SEP **SEV** **DGEST** **DITD**

INSTITUTO TECNOLÓGICO SUPERIOR DE TANTOYUCA

TESIS PROFESIONAL

"INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR (BAJO WINDOWS SERVER) PARA LA MATERIA DE REDES"

TESISTA

WENDY EVELYN SAN ROMÁN BARRERA

NÚMERO DE CONTROL

S053S0017

POR EL TITULO DE

INGENIERÍA EN SISTEMAS COMPUTACIONALES

FECHA DE EXAMEN

AGOSTO 2011

INDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I. MARCO CONCEPTUAL

1.1 Antecedentes

1.2 Introducción

1.3 Justificación

1.4 Objetivos (General y específicos)

1.5 Alcances, Limitaciones y Delimitaciones del estudio

En el siguiente capítulo se hablará acerca de los factores que deben de ir en el estudio de una investigación. En la sección 1.2 se describe una breve introducción, en la sección 1.3 se da a conocer la justificación punto muy importante para tener un buen respaldo del motivo por el cual se decidió llevar acabo dicho proyecto. En la sección 1.4 se describen los objetivos del presente proyecto. En la sección 1.5 se dan a conocer los alcances, las limitantes y las delimitaciones que tuvo el proyecto.

1.1 Antecedentes

El principal motivo detrás de esta evolución, es la necesidad que tienen las organizaciones (empresas o instituciones públicas o privadas), de realizar sus operaciones más ágil y eficientemente, debido a la creciente presión competitiva a la que están sometidas, lo cual se traduce en la necesidad de que su personal sea más productivo, que se reduzcan los costos y gastos de operación, al mismo tiempo que se generan productos y servicios más rápidamente y con mejor calidad.

En este contexto, es necesario establecer una infraestructura de procesamiento de información, que cuente con los elementos requeridos para proveer información adecuada, exacta y oportuna en la toma de decisiones y para proporcionar un mejor servicio a los clientes.

El modelo Cliente/Servidor reúne las características necesarias para proveer esta infraestructura, independientemente del tamaño y complejidad de las operaciones de las organizaciones públicas o privadas y, consecuentemente desempeña un papel importante en este proceso de evolución.

1.2 Introducción

Una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Las redes de cómputo de las organizaciones, planteles educativos, empresas, etc. se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, cada vez más, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter proactivo para evitar problemas.

Anteriormente, cuando no se disponía de las herramientas que hoy existen, era necesario contratar a una empresa especializada para esta labor, con un costo muy elevado.

Dentro de la seguridad de una red, una de las herramientas más importantes es el monitoreo de red ya que atravez de esta herramienta asegura al administrador y a los usuarios el mantener una red más segura y fiable.

El término **Monitoreo de red** describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, u otras alarmas. Para lograr que una red se mantenga constantemente operable y segura se debe de contar con un servidor, y posteriormente mantenerle instalado ya sea uno o varios sistemas de monitoreo y para ello en este proyecto se instala el servidor explicando paso a paso la instalación de la plataforma Windows server 2003,y posteriormente configurarlo de manera que el servidor brinde las herramientas para monitorear la red por medio de sistemas de monitoreo, dándose a conocer 3 de ellos, otro punto que abarcará la configuración del servidor es el dar de alta a los usuarios que serán monitoreados por el servidor.

Este proyecto consiste en instalar y configurar un servidor a manera de que se realice un módulo didactico para la materia de Redes de Computadoras con el propósito de que el estudiante cuente con una herramienta de aprendizaje para que conozca el funcionamiento de un Servidor de Red.

LA "INSTALACION Y CONFIGURACION DE UN SERVIDOR (BAJO WINDOWS SERVER) PARA LA MATERIA DE REDES", ayudará al estudiante a tener una mejor comprensión de la administración de redes, al igual es de vital importancia que el instituto cuente con estas herramientas en las aulas para que así se tenga una mejor educación y contar con estudiantes cada día mas preparados.

1.3 Justificación

El contar con una red segura, es importante para cualquier institución, ya que representa la seguridad de la información y de los equipos.

Dentro de la seguridad, se incluyen actividades del proceso de monitoreo, considerando dentro de esta, la verificación del buen uso de los recursos de la red tales como ancho de banda, enlaces, servidores, etc.

En el ITSTA no se cuenta con un sistema de monitoreo, motivo por el cual se propone el desarrollo del proyecto "INSTALACION Y CONFIGURACION DE UN SERVIDOR (BAJO WINDOWS SERVER 2003) PARA LA MATERIA DE REDES".

A los estudiantes de la carrera de Ingeniería en Sistemas computacionales les será de gran ayuda el contar con una herramienta para su formación como futuros ingenieros, ya que por parte de los alumnos, en ocasiones no llegan a realizar sus actividades cómo ellos lo necesitan.

Por ello es de vital importancia que con el paso del tiempo y a las necesidades, se vayan dando alternativas y soluciones el contar con herramientas para el aprendizaje de los alumnos para hacer que su entendimiento lo lleven a la práctica y que tengan un panorama más claro de cómo funciona un Servidor de red.

Este proyecto permitirá al alumno contar con una herramienta para que sus conocimientos los oriente más a la práctica y así poder desenvolverse aun más en la administración de Redes.

1.4 Objetivo General

Instalar y configurar un servidor de usuarios (bajo Windows Server 2003) para la materia de Redes de computadoras con el propósito de orientar al estudiante a que tenga una mejor comprensión de la administración de Redes.

Objetivos Específicos

- Motivar al estudiante sobre la materia de Redes de Computadoras.
- Permitir a los estudiantes que conozcan las operaciones básicas de un servidor de red.
- Orientar al estudiante a que tenga una mejor comprensión de la administración de Redes.
- Hacer conciencia al estudiante de no hacer un mal uso de la red.
- Controlar el tráfico malicioso en la red.
- Mantener una mejor administración de los recursos de la red
- Implementar estrategias de seguridad basadas en el monitoreo.
- Facilitar el flujo de información.
- Minimizar el tiempo empleado en los procesos.

1.5 Alcances y Limitaciones

Alcances

- Se pretende que dicho Proyecto sea implementado en el laboratorio de Redes, con la finalidad de que los estudiantes conozcan las operaciones básicas de un servidor de red, instalando varios software de monitoreo para que los alumnos tengan los conocimientos y habilidades de monitorear una red.

Se manejan 4 software de monitoreo que son:

- Radmin (Remote Administrator).
- Sspro
- Observer
- Wireshark

Limitaciones

- Este proyecto será implementado en el laboratorio de redes del Instituto Tecnologico Superior de Tantoyuca, sin embargo el proyecto no abarca en toda la red del ITSTa.
- El Instituto Tecnologico Superior de Tantoyuca, no cuenta con equipos que tenga las características suficientes propias para la instalación de un servidor.

Delimitaciones

- Se instalará un servidor bajo el sistema operativo Windows server 2003 y se configurará con las opciones administrativas básicas para la administración de usuarios.

CAPÍTULO II. MARCO TEÓRICO

2.1 Concepto de servidor

2.1.1. Tipos de servidores

2.2 Arquitectura cliente-servidor

2.3. Windows server 2003

2.3.1 Beneficios de la familia de Windows Server 2003

2.3.2 Tecnologías Básicas de Windows Server 2003

2.3.3 Requerimientos para la instalación de Windows Server 2003

2.3.4 Versiones de Windows Server 2003

2.4 Concepto de Dominio

2.3.1 Objetivos del dominio

2.5 Concepto de Active Directory

2.5.1 Elementos que administra Active Directory

2.5.2 Estructura Lógica de Active Directory

2.5.3 Estructura Física de Active Directory

2.5.4 Almacén de datos de Active Directory

2.6 Controladores de Dominio

2.7. Introducción a las cuentas de usuarios y equipos.

2.7.1 Tipos de cuentas de usuarios

2.7.2 Creación de cuentas de usuarios

2.7.3 Diseño de cuentas de usuarios

2.7.4 Proteger cuentas de usuarios.

2.8 Introducción a los grupos

2.8.1 Ámbito de grupo

2.8.2 Tipos de grupos

2.8.3 Grupos predeterminados

2.9 Introducción a las directivas

2.9.1 Configuración de seguridad

En el presente capítulo se darán a conocer las herramientas que se necesitan para el desarrollo de este proyecto, así como también se hará una breve descripción de ellas. Cabe destacar que fue necesario descargar aplicaciones con licencias permisivas haciendo uso del internet.

2.1 Concepto de servidor

En informática, un **servidor** es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

También se suele denominar con la palabra servidor a:

- Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

- Una computadora en la que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes, tanto si se trata de un ordenador central (*mainframe*), un miniordenador, un ordenador personal, una PDA o un sistema embebido; sin embargo, hay computadoras destinadas únicamente a proveer los servicios de estos programas: estos son los servidores por antonomasia.

- Un servidor no es necesariamente una máquina de última generación de grandes proporciones, no es necesariamente un superordenador; un servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente (ej.: servidores web, bases de datos grandes, etc. Procesadores especiales y hasta varios terabytes de memoria). Todo esto depende del uso que se le dé al servidor.

2.1.1 Tipos de servidores

- **Servidor de usuarios**: Un servidor de usuarios es aquella máquina que valida a los usuarios de la red cuando escriben su nombre de usuario y contraseña al iniciar sesión. Si el nombre de usuario y contraseña escritos por el usuario no son reconocidos por el servidor de usuarios, no se le permitirá acceder a los recursos en red. En Windows NT esta máquina recibe el nombre de Controlador principal de dominio. Los usuarios de la red se dice que inician sesión en el dominio del servidor (tienen que haber sido dados de alta previamente en el servidor como usuarios del dominio). El administrador de la red se encarga de la gestión de usuarios: altas, bajas, cambios de contraseña, etc.

- **Servidor de archivo**: es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.

- **Servidor de impresiones**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.

- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

- **Servidor de fax**: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

- **Servidor de la telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema

interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, p. ej., la entrada excesiva de la voz sobre IP (VoIP), etc.

- **Servidor proxy**: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente), también proporciona servicios de seguridad, o sea, incluye un cortafuegos. Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

- **Servidor del acceso remoto (RAS)**: controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autentificación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.

- **Servidor de uso**: realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza la interfaz operadora o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de Base de Datos** (database server): provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo

cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

- **Servidor de reserva**: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clustering.

- **Servidor de impresión**: muchas impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un "print server" (servidor de impresión), a actuar como intermediario entre la impresora y el dispositivo que está solicitando que se termine un trabajo de impresión.

2.2 Arquitectura cliente-servidor

La modalidad o arquitectura Cliente/Servidor es aquella en la que confluyen una serie de aplicaciones basadas en dos categorías que cumplen funciones diferentes (una requiere servicios y la otra los brinda) pero que a la vez, pueden realizar tanto actividades en forma conjunta como independientemente. Esas dos categorías son justamente cliente y servidor.

En el caso del cliente, es aquel que requiere un servicio del servidor. En esta categoría se realizan funciones de software basándose en el hardware pero en caso de no tener la capacidad de procesar los datos necesarios, recurre al servidor y espera a que este le brinde los servicios solicitados. El cliente es una estación de trabajo o computadora que está conectada a una red a través de la cual puede acceder al servidor.

Por el contrario, el servidor es la máquina desde la que se suministran servicios y que está a la espera del requerimiento del cliente. Una vez hecho, busca la información

solicitada y le envía la respuesta al cliente; incluso puede enviar varios servicios a la vez, lo que es posible porque entre ellos están conectados mediante redes LAN o WAN.

Entre las características fundamentales de esta arquitectura encontramos que tanto el cliente como el servidor pueden realizar tareas en forma conjunta como separada ya que el cliente también tiene sus propias aplicaciones, archivos y bases de datos y que además, pueden estar en la misma plataforma o en plataformas diferentes. Por otra parte, el servidor puede brindar varios servicios a la vez, tanto al mismo cliente como a clientes múltiples.

2.3 Windows Server 2003

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

2.3.1 Beneficios de la Familia Windows Server 2003

Windows Server 2003 cuenta con cuatro beneficios principales:

Beneficios	Descripción
Seguridad	Windows Server 2003 es el sistema operativo de servidor más rápido y más seguro que ha existido. Windows Server 2003 ofrece fiabilidad al: • Proporcionar una infraestructura integrada que ayuda a asegurar que su información de negocios estará segura. • Proporcionar fiabilidad, disponibilidad, y escalabilidad para que usted pueda ofrecer la infraestructura de red que los usuarios solicitan.
Productividad	Windows Server 2003 ofrece herramientas que le permiten implementar, administrar y usar su infraestructura de red para obtener una productividad máxima. Windows Server 2003 realiza esto al: • Proporcionar herramientas flexibles que ayuden a ajustar su diseño e implementación a sus necesidades organizativas y de red. • Ayudarle a administrar su red al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones. • Ayudar a mantener bajos los gastos generales al permitirles a los usuarios trabajar más por su cuenta.
Conectividad	Windows Server 2003 puede ayudarle a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes. Windows Server 2003 realiza esto al:

	□ Proporcionar un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudarle a crear más rápido, fácil y seguro una Intranet dinámica y sitios de Internet. □ Proporcionar un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios Web en XML más fácilmente. □ Brindar las herramientas que le permitan conectar servicios Web a aplicaciones internas, proveedores y socios.
Valor de Negocio	Windows Server 2003, cuando está combinado con productos Microsoft como hardware, software y servicios de los socios de negocios del canal brindan la posibilidad de ayudarle a obtener el rendimiento más alto de sus inversiones de infraestructura. Windows Server 2003 lleva a cabo esto al: □ Proporcionar una guía de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. □ Ayudarle a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación de su servidor. □ Bajar el coste total de propiedad (TCO) para recuperar rápido la inversión.

Tabla 1.- Beneficios de la Familia de Windows server 2003

2.3.2 Tecnologías Básicas de Windows Server 2003

Nuevas tecnologías y características que hacen de Windows Server 2003 una plataforma de servidor ideal para organizaciones de cualquier tamaño. Conozca como este sistema operativo de servidor puede hacer que su organización y sus empleados sean más productivos y estén mejor conectados.

Seguridad

Windows Server 2003 es la versión de sistema operativo más fiable y segura producida hasta ahora por Microsoft. Estos son sus puntos Fuertes:

- **Disponibilidad.** Mediante arquitecturas en clúster, que son la base fundamental de las infraestructuras informáticas en entornos de misión crítica en muchas organizaciones, donde se aplican a comercio electrónico, aplicaciones de línea de negocio o servicios corporativos centralizados de alta disponibilidad. La instalación y configuración de un clúster con Windows Server 2003 es sencilla y ofrece un rendimiento extraordinario, con una mejor recuperación y un nivel de servicio excepcional, llegando en algunos casos al 99,99%. La familia de Windows Server 2003 soporta clusters de servidor de hasta 8 nodos. Si uno de los nodos en un clúster no se puede usar debido a un fallo o por mantenimiento, inmediatamente otro nodo empieza a dar servicio, un proceso conocido como recuperación de fallos. Windows Server 2003 también soporta balanceo de carga

  de red, el cual nivela el tráfico de entrada dentro del Protocolo de Internet (IP), a través de los nodos en un clúster.
- **Escalabilidad.** Windows Server 2003 ofrece escalabilidad vertical, con soporte a sistemas de multiprocesamiento simétrico (SMP), y horizontal ("Scale-out") por medio de clusters. La gama de servidores Windows Server 2003 puede funcionar

desde sistemas monoprocesador hasta multiprocesadores de 32 vías, y sistemas de 64 bits.

- **Fiabilidad.** La escala que adquieren las redes extensas y locales hoy día, dan como resultado un mundo interconectado donde la seguridad es la preocupación principal de los usuarios y administradores. La gama de productos Windows Server System, y en particular Windows Server 2003 han sido objeto de una revisión completa para reforzar su seguridad en todas las fases del ciclo de vida del producto, desde su mismo diseño hasta su mantenimiento.

- Los negocios han hecho crecer la tradicional red de área local (LAN) al combinar redes internas, externas y sitios de Internet. Como resultado de esto, el aumento de seguridad en los sistemas es ahora más crítica que antes. Como parte del compromiso de Microsoft de brindar computación segura, la compañía ha revisado intensamente la familia Windows para identificar posibles fallos y debilidades. Windows Server 2003 ofrece muchas mejoras y características nuevas e importantes de seguridad incluyendo:
    - **Protección frente a errores en tiempo de ejecución.** Con esta mejora, Windows Server 2003 aumenta su fiabilidad y proporciona un entorno seguro, ya que se reducen las vulnerabilidades causadas por errores comunes de programación. Se producen, además, comprobaciones de seguridad en tiempo de ejecución y bloqueo de ciertas operaciones no permitidas.
    - **Internet Information Services 6.0.** La configuración por defecto de Internet Information Services (IIS) 6.0 es la de máxima seguridad. Entre sus características de seguridad avanzadas se incluyen el cifrado selectivo de datos, autenticación avanzada y acceso seguro al control de procesos.

Productividad

Las mejoras que proporciona Windows Server 2003 en materia de productividad se extienden a numerosas áreas, entre ellas:

- **Servicios de impresión y archivos.** las nuevas mejoras introducidas se orientan a facilitar la administración y seguridad de los recursos de archivo compartido, a dar soporte a nuevas tecnologías de almacenamiento e impresión y a una mayor escalabilidad y rendimiento de las soluciones de recursos compartidos, reduciéndose así el TCO.
- **Active Directory.** Windows Server 2003 incorpora muchas mejoras para Active Directory, haciéndolo mas versátil, fiable y económico de usar, con una mayor escalabilidad y rendimiento. Añade además mejoras que permiten una mayor flexibilidad a la hora de diseñar, implantar y administrar el servicio de directorio corporativo, especialmente en grandes organizaciones.
- **Servicios de Administración.** La proliferación de nuevas plataformas y dispositivos móviles ha provocado un aumento de la complejidad y coste de la administración de las redes corporativas. La clave para una reducción efectiva de los costes de mantenimiento está en la automatización de procesos, y para ello, Windows Server 2003 incluye diversas herramientas de administración automatizada, como Microsoft Software Update Services (SUS) y asistentes de configuración de servidor para ayudar a automatizar las instalaciones. La administración de Políticas de Grupo se hace más fácil con la nueva Consola para Administración de Políticas de Grupo (GPMC), y las nuevas herramientas de línea de comandos permiten que los administradores realicen la mayoría de las tareas desde la consola de comandos y con muy pocas operaciones.
- **Administración de almacenamiento.** Windows Server 2003 introduce novedades y mejoras en las herramientas de administración del almacenamiento, haciendo que sea más fácil y más seguro manejar y dar mantenimiento a discos y volúmenes, respaldar y recuperar datos, y conectarse a una red de almacenamiento (SAN).

- **Terminal Services.** Con este servicio, desde un servidor Windows Server 2003 se pueden ejecutar aplicaciones en modo de terminal remoto Windows,

prácticamente desde cualquier dispositivo, incluso en sistemas que no son Windows.

Conectividad

Windows Server 2003 incluye características y mejoras nuevas para asegurarse de que su organización y usuarios permanezcan siempre conectados:

- **Servicios Web XML.** IIS 6.0 es un componente importante de la familia Windows. Los administradores y desarrolladores de aplicaciones Web disponen ya de una plataforma Web rápida que sea tanto escalable como segura. Las mejoras significativas de arquitectura en IIS abarcan un modelo de procesos nuevo que en gran medida aumenta la fiabilidad, la escalabilidad y el rendimiento.
- **Comunicaciones y redes.** Las comunicaciones y redes son, hoy más que nunca, un elemento crucial para las organizaciones, en un mundo globalizado. Los usuarios necesitan conectarse a la red desde cualquier lugar y cualquier dispositivo. Se amplía esta necesidad a los clientes, colaboradores, socios y otros agentes externos a las propias organizaciones, que deben intercambiar información y, de nuevo, la seguridad y la disponibilidad son requisitos ineludibles. Las nuevas características y mejoras en redes en la familia de Windows Server 2003 incrementan la versatilidad, manejabilidad y fiabilidad de infraestructura de red.
- **Servicios empresariales UDDI.** Windows Server 2003 incluye servicios empresariales UDDI, una infraestructura dinámica y flexible para servicios Web XML. Esta solución basada en estándares le permite a las compañías llevar a cabo sus propios servicios internos UDDI para redes de uso interno y externo. Los desarrolladores pueden encontrar y reutilizar fácil y rápidamente los servicios Web disponibles dentro de la organización. Los administradores TI pueden catalogar y administrar los recursos programables de su red. Con servicios

empresariales UDDI, las compañías pueden crear e implementar aplicaciones más inteligentes y seguras.

- **Servicios de Windows Media.** Windows Server 2003 incluye los servicios de difusión multimedia más poderosos de la industria. Estos servicios son parte de la nueva versión de la plataforma de tecnologías de Microsoft Windows Media que también incluyen un nuevo reproductor de Windows Media, un codificador de Windows Media, codecs de audio y video y un paquete para desarrollo de software de Windows Media.

2.3.3 Requerimientos para la Instalación de Windows Server 2003

Para garantizar que se obtienen un rendimiento adecuado, compruebe que los equipos donde instale o actualice Windows Server 2003, Enterprise Edition cumplan los requisitos siguientes:

Para un equipo basado en x86:

- Uno o más procesadores con una velocidad mínima recomendada de 550 megahercios (MHz). La velocidad mínima admitida es 133 MHz. Se admiten ocho procesadores por equipo como máximo. Se recomiendan los procesadores de la familia Intel Pentium/Celeron, AMD K6/Athlon/Duron u otros procesadores compatibles.
- 256 megabytes (MB) de memoria RAM como (mínimo recomendado). 128 MB es el mínimo admitido, 32 gigabytes (GB) es el máximo admitido. Para los equipos que tengan más de 4 GB de memoria RAM, haga clic en el vínculo correspondiente de Recursos de soporte para confirmar la compatibilidad de hardware.

Para un equipo con arquitectura basada en Itanium:

- Uno o más procesadores con una velocidad mínima de 733 MHz. Se admiten ocho procesadores por equipo como máximo.
- 1 GB de memoria RAM, como mínimo, y 1024 GB (1 Terabyte), como máximo. Para los equipos que tengan más de 4 GB de memoria RAM, haga clic en el vínculo correspondiente de Recursos de soporte para confirmar la compatibilidad de hardware.

Para un equipo basado en x64:

- Uno o varios procesadores con una velocidad mínima de 1,4 GHz Se admiten ocho procesadores por equipo como máximo.
- 1 GB de memoria RAM, como mínimo, y 1024 GB (1 Terabyte), como máximo. Para los equipos que tengan más de 4 GB de memoria RAM, haga clic en el vínculo correspondiente de Recursos de soporte para confirmar la compatibilidad de hardware.

- Una partición de disco duro o un volumen con suficiente espacio libre para alojar el proceso de instalación. Para asegurar la flexibilidad en un uso futuro del sistema operativo, es recomendable que deje mucho más espacio que el mínimo necesario para ejecutar el programa de instalación, que es, aproximadamente, de 2 GB a 3 GB para versiones basadas en x86 de Windows Server 2003, y de 4 GB para versiones basadas en x64 de Windows Server 2003. Es necesario más espacio si ejecuta el programa de instalación a través de una red en lugar de hacerlo desde un CD ROM, o si realiza la instalación en una partición FAT o FAT32 en el caso de versiones de Windows Server 2003 basados en x86 o x64. (NTFS es el sistema de archivos recomendado para versiones de Windows Server 2003 basados en x86 o x64. Las versiones de Windows Server 2003 basadas en Itanium sólo admiten NTFS).

Además, una actualización de controlador de dominio de Windows NT 4.0 puede requerir mucho más espacio que otras instalaciones o actualizaciones, ya que la base de datos de cuentas de usuario existentes puede expandirse hasta multiplicarse por diez al agregar la funcionalidad de Active Directory.

2.3.4 Versiones de Windows server2003

Microsoft Windows Server 2003 Web Edition	Para servicios web y hosting, esta versión provee una plataforma para el desarrollo y la instalación rápida de servicios y aplicaciones web. Solo Versión OEM
Microsoft Windows Server 2003 Standard Edition	Para servicios de administración de Redes, esta versión de Windows Server 2003 es ideal para file and print servers, web servers, y workgroups. También provee acceso remoto a redes.
Microsoft Windows Server 2003 Enterprise Edition	Contiene todas las características de Windows Server 2003 Standard y provee escalabilidad y disponibilidad incrementada. Esta versión es ideal para servers utilizados en grandes redes y para bases de datos de uso intensivo.
Microsoft Windows Server 2003 Datacenter Edition	Contiene todas las características de Windows Server 2003 Enterprise Edition y, además, soporte para más memoria y más CPU por computadora. Esta versión es ideal para uso de datawarehouses de gran tamaño, procesamiento online, transacciones (OLTP) y proyectos de consolidación de servidores.

Tabla 2.- Versiones de Windows Server 2003

2.4 Concepto de dominio

La unidad central de la estructura lógica del Directorio Activo es el dominio. Un dominio es un conjunto de equipos que comparten una base de datos de directorio común. Dentro de una organización, el Directorio Activo se compone de uno o más dominios, cada uno de ellos soportado, al menos, por un controlador de dominio. Como hemos visto, cada dominio se identifica unívocamente por un nombre de dominio DNS, que debe ser el sufijo DNS principal de todos los ordenadores miembros del dominio, incluyendo el o los controladores.

2.4.1 Objetivos del dominio

- **Delimitar la seguridad**. Un dominio Windows 2000 define un límite de seguridad. Las directivas de seguridad, los derechos administrativos y las listas de control de acceso (*Access Control Lists*, ACLs) no se comparten entre los dominios.

  Active Directory puede incluir uno o más dominios, teniendo cada uno sus propias directivas de seguridad.

- **Replicar información**. Un dominio es una partición del directorio, las cuales son unidades de replicación. Cada dominio almacena solo la información sobre los objetos localizados en este dominio. Active Directory utiliza un modelo de replicación con varios maestros. Todos los controladores de dominio del dominio pueden recibir cambios realizados sobre los objetos, y pueden replicar estos cambios a todos los controladores de dominio en el dominio.

- **Aplicar Políticas de Grupo**. Un dominio define un posible ámbito para las políticas. Al aplicar un objeto de política de grupo (GPO) al dominio, este establece como los recursos del dominio se configuran y se usan. Estas políticas se aplican dentro del dominio y no a través de los dominios.

- **Delegar permisos administrativos**. En las redes que ejecutan Windows 2000, se puede delegar a medida la autoridad administrativa tanto para unidades organizativas (OUs) individuales como a dominios individuales, lo cual reduce el número de administradores necesarios con amplios permisos administrativos. Ya que un dominio representa un límite de seguridad, los permisos administrativos se limitan al dominio.

2.5 Concepto de Active Directory

Hoy en día, las computadoras existentes en cualquier organización se encuentran formando parte de redes de ordenadores, de forma que pueden intercambiar información. Desde el punto de vista de la administración de sistemas, la mejor forma de aprovechar esta característica es la creación de un *dominio* de sistemas, en donde la información administrativa y de seguridad se encuentra *centralizada* en uno o varios servidores, facilitando así la labor del administrador. Windows 2000 utiliza el concepto de **directorio** para implementar dominios de sistemas Windows 2000.

En el ámbito de las redes de ordenadores, el concepto de *directorio* (o almacén de datos) es una estructura jerárquica que almacena información sobre objetos en la red, normalmente implementada como una base de datos optimizada para operaciones de lectura y que soporta búsquedas de grandes datos de información y con capacidades de exploración.

Active Directory es el servicio de directorio de una red de Windows 2000. Este servicio de directorio es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y *administrar* centralizadamente el acceso a los recursos de la red.

Como veremos, al instalar el Directorio Activo en uno o varios sistemas Windows 2000 (Server) de nuestra red, convertimos a dichos ordenadores en los servidores del dominio, o más correctamente, en los denominados *Controladores de Dominio* (*Domain Controllers*). El resto de los equipos de la red pueden convertirse entonces en los *clientes* de dicho servicio de directorio, con lo que reciben toda la información almacenada en los controladores. Esta información incluye no sólo las cuentas de usuario, grupo, equipo, etc., sino también los perfiles de usuario y equipo, directivas de seguridad, servicios de red, etc. El Directorio Activo se convierte así en la herramienta fundamental de administración de toda la organización.

2.5.1 Objetos que administra Active Directory

Toda la información sobre los usuarios, grupos, equipos, servidores y políticas de seguridad en Active Directory se organizan y clasifican en diferentes objetos de Active Directory. Un objeto de Active Directory puede ser definido como un conjunto de atributos que representa un recurso en la red. Cada objeto tiene un nombre único o identificador único, un *nombre completo. Los* objetos también pueden contener otros objetos. Estos objetos son conocidos como *los contenedores.* En los usuarios de Active Directory y equipos de consola, los tipos por defecto en el objeto creado un nuevo dominio de Active Directory son:

- unidad organizativa,
- usuario,
- equipo de Contacto,
- Grupo,
- carpetas compartidas y
- una impresora compartida.

La estructura del directorio activo está dividida en dos: estructura lógica y estructura física.

2.5.2 Estructura Lógica de Active Directory

La estructura lógica del Directorio Activo se centra en la administración de los *recursos* de la red organizativa, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes. Como veremos, la estructura lógica de la organización se basa en el concepto de *dominio*, o unidad mínima de directorio, que internamente contiene información sobre los recursos (usuarios, grupos, directivas, etc.) disponibles para los ordenadores que forman parte de dicho dominio. Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de *unidades organizativas*, que permiten una administración independiente sin la necesidad de crear múltiples dominios. Sin embargo, si la organización desea estructurarse en varios dominios, también puede hacerlo, mediante los conceptos de *árbol* y *bosque*; ambos son jerarquías de dominios a distintos niveles, en función de si los dominios comparten o no un espacio de nombres común. A continuación se presentan todos estos conceptos de forma más detallada.

Los dominios, unidades organizativas (OU), árboles y los bosques se consideran estructuras lógicas

- ***Los dominios*** son la estructura lógica principal de Active Directory, ya que contienen objetos de Active Directory. Los objetos de red, tales como usuarios, impresoras, recursos compartidos, y más, se almacenan en los dominios.

Los dominios son también *los límites de seguridad. El* acceso a los objetos en el dominio es controlado por las listas de control de acceso (ACL).

- ***Los árboles de dominio****:* Cuando el grupo de varios dominios en una estructura jerárquica mediante la adición de *los dominios secundarios* de un *dominio principal,* que son básicamente la formación de un árbol de dominios. Los dominios son considerados como parte del mismo árbol de dominios cuando tienen una *estructura de nombres*

contiguo. Una *de dos vías* relación de *confianza transitiva,* se crea automáticamente entre el dominio de dominio principal y secundario al crear el dominio secundario.

- ***Bosques**:* Un bosque es la agrupación de varios árboles de dominio en una estructura jerárquica. Dominio de los árboles en un bosque tiene un esquema común, la configuración y de catálogo global. Dominios en el bosque están vinculados por dos vías confianza transitiva. A través del *nivel funcional del bosque,* puede habilitar los bosques amplios de las características adicionales de Active Directory. El bosque niveles funcionales que se pueden establecer son Windows 2000, Windows Server 2003 provisional, y Windows Server 2003.
- ***Unidad organizativa (OU):*** Una OU es un contenedor que le permite organizar objetos como usuarios, equipos y otras unidades organizativas, incluso en un dominio para formar un grupo administrativo lógico. Una OU es el más pequeño componente de Active Directory en los que puede *delegar la autoridad administrativa.* Un dominio puede tener propia jerarquía de unidad organizativa única.

Por tanto, el objetivo de las unidades organizativas es *estructurar* u organizar el conjunto de los objetos del directorio, agrupándolos de forma coherente. En el Directorio Activo, las unidades organizativas permiten:

a. **Conseguir una estructuración lógica** de los objetos del directorio, de acuerdo con la organización de la *empresa* (por departamentos o secciones, sedes, delegaciones geográficas, etc.). Entre otras ventajas, esta organización le permite al administrador del dominio una gestión más lógica de usuarios, grupos, equipos, etc., pero también le permite a cualquier usuario una búsqueda de los objetos más sencilla cuando explora el directorio buscando recursos (por ejemplo, se podría localizar fácilmente las impresoras compartidas del edificio central de la delegación de Alicante).

b. **Delegar la administración**. Cada unidad organizativa puede administrarse de forma independiente. En concreto, se puede otorgar la administración total o parcial de una unidad organizativa a un usuario o grupo de usuarios cualquiera. Esto permite

delegar la administración de subconjuntos estancos del dominio a ciertos usuarios que posean el nivel de responsabilidad adecuada.

Establecer de forma centralizada comportamientos distintos a usuarios y equipos. A cada unidad organizativa pueden vincularse políticas de grupo, que aplican comportamientos (generalmente en forma de restricciones) a los usuarios y equipos cuyas cuentas se ubican en dicha unidad. De esta forma, podemos aplicar restricciones distintas a subconjuntos de usuarios y equipos del dominio, en función exclusivamente de la unidad organizativa donde se ubican. Por ejemplo, podemos limitar a los usuarios del departamento de contabilidad para que sólo puedan utilizar ciertas aplicaciones, pero que esto no se aplique a los usuarios del departamento de informática.

2.5.3 Estructura Física de Active Directory

La estructura física de Active Directory define dónde y cuándo se producen el tráfico de replicación y de inicio de sesión. Una buena comprensión de los componentes físicos de Active Directory permite optimizar el tráfico de red y el proceso de inicio de sesión, así como solventar problemas de replicación.

Sitios: En Active Directory, los sitios se forman a través de la agrupación de múltiples subredes. Los sitios son generalmente definidos como lugares en los que el acceso de red es muy fiable, rápido y no muy caro.

Controladores de dominio: Un controlador de dominio (*Domain Controller*, DC) es un equipo donde se ejecuta Windows 2000 Server y que almacena una réplica del directorio. Los controladores de dominio ejecutan el servicio KDC, que es responsable de autenticar inicios de sesión de usuario.

La información almacenada en cada controlador de dominio en el almacén de directorios se divide en tres categorías (particiones): dominio, esquema y datos de configuración. Estas particiones del directorio son las unidades de replicación:

- **Partición de directorio de dominio**: contiene todos los objetos del directorio para este dominio. Los datos del dominio en cada dominio se replican a cada controlador de domino en este dominio, pero no más allá del dominio.

- **Partición del directorio de esquema**: contiene todos los tipos de objetos y atributos que pueden ser creados en el Active Directory. Estos datos son comunes a todos los dominios en el bosque. Por tanto los datos del esquema se replican a todos los controladores de dominio del bosque.

- **Partición de directorio de configuración**: contiene la topología de replicación y los metadatos. Por ejemplo, aplicaciones compatibles con Active Directory almacenan información en esta partición del directorio. Estos datos son comunes a todos los dominios en el bosque, y se replican a todos los controladores de dominio en el bosque.

Además de estas tres particiones de directorio de escritura, existe una cuarta categoría de información almacenada en un controlador de dominio: **el catálogo global.** Un catálogo global es un controlador de dominio que almacena las particiones de directorio de escritura, así como copias parciales de sólo lectura de todas las demás particiones de directorio de dominio del bosque.

2.5.4 Almacén de datos de Active Directory

El servicio de directorio de Active Directory utiliza un almacén de datos para toda la información de directorio. Este almacén de datos se suele denominar directorio. El directorio contiene información acerca de objetos como usuarios, grupos, equipos, dominios, unidades organizativas y directivas de seguridad. Esta información se puede publicar para que otros usuarios y administradores hagan uso de ella.

El directorio se almacena en controladores de dominio y las aplicaciones de red o los servicios tienen su acceso concedido. Un dominio puede tener uno o varios controladores de dominio. Cada controlador de dominio dispone de una copia del directorio en todo el dominio en el que está ubicado. Los cambios realizados en el directorio en un controlador de dominio se replican al resto de los controladores en el dominio, el árbol de dominios o el bosque. Active Directory utiliza cuatro tipos diferentes de particiones de directorio para almacenar y copiar distintas clases de datos. Las particiones de directorio contienen datos de dominio, configuración, esquema y aplicación. Este diseño de almacenamiento y replicación proporciona la información de directorio a los usuarios y administradores de todo el dominio.

Los datos del directorio se almacenan en el archivo Ntds.dit del controlador de dominio. Se recomienda almacenar este archivo en una partición NTFS. Para obtener más información acerca de la herramienta utilizada para administrar la base de datos y los archivos de registro de Active Directory, Los datos privados se almacenan de forma segura y los datos públicos del directorio se guardan en un volumen del sistema compartido, desde el que se pueden replicar a otros controladores del dominio. Para obtener más información acerca de la replicación.

Los datos de directorio replicados entre controladores de dominio incluyen la información siguiente:

- **Datos del dominio**

Los datos del dominio contienen información acerca de los objetos de un dominio. Se trata de información como contactos de correo electrónico, atributos de cuentas de

usuarios y equipos, así como recursos publicados que son de interés para administradores y usuarios.

Por ejemplo, cuando una cuenta de usuario se agrega a la red, un objeto de la cuenta de usuario y sus atributos se almacenan en los datos de dominio. Cuando se producen cambios en los objetos de directorio de la organización, como puede ser la creación de un objeto, su eliminación o la modificación de los atributos, estos datos se almacenan en los datos de dominio.

- **Datos de configuración**

Los datos de configuración describen la topología del directorio. Estos datos de configuración incluyen una lista de todos los dominios, árboles y bosques, así como las ubicaciones de los controladores de dominio y los catálogos globales.

- **Datos de esquema**

El esquema es la definición formal de todos los datos de objetos y atributos que se pueden almacenar en el directorio. Los controladores de dominio que ejecutan Windows Server 2003 incluyen un esquema predeterminado que define muchos tipos de objetos, como cuentas de usuarios y equipos, grupos, dominios, unidades organizativas y directivas de seguridad. Los administradores y los programadores pueden ampliar este esquema mediante la definición de nuevos tipos de objetos y atributos o bien con la adición de atributos nuevos para los objetos existentes. Los objetos del esquema están protegidos por listas de control de acceso, lo que asegura que sólo los usuarios autorizados puedan modificar el esquema.

- **Datos de aplicación.**

Los datos almacenados en la partición de directorio de aplicaciones son de utilidad en aquellos casos en los que se necesita replicar la información, pero no

forzosamente a escala global. De manera predeterminada, las particiones de directorio de aplicaciones no forman parte del almacén de datos del directorio. El administrador es el encargado de crearlas, configurarlas y administrarlas.

2.6 Controladores de Dominio

El **controlador de dominio** es el centro neurálgico de un dominio Windows, tal como un servidor NIS lo es del servicio de información de una red Unix. Los controladores de dominio tienen una serie de responsabilidades. Una de ellas es la autentificación. La autentificación es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña.

Cada controlador de dominio usa un **security account manager** (SAM), o NTDS en Windows 2003 Server (que es la forma promovida de la SAM, al pasar como Controlador de Dominio), para mantener una lista de pares de nombre de usuario y contraseña. El controlador de dominio entonces crea un repositorio centralizado de passwords, que están enlazados a los nombres de usuarios (un password por usuario), lo cual es más eficiente que mantener en cada máquina cliente centenares de passwords para cada recurso de red disponible.

En un dominio Windows, cuando un cliente no autorizado solicita un acceso a los recursos compartidos de un servidor, el servidor actúa y pregunta al controlador de dominio si ese usuario está autentificado. Si lo está, el servidor establecerá una conexión de sesión con los derechos de acceso correspondientes para ese servicio y usuario. Si no lo está, la conexión es denegada.

Un ordenador en el que se ejecute Windows 2003 puede desempeñar tres funciones distintas en una red:

- ***Controlador de dominio***. Es un servidor que se encarga de la seguridad de un dominio, es decir, administra toda la información correspondiente a usuarios y recursos de su dominio. Todo dominio necesita almenos un controlador.

- Servidor miembro. Es un equipo en el que se ejecuta Windows 2003 y pertenece al dominio, pero que no actúa como controlador de dominio. Puede realizar funciones de servidor de aplicaciones, de impresión, etc.

- Servidor independiente. Es cuando un servidor se incorpora a un grupo en lugar de a un dominio.

2.7 Introducción a las cuentas de usuarios

Las cuentas de usuario y las cuentas de equipo de Active Directory representan una entidad física como una persona o un equipo. Las cuentas de usuario también se pueden utilizar cómo cuentas de servicio dedicadas para algunas aplicaciones.

Las cuentas de usuario y de equipo (así como los grupos) se denominan también principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asigna automáticamente identificadores de seguridad (SID), que se utilizan para tener acceso a los recursos del dominio. Una cuenta de usuario o de equipo se utiliza para:

- **Autenticar la identidad de un usuario o equipo**. Una cuenta de usuario permite que un usuario inicie una sesión en equipos y dominios con una identidad que puede ser autenticada por el dominio. Para obtener información acerca de la autenticación. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Para aumentar la seguridad, debe evitar que varios usuarios compartan una misma cuenta.
- **Autorizar o denegar el acceso a los recursos del dominio.** Después de que el usuario haya sido autenticado, se le autoriza o deniega el acceso a los recursos

del dominio según los permisos explícitos asignados a dicho usuario en el recurso.

- **Administrar otros principales de seguridad**. Active Directory crea un objeto de principal de seguridad externo en el dominio local para representar cada principal de seguridad de un dominio de confianza externo. Para obtener más información acerca de los principales de seguridad externos,
-

2.7.1 Tipos de cuentas de usuarios

Existen dos tipos de cuentas de usuario:

Cuentas creadas por nosotros como administradores del dominio: Estas cuentas contienen información acerca del usuario, incluyendo el nombre y la contraseña del usuario, permiten que el usuario inicie una sesión en la red y, con los permisos apropiados, tenga acceso a los recursos de la red.

Cuentas predefinidas o incorporadas: Se trata de cuentas creadas durante la instalación de Windows NT. Estas cuentas son:

- **Invitado:** La cuenta incorporada Invitado se utiliza para ofrecer a los usuarios ocasionarles la posibilidad de iniciar sesiones y tener acceso a los recursos del dominio o equipo local. Por ejemplo, un empleado que necesite tener acceso al equipo durante un periodo breve de tiempo. La cuenta Invitado está deshabilitada de forma predeterminada. No se debe habilitar esta cuenta en una red de alta seguridad. Para mayor seguridad, cambie el nombre de esta cuenta y asígnele una contraseña.
- **Administrador:** La cuenta incorporada Administrador se utiliza para administrar la configuración global del equipo y del dominio. El Administrador puede realizar todas las tareas, como la creación o modificación de cuentas de usuario y de grupo, la administración de las directivas de seguridad, la creación de

impresoras, y la asignación de permisos y derechos a las cuentas de usuario para que tengan acceso a los recursos.

- **Otras cuentas:** Dependiendo de las aplicaciones instaladas pueden aparecer más cuentas predefinidas.

2.7.2 Creación de cuentas de usuarios

Se pueden crear cuentas de usuario de dominio (globales) o cuentas de usuario local.

Cuenta de usuario de dominio: Una cuenta de usuario de dominio se crea mediante el *Administrador de usuarios para dominios*. Cuando se crea una cuenta de usuario en un dominio, la cuenta de usuario se crea siempre en la base de datos del directorio maestro del PDC del dominio. En todos los controladores de reserva (BDC) se almacena una copia de la base de datos del directorio maestro (SAM). Una vez creada la cuenta de usuario en el PDC, un usuario puede iniciar la sesión en el dominio desde cualquier equipo de la red. Pueden pasar algunos minutos hasta que las copias de la base de datos del directorio de los BDC estén sincronizadas con el PDC; esto puede impedir que los usuarios con cuentas nuevas inicien una sesión.

Para sincronizar manualmente la base de datos en todos los controladores de dominio, utilizaremos el *Administrador de servidores*. Se pueden crear cuentas de usuario de dominio desde equipos que ejecuten Windows NT Workstation y Microsoft Windows 95 si instala las Herramientas de Windows NT Server. Las herramientas administrativas para Windows 95 y Windows NT Workstation están incluidas en el CD-ROM de instalación de Windows NT Server 4.0 en la ruta: \Clients\Srvtools\Win95 o \Clients\Srvtools\Winnt.

Cuenta de usuario local: Las cuentas de usuario locales se crean en un servidor miembro o en un equipo que ejecute Microsoft Windows NT Workstation, mediante el *Administrador de usuarios*. Cuando crea una cuenta de usuario local, se crea sólo en la

base de datos del directorio local del equipo. Con una cuenta de usuario local, un usuario puede iniciar una sesión y tener acceso únicamente a los recursos de dicho equipo.

2.7.3 Diseño de cuentas de usuarios

Para diseñar cuentas de usuario lo primero que tendremos que tener en cuenta es establecer una convención de nombres.

La convención de nombres establece cómo se identificará a los usuarios en la red. Una convención de nombres coherente hará que el administrador y los usuarios puedan recordar más fácilmente los nombres de los usuarios y encontrarlos en listas. Para determinar una convención de nombres, tendremos en cuenta lo siguiente:

1. Los nombres de usuario deben ser únicos. Si existe un gran número de usuarios, el diseño debe contar con la posibilidad de empleados con nombres duplicados, habrá que determinar un criterio a seguir para no asignar el mismo nombre de cuenta a dichos usuarios. Por ejemplo: José Fernández, JoseF y JoseFdz.
2. Los nombres de usuario pueden contener cualquier carácter en mayúsculas o minúsculas excepto los siguientes caracteres: “ / \ [ ] : ; =, + * ¿ < >. Podemos utilizar una combinación de caracteres especiales y alfanuméricos en la convención de nombres de usuario para facilitar la identificación de los usuarios.

2.7.4 Proteger cuentas de usuarios

Si un administrador de red no modifica ni deshabilita los derechos y permisos de las cuentas integradas, cualquier usuario o servicio malintencionado podría usarlos para iniciar una sesión, de manera ilegal, en un dominio mediante la identidad Administrador o Invitado. Una práctica recomendable de seguridad para proteger estas cuentas consiste en cambiar sus nombres o deshabilitarlas. Dado que una cuenta de usuario con el nombre cambiado conserva su identificador de seguridad (SID), conserva también todas las demás propiedades, como su descripción, la contraseña, la pertenencia al grupo, el perfil de usuario, la información de cuenta y todos los permisos y derechos de usuario asignados.

Para obtener la seguridad que proporciona la autenticación y autorización de usuarios, cree una cuenta de usuario individual para cada usuario que participe en la red, mediante Usuarios y equipos de Active Directory. Cada cuenta de usuario, incluidas las cuentas Administrador y Invitado, puede agregarse a un grupo para controlar los derechos y permisos asignados a la cuenta. Al usar las cuentas y grupos apropiados para la red se garantiza que los usuarios que se conectan a una red se puedan identificar y sólo puedan tener acceso a los recursos permitidos.

Puede contribuir a defender su dominio contra posibles intrusos exigiendo contraseñas seguras e implementando una directiva de bloqueo de cuentas. Las contraseñas seguras reducen el riesgo de suposiciones inteligentes y ataques de diccionario contra las contraseñas.

2.8 Introducción a los grupos

Un grupo es una recopilación de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una unidad individual. Los usuarios y los equipos que pertenecen a un grupo determinado se designan miembros del grupo.

La utilización de grupos permite simplificar las tareas de administración, ya que se asigna un conjunto común de permisos y derechos a varias cuentas, en vez de tener que asignarlos a cada cuenta de manera individual.

Los grupos pueden estar basados en directorios o ser locales en un equipo concreto. Los grupos de Active Directory son objetos de directorio que residen en un dominio y en objetos contenedores de unidades organizativas. Active Directory proporciona un conjunto de grupos predeterminados tras su instalación, pero también permite crear grupos nuevos.

Los grupos locales son aquellos que se encuentran en equipos locales y no en Active Directory. Se tratan en Grupos locales predeterminados.

Los grupos en Active Directory permiten:

- Simplificar la administración con la asignación de permisos de un recurso compartido a un grupo y no a usuarios individuales. Así se asigna el mismo acceso al recurso para todos los miembros del grupo.
- Delegar la administración con una única asignación de derechos de usuario a un grupo mediante la Directiva de grupo y después agregar al grupo los miembros necesarios que desee que tengan los mismos derechos.
- Crear listas de distribución de correo electrónico.

2.8.1 Ámbito de grupo

Los grupos se caracterizan por su ámbito y tipo:

Cualquier grupo, ya sea un grupo de seguridad o un grupo de distribución, se caracterizan por tener un ámbito que identifica el alcance de aplicación del grupo en el árbol de dominios o en el bosque. El límite, o el alcance, de un ámbito de grupo también está determinado por la configuración de nivel funcional de dominio del dominio en el que se encuentra. Existen tres ámbitos de grupo: universal, global y dominio local.

En la tabla siguiente se describen las diferencias entre los ámbitos de cada grupo.

Ámbito de grupo	**El grupo puede incluir como miembros…**	**Al grupo se le pueden asignar permisos en…**	**El ámbito de grupo se puede convertir a…**
Universal	• Las cuentas de cualquier dominio del bosque en el que se encuentra este grupo universal • Los grupos globales de cualquier dominio del bosque en el que se encuentra este grupo universal • Los grupos universales de cualquier dominio del bosque en el que se encuentra este grupo universal	Cualquier dominio o bosque	• Dominio local • Global (siempre que no exista otro grupo universal como miembro)
Global	• Las cuentas del mismo dominio que el grupo global principal • Los grupos globales del mismo dominio que el grupo global principal	Los permisos de miembro se pueden asignar en cualquier dominio	Universal (siempre que no sea miembro de otro grupo global)
Dominio local	• Cuentas de cualquier dominio • Grupos globales de cualquier dominio • Grupos universales de cualquier dominio • Grupos locales de dominio pero sólo del mismo dominio que el grupo local de dominio principal	Los permisos de miembro sólo se pueden asignar en el mismo dominio que el grupo local de dominio principal	Universal (siempre que no exista otro local de dominio como miembro

Tabla 3.- Diferencias de los ámbitos de cada grupo

2.8.2 Tipos de grupo

Los grupos se utilizan para reunir las cuentas de usuario, las cuentas de equipo y otras cuentas de grupo en unidades administrables. Al trabajar con grupos en lugar de usuarios individuales se simplifica el mantenimiento y la administración de la red.

Hay dos tipos de grupos en Active Directory: **grupos de distribución y grupos de seguridad.** Puede utilizar los grupos de distribución para crear listas de distribución de correo electrónico y los grupos de seguridad para asignar permisos a los recursos compartidos.

Grupos de distribución

Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Exchange) para enviar correo electrónico a grupos de usuarios. Los grupos de distribución no tienen habilitada la seguridad, lo que significa que no se pueden incluir en las listas de control de acceso discrecional (DACL). Si necesita un grupo para controlar el acceso a los recursos compartidos, cree un grupo de seguridad.

Grupos de seguridad

Si se utilizan adecuadamente, los grupos de seguridad suponen un modo eficaz de asignar el acceso a los recursos de su red. Los grupos de seguridad permiten:

- **Asignar derechos de usuario a grupos de seguridad en Active Directory** Los derechos de usuario se asignan a los grupos de seguridad para determinar qué acciones pueden llevar a cabo los miembros del grupo en el ámbito de un dominio (o bosque). Los derechos de usuario se asignan automáticamente a varios grupos de seguridad durante la instalación de Active Directory para facilitar a los administradores la definición de la función administrativa de un usuario dentro del dominio. Por ejemplo, un usuario que se agrega al grupo Operadores de copia en Active Directory puede restaurar y hacer copias de seguridad de los archivos y directorios ubicados en cada controlador del dominio. Esto es posible porque, de manera predeterminada, los derechos de usuario para Hacer copias de seguridad de archivos y directorios y Restaurar archivos y

directorios se asignan automáticamente al grupo Operadores de copia de seguridad. Por tanto, los miembros de este grupo heredan los derechos de usuario asignados al grupo.

- **Asignar permisos a grupos de seguridad en recursos**. Los permisos no se deben confundir con los derechos de usuario. Los permisos se asignan al grupo de seguridad en el recurso compartido. Los permisos determinan qué usuarios pueden tener acceso al recurso y el nivel de acceso, como Control total. Algunos de los permisos establecidos en los objetos de dominio se asignan automáticamente para permitir varios niveles de acceso a los grupos de seguridad predeterminados, como el grupo Operadores de cuentas o Administradores del dominio. Para obtener más información acerca de los permisos, vea Control de acceso en Active Directory.

Los grupos de seguridad se muestran en las DACL que definen los permisos sobre recursos y objetos. Los administradores deben asignar los permisos para recursos (archivos compartidos, impresoras, etc.) a un grupo de seguridad, no a usuarios individuales. Así los permisos se asignan una vez al grupo en lugar de varias veces a cada usuario individual. Cada cuenta agregada al grupo recibe los derechos asignados a ese grupo en Active Directory y los permisos definidos para el grupo en el recurso.

2.8.3 Grupos predeterminados

Los grupos predeterminados, como el grupo Administradores de dominio, son grupos de seguridad que se crean automáticamente al crear un dominio de Active Directory. Estos grupos predefinidos permiten controlar el acceso a los recursos compartidos y delegar funciones administrativas específicas en todo el dominio.

2.9 Introducción a las directivas

La configuración de la Directiva de grupo define los distintos componentes del entorno de escritorio del usuario que un administrador del sistema necesita administrar, como los programas que están disponibles a los usuarios, los que aparecen en el escritorio del usuario y las opciones del menú Inicio. Las opciones de Directiva de grupo que especifique se incluyen en un objeto de Directiva de grupo que, a su vez, se asocia a los objetos de Active Directory seleccionados: sitios, dominios o unidades organizativas.

La Directiva de grupo no sólo se aplica a los usuarios y a los equipos cliente, sino también a los servidores miembro, a los controladores de dominio y a cualquier otro equipo Windows Server 2003 dentro del ámbito de administración. De forma predeterminada, la Directiva de grupo que se aplica a un dominio (es decir, la que se aplica en el nivel de dominio justo encima de la raíz de Usuarios y equipos de Active Directory) afecta a todos los equipos y usuarios del dominio. Usuarios y equipos de Active Directory proporciona también una unidad organizativa integrada llamada Controladores de dominio. Si almacena aquí sus cuentas de controlador de dominio, puede utilizar el objeto de Directiva de grupo Directiva predeterminada de controladores de dominio para administrar los controladores de dominio independientemente de los demás equipos.

Los objetos de Directiva de grupo se vinculan a los contenedores de sitio, dominio y unidad organizativa en Active Directory. El orden de prioridad predeterminado sigue el orden jerárquico de Active Directory: primero los sitios, luego los dominios y después cada unidad organizativa. Un objeto de Directiva de grupo puede estar asociado a varios contenedores de Active Directory, o varios contenedores pueden estar vinculados a un único objeto de Directiva de grupo.

La Directiva de grupo incluye opciones de directiva para Configuración de usuario, que afectan a los usuarios, y para Configuración del equipo, que afectan a los equipos.

Con la Directiva de grupo, puede hacer lo siguiente:

Un objeto de directiva de grupo (GPO: Group Policy Object) 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
- Etc.

Se definen dos categorías de tipos troncales de directivas:

1. Según su **función**
2. Según su **objeto de configuración**

Directivas según su función

Hay dos tipos troncales de directivas según su función:

1. **Directivas de seguridad**: ¿Cuántos caracteres tiene una contraseña? ¿Cada cuánto tiempo debe ser cambiada ésta?, etc. Pueden ser aplicadas:

    a. ***A nivel de dominio***: Son aplicadas en todas las máquinas del dominio.
    b. ***A nivel de controladores de dominio***: Se aplican tan sólo en los controladores de dominio, pero sin suplantar a las del dominio (en caso de entrar en contradicción una y otra, se aplica la del dominio, no la de los controladores de dominio).

2. **Directivas de Entorno (GPO -> Group Policy Object)**: ¿Quién tiene acceso al panel de control? ¿Cuál es el tamaño máximo del archivo de registro de sistema? Pueden ser aplicadas:
    a. A nivel de **equipo local**
    b. A nivel de **sitio**
    c. A nivel de **dominio**

d. A nivel de **Unidad Organizativa (OU)**.

Directivas según el objeto al que configuran

Respecto al objeto al que configuran también son dos:

e. **Configuración del equipo**: que se divide en:
   i. Configuración de **software**
   ii. Configuración de **Windows**
   iii. **Plantillas** administrativas

f. **Configuración del usuario**, que al igual que la de Windows se divide en:
   i. Configuración de **software**
   ii. Configuración de **Windows**
   iii.
   iv. Plantillas **administrativas**

Las **GPO's pueden estar contenidas en cuatro tipos de objetos:**

1. **Equipos Locales**: son aplicadas únicamente en el equipo que las tiene asignadas independientemente del dominio al que pertenezcan. Son modificadas con "gpedit.msc". Estas son las únicas políticas que se aplican a los equipos que no están en un dominio, como servidores independientes (stand alone) o clientes en red igual a igual (peer to peer).
2. **Sitios de Active Directory**: se aplican para todos los equipos y/o usuarios de un sitio, independientemente del dominio del mismo bosque al que pertenezcan.
3. **Dominios de Active Directory**: se aplican a todos los equipos y/o usuarios de un dominio.
4. **Unidades Organizativas de Active Directory**: se aplican únicamente a los equipos y/o usuarios que pertenezcan a la propia unidad organizativa (OU)

2.9.1 Propiedades de una GPO

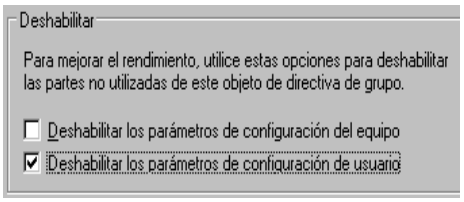
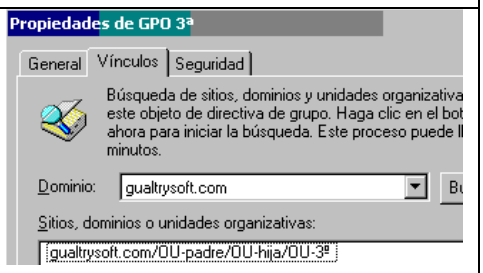
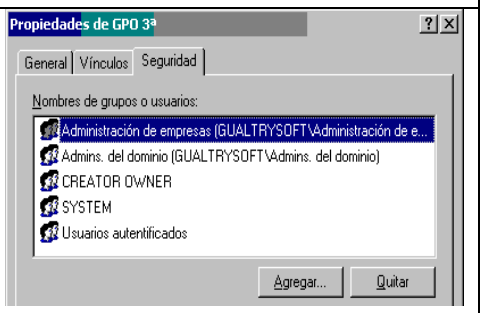
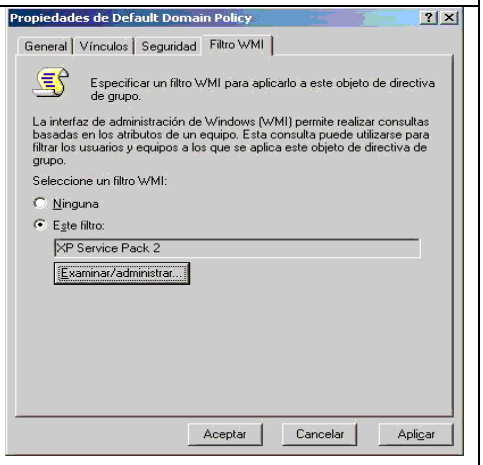
Pestaña	Función	Captura
General	Muestra información sobre la GPO y permite deshabilitar toda la rama de configuración del equipo y/o toda la rama de configuración de usuario. Esto sirve para agilizar la aplicación de la GPO, mejorando el rendimiento. Como en nuestro caso la política que obliga a hacer CTRL+ALT+SUPR para iniciar sesión es una configuración de equipo, podremos marcar la casilla que deshabilita los parámetros de configuración de usuario.	
Vínculos	Permite buscar los sitios, dominios y OU's en los que está agregada la GPO. Con el desplegable "Dominio" podemos seleccionar el dominio del bosque en el que buscamos.	
Seguridad	Sirve para establecer los permisos de la GPO'. Podemos asignar permisos a los siguientes objetos: 1. Usuarios 2. Equipos 3. Grupos 4. Principios de seguridad incorporados	
Filtro WMI	Sirve para realizar búsquedas basadas en WMI de características específicas de los equipos a los que se aplica la GPO. Estas características pueden ser: 1. Un patrón de nombre de equipo 2. Tipo de Sistema Operativo 3. Nivel de Service Pack 4. Cualquier característica del equipo que podamos consultar con WQL Los equipos con Windows 2000 ignoran este tipo de filtros y procesan las GPOs sin tener en cuenta si por sus características deberían hacerlo o no. Por ello, una forma de ejecutar políticas que sólo se apliquen a equipos con Windows 2000 es filtrar con WMI poniendo que el tipo de SO es Windows 2000 o que el tipo de SO no es Windows XP. Si queremos aplicar políticas con filtros WMI a equipos con tan sólo XP o 2003, será necesario que nos llevemos las cuentas de los Windows 2000 a otra OU en la que no estarán vinculadas esas GPOs.	

Tabla 4.- propiedades de una GPO

Pestaña "Seguridad"

La pestaña "***Seguridad***" nos permite realizar dos tareas con las GPO's:

1. **Filtrar el alcance de la GPO**, permitiendo que sea sólo aplicada a los usuarios, equipos, grupos y/o Principios de seguridad incorporados (objetos "Builtin", etc.).
2. **Delegar el control de la GPO**, permitiendo así la modificación, etc., a determinados usuarios, equipos, grupos y/o Principios de seguridad incorporados.

Hay que tener en cuenta que *esto se hace sobre toda la GPO*, no se puede especificar únicamente a algunas políticas de la GPO, si no que se hace para todas las contenidas en la GPO.

Para realizar el filtrado del alcance y la delegación del control se utilizan permisos que se aplican a los objetos en que están especificados. Estos permisos pueden ser concedidos o denegados, prevaleciendo la denegación sobre la concesión. De forma predeterminada estas son las entradas de seguridad de una GPO (se indican aquellos permisos que están, concedidos):

Grupo de seguridad	***Configuración predeterminada***
Usuarios autentificados	Leer, aplicar directiva de grupo y permisos adicionales
CREATOR OWNER	Permisos adicionales
Administradores del Dominio	Leer, escribir, crear todos los objetos secundarios, eliminar todos los objetos secundarios y permisos adicionales
Administración de empresas	Leer, escribir, crear todos los objetos secundarios, eliminar todos los objetos secundarios y permisos adicionales
SYSTEM	Leer, escribir, crear todos los objetos secundarios, eliminar todos los objetos secundarios y permisos adicionales

Tabla 5.- Permisos que se aplican a los objetos.

2.10 Introducción al complemento editor de objetos de directiva de grupo (GPMC)

La Consola de administración de Directivas de grupo (GPMC) de Microsoft es una nueva herramienta para la administración de Directivas de grupo que ayuda a los administradores a administrar una empresa de forma más rentable al mejorar la capacidad de administración y aumentar la productividad. Consta del nuevo complemento Microsoft Management Console (MMC) y de un conjunto de interfaces programables mediante secuencias de comandos.

GPMC simplifica la administración de la Directivas de grupo al proporcionar un único lugar para administrar aspectos esenciales de la Directiva de grupo. Atiende los requisitos principales de implementación de la Directiva de grupo exigidos por los clientes mediante las siguientes funciones.

- Una interfaz de usuario (IU) que simplifica enormemente el uso de la Directiva de grupo.
- Operaciones de copia de seguridad/restauración de objetos de Directiva de grupo.
- Operaciones de importar/exportar y copiar/pegar objetos de Directiva de grupo y filtros del Instrumental de administración de Windows (WMI).
- Administración simplificada de la seguridad relacionada con la Directiva de grupo.
- Informes HTML (Lenguaje de marcado de hipertexto) de la configuración de objetos de Directiva de grupo y datos del Conjunto resultante de directivas (RSoP).
- Secuencias de comandos de tareas relacionadas con directivas expuestas dentro de esta herramienta (y no de la configuración de un objeto de Directiva de grupo).

Hasta ahora, los administradores necesitaban utilizar varias herramientas de Microsoft para administrar la Directiva de grupo, como los complementos Usuarios y equipos de Active Directory, Sitios y servicios de Active Directory y Conjunto resultante

de directivas. GPMC integra las funciones de Directiva de grupo existentes en estas herramientas en una única consola unificada con nuevas capacidades.

Una característica integrada en GPMC es la compatibilidad para administrar varios dominios y bosques, lo que permite a los administradores administrar la Directiva de grupo de toda la empresa. Los administradores tienen un control total sobre los bosques y dominios incluidos en GPMC, lo que permite mostrar únicamente las partes pertinentes de un entorno.

2.11 Configurar directivas de contraseñas con objetos de Directiva de grupo

En Windows 2000, Windows XP y Windows Server 2003 se pueden configurar seis opciones relacionadas con las características de contraseñas: **Forzar el historial de contraseñas**, **Vigencia máxima de la contraseña**, **Vigencia mínima de la contraseña**, **Longitud mínima de contraseña**, **Las contraseñas deben cumplir los requerimientos de complejidad** y **Almacenar contraseñas usando cifrado reversible**. Para obtener ayuda sobre cómo determinar los valores de estas opciones adecuados a los requisitos del negocio de su organización, consulte **Seleccionar contraseñas seguras** (en inglés) en el sitio Web de Instrucciones de seguridad de Microsoft.

- **Forzar el historial de contraseñas** determina el número de contraseñas nuevas exclusivas que un usuario debe utilizar para poder volver a usar una contraseña antigua. El valor de esta opción puede estar comprendido entre 0 y 24; si se establece en 0, se deshabilita la opción de forzar el historial de contraseñas. Para la mayoría de las organizaciones, este valor debe estar establecido en 24 contraseñas.

- **Vigencia máxima de la contraseña** determina el número de días que un usuario puede utilizar una contraseña antes de que se le obligue a cambiarla. El valor de esta opción puede estar comprendido entre 0 y 999; si se establece en 0, las contraseñas no caducan nunca. La definición de un valor bajo para esta opción puede resultar frustrante para los usuarios, y si el valor es demasiado alto o se deshabilita la opción, los piratas informáticos dispondrán de más tiempo para averiguar las contraseñas. Para la mayoría de las organizaciones, este valor debe estar establecido en 42 días.

- **Vigencia mínima de las contraseñas** determina el número de días que un usuario puede conservar una nueva contraseña hasta que pueda cambiarla. Esta opción está diseñada para utilizarla junto con la opción puede estar comprendido entre 0 y 999; si se establece en 0, las contraseñas no caducan nunca. La definición de un valor bajo para esta opción puede resultar frustrante para los usuarios, y si el valor es demasiado alto o se deshabilita la opción, los piratas informáticos dispondrán de más tiempo para averiguar las contraseñas. Para la mayoría de las organizaciones, este valor debe estar establecido en 42 días.

  Forzar el historial de contraseñas, de forma que los usuarios no puedan restablecer rápidamente sus contraseñas tantas veces como sea necesario para luego cambiar a sus contraseñas antiguas. El valor de esta opción puede estar comprendido entre 0 y 999; si se establece en 0, los usuarios podrán cambiar inmediatamente sus nuevas contraseñas. El valor recomendado es dos días.

- **Longitud mínima de la contraseña** determina el número mínimo de caracteres que puede tener una contraseña. Aunque Windows 2000, Windows XP y Windows Server 2003 admiten contraseñas de hasta 28 caracteres de longitud, el valor de esta opción sólo puede estar comprendido entre 0 y 14. Si se establece en 0, los usuarios podrán

tener contraseñas en blanco, por lo que no debe utilizar este valor. El valor recomendado es 8 caracteres.

- **Las contraseñas deben cumplir los requerimientos de complejidad** determina si la complejidad de las contraseñas es obligatoria. Si se habilita esta opción, las contraseñas de los usuarios deben satisfacer los siguientes requisitos:
  - La contraseña debe tener seis caracteres como mínimo.
  - La contraseña contiene caracteres de al menos tres de las cinco clases siguientes:
    - Caracteres en mayúsculas del alfabeto inglés (A – Z)
    - Caracteres en minúsculas del alfabeto inglés (a – z)
    - Dígitos en base 10 (0 – 9)
    - Caracteres no alfanuméricos (por ejemplo: !, $, # o %)
    - Caracteres Unicode
  - La contraseña no contiene tres o más caracteres del nombre de cuenta del usuario.
  - Si el nombre de cuenta es menor de tres caracteres de longitud, esta comprobación no se realiza porque la probabilidad de que se rechazaran las contraseñas es demasiado alta. Cuando se comprueba el nombre completo del usuario, varios caracteres se tratan como delimitadores que separan el nombre en elementos individuales: comas, puntos, guiones, caracteres de subrayado, espacios, signos de libra esterlina y tabuladores. Se buscará en la contraseña todos los elementos que tengan una longitud de tres o más caracteres. Si se encuentra alguno, se rechazará el cambio de contraseña. Por ejemplo, el nombre "Susana F Medrano" se dividiría en tres elementos: "Susana", "F" y "Medrano". Como el segundo elemento sólo tiene un carácter, se omite. Por tanto, este usuario no podría tener una contraseña que incluyera "Susana" o "Medrano" como una subcadena en la contraseña. En todas estas comprobaciones no se distingue entre mayúsculas y minúsculas.
  - Estos requisitos de complejidad se exigen al cambiar la contraseña o al crear una nueva. Se recomienda que habilite esta opción.

2.12 Introducción a Windows XP Professional

Windows XP Professional proporciona un nuevo estándar en confiabilidad y desempeño. Este sistema operativo está diseñado para negocios de todos tamaños y para usuarios que demandan el máximo desempeño de su experiencia informática. Tomando como punto de partida el ya probado sistema operativo Windows 2000, Windows XP Professional representa una base de total confianza que mantendrá los equipos en perfecto funcionamiento siempre que sea necesario. Windows XP es más confiable y, además, contribuye a una más fácil recuperación tras problemas en el sistema. Las características de seguridad de Windows XP Professional protegen los datos confidenciales en su equipo y en el momento de transmitirlos a través de una red o Internet. Windows XP dispone de los estándares de seguridad y la protección antivirus más recientes, con los que ofrece protección contra algunos de los tipos de ataque a través de Internet más comunes. Desde su aspecto claro y renovado a sus diseños intuitivos y basados en tareas, Windows XP Professional simplifica al máximo el uso de su PC. Hará más en menos tiempo, encontrará lo que busca en un instante y organizará los archivos y carpetas como más le convenga. En otras palabras, Windows XP Professional le ayuda a trabajar de forma más inteligente

2.12.1 Características de Windows XP Professional

CARACTERISTICAS	DESCRIPCION
Cuentas de usuario protegidas	Es posible crear cuentas separadas para cada una de las personas que utiliza un PC. Crea un juego independiente de carpetas para almacenar los archivos y las configuraciones de cada usuario (Mis documentos, Favoritos, Menú Inicio, etc.)
Protección contra intrusos	Incluye un firewall básico que impide el acceso de intrusos por Internet. Otra función útil para evitar intrusos es un sistema de encriptación de archivos
Restauración del sistema	Restauración del sistema, que permite devolver el sistema a un estado previo en caso de que se presente una falla grave.
NTFS, un sistema de archivos más sólido	NTFS es la mejor opción; es más sólido, más seguro y facilita la recuperación de los archivos en caso de fallas.
Sólo para computadores recientes	Un PC bien dotado XP es más rápido que los Windows anteriores. La profunda renovación tecnológica de Windows XP trae grandes beneficios a los usuarios de PC. Sin embargo, tiene un lado negativo: sólo los PC recientes pueden instalar Windows XP
Menor compatibilidad	Según Microsoft, XP es compatible con 90 por ciento de los 1.500 programas más populares para Windows 98 y ME XP soporta por ahora 12.000 dispositivos de hardware. Si una aplicación no es compatible, Windows XP tiene un truco que podría hacer que funcione: le hace creer que está trabajando con una versión anterior de Windows. Esta función se llamada Modo de compatibilidad, pero no es ciento por ciento efectiva.
La instalación es más complicada	El primer paso antes de instalar XP es verificar si es compatible con el hardware y software del PC; esta comprobación se realiza mediante una utilidad incluida en el CD-ROM de XP.

Defensa antipiratería	Windows XP tiene una característica nueva que combate la piratería: la activación. Lo que hace ese sistema es revisar los componentes del PC y enviar a Microsoft un informe. Con base en esos datos, Microsoft tiene una especie de 'huella digital' de su PC. Si después se trata de instalar esa misma copia de Windows XP en otro PC, Microsoft sabrá que se trata de una instalación ilegal y la rechazará.
Actualizaciones posibles	Windows XP Professional, se puede actualizar desde Windows 98 (o 98 SE), Windows ME, Windows NT 4.0 Workstation o Windows 2000 Professional.

Tabla 6.- Características de Windows XP Professional

12.2.2 Requerimientos para la instalación de Windows XP Professional

El PC recomendado por Microsoft para usar Windows XP debe tener un procesador con una velocidad de reloj de 300 MHz hacia arriba, 128 MB de memoria RAM y 1,5 gigabytes (GB) de espacio libre en el disco duro.

2.13 Introducción a los sistemas de monitoreo de red

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, cada vez más, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez más importante y de carácter pro-activo para evitar problemas y mejorar la calidad del servicio que se brinda a los usuarios de las distintas redes.

El término Monitoreo de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Con las herramientas de los sistemas de monitoreo de redes, se pueden analizar:

- Control de desempeño de la red
- Monitoreo del Consumo de ancho de banda
- Monitoreo de Protocolos en la red
- Monitoreo del uso de Internet

2.13.1 Introducción a RADMIN 3.2

Radmin es un software de acceso y control remoto seguro que permite trabajar sobre un equipo remoto como si estuviera sentado delante, y tener acceso desde varias ubicaciones. Radmin incluye plena compatibilidad con Windows 7 (32-bit y 64-bit), transferencia de archivos, charlas de texto y voz multiusuario, seguridad Windows, acceso telnet, varios monitores y la tecnología única DirectScreenTransfer™. Radmin utiliza el omnipresente protocolo TCP/IP, el protocolo más extendido y utilizado en LAN y WAN e Internet. Significa poder tener conexión remota a un PC desde cualquier parte del mundo. Radmin se utiliza en miles de PC corporativos de todo el mundo.

Características del software:

- Control remoto
- Visualización remota
- Transferencia de archivos
- Charla de voz y texto
- Encendido, reinicio, acceso a la configuración de BIOS remoto de un equipo remoto con el NUEVO soporte Intel AMT.
- Funciona a través de Internet o LAN
- La sencilla interfaz permite instalar y configurar Radmin en unos pocos clics.

Entre la cantidad de herramientas que tiene Radmin, se destacan:

El poder gestionar archivos entre la máquina origen y la máquina a controlar, puedes ver el disco duro de la máquina conectada a la red como si estuvieras frente al mismo ordenador (esto es ideal, para no tener que andar de aquí para allá con pendrives moviendo archivos).

El poder controlar el otro equipo completamente, en vivo y en directo, como una máquina virtual, con tan solo tipear la IP correspondiente, y ingresar el usuario y contraseña, puedes manejar el otro ordenador (con teclado y mouse), como si fuera en el que estás sentado, esto es ideal, para el que maneja un cyber y además de curiosiar, puede dar soporte a los usuarios que tienen problemas, sin siquiera enfriar su banco.

Además es posible ver el otro equipo en modo stealth (oculto), con milésimas de segundo de diferencia.

Entre tantas características espectaculares, es posible enviar un mensaje directo al PC correspondiente, apagar el PC, entrar en su shell.

Un programa de control remoto espectacular para el hogar, cyber o compañías grandes, en las que se necesita supervisar a los usuarios.

Radmin Server 3 requiere la activación tras el período de prueba de 30 días. **Radmin Viewer 3** es gratuito y no requiere activación. Si no activa el software de servidor, no podrá utilizarlo tras los 30 días. Para efectuar la activación, es necesario seguir el proceso de activación. Tras la adquisición de una licencia, debe recibir un número de serie personal. Utilícelo para activar Radmin Server 3.

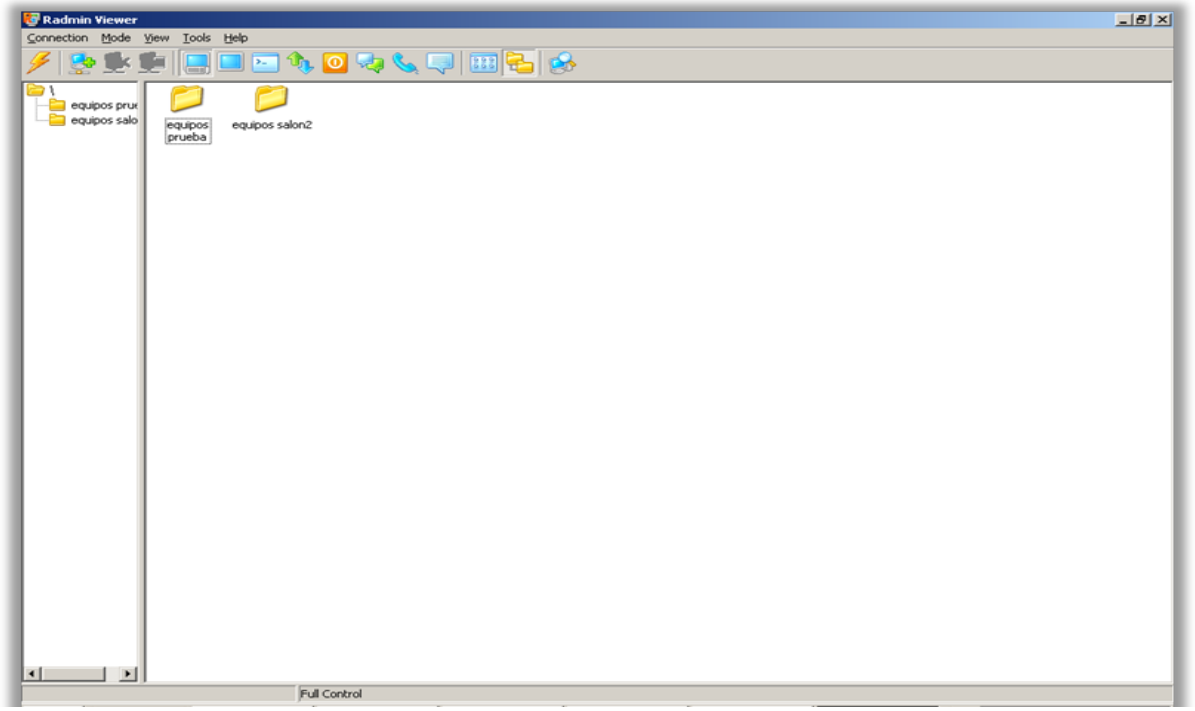


Figura 1.- interfaz de Radmin Viewer 3.2

2.13.1 Introducción a OBSERVER

Observer es un analizador de protocolos, rico en características especiales, flexibles y fáciles de usar. Un administrador de redes o un técnico del área de soporte, sabe que, un analizador de protocolos es una herramienta necesaria para cuando se presentan problemas en la red o cuando necesita saber que tan bien o tan ocupada está la red.

Observer le permite introducirse al nivel de paquetes individuales hasta obtener vistas generales de la actividad de la red. Ofreciendo gran diversidad de niveles de revisión. Descubre e identifica los nodos de la red, monitorea los nodos descubriendo su disponibilidad y rendimiento, decodifica protocolos, produce estadísticas útiles de las actividades que se realizan en la red, ayuda a resolver problemas y reporta el status actual de los dispositivos de la red y sus conexiones.

Observer va de lo general a lo particular en varios aspectos de la red, permitiéndole, filtrar el tráfico basado en direcciones de la red, tipos de protocolo y otros criterios de selección.

Observer acelera el diagnóstico de un problema en la red, revelando la naturaleza del problema, ubicación e impacto. Relacionado la actividad actual con una línea de base de actividad normal previamente capturada, se convierte en parte de la caja de herramientas de planeación informándole de sus tendencias y cambios.

Características particulares de observer, para el análisis y monitoreo de redes:

- Gran capacidad de interpretación y decodificación de protocolos (>500)
- Utiles comentarios del sistema experto
- Gran versatilidad y facilidad de manejo de ventanas para determinar problemas
- La excelente utilidad, facilidad y claridad de sus reportes

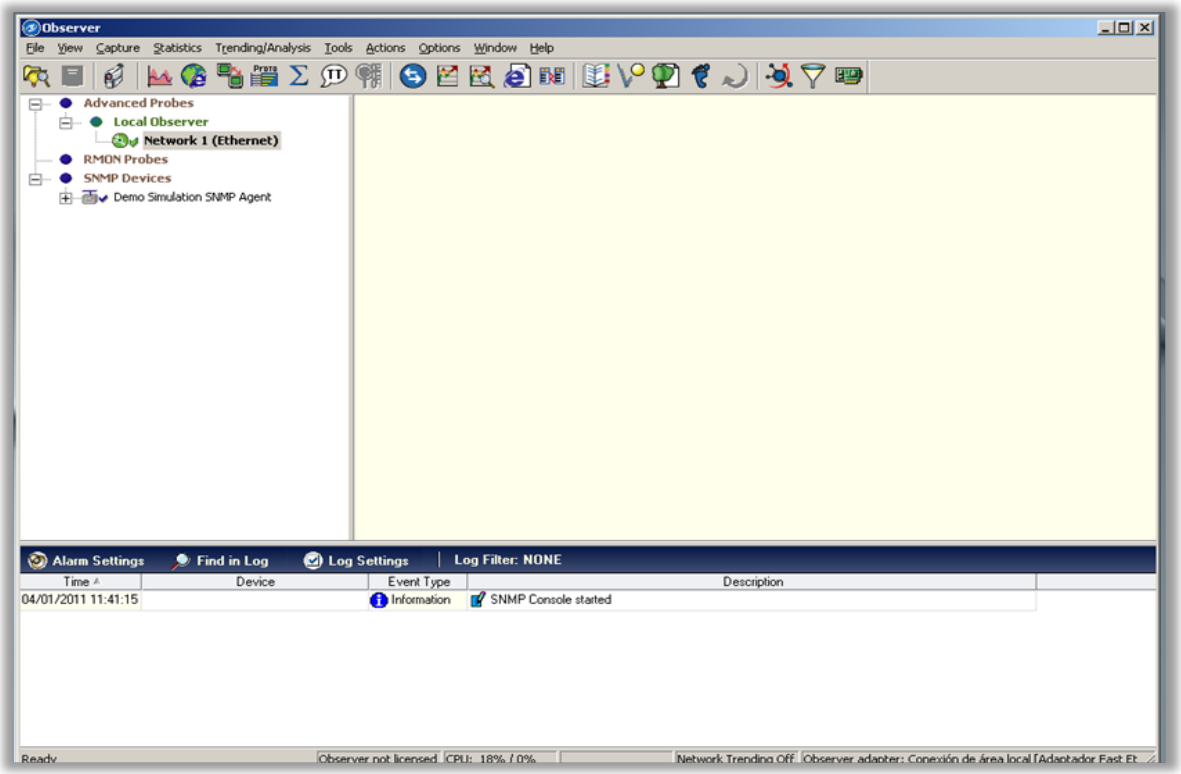


Figura 2.- Interfaz de OBSERVER

2.13.3 Introducción a System Surveillance Pro v5.5

SSPro es un todo en una solución de software de seguimiento. Una herramienta esencial para los padres preocupados con la actividad en línea y los administradores de redes que deseen controlar el uso de la computadora de su empleado, registros de pulsaciones de teclado introducidas SSPro, ejecutar programas, sitios web visitados, mensajes instantáneos, fotos de la pantalla y mucho más! Configurar correo electrónico SSPro de las características de datos para enviar fotos de la pantalla y registra fuera del sitio para ver a distancia. SSPro de características incorporadas de la palabra clave pornográficos permiten a los usuarios bloquear y / o ser notificado cuando se encuentra contenido objetable. ¿Quieres definir sus propias palabras clave? No hay problema, SSPro permite que, con demasiada SSPro página web también incluye bloqueo selectivo / filtrado de Internet, controlar la programación, puesta en relación selectiva, los informes HTML actividad, advertencias de usuario opcionales, los límites de uso del

programa, y la configuración de varios equipos en red. Muy fácil de configurar y utilizar, SSPro soporta la mayoría de programas de chat y los navegadores como AIM, AOL, Yahoo, MSN, ICQ, GoogleTalk, IE, Netscape, Firefox y muchos más. Simple keyloggers (capturadores de teclado)

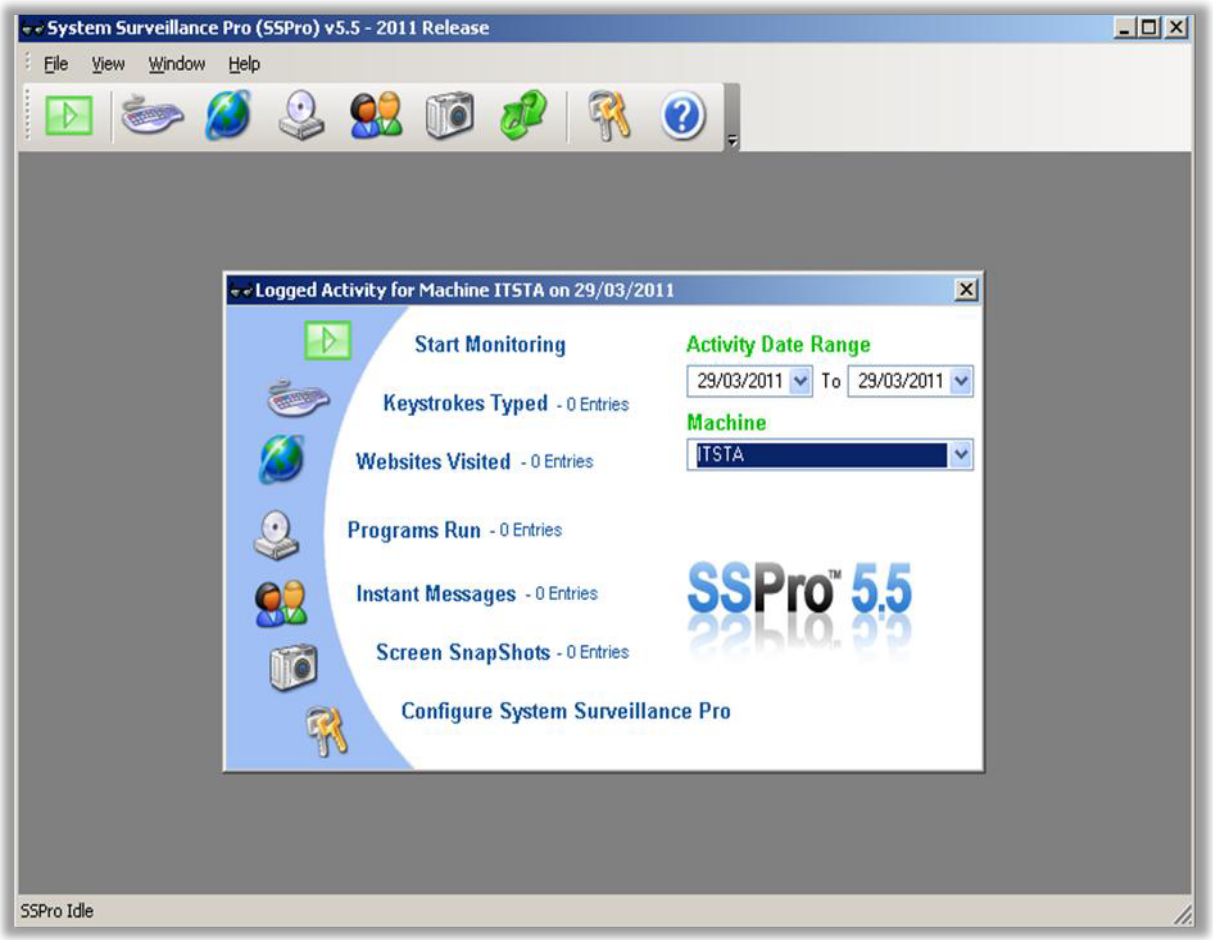


Figura 3.- interfaz de SSPRO v5.5

2.13.4 Diferencias de los sistemas de monitoreo de red

Radmin 3.2

Tipo Licencia:	El Radmin server es de paga y el Radmin Viewer es gratuito.
Tiempo de periodo de prueba:	30 días
Interfaz:	Amigable
Compatibilidad de sistemas operativos:	Windows Vista/XP/2008/2003/2000 (32-bit) y Windows Vista/XP/2008/2003 (64-bit).
Facilidad de uso:	Excelente facilidad de uso
Herramientas que presentan:	✓ Visualización remota ✓ Transferencia de archivos ✓ Charla de voz y texto ✓ Encendido, reinicio, acceso a la configuración de BIOS remoto. ✓ Funciona a través de Internet o LAN ✓ La sencilla interfaz permite instalar y configurar Radmin en unos pocos clics.

Tabla 7. - Caracteristicas de RADMIN 3.2

Observer

Software libre o de paga:	Tiempo de periodo de prueba
Tiempo de periodo de prueba:	Trial
Interfaz:	Amigable
Compatibilidad de sistemas operativos:	Windows
Facilidad de uso:	Buena facilidad de uso
Herramientas que presentan:	✓ Descubre e identifica los nodos de la red. ✓ Puede monitorear desde un simple segmento hasta multisegmentos en redes LAN, Wireless, LANs y WANs, una vez que se haya actualizado el software a las versiones más completas. ✓ Monitorea los nodos descubriendo su disponibilidad y rendimiento decodifica protocolos. ✓ Produce estadísticas útiles de las actividades que se realizan en la red. ✓ Ayuda a resolver problemas y reporta el status actual de los dispositivos de la red y sus conexiones. ✓ La excelente utilidad, facilidad y claridad de sus reportes. ✓ La sencilla interfaz permite instalar y configurar Radmin en unos pocos clics.

Tabla 8.- Características de OBSERVER

System Surveillance pro v5.5

Software libre o de paga:	De paga
Tiempo de periodo de prueba:	8 días
Interfaz:	Amigable
Compatibilidad de sistemas operativos:	Windows
Facilidad de uso:	Excelente facilidad de uso
Herramientas que presentan:	✓ Soporta la mayoría de programas de chat y los navegadores como AIM, AOL, Yahoo, MSN, ICQ, GoogleTalk, IE, Netscape, Firefox y muchos más. ✓ Key loggers (capturador de pantalla)

Tabla 9.- Características de SSPRO v.5.5

CAPÍTULO III. MARCO OPERATIVO

3.1 Instalación de Windows Server 2003

3.2 Instalación de active Directory (Controlador de dominio)

3.3 Crear usuarios de dominio

3.4 Crear usuarios locales de Windows Server 2003

3.5 Crear Grupos

3.6 instalar y configurar GPMC

3.7 Configurar directivas de grupo

3.7.1 Como se crea una GPO

3.7.2 Como se elimina una directiva

3.7.3 Como se define un objeto de directiva de grupo

3.7.4 ¿Cómo se vincula una política ya existente?

3.7.5 Administrar objetos de directiva de grupos

3.7.5.1 Ver objetos de Directiva de grupo del dominio

3.7.5.2 Para ver objetos de Directiva de grupo asociados a un contenedor determinado

3.7.5.3 Para ver todos los objetos de Directiva de grupo asociados a un contenedor determinado

3.7.5.4 Buscar objetos de Directiva de grupo

3.7.5.5 Para buscar un objeto de Directiva de grupo específico mediante varios parámetros de búsqueda

3.7.5.6 Para ver las directivas que aplica un objeto de Directiva de grupo

3.8 Hacer una copia de seguridad y restaurar objetos de Directiva de grupo

3.8.1 Hacer una copia de seguridad de un objeto de Directiva de grupo

3.8.2 Para hacer una copia de seguridad del objeto Directiva de directiva alumnos del dominio

3.9 Administrar copias de seguridad

3.9.1 Para administrar las copias de seguridad de objetos de Directiva de grupo disponibles

3.10 Restaurar una copia de seguridad

3.10.1 Para restaurar el objeto Directiva de contraseñas del dominio

3.11 Administrar la directiva de grupo

3.12 Crear un grupo de trabajo en Windows XP Professional y/o unirse a él.

.

En el presente capítulo se dará a conocer la aplicación de las herramientas ya vistas en el capítulo anterior pero de manera visual. Cabe mencionar que antes de empezar con la instalación y configuración del servidor se debe de tener una estructura organizada del dominio. Posteriormente se describe detalladamente como fue desarrollado este proyecto.

3.1 Instalación de Windows Server 2003

Antes de instalar Windows Server 2003, complete las siguientes tareas:

- Verificar que todo el hardware esté listo.
- Verificar que los componentes cumplan el mínimo hardware requerido.
- Seleccionar el sistema de archivos para la partición, en cual instalará Windows Server 2003, a menos que usted necesite una configuración dual boot de formato usando NTFS.
- Determinar el nombre del dominio al que Usted quiere agregar o el workgroup que creará. Si va a usar un dominio, el nombre estará en formato DNS: server.domain (donde server es el nombre de su computadora y dominio es el nombre del dominio al cual pertenece su computadora). Si agrega a un workgroup, el nombre estará en formato (NetBIOS).
- Crear una cuenta de computadora en el dominio, usando el nombre de la computadora que Usted está instalando. Aunque un administrador de dominio puede crear una cuenta de computadora antes de la instalación, Usted puede crear también una cuenta de computadora durante la instalación si tiene privilegios administrativos suficientes en el dominio. Por defecto, los usuarios pueden crear hasta 10 cuentas de computadora en el dominio.
- Determinar la contraseña para la cuenta del Administrador local.

Figura 4.- Arranque del BIOS.

(1) En la BIOS se configura la secuencia de arranque, donde se incluirá el lector de CD-ROM Si el Hdd no estuviese vacío, es decir que tenga un s.o., entonces deberíamos ponerlo el primero en la secuencia.

(2) Acciones: Lo que va haciendo el programa de instalación, copiando archivos tales, cuales, etc.

Opciones: Además de la posible información, es posible, pulsando alguna tecla de Función (F2, F6, F5...) acceder a ciertas opciones durante la instalación.

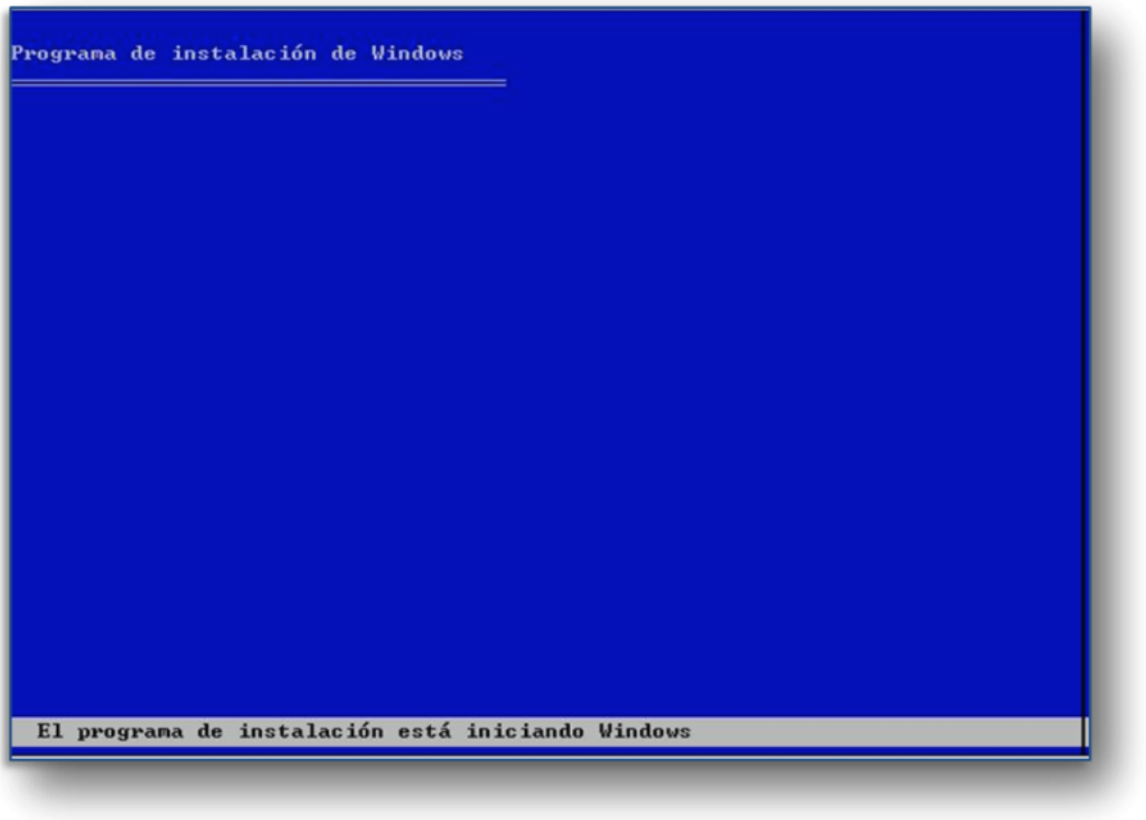


Figura 5.- Iniciando la Instalación de Windows

Aquí se nos muestra las tres posibilidades que el programa de instalación nos ofrece, La primera es la que elegiremos para continuar con la instalación. La segunda nos serviría en el caso de querer recuperar una instalación anterior, y se nos ofrecerán algunas alternativas. La tercera finalizará el proceso sin instalar w2k3

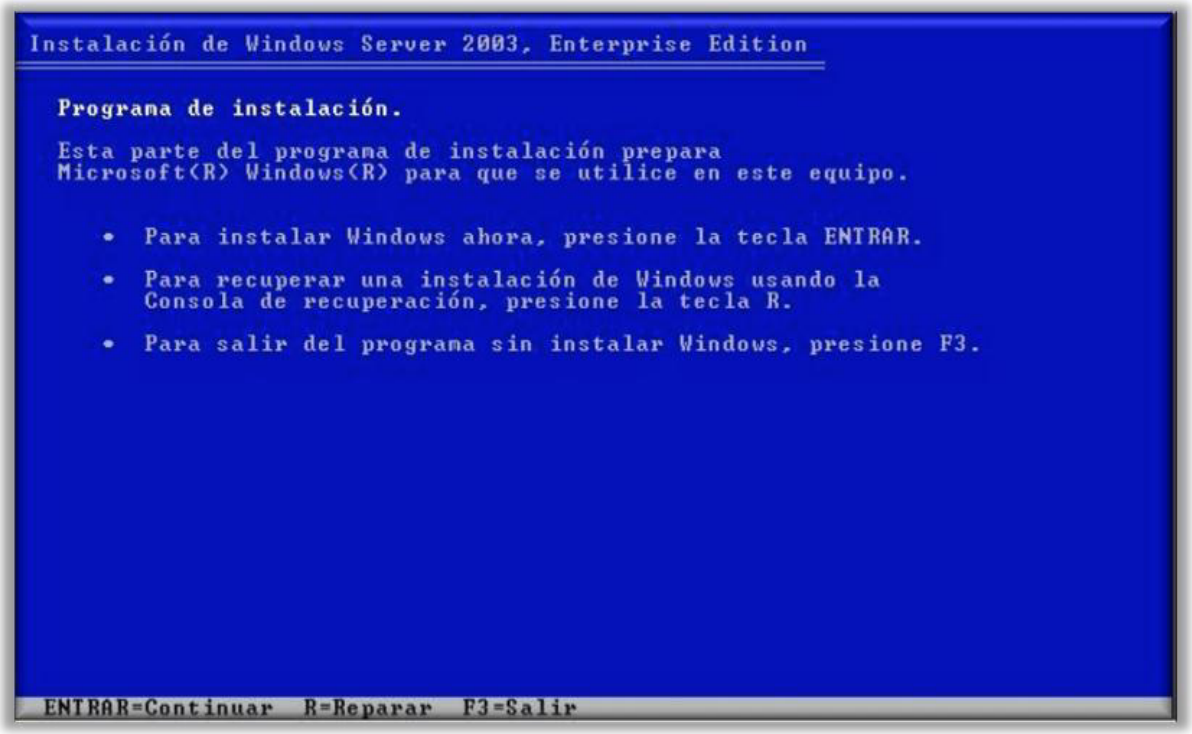


Figura 6.- Programa de Instalación

Se nos mostrará la licencia de uso del sistema, pulsaremos la tecla F8 para aceptarla y seguir con la instalación.

Aquí se nos muestra la información del espacio que tenemos, discos y particiones. En la imagen, un disco con 5114MB sin particiones. Podemos pulsar Entrar para instalar Windows en el espacio remarcado, o, escoger el resto de opciones para crear/eliminar particiones existentes.

Figura 7.- Contrato de Licencia

En la imagen siguiente nos muestra la información del espacio que tenemos, discos y particiones. En la imagen, un disco con 5114MB (ejemplo) sin particiones. Podemos pulsar Entrar para instalar Windows en el espacio remarcado, o, escoger el resto de opciones para crear/eliminar particiones existentes

.Figura 8.- Espacio del disco disponible

Figura 9.- Creación de una nueva partición

Después de utilizar “C” y seguir las indicaciones de dicha opción, hemos creado una partición en el espacio que teníamos. La remarcamos y pulsamos ENTRAR para instalar W2k3 en ella.

Ahora se nos solicita el formato del sistema de archivos, los marcados como rápidos servirían si las particiones existen y ya tienen montado un sistema de archivos, fat o ntfs respectivamente, y se borraría todo lo que contienen. Las otras dos montarían el sistema de archivos y formatearían la partición con el mismo. Lo mejor es elegir **NTFS**, sin ninguna duda, no debe perderse las posibilidades que nos ofrece este sistema en un servidor. Pulsaremos ENTRAR cuando lo tengamos elegido.

Figura 10.- Formateo de la unidad

Figura 11.- Progreso del formateo de la unidad.

Finalizada la comprobación, creará una lista de archivos para copiar.

Aquí nos muestra el progreso de copia de los archivos de la lista creada por el programa de instalación.

Figura 12.- progreso de copia de archivos creada por Windows

Al finalizar la copia nos indica que va a iniciar la configuración, desde el archivo que se nos indica en la barra inferior.

Figura 13.- El equipo se reiniciará automáticamente o pulsando nosotros mismos entrar.

Después de instalar las características de seguridad y configurar los dispositivos el Wizard le solicitará la siguiente información:

- Configuración Regional,
- Nombre y organización
- Product key (de 25 caracteres)
- Modo de Licenciamiento
- Nombre para la computadora y contraseña para la cuenta del Administrador local. Componentes opcionales de Windows Server 2003.
- Los dos minutos ya va por la instalación de dispositivos, aquí puede darnos una serie de pantallazos, cosa normal ya que estará instalando los controladores de la tarjeta gráfica/vídeo

Figura 14.- Finalización de Windows Server 2003, pulsando la secuencia de teclas indicada en la Imagen iniciaremos sesión.

3.2 Instalación de active directory

Nos vamos **inicio/Ejecutar** y escribimos **DCPROMO** para iniciar el asistente de instalación.

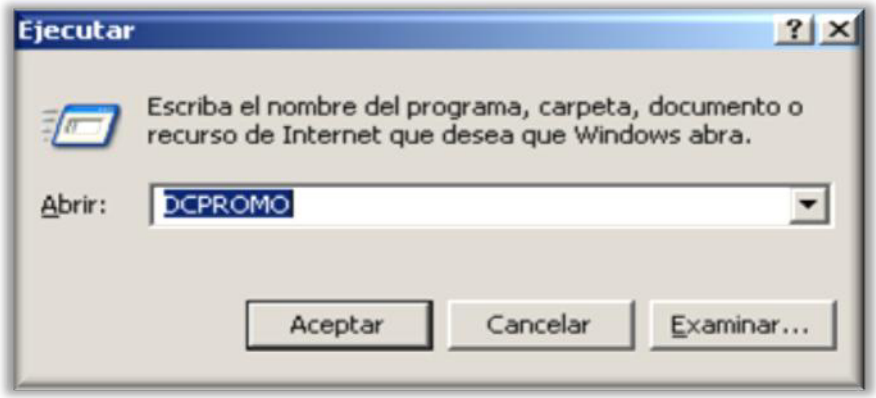


Figura 15.- Instrucción para iniciar el asistente.

Se nos inicia el asistente de instalación de Active Directory.

Figura 16.- Asistente de Active Directory

Figura 17.-Descripción de compatibilidad de sistemas operativos

Nos da la opción de crear un dominio nuevo o añadir un controlador adicional a un dominio existente. Nosotros vamos a crear un dominio nuevo por lo que escogeremos esta opción y seguiremos adelante. El servidor DNS tiene que estar disponible en la red para poder utilizar Active Directory. Podremos tener un servidor DNS distinto al controlador de dominio o agregar estas funciones al mismo servidor

18.- Figura Crear el nuevo dominio.

Llegado este punto deberemos indicar el nombre del dominio que estamos creando. Tenemos tres posibilidades a la hora de nombrar un dominio: utilizar el mismo nombre que el dominio que tenemos registrado en Internet, utilizar un subdominio de éste o utilizar un nombre distinto para el dominio de Windows. En nuestro caso el nombre de dominio será: *"midominioITSTA.local"*. Si en la red tenemos equipos con sistemas operativos antiguos, no van a reconocer el nombre del dominio tal como lo hemos escrito. Por lo tanto deberemos recurrir a su nombre Netbios, que en este caso es *MIDOMINIOITSTA.*

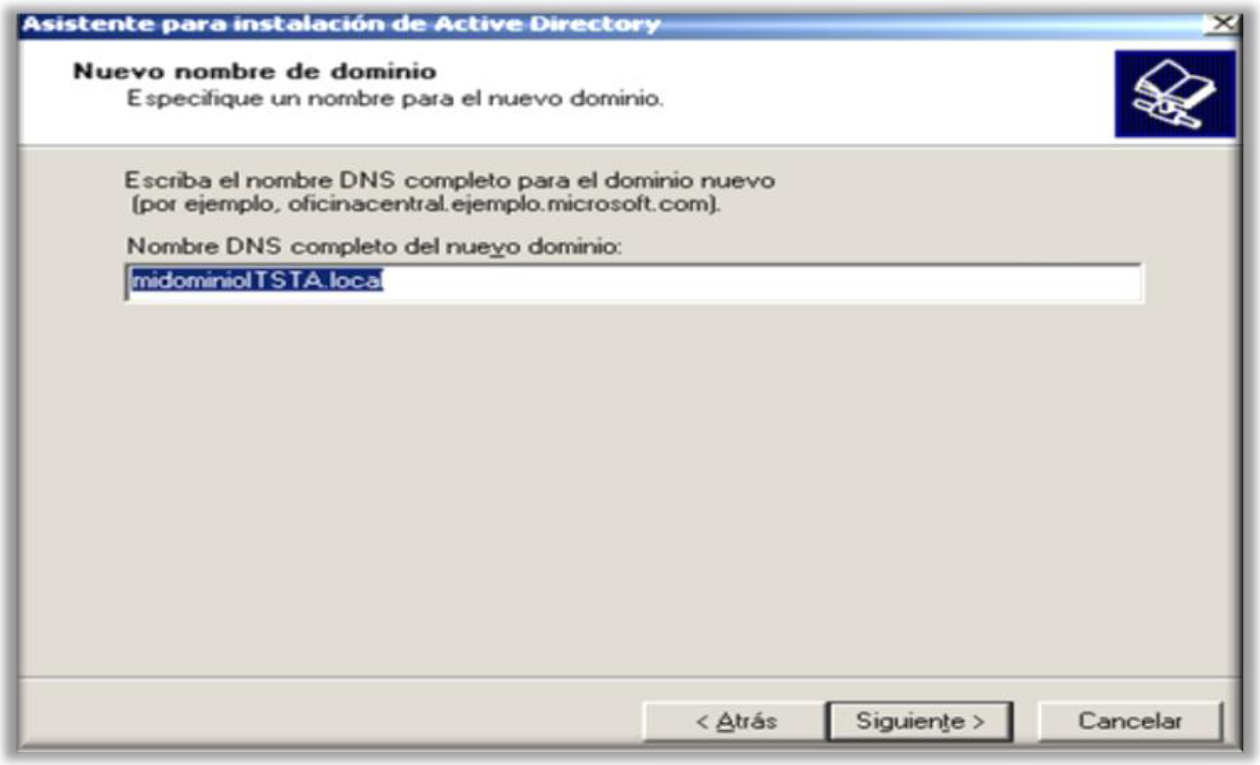


Figura19.- Nombre DNS para el dominio.

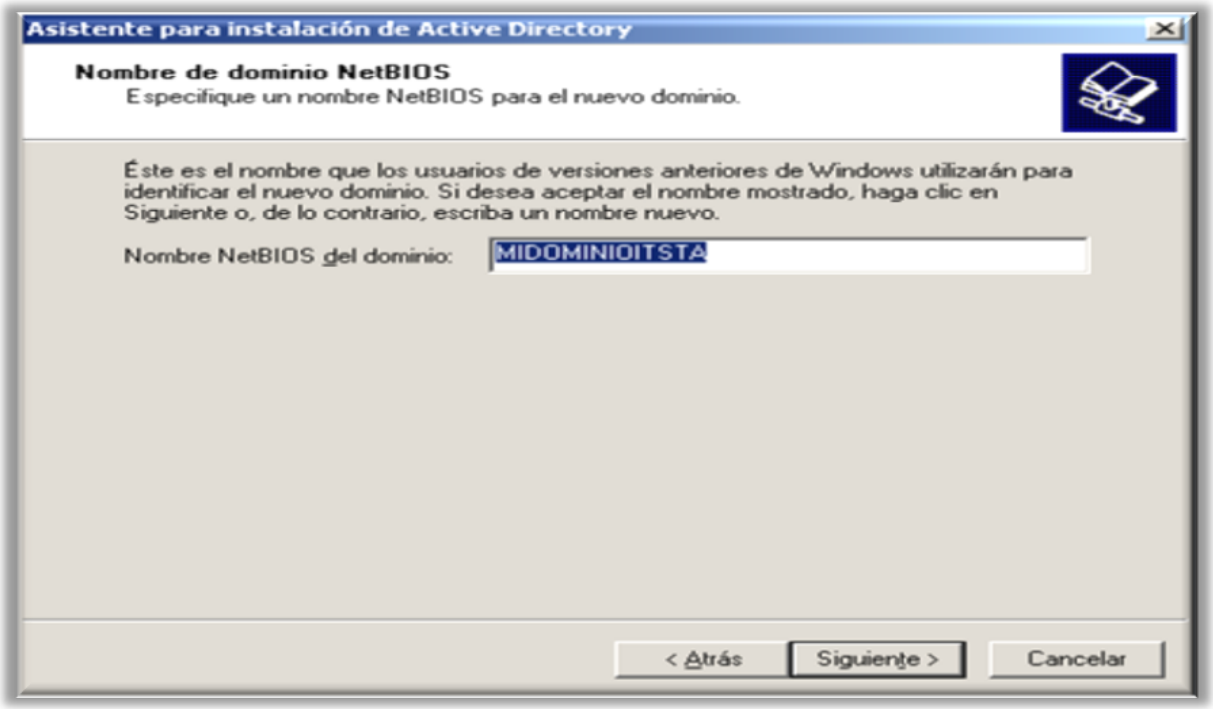


Figura 20.-Nombre NetBIOS del dominio

Nos crea la base de datos de Active directory. La localización por defecto es" *%Systemroot \Ntds*

Figura 21.- Ubicación para almacenar la base de Active Directory

Crea la carpeta compartida del volumen del sistema. Esta estructura se replica para todos los controladores de dominio. Contiene las siguientes carpetas: La carpeta compartida SYSVOL que contiene la información de las políticas de grupo y la carpeta compartida Net Logon, que contienen los logon scripts para computadoras en las que no esta instalado Windows 2003 Server. El lugar por defecto será:" *%Systemroot \SYSVOL "*

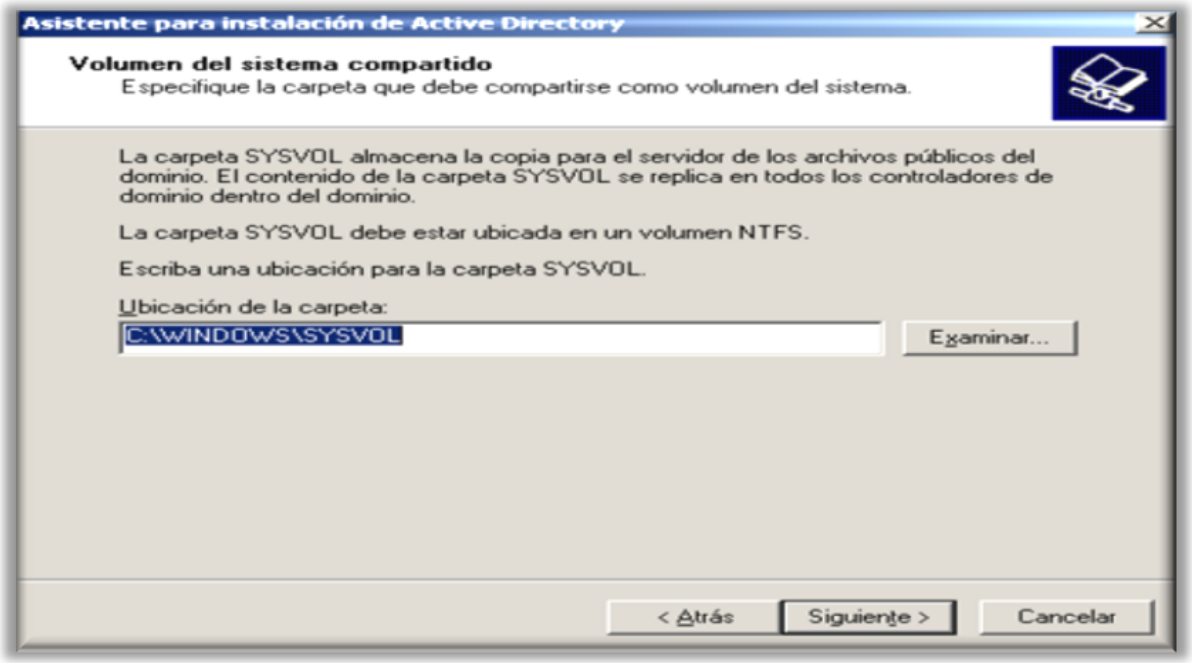


Figura 22.-Crear carpeta compartida del volumen del sistema

Nos aparecerá un error de diagnostico del servicio DNS. Elegiremos la última opción: *"Corregir el problema más adelante"*

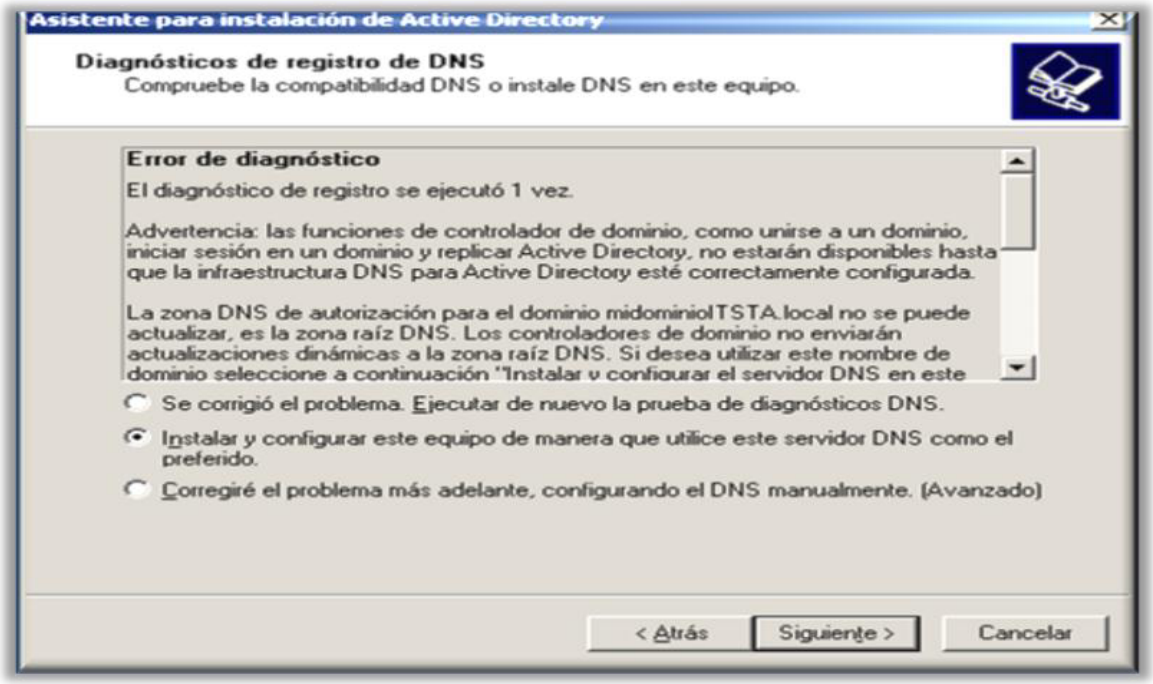


Figura 23.-Diagnostico e instalación del servicio DNS en el equipo.

En el siguiente paso deberemos introducir la contraseña del usuario Administrador que se utilizará en el caso que necesitamos restaurar el directorio. En este punto debemos tener un par de cosas claras:

1. Al instalar el sistema operativo, se crea el usuario Administrador del equipo (Administrador local) y se establece su contraseña.
2. Al crear el dominio, se crea la cuenta Administrador del dominio, cuya contraseña coincide con la del administrador local.
3. Además, se permite modificar la contraseña del administrador local, ya que será la que se utilice en el caso de que sea necesario restaurar el dominio. Esto es lógico, ya que, al restaurar el dominio, no puede estar funcionando el servicio Active directory, por lo que sólo podemos usar la cuenta del administrador local.

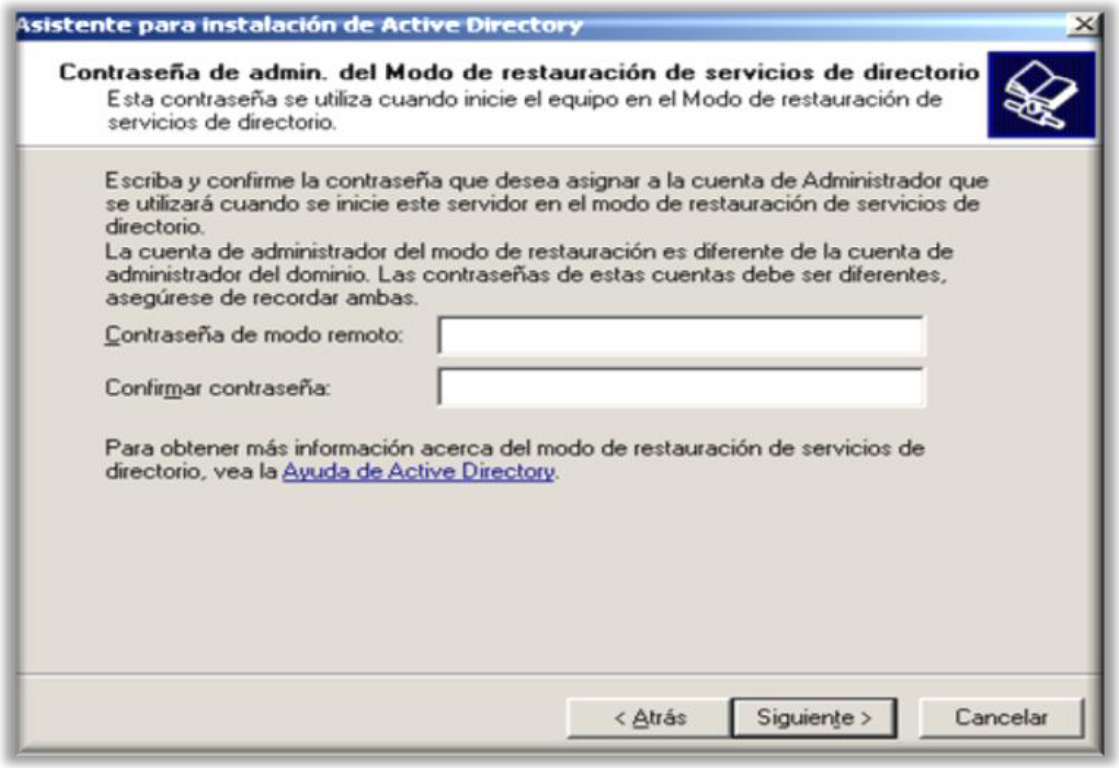


Figura 24.- Ingresar contraseña en modo de restauración del directorio.

El asistente nos mostrará un resumen de la configuración que hemos establecido en los pasos anteriores. Si alguna cosa no es correcta, este será el momento de corregirla. Dar clic en siguiente.

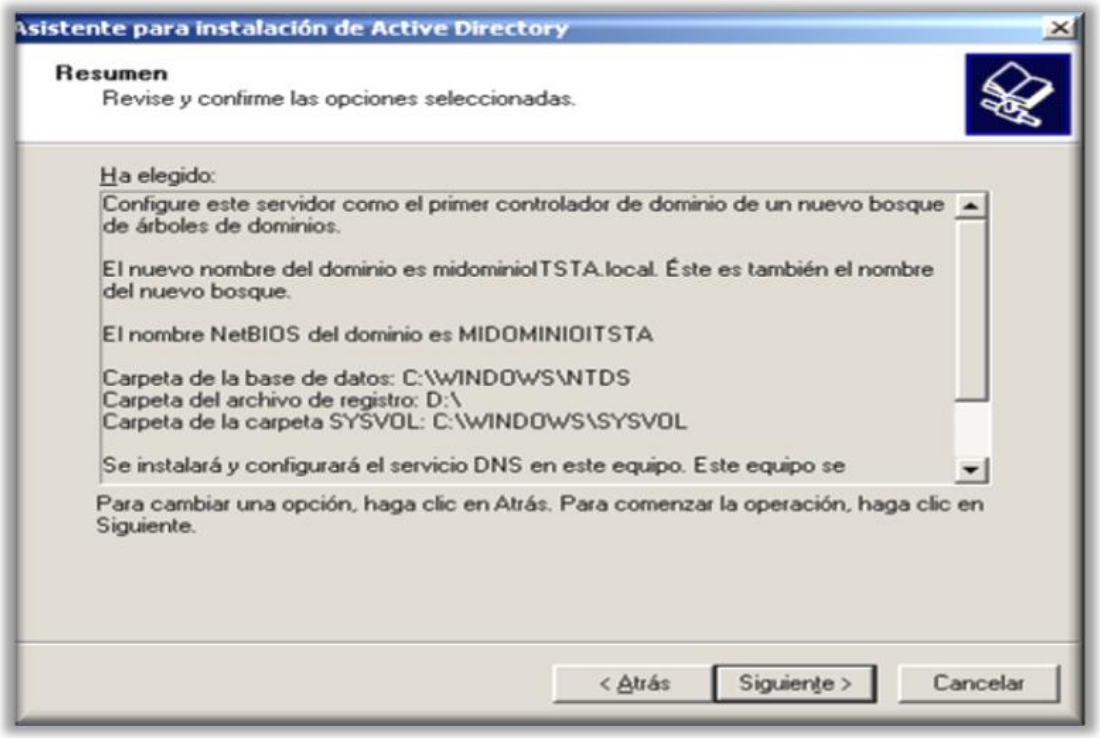


Figura 25.- Resumen de la configuración.

Figura 26.- Finalización del asistente para la instalación de Active Directory.

El Controlador de dominio estará instalado. Para comprobarlo podemos ir a *"Mis sitios de red"* y observar que nos aparece el dominio que hemos creado y que el único equipo que de momento tenemos es el servidor.

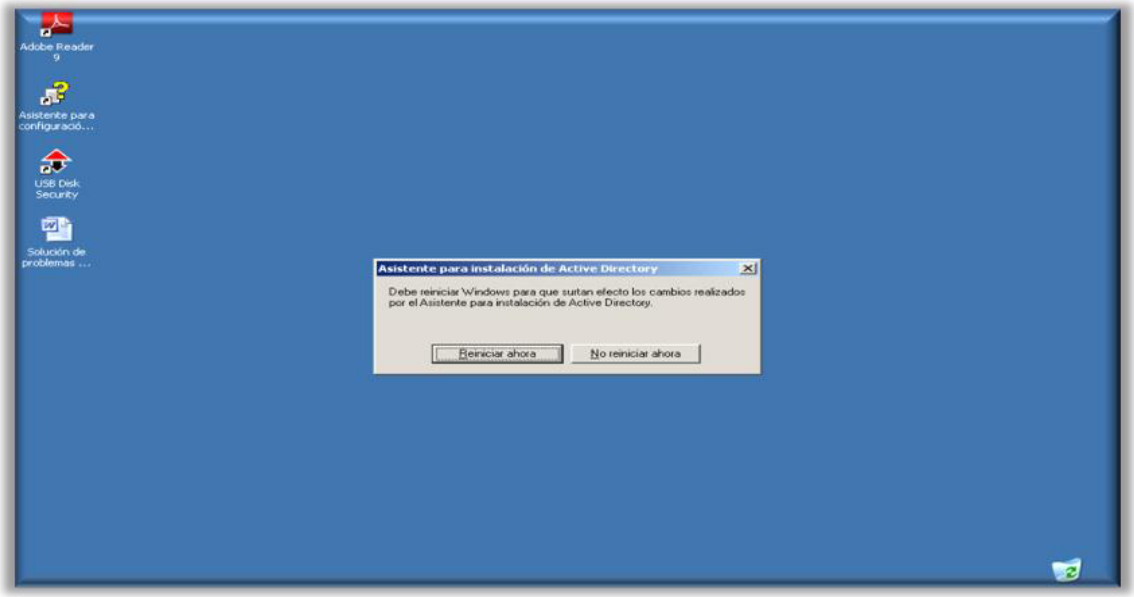


Figura 27.- Reiniciar el equipo.

3.3 Crear usuarios de dominio de Windows Server 2003

Hacer clic en Inicio, seleccionar Herramientas Administrativas y hacer clic en Usuarios y equipos de Active Directory

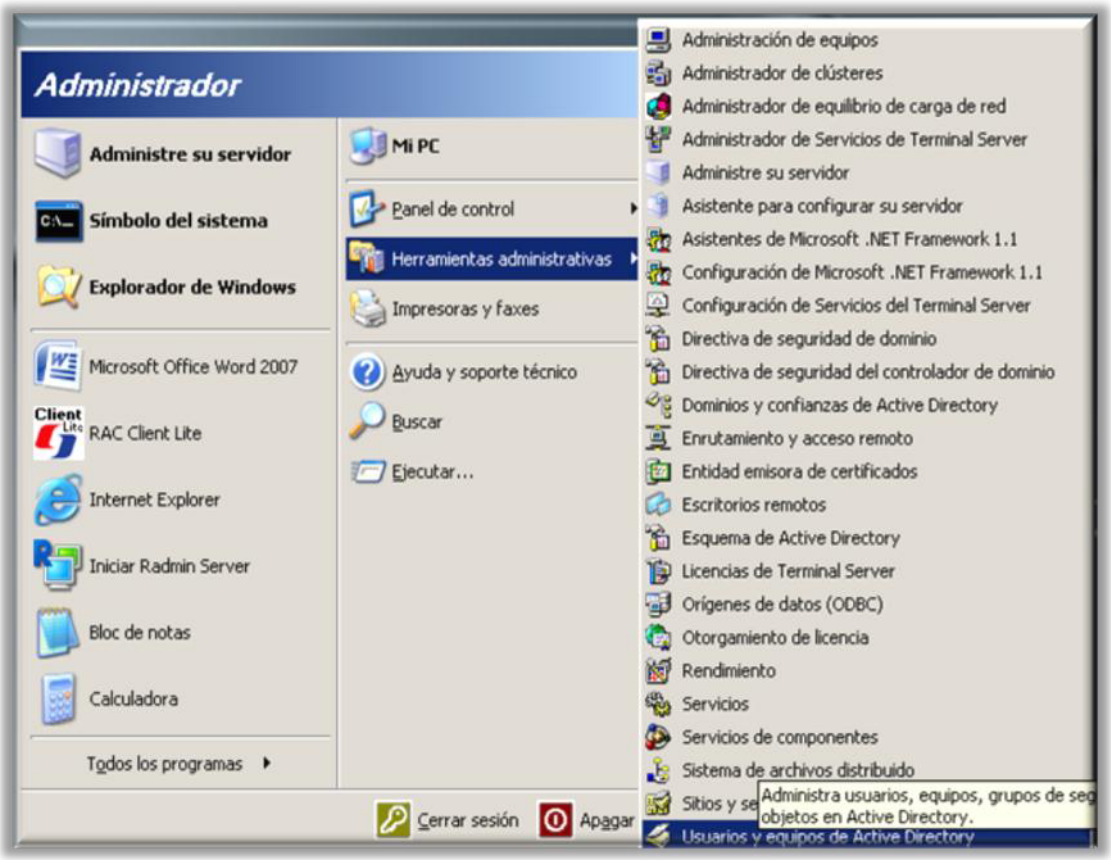


Figura 28.- abrir la ventana para crear usuarios

Hacer clic con el botón secundario del mouse (ratón) sobre el dominio, la Unidad Organizacional (OU) o contenedor donde se va a crear el usuario.

Seleccionar Nuevo y luego hacer clic en Usuario.

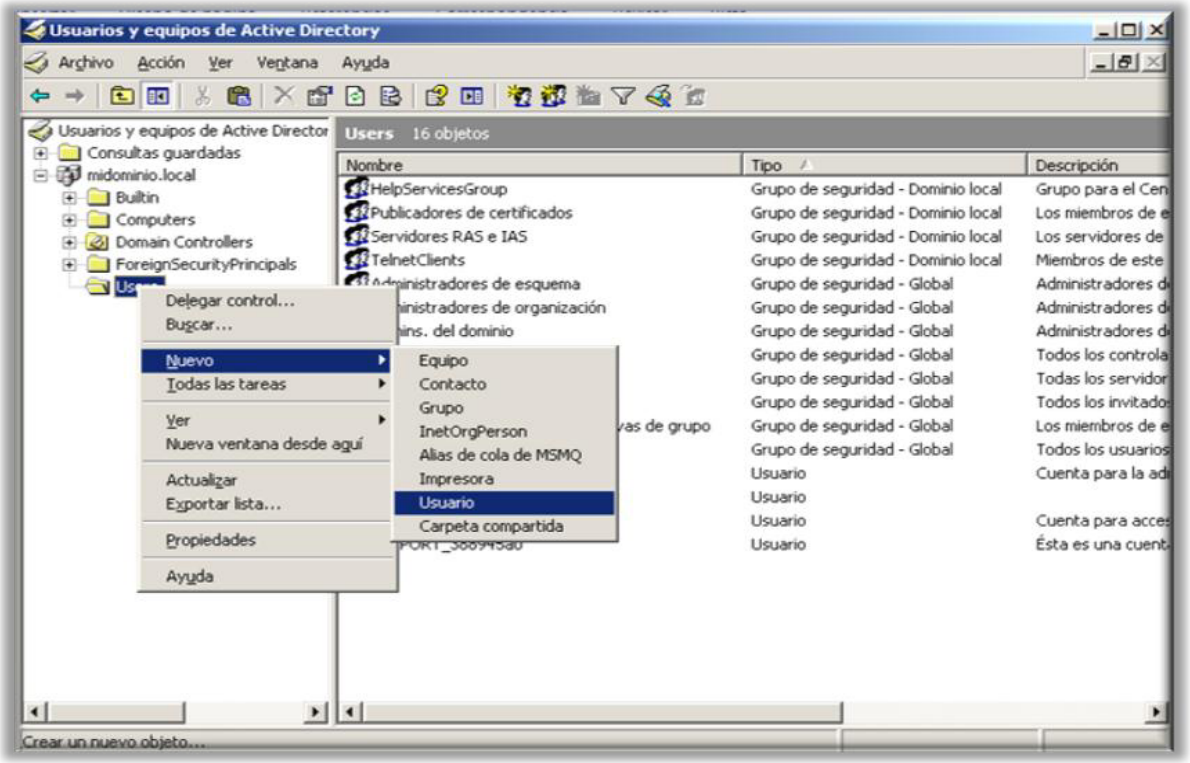
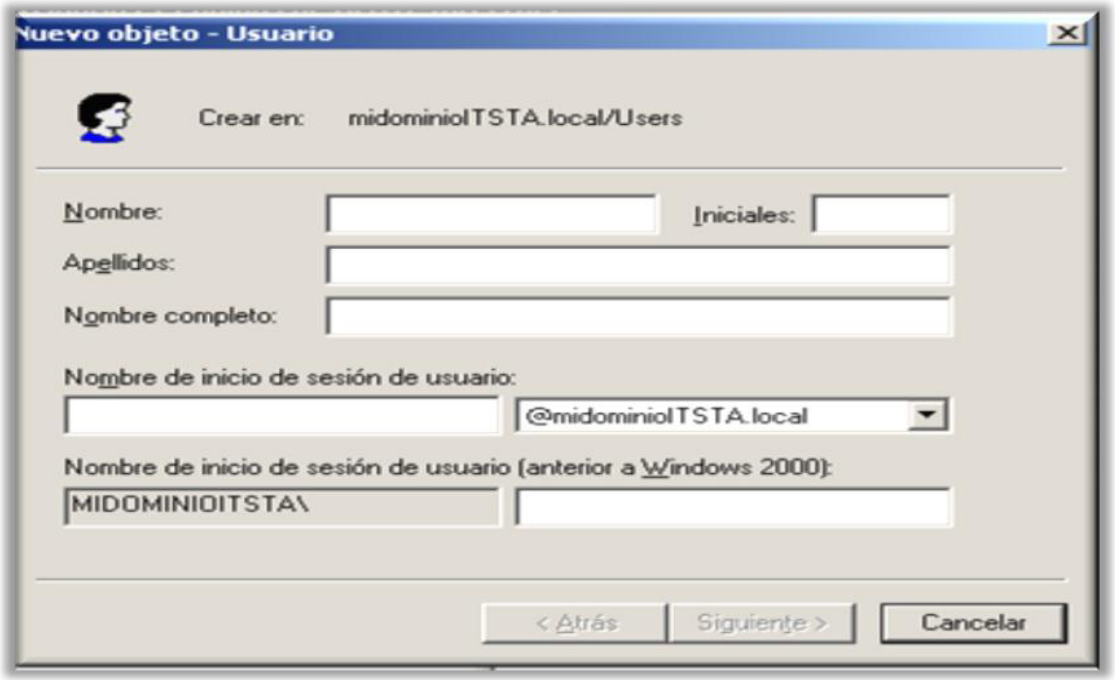


Figura 29.-interfaz para crear un usuario

Escribir el nombre de usuario y los nombres de inicio de sesión, hacer clic en Siguiente



. Figura 30.- tabla para llenar los datos del usuario

Escribir la contraseña y Seleccione las opciones adecuadas para la nueva cuenta y hacer clic en Siguiente.

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión (recomendado)
- El usuario no puede cambiar la contraseña
- Contraseña próximo expira
- Cuenta deshabilitada
- Haga clic en el botón Siguiente
- Haga clic en el botón Finalizar

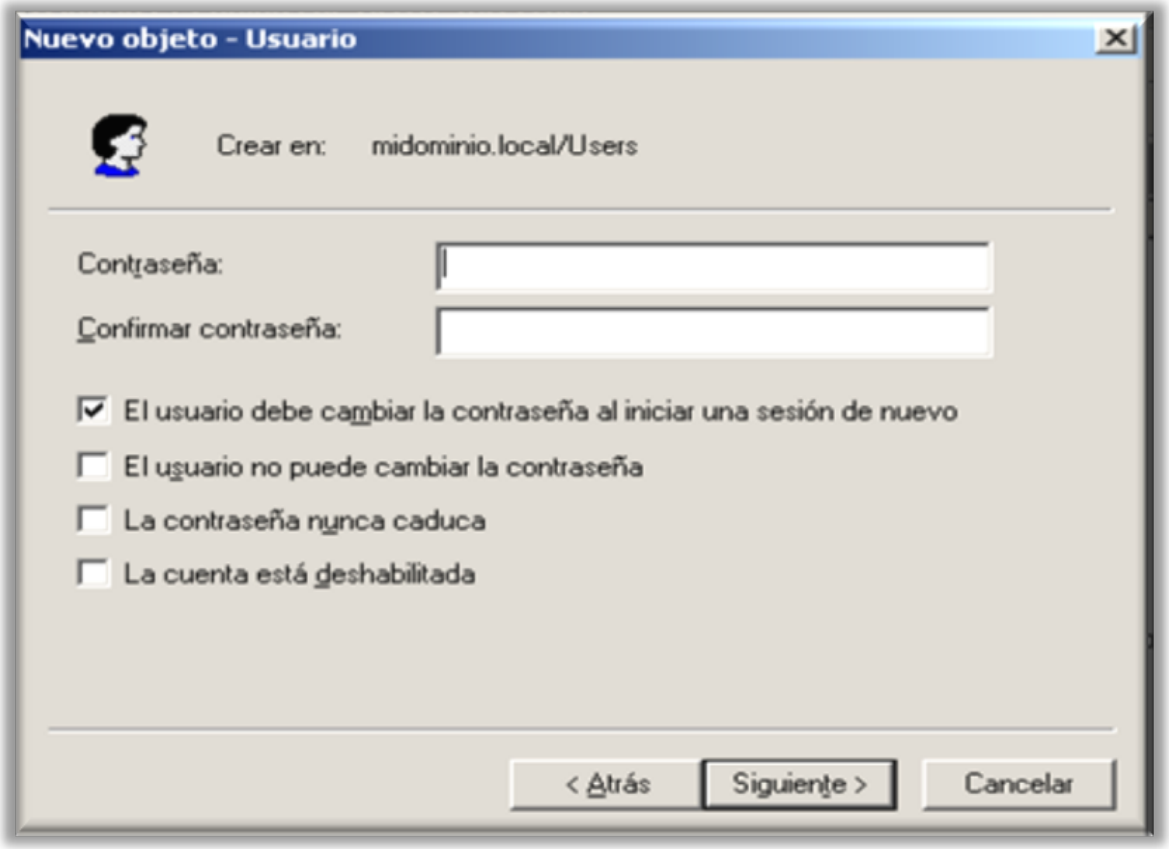


Figura 31.- tabla para ingresar la contraseña para el nuevo usuario

Leer la descripción del objeto y hacer clic en Finalizar.

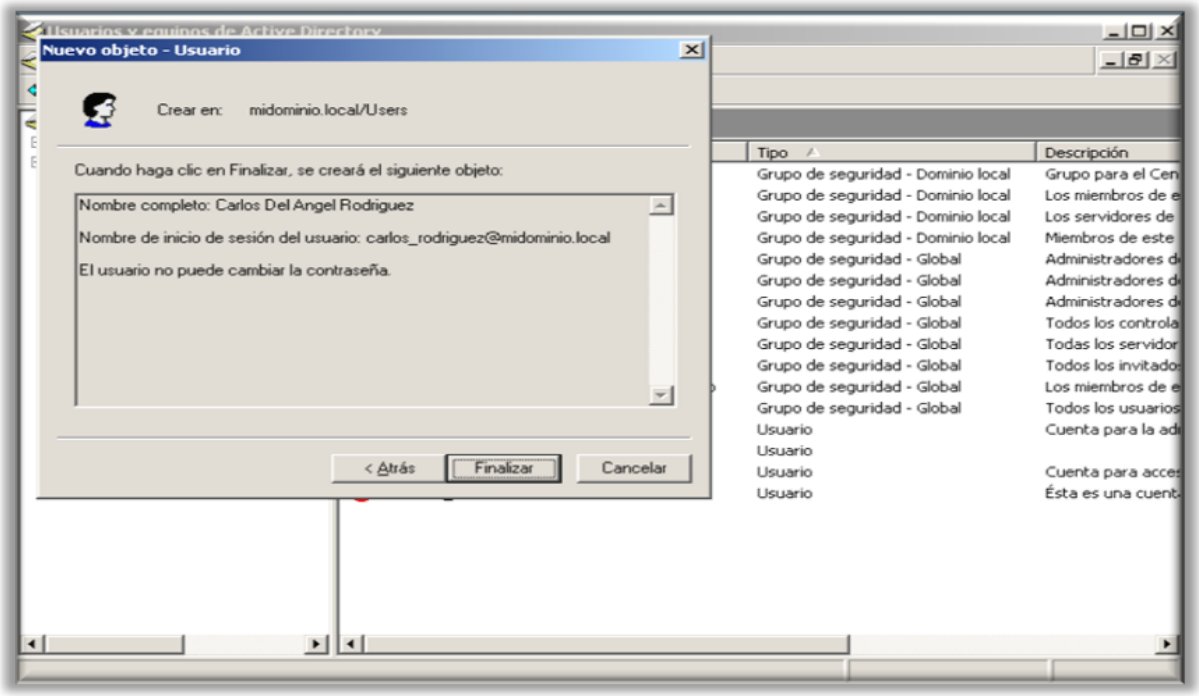


Figura 32.-informacion del usuario creado.

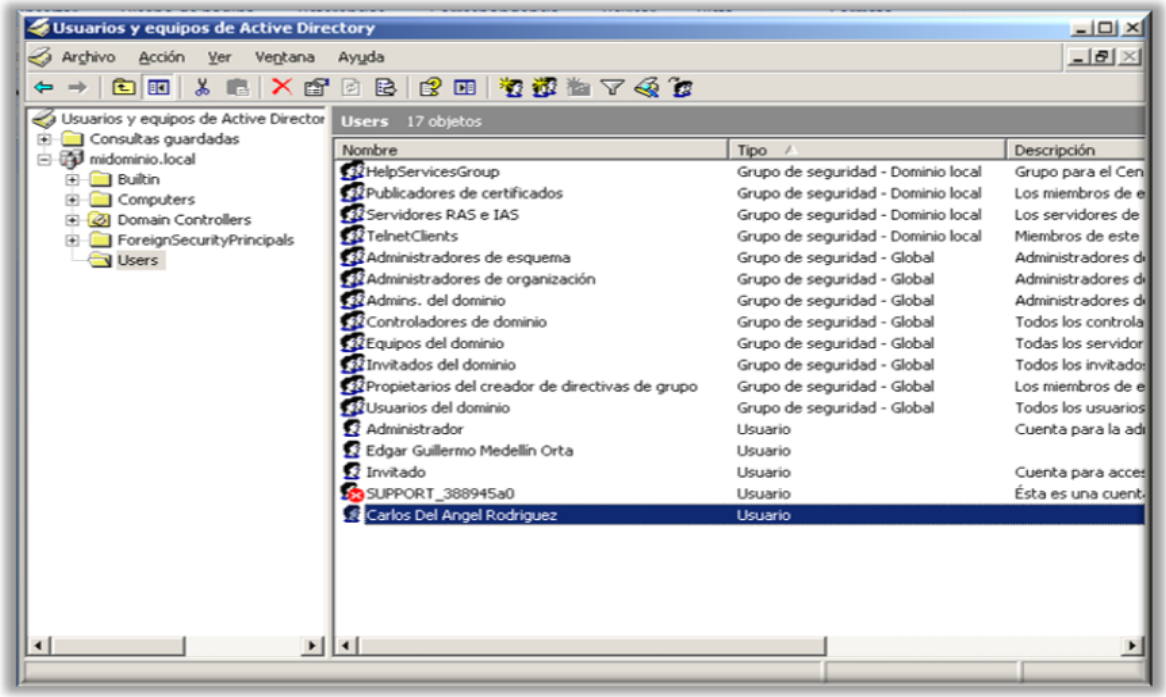


Figura 33.- usuario dado de alta en el dominio.

3.4 Crear usuarios locales de Windows server 2003

Hacer clic en inicio, ejecutar y a continuación escribir lo siguiente ***RunDll32 netplwiz.dll, UsersRunDll***

Figura 34.- instrucción para abrir la consola para crear usuarios locales

Nos aparecerá la consola cómo se nos muestra en la figura. Se nos muestra que sólo tenemos una cuenta de usuario local que es la de administración. Para crear una cuenta nueva local hacemos clic es agregar.

Figura 35.-consola para crear usuarios locales

Enseguida agregamos el usuario con el que queremos que entre localmente, para eso le damos examinar para que compruebe si el usuario esta dado de alta y que el dominio sea el correcto.

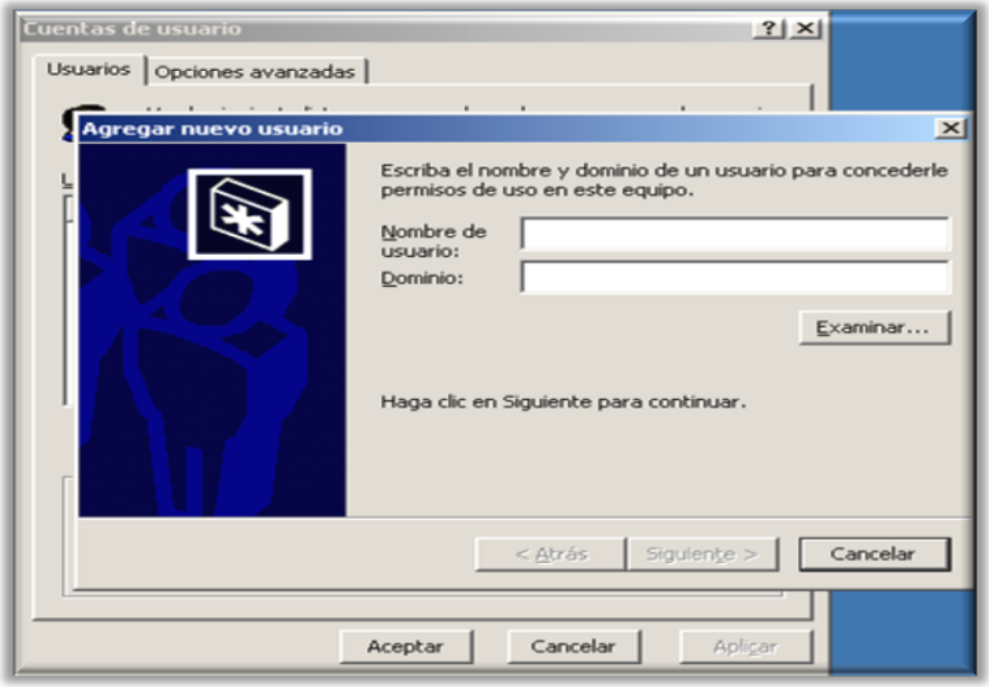


Figura 36.-tabla para ingresar datos del nuevo usuario local

Aquí se nos muestra que el usuario es correcto. Hacer clic en aceptar.

Figura 37.- comprobación de los datos.

Elegir el nivel de acceso que se le concederá al usuario.

Figura 38.- tabla para seleccionar el nivel de acceso que tendrá el usuario local en el dominio

Aquí podemos observar que el usuario local ya esta creado.

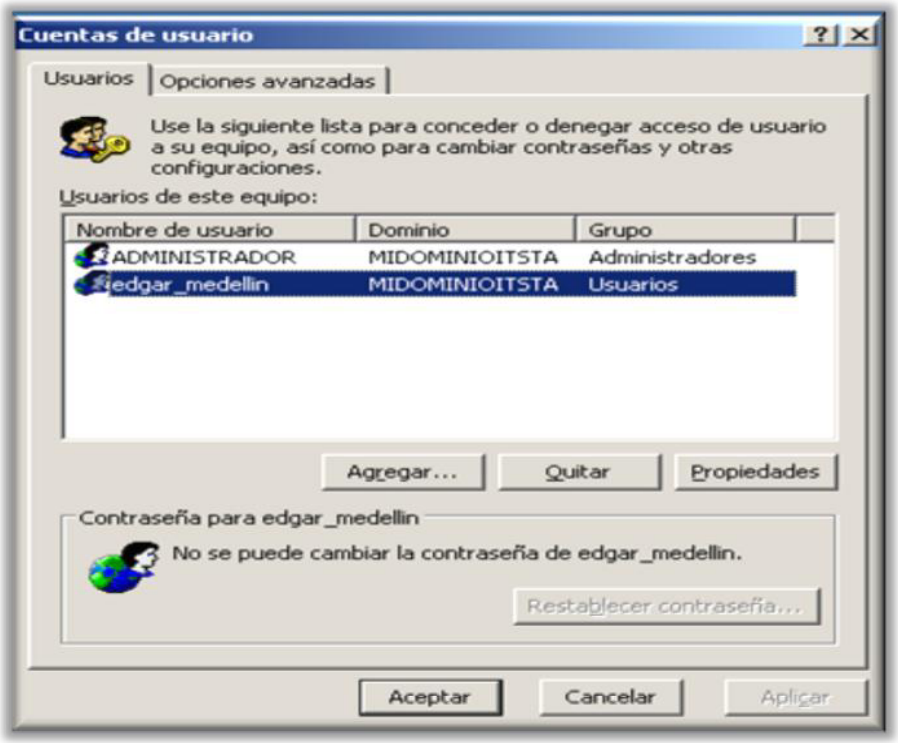


Figura 39.- usuario dado de alta en el dominio como usuario local.

A continuación al usuario local creado, se le dará los permisos para entrar al servidor localmente. Damos clic en inicio, herramientas administrativas y elegimos Directiva de seguridad de dominio.

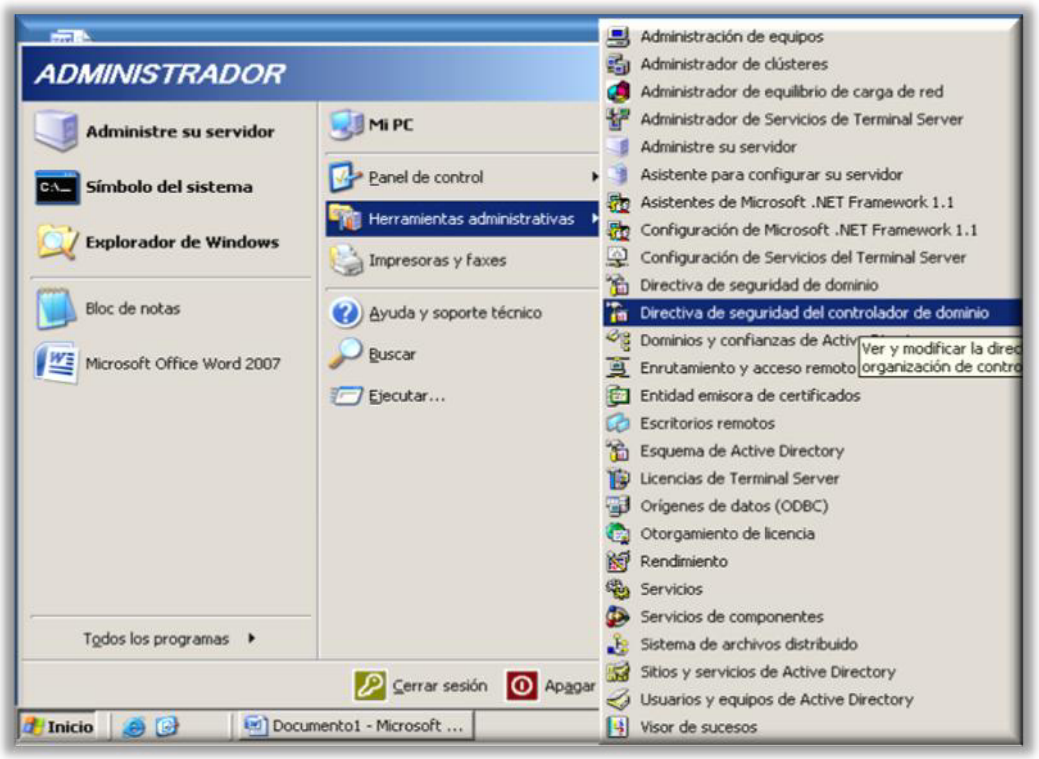


Figura 40.- instrucción para abrir la opción para asignarle los permisos al usuario.

Nos aparecerá una ventana cómo se muestra en la figura 37. A continuación damos clic en configuracion de Windows, configuracion de seguridad y hacemos clic en Asignación de derechos de cuentas.

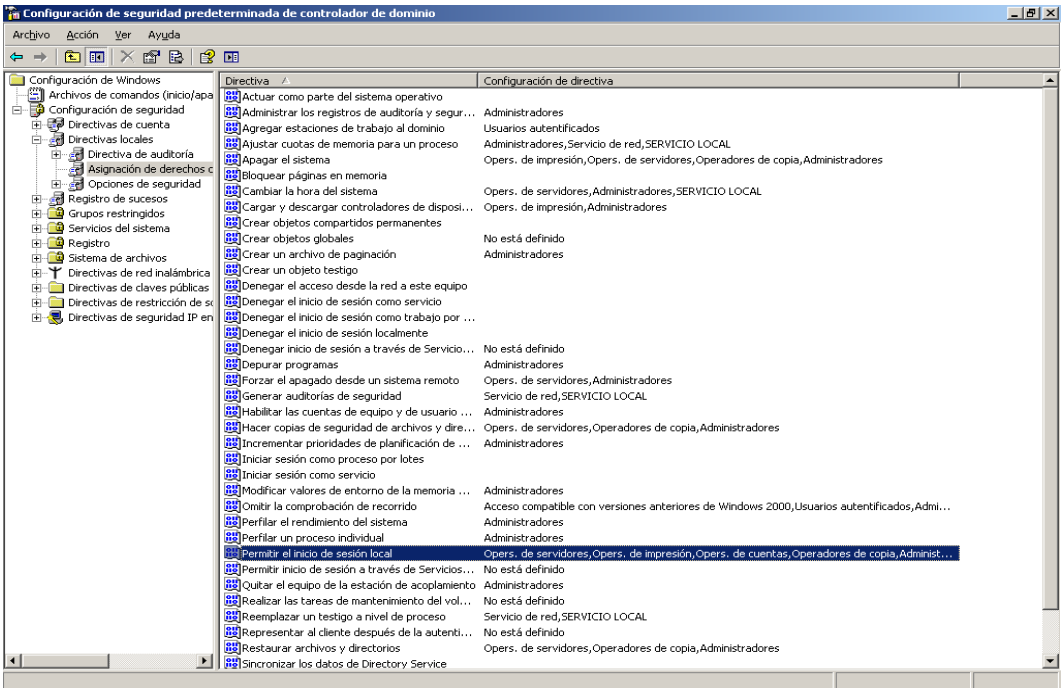


Figura 41.-ventana para asignarle los derechos al usuario local.

Dar clic en la opción que dice, permitir el inicio de sesión local. En propiedades de permitir el inicio de sesión local, dar clic en agregar usuario o grupo.

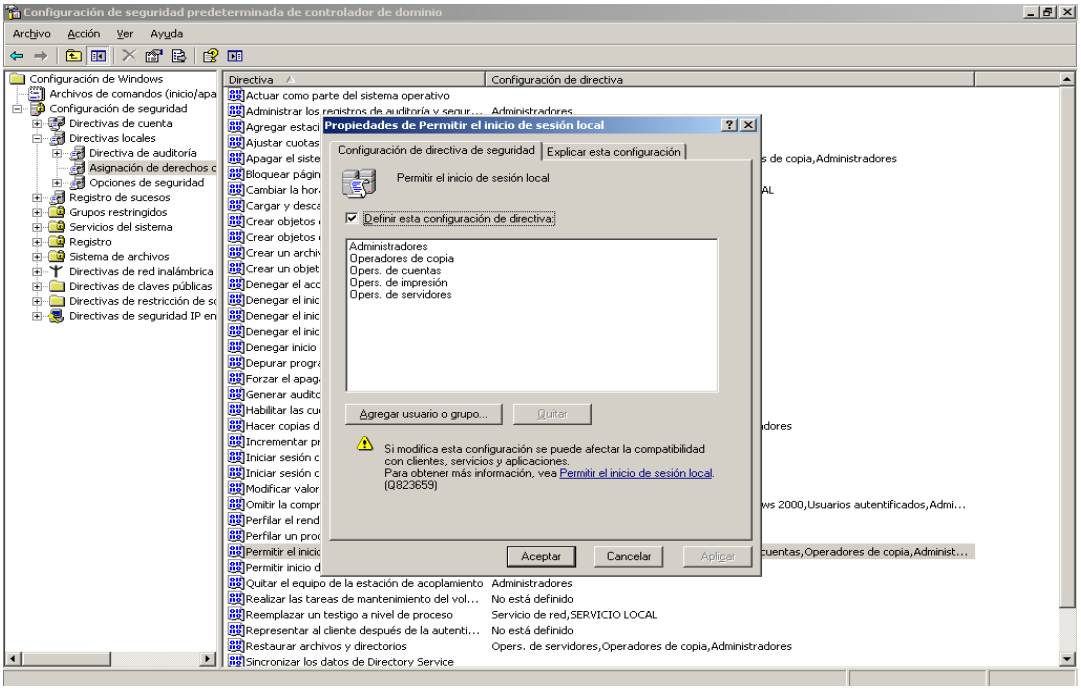


Figura 42.- imagen para agregar al usuario al que se le dará los derechos

Ingresamos el nombre del usuario del que dimos de alta para que pueda iniciar sesión localmente y le damos clic en comprobar nombres.

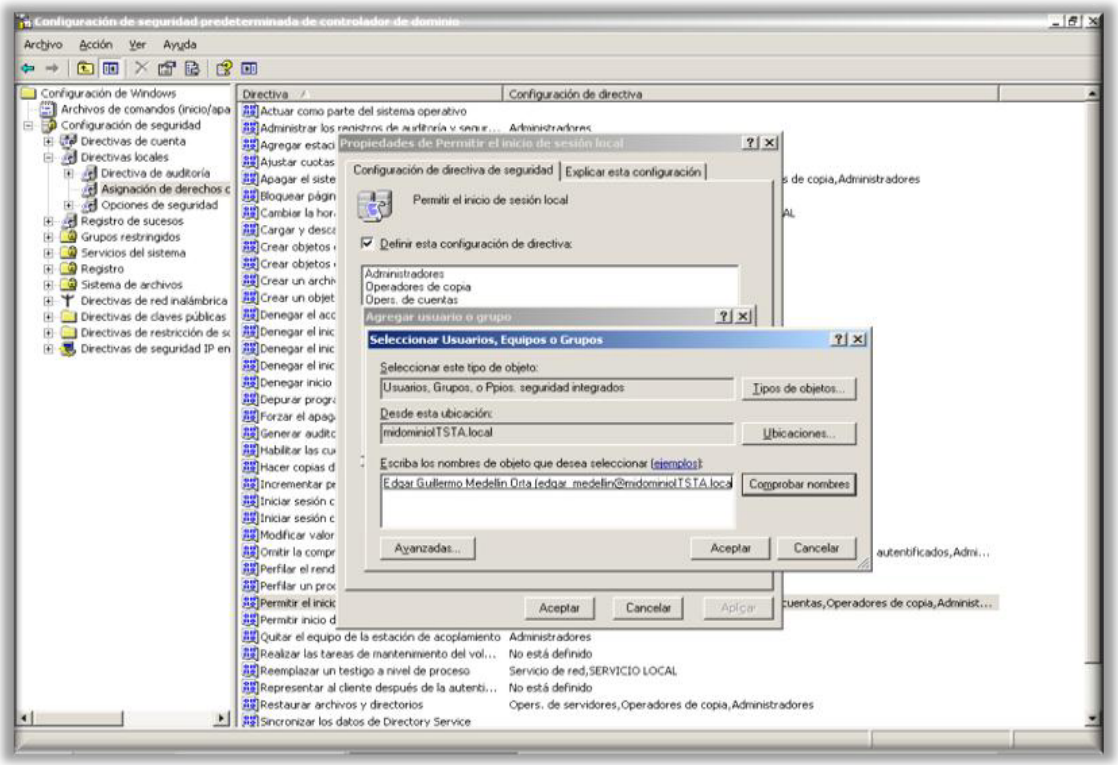


Figura 43.- comprobar el nombre del usuario

Una vez que se comprueba el nombre del usuario y al dominio que pertenece le damos clic en aceptar.

Nuestro usuario ya está configurado para el inicio de sesión local. Por ultimo hacer clic en aceptar.

3.5 Crear grupos

Hacer clic en **Inicio,** seleccionar **Herramientas Administrativas** y hacer clic en **Usuarios y equipos de Active Directory**.

Figura 44.- imagen para agregar grupos

Hacer clic con el botón secundario del mouse sobre el dominio, la Unidad Organizacional (OU) o contenedor donde se va a crear el grupo. Seleccionar **Nuevo** y luego hacer clic en **Grupo**.

Escribir el nombre del grupo.

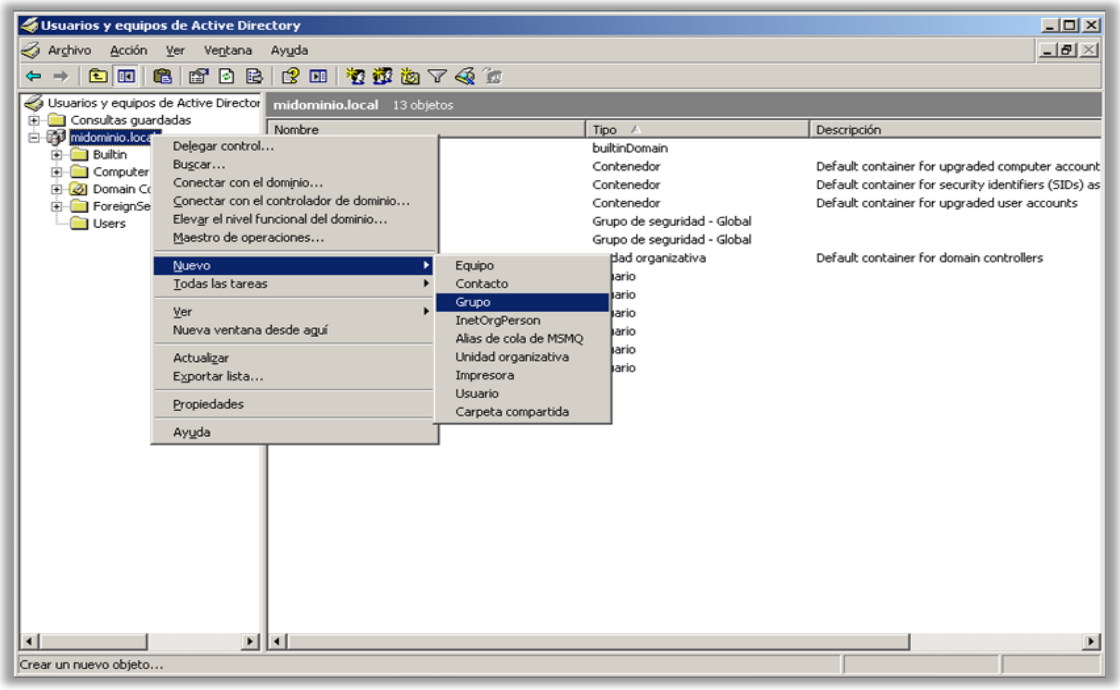


Figura 45.-imagen para abrir la ventana para crear un nuevo grupo de dominio.

Seleccionar el Ámbito de Grupo y el Tipo de Grupo y hacer clic en **Aceptar**.

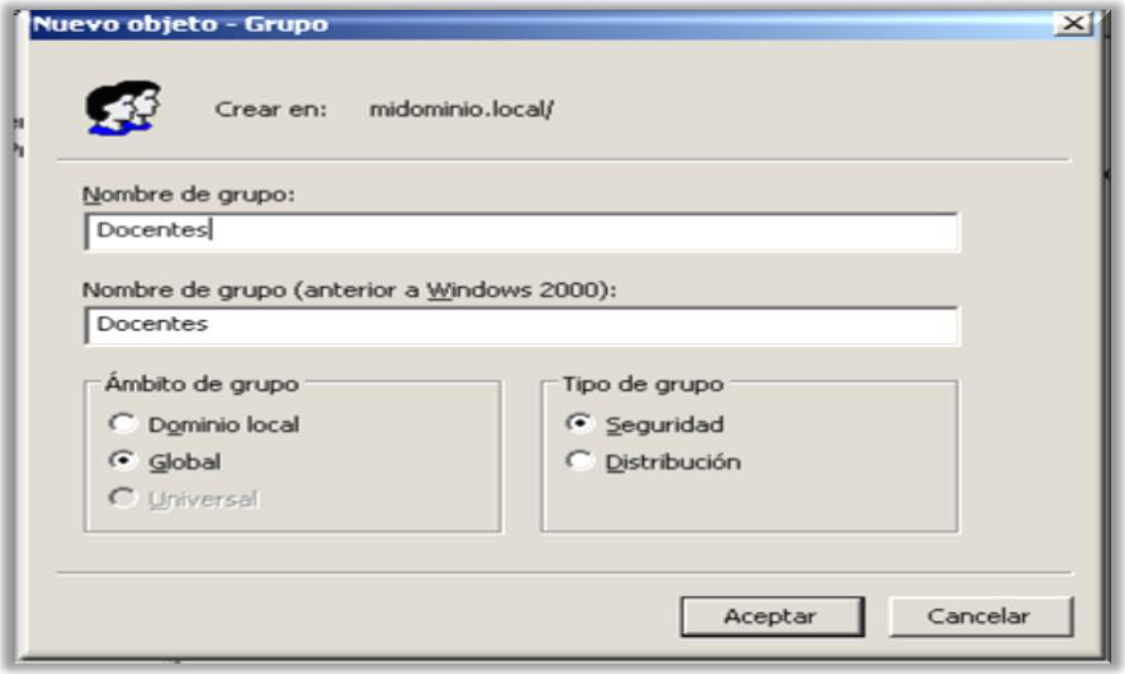


Figura 46.-agregar el nombre y el ámbito del nuevo grupo

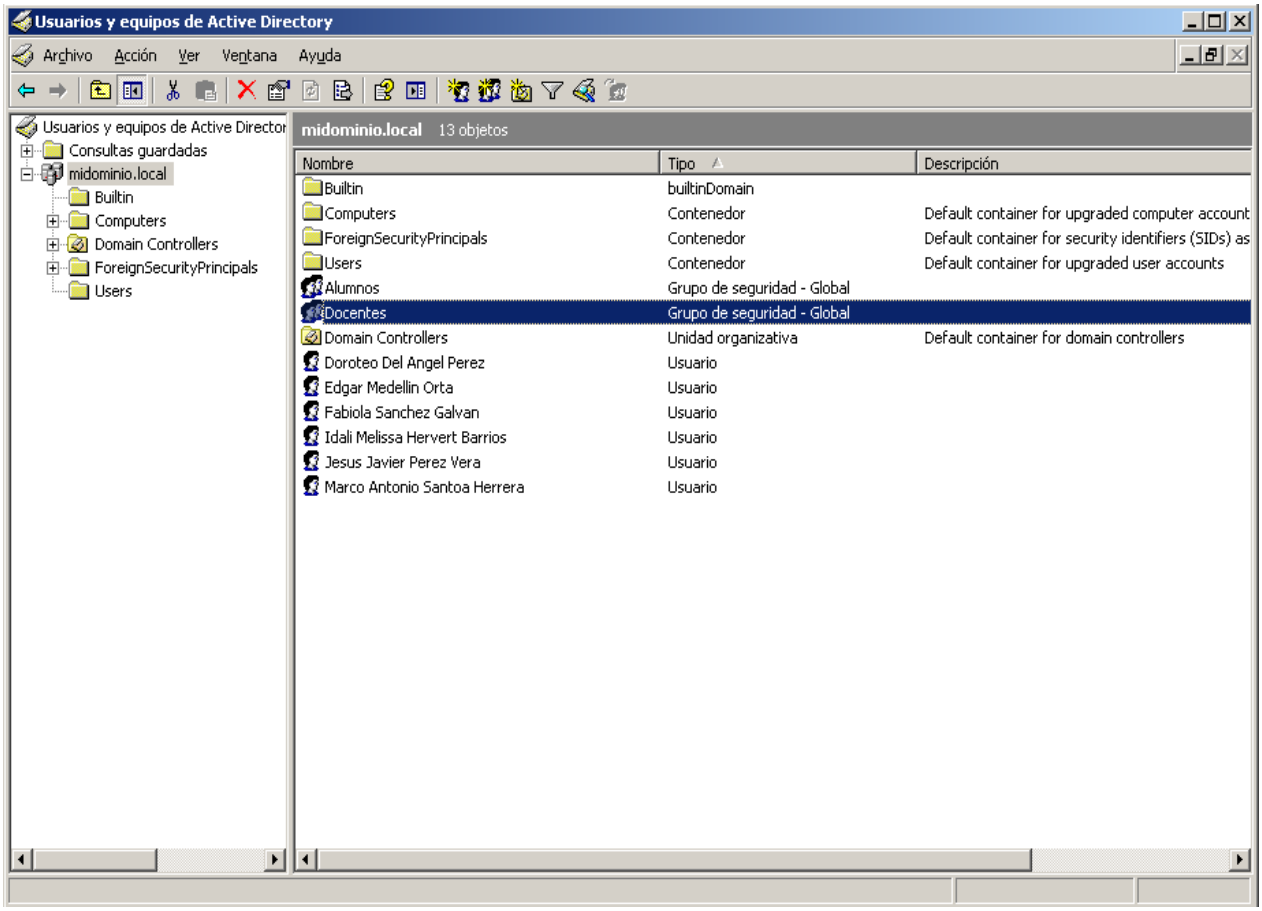


Figura 47.- grupo dado de alta en el dominio.

3.6 Instalar y Configurar GPMC

Instalar GPMC

La instalación de GPMC es un proceso simple que requiere la ejecución de un paquete de Windows Installer (.MSI). Para descargar la última versión, visite el sitio de Windows Server System para la administración de Directivas de grupo en http://www.microsoft.com/windowsserver2003/gpmc/default.mspx (en inglés).

Para instalar la Consola de administración de Directivas de grupo

1. En el servidor **ITSTA**, desplácese a la carpeta que contiene **gpmc.msi**, haga doble clic en el paquete **gpmc.msi** y, a continuación, haga clic en **Siguiente**.
2. Haga clic en **Acepto** para aceptar el Contrato de licencia de usuario final y, a continuación, haga clic en **Siguiente**.
3. Haga clic en **Finalizar** para completar la instalación de GPMC.

Una vez finalizada la instalación, la ficha Directiva de grupo que aparecía en la página Propiedades de sitios, dominios y unidades organizativas de los complementos de Active Directory se actualiza con un vínculo directo a GPMC. La funcionalidad que existía anteriormente en la ficha Directiva de grupo ya no está disponible, puesto que todas las funciones para administrar la Directiva de grupo están disponibles en GPMC.

Para abrir el complemento GPMC

1. En el servidor **ITSTA**, haga clic en el botón **Inicio**, en **Ejecutar**, escriba **GPMC.msc** y, a continuación, haga clic en **Aceptar**.

   Nota: puede utilizar también alguno de los métodos siguientes para ejecutar GPMC.

   - Haga clic en el acceso directo **Administración de directiva de grupo** en la carpeta **Herramientas administrativas** en el menú **Inicio** o en el Panel de control.
   - Crear una consola MMC personalizada: haga clic en el botón **Inicio** y en **Ejecutar**, escriba **MMC** y, a continuación, haga clic en **Aceptar**. Seleccione **Archivo**, haga clic en **Agregar** o **quitar complemento** y luego en **Agregar**. Haga clic para resaltar **Administración de directiva de grupo**, haga clic en **Agregar**, en **Cerrar** y después en **Aceptar**.

3.7 Configurar Directivas de Grupo

3.7.1 Como se crea una GPO

Para crear una directiva de seguridad, primero se debe de abrir usuarios y equipos de Active Directory en las herramientas administrativas.

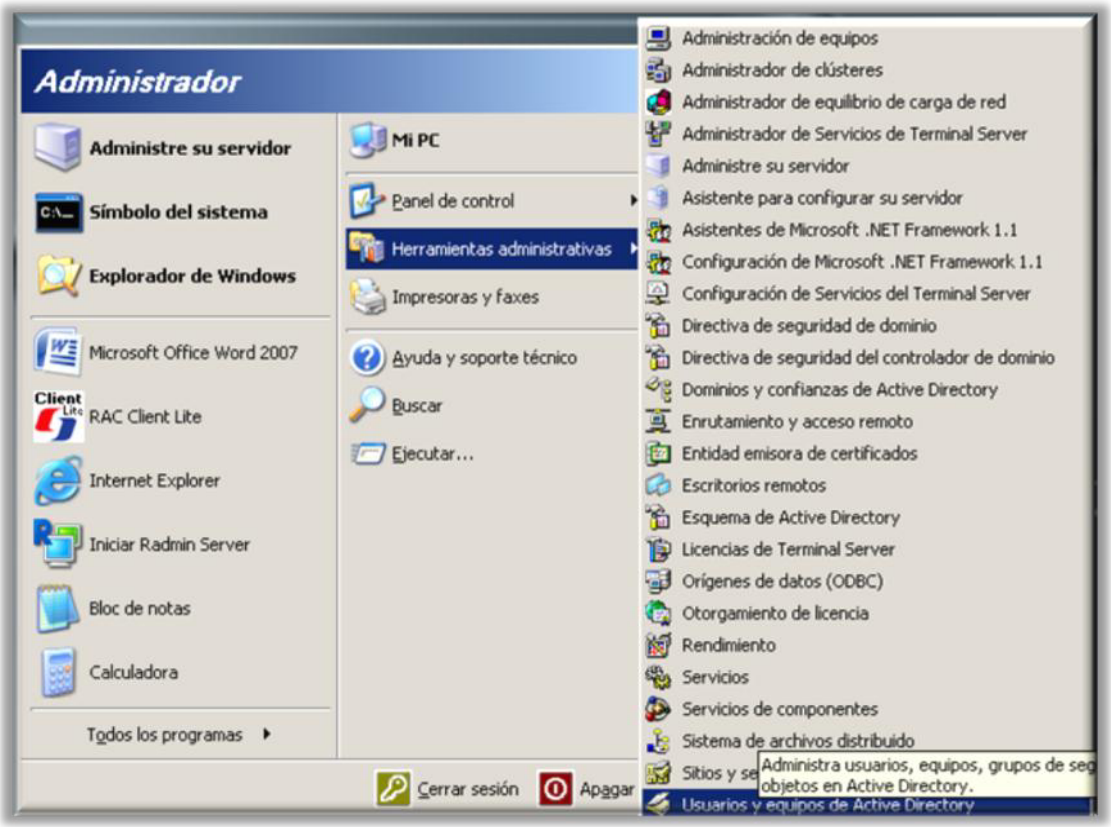


Figura 48.- abrir la ventana de los usuarios y equipos de active directory

Una vez que se haya abierto la ventana de los usuarios y equipos de Directory Active, para abrir la consola de administración de directivas de grupo (GPMC) seleccionamos cualquier carpeta en donde se encuentren los grupos.

En este caso seleccionamos el grupo de salón_redes que es la carpeta en donde se encuentra el grupo de alumnos. Hacemos clic derecho, seleccionamos propiedades y se abrirá la siguiente imagen:

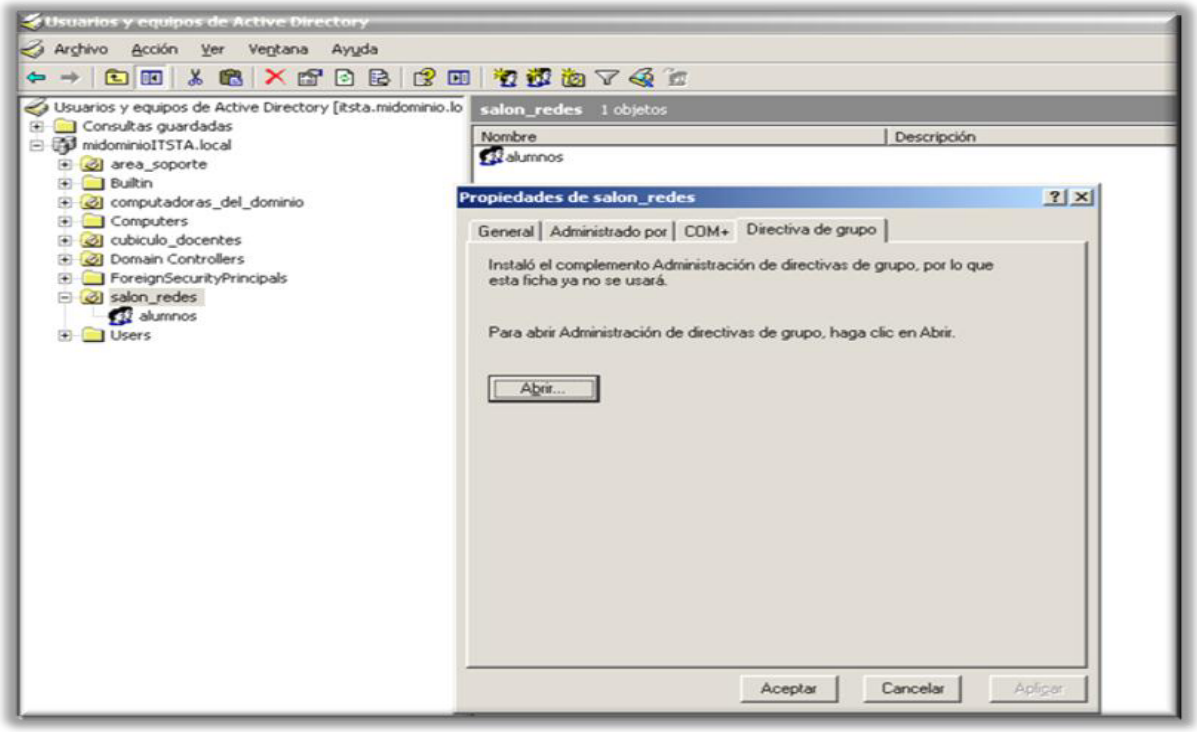


Figura 49.- abrir la consola de administración de directivas de grupo.

Se hace clic en abrir, para que nos habrá el administrador de directivas de como se muestra en la figura

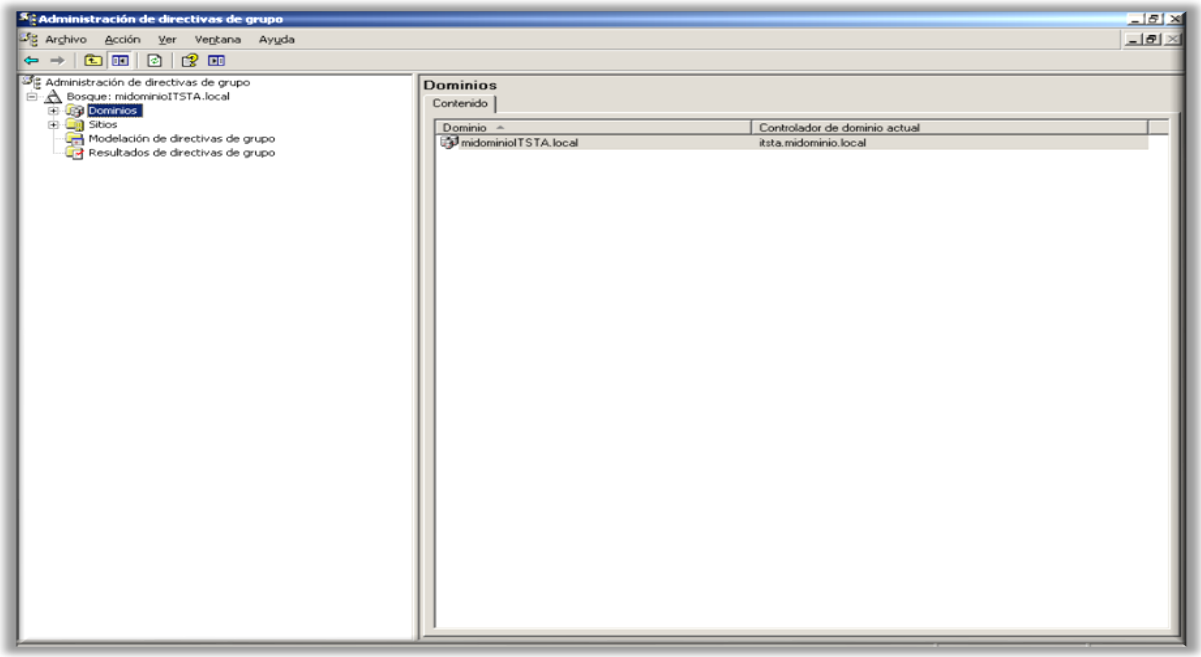


Figura 50.- consola de administración de directivas de grupo

Seleccionamos la carpeta salón_redes y hacemos clic en crear y vincular una nueva GPO. Enseguida se abrirá una ventana como se muestra en la figura y nos pedirá que ingresemos el nombre para la nueva GPO.

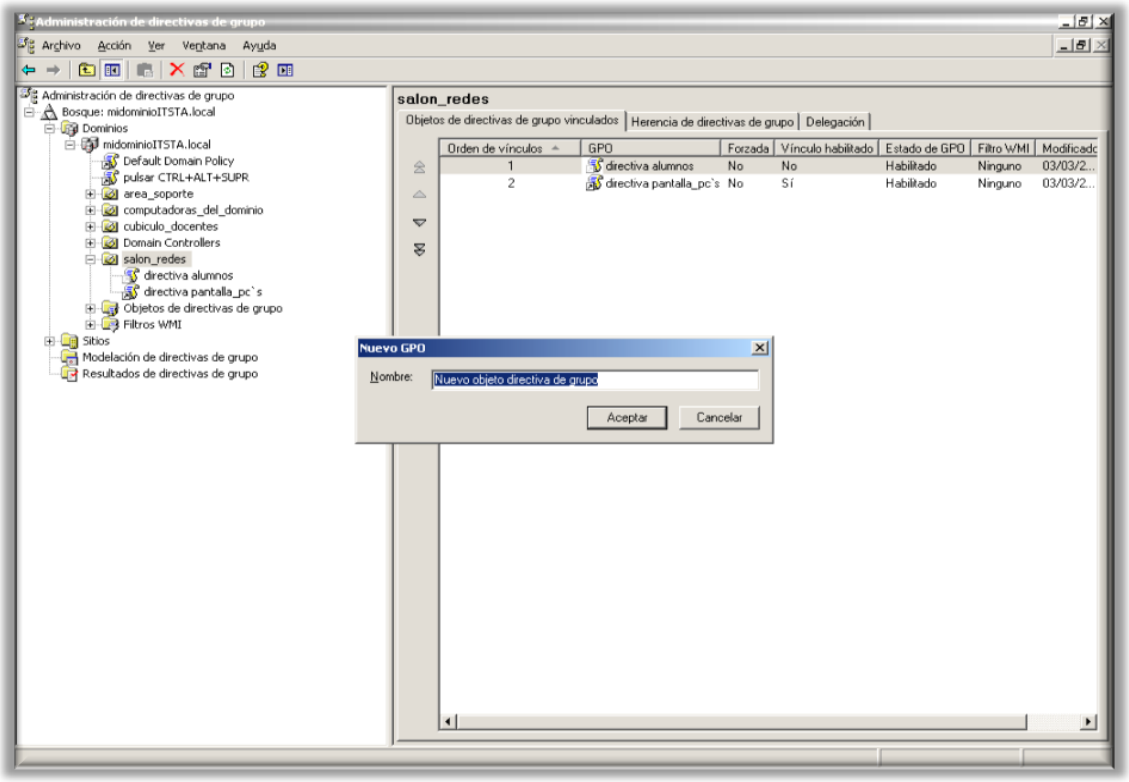


Figura 51.- imagen para ingresar el nombre de la nueva GPO.

Y listo tenemos nuestra directiva creada.

3.7.2 Como se elimina una directiva

Para eliminar una directiva de seguridad es muy simple. Seleccionamos la directiva a eliminar y hacemos clic derecho sobre ella y seleccionamos eliminar como se muestra en la siguiente figura.

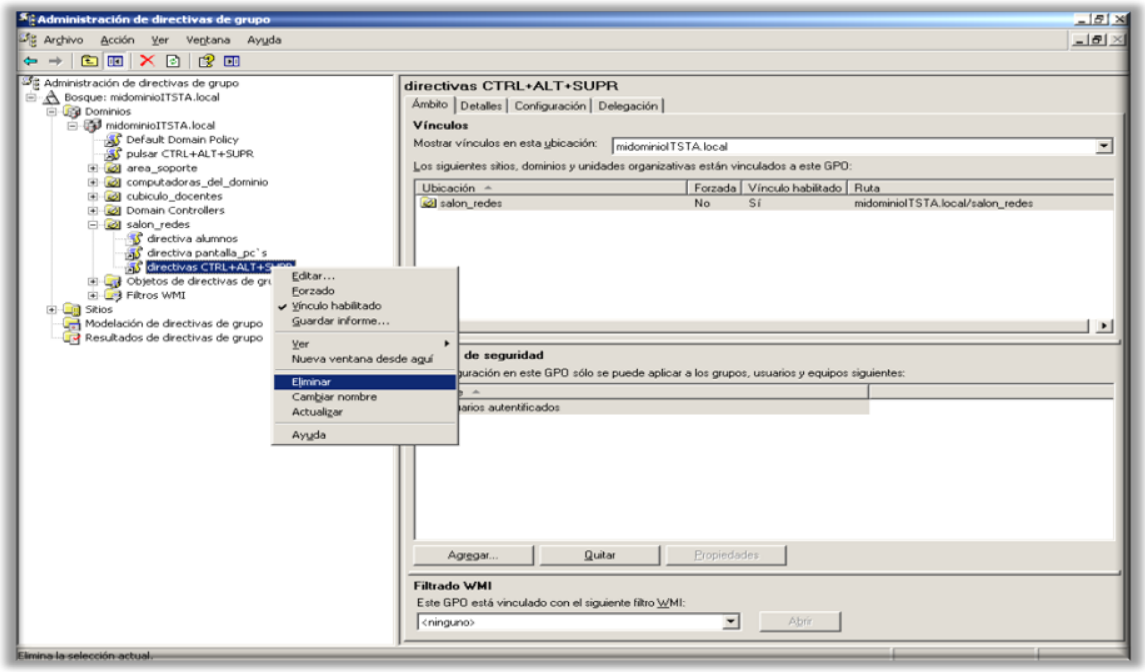


Figura 52.- eliminar directiva de grupo.

Aparecerá un cuadro como se muestra en la siguiente figura y le damos clic en aceptar.

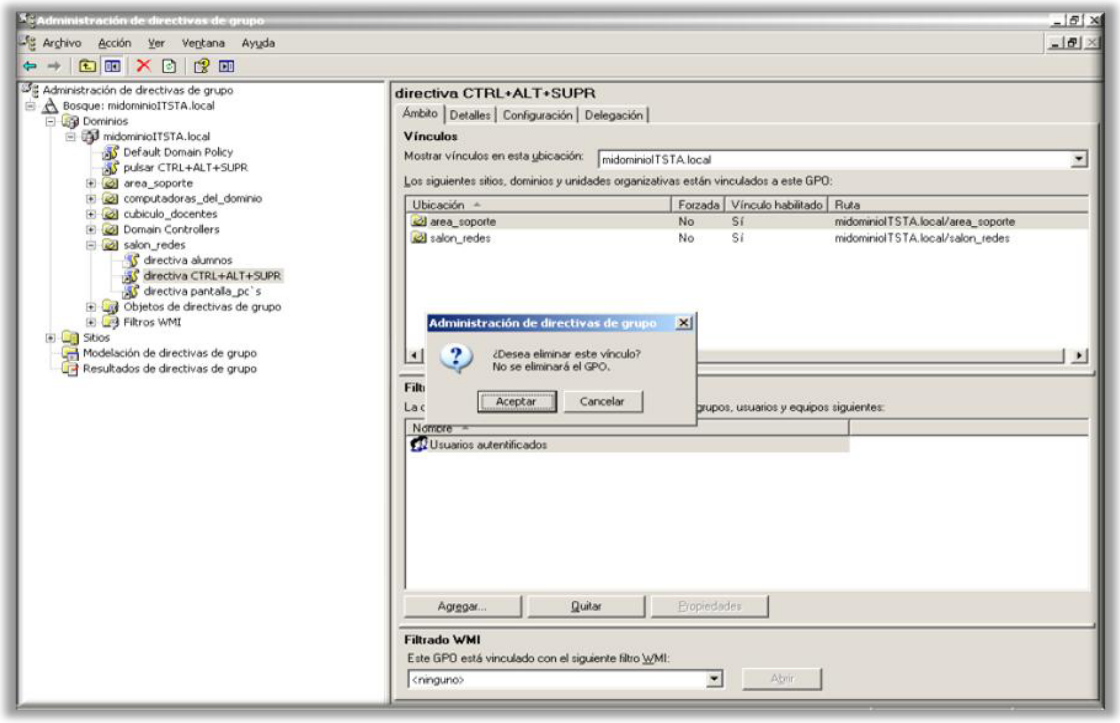


Figura 53.- directiva de grupo eliminada

3.7.3 Como se define un objeto de directiva de grupo

Para definir las políticas, seleccionamos la directiva de grupo y hacemos clic derecho sobre ella, y seleccionamos editar.

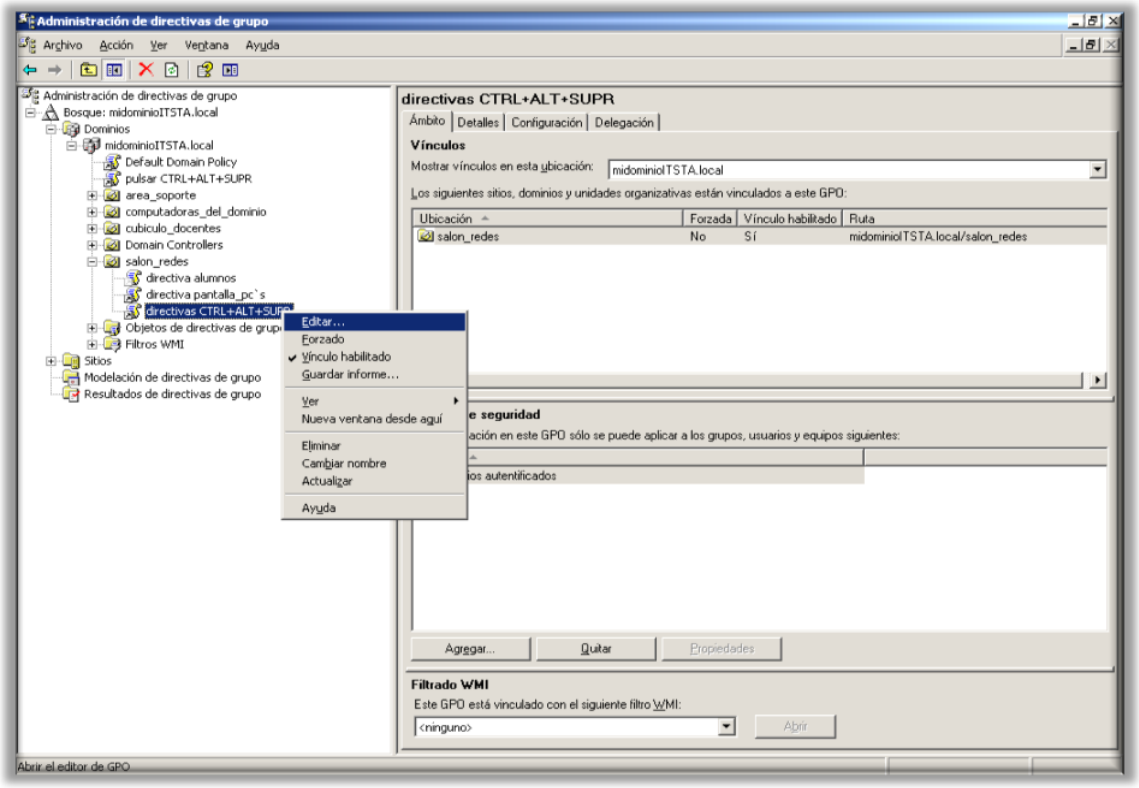


Figura 54.- abrir el editor de objetos de grupo.

Enseguida se abrirá una ventana como se muestra en la figura 55.

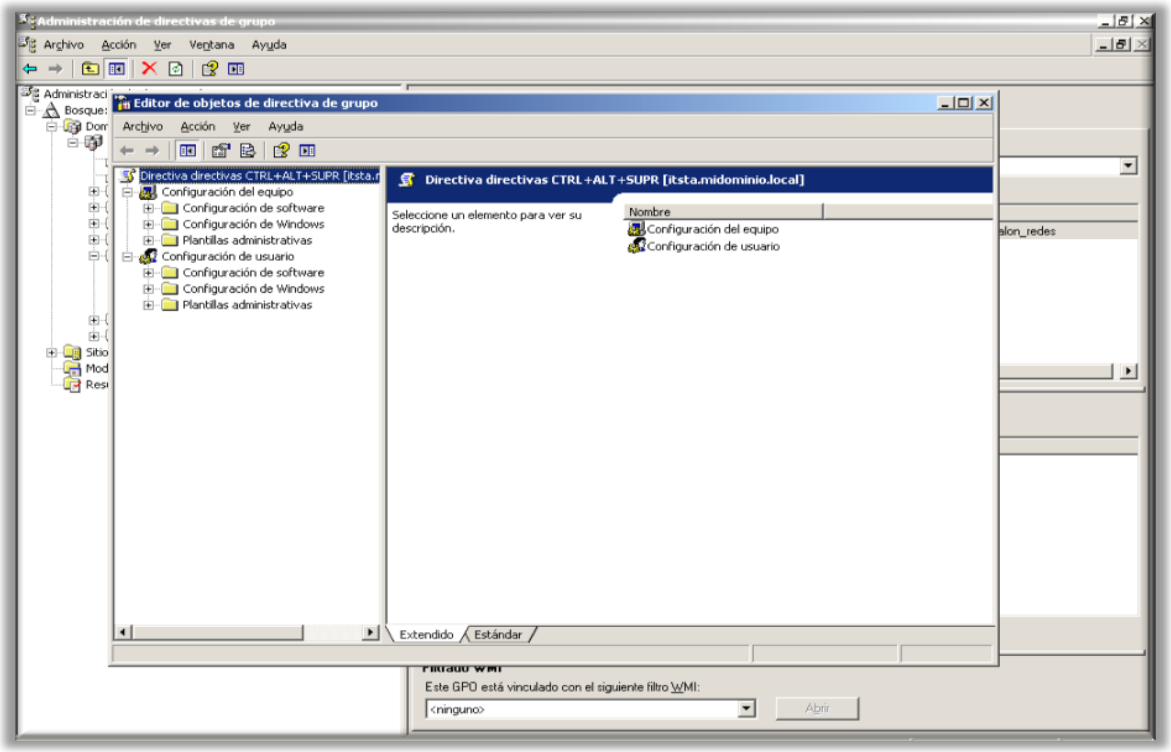


Figura 55.- Consola de editor de objetos de directiva de grupo.

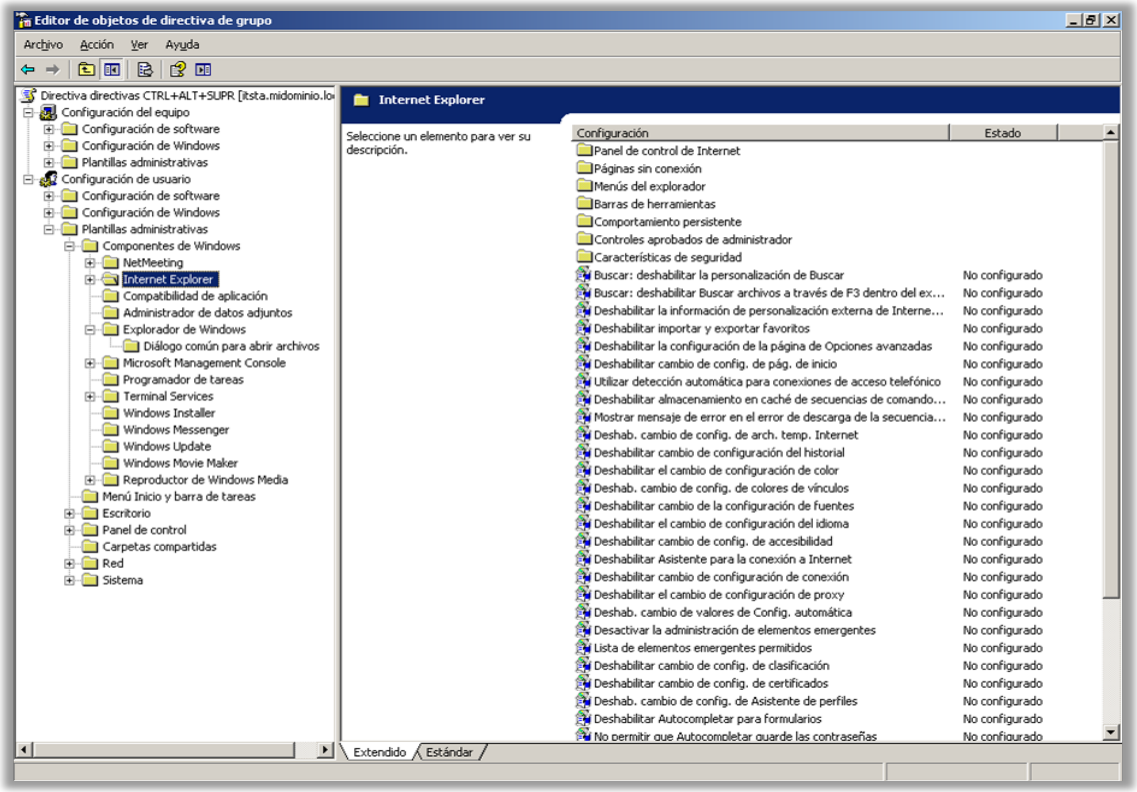


Figura 56.- herramientas para definir las directivas.

Hacemos doble clic sobre la directiva "Inicio de sesión interactivo: no requerir Ctrl.+Alt+Supr" y podremos **definir** ésta política como **deshabilitada**:

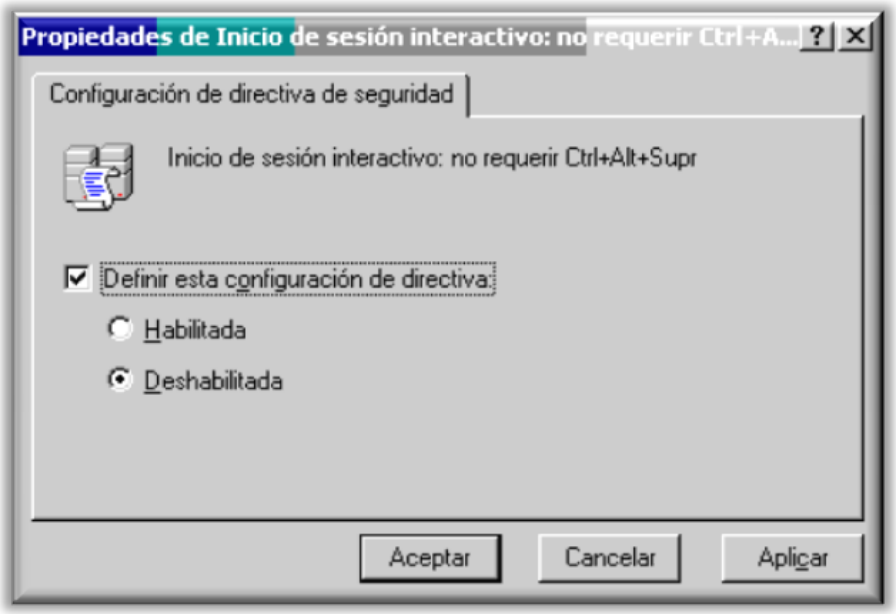


Figura 57.- Configuración de directiva de seguridad.

La casilla "***Definir esta configuración de directiva***" tiene el efecto:

Marcada	***La política quedará definida*** con el valor seleccionado en las opciones de debajo.
Sin Marcar	***La política hereda su definición*** o no ***y si está habilitada*** o no en caso de haber sido definida en un contenedor superior (en nuestro ejemplo desde el propio equipo o el sitio, ya que estamos a nivel de dominio).

A su vez, cuando la casilla está marcada podemos elegir entre las opciones:

Habilitada	Hace que la política quede habilitada. Esto significa que ***se realizará la configuración que la propia política define con su nombre*** y por tanto, en nuestro ejemplo, provoca que no sea necesario que el usuario pulse CTRL+ALT+SUPR para iniciar sesión.
Deshabilitada	Cuando se deshabilita la política, ***se impide que se realice la configuración que la propia política define con su nombre***. Por tanto, en el ejemplo, obliga al usuario a pulsar CTRL+ALT+SUPR para iniciar sesión.

3.7.4 ¿Cómo se vincula una política ya existente?

Para vincular una política existente ya sea a otro grupo del mismo dominio o a otra unidad organizativa, se debe de seleccionar la GPO que va a ser vinculada y debemos de habilitar la opción de vínculo habilitado como se muestra en la figura

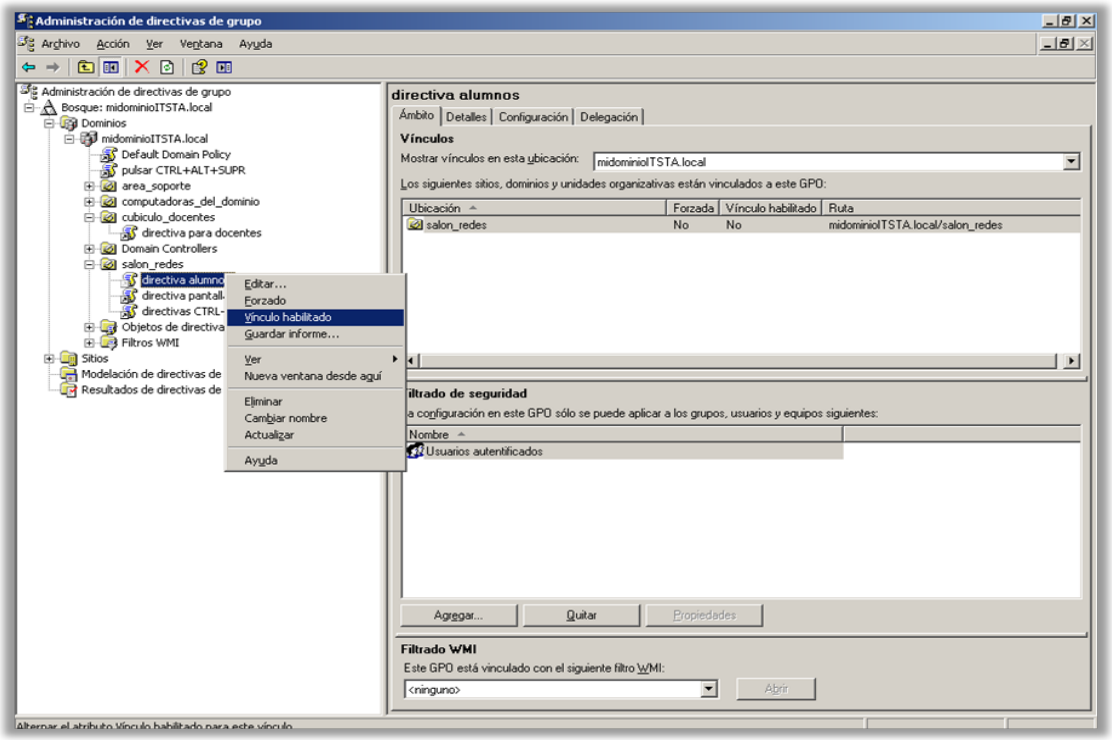


Figura 58.- habilitar la opción de vincular a las directivas

En la siguiente figura muestra las GPO´S las cuales tienen el vínculo habilitado y cuáles no, en este caso todas están habilitadas.

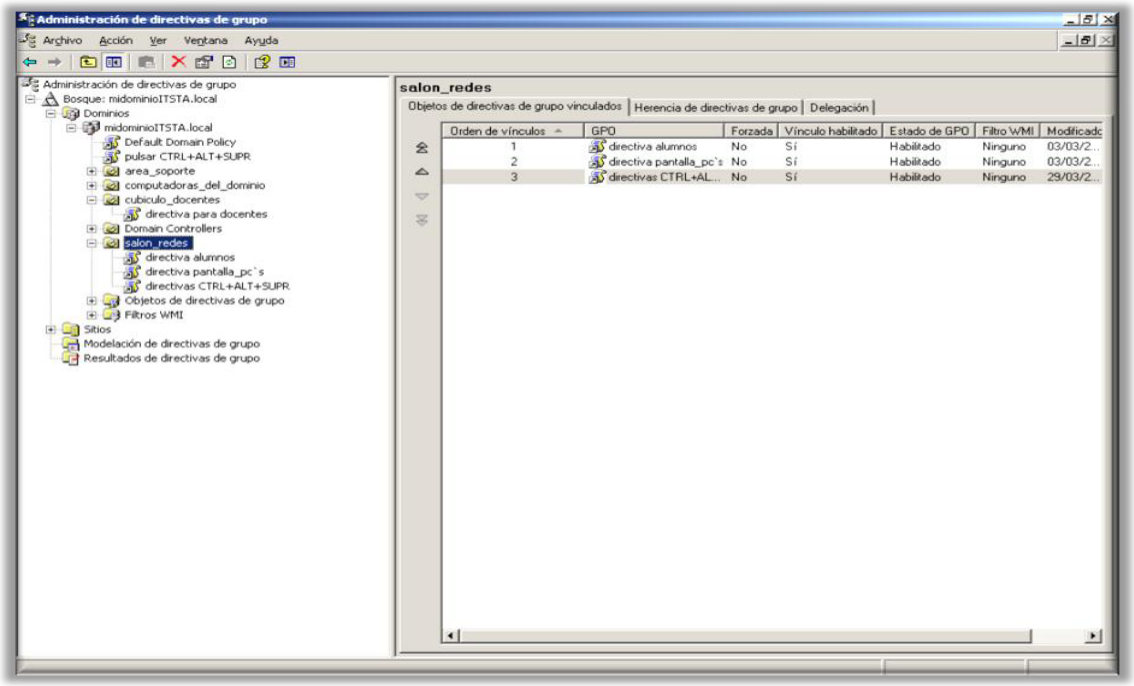


Figura 59.- directivas con el vínculo habilitado.

Una vez habilitado el vínculo de la directiva, seleccionamos ya sea la unidad organizativa, grupo, y/o dominio en donde deseamos vincular la GPO. En este caso vincularemos una GPO en la unidad organizativa cubículo_docentes.

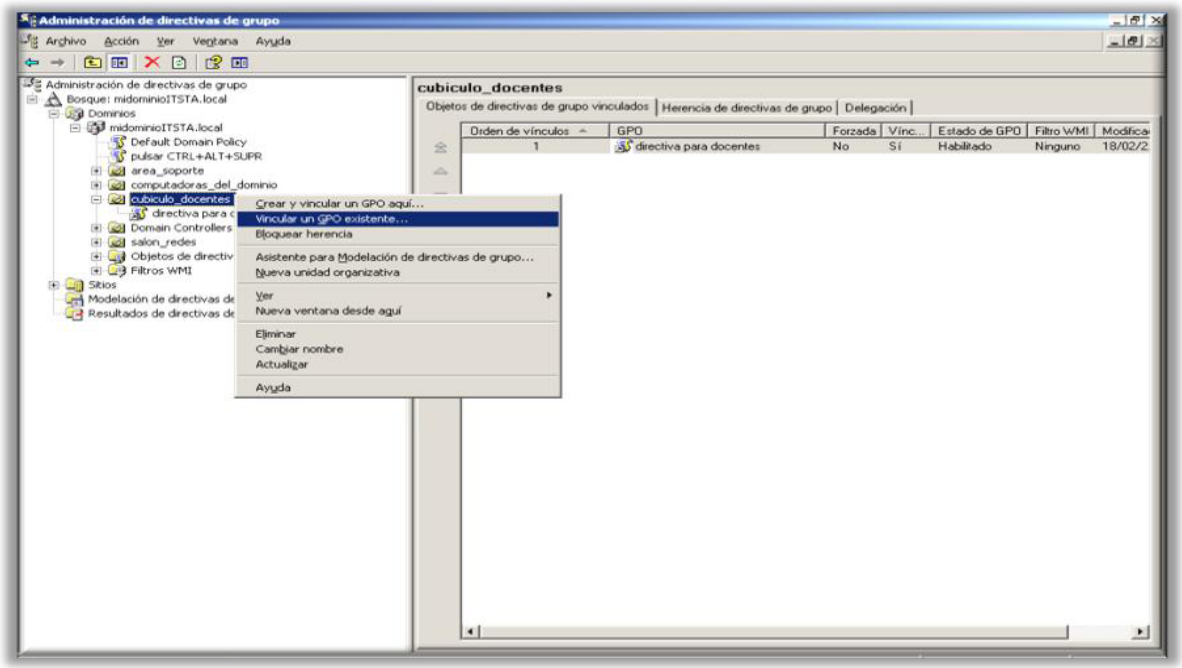


Figura 60.- vincular una directiva existente

Y nos aparecerá una ventana en donde se mostraran todas las GPO´S existentes en el dominio. Seleccionamos la GPO que deseamos vincular y hacemos clic en aceptar como se muestra en la siguiente figura.

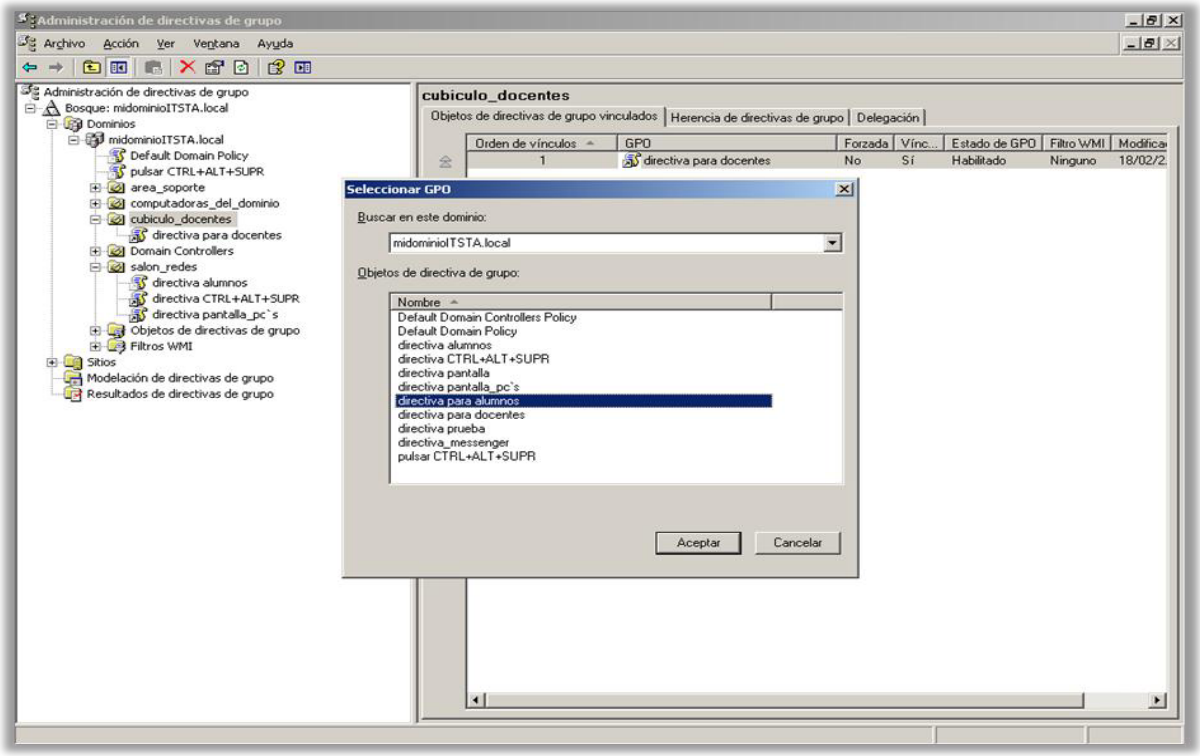


Figura 61.- seleccionar la directiva que se desea vincular.

Y listo, tenemos nuestra GPO vinculada.

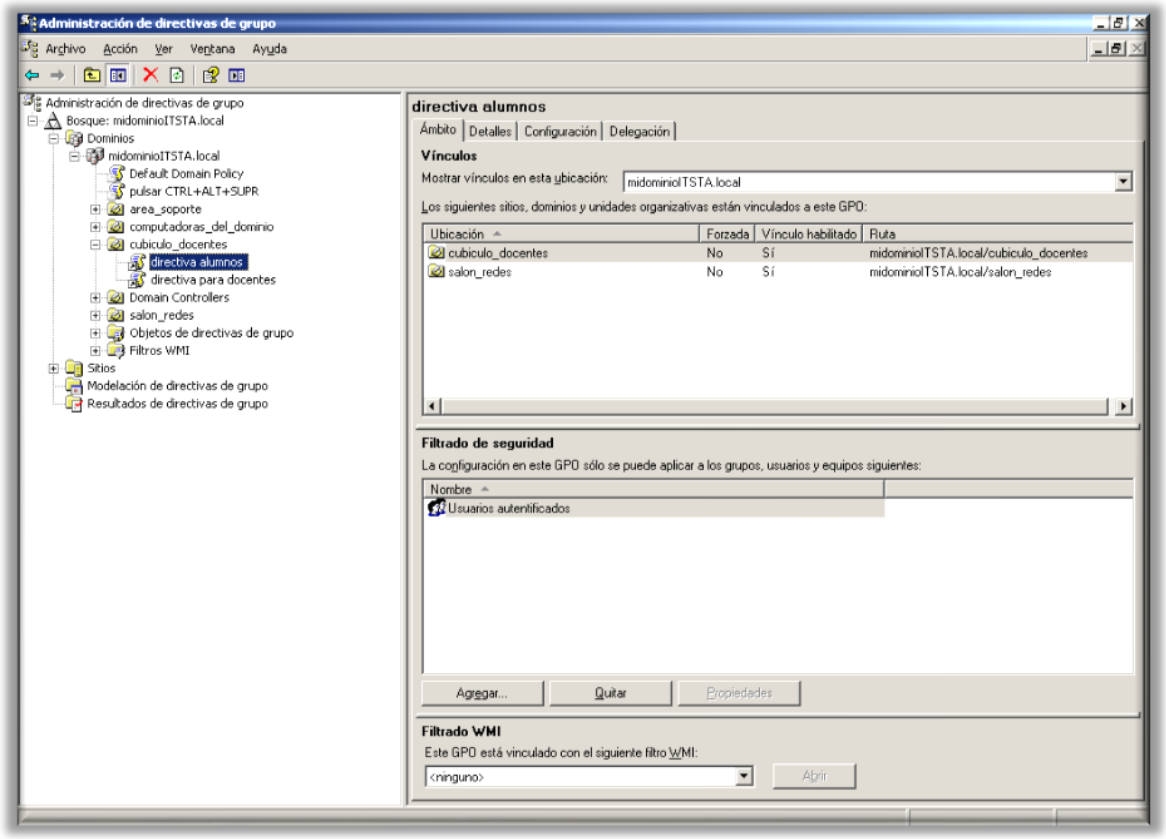


Figura 62.- GPO creada

3.7.5 Administrar objetos de directiva de grupos

3.7.5.1 Ver objetos de Directiva de grupo del dominio

En cada dominio GPMC proporciona una vista basada en directivas de Active Directory y de los componentes asociados a la Directiva de grupo, como objetos de Directiva de grupo, filtros WMI y vínculos de objetos de Directiva de grupo. La vista de GPMC es similar a la vista del complemento de MMC Usuarios y equipos de Active Directory en la que se muestra la jerarquía de unidades organizativas. Sin embargo, GPMC difiere de este complemento porque en lugar de mostrar usuarios, equipos y grupos en las unidades organizativas, muestra los objetos de Directiva de grupo que están vinculados a cada contenedor, así como los propios objetos.

En cada nodo de dominio de GPMC se muestran los siguientes elementos.

- Todos los objetos de Directiva de grupo vinculados al dominio.
- Todas las unidades organizativas de nivel superior y una vista de árbol de las unidades organizativas anidadas y los objetos de Directiva de grupo vinculados a cada unidad organizativa.
- El contenedor Objetos de Directiva de grupo que muestra todos los objetos de Directiva de grupo del dominio.
- El contenedor Filtros de WMI que muestra todos los filtros de WMI del dominio.

3.7.5.2 Para ver objetos de Directiva de grupo asociados a un contenedor determinado

1.- En el árbol **Dominios**, haga clic en el árbol **midominioITSTA.local**. Los objetos de Directiva de grupo asociados al contenedor (la raíz del dominio) aparecen como se muestra en la Figura 64. Este concepto se puede aplicar a cualquier contenedor de dominio.

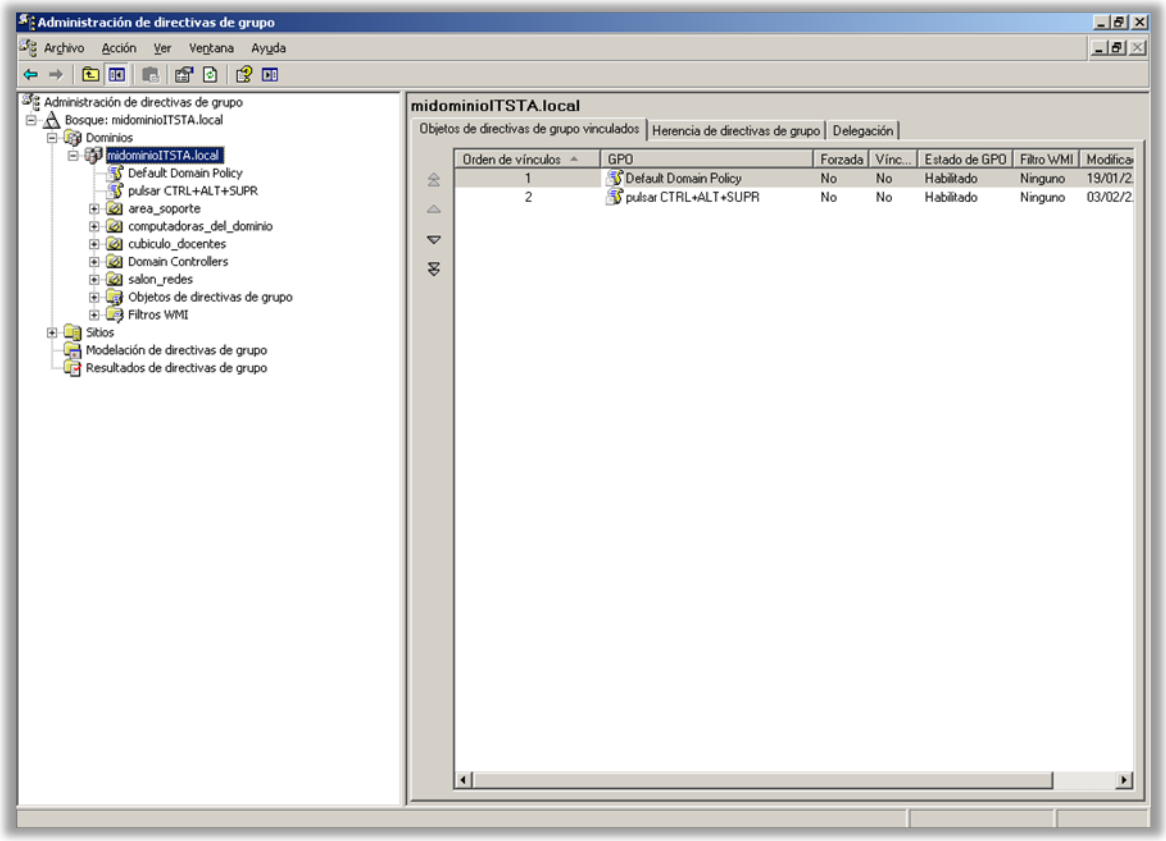


Figura 63.- Objetos de Directiva de grupo en la raíz del dominio

3.7.5.3 Para ver todos los objetos de Directiva de grupo asociados a un contenedor determinado

En el árbol **Dominios**, haga clic en el signo más (**+**) situado junto a **midominioITSTA.local** y, a continuación, haga clic en **Objetos de Directiva de grupo**.

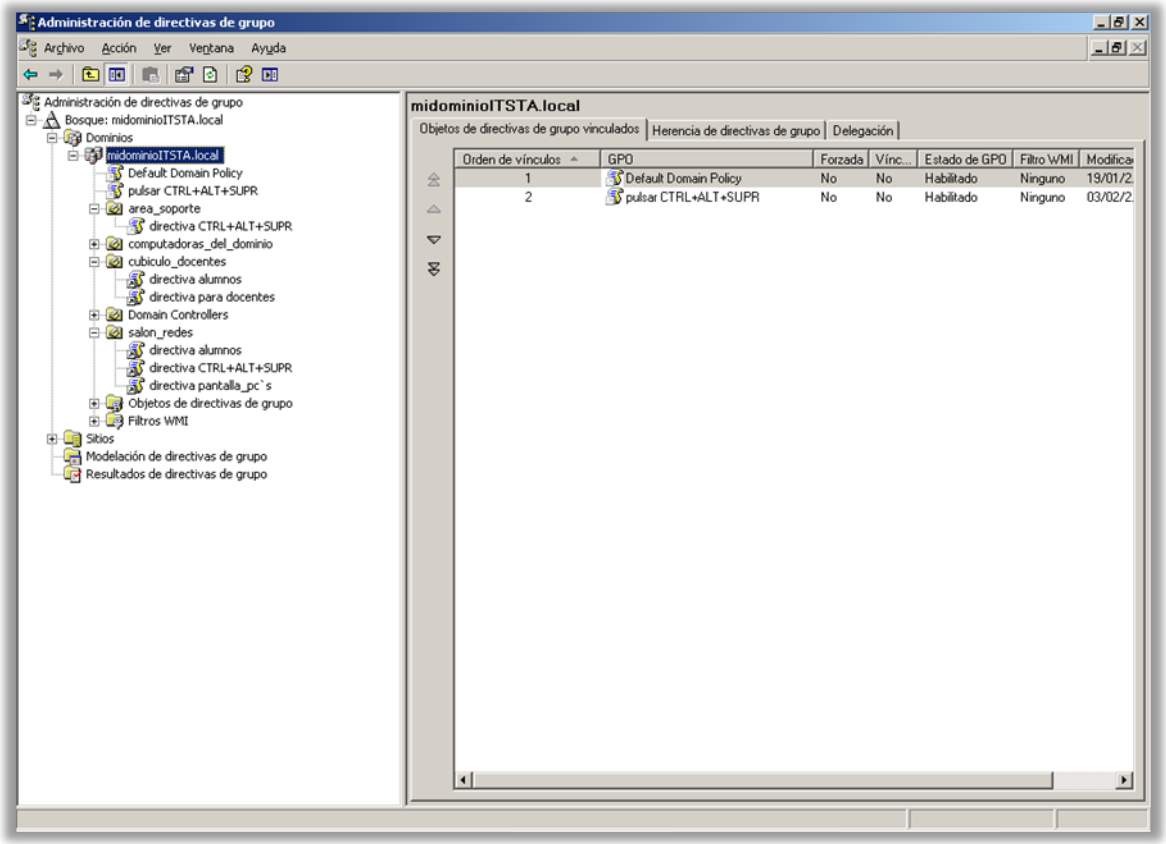


Figura 64.-objetos de directiva de grupo del dominio

3.7.5.4 Buscar objetos de Directiva de grupo

Se pueden buscar objetos de Directiva de grupo en el nivel de bosque o de dominio. Para ajustar los resultados de búsqueda en un conjunto grande de objetos de Directiva de grupo se pueden utilizar uno o varios parámetros de búsqueda.

3.7.5.5 Para buscar un objeto de Directiva de grupo específico mediante varios parámetros de búsqueda

En el árbol de la consola, haga clic con el botón secundario del *mouse* en **Bosque: midominiolTSTA.local** y, a continuación, haga clic en **Buscar**.

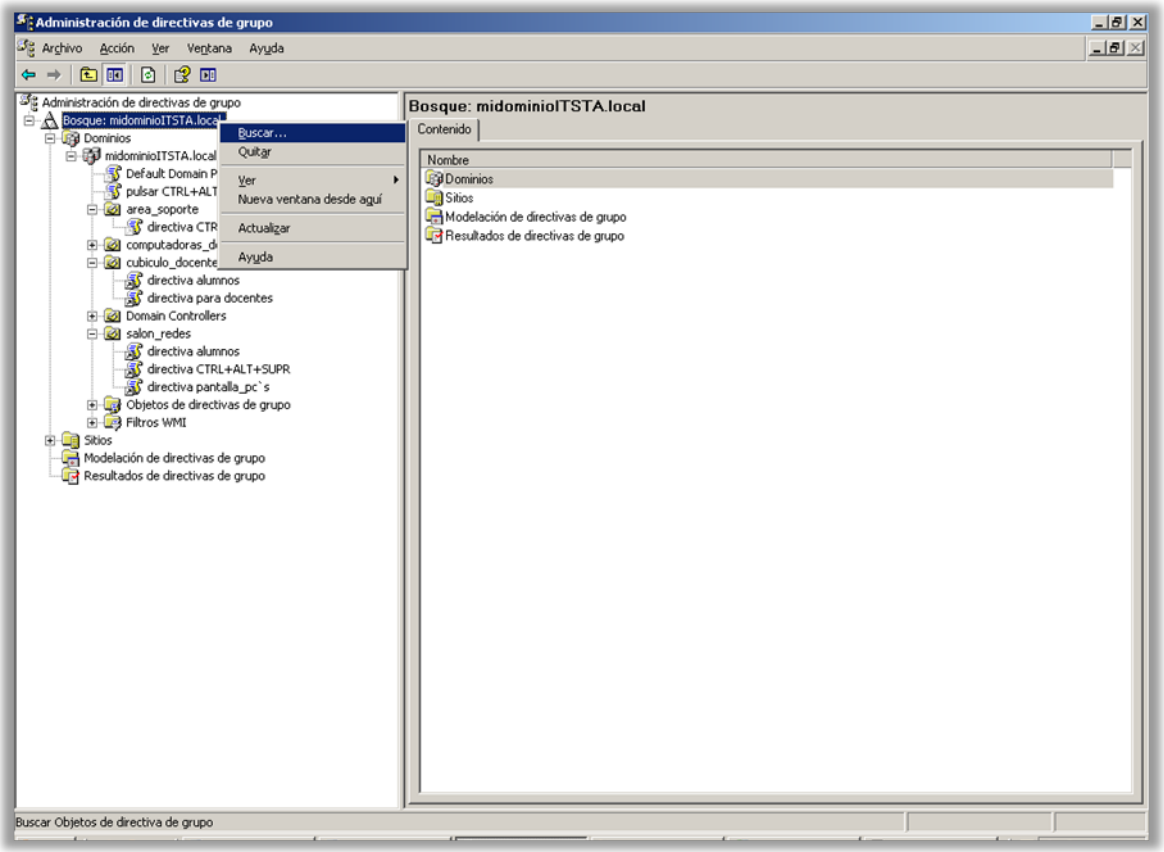


Figura 65.-buscar directiva de grupo

En el cuadro **Search item**, seleccione **Nombre del GPO**, escriba **directiva alumnos** para **Valor** y, a continuación, haga clic en Agregar.

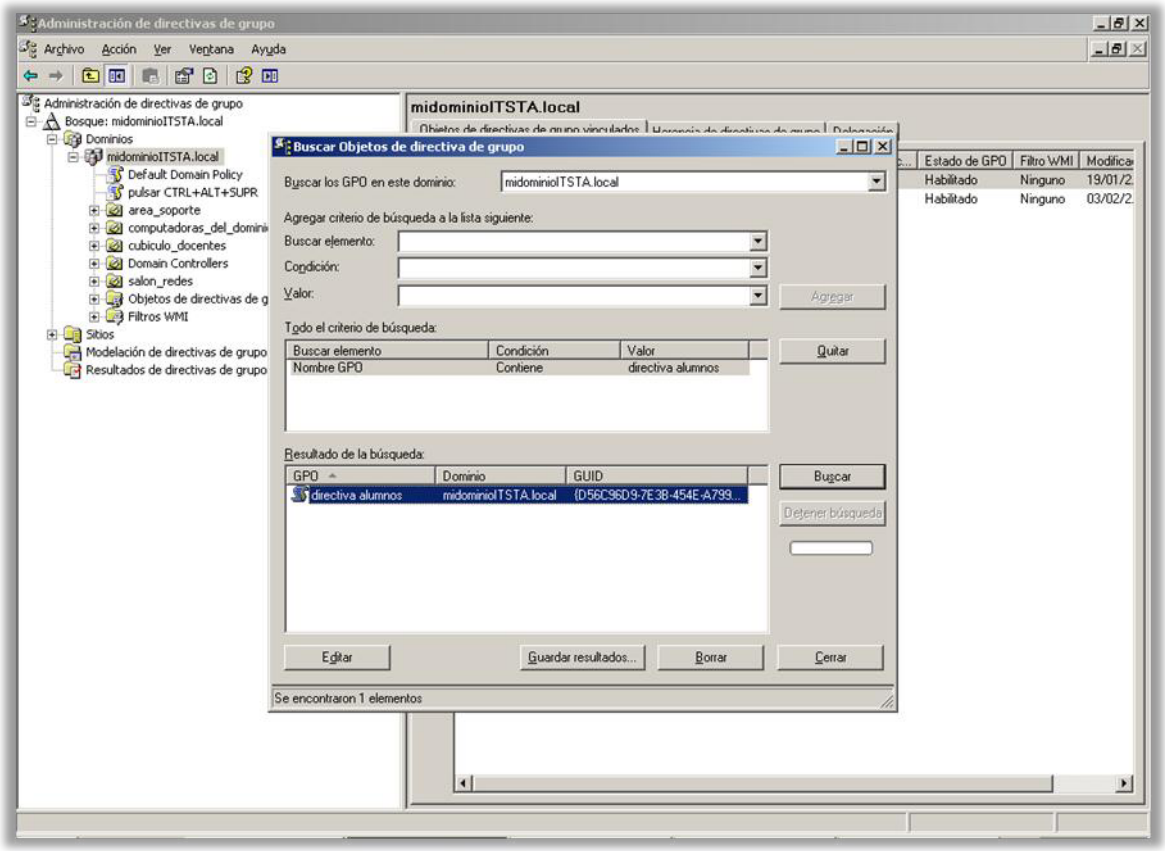


Figura 66.- resultados de la búsqueda

En el cuadro **Search item**, seleccione **Configuración del equipo**, seleccione **Seguridad** para **Valor** y, a continuación, haga clic en **Agregar**.

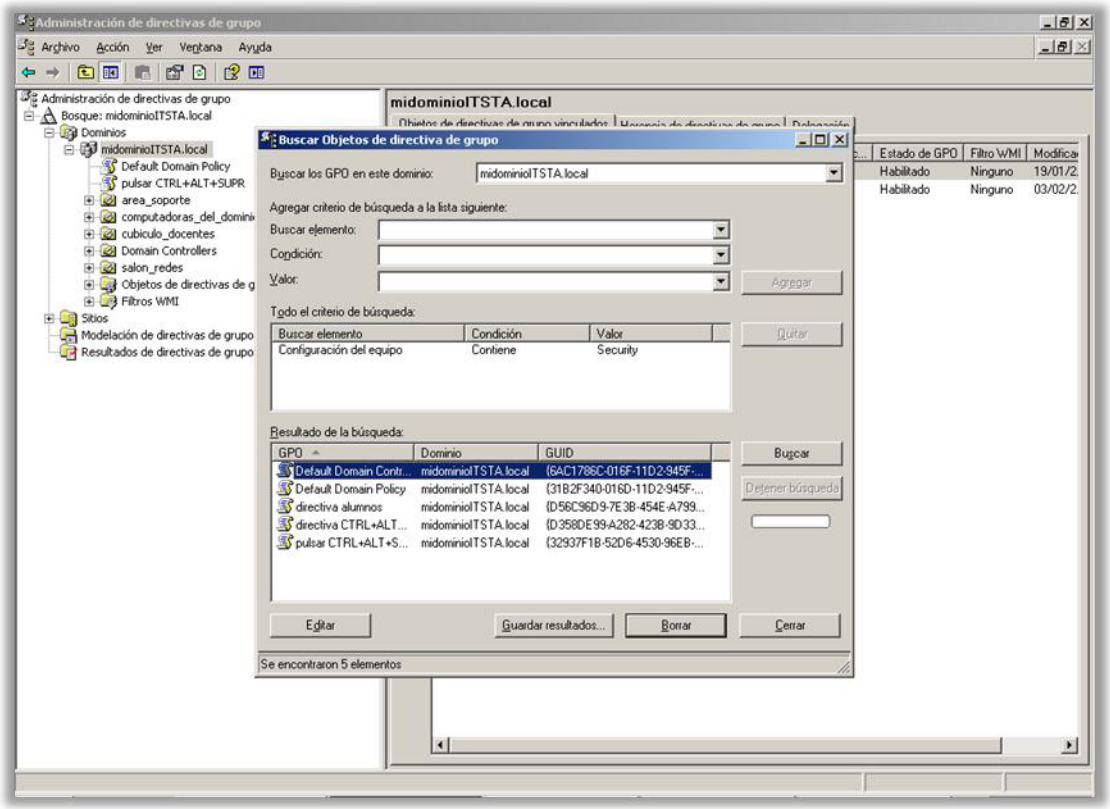


Figura 67.- Búsqueda de objetos de Directiva de grupo basada en criterios

Cuando obtenga los resultados de la búsqueda, puede realizar alguna de las operaciones siguientes:

- Para abrir el objeto de Directiva de grupo y modificarlo, haga clic en **Editar**.
- Para guardar los resultados de búsqueda, haga clic en **Save results**. En el cuadro de diálogo **Save GPO Search Results**, especifique el nombre del archivo donde desea guardar los resultados y, a continuación, haga clic en **Guardar**.
- Para desplazarse a un **objeto de Directiva de grupo** incluido en la búsqueda, haga doble clic en el **objeto de Directiva de grupo** en la lista de resultados de búsqueda.
- Para borrar los resultados de búsqueda, haga clic en **Borrar**.
- Para cerrar el cuadro de diálogo **Search for Group Policy Objects**, haga clic en **Cerrar**.

3.7.5.6 Para ver las directivas que aplica un objeto de Directiva de grupo

En el panel de resultados **directiva de usuarios**, haga clic en la ficha **Configuración** y luego en **Show All**. Aparecerá un resumen de todas las opciones de directiva definidas, como se muestra en la Figura 6. Las opciones no definidas no se muestran.

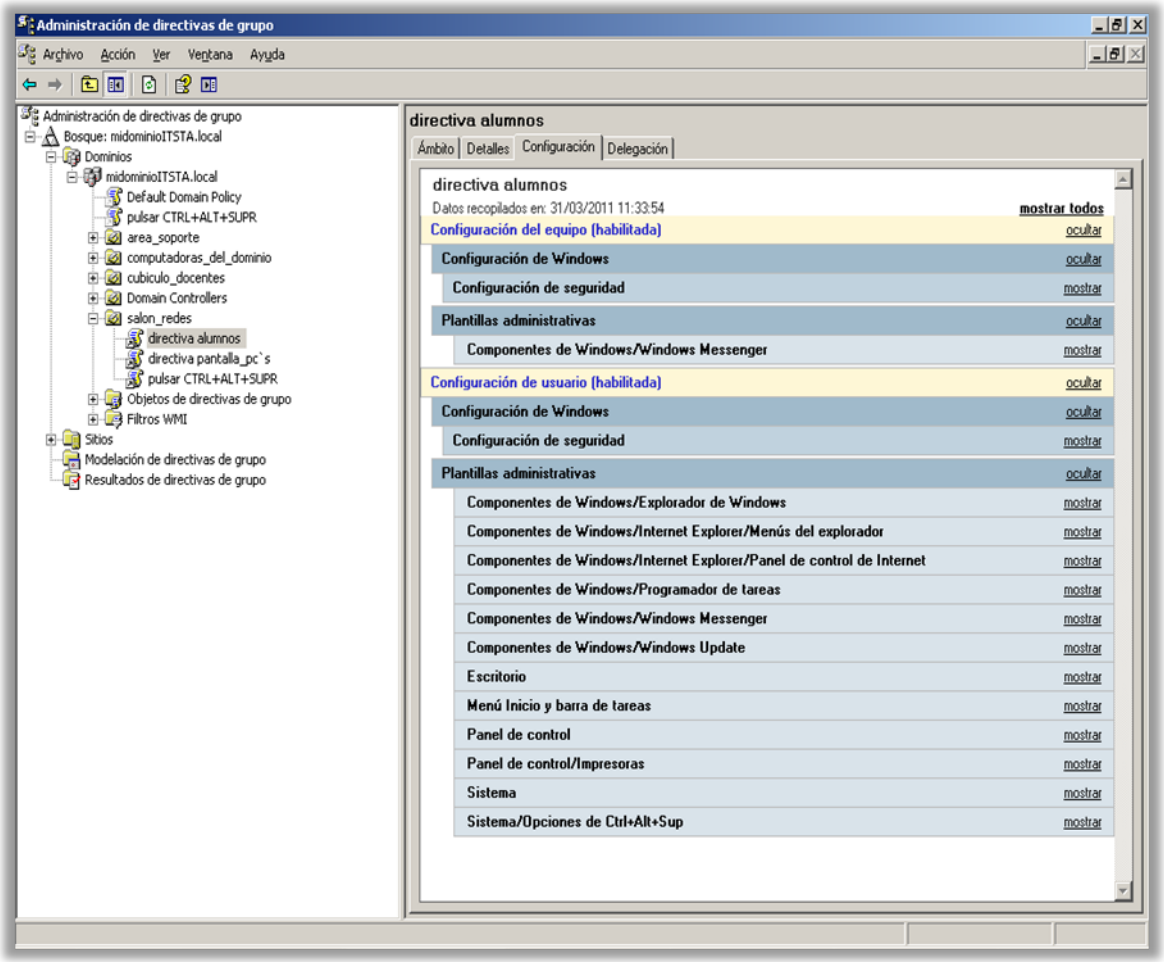


Figura 68. - Configuración de la directiva

3.8 Hacer una copia de seguridad y restaurar objetos de Directiva de grupo

3.8.1 Hacer una copia de seguridad de un objeto de Directiva de grupo

Cuando se hace una copia de seguridad de un objeto de Directiva de grupo se copian los datos del objeto en el sistema de archivos. La función de copia de seguridad sirve también como utilidad de exportación para los objetos de Directiva de grupo. Se puede utilizar una copia de seguridad de un objeto de Directiva de grupo para restablecerlo al estado de copia de seguridad o para importar la configuración de la copia de seguridad a otro objeto de Directiva de grupo.

Al hacer una copia de seguridad de un objeto de Directiva de grupo se guarda en el sistema de archivos toda la información almacenada en el interior del objeto. Esta información es la siguiente:

- El identificador único global (GUID) del objeto de Directiva de grupo y la configuración del objeto en el dominio
- La lista de control de acceso discrecional (DACL) del objeto de Directiva de grupo
- El vínculo del filtro de WMI, si hay alguno, pero no el filtro en sí
- Los vínculos a directivas de seguridad IP, si existe alguno
- El informe XML (Lenguaje de marcado extensible) de la configuración del objeto de Directiva de grupo, que se puede consultar como HTML desde GPMC
- La marca de fecha y hora de la copia de seguridad
- La descripción especificada por el usuario de la copia de seguridad

Al hacer una copia de seguridad de un objeto de Directiva de grupo sólo se guardan los datos almacenados dentro del objeto. Los datos almacenados fuera del objeto son los siguientes:

- Los vínculos a un sitio, dominio o unidad organizativa
- Los filtros de WMI
- La directiva de seguridad IP

Estos datos no están disponibles cuando se restaura la copia de seguridad al objeto de Directiva de grupo original o cuando se importa a un nuevo objeto.

3.8.2 Para hacer una copia de seguridad del objeto Directiva de directiva alumnos del dominio

En la ventana **Administración de directiva de grupo**, bajo el árbol **midominio.local**, haga clic en la carpeta **Objetos de Directiva de grupo**.

En la carpeta **Objetos de Directiva de grupo**, haga clic con el botón secundario del *mouse* en el objeto de Directiva de grupo **directiva alumnos del dominio** y, a continuación, haga clic en **Back Up**.

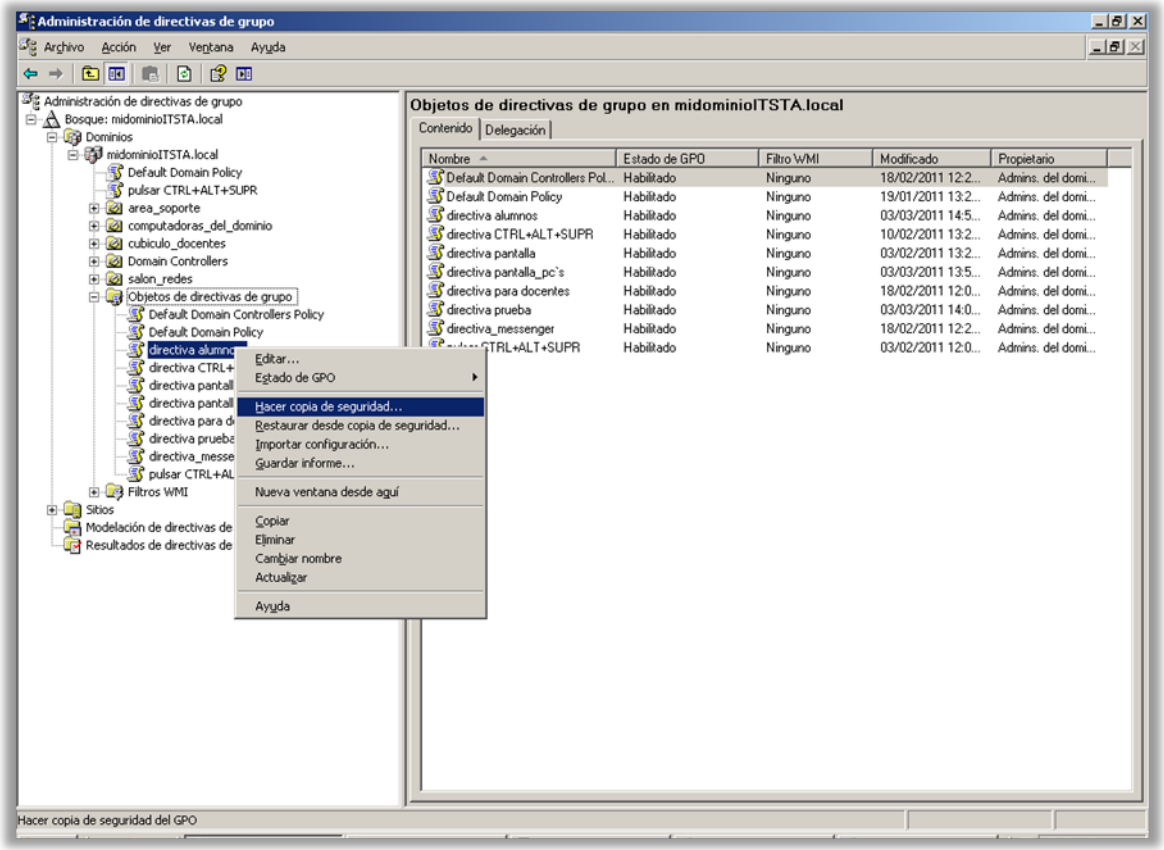


Figura 69.- hacer una copia de seguridad de la directiva

En el cuadro de diálogo **Back Up Group Policy Object**, escriba **c:\windows** para **Ubicación**, escriba **Copia de seguridad de la directiva de alumnos del dominio** para **Descripción** y, después, haga clic en **Back Up**.

Una vez realizada la copia de seguridad, haga clic en **Aceptar** para continuar.

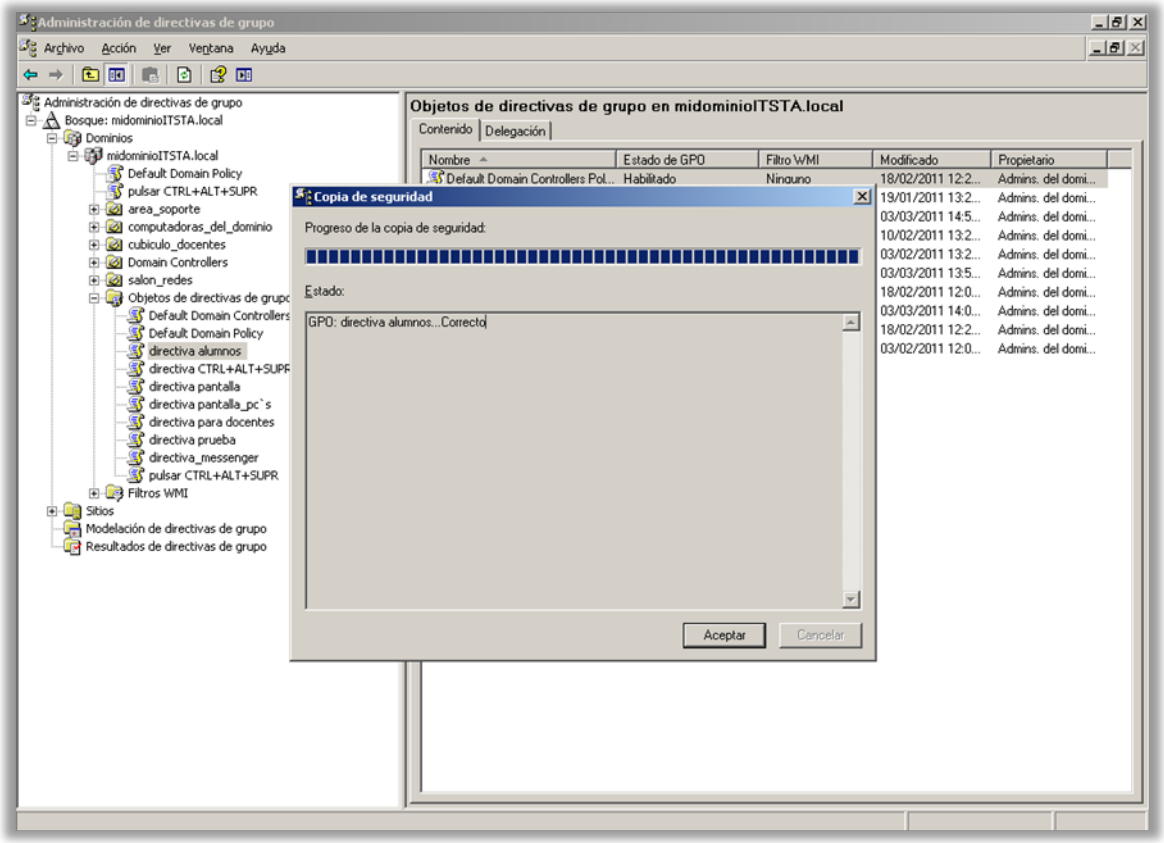


Figura 70.- copia de seguridad finalizada

3.9 Administrar copias de seguridad

En la misma ubicación del sistema de archivos se pueden almacenar varias copias de seguridad del mismo o de otro objeto de Directiva de grupo. Cada copia de seguridad se identifica mediante un identificador de copia de seguridad exclusivo. El grupo de copias de seguridad de una ubicación del sistema de archivos determinada se puede administrar con el cuadro de diálogo Manage Backups de GPMC o mediante interfaces programables con secuencias de comandos. El cuadro de diálogo Manage Backups está disponible haciendo clic con el botón secundario del *mouse* en el nodo Dominio o en el nodo Objetos de Directiva de grupo de un determinado dominio. Cuando se abre Manage Backups desde el nodo Objetos de Directiva de grupo, la vista se filtra automáticamente para que sólo aparezcan las copias de seguridad de los objetos de Directiva de grupo de ese dominio. Cuando se abre desde el nodo Dominio, en el cuadro de diálogo Manage Backups se muestran todas las copias de seguridad, sean del dominio que sean.

3.9.1 Para administrar las copias de seguridad de objetos de Directiva de grupo disponibles

En la ventana **Administración de directiva de grupo**, bajo el árbol **midominio.local**, haga clic con el botón secundario del *mouse* en la carpeta **Objetos de Directiva de grupo** y, a continuación, haga clic en **Manage Backups**. La ventana Manage Backups debe tener un aspecto similar al de la Figura 72.

En la ventana **Manage Backups**, haga clic para resaltar la **Copia de seguridad de la directiva de contraseñas del dominio** creada anteriormente y, después, haga clic en **Ver configuración**.

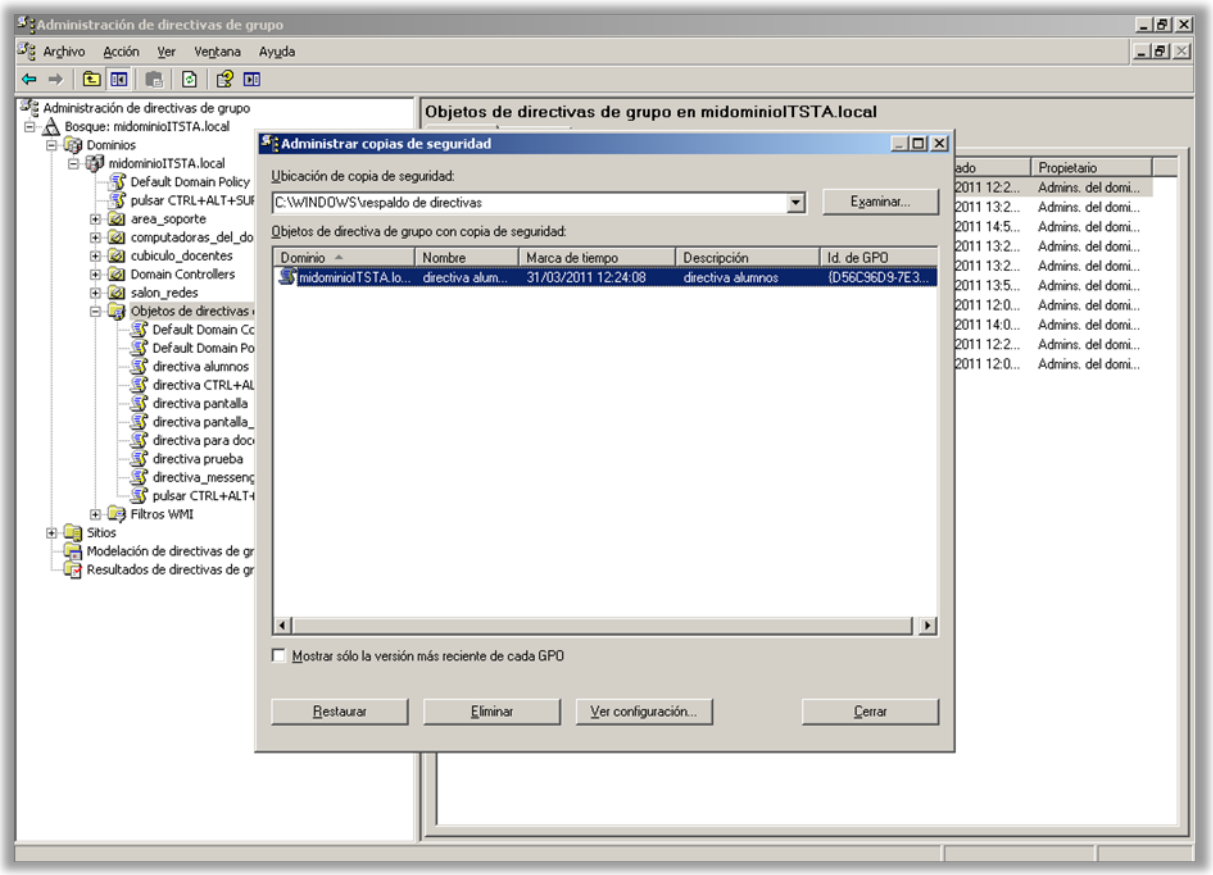


Figura 71. Administrar copias de seguridad

Una vez dando clic en ver configuración se abrirá una ventana de Internet Explorer como se muestra en la figura 74, mostrando a detalle cada una de las directivas, en este caso se muestra la directiva de alumnos, desplegándose los detalles de la configuración de la directiva de grupo. Y de esta manera poder observar y recordar la configuración de la directiva de la copia de seguridad del objeto que tenía establecido.

Revise la información detallada sobre el objeto de Directiva de grupo y, a continuación, cierre **Internet Explorer**.

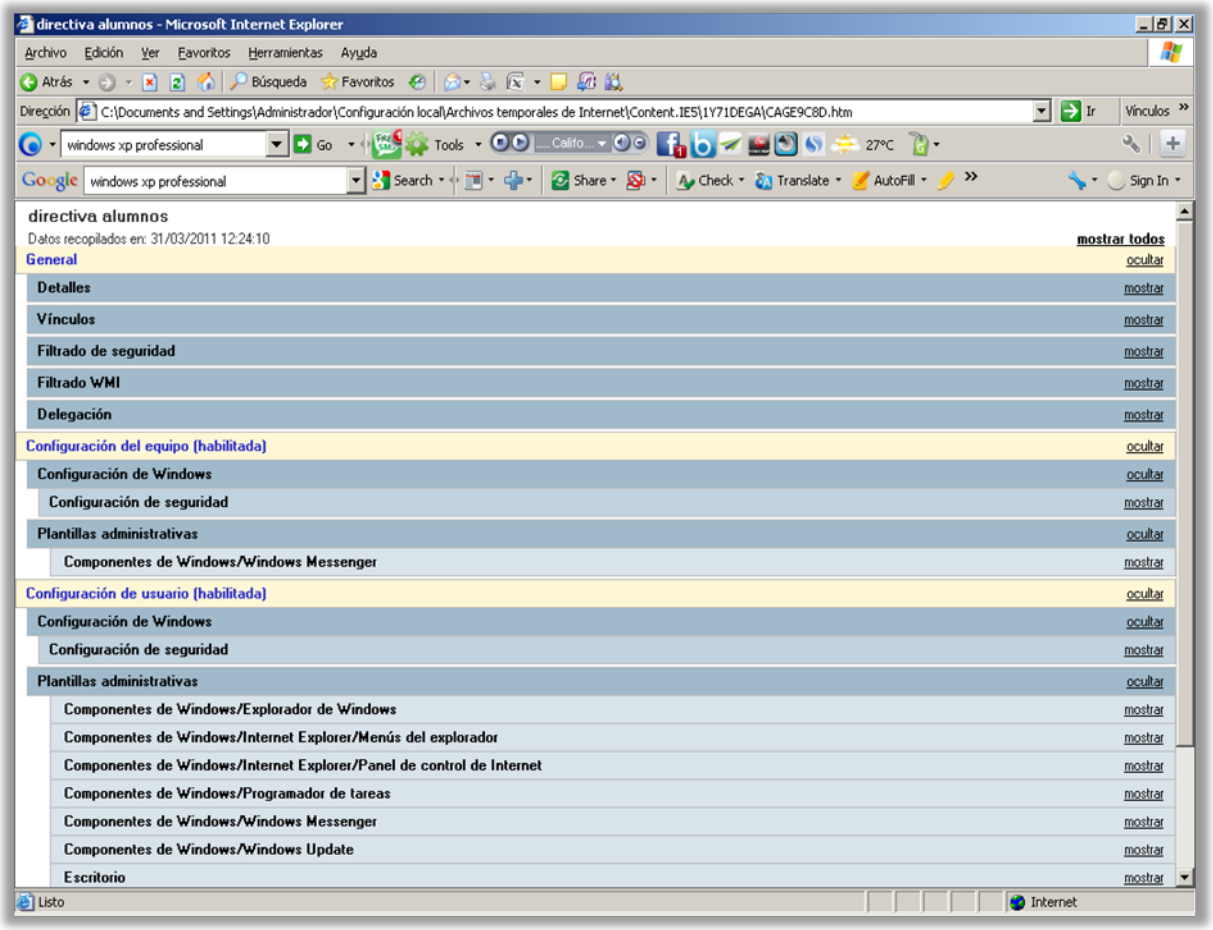


Figura 72.- configuración de la directiva de alumnos

3.10 Restaurar una copia de seguridad

Cuando se restaura un objeto de Directiva de grupo se vuelve a crear el objeto a partir de los datos incluidos en la copia de seguridad. Una operación de restauración se puede utilizar en las siguientes circunstancias: se ha hecho una copia de seguridad del objeto de Directiva de grupo pero se ha eliminado, o el objeto de Directiva de grupo está activo pero desea restablecerlo a un estado anterior conocido. Una operación de restauración reemplaza los siguientes componentes de un objeto de Directiva de grupo.

- La Configuración del objeto
- La lista DACL del objeto
- Los vínculos de filtro de WMI (pero no los propios filtros)

La operación de restauración no restaura objetos que no forman parte del objeto de Directiva de grupo. Estos objetos incluyen vínculos a un sitio, dominio o unidad organizativa, filtros de WMI y directivas IPSec.

3.10.1 Para restaurar el objeto Directiva de contraseñas del dominio

1. En la ventana **Manage Backups**, haga clic en **Restore**.
2. Cuando se le indique, haga clic en Aceptar para restaurar la copia de seguridad seleccionada.
3. Haga clic en Aceptar cuando termine la restauración del objeto de directiva de grupo.
4. En el cuadro de dialogo **Manage backups**, haga clic en cerrar. Como se muestra en la figura 73.

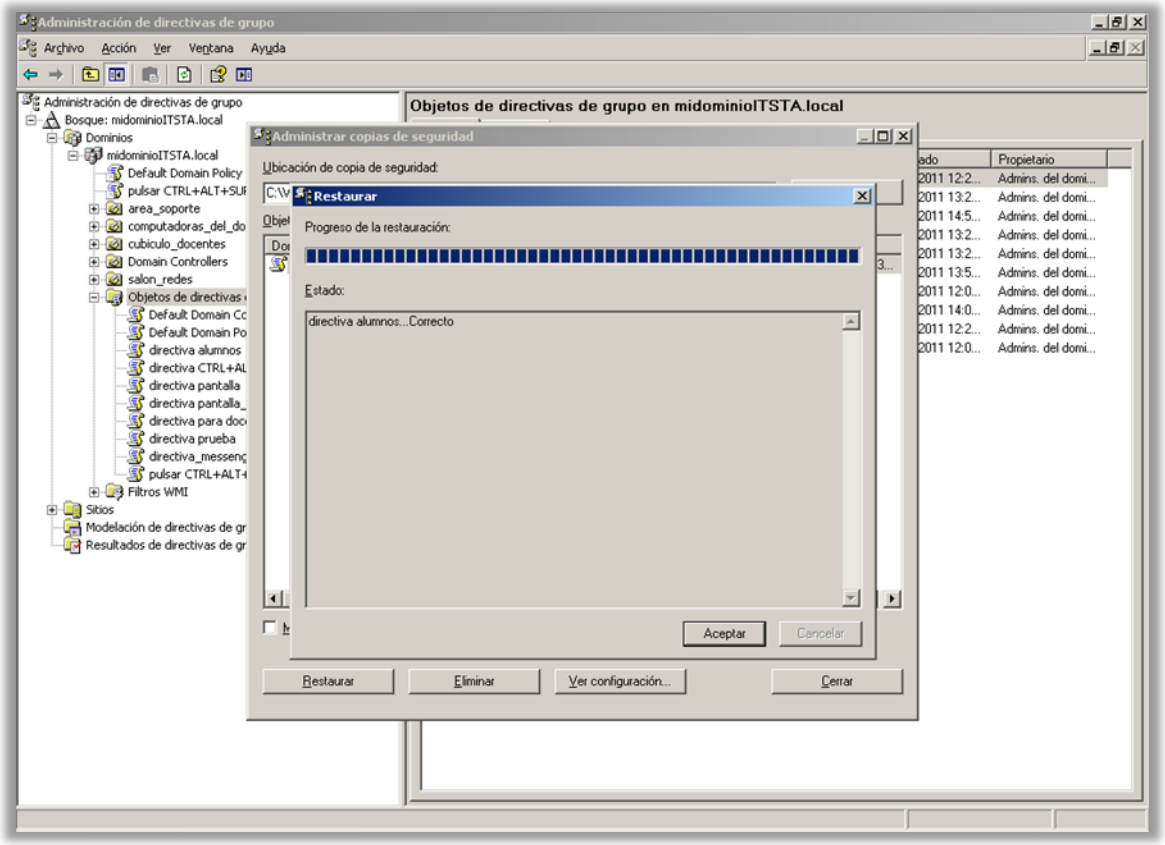


Figura 73.- finalización de la restauración de la copia de seguridad de la directiva.

3.11 Administrar la directiva de grupo

Para administrar la directiva de grupo:

Obtenga acceso al menú contextual de un sitio, un dominio o una unidad organizativa.

Seleccione propiedades y, después, haga clic en la ficha directiva de grupo. Aparecerá la página propiedades de directiva de grupo.

A continuación se muestran todos los objetos de directiva de grupo que están asociados a la unidad organizativa, dominio o sitio actualmente seleccionado. Los vínculos son objetos: tienen un menú contextual al que pueda tener acceso haciendo clic con el botón secundario del mouse en el objeto. (Al hacer clic con el botón secundario del mouse en el espacio en blanco se muestra un menú contextual para crear un nuevo vínculo, agregar un vínculo o actualizar la lista).

En la imagen también se muestra una lista de objetos de directiva de grupo ordenados, con el objeto con la prioridad más alta al principio de la lista. Puede cambiar el orden de la lista seleccionando un objeto de directiva de grupo y utilizando las teclas de dirección **arriba y abajo.**

Para asociar (vincular) un objeto de directiva de grupo, haga clic en el botón **agregar.**

Para modificar un objeto de directiva de grupo de la lista, selecciónelo, y a continuación haga clic en el botón **Editar** o haga doble clic en el objeto. Se iniciara el editor e objetos de directiva de grupo, donde podrá modificar el objeto de directiva de grupo (consulte Modificar un objeto de Directiva de grupo).

Para eliminar permanentemente un objeto de directiva de grupo de la lista, selecciónelo, y después haga clic en el botón **Eliminar**. Cuando se le indique, seleccione **quitar el vinculo y eliminar el objeto de directiva de grupo permanentemente**. Tenga cuidado al eliminar un e objeto de directiva de grupo ya que podría estar asociado a otro sitio, dominio o unidad organizativa. Si solo desea quitar la asociación del objeto de directiva de grupo con el contenedor actual, seleccione el objeto de la lista de vínculos, haga clic en **Eliminar** y, después, cuando se le indique, seleccione **Quitar el vinculo de la lista.**

Para averiguar que otros sitios, dominios o unidades organizativas están asociados a un objeto de directiva de grupo determinado, haga clic con el botón secundario del mouse en el objeto, seleccione **Propiedades** en el menú contextual y, a continuación, haga clic en la ficha **Vínculos** de la página propiedades del objeto de directiva de grupo. Haga clic en **Buscar ahora** para recuperar la lista de vínculos actuales de este objeto de directiva de grupo.

Puede definir la opción No **reemplazar** haciendo clic con el botón secundario del mouse en el objeto de directiva de grupo. Esta opción marca el objeto de directiva de grupo seleccionado para que sus directivas no puedan ser reemplazadas por otro objeto de directiva de grupo.

Nota: puede habilitar la opción No reemplazar en varios objetos de directiva de grupo. Todos los objetos de directiva de grupo marcados como No reemplazar tendrán

prioridad sobre los que no están marcados con esta opción. De los marcados como No reemplazar, los que tienen la prioridad más alta, se aplicaran después de los demás objetos de directiva de grupo marcados con esta opción.

Puede definir el objeto de directiva de grupo como **Deshabilitado** haciendo clic con el botón secundario del mouse en el, con lo que deshabilitara (desactivara) el objeto de directiva de grupo sin quitarlo de la lista.

Nota: también es posible deshabilitar solo la parte de usuario yo Equipo del objeto de directiva de grupo. Para ello, haga clic con el botón secundario del mouse en el objeto de directiva de grupo, haga clic en **Propiedades** y, a continuación, en la ficha general, haga clic en **Deshabilitar los parámetros de configuración del equipo o Deshabilitar los parámetros de configuración de usuario.**

En la página de propiedades de directiva de grupo del contenedor de active Directory puede definir **Bloquear la herencia de directivas** para invalidar todos los objetos de directiva de grupo que se encuentran en la parte superior de la jerarquía. Sin embargo, no puede bloquear ningún objeto de directiva de grupo de aplicación forzosa mediante la casilla de verificación **No reemplazar**; estos objetos de directiva de grupo siempre se aplican.

Nota: las opciones de directiva incluidas en objeto de directiva de grupo local no se reemplazan específicamente por opciones de directiva basadas en dominio siempre se aplican. Bloquear la herencia de directivas no quitara la directiva local en ningún nivel.

3.12 Unirse a un dominio mediante una estación de trabajo con Windows XP Profesional

Cuando configura una red, Windows crea automáticamente un grupo de trabajo y le da un nombre. Puede unirse a un grupo de trabajo existente de una red o crear uno nuevo. Cuando se configura el servidor como un controlador de dominio, se crea un dominio en donde nuestras estaciones de trabajo se unirán a él.

Para que los equipos se unan a un dominio se sigue los siguientes pasos:

En el panel de control, accedemos a sistema y seguridad, y hacemos cli en seguridad, posteriormente haga clic en Cambiar la configuración. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación. Aparecerá una ventana como en la figura 76

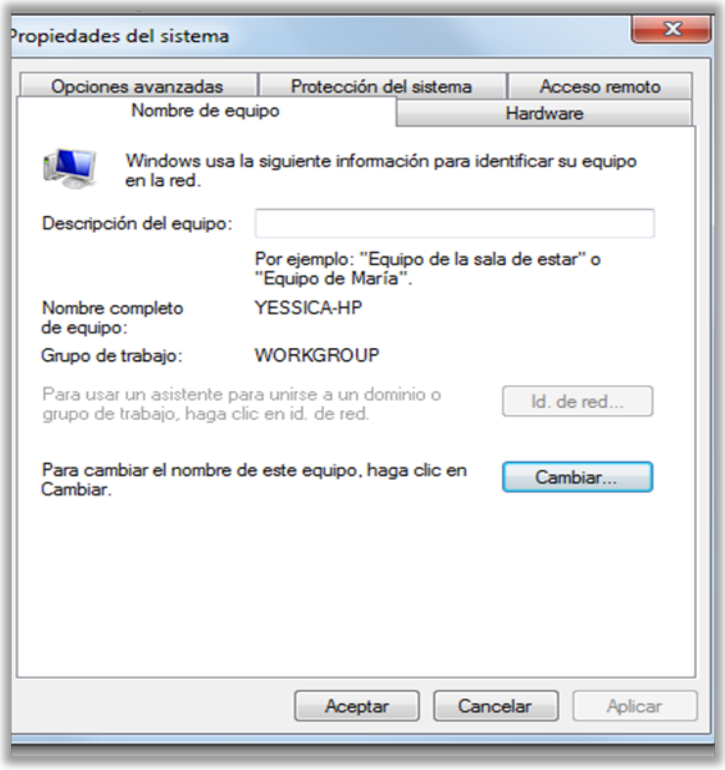


Figura 74.- imagen para agregar un equipo ya sea a un grupo de trabajo o a un dominio.

Haga cli en cambiar y se abrirá una ventana como en la figura 77 y seleccionamos dominio y enseguida escribimos el nombre del dominio al que se desee unirse.

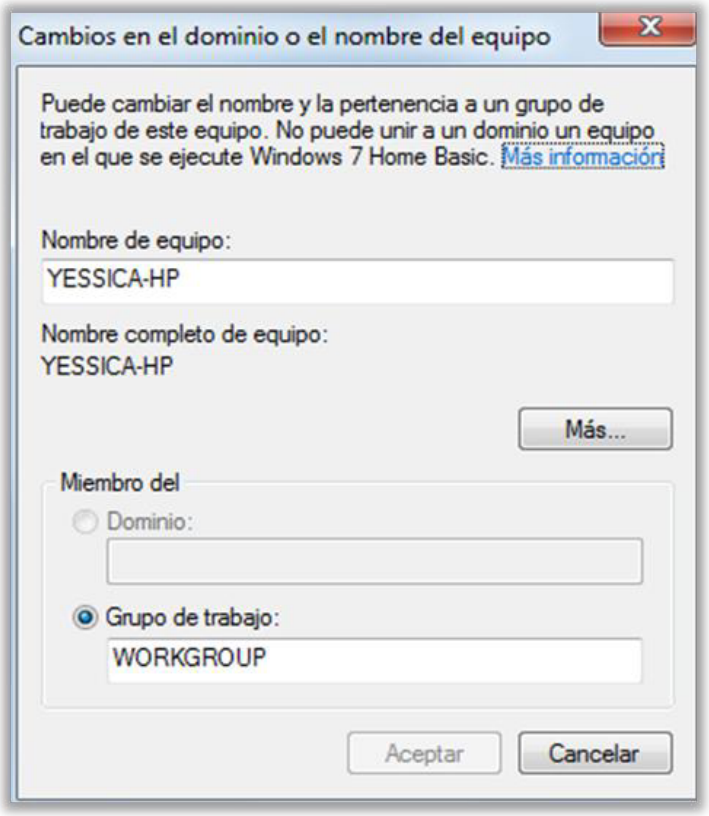


Figura 75.- unirse a un dominio.

Si el equipo formaba parte de un dominio antes de unirse al grupo de trabajo, se quitará del dominio y la cuenta del equipo en ese dominio se deshabilitará.

Nota:

Si la red incluye equipos que ejecutan Windows XP, es posible que deba cambiar el nombre del grupo de trabajo en esos equipos de forma que coincida con el nombre del grupo de trabajo de los equipos que ejecutan esta versión de Windows para poder ver y conectarse a todos los equipos de la red.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

4.2 Recomendaciones

En el presente capitulo se darán a conocer los resultados del proyecto. También se hará hincapié a algunas recomendaciones por si en un futuro el proyecto se lleve a cabo.

4.1Conclusiones

Con el paso del tiempo la necesidad de contar con una red estructurada, segura y sobre todo operativa, hoy en día ya no es un lujo para una empresa e institución ya que con la llegada del internet existen muchas herramientas para que se vea amenazada nuestra red y sobre todo nuestra información.

El contar con un controlador de dominio es de vital importancia en cualquier red, ya que el administrador se verá beneficiado a simplificarse la tarea de administrar a todos los usuarios de la red y recursos de la red como son: impresoras, routers, switch, ancho de banda, etc. Ya que a diferencia del contar con un servidor de usuarios con el grupo de trabajo el administrador tendrá que asignarle contraseñas y ciertos parámetros de seguridad a usuario por usuario y esto se hace una tarea muy tediosa para el administrador. Ya que a diferencia del grupo de trabajo con el controlador de dominio se ahorrará todo ese trabajo y hará su tarea de una manera más exacta y fácil.

Es de gran ayuda el poder contar con un módulo didáctico para la materia de redes que es una de las ramas más importantes y demandantes en el mundo laboral, los alumnos que cursaran esta materia realmente tendrán demasiados beneficios uno de los más importantes es que los estudiantes aprendan a hacer uso de los sistemas de monitoreo de red y aprender internamente como funciona una red. Al igual que también como en la formación como ingenieros en sistemas computacionales identifiquen y aprendan a examinar los problemas de seguridad en la red.

4.2 Recomendaciones

Es recomendable utilizar el Sistema operativo Windows XP Professional en las maquinas cliente.

Para el excelente funcionamiento se debe de asignar el control del servidor a un administrador experto en redes para que no llegue a ocurrir daños que pueda provocar fallos en el sistema.

Si en dado caso se viera la necesidad de reinstalar el servidor se debe de tomar en cuenta varios puntos antes de la instalación como son:

- El tipo de licencia
- El espacio en el disco duro para la instalación del sistema operativo Windows server 2003.
- Definir el nombre del dominio.
- Se deben de definir muy bien las directivas de seguridad basándose en el tipo de usuarios, asignándole o denegándole derechos y permisos.

Es recomendable que se implanten ciertas políticas para este sistema, se menciona porque cada cierto tiempo se van dando de alta usuarios y los permisos y derechos pueden ser cambiados de acuerdo a las necesidades de cada usuario.

Por último este proyecto está abierto para todas aquellas mejoras posibles que se le puedan realizar o agregarle, solamente es necesario en que se pongan de acuerdo con el asesor del proyecto.

REFERENCIAS BIBLIOGRAFICAS

José Luis raya, Laura raya, Miguel A. Martínez
Domine Microsoft Windows server 2003
Alfaomega Ra-Ma
México, Mayo 2007

Guía detallada de infraestructura común para la implementación de Windows Server 2003
http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/domcntrl.mspx
Publicado: septiembre 17, aaaa

Guía detallada de aplicación de directivas de contraseñas seguras
http://www.microsoft.com/spain/technet/recursos/articulos/strngpw.mspx
Publicado: septiembre 17, 2004

Crear cuentas de usuario en Windows Server 2003
http://redeswindows.wordpress.com/2010/12/02/crear-cuentas-de-usuario-en-windows-server-2003/
Posted Tue, Dec 20 2005 14:29 by juansa

Guía detallada de administración de Active Directory
http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/admng.mspx
Publicado: septiembre 17, aaaa

Introducción al sistema de monitoreo System Surveillance Pro 5.5
http://www.64bitprogramlar.com/system-surveillance-pro-5-5-1269.html
Monday, 26 July, 2010

Introducción al sistema de monitoreo Radmin 3.2

http://www.radmin.es/download/files/manuals/radmin22es.pdf

Demostración de Observer la Herramienta de Análisis y Monitoreo de Redes
http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/demostracion-de-observer.html

Marzo 17/2011
Foro y debate Emagister donde se dan soluciones a las distintas problemáticas.
www.emagister.com.mx

Manual de instalación paso a paso del sistema Windows server 2003© Microsoft Corporation
http://multingles.net/docs/juansa/w2003.pdf

Windows 2000 Server. Instalación, Configuración y Administración
http://www.monografias.com/trabajos26/windows-server/windows-server.shtml

Windows Server 2003 como un Controlador de dominio.
http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/domcntrl.mspx
Publicado: septiembre 17, aaaa

Objetos que administra un dominio
http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch03s03.html