damos clic en ***Propiedades*** con lo que aparecerá la siguiente pantalla.



Aquí debemos seleccionar las primeras opciones en ambos casos es decir *"Obtener una dirección IP automáticamente"* y *"Obtener la dirección del servidor DNS automáticamente."* Después damos clic en ***Aceptar*** y nos regresará a la pantalla anterior en la cual también damos clic en ***Aceptar*** y se cerrará la ventana.

Ahora para corroborar que nuestro servidor le está asignando una IP, abrimos una consola de comandos y tecleamos el comando *ipconfig*, que muestra la configuración actual del Protocolo de Internet (IP), el cual mostrará una pantalla similar a esta:



Como podemos observar nuestro equipo cuenta ya con una dirección IP que le fue otorgada por nuestro servidor DHCP, ya que esta IP se encuentra dentro del rango que

pusimos en nuestro ámbito a distribuir y además nuestro *sufijo de conexión específica DNS* es **netdos.acatlan.unam.mx** lo cual indica que está correcto.

Ahora probaremos el funcionamiento de la configuración que realizamos de NAT, es decir que podremos navegar en Internet.

Para esto abriremos una ventana de Internet Explorer e iremos al sitio Web de la UNAM http://www.unam.mx, teclearemos la dirección en la barra de direcciones del navegador y debemos de poder conectarnos al sitio sin ningún problema.

Bien, esto muestra que todo funciona correctamente.

CAPÍTULO 4. RECOMENDACIONES DE SEGURIDAD

4.1. Recomendaciones para los administradores de la red.

Con el incremento de usuarios en Internet, es cada vez más fácil obtener información sobre vulnerabilidades de un equipo o sistema operativo, pudiendo atacar con facilidad equipos conectados permanentemente a Internet que no disponen de un responsable para administrarlos, y ofrecen una serie de servicios que no se ocupan.

La seguridad no es algo que le pertenezca a un área determinada dentro de los servicios informáticos de las organizaciones, sino que prácticamente depende de todos los niveles de servicio.

Muchas organizaciones no tienen establecida una política de seguridad en la que indiquen los derechos y obligaciones, o sanciones en las que pueden incurrir los usuarios.

En organizaciones pequeñas es todavía frecuente emplear el mismo equipo como servidor de: INTERNET, DNS, FTP, WWW, CORREO, etc. y aparte como equipo de trabajo, con lo cual aumenta más el riesgo tener un ataque o una vulnerabilidad por todos los servicios que ofrece.

Por esos motivos se plantean las siguientes recomendaciones generales de seguridad para tratar de limitar el número y alcance de estos incidentes.

Antes que nada instale un antivirus, con el cual pueda actualizar todos los equipos de la red al mismo tiempo. En este caso se implantó la solución de Norton Antivirus de la compañía Symantec la cual proporciona una consola para administrar todos los equipos en la red y sus actualizaciones se pueden programar para no afectar la operación diaria, con resultados bastante buenos y fácil de administrar.

4.1.1. Seguridad a nivel de Red

Los ataques a nivel de red siguen siendo bastante frecuentes principalmente los de denegación de servicio (DoS)[1]. También es frecuente el empleo de herramientas automatizadas de escaneo y comprobación de vulnerabilidades en redes, así como la utilización de programas específicos que explotan una determinada vulnerabilidad del servidor o servicio concreto para atacarlo.

Filtrado de Paquetes

Aunque la seguridad a nivel sistema sigue teniendo una importancia vital, los fallos en varios servicios TCP/IP hace imprescindible el uso de filtros en el nivel de red, que permitan a una organización restringir el acceso externo a estos servicios. De esta manera sólo aquellos servicios que deban estar accesibles desde fuera de la red local serán

[1] En Internet, un DoS o ataque de denegación de servicio es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar.

permitidos a través de reglas en los routers esto se puede hacer mediante la implantación de un Firewall.[2]

El filtrado que se realice dependerá mucho de los servicios que brinde la organización aquí ponemos una lista de algunos servicios y los puertos asociados a el.

Nombre	Puerto	Tipo de conexión
echo	7	TCP y UDP
ssh	22	TCP y UDP
telnet	23	TCP y UDP
smtp	25	TCP y UDP
name server	42	TCP y UDP
domain name	53	TCP y UDP
http	80	TCP y UDP
pop3	110	TCP y UDP

[2] Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

sftp	115	TCP y UDP
nntp	119	TCP y UDP
imap	143	TCP y UDP
sqlsrv	156	TCP y UDP
snmp	161	TCP y UDP
send	169	TCP y UDP
irc	194	TCP y UDP
telnets	992	TCP y UDP

Dependiendo del servicio que se requiera WWW, FTP o cualquier otro se deberá crear la regla correspondiente ya sea de entrada o de salida en el Firewall para que se pueda tener acceso. Entre menos servicios brindemos se tendrá un mejor control, el cual se verá reflejado en una mayor seguridad.

4.1.2. Separación de las redes

Se deberá segmentar la red en medida de lo posible, las áreas de acceso general (biblioteca, aulas para profesores, áreas para estudiantes) deben estar separadas mediante switches o routers del resto de la red, para evitar que se puedan obtener claves de acceso o algún otro tipo de información. Esto también mejorará la autentificación e intercambio de información entre equipos del mismo segmento.

Hay que considerar las posibilidades de gestión y consola remota que disponen tanto switches y routers por lo que hay que cambiar el password por default o deshabilitar la administración remota si es que no se va a hacer uso de ella.

4.1.3. Recomendación a nivel de sistema

Las configuraciones establecidas por default en muchos sistemas operativos no son las más adecuadas desde el punto de vista de seguridad, además el desconocimiento y la desinformación de los responsables de estos equipos es motivo frecuente de problemas de seguridad.

Los ataques con más éxito en los sistemas informáticos se basan en aprovechar vulnerabilidades en el software que no ha sido actualizado a la última versión facilitada por el fabricante o que no se han aplicado los últimos parches disponibles.

A la hora de instalar un parche se recomienda comprobar la firma digital, si esta existe y

el checksum para verificar que se trata de una copia válida. El MD5 comprueba la integridad y la no alteración del paquete y la firma PGP la autenticidad del autor.

Es muy importante estar al día y revisar el software que se utiliza, tanto en servidores como en estaciones de trabajo especialmente aquel que tenga que ver con la conectividad a Internet, administración de servicios de red, etc. y actualizarlo con las últimas versiones disponibles. Al menos se recomienda tener la penúltima versión disponible del software en cuestión, ya que en algunas ocasiones la última versión podría traer consecuencias al implantarlo en un ambiente productivo es decir, podíamos afectar nuestra operación diaria.

Por último comentar que no es suficiente con instalar la última versión o actualización disponible, sino que es necesario configurarla convenientemente, de manera que se cierren los resquicios que pueden dejar las instalaciones por default. Esta corrección es importante no sólo en los sistemas operativos, sino también en el software en general.

4.1.4. Filtrado de servicios

Para evitar riesgos innecesarios, se deben configurar TODAS las máquinas de una organización para que ofrezcan únicamente los servicios que se tenga en mente ofrecer y no otros. Esto disminuirá considerablemente el riesgo de que estas máquinas sean atacadas aprovechando servicios completamente descuidados y que en muchas ocasiones no se es conciente que se están ofreciendo.

Es necesario asegurarse de que no existen debilidades en los archivos de configuración de los servicios ofrecidos y que los servicios se ofrezcan sólo al conjunto de usuarios para los cuales se diseñó.

4.1.5. Estaciones de trabajo

En la actualidad es muy común encontrar al menos un equipo en la organización que tenga Windows 9x/Me.

Se recomienda, con toda rotundidad que Windows 9x/Me se considere comprometido desde el mismo momento en que inicia, ninguna versión de Windows 9x/Me deberá ser utilizada como sistema operativo en una red donde algún recurso necesite ser asegurado.

En sistemas NT/2000/XP es preciso tener instalados el último Service Pack disponible y los últimos hotfixes disponibles así como usar el sistema de archivos NTFS ya que permite asignar permisos individuales o por grupo.

4.2. Política de contraseñas

Sin duda, uno de los métodos más habituales usados por los hackers para comprometer un sistema es el robo de contraseñas. Robando un nombre de usuario y su contraseña

correspondiente, un intruso puede reduciendo las probabilidades de ser detectado ganar acceso a un sistema, modificarlo y usarlo como trampolín para atacar otros sistemas.

La mayoría de los sistemas no tienen ningún mecanismo de control sobre las contraseñas que utilizan sus usuarios y en la mayoría de los casos existe por lo menos una contraseña en el sistema que puede ser fácil de descubrir, comprometiendo la seguridad de toda la red. Así que se recomienda habilitar en el servidor la política de complejidad en las contraseñas que usaran los usuarios de la red.

4.2.1. Contraseñas débiles

Se debe desarrollar una guía que ayude a los usuarios a la hora de escoger una contraseña lo suficientemente fuerte (robusta) para que no sean vulnerables a los ataques de diccionario o de fuerza bruta que suelen realizar la mayoría de las utilidades diseñadas para romper contraseñas.

Siga estas recomendaciones al momento de escoger su contraseña:

- No utilizar palabras del diccionario.
- No utilizar palabras que estén relacionadas con el usuario nombre de la esposa o marido, domicilio, fecha de nacimiento, nombre de la mascota, etc.
- Utilizar contraseñas con longitud mínima de 8 caracteres.
- No usar el nombre del usuario o una variante como el nombre de usuario invertido.
- Utilizar combinación de caracteres es decir debe contener mayúsculas, minúsculas, caracteres especiales y números.
- No almacenar la información de su cuenta (usuario y password) en archivos de texto o en postit.

Si se tiene más de una cuenta en distintos sistemas (Windows, Unix, Mac) no es recomendable utilizar la misma contraseña en todas, ya que si la seguridad de alguno quedara comprometida por lo tanto lo quedará en los demás.

Recomendaciones dirigidas a los administradores de la red.

Utilizar regularmente programas tipo crack para revisar la complejidad de las contraseñas del sistema y de esta manera encontrar las más débiles forzando al cambio de las mismas. Es mejor que nosotros conozcamos antes la debilidad de nuestras contraseñas que un atacante.

Establecer una política de cambios periódicos de las contraseñas cada 2 semanas o cada mes, esto dependerá de las propias políticas de cada organización y también se aconseja que no se usen contraseñas anteriores.

4.2.2. Cuentas sin contraseña y cuentas de invitados.

Cambiar todas las contraseñas que se instalan por default durante la instalación del Sistema Operativo.

No permitir la existencia de cuentas sin contraseña.

Eliminar cuentas de usuarios que ya no estén laborando en la organización o que no se estén utilizando.

Deshabilitar la cuenta de Invitado.

Eliminar las cuentas que pertenecen al grupo de Invitados.

Evitar la existencia de cuentas compartidas.

Renombrar la cuenta de administrador.

4.2.3. Administración y auditorias

Es necesario que se disponga de una forma para el registro de usuarios bien definido, donde se incluya una sección que deberá ser firmada por el usuario aceptando las condiciones y responsabilidades que supone tener una cuenta en la red.

Asegurarse de que existen copias de seguridad de la partición del disco donde se almacena la información de los usuarios siempre que esto sea posible y se dispongan de los medios para hacerlo.

Habilitar la auditoria de inicio de sesión, tanto exitoso como no exitoso.

Establecer una política de asignación de cuotas de disco para los usuarios, así como un procedimiento de comprobación con el fin de controlar que ningún usuario exceda el límite de espacio asignado.

Restringir el número de cuentas de administrador a un mínimo de dos.

La contraseña de administrador debe ser compleja, con un mínimo de 8 caracteres y debe ser modificada constantemente (mensualmente).

4.3. Recomendaciones para usuarios finales

Los administradores de red preocupados por la seguridad de sus sistemas deben estar continuamente informados de las nuevas versiones de los productos instalados en sus equipos. Pero no sólo los profesionales deben preocuparse de estos detalles, los usuarios finales también se pueden ver afectados por múltiples problemas si no actualizan su software.

Muchos pueden pensar que el problema de la seguridad sólo atañe a los administradores, informáticos y profesionales del sector. Pues esto es totalmente falso. El usuario final también debe preocuparse por la integridad de su sistema de casa.

Desde el clásico antivirus hasta el navegador de Internet, son programas imprescindibles que deben actualizarse con regularidad. Una configuración incorrecta o por default puede dejar abierto el sistema a cualquier intruso aficionado o profesional.

Un virus puede inutilizar todo nuestro equipo, o un troyano[3] puede revelar todas nuestras cuentas de acceso a Internet, correo entre otras cosas. Por todo ello, la seguridad también afecta a los usuarios domésticos, ya que hoy en día es común que un usuario trabaje en varios equipos al mismo tiempo casa, oficina, escuela, etc.

[3]Se denomina troyano (o caballo de Troya) a un virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información.

Por eso si el usuario ocupa la computadora de su casa alternadamente con la de la oficina o escuela, esta también deberá tener instaladas las últimas actualizaciones disponibles para:

- Sistema Operativo
- Office
- Navegador (Internet Explorer u otro)
- Cliente de correo (Outlook u otro)
- Aplicaciones que tenga instaladas
- Antivirus

El no hacerlo aumentará el riesgo de sufrir algún ataque o intrusión al equipo, o infectarnos de algún virus o gusano.

Instale un antivirus, no entraremos en la polémica de decir cual de todos los que hay en el mercado Norton, Mcafee, Panda, Trend Micro, Etrust, Kaspersky etc. es mejor, simplemente diremos que lo más importante de tener un antivirus es tenerlo actualizado no importa cual sea. Se recomienda actualizarlo al menos una vez cada semana, de preferencia diario y tener activa la protección en tiempo real.

No debemos olvidar, que al tener un equipo asignado en la red de alguna institución, la persona responsable de ese equipo es así mismo, el responsable de la seguridad del mismo, independientemente de la seguridad global de la institución. Si un hacker logra entrar en ese equipo y ataca por ejemplo, a un equipo del gobierno de Australia, usted tendrá parte de responsabilidad por el hecho de que el ataque provenga de su máquina.

Por eso en medida de lo posible siga estas sugerencias:

- No comparta recursos si no es necesario.
- Si necesita compartirlos, hágalo con una buena contraseña y asegúrese de que se comparte con las personas que lo necesitan y no este accesible a todo el mundo.
- Siempre que sea posible compártalos como de “sólo lectura” para evitar que borren o que llenen el directorio con archivos que no son suyos.
- Nunca comparta su disco duro con privilegios de escritura o control total ni siquiera con contraseña.

En general no se recomienda que se comparta información importante de forma

permanente por este método, pues no se sabe cuando alguien estará tratando de encontrar mediante algún programa de ataque de fuerza bruta o diccionario la posible contraseña.

Si le llega un archivo ejecutable por correo que usted no haya solicitado, NO LO EJECUTE, incluso si el correo proviene de alguna persona conocida ya que algunos virus tienen la capacidad de usar nuestros lista contactos de correo para enviar correos contaminados en nuestro nombre. Lo más recomendable es borrarlo o en todo caso comprobar si el remitente realmente lo ha enviado conscientemente, de lo contrario bórrelo definitivamente.

Abra los documentos de Excel o Word sin macros, probablemente sea un virus salvo cuando expresamente el remitente le informe que el archivo contiene macros.

Debido a que actualmente el Internet es más común y que casi cualquier persona tiene acceso a una computadora esto ha provocado la aparición del spyware que podríamos definir como:

"Aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos."

Por eso se debe tener algún programa que lo elimine como por ejemplo:

- ✓ Microsoft Windows Defender
- ✓ Ad-Aware SE
- ✓ Spybot Search & Destroy
- ✓ Sin espías Antispyware

De entre muchos más.

Algunos son gratuitos y otros de evaluación por un lapso de 30 días, después de este plazo se tendrán que pagar las respectivas licencias.

Puede descargarlos de de la página Web del Autor, o puede hacer una búsqueda en el buscador de su preferencia y lo llevará al sitio correspondiente.

Si ya cuenta con uno actualícelo y ejecútelo una vez a la semana o al menos cada quince días.

Los principales síntomas del Spyware son:

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas pop-ups, incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos.
- Barras de búsquedas de sitios como la de Alexa, Hotbar, etc. que no se pueden eliminar.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- La navegación por la red se hace cada día más lenta.

Si su equipo presenta alguno de estos síntomas lo más probable es que tenga Spyware.

También vigile el acceso físico al equipo, si alguien más tiene acceso a su computadora puede encenderla y obtener la información que esta en ella. Para eso cree cuentas personalizadas a cada usuario que utilizará el equipo y establezca los privilegios requeridos a cada una, esto no afectará la funcionalidad de los programas instalados, simplemente limitara la ejecución de tareas administrativas como instalar o desinstalar programas que requieren una cuenta con privilegios de administrador del sistema para hacerlo.

Actualmente el sistema operativo Windows XP Home y Profesional incorpora un firewall en su Service Pack 2 el cual nos puede proteger de intrusos, por lo que es conveniente

tenerlo activado. Si nosotros trabajamos con una versión anterior a Windows XP podemos instalar alguno de terceros, en el mercado existen varios firewalls personales y en especial Zone Alarm cuenta con una versión gratuita para usuarios personales. La cual recomiendo y se puede descargar de la página oficial[4].

Para mayor información acerca del uso del firewall de Windows XP se puede consultar la siguiente liga: http://www.microsoft.com/latam/windowsxp/using/security/internet/sp2_wfintro.mspx en la cual se describe a detalle como configurarlo adecuadamente.

Con todo lo anterior podemos decir que nuestro equipo está razonablemente seguro pero sin embargo nos falta todavía protegernos de una amenaza grave, y que según las tendencias actuales, va a ser cada vez más presente la llamada “Ingeniería Social”.

La cual podemos definir como la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente revelen datos o realicen actos que normalmente no harían.

La Ingeniería Social solamente se puede prevenir manteniéndonos alertas y desconfiando de cualquier situación que tenga algún elemento extraño o diferente.

Por ejemplo, si nos llega un correo aparentemente de un amigo diciendo que "como respuesta a tu correo, te envío el archivo solicitado", pero nosotros nunca enviamos el correo en cuestión. Es claro que se trata de un gusano informático que infectó a nuestro amigo, o a alguna persona que tenía a nuestro amigo en su lista de direcciones, y está tratando de inducirnos a abrir el archivo adjunto para infectar nuestro equipo.

[4] http://www.zonelabs.com

Últimamente están proliferando los correos electrónicos o llamadas telefónicas supuestamente a nombre de nuestro banco solicitando datos de nuestra cuenta.

En algunas otras ocasiones nos envían correos de supuestas actualizaciones Microsoft las cuales son falsas ya que ni Microsoft ni ninguna otra compañía que fabrique software envía actualizaciones por correo, éstas siempre deberán descargarse de la página oficial del fabricante.

Los bancos y en general las empresas nunca solicitan ni envían este tipo de datos por correo, así que ignore cualquier mensaje en este sentido y denúncielo a su administrador si así corresponde o a la empresa suplantada.

CONCLUSIONES

Con base en los resultados observados al implementar la solución basada en Windows 2000 Server, podemos afirmar que se tuvieron mejoras considerables para la administración de equipos, usuarios y en general de la disponibilidad de todos los recursos de la nueva red.

Se obtuvieron ahorros significativos de tiempo al momento de instalar los equipos y de configurarlos, ya que al estar en red se pueden instalar de manera desatendida (remota) o se pueden tener múltiples instalaciones al mismo tiempo; también se obtienen mejoras en cuanto a la seguridad, ya que el usuario final no puede iniciar sesión en un equipo si no cuenta con su usuario y password dentro de la red.

Al mismo tiempo, sólo pueden hacer uso de los programas y recursos que fueron autorizados para el perfil de cada usuario o grupo de usuarios, otro de los beneficios es que los usuarios no podrá instalar ningún programa sin contar con la autorización del administrador, ya que las instalaciones requieren de privilegios adicionales (permisos) para poder ejecutarlas lo cual nos garantiza el uso correcto del equipo.

La implantación de la consola de Antivirus permitió centralizar la administración del mismo ya que desde el servidor podemos manejar todos los equipos de la red, es decir en el servidor se instala la consola central de antivirus que en este caso es Norton Antivirus de Symantec y en los equipos sólo se instala un cliente, el cual se puede distribuir desde la misma consola y así las actualizaciones se bajan al servidor y este las distribuye de forma automática sin afectar al usuario, lo cual nos garantiza que todos los equipos de la red tengan antivirus, estén actualizados y no generamos trafico excesivo en la red ya que controlamos la hora de las actualizaciones.

El otorgarle al usuario un espacio de almacenamiento dentro del servidor donde puede guardar su información le resultó muy útil, ya que no importa en que equipo trabaje su información siempre está disponible y el usuario la accesa como si fuera una unidad más en el equipo y sólo la transporta cuando él lo decida.

En general se obtuvieron resultados muy favorables respecto a la situación original, con lo cual puedo recomendar este tipo de soluciones basadas en Windows. Se obtiene un servicio de calidad, de mayor disponibilidad, con mayor seguridad que en el anterior esquema de trabajo con lo cual se ven beneficiados tanto usuarios como administradores.

Los conocimientos adquiridos a lo largo de la carrera y en especial de las materias como: Sistemas Operativos, Teoría de la Computación I, Base de Datos, ayudaron a comprender mejor el entorno y algunos aspectos del problema al que me enfrentaba.

Sin embargo en otros temas descubrí que mi falta de conocimiento y experiencia en el

tema era grande, afortunadamente una de las ventajas que da la formación matemática es el ser autodidacta aplicando alguna una metodología para investigar lo cual me facilitó la búsqueda de información para solucionar este reto que se me presentaba.

Al mismo tiempo me di cuenta de las carencias que tenemos al terminar la carrera ya que en el caso muy particular del área de Sistemas nos hacen falta laboratorios de prueba, ya que la mayoría de las materias se enfocan a la teoría o en su defecto a la programación y no todos somos fanáticos de programar.

Además se tiene la falsa creencia que si eres del área de sistemas terminaras como Programador, o serás de Soporte Técnico sin desdeñar a todas las personas que se dedican a estas actividades y con el auge de escuelas “patito”, el nicho de mercado se reduce considerablemente ya que tenemos profesionistas preparados sin experiencia y gente técnica que maneja las herramientas pero sin tener conocimientos sólidos de lo que maneja o sin saber algo más del porque se maneja de una u otra manera.

Mi propuesta en ese sentido seria la de hacer laboratorios para enseñarle a los alumnos que la teoría que aprendemos se aplica en algo tangible. Eso les dará más herramientas para que decidan sobre que área se desarrollaran profesionalmente y no sigan con falsos mitos del área de sistemas.

También propongo que se hagan pláticas o talleres donde inviten a la gente egresada de MAC para que transmita su experiencia y conocimientos adquiridos durante su trayectoria laboral, puede ser durante la semana de MAC o en alguna otra fecha pero la intención seria que se les platique de que es lo que está pasando en el mercado laboral actual, ya que la competencia día a día es más y aunque puedo decir que la mayoría de la gente egresada de la carrera tiene una preparación aceptable aún tenemos áreas de oportunidad que si las aprovechamos ayudarán a que egresen mejores profesionistas.

BIBLIOGRAFÍA

- Cómo construir una intranet con Windows 2000 Server

  José Luis Raya Cabrera, Laura Raya González

  Alfaomega, c2001

- Mastering Windows 2000 Server

  Mark Minasi

  Sybex, Inc., 2001 3ra Edicion

- Configuring Windows 2000 Server Security

  Rockland, Ma. Syngress Media Inc., 2000.

- Windows 2000 Administration

  Spalding, George

  Osborne McGraw-Hill 2000

- Windows 2000 Profesional

  Eckel, Erik; Alderman, Brian

  Paraglyph Press 2001

Romo, José Fabian. La video conferencia en las redes de datos traductor de direcciones de red: NAT [en línea] [Consulta: 29 de Octubre de 2006] <http://www.trucoswindows.net/foro/topico-30085-ip-homologada.html>

Wikipedia la enciclopedia libre. Enciclopedia [en línea] <http://es.wikipedia.org/wiki/Protocolo_de_red> [Consulta: 20 de Noviembre de 2006, 15 de Enero de 2007]

Microsoft Corporation. Windows 2000 Server Resource Kit [en línea] Ultima Actualización: 2007 [Consulta: 21 de Agosto de 2006, 4 de Septiembre de 2006, 18 de Septiembre de 2006, 16 de Octubre de 2006, 13 de Noviembre de 2006, 12 de Febrero de 2007]. Active Directory Infrastructure, Planning for Active Directory, Domain Planning

Process, Assigning DNS Names to Create a Domain Hierarchy, TCP/IP Protocol Architecture, Host Name Resolution.

Disponible en World Wide Web: <http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/default.mspx>.