PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE INGENIERÍA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

IMPLEMENTACIÓN DE UN CONTROLADOR DE DOMINIO BASADO EN LA PLATAFORMA MICROSOFT WINDOWS SERVER 2003 EN LA PUCESA EN EL PERIODO 2007

Autores:

ÁLVARO FABIAN VILLACRÉS BARRERA
NELSON EDUARDO CORTEZ GARZÓN

Asesor:

ING. VERÓNICA PAILIACHO

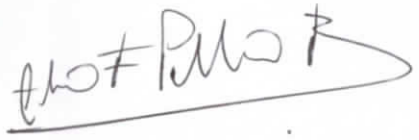
Ambato – Ecuador

Febrero 2007

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Álvaro Fabián Villacrés Barrera portador de la cédula de ciudadanía No. 1802608669 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del Título de Ingeniería en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto son de exclusiva responsabilidad legal y académica del autor.

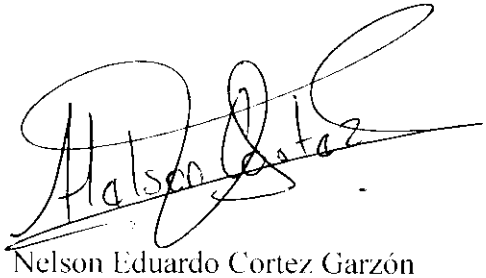


Álvaro Fabián Villacrés Barrera
CI. 180260866-9

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Nelson Eduardo Cortez Garzón portador de la cédula de ciudadanía No. 1803413572 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del Título de Ingeniería en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto son de exclusiva responsabilidad legal y académica del autor.



Nelson Eduardo Cortez Garzón

CI. 1803413572

ÍNDICE

CAPÍTULO I

CAPÍTULO II

CAPÍTULO IV

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

1. PROYECTO DE INVESTIGACIÓN

1.1 Introducción

En la actualidad la administración de redes no es solo la interconexión entre un conjunto de computadores que permiten la transmisión de datos, sino que se ha convertido en un campo muy amplio el cual envuelve muchos ámbitos que permiten controlar recursos compartidos de la red y sus objetos.

Existen diferentes técnicas en las que se puede aplicar un controlador de dominio, sin embargo en el presente proyecto se implementará una estrategia organizacional que estandarizará grupos, unidades organizativas, usuarios y equipos.

En una red que cuenta con muchos usuarios es necesario llevar el control de autenticación para autorizar o denegar los recursos de la red, auditando las acciones realizadas por los usuarios o cuentas de equipo con políticas de seguridad.

Esto conlleva a un proceso de investigación, pruebas e implementación de una herramienta como el Sistema Operativo Microsoft Windows Server 2003 que permite una correcta administración de la red.

La Pontificia Universidad Católica del Ecuador Sede Ambato se verá beneficiada con esta estrategia de administración puesto que ayuda al correcto mantenimiento de la red.

1.2 Planteamiento del problema

Carencia de un Controlador de Dominio para administrar los recursos de red de la PUCESA en el periodo 2006 -2007.

1.3 Problematización

- Necesidad de un equipo adecuado para la implementación de un Controlador de Dominio.
- Carencia de un esquema de grupos, unidades organizativas, usuarios y equipos finales en la red.
- Falta de control de usuarios y equipos no identificados en la red.
- Falta de seguridades que protejan la configuración de los equipos.

1.4 Delimitación

1.4.1 Tiempo

El proyecto esta previsto realizarlo en ocho meses a partir de la fecha de aprobación del plan.

1.4.2 Espacial

El proyecto será realizado en la Pontificia Universidad Católica del Ecuador sede Ambato, específicamente en el centro de cómputo.

1.4.3 Técnico

En la investigación e implementación del Controlador de Dominio basado en Microsoft Windows Server 2003, abarcará solo tres aspectos: Creación de

1.6 Importancia

El proyecto está destinado para mejorar el control y administración de los recursos de red. Con la implementación de un Controlador de Dominio se da inicio a lo que es una infraestructura de red organizada y de última tecnología, con esto pretendemos encauzar a la PUCESA, por nuevos caminos para la centralización de la información.

1.7 Objetivos

1.7.1 Objetivo General

Implementar un Controlador de Dominio basado en la plataforma Microsoft Windows Server 2003 para administrar los recursos de red de la PUCESA en el periodo 2007.

1.7.2 Objetivos Específicos

- Dotación de un equipo servidor HP ProLiant ML 150 G2 con un procesador Intel Xeon de 3.2 GHZ y 1024 MB de RAM, capacidad suficiente para asegurar el buen funcionamiento de dicha aplicación.
- Creación de Grupos y Unidades Organizativas, para administrar el acceso de usuarios y equipos a recursos compartidos de la red, con asignación de permisos y privilegios.
- Creación de Cuentas de usuarios y equipos, para autenticar la identidad y autorizar o denegar los recursos de la red auditando las acciones realizadas por los usuarios o cuentas de equipo con políticas de seguridad.
- Ejecución del servicio DHCP, el cual permite controlar a los usuarios y equipos dentro de la red.

- Aplicación de Políticas de Seguridad a nivel de Dominio y Unidades Organizativas.

1.8 Hipótesis

Luego de la implementación de un Controlador de Dominio basado en la plataforma Microsoft Windows Server 2003 en la PUCESA en el periodo 2007 se obtendrá una mejora en el control y administración de los recursos de red satisfaciendo las necesidades del centro de cómputo.

1.9 Aspectos Metodológicos

1.9.1 Paradigma de Investigación

- El paradigma racionalista será utilizado en este proyecto, ya que parte de una idea que la mantenemos y la realizaremos en el tiempo y lugar establecidos.
- También se utilizará el paradigma pragmatista, ya que se ocuparán conceptos teóricos investigados que conllevarán al éxito del proyecto.

1.9.2 Metodología de la Investigación

Se tendrá presente el siguiente método:

Método Científico.- El tratamiento que se da al problema es experimental ya que se utilizará equipo y software de última generación.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Revisión de Microsoft Windows Server 2003

Para poder apreciar de mejor manera las capacidades y funcionalidades del nuevo sistema operativo de Microsoft Windows Server 2003 hay que entender los orígenes. Windows NT Server fue el primer sistema operativo de Microsoft que fue construido con la idea de red Cliente Servidor e introducir la idea de dominios, con unidades organizativas a las cuales pertenecían usuarios y computadores, después con el lanzamiento de Windows Server 2000, Microsoft afirma completamente un poderoso servicio de directorio llamado Active Directory, que provee una administración centralizada orientada a objetos.

2.1.1 Características de Microsoft Windows Server 2003

- **Sistema de ficheros NTFS.-** Permite encriptación y compresión de archivos, carpetas y unidades completas.
- **Gestión de almacenamiento.-** Consiste en utilizar un algoritmo de cache para pasar los datos menos usados de disco duro a medios ópticos o mas lentos y volverlos a leer a disco duro cuando se necesitan.
- **Windows driver model.-** Implementación básica de los dispositivos más utilizados.
- **Active Directory.-** Directorio de organización, permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.
- **Políticas de seguridad.-** Implementación de directivas de grupo.
- **DNS.-** Registro de IP's automáticamente.

2.1.2 Versiones de Microsoft Windows Server 2003

- **Web Edition.-** Diseñado para los servicios y el hospedaje Web, ofrece una plataforma para desarrollar e implementar rápidamente servicios y aplicaciones Web.
- **Standard Edition.-** El más versátil de todos, ofrece un gran número de servicios útiles para empresas de cualquier tamaño.
- **Enterprise Edition.-** Desarrollado para empresas de tamaño medio o grande, permite disponer de infraestructura comercial, aplicaciones de unidad de negocio y transacciones de comercio electrónico.
- **Datacenter Edition.-** Concebido para permitir la creación de importantes soluciones empresariales que requieren las bases de datos más escalables y un procesamiento de transacciones de gran volumen. También resulta una plataforma ideal para la consolidación de servidores.

2.1.3 El Árbol Familiar de los Sistemas operativos NT

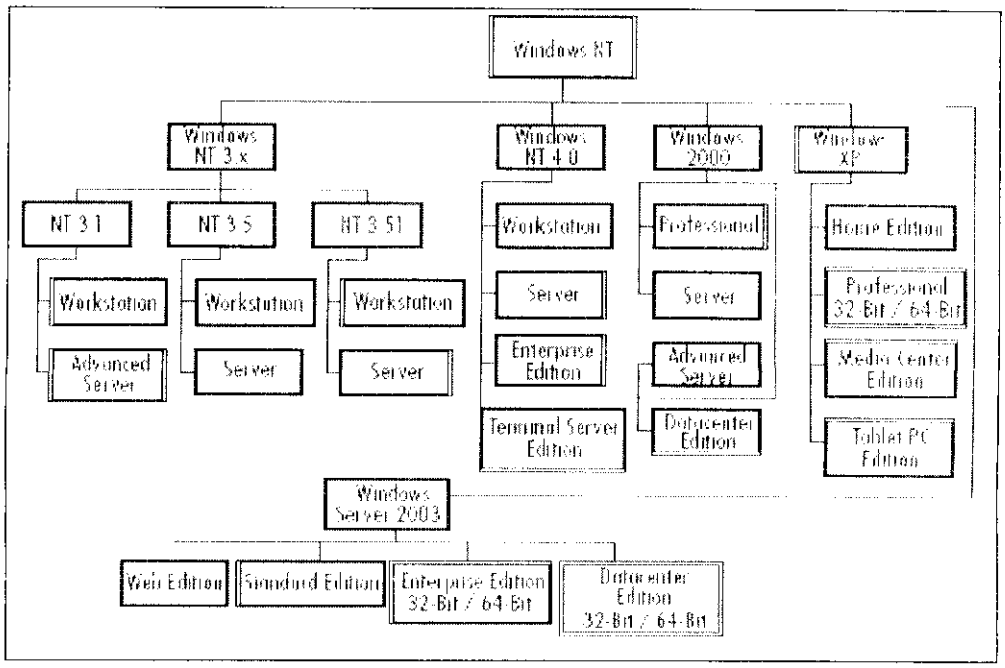


Figura 2-1 El árbol familiar de los SO NT

2.1.4 Fundamentos del Sistema Operativo Windows Server

"Windows empezó como un producto, que hacía que los computadores fueran independientes de otros[1]". La industria computacional respondió ante las necesidades de los usuarios, de compartir recursos entre máquinas dentro de una red, dando origen a las redes p2p, a lo largo de los años las redes p2p perdieron popularidad por la dificultad de administración, apareciendo el modelo red cliente-servidor, introduciendo el concepto de dominio. Consecuentemente Microsoft introdujo un nuevo servicio de directorio llamado Active Directory para hacer mas fácil la localización de los recursos a lo largo de la red. Windows Server 2003 permite manejar cualquier modelo de red, desde p2p hasta un Dominio.

2.1.5 Redes cliente – servidor Windows Server 2003

Es la tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo y/o, a través de la organización, en múltiples plataformas. El modelo soporta un medio ambiente distribuido en el cual los requerimientos de servicio hechos por estaciones de trabajo inteligentes o clientes, resultan en un trabajo realizado por otros computadores llamados servidores, es decir los usuarios obtendrán mejores rendimientos de los recursos que ofrece la red, mientras que los administradores de red, obtendrán grandes beneficios como por ejemplo el control y la autenticación centralizada de los usuarios. Esto hace más seguro el ambiente de red.

- **Administración Centralizada**

  Para los administradores es la única manera segura y fiable de llevar una excelente administración de red. Es decir todos los recursos con los que puede contar una red están centralizados por ejemplo: la

[1] MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment. Pagina 16, Deborah Littlejohn "y" Dr. Thomas W. Zinder, 2003

2.2 TCP/IP

2.2.1 Definición

TCP/IP es un protocolo de red que permite la conexión de equipos en un entorno Lan y Wan, desarrollando un trabajo robusto, escalable, multiplataforma y cliente servidor. TCP/IP proporciona utilidades básicas que permiten a equipos conectar y compartir información con otros sistemas, es decir, permite utilidades que conectan equipos Windows con sistemas diferentes y compartir información con los mismos.

El conjunto de protocolos TCP/IP esta implementado en muchos paquetes de software de TCP/IP disponibles para muchas plataformas distintas. En la actualidad, el software TCP/IP sigue siendo de uso generalizado en Internet y se utiliza a menudo para crear conjuntos de redes privadas enrutadas de gran tamaño.

2.2.2 El Modelo

TCP/IP, esta basado en un modelo de referencia de cuatro niveles como se detalla en la tabla 2-1. Cada nivel del modelo TCP/IP corresponde a uno o más niveles del modelo de referencia intereconexión de sistemas abiertos (OSI, Open System Interconnection) de siete niveles, puestos por la organización Internacional de Normalización (ISO, International Organization for Standarization)

Nivel	Descripción	Protocolos
Aplicación	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
Transporte	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.	TCP, UDP, RTP
Internet	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.	IP, ICMP, ARP, RARP
Interfaz de red	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-23

Tabla 2-1 Protocolos TCP/IP

2.2.3 Utilidades

Existen algunos tipos de utilidades basadas en TCP/IP como:

- "Utilidades de conectividad como por ejemplo FTP, RCP, TELNET, etc, que permiten utilizar e interactuar con recursos en diversos hosts con sistemas por ejemplo Microsoft o UNIX, etc.

- Utilidades de diagnóstico que permiten detectar y resolver problemas en la red, como por ejemplo IPCONFIG, NSLOOKUP, PING, TRACERT, etc.[3]".

2.3 Direccionamiento IP y máscara de subred

2.3.1 Direccionamiento IP

Cada host TCP/IP esta identificado por una dirección IP lógica. Esta dirección es única para cada host que se comunica mediante TCP/IP. La dirección IP de 32 bits identifica la ubicación de un sistema host en la red. Cada dirección IP esta dividida internamente en dos partes: un Id. de red y un Id. de host:

- El Id. de red, también conocido como dirección de red, identifica un único segmento de red dentro de un conjunto de redes (una red de redes) TCP/IP más grande. Todos los sistemas que están conectados y comparten el acceso a la misma red tienen un Id. de red común en su dirección IP completa. Este Id. también se utiliza para identificar de forma exclusiva cada red en un conjunto de redes más grande.
- El Id. del host también conocido como dirección de host, identifica un nodo TCP/IP (estación de trabajo, servidor, enrutador u otro dispositivo TCP/IP) dentro de cada red. El Id. de host de cada dispositivo identifica de forma exclusiva un único sistema en su propia red.

[3] Microsoft Training and Certification Modulo 2: Planning and Optimizing a TCPI/IP Physical and logical Network 2278, Pagina 43, 2005

Ejemplo de una dirección IP de 32 bits (figura 2-3):

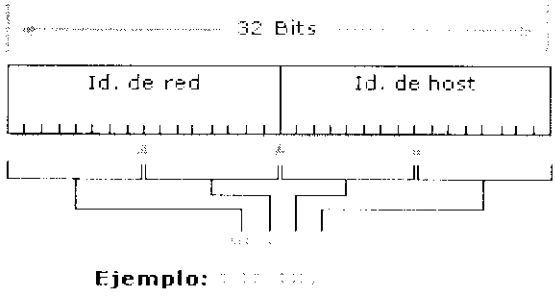


Figura 2-3 Dirección IP

2.3.2 Clases de direcciones IP

La comunidad de Internet ha definido cinco clases de direcciones. Las direcciones de las clases A, B y C se utilizan para la asignación de nodos TCP/IP. La clase de dirección define los bits que se utilizan para las partes de Id. de red e Id. de host de cada dirección. La clase de dirección también define el número de redes y hosts que se pueden admitir por cada red.

En la tabla 2-2 se utiliza w.x.y.z para designar los valores de los cuatro octetos de cualquier dirección IP dada.

- Por lo que, el valor del primer octeto (w) de una dirección IP dada, indica la clase de dirección A, B o C.
- Como están divididos los octetos de una dirección en el Id. de red y el Id. de host, es decir en dependencia de la clase el Id. de red se mantendrá, mientras que el Id. de host variara para cada clase.
- El numero de redes y hosts posibles por cada red que hay disponibles para cada clase.
- Para lo anterior mencionado tener en cuenta el enmascaramiento de red.

creación de subredes IP. Con la creación de subredes IP, se puede dividir la parte de Id. de host predeterminada en una dirección IP para especificar subredes, que son subdivisiones del Id. de red basado en la clases original.

2.4 Planificación de una Red basada en Windows Server 2003

"La planificación es el primer paso en construir una red basada en Windows Server 2003 que es confiable, de alto rendimiento y de alta disponibilidad[4]". Lo siguiente es una descripción básica de la planificación de la infraestructura de una red que presenta las estrategias de la planificación.

2.4.1 Descripción básica de la planificación de la infraestructura de red

Una planificación apropiada de la infraestructura de la red es esencial para crear un diseño de red viable, se necesitará un entendimiento de requisitos del negocio, de tecnologías actuales y emergentes de red. Cuando se planea la nueva infraestructura de una red o se mejora una red, se pueden seguir todos o algunos de los siguientes pasos:

- Documentar los requisitos del negocio, del cliente u organización.
- Crear una línea de fondo del hardware existente y la utilización de la red.
- Determinar la capacidad necesaria para la instalación física de la red, incluidos el hardware del cliente, el servidor, y también la asignación de la red para los servicios de red y las aplicaciones.
- Seleccionar un protocolo de red apropiado y un esquema de direccionamiento que sirve para el tamaño existente de la red y que asignará espacio para cualquier expansión prevista, las fusiones o las adquisiciones.

---

[4] MCSE Exam 70-293: Planning and Maintaining a Windows Server 2003 Network Infrastructure, Pagina 2, Martin Grasdal "y" Laura E. Hunter, 2003

- Especificar e implementar las tecnologías que podrán resolver las necesidades de la red, y al mismo tiempo permitir el espacio para el crecimiento futuro.

2.4.2 Estrategias de la Planificación

"Al diseñar una nueva red, comenzar con los requisitos del negocio, como la fuente principal de la información para la planificación[5]". Crear una infraestructura de red que cubra las necesidades del negocio como la tolerancia de los fallos, la seguridad, la escalabilidad y el rendimiento. Balancear estos requisitos con los tipos de servicios que los usuarios y clientes esperarán de una red moderna, el acceso al Internet, los archivos, la impresión y los servicios de las aplicaciones.

Después de determinar los requisitos del negocio de la red, lo siguiente es analizar los requisitos técnicos del negocio. Puede ser que estos requisitos se aplican a cualquier aplicación que ya está en uso o que se planea implementar, así como al hardware asociado y el sistema operador. Notar con cuidado todos estos requisitos para no crear dificultades luego en el proceso de implementación. Analizar y documentar la red existente, incluido el hardware, el software y los servicios de red que ya están en uso, esta consideración facilitará la planificación de la nueva red.

Por último, cualquier plan de red bien formado debería tener en cuenta los posibles cambios futuros en la organización, incluido el apoyo de las nuevas tecnologías y los sistemas operativos, así como el hardware y los usuarios adicionales. Los requisitos del negocio pueden cambiarse por una fusión, una adquisición o el crecimiento y expansión. Aunque sea imposible prever todos los posibles cambios de esta naturaleza, un buen diseño de red será suficientemente flexible para acomodar los ajustes necesarios.

---

[5] MCSE Exam 70-293: Planning and Maintaining a Windows Server 2003 Network Infrastructure. Pagina 3, Martin Grasdal "y" Laura E. Hunter, 2003

2.4.3 Uso de las Herramientas de la Planificación de Red

Hay un número de herramientas disponibles que ayudan en el desarrollo de un plan para la infraestructura de red. La primera y mejor de estas, sin embargo, puede ser la más sencilla: el papel y el esfero. Siempre comenzar con la determinación de los requisitos del negocio que usará la red. La mejor manera de hacer esto es mediante las interacciones cara a cara, por las entrevistas con los usuarios relevantes y los usuarios involucrados del negocio. Esto no solamente permitirá construir una imagen completa de los requisitos de la red. Este tipo de participación es crucial para asegurar el despliegue exitoso de cualquier nueva o mejor tecnología.

Después de conseguir un buen entendimiento de la estructura organizacional y las necesidades computacionales del negocio, se deberá hacer una lista del hardware y software que está utilizado. Este inventario debería ser lo más detallado posible, incluyendo la configuración del hardware de las estaciones de trabajo, así como los nombres de los usuarios y los números de las versiones del sistema operativo y las aplicaciones del negocio que están funcionando.

2.4.4 Análisis de las Necesidades Organizacionales

Entender las necesidades de un negocio u otra organización es un paso fundamental para crear una red bien diseñada. El análisis se concentra en el flujo de la información, reconociendo donde se originan los datos en la red y como deberían diseminarse a los usuarios que lo requieren. También se discutirán las prioridades más comunes. Estas prioridades incluyen desde el rendimiento y la disponibilidad que afectan a una red entera, hasta los servicios más específicos como el compartimiento de los archivos, y los servicios audiovisuales. Todos estos problemas deberían tomarse en cuenta para asegurar el éxito del diseño de red.

Hay otras estructuras que permiten una autonomía más alta dentro de sus unidades de negocio donde los departamentos variados o equipos de proyectos funcionan más independientemente. Se puede crear un ambiente AD que consiste en Múltiples Dominios, los cuales permiten que, cada uno de sus dominios tenga sus propios requisitos de seguridad. Y también se puede combinar estos modelos para resolver los requisitos de algunas organizaciones. Como se muestra en la figura 2-5.

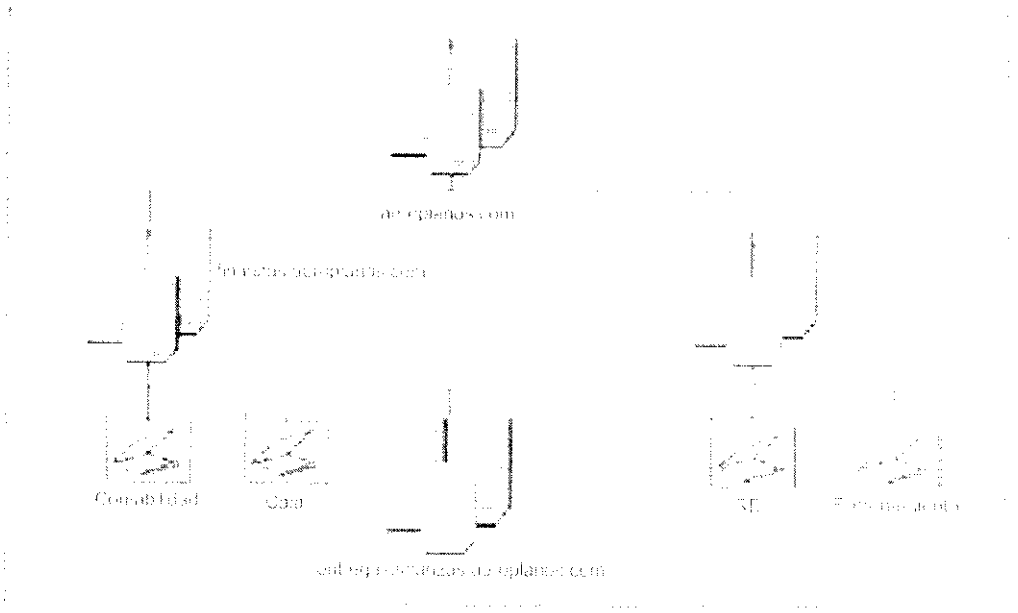


Figura 2-5 Combinación de Organización Centralizada y Descentralizada

2.4.6 La planificación para el crecimiento

"Si hay una verdad universal del diseño de las redes, es que las redes y sus requisitos de recursos, siempre van a crecer al final[7]". El diseño de red necesita considerar no solamente lo que requieren los usuarios de hoy, sino también lo que probablemente van a necesitar en el futuro. Aún si los usuarios o clientes no han pensado en el crecimiento futuro, se debe prever posibles cambios en el diseño de red para acomodar el aumento razonable de la población de usuarios.

[7] MCSE Exam 70-293: Planning and Maintaining a Windows Server 2003 Network Infrastructure, Pagina 28. Martin Grasdal "y" Laura E. Hunter, 2003

Una de las mejores maneras de asegurar que el diseño apoye las necesidades futuras de la red, es implementar las tecnologías bien conocidas y basadas en estándares, en vez de las que son experimentales. Desplegar el hardware y el software de la manera más consistente y bien documentada posible, para poder hacer el mantenimiento y las actualizaciones lo más rápido posible.

2.4.7 Planificación de una Estrategia de Direccionamiento IP

Antes de implementar una infraestructura de red IP, hay detalles que se deben considerar tales como: Un entendimiento de subred es un requisito para implementar un esquema de direccionamiento, decidir que clase de dirección se aplicará, y determinar si el acceso al Internet es necesario para todos o solo algunos computadores. En cualquier caso la implementación de subredes permitirá crear segmentos lógicos en la red simplificando la administración. Para utilizar un esquema bien planificado de subred, se debe manejar las necesidades actuales y planear para la expansión con las necesidades futuras.

2.4.8 El Análisis de los requisitos de Hardware

Antes de implementar cierto tipo de red, se deben identificar las necesidades de hardware para la red. ¿Si para cada ubicación física, se necesita proveer algún tipo de router?. Tal vez implementar una solución WAN, lo cual también requiere un hardware especial, ¿hará falta servidores de DHCP en cada ubicación o un agente de retraso DHCP?, ¿hará falta alguna forma de resolución de nombre, típicamente DNS y posiblemente WINS?. Dependiendo del tráfico y si existen un gran número de usuarios, puede ser que se deba instalar unos interruptores para apoyar con la administración del trafico de la red.

Para un servidor DHCP, los dos factores principales que afectan al rendimiento son la cantidad de RAM (random access memory) y la velocidad de ingreso/salida del disco (disk input/output). Siempre proveer la cantidad

de RAM mas grande posible y el ingreso/salida de disco más rápido para el mejor rendimiento en un servidor DHCP. Las mismas reglas se aplican para los servidores de WINS y DNS, aunque el DNS es más dependiente del ancho de banda de la red. En todo caso, las actualizaciones frecuentes de la zona requieren más RAM para un mejor rendimiento.

Si se esta utilizando el DNS de Active Directory, hay otras consideraciones relacionadas a AD, tales como:

- Una utilización aumentada de la red debido a las actualizaciones dinámicas de DNS relacionadas a la integración de DCHP.
- Los requisitos aumentados de RAM debido al volumen aumentado de los datos.

2.5 Controlador de Dominio (Active Directory)

2.5.1 Introducción

"El servicio de directorio de Active Directory se puede instalar en servidores que ejecuten Microsoft Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition y en versiones anteriores que corresponde a toda la línea Microsoft Windows Server 2000[8]". Active Directory almacena información sobre los objetos de la red y facilita la búsqueda y utilización de esta información para los usuarios y administradores. Active Directory utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de la información del directorio.

Este almacén de datos, también denominado directorio, contiene información sobre los objetos de Active Directory. Estos objetos suelen incluir recursos

[8] Microsoft Technet: Microsoft Windows Server 2003 TechCenter, CD1, Mayo 2006

compartidos como servidores, volúmenes, impresoras, cuentas de usuario de red y cuentas de equipo. La seguridad está integrada en Active Directory mediante la autenticación del inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión en la red, los administradores pueden administrar datos del directorio y de la organización en cualquier punto de la red, y los usuarios autorizados de la red pueden tener acceso a recursos en cualquier lugar de la red. La administración basada en directivas facilita la tarea del administrador incluso en las redes más complejas.

Active Directory también incluye:

- Un conjunto de reglas, el esquema, que define las clases de objetos y los atributos que contiene el directorio, así como las restricciones y los límites en las instancias de estos objetos y el formato de sus nombres.
- Un catálogo global que contiene información acerca de cada uno de los objetos del directorio. Esto permite a los usuarios y administradores encontrar información del directorio.
- Un sistema de índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar y encontrar los objetos y sus propiedades.
- Un servicio de replicación que distribuye los datos del directorio por toda la red. Todos los controladores de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio para su dominio. Cualquier cambio en los datos del directorio se replica en todos los controladores del dominio.
- Compatibilidad con el software de cliente de Active Directory, lo que permite que muchas de las características de Microsoft Windows 2000 Professional o Windows XP Professional también estén disponibles en los equipos que ejecutan Windows 95,

Windows 98 y NT Server 4.0. En los equipos que no ejecutan el software de cliente de Active Directory.

2.5.2 Precauciones y recomendaciones

Active Directory ofrece un entorno de directorio seguro para la organización gracias a la autenticación de inicio de sesión y la autorización de usuarios integradas. Para proteger todavía más Active Directory una vez implementado, considerar las siguientes precauciones y recomendaciones: El acceso físico a un controlador de dominio puede permitir el acceso no autorizado de un usuario malintencionado. Por lo tanto, se recomienda guardar al controlador de dominio bajo llave en un lugar seguro con acceso público limitado. Además, deberá limitar la pertenencia a los grupos Administradores de organización, Administradores del dominio, Operadores de cuentas, Operadores de servidores, Operadores de impresión y Operadores de copia de seguridad al personal de confianza de su organización.

2.5.3 Nombres de Objetos

Cada objeto de Active Directory es una instancia de una clase definida en el esquema. Cada clase tiene atributos que aseguran lo siguiente:

- La identificación única de cada objeto (instancia de una clase) en un almacén de datos del directorio.
- La compatibilidad con los Id. de seguridad utilizados en Windows NT 4.0 y versiones anteriores.

Se puede hacer referencia a cada objeto de Active Directory con varios nombres diferentes. Active Directory crea un nombre completo relativo y un nombre canónico para cada objeto, según la información proporcionada cuando se creó o modificó el objeto. También se puede hacer referencia a

cada objeto mediante su nombre completo, que se obtiene del nombre completo relativo del objeto y todos sus objetos de contenedor principal.

Los objetos principales de seguridad son objetos de Active Directory que se pueden utilizar para iniciar sesiones en la red y se les pueden asignar accesos a los recursos de dominio. Un administrador debe proporcionar los nombres de los objetos principales de seguridad (cuentas de usuario, cuentas de equipo y grupos) que son únicos en un dominio.

Los objetos principales de seguridad, como las cuentas de usuario, pueden cambiarse de nombre, moverse o incluirse en una jerarquía de dominios anidados. Para reducir los efectos de cambiar el nombre, mover o asignar nombres de cuenta de usuario en una jerarquía de dominios anidados, Active Directory proporciona un método que simplifica los nombres de inicio de sesión de los usuarios, mediante la creación de Unidades Organizativas.

2.5.4 Unidades Organizativas (UO)

La unidad organizativa es un tipo de objeto de directorio muy útil incluido en los dominios. "Las unidades organizativas son contenedores de Active Directory en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas[9]". Una unidad organizativa no puede contener objetos de otros dominios.

Una unidad organizativa es el ámbito o unidad más pequeña a la que se pueden asignar configuraciones de Directiva de Grupo o en la que se puede delegar la autoridad administrativa. Con las unidades organizativas, se pueden crear contenedores dentro de un dominio que representan las estructuras lógicas y jerárquicas existentes dentro de una organización. Esto permite administrar la configuración y el uso de cuentas y recursos, en función de su modelo organizativo.

---

[9] Microsoft Technet: Microsoft Windows Server 2003 TechCenter, CD1, Mayo 2006

Como se muestra en la figura 2-6, las unidades organizativas pueden contener otras unidades organizativas. La jerarquía de contenedores se puede extender tanto como sea necesario para modelar la jerarquía de la organización dentro de un dominio. Las unidades organizativas permiten disminuir el número de dominios necesarios en una red. Puede utilizar unidades organizativas para crear un modelo administrativo que se puede ampliar a cualquier tamaño.

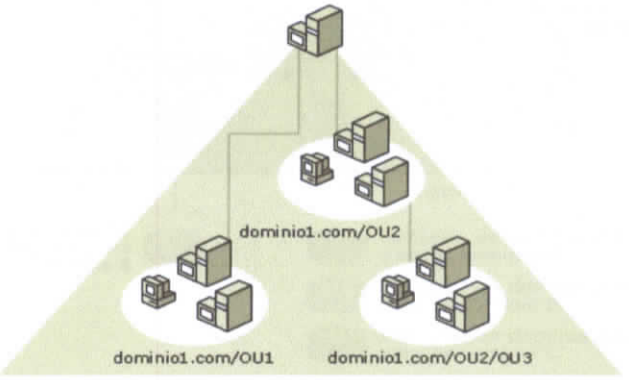


Figura 2-6 Unidades Organizativas

2.5.5 Descripción de controladores de Dominio

Al crear el primer controlador de dominio de la organización, también se crea el primer dominio, es decir, el primer sitio y se instala Active Directory. Los controladores de dominio que ejecutan Windows Server 2003 almacenan datos del directorio y administran las interacciones entre el usuario y el dominio, incluidos los procesos de inicio de sesión de los usuarios, la autenticación y las búsquedas en directorios. Los controladores de dominio se crean con el Asistente para instalación de Active Directory.

2.5.6 Descripción de Catalogo Global

2.5.6.1 Función

"Un catálogo global es un controlador de dominio que almacena una copia de todos los objetos de Active Directory de un conjunto de dominios. En el

Cada equipo de una red TCP/IP debe tener una dirección IP única. La dirección IP (junto con su máscara de subred relacionada) identifica al equipo host y a la subred a la que está conectado. Al mover un equipo a una subred diferente se debe cambiar la dirección IP. DHCP permite asignar dinámicamente una dirección IP a un cliente a partir de la base de datos de direcciones IP del servidor DHCP de la red local:

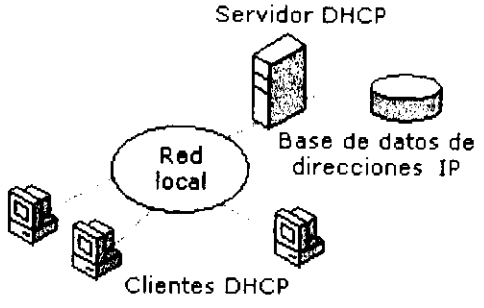


Figura 2-8 DHCP

"En las redes TCP/IP, DHCP reduce la complejidad y cantidad de trabajo administrativo para volver a configurar los equipos. La familia de Microsoft Windows Server 2003 proporciona un servicio DHCP que se puede utilizar para administrar la configuración de los clientes IP y automatizar la asignación de direcciones IP en la red[11]".

2.6.2 Ventajas del Uso

- **Configuración segura y confiable.**
  DHCP evita los errores de configuración que se producen por la necesidad de escribir los valores manualmente en cada equipo. Así mismo, DHCP ayuda a evitar los conflictos de direcciones que se producen al configurar un equipo nuevo en la red con una dirección IP ya asignada.
- **Reduce la administración de la configuración.**
  La utilización de un servidor DHCP puede reducir significativamente el tiempo necesario para configurar y modificar la configuración de

[11] Microsoft Technet: Microsoft Windows Server 2003 TechCenter, CD2, Mayo 2006

los equipos de la red. Los servidores se pueden configurar para que suministren un conjunto completo de valores de configuración adicionales al asignar concesiones de direcciones. Estos valores se asignan mediante opciones DHCP. Así mismo, el proceso de renovación de concesiones de DHCP ayuda a garantizar que en las situaciones en que sea necesario actualizar a menudo la configuración de los clientes (como en el caso de usuarios con equipos móviles o portátiles que cambian frecuentemente de ubicación), los clientes que se comunican directamente con los servidores DHCP puedan realizar estos cambios de forma eficaz y automática.

2.6.3 Funcionamiento

DHCP utiliza un modelo cliente-servidor. El administrador de la red establece uno o varios servidores DHCP que mantienen la información de configuración de TCP/IP y la proporcionan a los clientes. La base de datos del servidor incluye lo siguiente:

- Los parámetros de configuración válidos para todos los clientes de la red.
- Un conjunto de direcciones IP válidas para su asignación a los clientes, junto con direcciones reservadas para su asignación manual.
- La duración de las concesiones ofrecidas por el servidor. La concesión define el período de tiempo de uso de la dirección IP asignada.

Cuando hay un servidor DHCP instalado y configurado en la red, los clientes habilitados para DHCP pueden obtener dinámicamente sus direcciones IP y los parámetros de configuración relacionados cada vez que inician una sesión y se unen a la red. Los servidores DHCP proporcionan esta configuración a

los clientes que la solicitan, en forma de una oferta de concesión de direcciones.

2.6.4 Terminología

Término	Descripción
Ámbito	Un ámbito es el intervalo consecutivo completo de las direcciones IP posibles de una red. Normalmente los ámbitos definen una subred física de la red a la que se ofrecen los servicios DHCP. Los ámbitos también proporcionan el medio principal para que el servidor administre la distribución y asignación de direcciones IP, así como los parámetros de configuración relacionados, a los clientes de la red.
Intervalo de exclusión	Un intervalo de exclusión es una secuencia limitada de direcciones IP de un ámbito, excluida de las ofertas del servicio DHCP. Los intervalos de exclusión aseguran que el servidor no ofrecerá las direcciones de estos intervalos a los clientes DHCP de la red.
Conjunto de direcciones	Tras definir un ámbito DHCP y aplicar intervalos de exclusión, las direcciones restantes forman el conjunto de direcciones disponibles del ámbito. El servidor puede elegir cualquiera de las direcciones del conjunto para asignarla dinámicamente a los clientes DHCP de la red.
Concesión	Una concesión es un período de tiempo especificado por los servidores DHCP y durante el cual un equipo cliente puede utilizar una dirección IP asignada. Cuando se realiza una concesión a un cliente, la concesión está activa. Antes de que caduque la concesión, el cliente suele necesitar renovar la asignación de la concesión de dirección en el servidor. Una concesión queda inactiva cuando caduca o cuando se elimina del servidor. La duración de una concesión determina cuándo caducará y la frecuencia con la que el cliente necesita renovarla en el servidor.
Reserva	Las reservas aseguran que un dispositivo de hardware específico de la subred siempre podrá utilizar la misma dirección IP.
Tipos de opciones	Los tipos de opciones son otros parámetros de configuración del cliente que un servidor DHCP puede asignar al proporcionar concesiones a los clientes DHCP.

Tabla 2-4 Terminología de DHCP

2.6.5 Base de Datos

No hay límite definido para el número de registros que un servidor DHCP puede almacenar. El tamaño de la base de datos depende del número de clientes DHCP de la red. La base de datos DHCP crece a lo largo del tiempo según los clientes inician y terminan sesiones en la red. El tamaño de la base de datos DHCP no es directamente proporcional al número de entradas de concesiones de clientes activas. Con el tiempo, cuando algunas entradas de clientes DHCP se convierten en obsoletas y se eliminan, queda algún espacio sin utilizar.

Para recuperar el espacio sin utilizar se compacta la base de datos DHCP. A partir de Windows NT Server 4.0, la compactación dinámica de la base de datos se produce en los servidores DHCP como un proceso automático en segundo plano durante el tiempo de inactividad o después de las actualizaciones de la base de datos.

2.6.5.1 Archivos de las Base de Datos DHCP

La base de datos del servidor DHCP de la familia Windows Server 2003 utilizan el motor de almacenamiento JET de Exchange Server. Al instalar el servicio DHCP se crean automáticamente, en el directorio Systemroot\System32\Dhcp, los archivos que se indican en la tabla 2-5.

Archivo	Descripción
Dhcp.mdb	Archivo de base de datos del servidor DHCP.
Dhcp.tmp	Archivo temporal que la base de datos DHCP.
J50.log y J50######.log	Registro de todas las transacciones de base de datos. La base de datos de DHCP utiliza este archivo si es necesario recuperar datos.
J50.chk	Archivo de punto de comprobación.

Tabla 2-5 Archivo de la base de datos DHCP

2.7 DNS

2.7.1 Conceptos Básicos

2.7.1.1 Servidores

El sistema DNS (Domain Name System) es una base de datos distribuida que almacena información asociada a nombres de dominio en redes como Internet, es decir su principal función es asignar nombres de dominio a direcciones IP. Estas bases de datos residen en los servidores de DNS que administran el sistema. Las computadoras que actúan como servidores de DNS ejecutan un programa que administra la estructura de la base de datos y la información que contiene. Esta información se utiliza para proveer las respuestas a las solicitudes de clientes para resolución de nombre. Un servidor DNS o puede responder a la solicitud directamente o puede proveer una dirección a otro servidor de DNS que puede ayudar a resolver la consulta. También puede responder que no sabe o que esa información no existe.

Cada servidor de DNS se asigna una parte de namespace sobre el cual preside. El servidor DNS que es responsable para una porción contigua del namespace, se llama autorizado para esa porción contigua. La autoridad para una zona puede delegarse a otro servidor. A menudo los administradores delegan la autoridad para los subdominios a los otros servidores DNS.

2.7.1.2 Resolver

Los "resolver" DNS son programas que usan las consultas de DNS para pedir la información de los servidores de DNS. "Un resolver" suele ser parte de un programa de utilidad o se le puede conseguir acceso por medio de las funciones de biblioteca y puede comunicar con un servidor remoto de DNS o el servidor DNS que esta corriendo localmente.

numerosas computadoras puedan configurarse para administrar las zonas que se integran en el directorio activo de Windows.

Una zona pueden almacenarse como un archivo de texto o dentro de la estructura del directorio activo en un servidor DNS de Windows 2000/2003. Algunos servidores secundarios de DNS pueden almacenar una zona en su memoria y realizar una transferencia de zona cuando están reiniciados. Una transferencia de zona es cuando los registros de recursos de la zona se replican.

Hay 4 tipos de zonas que se apoyan en el Windows Server 2003:

- **Primaria estándar** – tiene la copia maestra de la base de datos de la zona y se replica a las zonas secundarias. Todos los cambios a la zona se hacen en la zona primaria.
- **Secundaria estándar** –tiene una copia solo de lectura de la base de datos de la zona que se utiliza para proveer la tolerancia de los fallos y una resolución de nombres más rápida por la red. La base de datos se actualiza por el proceso de transferencia de zona.
- **Integrada al Active Directory** – la información de zona que contiene el directorio activo de Windows y que se replica usando la replicación del Active Directory, que provee una mayor flexibilidad en el proceso de replicación.
- **Stub** – contienen solo los registros de recursos necesarios para identificar los servidores autorizados de DNS para la zona.

2.8 Servidor DNS Windows 2003

2.8.1 Funcionamiento

DNS es un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

"Por ejemplo, la mayoría de los usuarios prefieren un nombre descriptivo, fácil de utilizar, como COMPUTADOR_1 para localizar un equipo. Un nombre descriptivo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los sistemas de nombres como DNS proporcionan una forma de asignar estos nombres descriptivos de los equipos o servicios a sus direcciones numéricas[12]".

La figura 2-9 muestra un uso básico de DNS, consistente en la búsqueda de la dirección IP de un equipo basada en su nombre:

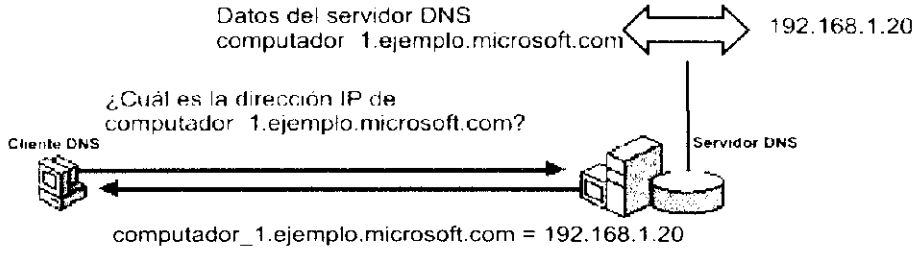


Figura 2-9 DNS

[12] Microsoft Technet: Microsoft Windows Server 2003 TechCenter, CD2, Mayo 2006

En este ejemplo, un equipo cliente consulta a un servidor DNS, preguntando la dirección IP de un equipo configurado para utilizar computador_1.ejemplo.microsoft.com como nombre de dominio. Como el servidor puede utilizar la base de datos local para responder la consulta, contesta con una respuesta que contiene la información solicitada, un registro de recursos de host (A) que contiene la información de dirección IP para computador_1.ejemplo.microsoft.com.

2.8.2 Características del Servidor

- **Compatibilidad con Active Directory**

  Se necesita DNS para compatibilizar el servicio de directorios Active Directory. Si instala Active Directory en un servidor, puede instalar y configurar automáticamente un servidor DNS si no puede localizarse un servidor DNS que cumpla los requisitos de Active Directory.

- **Administración más fácil**

  La consola DNS ofrece una interfaz gráfica de usuario mejorada para administrar el servicio de Servidor DNS. Además, existen varios asistentes nuevos para la configuración que permiten realizar tareas administrativas habituales del servidor. Además de la consola DNS, se proporcionan otras herramientas que le ayudarán a administrar y lograr la compatibilidad con los clientes y servidores DNS de la red.

2.8.3 Características del Cliente

El servicio cliente Sistema de nombres de dominio (DNS) se utiliza para resolver nombres de dominio DNS e implementa las características siguientes:

- **Almacenamiento en memoria caché para todo el sistema**

  Los registros de recursos (RR, Resource Records) de respuestas a consultas se agregan a la memoria caché del cliente cuando las

aplicaciones consultan a los servidores DNS. Esta información se almacena en la memoria caché durante un tiempo de vida (TTL) establecido y se puede volver a utilizar para responder a consultas posteriores.

- **Evitar los servidores DNS que no responden**
  El servicio Cliente DNS utiliza una lista de búsqueda de servidores, ordenada por preferencias. Esta lista incluye todos los servidores DNS alternativos y preferidos configurados para cada una de las conexiones de red activas en el sistema.

  La lista se basa en los criterios siguientes:

  - Se da prioridad superior a los servidores DNS preferidos.
  - Si no están disponibles los servidores DNS preferidos, se utilizan los servidores DNS alternativos.
  - Se quitarán temporalmente de estas listas los servidores que no respondan.

2.8.4 Cómo Funcionan las Consultas

Cuando un cliente DNS necesita buscar un nombre que se utiliza en un programa, consulta los servidores DNS para resolver el nombre. Cada mensaje de consulta que envía el cliente contiene tres grupos de información, que especifican una pregunta que tiene que responder el servidor:

- Un nombre de dominio DNS especificado, indicado como un nombre de dominio completo.
- Un tipo de consulta especificado, que puede establecer un registro de recursos por tipo o un tipo especializado de operación de consulta.
- Una clase especificada para el nombre de dominio DNS.

Por ejemplo, el nombre especificado puede ser el nombre completo de un equipo, como COMPUTADOR 1, y el tipo de consulta especificado para buscar un registro de recursos de dirección (X) por ese nombre. Considere una consulta DNS como una pregunta de un cliente a un servidor en dos partes, como "¿Tiene algún registro de recursos de dirección (X) de un equipo llamado COMPUTADOR 1?. Cuando el cliente recibe una respuesta del servidor, lee e interpreta el registro de recursos A respondido, y aprende la dirección IP del equipo al que preguntó por el nombre.

Las consultas DNS se resuelven de diferentes formas. A veces, un cliente responde a una consulta localmente mediante la información almacenada en la caché obtenida de una consulta anterior. El servidor DNS puede utilizar su propia caché de información de registros de recursos para responder a una consulta. Un servidor DNS también puede consultar o ponerse en contacto con otros servidores DNS en nombre del cliente solicitante para resolver el nombre por completo y, a continuación, enviar una respuesta al cliente. Este proceso se llama recursividad.

En general, el proceso de consulta DNS se realiza en dos partes:

- La consulta de un nombre comienza en un equipo cliente y se pasa a resolver, el servicio Cliente DNS, para proceder a su resolución.
- Cuando la consulta no se puede resolver localmente, se puede consultar a los servidores DNS según sea necesario para resolver el nombre.

2.9 Descripción de Cuentas de Usuario y Equipos

2.9.1 Cuentas de Usuarios y Equipos

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 como 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. 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.
- **Auditar las acciones realizadas con la cuenta de usuario o de equipo**.- La auditoria puede ayudar a supervisar la seguridad de las cuentas.

2.9.1.1 Cuentas de Usuario

El contenedor Usuarios ubicado en Usuarios y Equipos de Active Directory incluye tres cuentas de usuario integradas: Administrador, Invitado y

Asistente de ayuda (tabla 2-6). Estas cuentas de usuario integradas se crean automáticamente al crear el dominio.

Cada cuenta integrada tiene una combinación diferente de derechos y permisos. La cuenta Administrador tiene los derechos y permisos más amplios sobre el dominio, mientras que la cuenta Invitado tiene derechos y permisos limitados. En la siguiente tabla se describe cada una de las cuentas de usuario predeterminadas en los controladores de dominio que ejecutan Windows Server 2003.

Cuenta de usuario predeterminada	**Descripción**
Cuenta Administrador	La cuenta Administrador tiene control total sobre el dominio y puede asignar derechos de usuario y permisos de control de acceso a los usuarios según sea necesario. Sólo debe utilizar esta cuenta para aquellas tareas que requieran credenciales administrativas. Se recomienda configurarla con una contraseña segura La cuenta Administrador es un miembro predeterminado de los grupos Administradores, Administradores de dominio, Administradores de organización, Propietarios del creador de directivas de grupo y Administradores de esquema en Active Directory. La cuenta Administrador nunca se puede eliminar ni quitar del grupo Administradores, pero es posible cambiarle el nombre o deshabilitarla. Como es sabido que la cuenta Administrador existe en muchas versiones de Windows, si le cambia el nombre o la deshabilita dificultará el acceso a ella a usuarios malintencionados. La cuenta Administrador es la primera cuenta que se crea cuando se instala un nuevo dominio con el Asistente para instalación de Active Directory.
Cuenta Invitado	La cuenta Invitado sólo la utilizan los usuarios que no poseen una cuenta real en el dominio. Un usuario con su cuenta deshabilitada (pero no eliminada) también puede utilizar la cuenta Invitado. La cuenta

Cuenta de usuario predeterminada	Descripción
	Invitado no requiere ninguna contraseña. Puede asignar derechos y permisos para la cuenta Invitado de la misma forma que para cualquier cuenta de usuario. De forma predeterminada, la cuenta Invitado es miembro del grupo integrado Invitados y del grupo global Invitados del dominio, que permite a un usuario iniciar una sesión en un dominio. La cuenta Invitado está deshabilitada de forma predeterminada, y se recomienda que permanezca así.
Cuenta Asistente de ayuda (se instala con una sesión de Asistencia remota)	Se trata de la cuenta principal que se utiliza para establecer una sesión de Asistencia remota. La cuenta se crea automáticamente al solicitar una sesión de Asistencia remota, y tiene limitado el acceso al equipo. El servicio Administrador de sesión de Ayuda de escritorio remoto administra la cuenta Asistente de ayuda, que se eliminará automáticamente si no hay solicitudes de Asistencia remota pendientes.

Tabla 2-6 Cuentas de Usuario

2.9.1.2 Proteger Cuentas de Usuario

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.

Se pueden usar los grupos de seguridad para asignar los derechos de usuario a los usuarios. Los derechos de usuario incluyen las acciones como los archivos de respaldo y los directorios o los archivos de restauración y directorios, ambos se asignan al grupo de operadores de respaldo por defecto. Se pueden delegar los derechos a los grupos para permitir que los miembros del grupo realicen una función administrativa específica que normalmente no se permite con sus derechos de usuario estándares. También es posible asignar los permisos a los grupos de seguridad para permitir que tengan acceso a los recursos de red, tales como las impresoras y los compartimientos de archivos.

Cuando se usan los grupos en Active Directory, hay 3 mayores beneficios:

- Los grupos de seguridad permiten simplificar y reducir los requisitos administrativos por asignar los permisos y los derechos para un recurso compartido (por ej. una impresora) al grupo en lugar de asignar a cada usuario individual que requiere el acceso. De esta manera, todos los usuarios y los grupos que son miembros del grupo recibirán los permisos y derechos configurados por herencia.
- Los grupos de seguridad permiten delegar rápida y eficazmente las responsabilidades administrativas para el rendimiento de unas tareas específicas en el directorio activo.
- Los grupos de seguridad y distribución permiten crear rápidamente los grupos de distribución de e-mail por asignar una dirección de e-mail al grupo mismo. Todos los miembros del grupo que tienen buzón de correo recibirán un e-mail cuando se envía a la dirección de e-mail del grupo.

2.9.1.4.2 Grupos Locales, Locales del Dominio, Globales y Universales

- **Grupos locales**

  Los grupos locales pueden contener las cuentas de usuario de la máquina local, las cuentas de usuario del dominio al cual la máquina local esta conectado, o las cuentas de usuario de cualquier dominio confiable del dominio de la máquina a la cual esta conectada. Solo los grupos locales pueden administrar los permisos para los recursos locales (local a una sola máquina).

- **Grupos del Dominio Local**

  Los grupos de dominio local pueden incluir los otros grupos y las cuentas de usuario o computadora del Windows Server 2003, Windows Server 2000 y de dominios de Windows NT. Solamente los permisos para el dominio en el cual se define el grupo pueden asignarse a los grupos locales dominio.

- **Grupos Globales**

  Los grupos globales incluyen otros grupos y cuentas de usuario/computadora solamente del dominio en el cual se define el grupo.

- **Grupos Universales**

  Los grupos universales incluyen otros grupos y cuentas de usuario/computadora de cualquier dominio en el conjunto de dominios. Los permisos para cualquier dominio en el conjunto de dominios pueden asignarse a los grupos universales. Los grupos universales solo son disponibles si el nivel de dominio funcional esta configurado a modo nativo de Windows 2000.

2.10 Manejo de Acceso a Recursos

2.10.1 Introducción al Control de Acceso

"El control de acceso es el proceso de autorizar a los usuarios, grupos y equipos a tener acceso a los objetos de la red. Los conceptos clave que componen el control de acceso son permisos, derechos de usuario y auditoría de objetos[13]".

2.10.2 Permisos

Los permisos definen el tipo de acceso concedido al usuario o grupo para un objeto o una propiedad de objeto. Por ejemplo, al grupo Materias se le pueden conceder los permisos de lectura y escritura para el archivo denominado calificaciones.txt. Los permisos se aplican a cualquier objeto protegido como archivos, objetos de Active Directory u objetos del Registro. Los permisos se pueden conceder a cualquier usuario, grupo o equipo. Es recomendable asignarlos a grupos.

Puede asignar permisos para objetos a:

- Grupos, usuarios e Identificadores de seguridad del dominio.
- Grupos y usuarios del dominio y de cualquier dominio de confianza.
- Grupos y usuarios locales del equipo en que reside el objeto.

Los permisos adjuntos a un objeto dependerán del tipo de objeto. Por ejemplo, los permisos que se pueden asignar a un archivo son diferentes de los que se pueden asignar a una clave de registro. Sin embargo, algunos permisos, son comunes a la mayoría de los tipos de objeto. Los permisos comunes son:

---

[13] Microsoft Technet: Microsoft Windows Server 2003 TechCenter. CD2, Mayo 2006

- Permisos de lectura.
- Permisos para modificar.
- Cambiar de propietario.
- Eliminar.

2.10.3 Herencia de Permisos

La herencia permite a los administradores asignar y administrar permisos fácilmente. Esta característica hace que los objetos de un contenedor hereden automáticamente todos los permisos heredables de ese contenedor. Por ejemplo, cuando se crean archivos en una carpeta, heredarán los permisos de la carpeta. Sólo se heredarán los permisos marcados para ello.

2.10.4 Derechos de Usuario

Los administradores pueden asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales. Estos derechos autorizan a los usuarios a realizar acciones específicas, como iniciar una sesión en un sistema de forma interactiva o realizar copias de seguridad de archivos y directorios. Los derechos de usuario se diferencian de los permisos en que se aplican a las cuentas de usuario, mientras que los permisos se asignan a los objetos.

Los derechos del usuario definen las capacidades en un ámbito local. Aunque se pueden aplicar a cuentas de usuario individuales, se administran mejor en una cuenta de grupo. De esta manera, se asegura que un usuario que inició la sesión como miembro de un grupo hereda automáticamente los derechos asociados al grupo. Al asignar derechos de usuario a los grupos en lugar de a usuarios individuales, se simplifican la tarea de administración de cuentas de usuario. Cuando los usuarios de un grupo requieren derechos de usuario, puede asignar una vez el conjunto de derechos de usuario al grupo, en lugar

de asignar repetidamente el mismo conjunto de derechos a cada cuenta de usuario.

Hay dos tipos de derechos de usuario: privilegios, como el derecho a realizar una copia de seguridad de archivos o directorios, y derechos de inicio de sesión, como el derecho a iniciar sesiones en un sistema de forma local.

2.11 Directivas de Grupo

2.11.1 Objetos de Directivas de Grupo

"Las configuraciones de directiva se almacenan en objetos de directiva de grupo (GPO, Group Policy Object). La configuración de cada GPO se edita en el Editor de objetos de directiva de grupo[14]".

Hay dos clases de GPO:

- **GPO basados en Active Directory**. Se almacenan en un dominio y se replican en todos los controladores de dicho dominio. Únicamente están disponibles en un entorno de Active Directory. Se aplican a los usuarios y equipos de los sitios, dominios o unidades organizativas a los que está vinculado el objeto de directiva de grupo. Es el mecanismo principal a través del cual se usa la directiva de grupo en un entorno de Active Directory.
- **GPO locales**. Sólo hay un GPO local almacenado en cada equipo. Los GPO locales son los GPO que tienen una menor influencia en un entorno de Active Directory; sólo cuentan con un subconjunto de las opciones que se pueden encontrar en los GPO basados en Active Directory.

[14] Microsoft Technet: Microsoft Windows Server 2003 TechCenter, CD2, Mayo 2006

2.11.2 Configuración de Usuarios y Equipo

"La configuración de los GPO se divide en **Configuración de usuario**, que incluye las opciones que se aplican a los usuarios cuando inician una sesión, y **Configuración del equipo** , que incluye las opciones que se aplican a los equipos cuando se inician[16]". La mayoría de opciones de configuración se encuentran sólo en una sección, pero algunas, como ejecutar secuencias de comandos de inicio de sesión de forma sincrónica, se encuentran en ambas. Si se encuentran en las dos secciones y hay un conflicto, se usa la configuración del equipo.

Las opciones "Configuración de usuario" y "Configuración del equipo" se dividen, a su vez, en un conjunto configurable de extensiones MMC para la directiva de grupo.

2.11.3 Cambiar el Estado de un GPO

De forma predeterminada, el estado de un GPO es Habilitado. Se puede cambiar a Configuración de usuario deshabilitada, que deshabilita la configuración de usuario del GPO; configuración de equipo deshabilitada, que deshabilita la configuración de equipo del GPO; o todas las configuraciones deshabilitadas, que deshabilita el GPO completo. Si un equipo cliente procesa un GPO, no se evalúan las partes deshabilitadas de dicho GPO.

De forma predeterminada, el estado de un GPO es Habilitado. Se puede cambiar a "Configuración de usuario deshabilitada", que afecta a todas las opciones de Configuración de usuario; "Configuración de equipo deshabilitada", que afecta a todas las opciones de configuración del equipo; o "Todas las configuraciones deshabilitadas", que deshabilitan el GPO completo. Si cambia el estado de un GPO, se ven afectados todos los sitios,

[16] Microsoft Technet: Microsoft Windows Server 2003 TechCenter. CD2, Mayo 2006

dominios y unidades organizativas que reciben una directiva del GPO. De esta manera, la deshabilitación de un GPO tiene mayor alcance que la deshabilitación de uno de sus vínculos.

2.12 Seguimiento de Rendimiento

La familia de servidores de Windows Server 2003 proporciona las siguientes herramientas como parte de la consola Rendimiento:

- Monitor de sistema.
- Registros y alertas de rendimiento.
- Administrador de tareas.

Supervisar el rendimiento del sistema es una parte importante del mantenimiento y la administración del sistema operativo. Los datos de rendimiento se utilizan para lo siguiente:

- Comprender la carga de trabajo y el efecto que produce en los recursos del sistema.
- Observar los cambios y las tendencias en las cargas de trabajo y en el uso de los recursos, de modo que se puedan programar las actualizaciones futuras.
- Probar los cambios de configuración u otros trabajos de ajuste.
- Diagnosticar problemas y componentes o procesos de destino para la optimización.

Las herramientas "Monitor de sistema" y "Registros y alertas de rendimiento" proporcionan datos detallados acerca de los recursos que utilizan componentes específicos del sistema operativo y programas que han sido diseñados para recopilar datos de rendimiento. Los gráficos ofrecen una pantalla de datos de supervisión y rendimiento. Los registros permiten diferentes posibilidades para la grabación de los datos. Las alertas envían una

CAPÍTULO III

3. DESARROLLO DEL PROYECTO

Todo el siguiente trabajo fue analizado e implementado en los laboratorios de computación de la PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

3.1 Análisis de la Red

- Dado que la red no tiene ningún servidor como gestionador de enlace entre los computadores que conforman la red, P2P es la calificación que recibe el entorno de red, en otras palabras todas las comunicaciones son directamente de usuario a usuario, de computador a computador.
- La administración de la red se lleva a cabo de forma descentralizada, es decir cada computador tiene un nivel de configuración, a la cual se accede única y exclusivamente manipulando directamente el computador.
- Existen cuentas locales como administradores en cada uno de los computadores, por lo que la autenticación se la realiza localmente, es decir manteniendo cuentas de usuario válidas en cada uno de los mismos.
- La red de los laboratorios de la Universidad mantiene una clase C, con mascara 255.255.255.0 y un rango de ip de 192.168.2.1 hasta la 192.168.2.254, tomando en cuenta que la red inalámbrica con la que se cuenta, esta dentro del rango anteriormente mencionado.
- Existe una aplicación y equipo importante como es el Servidor Proxy que mantiene la dirección IP 192.168.2.200.
- Los equipos que conforman la red conservan un estándar, en lo que concierne al hardware se puede destacar que todos los equipos tienen

un mínimo de PENTIUM IV y en el software un mínimo de WINDOWS XP PROFESSIONAL SERVICE PACK II.

3.2 Planificación Estratégica para la Construcción de un Controlador de Dominio Basado en Microsoft Windows Server 2003

Previa implementación del Controlador de Dominio se llevó a cabo una serie de reuniones con personal de la PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO. que esta relacionado directamente con la implementación del mencionado proyecto, en las cuales se definieron puntos y estandarizaciones necesarios para el perfecto funcionamiento y administración de la red, aplicados en los computadores que conforman la red de datos en los laboratorios informáticos. A continuación se encuentra detallada la previa planificación previa para el proyecto.

3.2.1 Controlador de Dominio

- **Nombre de Dominio:** Dado que el proyecto será implementado en los laboratorios de la universidad. el Dominio llevara el nombre de **PUCESA.INT.**
- **Esquema Organizacional:** Para la construcción del Controlador de Dominio se tomó en cuenta el esquema propuesto y se utilizó el mismo para la construcción (figura 3-1).

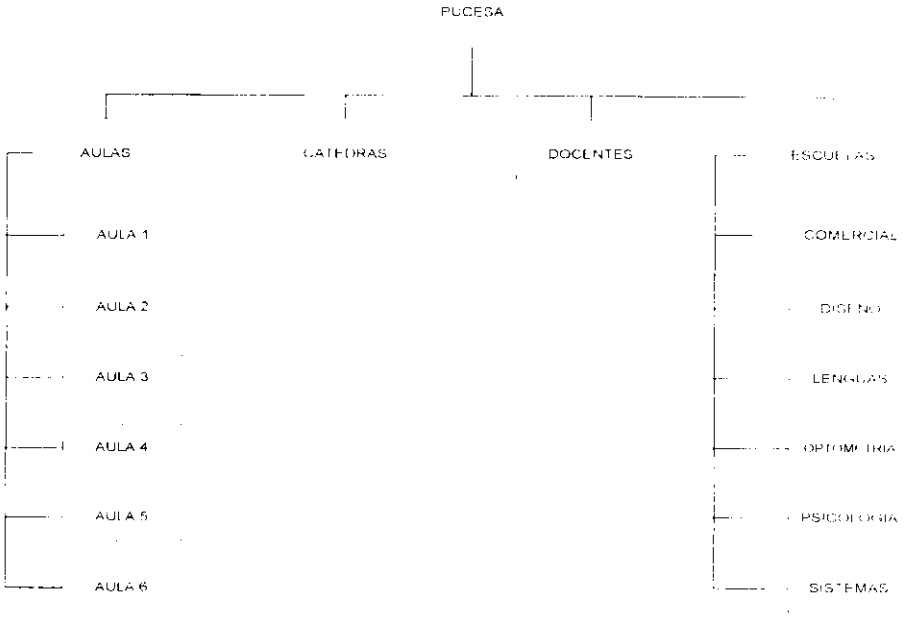


Figura 3-1 Esquema Organizacional

El esquema mencionado servirá como guía para la creación de Grupos y Unidades Organizativas, para administrar el acceso de usuarios y equipos a recursos compartidos de la red.

- **Nombre de Computador:** Definir los nombres de los equipos no es necesario puesto que ya existe una política para los mismos. Se expresa de la siguiente manera: LAB6_1

  LAB6: Significa el laboratorio al que pertenece.

  1 : Significa el número que le corresponde a dicho computador.

  El nombre del servidor que tiene el rol de Controlador de Dominio difiere de lo anterior llamándose de la siguiente manera: LABCD01.

- **Nombre de Usuario:** Se han definido tres tipos para los nombres de usuarios.
  - El número de cedula incluido el guión para Estudiantes y Docentes Ej. Álvaro Villacrés.

    Usuario: 180260866-9.
  - El código de materia para las cátedras Ej. Programación Avanzada.

    Usuario: is802.

- El nombre para los administradores de red Ej. Diego Santa Cruz.

  Usuario: Diego.

- **Horarios y lugar de ingreso:** Los tipos de usuarios mantienen diferentes configuraciones de ingreso como son.
  - Estudiantes, solo pueden acceder a los equipos del laboratorio 6 a excepción de los estudiantes de SISTEMAS que pueden ingresar al laboratorio 2 y horario no definido.
  - Profesores, Pueden ingresar a todos los computadores de los laboratorios y horario no definido.
  - Cátedras, con acceso a laboratorio 2, 3, 4, 5, 6 y con horario definido.
  - Administradores, pueden acceder a todos los computadores de los laboratorios y horario no definido.
- **Directivas de Grupo:** Las directivas están concebidas para centralizar una óptima administración con los objetos de la red, por lo tanto se crearán algunas que tienen que ver directamente con:
  - La configuración delicada de los sistemas operativos como por ejemplo Panel de Control, Conexiones de red, etc.
  - El acceso hacia que equipos que conforman los laboratorios tienen permiso de ingreso los usuarios.
  - La ejecución de comandos para configuración de parámetros dentro del Dominio.
- **Direccionamiento IP:** Mantiene la misma estrategia de direccionamiento:
  - Una red clase C es decir máscara 255.255.255.0 .
  - Dado que se utilizará un servicio DHCP para los computadores de escritorio, se asignaran direcciones IP en forma aleatoria, el rango dispuesto para el servicio será: 192.168.2.10 – 192.168.2.100. Y a partir de la dirección IP 192.168.2.101 en adelante será destinado para los equipos inalámbricos exceptuando, la 192.168.2.200 que es el servidor Proxy y la

192.168.2.250 que será el servidor de Controlador de Dominio.

3.2.2 Hardware

- **Equipo:** Dotación de un equipo que cumplirá con el rol de Controlador de Dominio, lo suficientemente robusto para soportar tal acceso a la red.
- **Localización:** La oficina de los administradores de red dispone del lugar adecuado para ubicar el servidor, de esta manera se facilita el acceso para el buen manejo y administración del Controlador de Dominio.
- **Adicionales:** La compra de un UPS personal a cargo de la Universidad, y la dotación de un monitor de 15'' .

3.2.3 Software

- **Sistema Operativo:** Microsoft Windows Server 2003 Enterprise Edition Service Pack I, fue el sistema operativo escogido para la realización del proyecto, por su versatilidad, por el tamaño de la organización en este caso la PUCESA con proyección a crecimiento y porque Microsoft posee un amplio campo de soporte técnico para dicho sistema operativo el cual permitirá dar solución a cualquier emergencia.

3.3 Instalación de Hardware y Software

3.3.1 Instalación del Equipo

El equipo a utilizar es **HP ProLiant ML 150 G2**, con las siguientes especificaciones:

Procesador, sistema operativo y memoria	
Procesador	Procesador Intel® Xeon 3.2 GHz
Memoria caché	2 MB de caché
Descripción del chipset	Chipset Intel® E7320 con FSB a 800 MHz
Tipo de memoria	SDRAM DDR PC2700 a 333 MHz
Memoria máxima	8 GB SDRAM ECC PC2700, (4) zócalos
Memoria Actual	1024 MB
Unidades internas	
Unidad de disco duro	1 Discos de 36.4 GB SCSI
Unidad de disco flexible	Disquetera de 1,44 MB
CD-ROM/DVD	Unidad de CD-ROM IDE (ATAPI) 48x
Características del sistema	
Descripción del chasis	Torre
Características de alimentación	Fuente de alimentación de 600 W no conectable en caliente
Interfaz de red	Tarjeta de red Broadcom 5721 10/100/1000 PCI-Express (integrada)
Facilidad del mantenimiento	Apertura de chasis y acceso a componentes sin necesidad de utilizar herramientas
Descripción del peso	17 kg

Tabla 3-1 Servidor HP ProLiant ML 150 G2

Figura 3-2 Servidor HP ProLiant ML 150 G2

Para la instalación del equipo se conectaron todos los periféricos de computación necesarios es decir, teclado, mouse y monitor, conectando a la energía eléctrica, sin dejar a un lado lo más importante como es un punto de red 10/100 Mbps.

3.3.2 Instalación del Sistema Operativo

Esta sección contiene paso a paso los detalles para la instalación de Microsoft Windows Server 2003.

- Iniciar el equipo con el CD booteable de instalación en el driver del CD-ROM.
- Presione una tecla para que inicie con el CD. Una vez que los drivers se hayan cargado y la ejecución de Windows Server 2003 ha iniciado, aparecerá una pantalla para confirmar la utilización del mencionado sistema operativo en el equipo (figura 3-3), presionar ENTRAR.

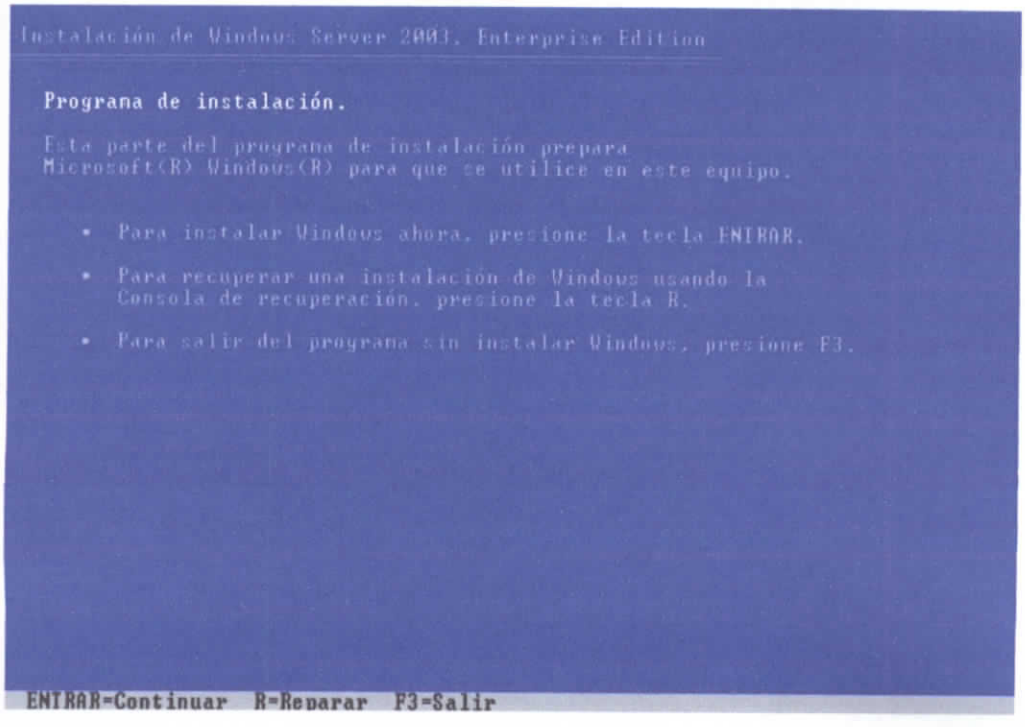


Figura 3-3 Preparación de Sistema *Operativo*

- Aparecerá una para confirmar y aceptar el contrato de licencia de Windows, presionar F8. Luego se presentará la pantalla de administración de particiones (figura 3-4) en la cual se muestran las particiones existentes o si no es así, se pueden crear las particiones necesarias como es en este caso. Crear la partición "C:\" presionado la tecla "C", lo cual permitirá la creación de la partición en la que se llevará a cabo la instalación del Sistema Operativo.

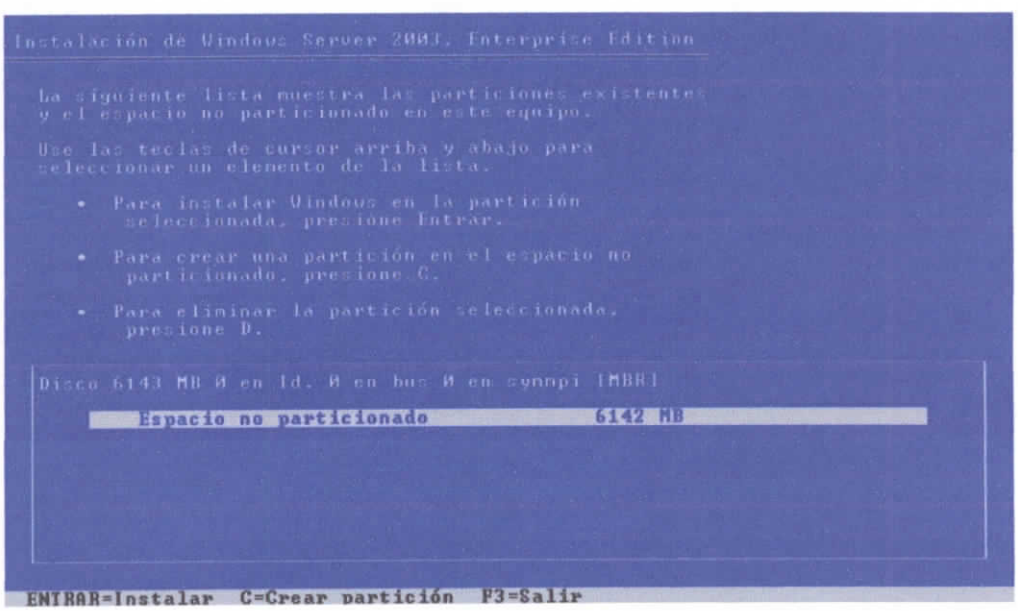


Figura 3-4 Administrador de particiones

- El Disco Duro tiene un espacio total disponible de 36.4 GB, se asignará la cantidad de 16000 MB a la primera partición, se digitará dicha cantidad en el espacio asignado por el asistente de instalación, y luego presionar ENTRAR. Escoger la partición C:\, presionamos ENTRAR.
- Utilizar la opción "FORMATEAR LA PARTICIÓN UTILIZANDO EL SISTEMA DE ARCHIVOS NTFS", luego presionar ENTRAR. El proceso tomará algunos minutos (figura 3-5).

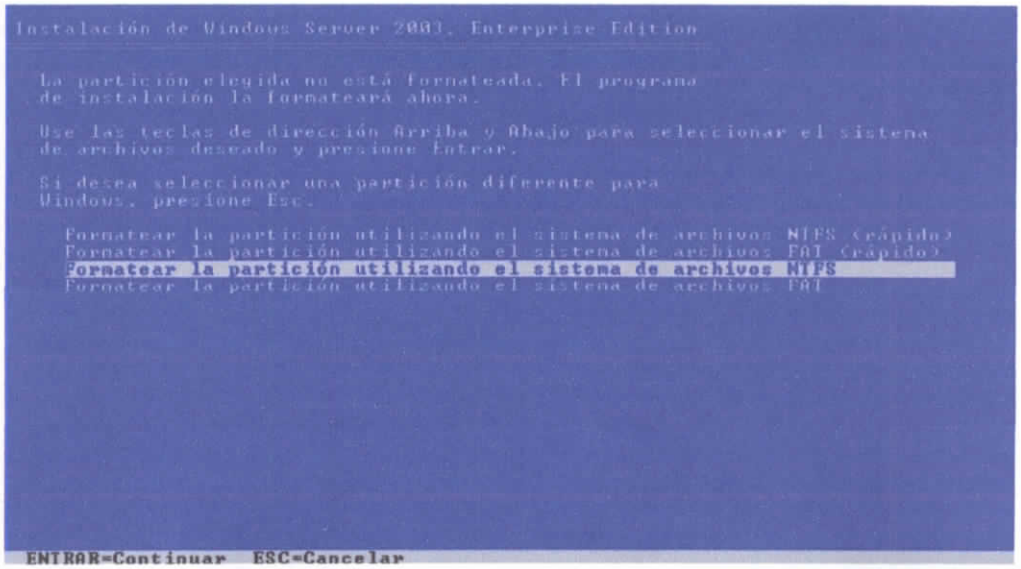


Figura 3-5 Formatear la partición

- Luego de transcurridos algunos minutos es aquí donde arranca la instalación de Windows 2003 Server, solicitándose la Configuración regional y de idioma.
- La siguiente pantalla es informativa la cual solicitará su nombre y el de la Organización (figura 3-6), clic en SIGUIENTE.

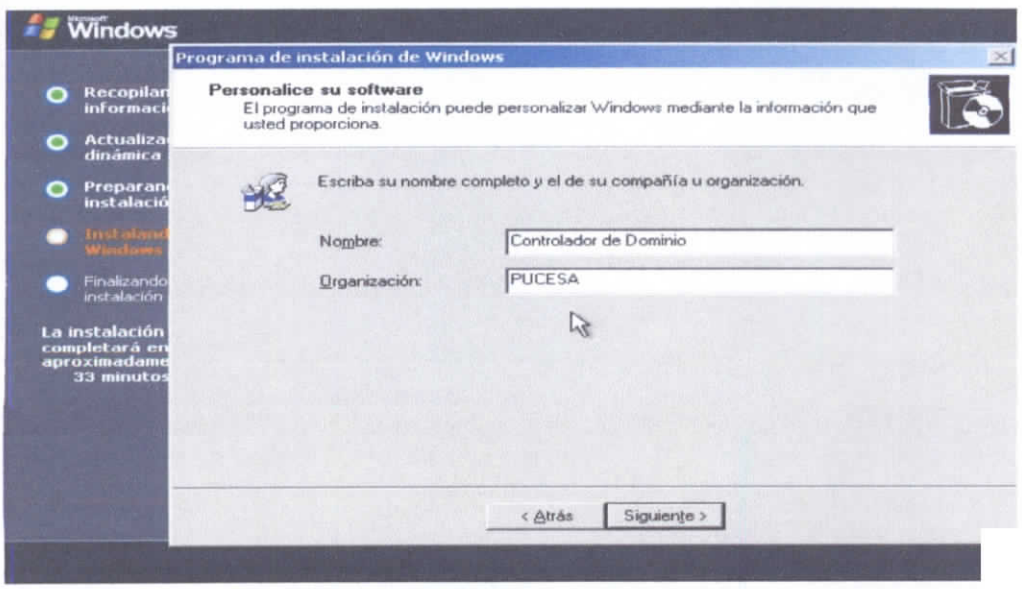


Figura 3-6 Nombre de responsable y organización

- Proporcionar la clave de producto para poder continuar.
- El modo de licencia que se utilizará es "POR SERVIDOR" y "300 CONEXIONES SIMULTANEAS" (figura 3-7), clic en SIGUIENTE.

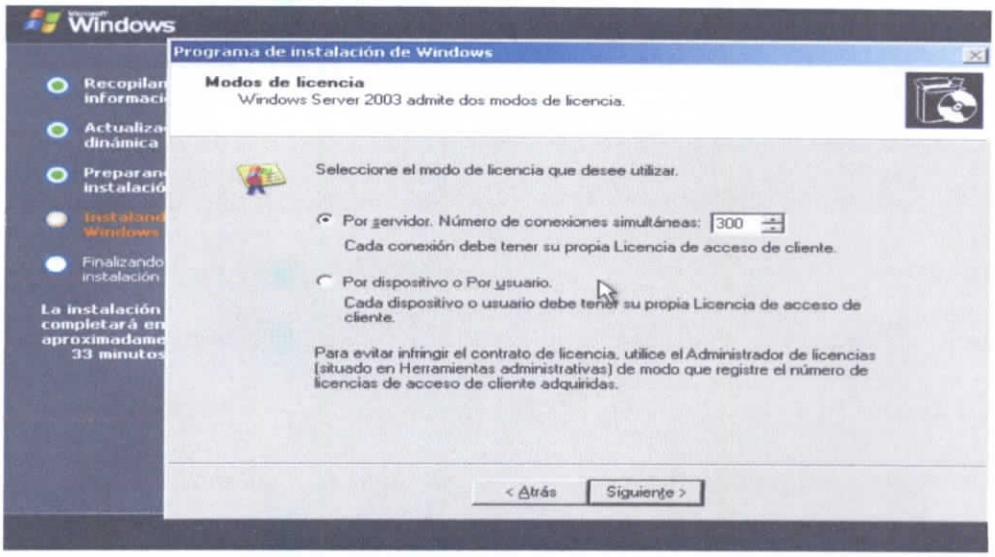


Figura 3-7 Modos de licencia

- Proporcionar el nombre del equipo para identificar en la red, digitar "LABCD01", también digitar la contraseña de la cuenta de administrador del equipo y confirmarla. Configurar: Fecha, hora y zona horaria.
- Transcurrido algunos minutos, se finalizará la instalación con la reiniciación del sistema, luego, al mismo se podrá ingresar con la cuenta de Administrador y la contraseña (figura 3-8) proporcionada anteriormente.

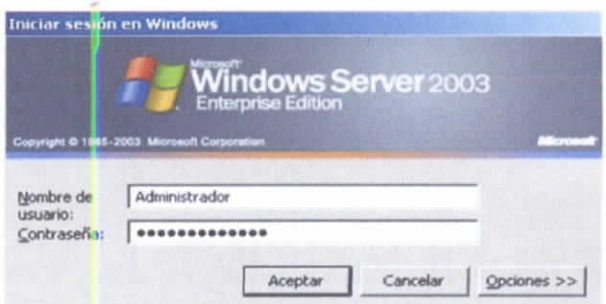


Figura 3-8 Iniciar sesión

3.4 Instalación de Active Directory (Controlador de Dominio)

Antes de la instalación recordar que un Controlador de Dominio en Windows Server 2003, esta estructurado en la base de datos distribuida de objetos que proporciona Active Directory, por tal motivo, se puede administrar un Dominio utilizando la herramienta Active Directory de Microsoft Windows Server 2003.

Para la instalación seguir los siguientes pasos:

- Verificar y configurar las conexiones de área local del servidor (figura 3-9), es decir, ingresar los siguientes parámetros:

  Dirección IP : 192.168.2.250

  Máscara de subred : 255.255.255.0

  Servidor DNS preferido : 192.168.2.250

  Por último clic en ACEPTAR en todas las ventanas que lo requieran

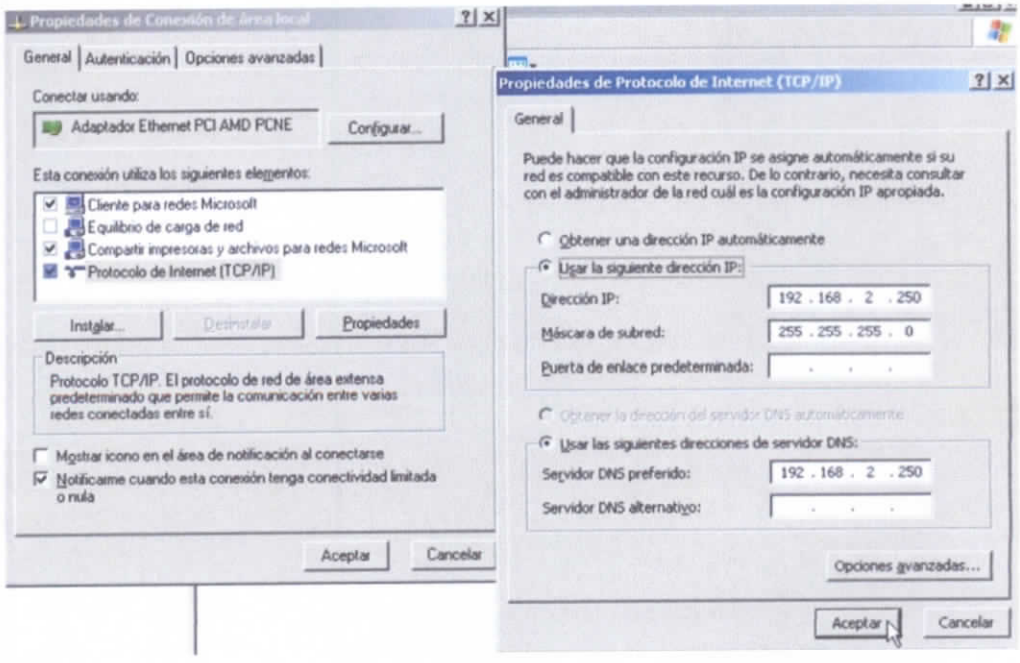


Figura 3-9 Configuración de conexión de área local

- Abrir la opción EJECUTAR, digitar el comando "DCPROMO" y presionar ACEPTAR (figura 3-10).

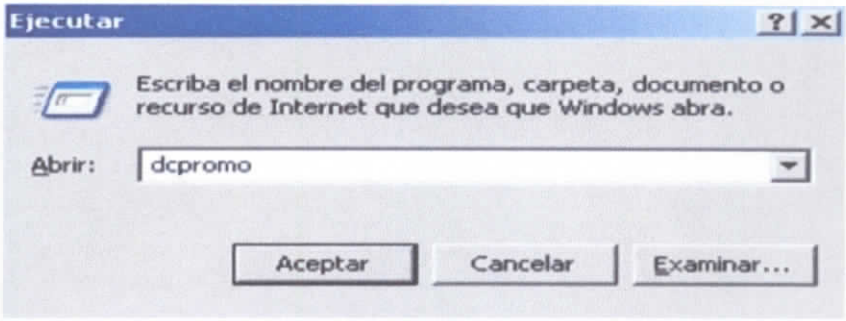


Figura 3-10 Ejecutar "dcpromo"

- De esta forma inicia el asistente de instalación de Active Directory.
- Confirmar compatibilidad del Sistema Operativo presionando en SIGUIENTE (figura 3-11).

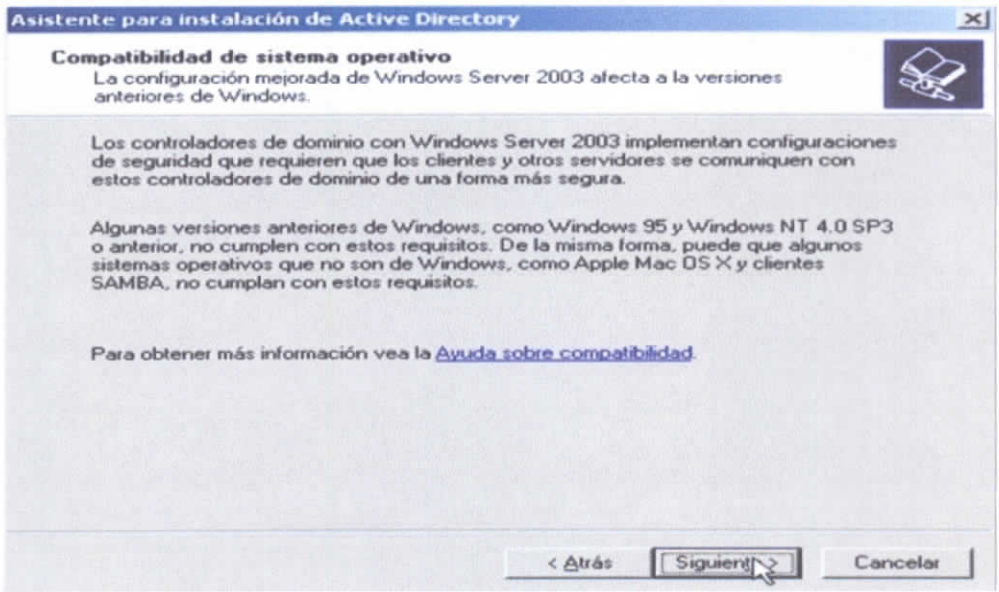


Figura 3-11 Compatibilidad del Sistema Operativo

- En este caso determinar que es el inicio de Controlador de Dominio, por lo tanto es el primero en un árbol o en un bosque de dominios, es decir el principal de toda la red, marcar la primera opción que dice CONTROLADOR DE DOMINIO PARA UN DOMINIO NUEVO, clic en SIGUIENTE (figura 3-12).

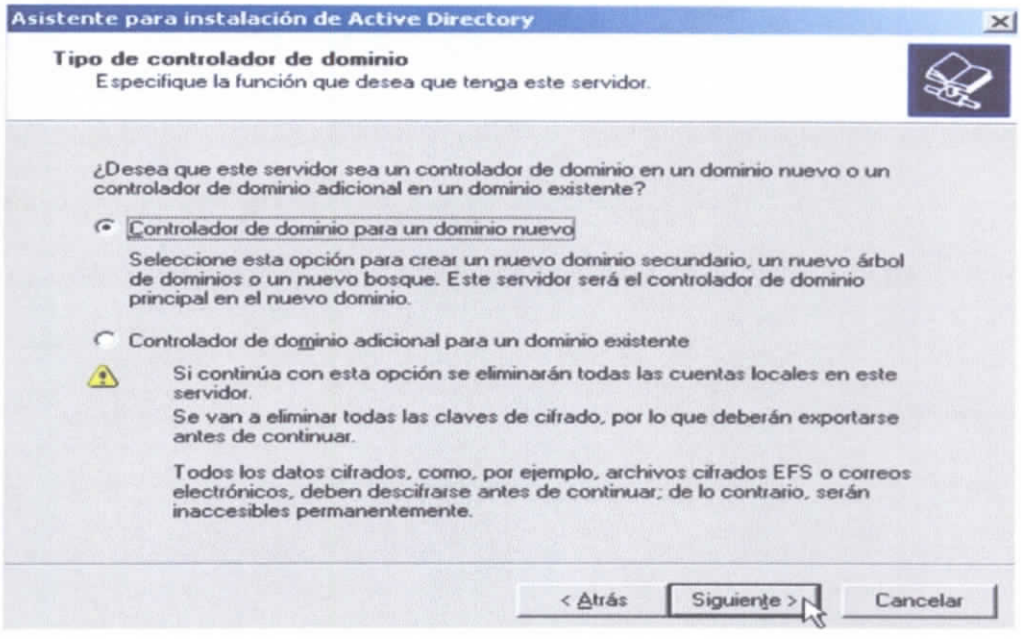


Figura 3-12 Tipo de controlador de dominio

- Marcar la alternativa DOMINIO EN UN BOSQUE NUEVO, puesto que se necesita crear un nuevo Dominio dentro del Controlador de Dominio principal, clic en SIGUIENTE (figura 3-13).

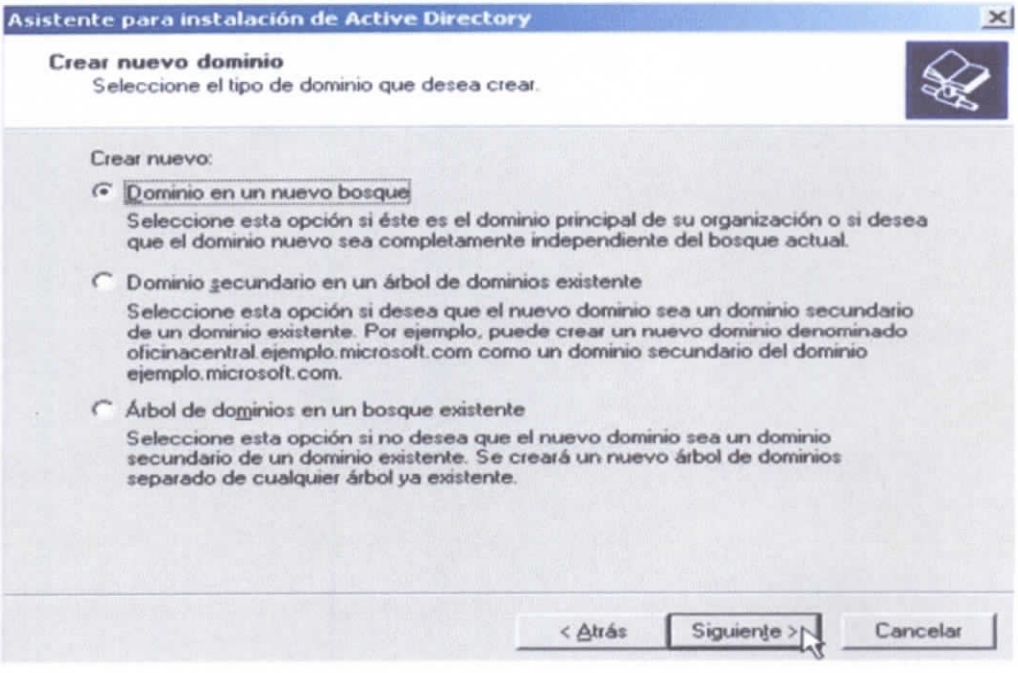


Figura 3-13 Crear nuevo dominio

- Digitar el nombre del dominio "PUCESA.INT" en el espacio dispuesto para el mismo, clic en SIGUIENTE (figura 3-14).

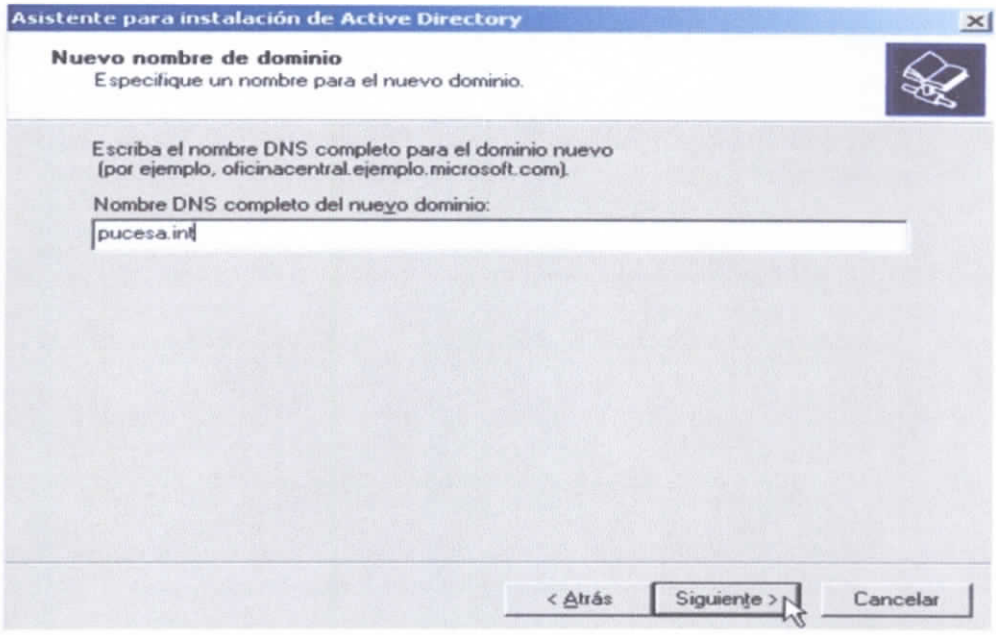


Figura 3-14 Nombre de dominio

- El nombre NetBIOS del dominio por defecto aparecerá PUCESA, clic en SIGUIENTE (figura 3-15).

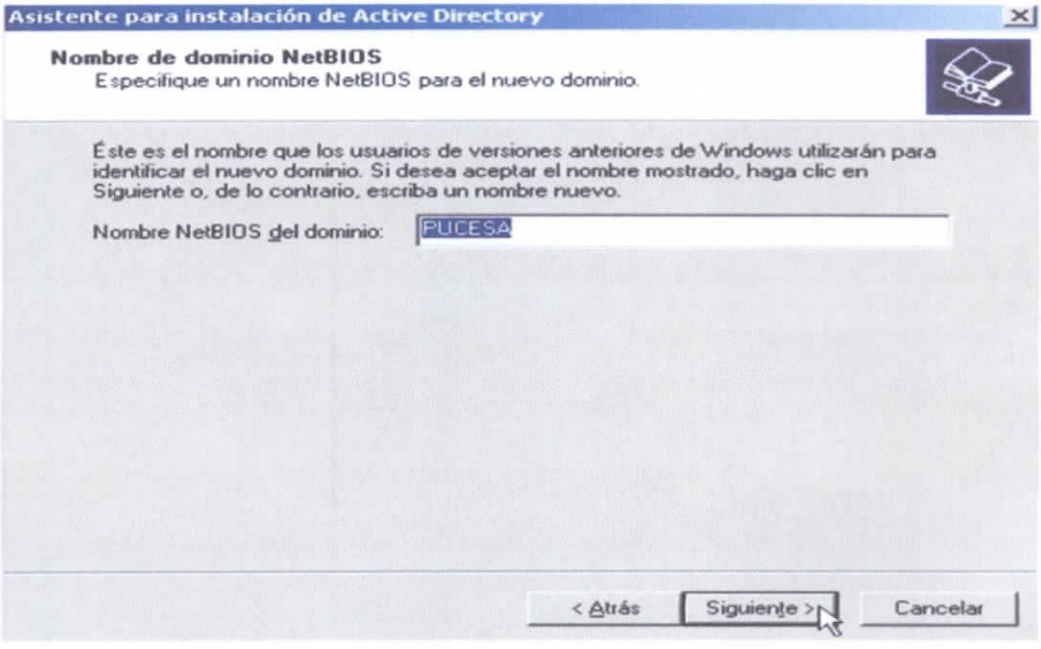


Figura 3-15 Nombre de dominio NetBIOS

- Por seguridad direccionar a la unidad D:\ las carpetas tanto de la base datos "D:\NTDS" como la del registro de Active Directory "D:\NTDS", lo anterior mencionado es una práctica recomendada por Microsoft para obtener un rendimiento y capacidad de recuperación óptimo, clic en SIGUIENTE (figura 3-16).

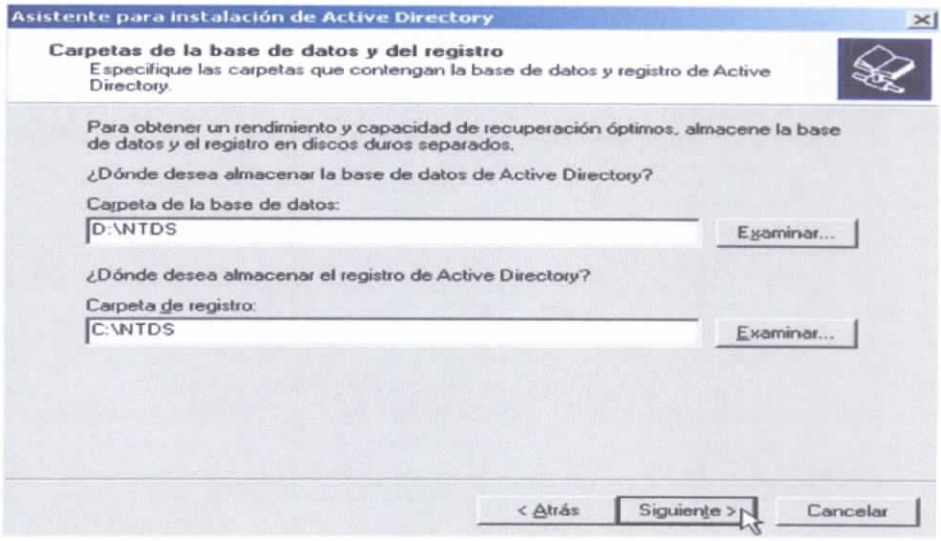


Figura 3-16 Carpetas de base de datos y registros de Active Directory

- De la misma manera la carpeta SYSVOL debe estar ubicada en una partición diferente, será ubicada de la siguiente manera, "D:\SYSVOL", clic en SIGUIENTE (figura 3-17).

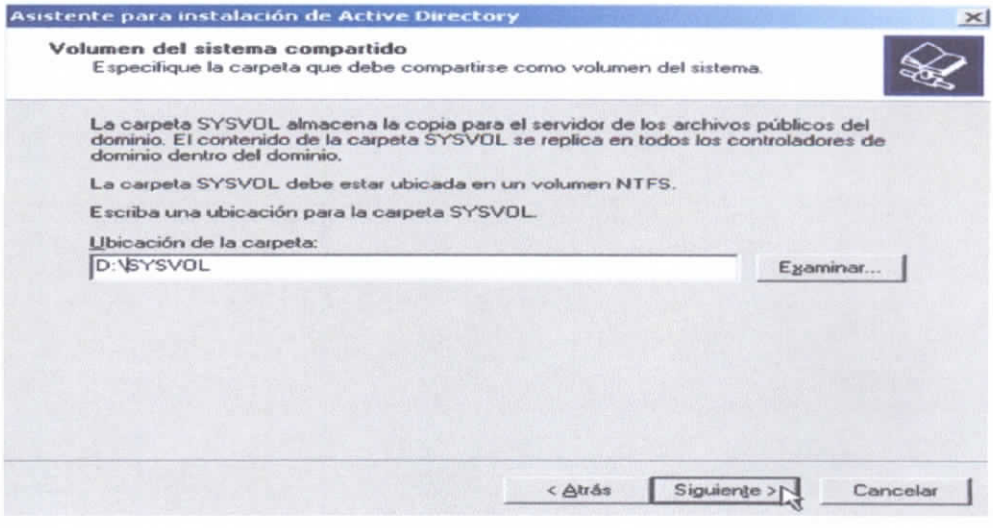


Figura 3-17 Carpeta de SYSVOL

- Marcar la tercera opción, CORREGIRÉ EL PROBLEMA MAS TARDE, CONFIGURANDO EL DNS MANUALMENTE. (AVANZADO), este error se despliega porque no se encuentra instalado el componente de DNS en el Sistema Operativo, hay que destacar que es un error informativo que más adelante se corregirá, clic en SIGUIENTE (figura 3-18).

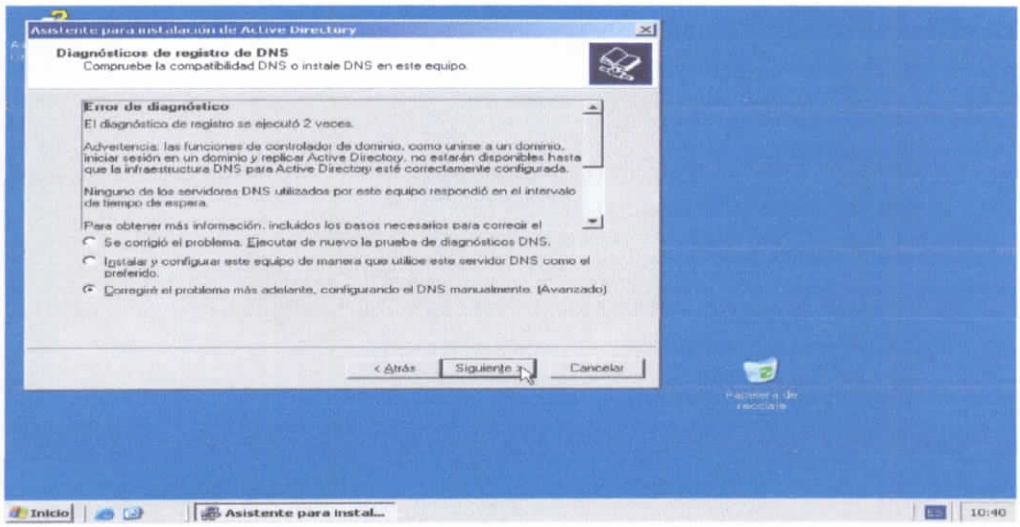


Figura 3-18 Error de diagnóstico

- Marcar la segunda opción, PERMISOS COMPATIBLES SOLO CON SISTEMAS OPERATIVOS DE SERVIDOR WINDOWS 2000 O WINDOWS SERVER 2003, clic en SIGUIENTE (figura 3-19).

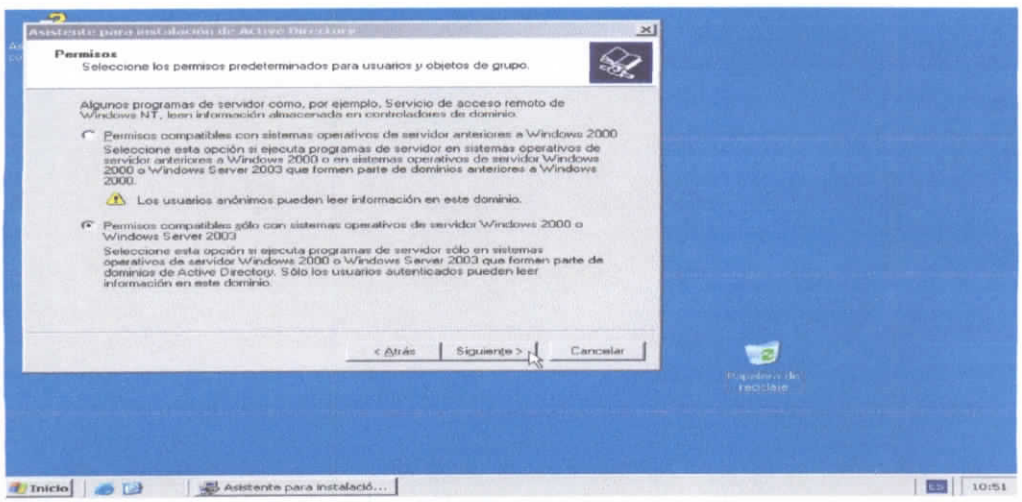


Figura 3-19 Permisos compatibles con versiones anteriores

- Digitar una contraseña y confirmar, la misma servirá para la restauración de servicios de directorio, clic en SIGUIENTE (figura 3-20).

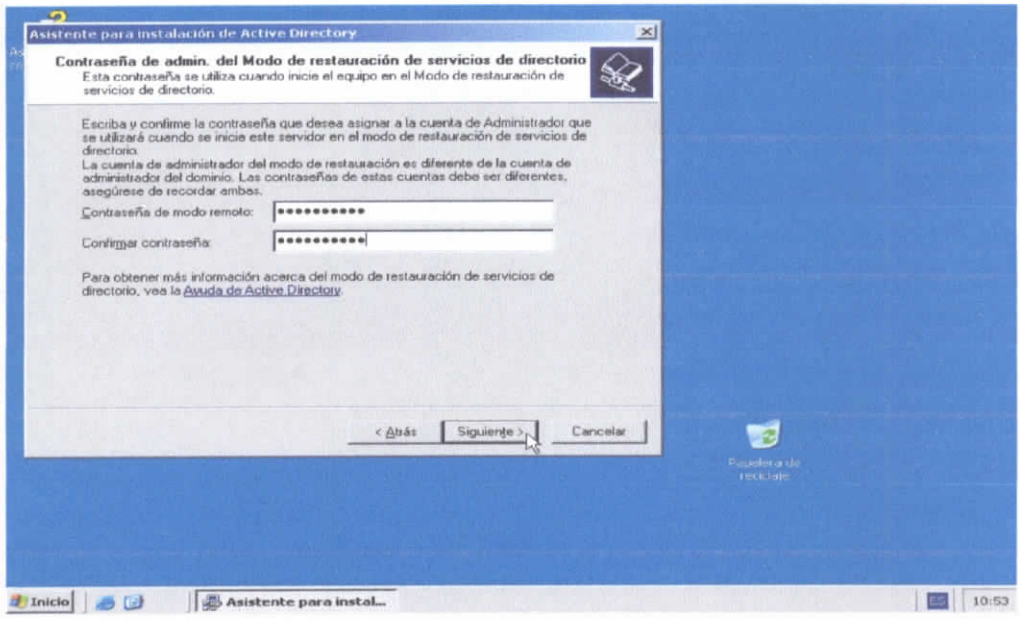


Figura 3-20 Contraseña para restauración de servicios de directo

- Confirmar el resumen de instalación y finalizar el asistente de instalación de Active Directory (figura 3-21).

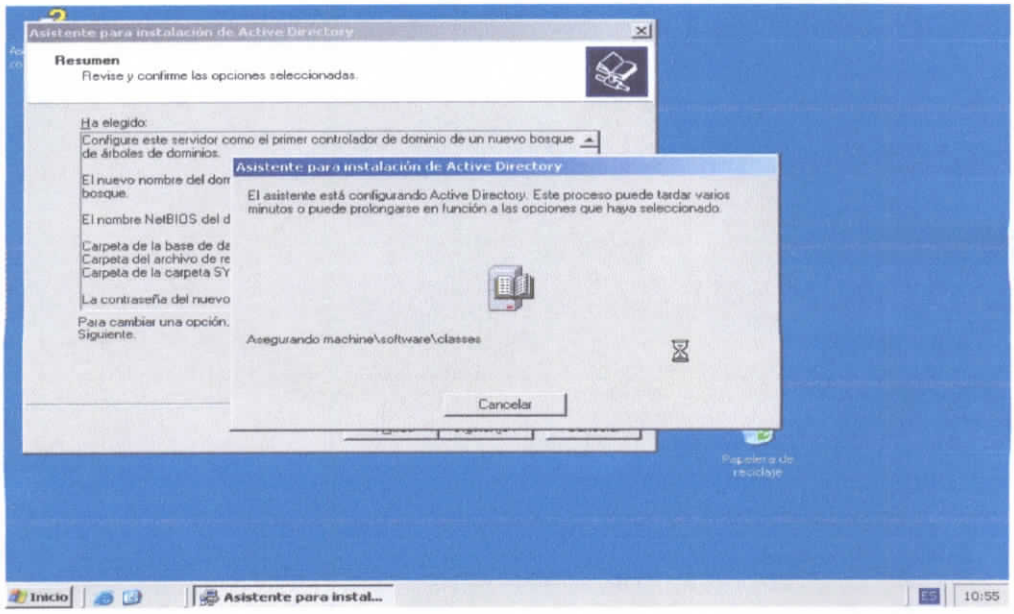


Figura 3-21 Finalización de instalación de Active Directory

3.5 Instalación de DNS (Domain Name System)

Para la instalación seguir los siguientes pasos:

- Ingresar al Panel del Control, doble clic en AGREGAR O QUITAR PROGRAMAS, clic en AGREGAR O QUITAR COMPONENTES DE WINDOWS (figura 3-22).

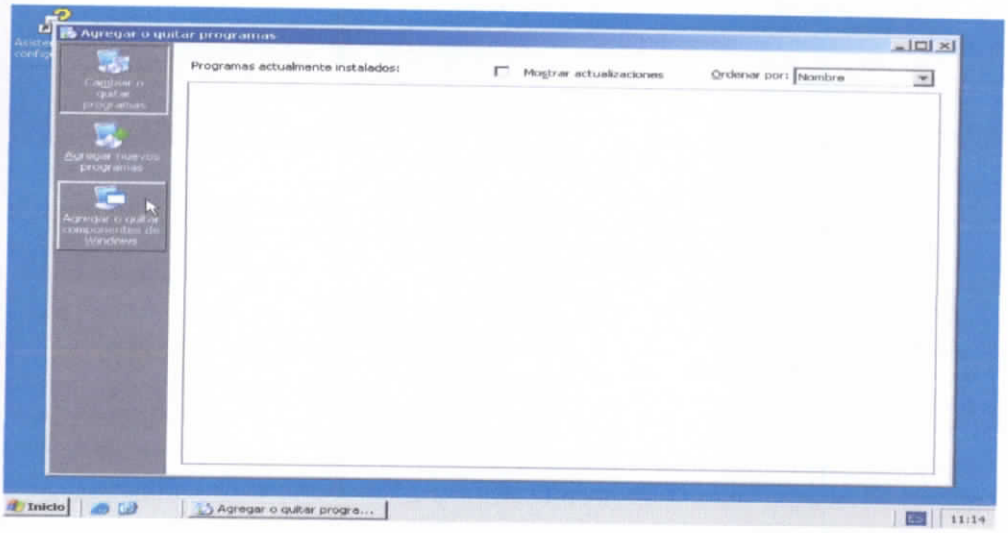


Figura 3-22 Agregar o quitar componente de Windows

- Clic en SERVICIOS DE RED, clic en DETALLES (figura 3-23).

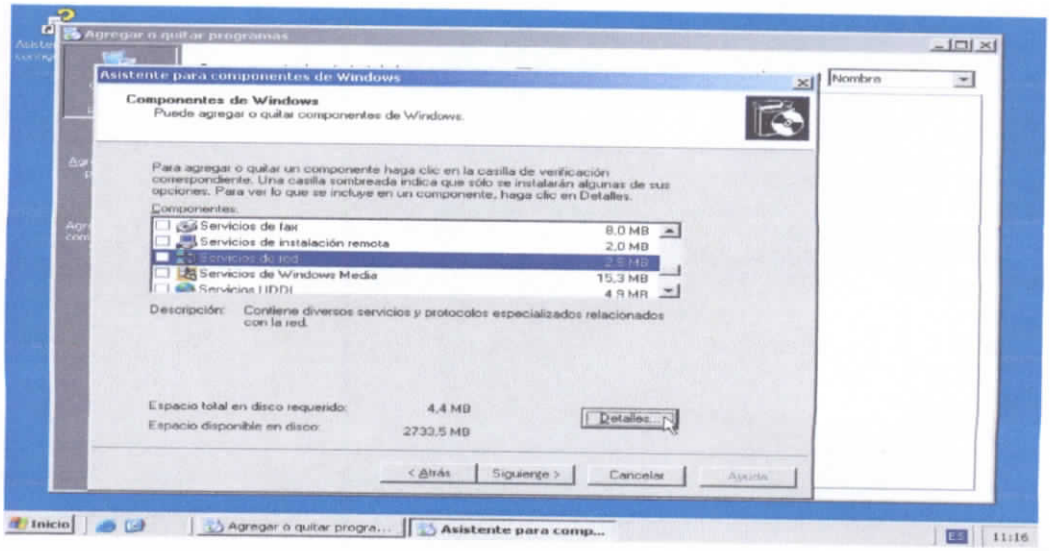


Figura 3-23 Servicios de red

- Marcar el casillero de SISTEMA DE NOMBRES DE DOMINIO (DNS), clic en ACEPTAR (figura 3-24).

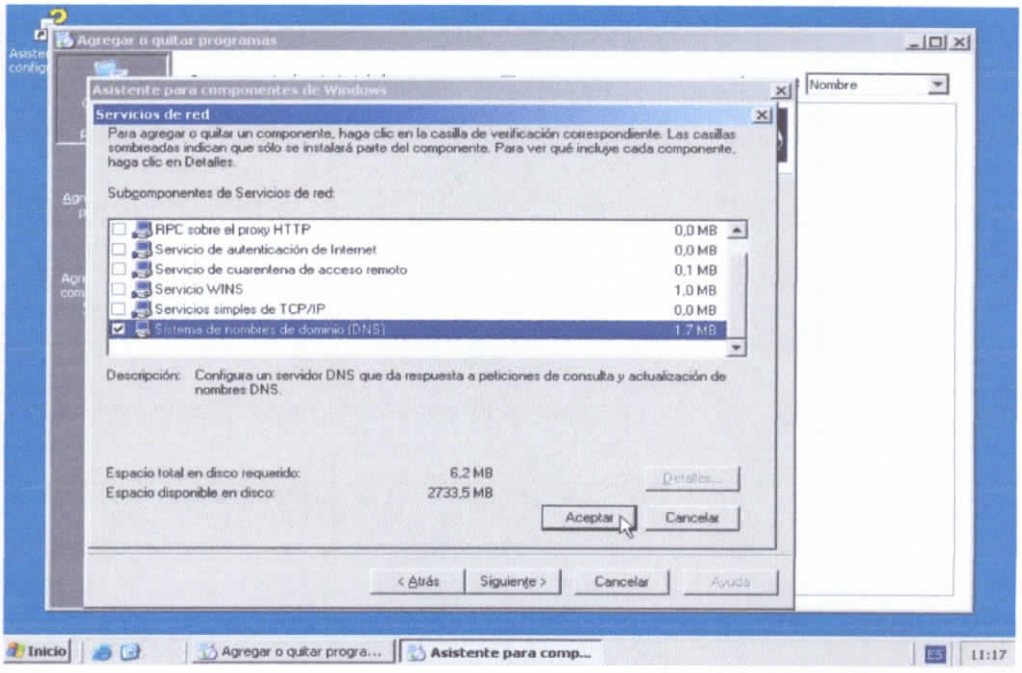


Figura 3-24 Agregar componente DNS

- Confirmar todas las restantes ventanas para agregar el componente DNS, hasta finalizar la instalación.
- Después del proceso anterior, revisar que el servicio de DNS este instalado correctamente, para esto, clic en TODOS LOS PROGRAMAS, clic en HERRAMIENTAS ADMINISTRATIVAS y clic en DNS (figura 3-25). DNS esta conformada por dos zonas, la primera ZONAS DE BÚSQUEDA DIRECTA se encuentra lista para realizar el registro por nombres de computadores, esto se debe a que previo a la instalación de DNS, se realizó la de Active Directory.

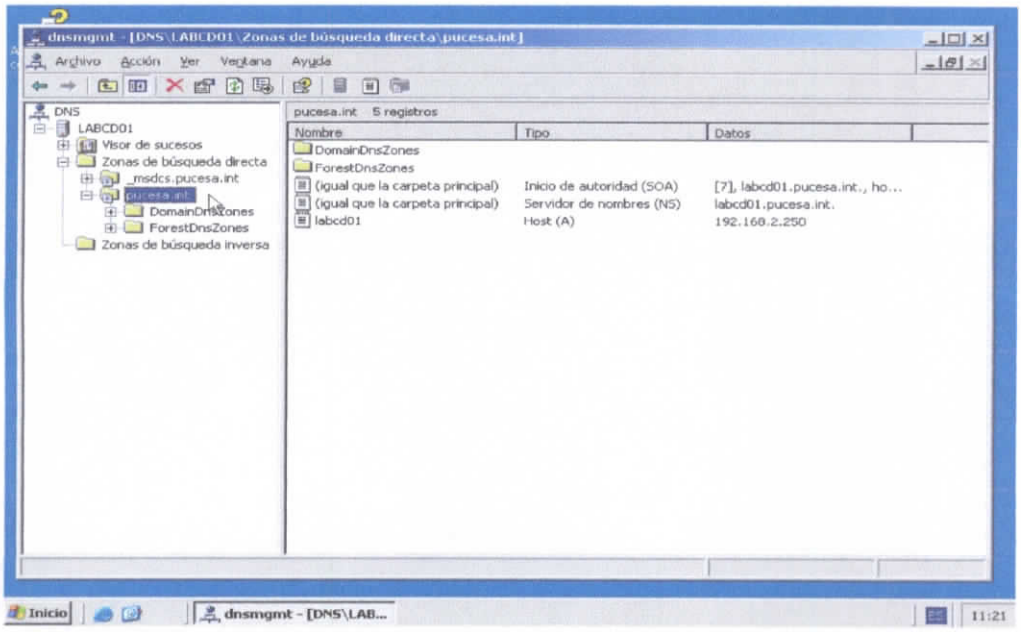


Figura 3-25 Comprobación de aplicación DNS

- La segunda zona a configurar es ZONAS DE BÚSQUEDA INVERSA, clic derecho en la misma , clic en CREAR NUEVA ZONA, en la ventana del asistente clic en SIGUIENTE (Figura 3 - 26).

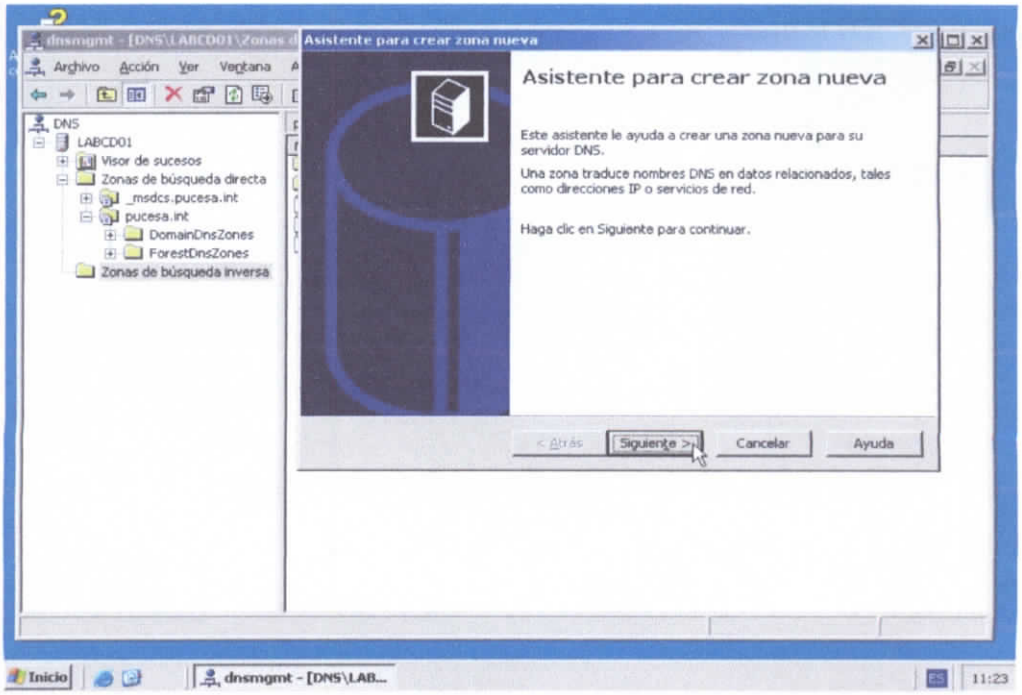


Figura 3-26 Asistente para crear zona nueva

- Marcar la ZONA PRINCIPAL puesto que es la primera en el Dominio, clic en SIGUIENTE (figura 3-27).

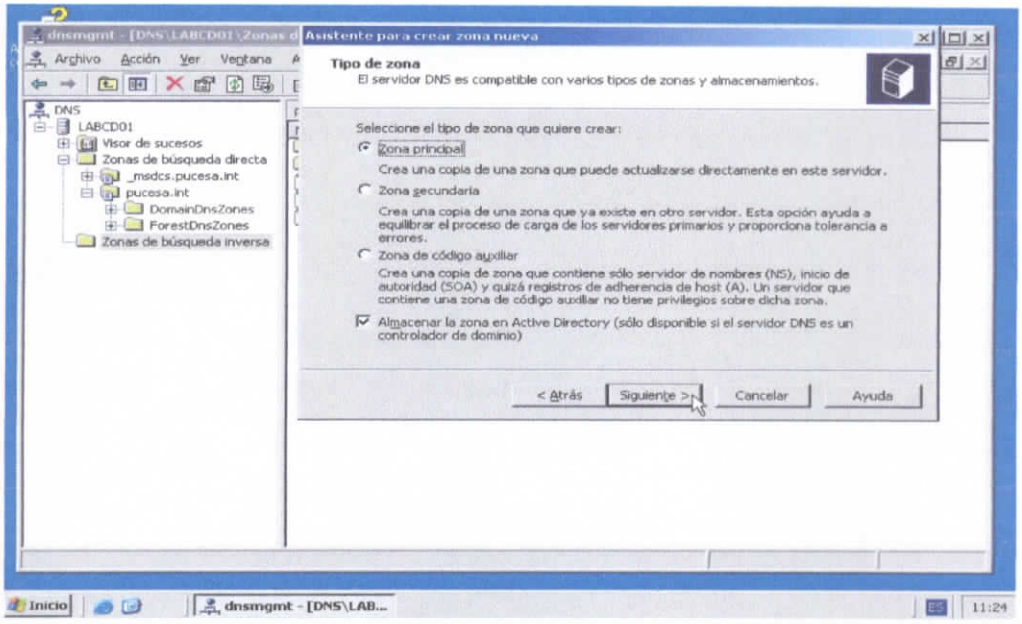


Figura 3-27 Tipo de zona

- Marcar la tercera opción PARA TODOS LOS CONTROLADORES DE DOMINIO EN EL DOMINIO PUCESA.INT DE ACTIVE DIRECTORY, clic en SIGUIENTE (figura 3-28).

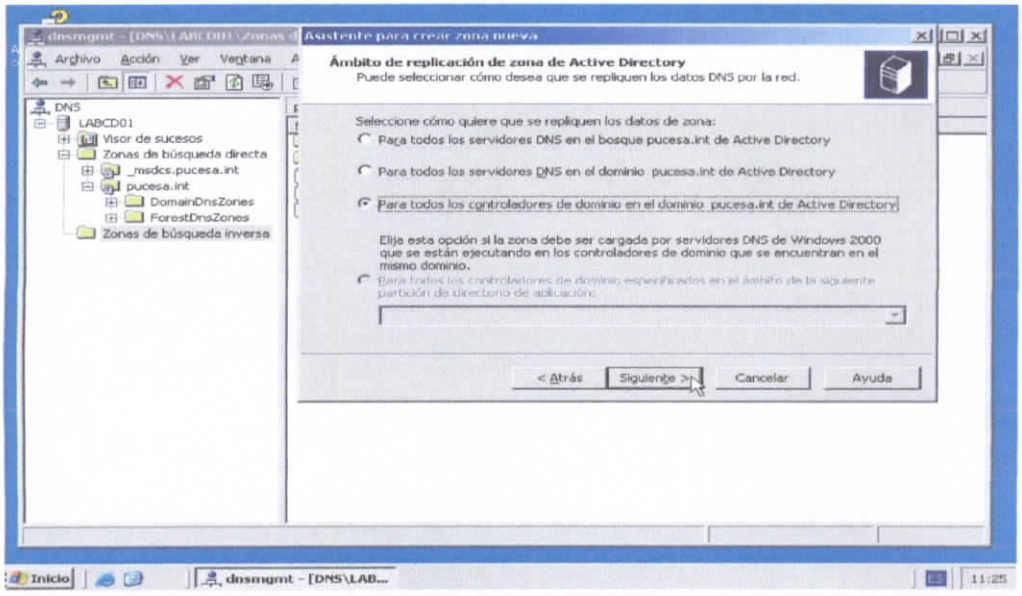


Figura 3-28 Ámbito de replicación de zona

- Escoger la primera opción ID DE RED y digitar 192.168.2 esto es para identificar la zona de búsqueda inversa, clic en SIGUIENTE (figura 3-29).

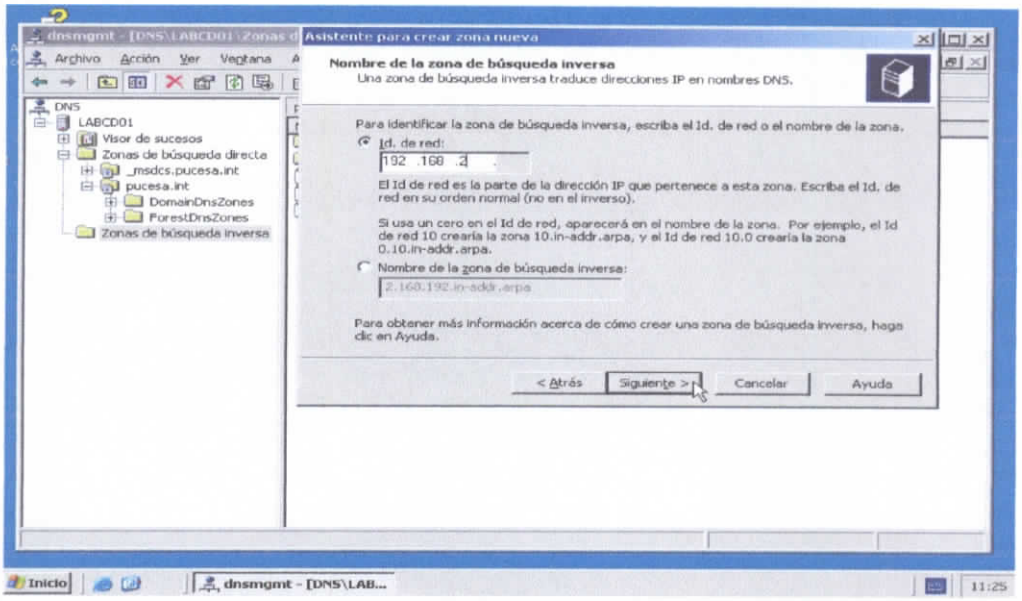


Figura 3-29 Nombre de la zona de búsqueda inversa

- Marcar la primera opción PERMITIR SOLO ACTUALIZACIONES DINÁMICAS SEGURAS, clic en SIGUIENTE (figura 3-30) y finalizar el asistente para crear zona nueva.

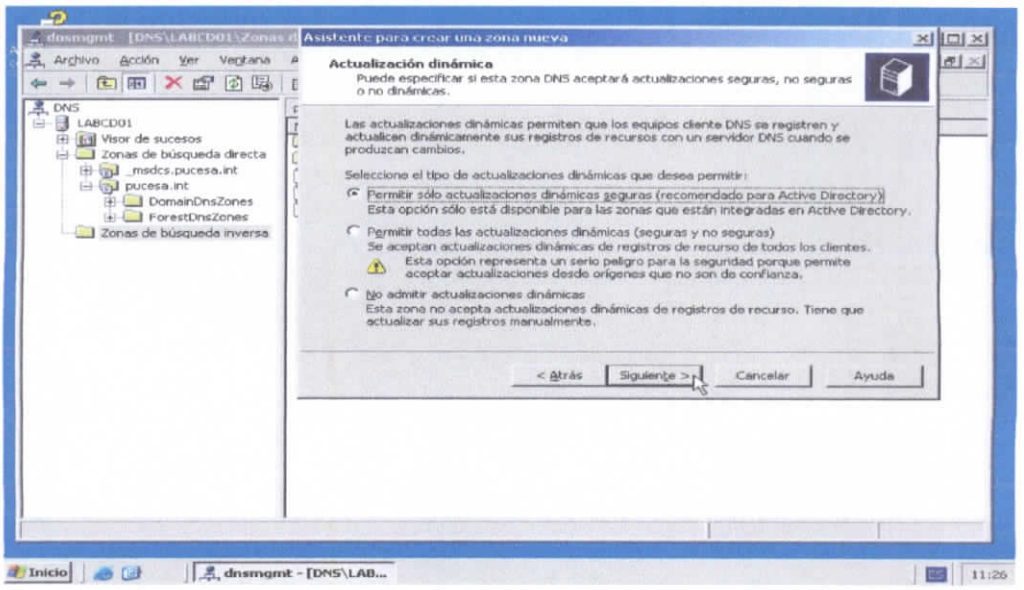


Figura 3-30 Actualización dinámica

3.6 Instalación de DHCP (Dynamic Host Configuration Protocol)

Para la instalación seguir los siguientes pasos:

- Ingresar al Panel del Control, doble clic en AGREGAR O QUITAR PROGRAMAS, clic en AGREGAR O QUITAR COMPONENTES DE WINDOWS (figura 3-31).

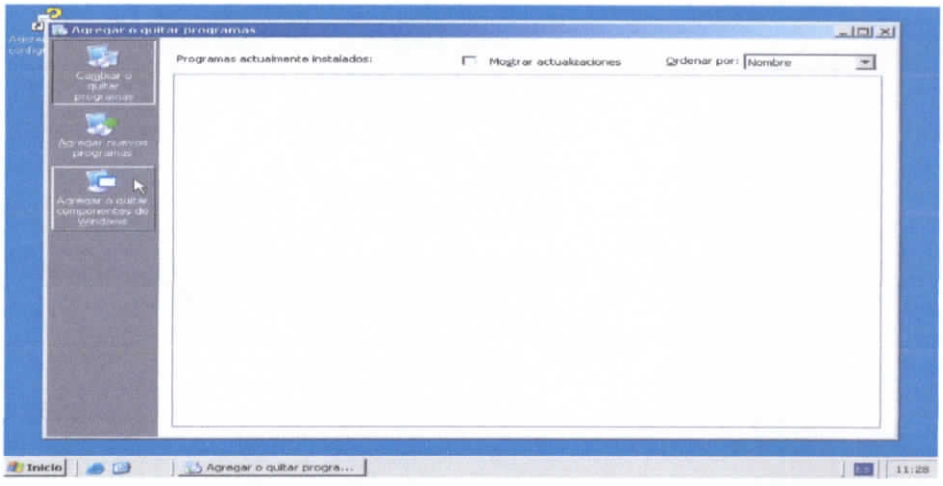


Figura 3-31 Agregar o quitar componentes de Windows

- Clic en SERVICIOS DE RED, clic en DETALLES (figura 3-32).

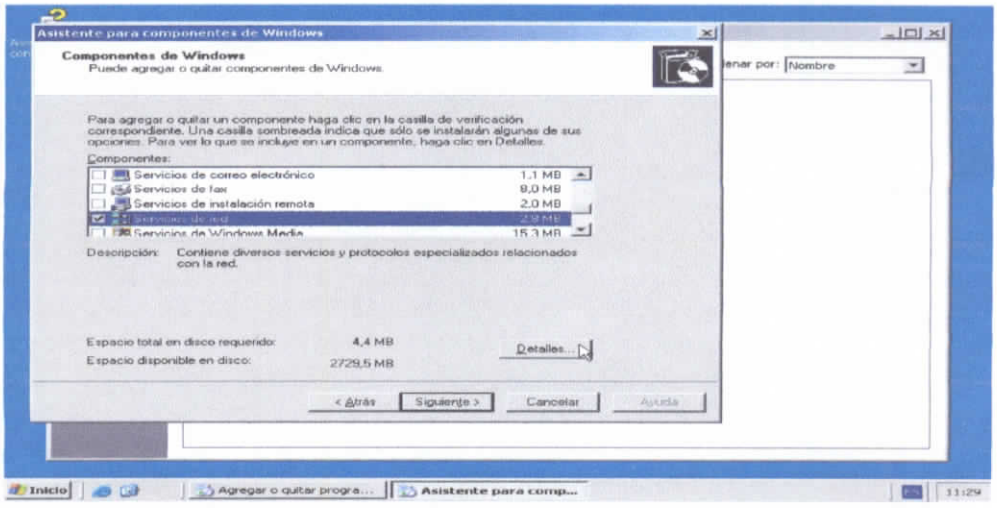


Figura 3-32 Servicios de red

- Marcar el casillero de PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) (figura 3-33), clic en ACEPTAR.

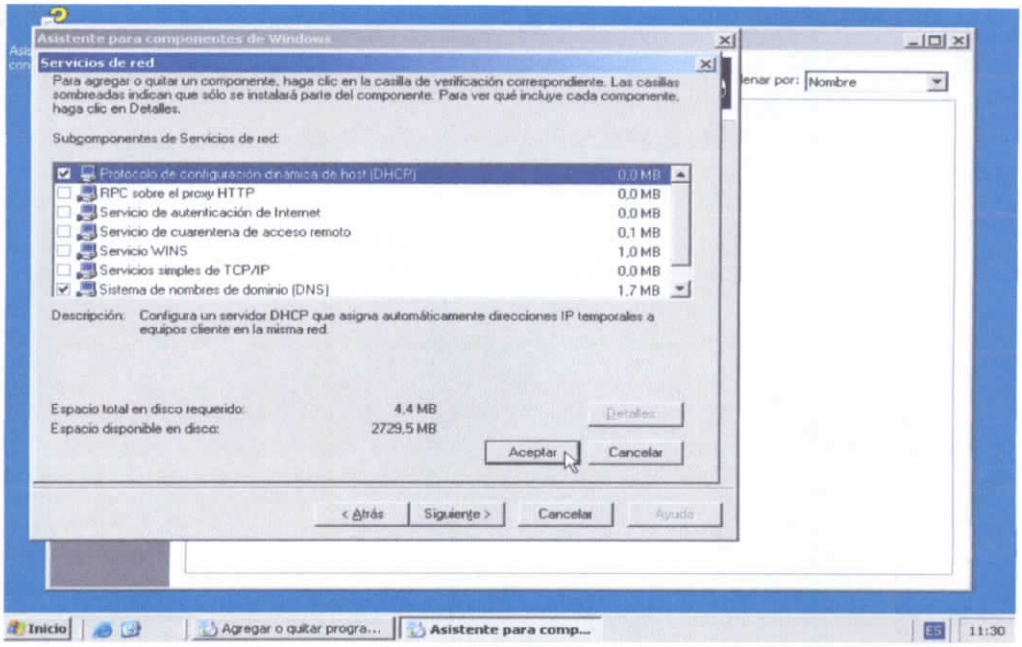


Figura 3-33 Seleccionar DHCP

- Confirmar las restantes ventanas de instalación de la aplicación DHCP y finalizar el asistente para componentes de Windows.
- Después del proceso anterior, revisar que la instalación de DHCP este instalado correctamente, para esto, clic en TODOS LOS PROGRAMAS, clic en HERRAMIENTAS ADMINISTRATIVAS y clic en DHCP (figura 3-34).

  DHCP es el protocolo que hace posible la distribución aleatoria de direcciones IP a los equipos disponibles de la red. Por defecto toma el nombre del equipo servidor DHCP en este caso LABCD01.PUCESA.INT

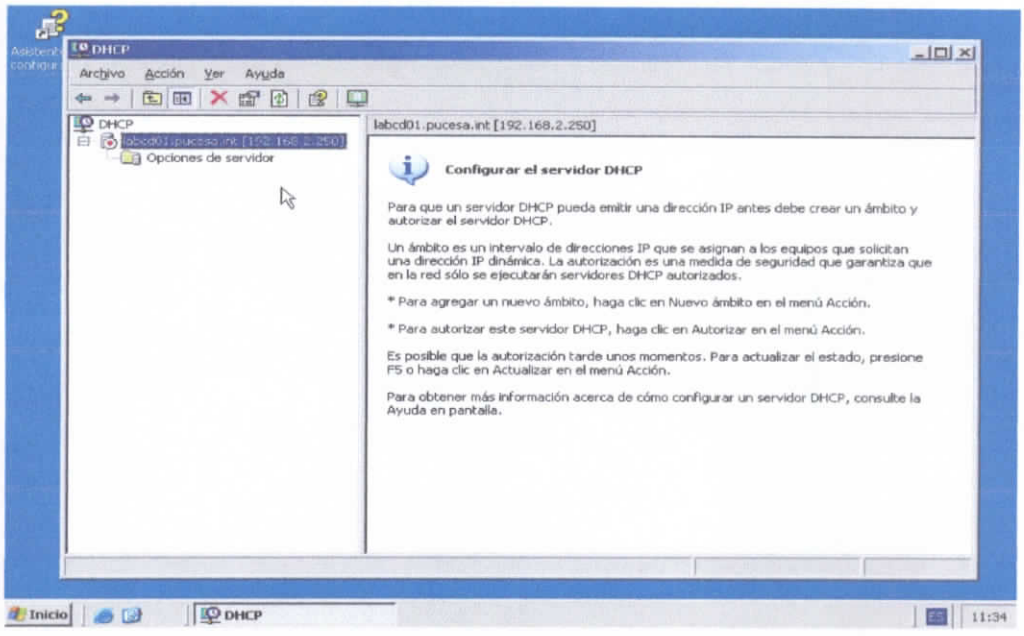


Figura 3-34 Comprobación de aplicación DHCP

- DHCP debe ser autorizado por el dominio para su ejecución de entrega de direcciones IP, por lo tanto clic derecho en LABCD01.PUCESA.INT, clic en AUTORIZAR (figura 3-35).

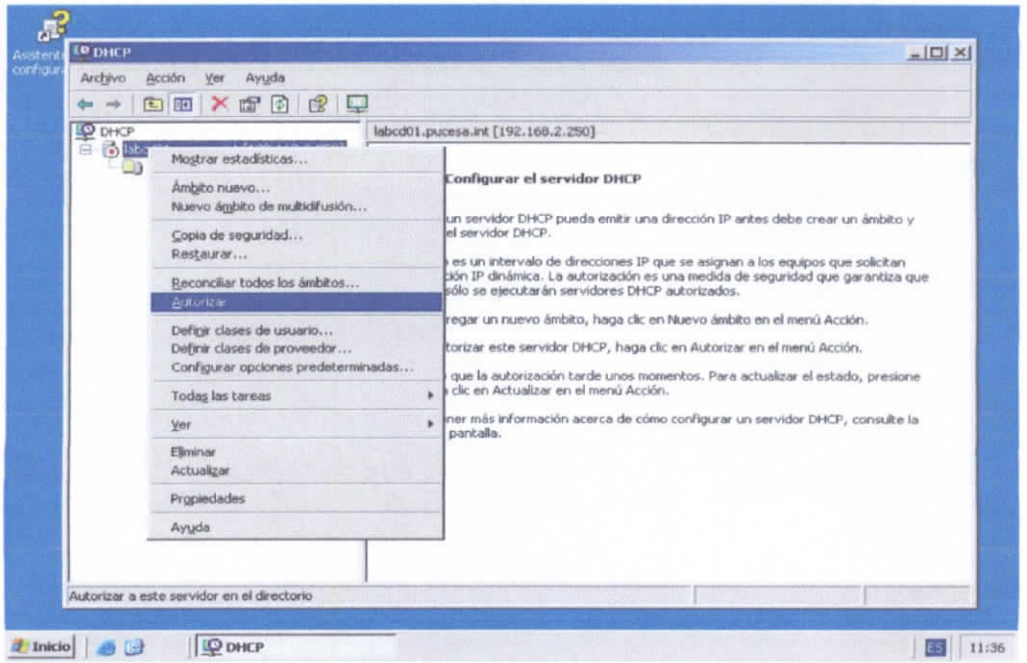


Figura 3-35 Activar DHCP

- Clic derecho en LABCD01.PUCESA.INT, clic en ÁMBITO NUEVO.... (figura 3-36). Iniciar el asistente para ámbito nuevo.

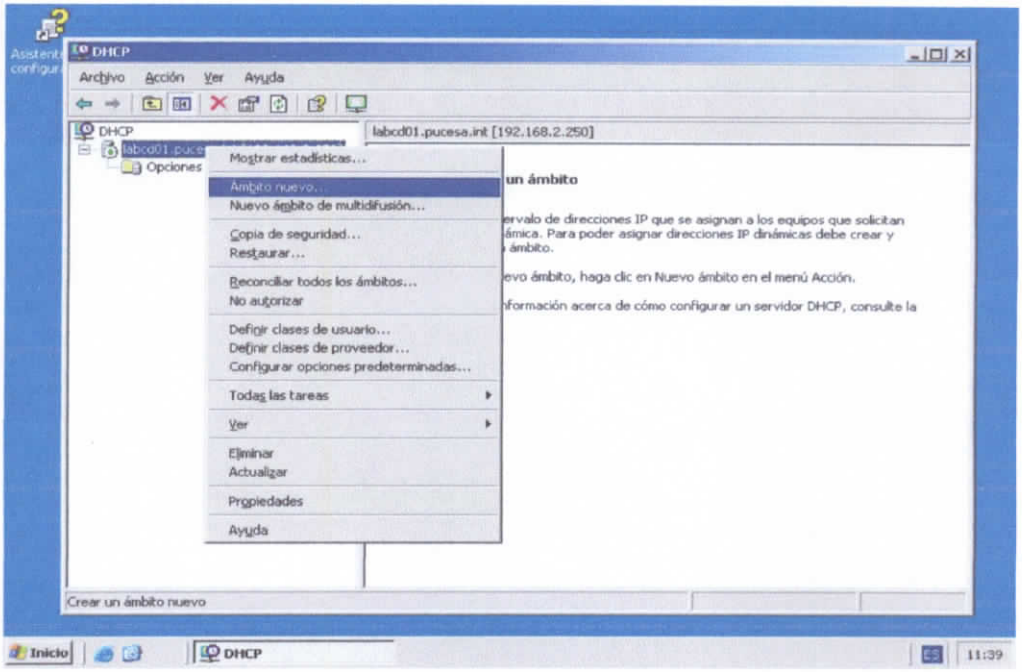


Figura 3-36 Ámbito nuevo

- Digitar "PUCESA.INT" en el espacio designado para el nombre, clic en SIGUIENTE (figura 3-37).

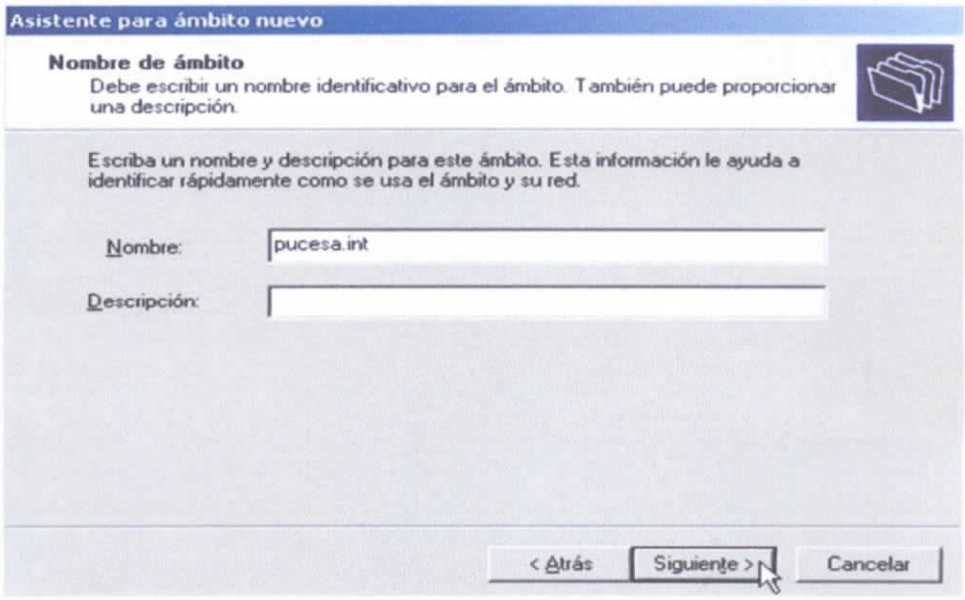


Figura 3-37 Nombre de ámbito

- El intervalo de direcciones IP es muy importante para la entrega aleatoria de las mismas por lo tanto debemos digitar lo siguiente (figura 3-38).

  Dirección IP inicial : 192.168.2.11
  Dirección IP final : 192.168.2.100
  Longitud : 24
  Mascara de subred : 255.255.255.0

  La dirección IP final cambio a 192.168.2.100 por solicitud del administrador de red

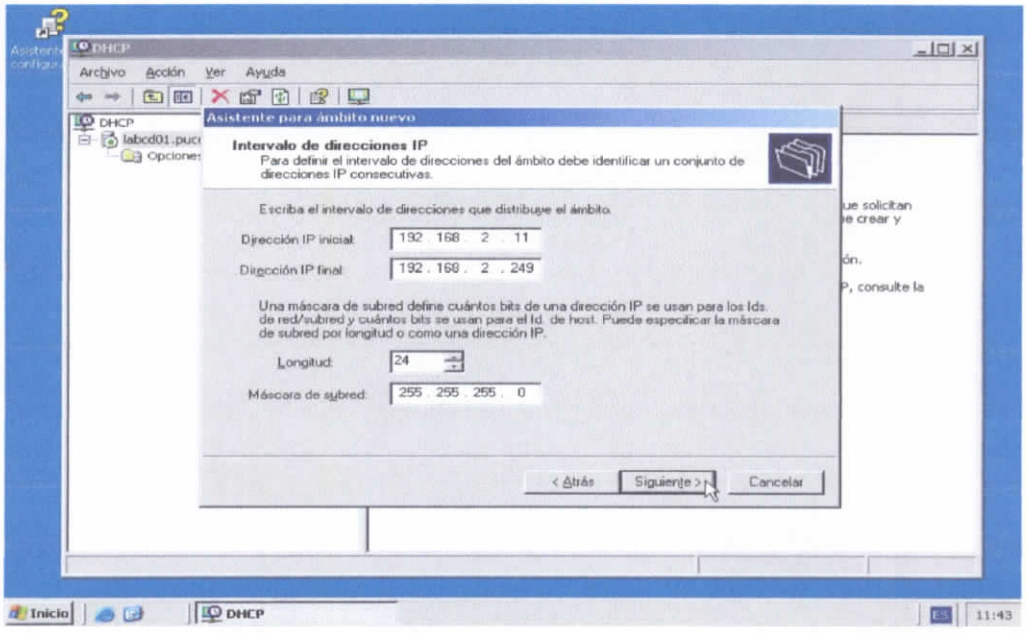


Figura 3-38 Intervalo de direcciones IP

- Dado que el servidor Proxy es muy importante para el servicio de Internet de los laboratorios debemos hacer una exclusión de la dirección IP 192.168.2.200 (figura 3-39) por lo tanto digitar lo siguiente:

  Dirección IP inicial : 192.168.2.200
  Dirección IP final : 192.168.2.200
  Clic en AGREGAR, clic en SIGUIENTE.

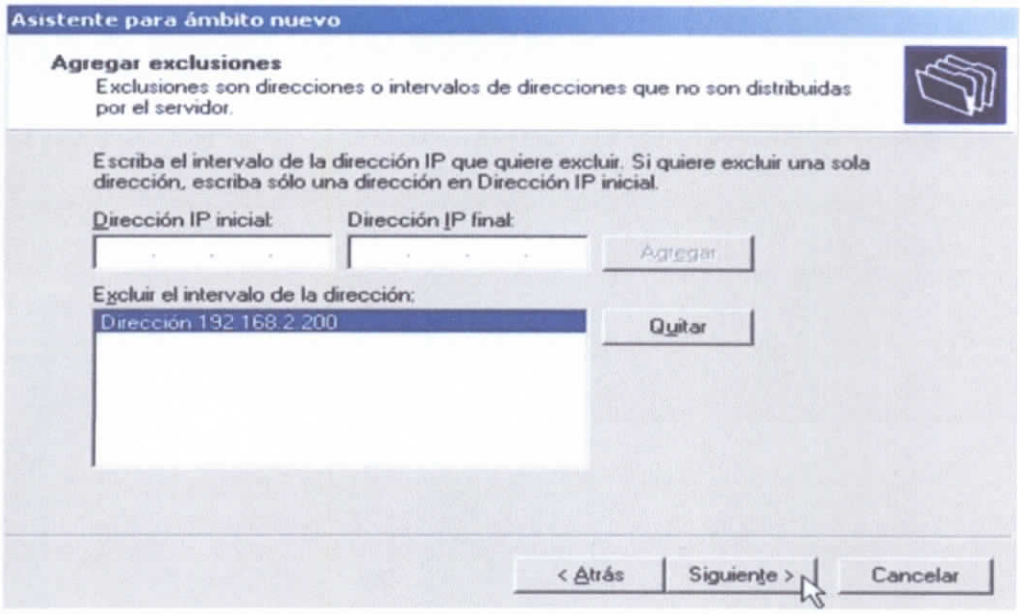


Figura 3-39 Agregar exclusiones

- La duración de conexión es decir el tiempo que DHCP sostendrá una dirección IP a un computador será de 8 DÍAS, digitar en días el número 8, clic en SIGUIENTE (figura 3-40).

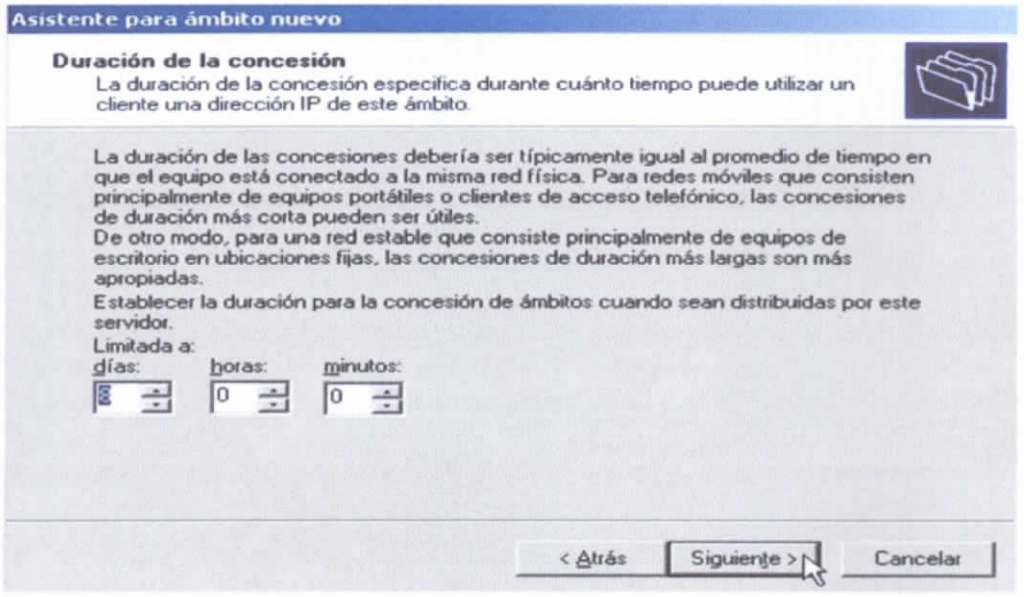


Figura 3-40 Duración de la concesión

- Marcar la segunda opción CONFIGURARE ESTAS OPCIONES MAS TARDE, clic en SIGUIENTE (figura 3-41). Finalizar el asistente para ámbito nuevo y reiniciar el equipo.

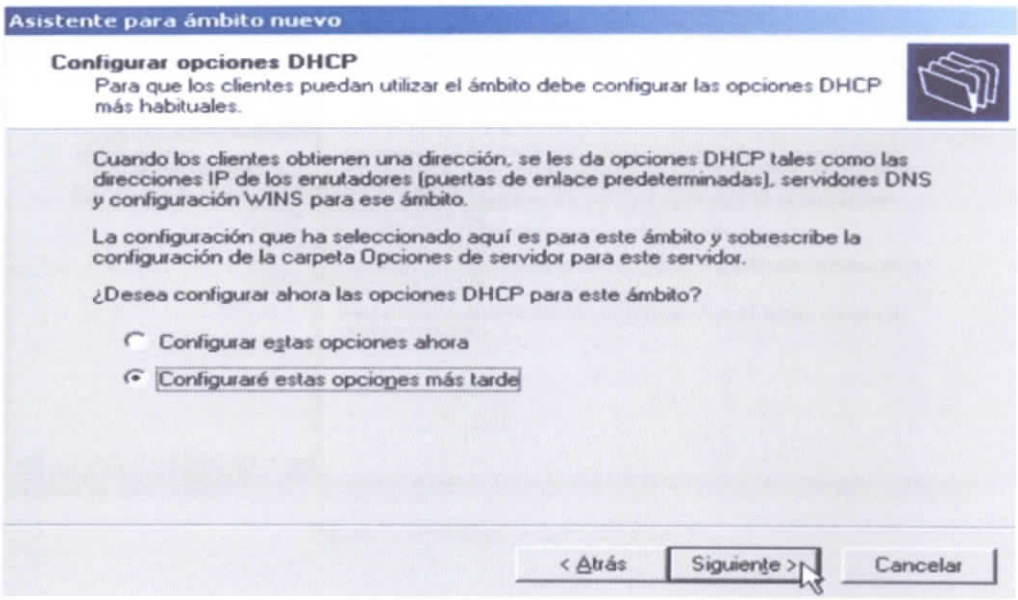


Figura 3-41 Configuración opciones DHCP

- Ingresar a la Herramienta Administrativa DHCP, clic derecho al ámbito, clic en ACTIVAR (figura 3-42).

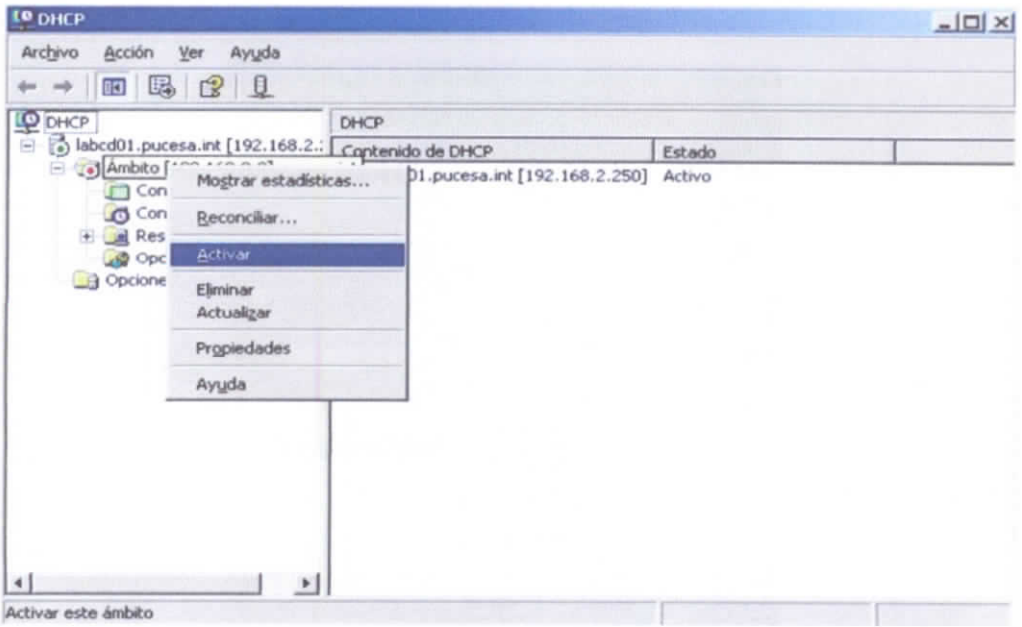


Figura 3-42 Activar servicio DHCP

3.7 Construcción y Pruebas del Controlador de Dominio

3.7.1 Creación de Unidades Organizativas (OU)

Las Unidades Organizativas son contenedores para algunos de los objetos que conforman el Dominio como son los usuarios, equipos, grupos etc. En dichos contenedores se pueden crear más UO.

Para crear Unidades Organizativas seguir los siguientes pasos.

- Ubicar la raíz de Active Directory, clic DERECHO, clic en NUEVO y clic en UNIDAD ORGANIZATIVA (figura 3-45).

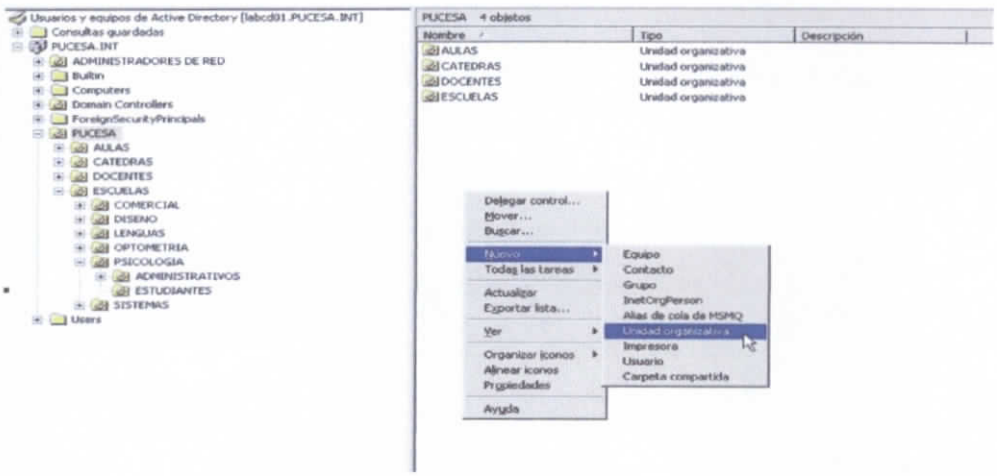


Figura 3-45 Creación UO

- Digitar el nombre de la UO requerida, clic en ACEPTAR (figura 3-46).

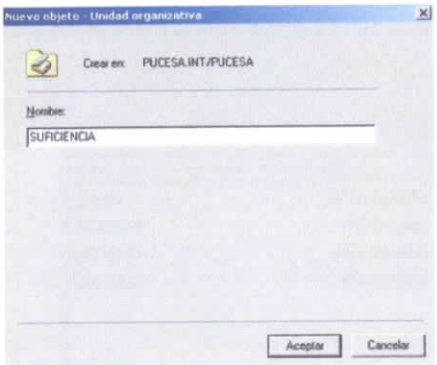


Figura 3-46 Nombre de UO

3.7.1.1 El Esquema Organizacional traducido al Controlador de Dominio

El esquema organizacional que fue realizado en la planificación estratégica de la infraestructura de red, contribuyó de manera directa en la construcción del Controlador de Dominio, obteniendo el siguiente resultado:

- PUCESA es la OU principal, dentro de la cual se encontrarán las siguientes OU: AULAS, CÁTEDRAS, DOCENTES, ESCUELAS (figura 3-47 y 3-48).

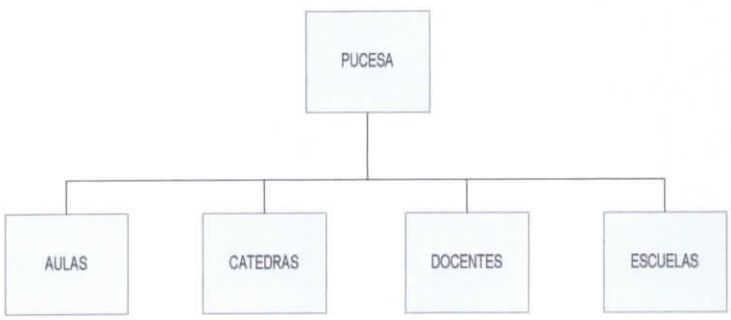


Figura 3-47 Esquema Organizacional

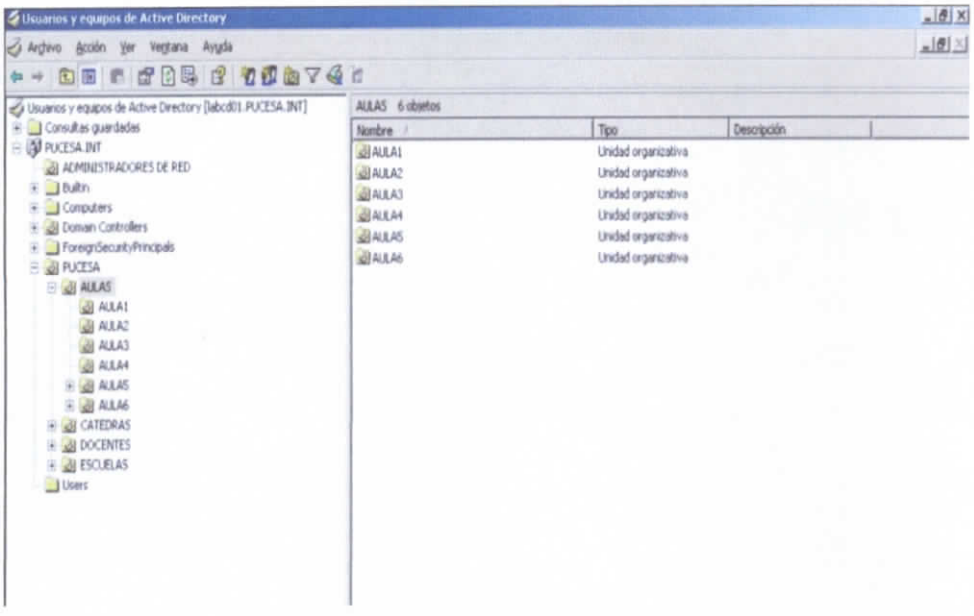


Figura 3-50 OU AULAS en Active Directory

- En la OU llamada CÁTEDRAS (figura 3-51 y 3-52), ingresar todo lo concerniente a las materias dictadas en la PUCESA.

Figura 3-51 OU CÁTEDRAS

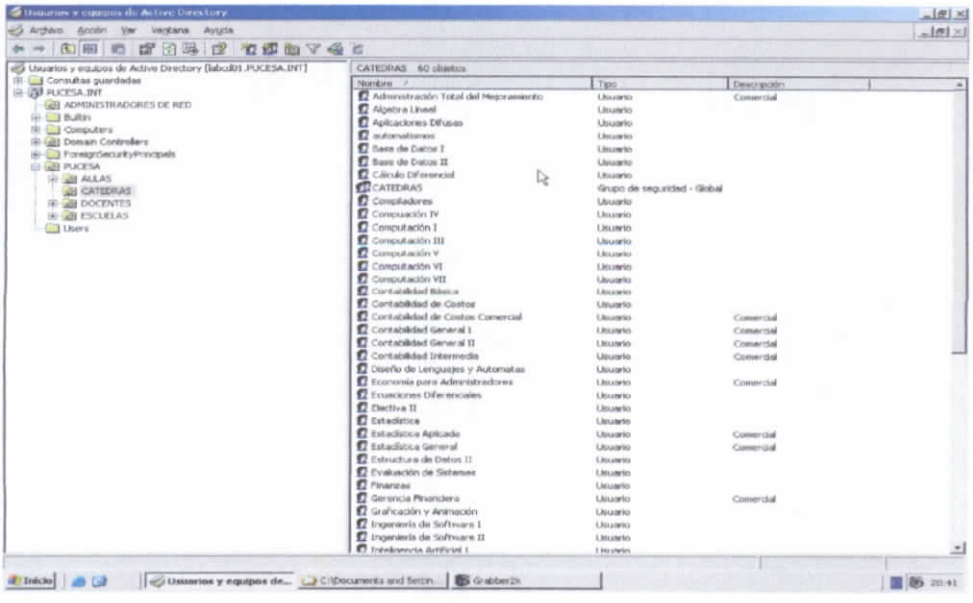


Figura 3-52 OU CÁTEDRAS en Active Directory

- Dentro de DOCENTES (figura 3-53 y 3-54) se encontrarán todos los profesores de la PUCESA

Figura 3-53 UO DOCENTES

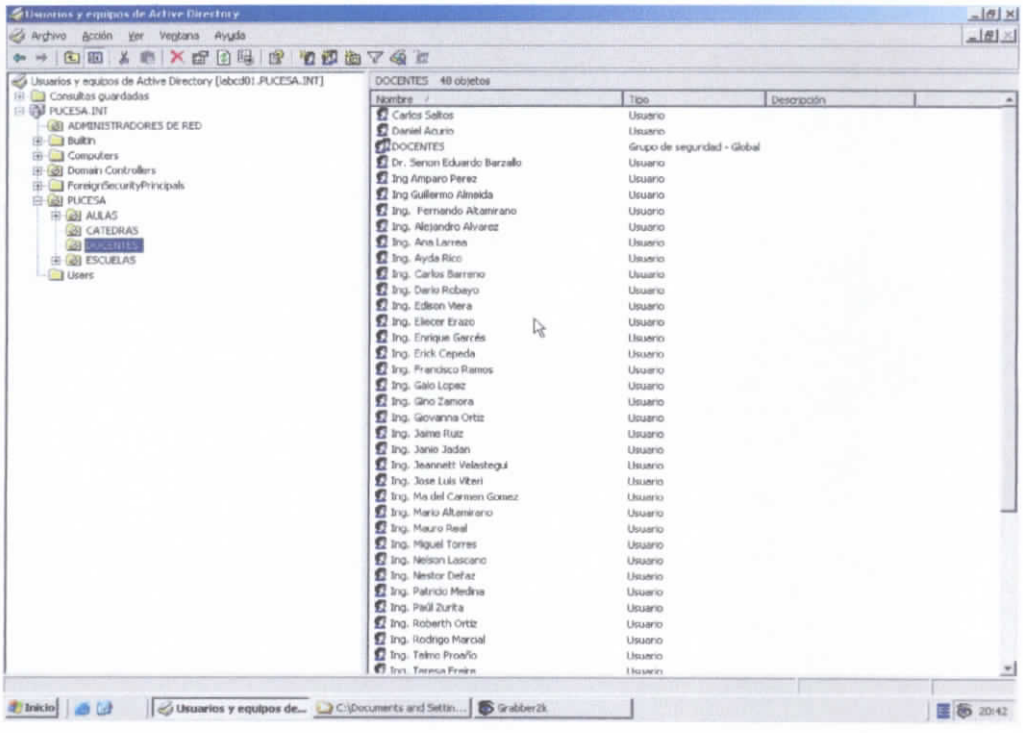


Figura 3-54 UO DOCENTES en Active Directory

- En la OU ESCUELAS se encuentran creadas los siguientes contenedores: COMERCIAL, DISENO, LENGUAS, OPTOMETRÍA, PSICOLOGÍA Y SISTEMAS (figura 3-55 y 3-56).

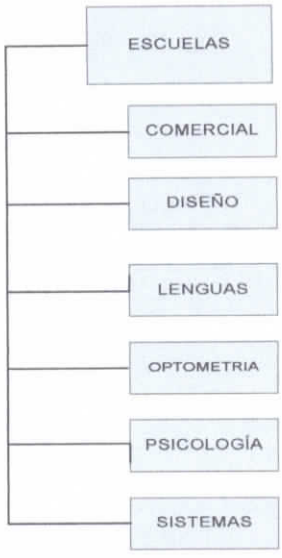


Figura 3-55 UO ESCUELAS

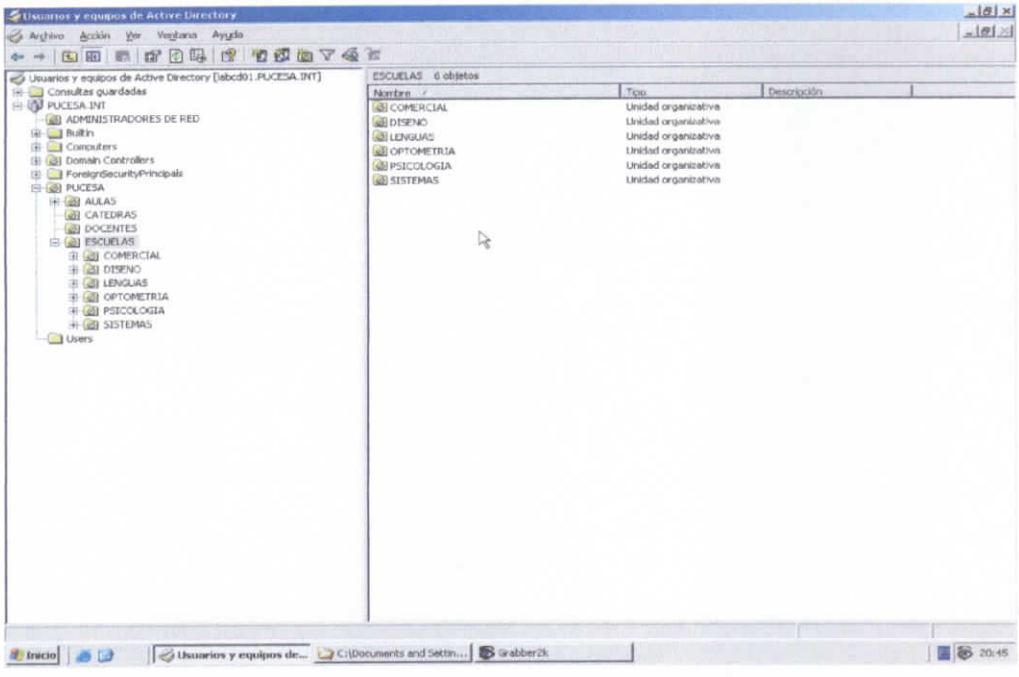


Figura 3-56 UO ESCUELAS en Active Directory

- En cada una de las Escuelas se creo dos contendedores, el primero ADMINISTRATIVOS y el segundo ESTUDIANTES dentro del mismo se encuentran los alumnos pertenecientes a esa UO (figura 3-57).

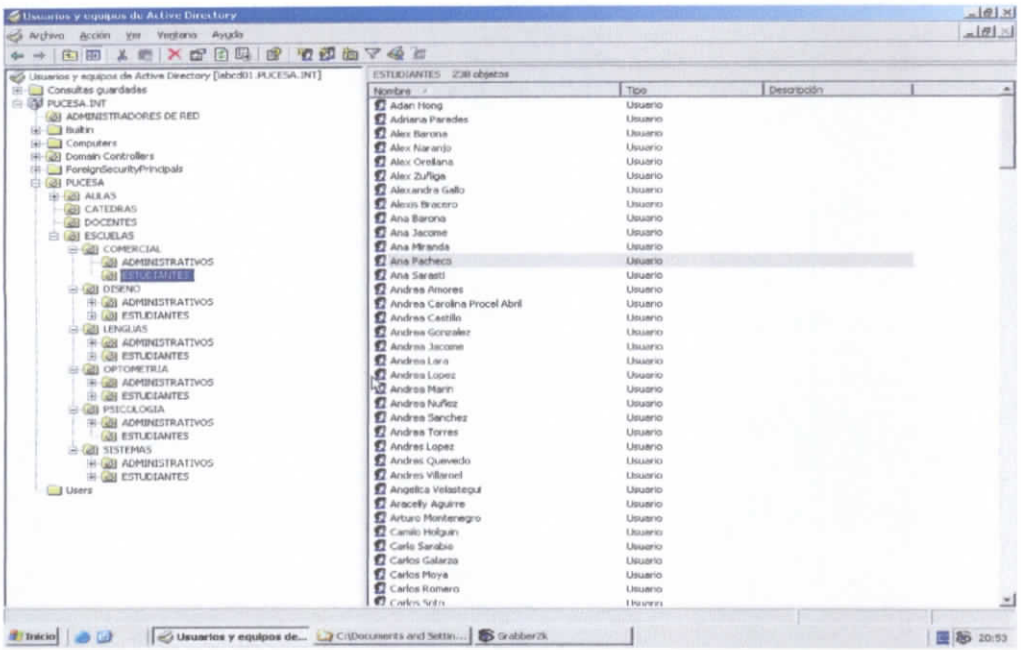


Figura 3-57 UO ADMINISTRATIVOS Y ESTUDIANTES

- En el mismo nivel de la Unidad Organizativa PUCESA, se encuentra ADMINISTRADORES DE RED (figura 3-58 y 3-59), en la misma están creados los usuarios con perfiles de administradores de Dominio.

Figura 3-58 UO ADMINISTRADORES DE RED

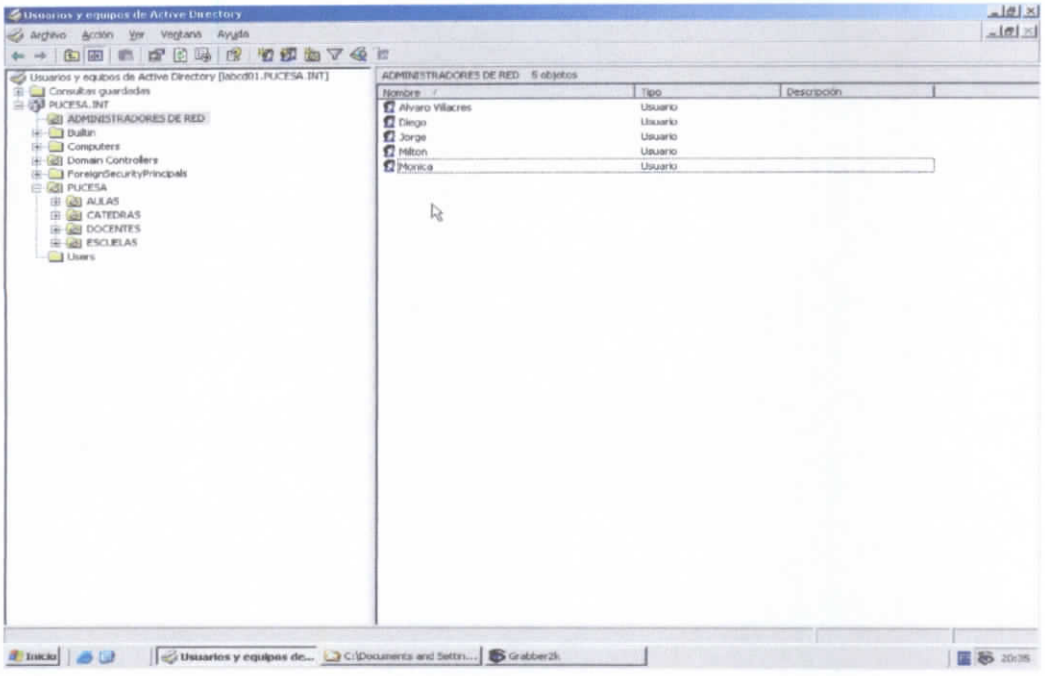


Figura 3-59 UO ADMINISTRADORES DE RED en Active Directory

3.7.2 Creación de Grupos

Para la creación de grupos seguir los siguientes pasos

- Ubicar la Unidad Organizativa en la que se creará el grupo requerido, clic DERECHO, clic en NUEVO y clic en GRUPO (figura 3-60).

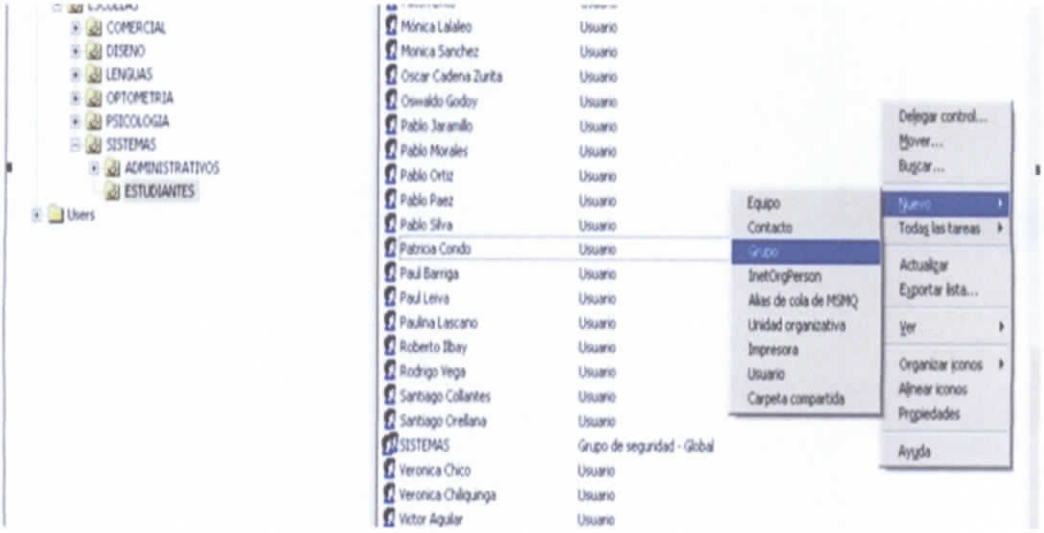


Figura 3-60 Creación de grupos

- Llenar el campo NOMBRE DE GRUPO, marcar el casillero que pertenece a GLOBAL y SEGURIDAD, clic en ACEPTAR (figura 3-61).

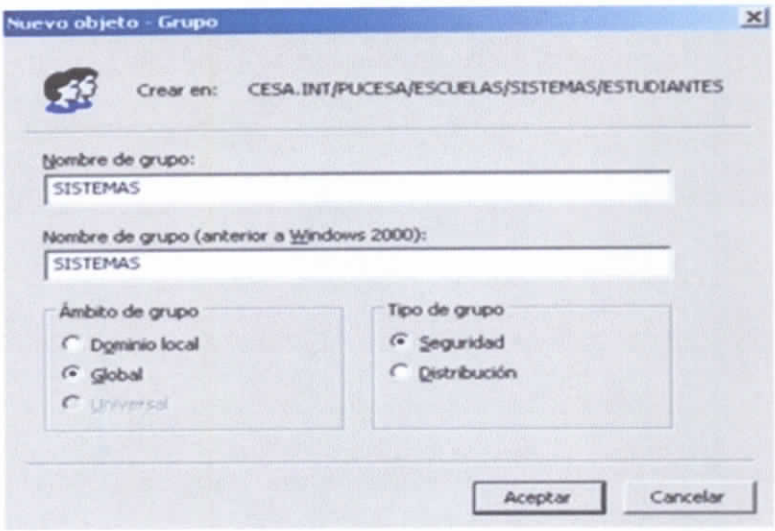


Figura 3-61 Nombre de grupo

- Para agregar usuarios al grupo requerido, ubicar el grupo solicitado, doble clic en grupo (figura 3-62).

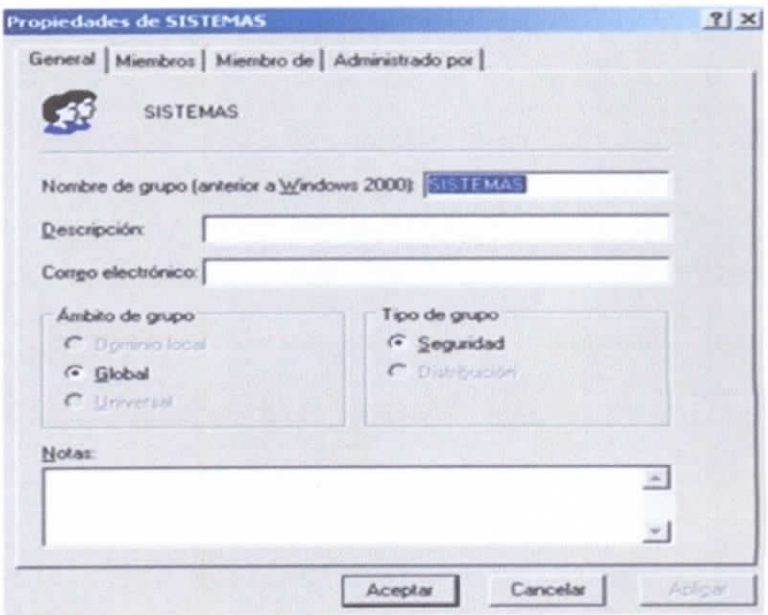


Figura 3-62 Propiedades del grupo

- Clic en la pestaña MIEMBROS (figura 3-63).

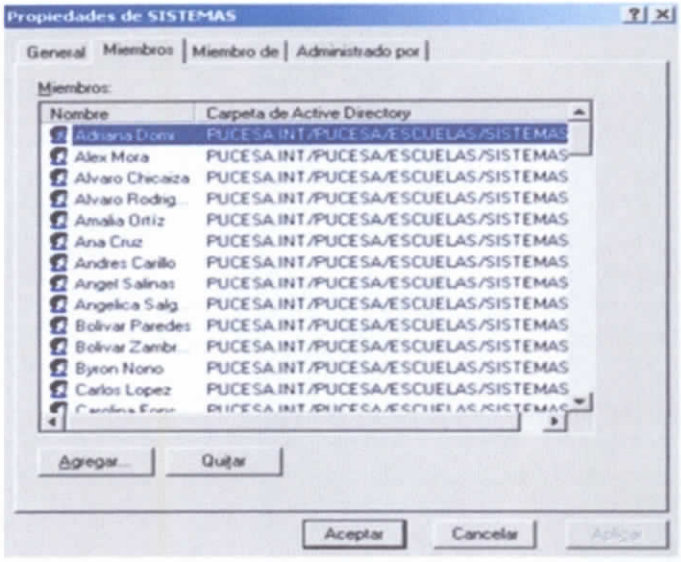


Figura 3-63 Miembros del grupo

- Clic de AGREGAR, para reconocer el usuario a agregar digitar parte o todo el nombre de inicio de sesión de usuario o el nombre de usuario, clic en COMPROBAR NOMBRE, hecho esto, se desplegará una ventana de NOMBRES MÚLTIPLES ENCONTRADOS en la cual se encontrará una lista de posibles alternativas o solamente el usuario requerido, clic en el usuario y clic en ACEPTAR (figura 3-64).

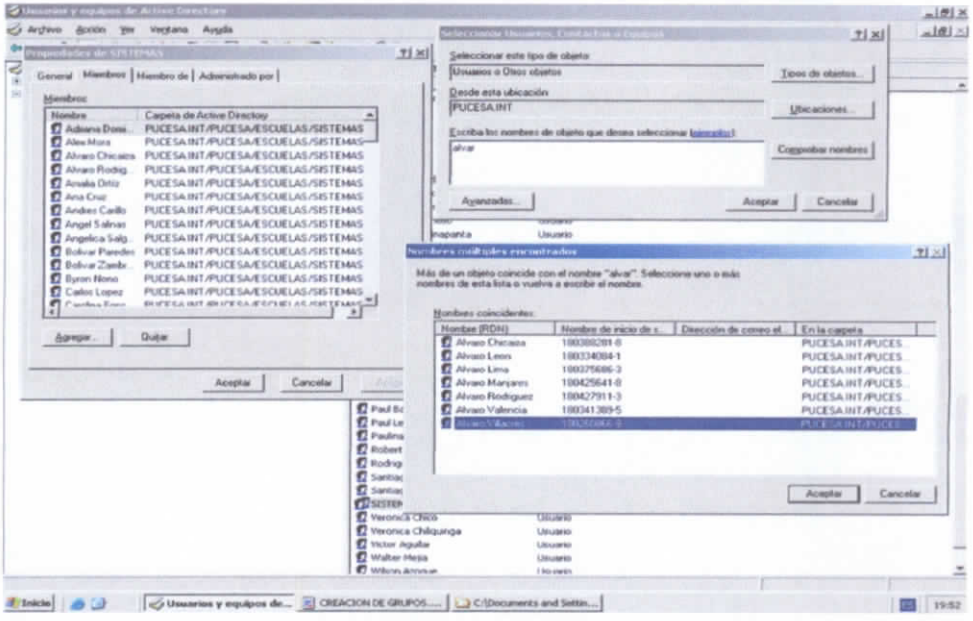


Figura 3-64 Agregar usuarios al grupo

- En la ventana de SELECCIONAR USUARIOS, CONTACTOS O EQUIPOS, se encontrará el usuario requerido ya reconocido y confirmar con clic en ACEPTAR (figura 3-65).

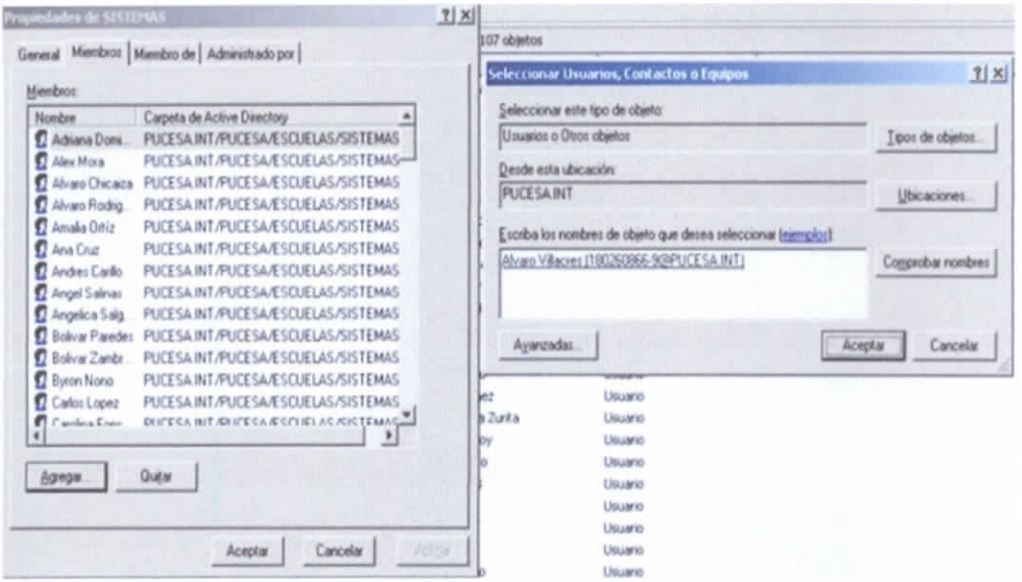


Figura 3-65 Seleccionar usuarios del grupo

- El usuario se encuentra agregado al grupo Clic en ACEPTAR (figura 3-66).

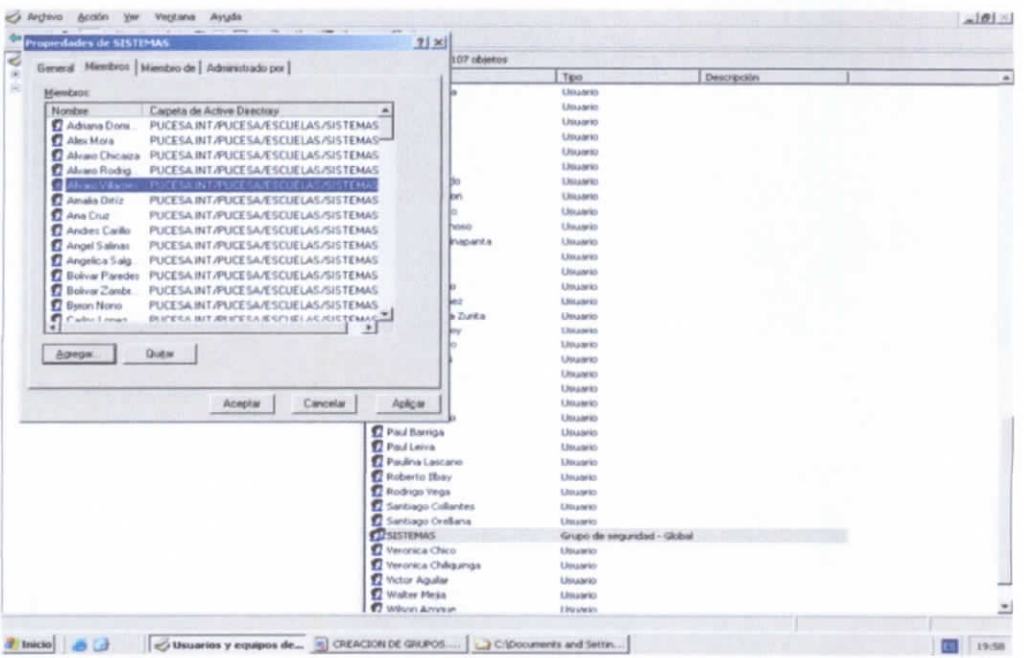


Figura 3-66 El usuario pertenece al grupo

3.7.3 Creación de Usuarios

Para la creación de usuarios seguir los siguientes pasos:

- Ubicar la Unidad Organizativa dentro de la cual se creará el usuario requerido, clic derecho, clic en NUEVO y clic en USUARIO (figura 3-67).

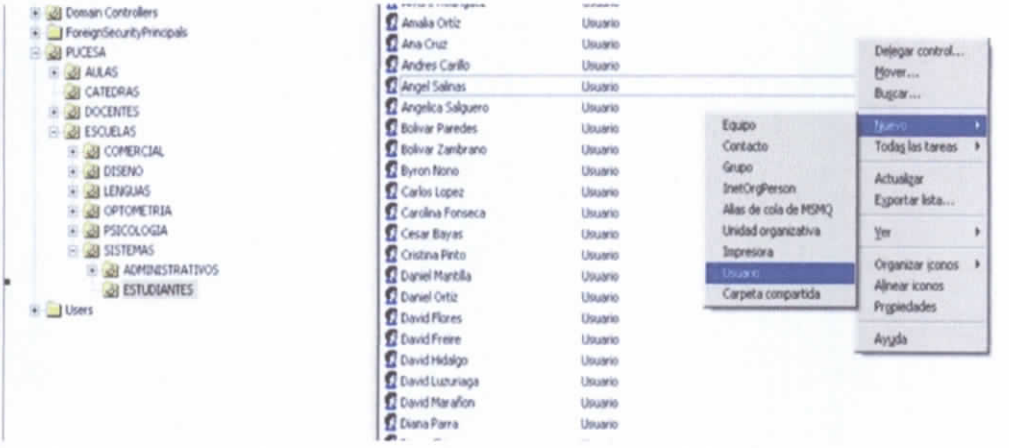


Figura 3-67 Creación de usuario

- La siguiente ventana muestra en que Unidad Organizativa se esta creando el usuario y solicita digitar todos los campos requeridos, tomar en cuenta la planificación realizada anteriormente para, el NOMBRE DE INICIO DE SESIÓN DE USUARIO Ej. 180260866-9, clic en SIGUIENTE (figura 3-68).

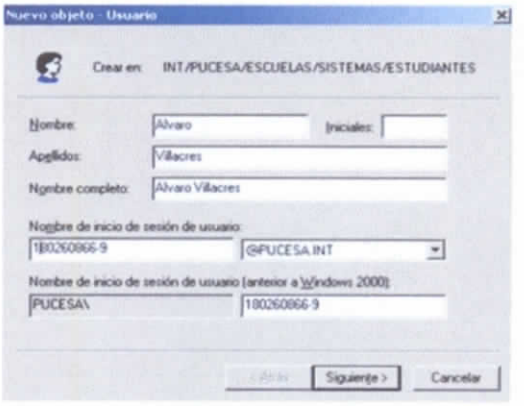


Figura 3-68 Información de nuevo usuario

- Digitar y confirmar la contraseña dispuesta para el usuario en cuestión, marcar el primer casillero EL USUARIO DEBE CAMBIAR LA CONTRASEÑA AL INICIAR UNA SESIÓN DE NUEVO lo anterior aplica solo a usuarios de Docentes y Estudiantes, clic en SIGUIENTE (figura 3-69). Creación de usuario finalizada.

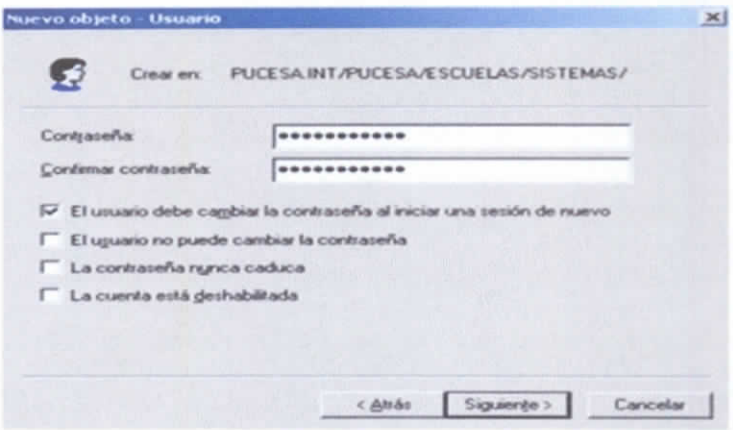


Figura 3-69 Contraseña del usuario

3.7.3.1 Configuración adicional de usuarios dentro del Dominio

- **Usuarios Estudiantes y Docentes:** En la creación de los mismos se estableció que la contraseña inicial debía ser igual al nombre de inicio de sesión de usuario, configurando para que el usuario cambie la contraseña en el primer inicio de sesión (figura 3-71).

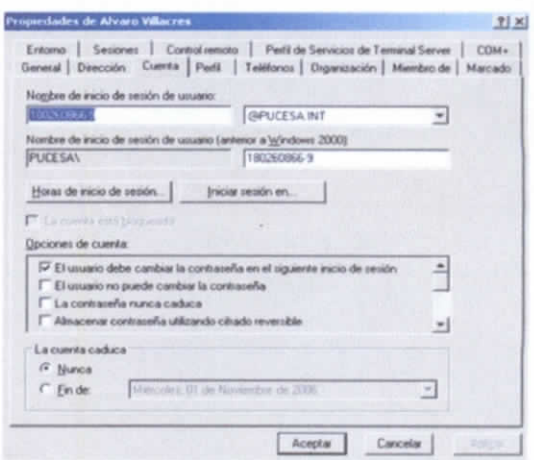


Figura 3-70 Usuarios estudiantes y docentes

Sin restricciones de horario (figura 3-71).

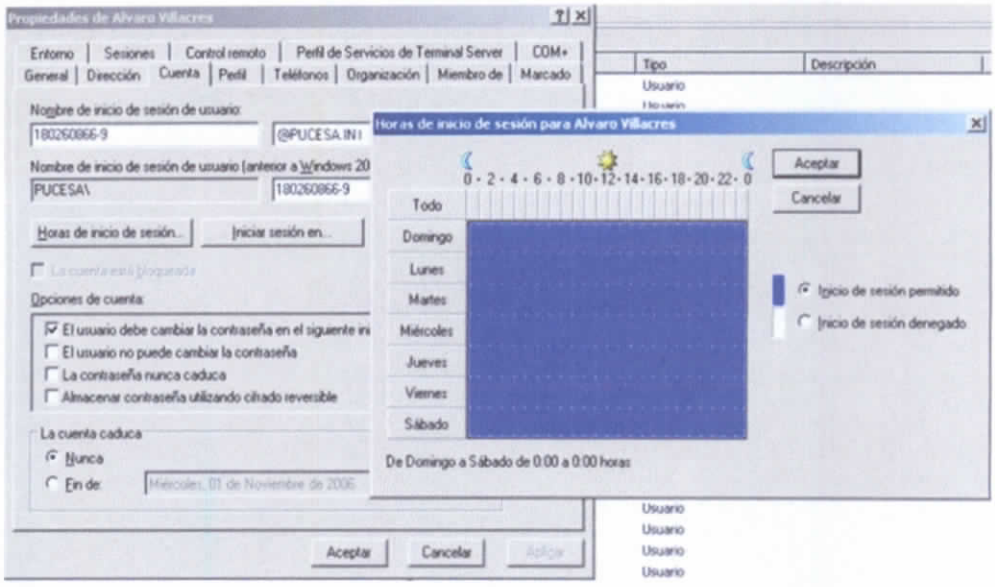


Figura 3-71 Configuración de restricción de horarios

- **Usuarios Cátedras:** En la creación de los mismos se estableció que la contraseña inicial debía ser igual al nombre de inicio de sesión de usuario, configurando que la contraseña nunca caduca y el usuario no puede cambiar la contraseña. Los usuarios de las cátedras están sujetos al horario de clases previamente definido (figura 3-72).

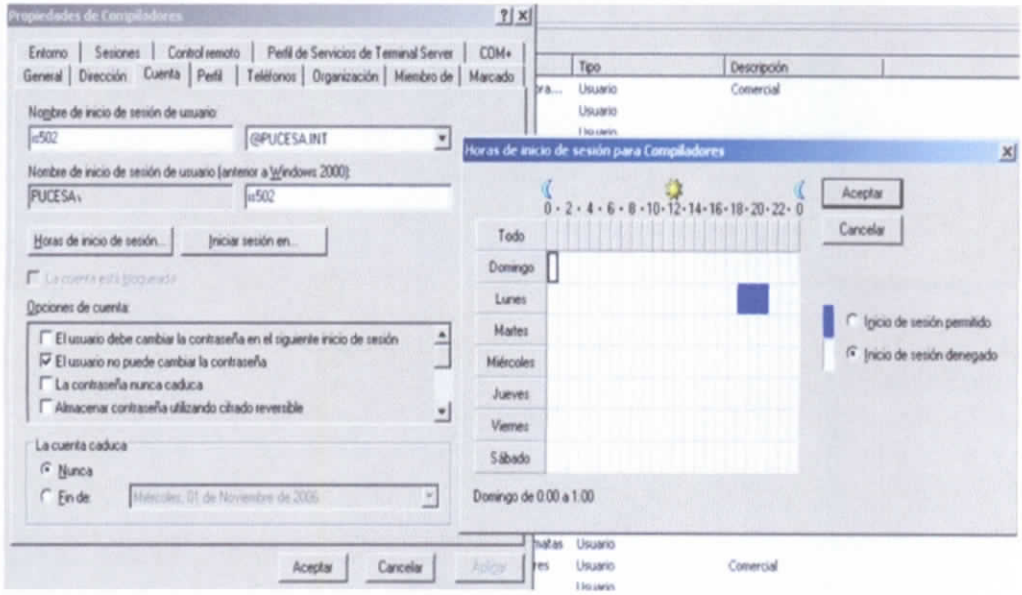


Figura 3-72 Usuarios cátedras

3.7.4 Creación de Directivas de Grupo

Las directivas de Grupo son herramientas que facilitan la administración de la red, que se aplican a los contenedores es decir a las Unidades Organizativas, afectándose a la configuración de usuarios y equipos independientemente que existan dentro de la misma UO.

Para crear Directiva de Grupo debemos seguir los siguientes pasos:

- Clic derecho en la UO requerida, clic en PROPIEDADES, clic en la pestaña DIRECTIVA DE GRUPO, clic en el botón NUEVO, escribir el nombre de la directiva, para dar la configuración solicitada a dicha directiva clic en EDITAR (figura 3-73).

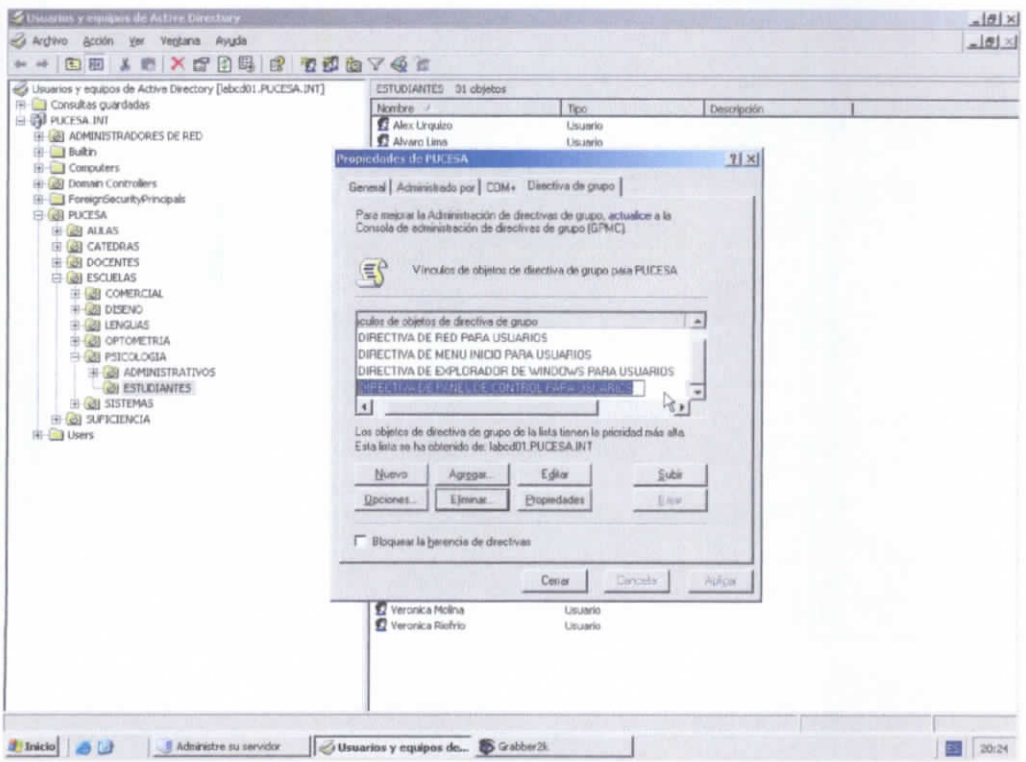


Figura 3-73 Directiva de grupo

- Realizar la configuración para afectar a los objetos que se encuentran dentro de la UO (figura 3-74)

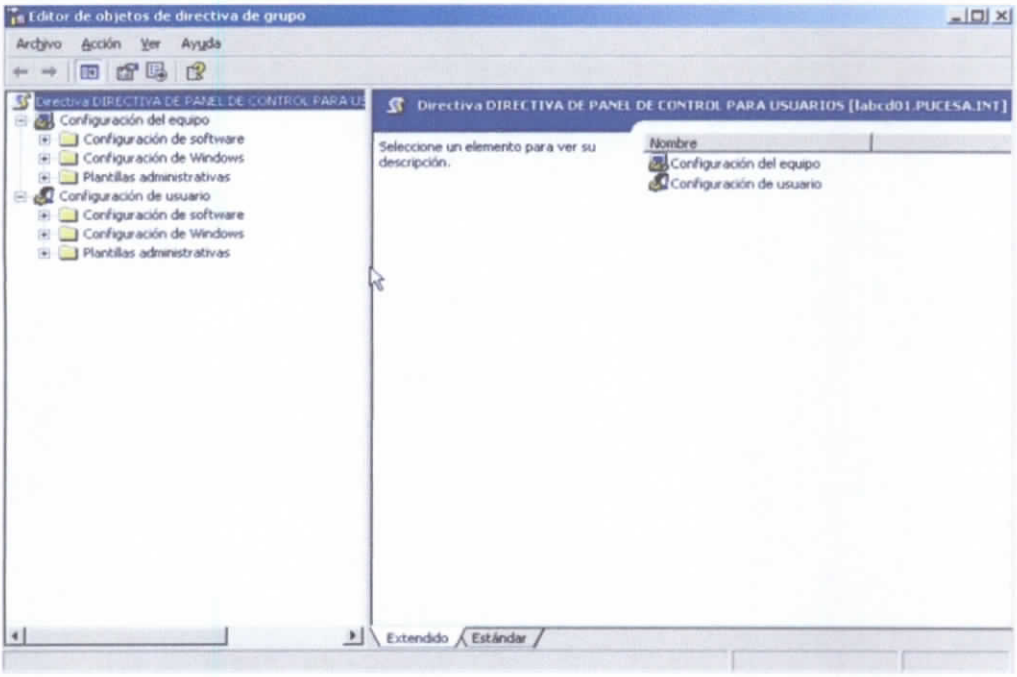


Figura 3-74 Configuración de directiva de grupo

3.7.4.1 Directivas de Grupo aplicadas a las Unidades Organizativas que conforman el Dominio

- Directivas aplicadas a la Unidad Organizativa PUCESA:

Nombre de la Directiva de Grupo: POLITICA GENERAL PARA TODOS LOS USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Configuración de Windows\Mantenimiento de Internet Explorer\Direcciones URL\Direcciones URL Importantes\Dirección URL de la página principal	http://www.google.com	Define la pagina web que se mostrara al iniciar el Internet Explorer
Configuración de Usuario\Configuración de Windows\Mantenimiento de Internet Explorer\Conexion\Configuración de los servidores Proxy\Habilitar Configuración proxy	192.168.2.200 3128	Configura la Dirección IP del proxy y puerto, designado para el sevicio de internet
Configuración de Usuario\Plantillas administrativas\Componentes de Windows\Internet explorer\Panel de control de internet\Página de opciones avanzadas\Mostrar videos en paginas web	Deshabilitado	Prohibe la visualización de videos en paginas web
Configuración de Usuario\Plantillas administrativas\Componentes de Windows\Internet explorer\Deshabilitar la configuración de la página de Opciones avanzadas	Habilitado	Prohibe la manipulación de las opciones avanzadas en el Internet Explorer

Tabla 3-2 Directiva General para todos los usuarios OU PUCESA

Nombre de la Directiva de Grupo: DIRECTIVA DE RED PARA TODOS LOS USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Red\Conexiones de red\Prohibir la configuracion TCP\IP avanzada	Habilitado	No permite el ingreso y manipulación de la configuración TCP/IP
Configuración de Usuario\Plantillas administrativas\Red\Conexiones de red\Prohibir el acceso al Asistente para nueva conexión LAN	Habilitado	Deniega la creacion de nuevas conexiones LAN

Tabla 3-3 Directiva de Red para todos los Usuarios UO PUCESA

Nombre de la Directiva de Grupo: DIRECTIVA DE MENU INICIO PARA TODOS LOS USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Menú Inicio y barra de tareas\Quitar el menu Ejecutar del menu inicio	Habilitado	Oculta el programa "Ejecutar" del menú inicio
Configuración de Usuario\Plantillas administrativas\Menu Inicio y barra de tareas\Bloquear la barra de tareas	Habilitado	Bloquea la barra de tareas prohibiendo la manipulación

Tabla 3-4 Directiva de Menú Inicio para todos los usuarios UO PUCESA

Nombre de la Directiva de Grupo: DIRECTIVA DE EXPLORADOR DE WINDOWS PARA TODOS LOS USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Componentes de Windows\Explorador de Windows\Quitar el menú Opciones de carpeta del menú Herramientas	Habilitado	Oculta el Menú "Opciones de carpeta" del menú Herramientas
Configuración de Usuario\Plantillas administrativas\Componentes de Windows\Explorador de Windows\Oculta el elemento Administrar del menú contextual del Explirador	Habilitado	Oculta el elemento Administrar al hacer click derecho a mi PC

Tabla 3-5 Directiva de Explorador de Windows para todos los Usuarios UO PUCESA

Nombre de la Directiva de Grupo: DIRECTIVA DE PANEL DE CONTROL PARA TODOS LOS USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Panel de control\Prohibir el acceso al Panel de Control	Habilitado	Prohibe el acceso al Panel de Control
Configuración de Usuario\Plantillas administrativas\Panel de control\Pantalla\Impedir cambios en el papel tapíz	Habilitado	Prohibe el cambio de panel tapíz en el escritorio

Tabla 3-6 Directiva de Panel de Control para todos los Usuarios UO PUCESA

- Directivas aplicadas a la Unidad Organizativa AULAS:

Nombre de la Directiva de Grupo: DIRECTIVA GENERAL DE COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de cuenta\Directiva de contraseñas\Longitud mínima de la contraseña	5 caracteres	Establece la longitud mínima de la contraseña
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de cuenta\Directiva de contraseñas\Vigencia maxima de la contraseña	30 días	Vigencia máxima de la contraseña
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de cuenta\Directiva de contraseñas\Vigencia mínima de la contraseña	5 dias	Vigencia mínima de la contraseña
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Inicio de sesion interactivo: no mostrar el ultimo nombre de usuario	Habilitada	No muestra el ultimo usuario que iniciado en dicho equipo
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Inicio de sesion interactivo: no requerir Ctrl + Alt + Spr	Habilitada	Elimina la necesidad de ejecutar Ctrl + Alt +Spr, para iniciar sesión
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Inicio de sesion interactivo: pedir al usuario cambiar la contrasña antes de caducidad	10 días	Solicita al usuario al usuario cambiar la contrasña antes de caducidad
Configurción del equipo\Plantillas administrativas\Sistema\Restaurar sistema\Desactivar restaurar sistema	Habilitado	Deshabilita restaurar sistema para impedir configuraciones anteriores

Tabla 3-7 Directiva General de Computadores UO AULAS

- Directivas aplicadas a la Unidad Organizativa AULA2:

Nombre de la Directiva de Grupo: ACCESO A COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Denegar el inicio de sesion localmente	escoger los grupos: Comercial, Diseño, Lenguas, Optometria, Psicologia y Sistemas	Niega el acceso de los grupos de usuarios mencionados al aula 2

Tabla 3-8 Acceso Computadores UO AULA2

- Directivas aplicadas a la Unidad Organizativa AULA3:

Nombre de la Directiva de Grupo: ACCESO A COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Denegar el inicio de sesión localmente	Escoger los grupos: Comercial, Diseño, Lenguas, Optometria, Psicologia y Sistemas	Niega el acceso de los grupos de usuarios mencionados al aula 3

Tabla 3-9 Acceso Computadores UO AULA3

- Directivas aplicadas a la Unidad Organizativa AULA4:

Nombre de la Directiva de Grupo: ACCESO A COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Denegar el inicio de sesión localmente	Escoger los grupos: Comercial, Diseño, Lenguas, Optometria, Psicologia y Sistemas	Niega el acceso de los grupos de usuarios mencionados al aula 4

Tabla 3-10 Acceso Computadores UO AULA4

- Directivas aplicadas a la Unidad Organizativa AULA5:

Nombre de la Directiva de Grupo: ACCESO A COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Denegar el inicio de sesión localmente	Escoger los grupos: Comercial, Diseño, Lenguas, Optometria, Psicologia y Sistemas	Niega el acceso de los grupos de usuarios mencionados al aula 5

Tabla 3-11 Acceso a Computadores UO AULA5

- Directivas aplicadas a Unidad Organizativa AULA6:

Nombre de la Directiva de Grupo: ACCESO A COMPUTADORES		
PATH	**VALOR**	**OBJETIVO**
Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Denegar el inicio de sesión localmente	Escoger los grupos: Catedras	Niega el acceso de los grupos de usuarios mencionados al aula 6

Tabla 3-12 Acceso a Computadores UO AULA6

- Directivas aplicadas a la Unidad Organizativa CATEDRAS:

Nombre de la Directiva de Grupo: DIRECTIVA MENU DE INICIO PARA USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Menú inicio y barra de tareas\Quitar el menú Eejecutar del menú Inicio	Deshabilitado	Hace visible el programa "Ejecutar" del menú inicio

Tabla 3-13 Directiva Menú de Inicio para Usuarios UO CÁTEDRAS

Nombre de la Directiva de Grupo: DIRECTIVA DE PANEL DE CONTROL PARA USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Panel de Control\Prohibir el acceso al Panel de contol	Deshabilitado	Habilita el acceso al Panel de Control

Tabla 3-14 Directiva de Panel de Control para Usuarios UO CÁTEDRAS

- Directivas aplicadas a la Unidad Organizativa DOCENTES:

Nombre de la Directiva de Grupo: DIRECTIVA MENU DE INICIO PARA USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Menú inicio y barra de tareas\Quitar el menú Eejecutar del menú Inicio	Deshabilitado	Hace visible el programa "Ejecutar" del menú inicio

Tabla 3-15 Directiva Menú de Inicio para Usuarios UO DOCENTES

Nombre de la Directiva de Grupo: DIRECTIVA DE PANEL DE CONTROL PARA USUARIOS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuario\Plantillas administrativas\Panel de Control\Prohibir el acceso al Panel de contol	Deshabilitado	Habilita el acceso al Panel de Control

Tabla 3-16 Directiva de Panel de Control para Usuarios UO DOCENTES

- Directivas aplicadas a la Unidad Organizativa ESCUELAS:

Nombre de la Directiva de Grupo: DIRECTIVA HABILITACIÓN DE IMPRESORAS		
PATH	**VALOR**	**OBJETIVO**
Configuración de Usuarios\Plantillas administrativas\Panel de Control \Impresoras\Impedir la agregación de impresoras	Deshabilitado	Prohibe la instalación de impresoras

Tabla 3-17 Directiva Habilitación de Impresoras UO ESCUELAS

3.8 Validación de Equipos en el Dominio "PUCESA.INT"

Cada uno de los computadores en los laboratorios para formar parte de la red tiene que ser validados en el Dominio "PUCESA.INT". En el proceso cada uno de los equipos tomara un Dirección IP asignada por el servidor de Dominio.

Para unir un computador al Dominio seguir los siguientes pasos

- Ubicar las Propiedades de Protocolo Internet (TCP\IP), en la misma ventana marcar la alternativa OBTENER UNA DIRECCIÓN IP AUTOMÁTICAMENTE, y marcar la opción USAR LAS SIGUIENTES DIRECCIONES DE SERVIDORES DNS, digitando la dirección IP: 192.168.2.250. Se ha completado la configuración de red en el equipo cliente (figura 3-75).

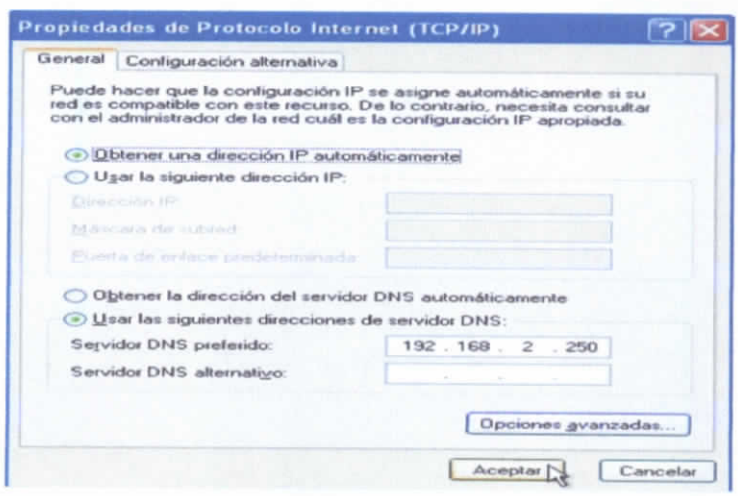


Figura 3-75 Propiedades de protocolo Internet (TCP/IP)

- Comprobar la dirección IP asignada mediante la herramienta "Símbolo del Sistema" utilizando el comando "ipconfig" (figura 3-76)

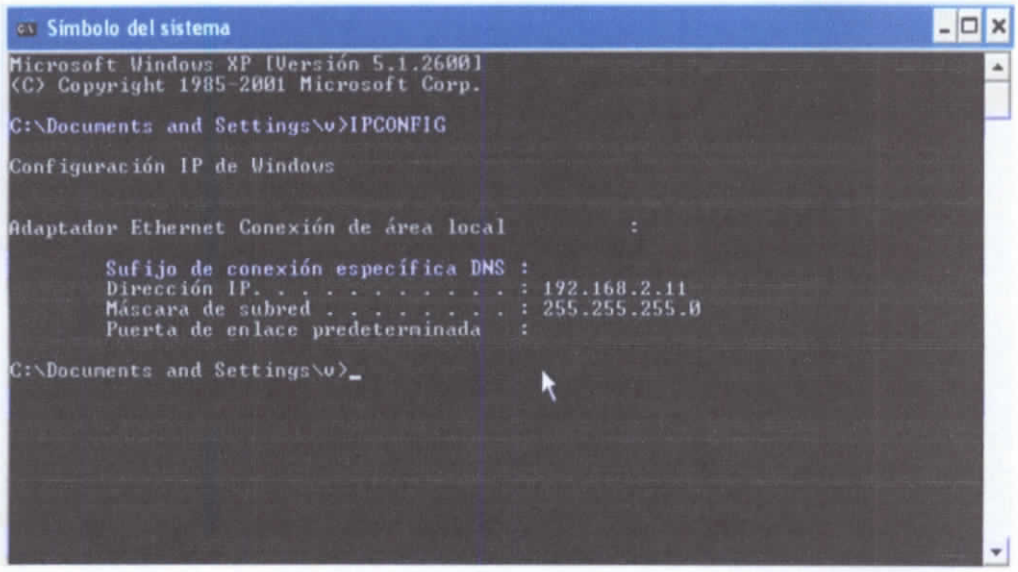


Figura 3-76 Comando ipconfig

- Clic derecho al icono de MI PC, clic en PROPIEDADES, escoger la pestaña NOMBRE DE EQUIPO y clic en el botón CAMBIAR (figura 3-77).

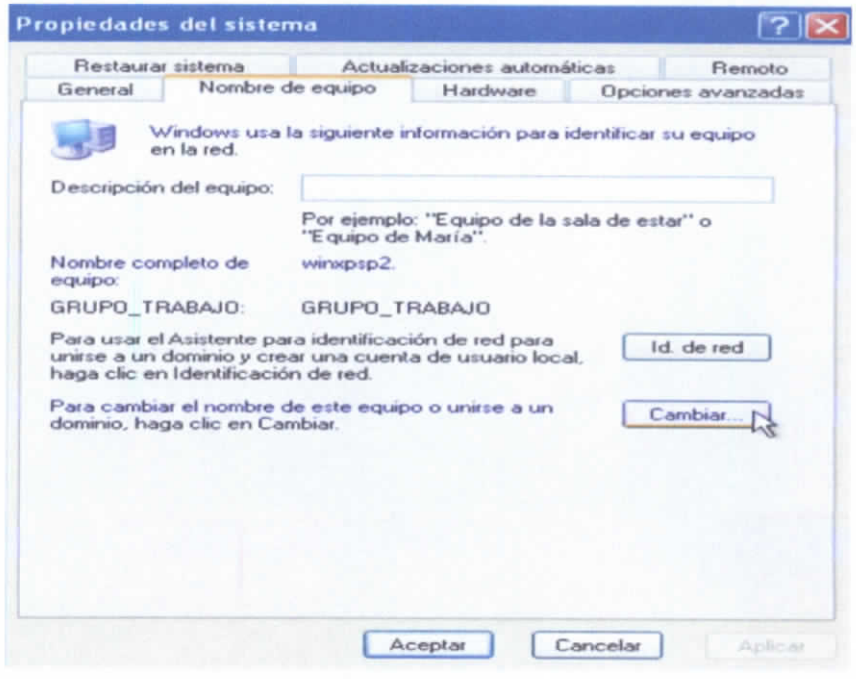


Figura 3-77 Propiedades del Sistema

- Escribir en el primer campo el nombre del equipo asignado, marcar la opción Dominio y escribir "PUCESA.INT", clic en MAS (figura 3-78).

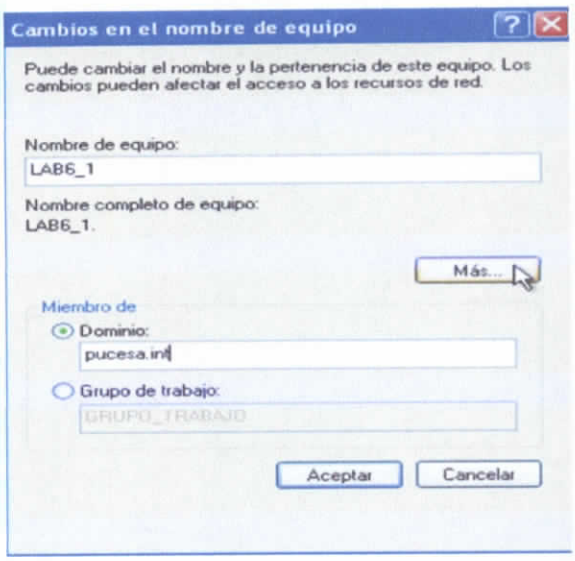


Figura 3-78 Nombre de Dominio

- En el único campo disponible digitar "PUCESA.INT", clic en ACEPTAR (figura 3-79).

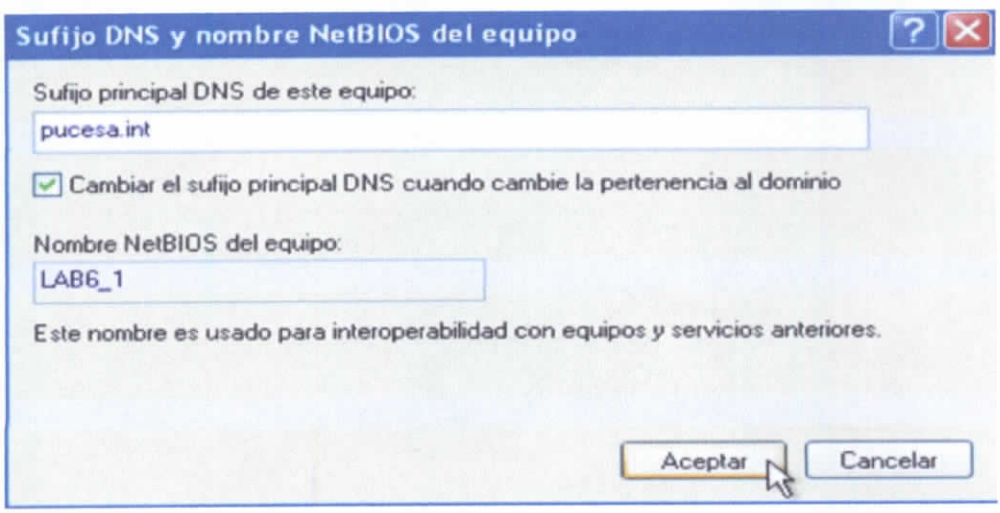


Figura 3-79 Sufijo DNS

- Clic en ACEPTAR (figura 3-80).

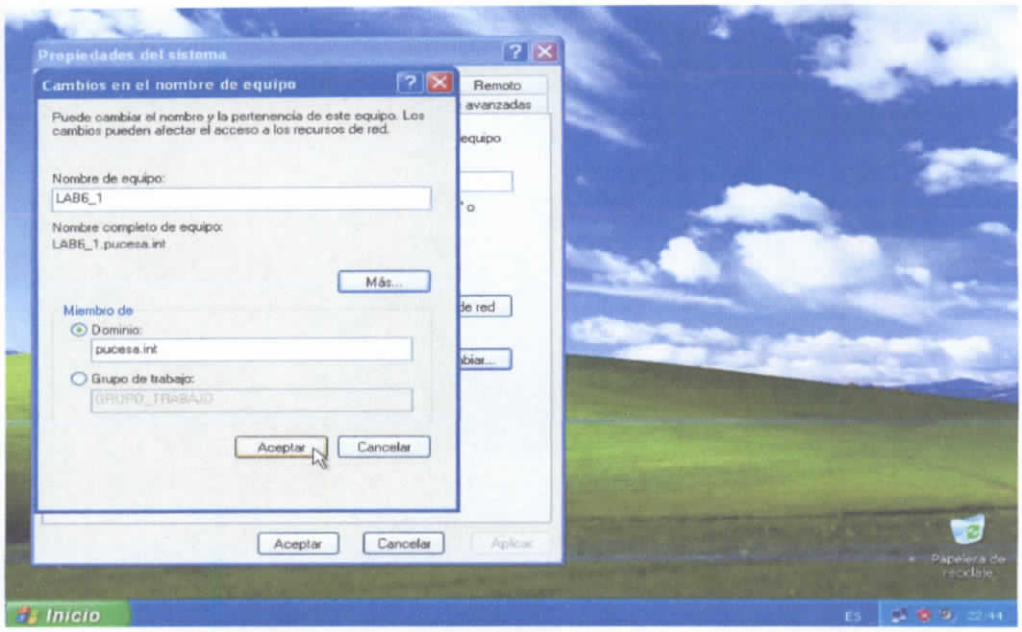


Figura 3-80 Confirmación de cambio de nombre de equipo

- Los nombres de los computadores contienen un carácter no estándar "_" por tal motivo se despliega una alerta, clic en SI (figura 3-81).

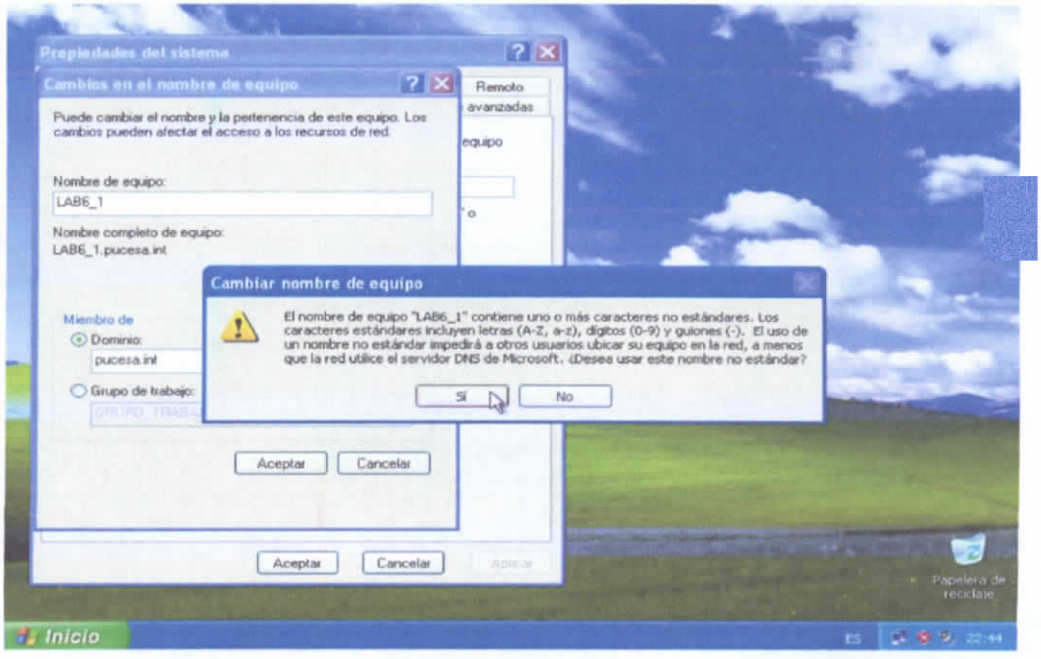


Figura 3-81 Confirmación de alerta

- En la siguiente ventana digitar el usuario "administrador" o algún usuario con perfil de administrador de Dominio con su correspondiente contraseña, para poder hacer efectiva la validación (figura 3-82). Aceptar las ventanas restantes de validación y por último reiniciar el equipo.

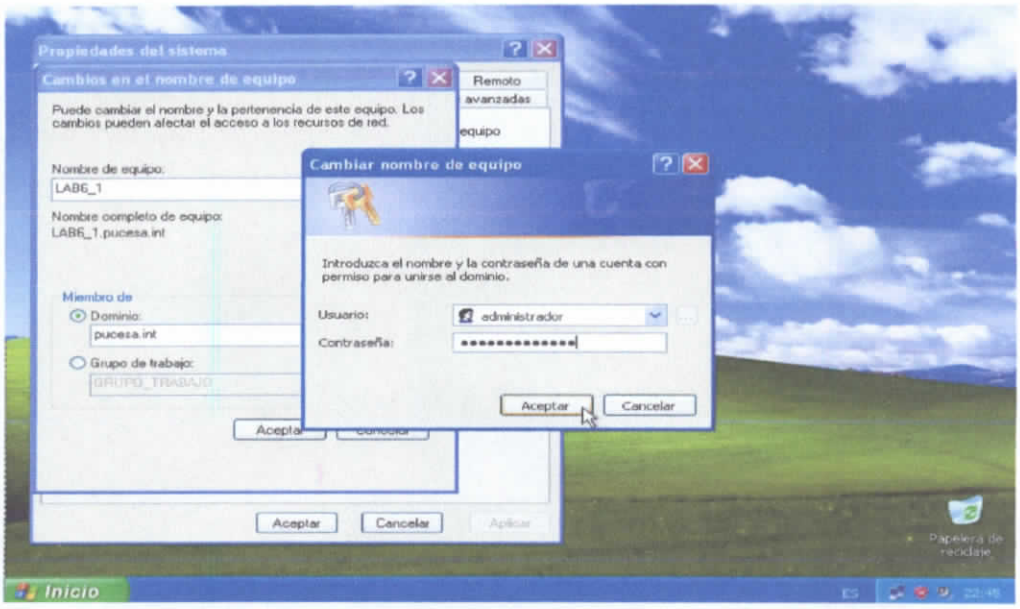


Figura 3-82 Confirmar usuario y contraseña

- Todos los computadores que ejecuten el proceso anterior ocuparán un registro en el Dominio PUCESA.INT.

  En la ZONA DE BÚSQUEDA DIRECTA perteneciente al DNS, cada equipo se registrará obteniendo como resultado (figura 3-83):

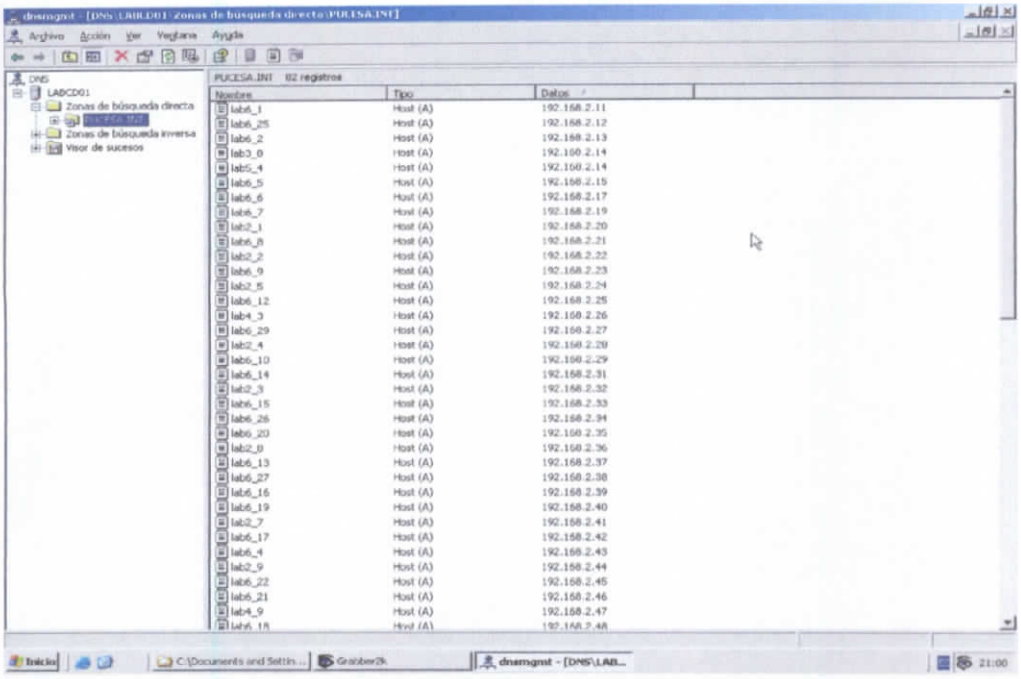


Figura 3-83 Equipos registrados en la zona de búsqueda directa

- De igual forma se creara el registro para cada computador en la ZONA DE BÚSQUEDA INVERSA perteneciente al DNS (figura 3-84).

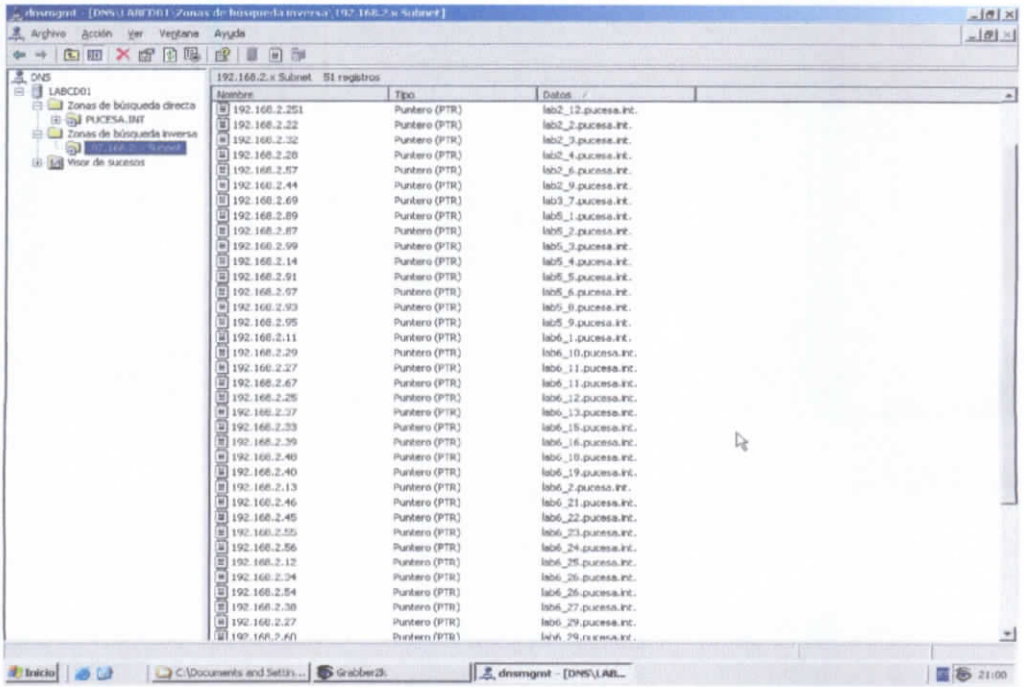


Figura 3-84 Equipos registrados en la zona de búsqueda inversa

- En cada validación de equipo, el protocolo de DHCP, hará una concesión designando una dirección IP, y cada una de estas, se registrará en la Herramienta Administrativa DHCP, obteniendo como resultado lo siguiente (figura 3-85).

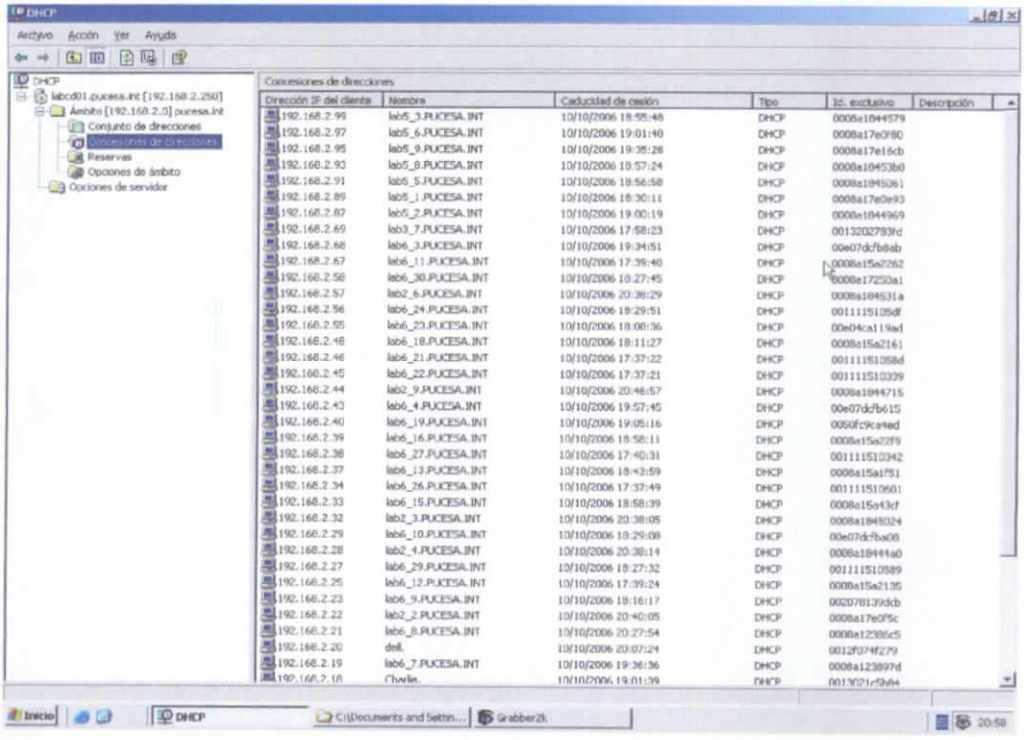


Figura 3-85 Concesión de direcciones IP

3.9 Capacitación y Seguridad

3.9.1 Capacitación al personal del Centro de Cómputo de la PUCESA

- La capacitación se realizó el día Jueves 21 de Septiembre .
- Dirigido al Personal de Cómputo de la PUCESA, directamente al Ing. Diego Santa Cruz y al Ing. Milton Jerez.
- Se realizo en el Laboratorio 6 específicamente en los equipos LAB6_3, LAB6_4 y el servidor LABCD01.
- En la capacitación se contó con la presencia de la Directora de Tesis la Ing. Verónica Pailiacho.

- Cabe recalcar que se ha llevado una constante capacitación, puesto que se han realizado continuas supervisiones del funcionamiento del Controlador de Dominio por parte del grupo ejecutor de Tesis.

3.9.2 Copia de Seguridad

La copia de seguridad no es otra cosa que el respaldo de todo el sistema del Windows Server 2003 esto incluye el Controlador de Dominio (ESTADO DEL SISTEMA). Para realizar dicho proceso se debe seguir los siguientes pasos:

- Localizar TODOS LOS PROGRAMAS – ACCESORIOS – HERRAMIENTAS DEL SISTEMA, clic en COPIA DE SEGURIDAD (figura 3-86).

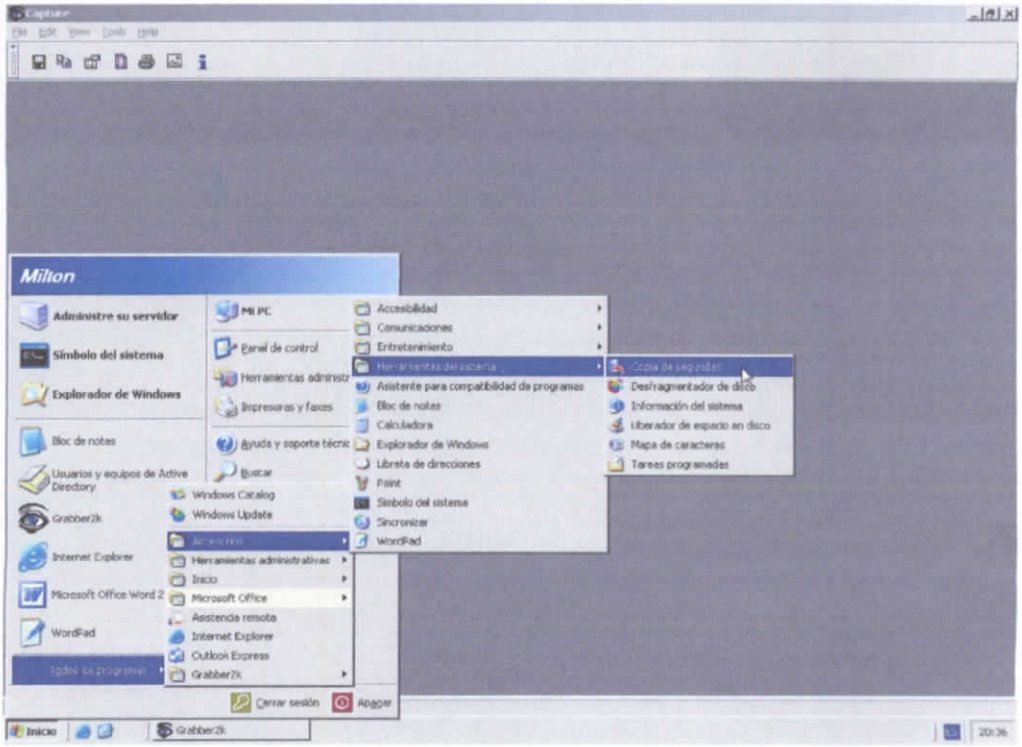


Figura 3-86 Copia de seguridad

- Se desplegará el Asistente para copia de seguridad o restauración, clic en SIGUIENTE (figura 3-87).

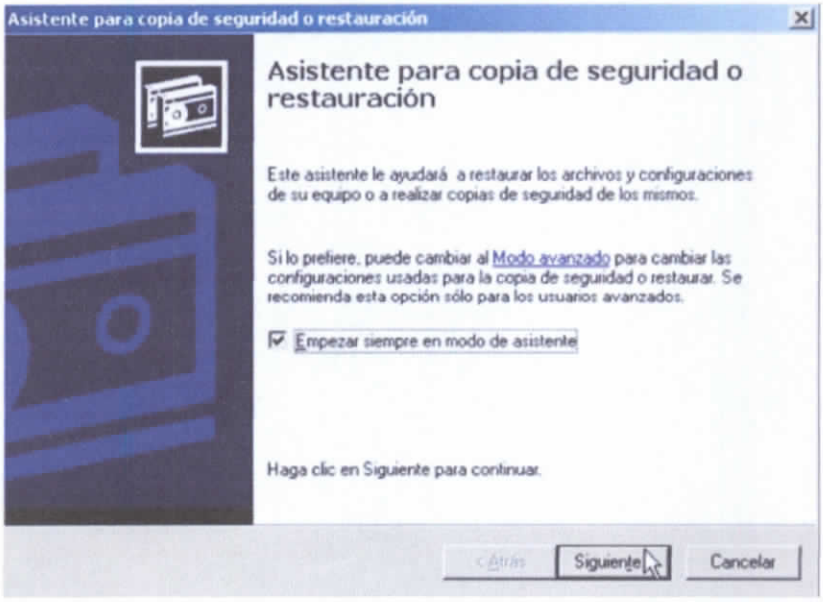


Figura 3-87 Asistente para copia de seguridad

- Marcar la opción EFECTUAR UNA COPIA DE SEGURIDAD DE ARCHIVOS Y CONFIGURACIÓN, clic en SIGUIENTE (figura 3-88).

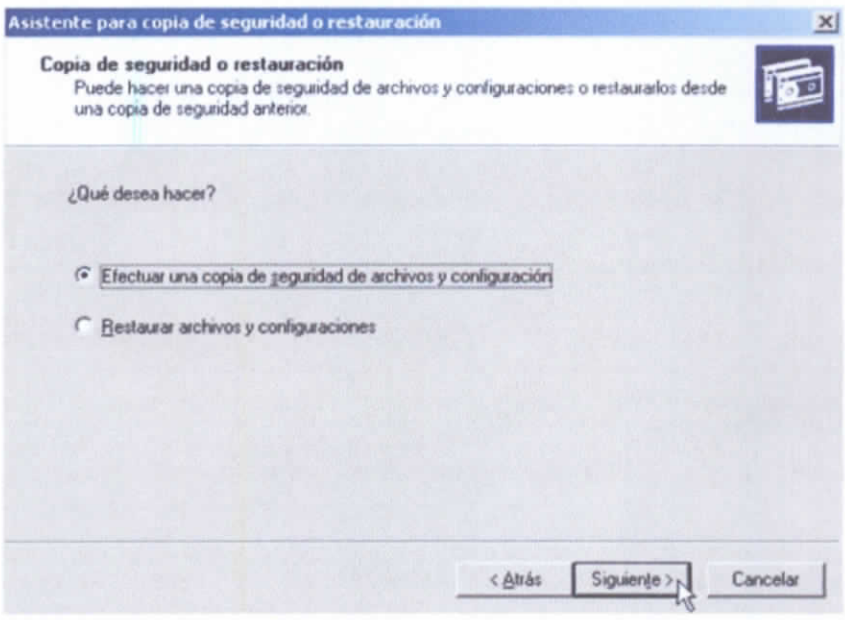


Figura 3-88 Ejecutar una copia de seguridad

- Escoger la segunda alternativa ELEGIR LO QUE DESEO INCLUIR EN LA COPIA DE SEGURIDAD, clic en SIGUIENTE (figura 3-89).

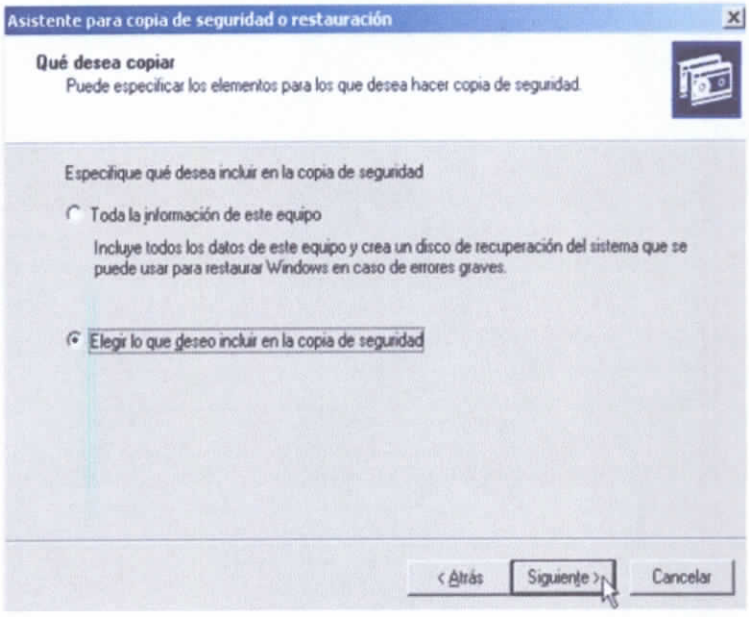


Figura 3-89 Elegir lo que se desea respaldar

- Para elegir el elemento que se desea incluir en la copia de seguridad, dar clic en el casillero que pertenece a SYSTEM STATE, clic en SIGUIENTE (figura 3-90).

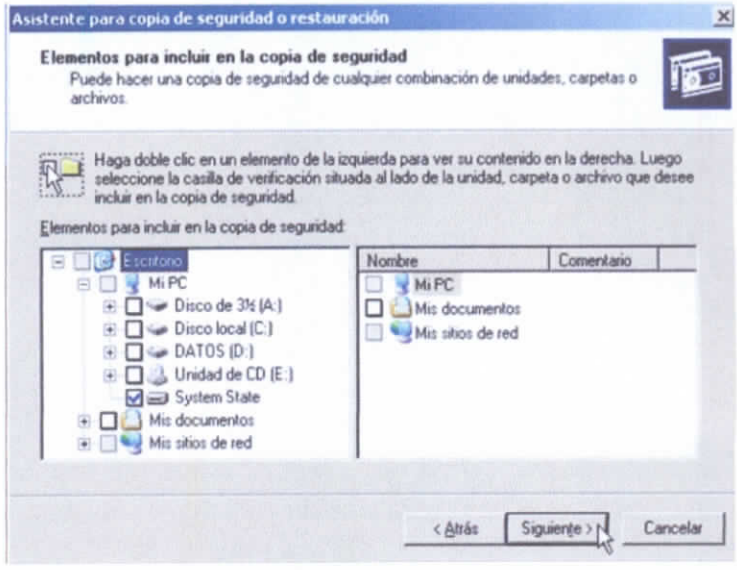


Figura 3-90 Escoger System State

- Clic en examinar para asignar la ubicación donde estará alojado el archivo que se obtendrá como resultado de este proceso, escribir el nombre que tendrá el archivo, clic en SIGUIENTE (figura 3-91). Posterior a esto finalizar el asistente para copia de seguridad o restauración.

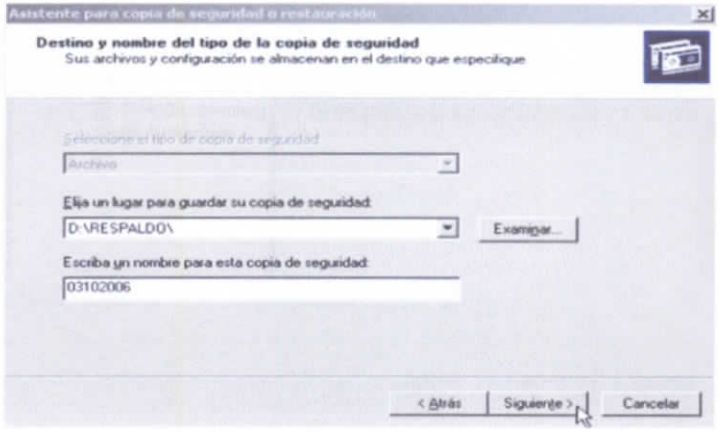


Figura 3-91 Destino y nombre de la copia de seguridad

Con la copia de seguridad se podrá realizar el proceso de restauración tomando en cuenta, que dicho proceso hay que hacerlo en el mismo servidor. Para realizar la restauración de seguridad, seguir los siguientes pasos

- Ejecutar el asistente para copia de seguridad o restauración. Marcar la segunda opción RESTAURAR ARCHIVOS Y CONFIGURACIONES, clic en SIGUIENTE (figura 3-92).

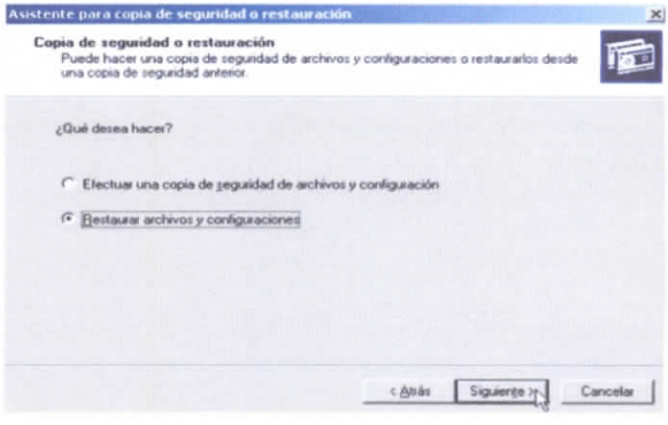


Figura 3-92 Escoger restaurar archivos y configuraciones

CAPÍTULO IV

4. VERIFICACIÓN Y VALIDACIÓN DE RESULTADOS

4.1 Verificación de la Hipótesis

Luego de la implementación de un Controlador de Dominio basado en la plataforma Windows 2003 Server en la PUCESA en el periodo 2006-2007 se obtendrá una mejora en el control y administración de los recursos de red satisfaciendo las necesidades del centro de cómputo.

Se demuestra la hipótesis mediante el método lógico Modus Ponendo Ponens.

A = Variable Independiente
B = Variable Dependiente
A = Implementación de un Controlador de Dominio
B = Mejora en el control y administración de los recursos de red

$$\begin{array}{l} A \rightarrow B \\ A \\ \hline B \end{array}$$

Esto quiere decir que:

Al implementar un Controlador de Dominio en la Pontificia Universidad Católica del Ecuador Sede Ambato, se está contribuyendo a la mejora de control y administración de recursos de red, con la que podrán contar el personal del Centro de Cómputo.

4.2 Validación de Resultados

La validación de este proyecto, se realizó el día 25 de Septiembre, al inicio de clases en el periodo Septiembre 2006 – Febrero 2007 de la PUCESA.

Los certificados fueron emitidos por las siguientes personas, quienes validaron el proyecto.

Ing. Santiago Acurio	ver anexos
Ing. Diego Santacruz	ver anexos

4.3 Conclusiones

- Al implementar un Controlador de Dominio basado en la plataforma Windows 2003 Server en la PUCESA en el periodo 2006 – 2007, se hizo un cambio tecnológico muy importante por el ambiente cliente-servidor que se mantiene en la actualidad.
- El Servidor HP ProLiant ML 150 G2, que fue escogido para la implementación del proyecto, aseguró el buen funcionamiento del Controlador de Dominio.
- Mediante la creación de Grupos y Unidades Organizativas se mantiene un esquema organizacional que ayuda a la administración para el acceso a recursos compartidos de la red.
- Con la creación de cuentas de usuario y equipos según las necesidades del centro de cómputo, se logró tener un control de identificación mediante la autenticación de usuarios en los computadores.
- El servicio de DHCP permitió evitar y reducir los errores de configuración que se producen generalmente por la necesidad de escribir los valores de configuración manualmente en cada equipo.

- Aplicando las Políticas de Seguridad propuestas, se protege en gran medida la configuración de usuario y computadores en los laboratorios de la PUCESA.

4.4 Recomendaciones

- Respaldar una vez al mes el "Estado del Sistemas" por motivos de seguridad, en caso de desastre.
- Utilizar un Firewall para mejorar la seguridad de la red interna contra Internet, y llevar el control de acceso, permisos, tiempos para la utilización de Internet por parte de los usuarios.
- Llevar un esquema de software de distribución para actualizaciones en plataforma Microsoft y Antivirus.
- Contar con un sistema de UPS, capaz de abastecer de energía eléctrica a los equipos importantes del centro de cómputo en caso de corte de luz y que tenga la función de regulador de voltaje para asegurar el buen funcionamiento de los equipos.

ANEXOS

BIBLIOGRAFÍA

LIBROS:

- SYNGRES
    - MCSA/MCSE : Administrando un ambiente Windows Server 2003
    - MCSA/MCSE : Implementando y administrando una infraestructura de red en Windows Server 2003
    - MCSA/MCSE : Planificando y administrando una infraestructura de red en Windows Server 2003
    - MCSA/MCSE: Planificando, Implementando y administrando una infraestructura de Directorio Activo.
- MICROSOFT ENTRENAMIENTO Y CERTIFICACIÓN
    - Curso NT1561: Revisión del servicio de Directorio Activo Windows 2000
    - Curso 2274: Administrando un ambiente Microsoft Windows Server 2003
    - Curso 2275: Administrando un ambiente Windows Server 2003
    - Curso 2276: Implementando una infraestructura de red Microsoft Windows Server 2003: red de hosts
    - Curso 2277: Implementando, administrando y manteniendo una infraestructura de red Microsoft Windows Server 2003
    - Curso 2278: Planificando y manteniendo una infraestructura de red Microsoft Windows Server 2003
    - Curso 2279: Planificando, implementando y manteniendo un infraestructura de Directorio Activo Microsoft Windows Server 2003.

INTERNET

- http://www.syngres.com
- http://www.microsoft.com
- http://technet2.microsoft.com
- http://technet2.microsoft.com/WindowsServer/en/Library/4af3271a-4407-4ca5-9cd5-e05b79046d081033.mspx
- http://www.abcdatos.com/tutoriales/tutorial/o470.html
- http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/domcntrl.mspx

GLOSARIO DE TÉRMINOS

ARP: Address Resolution Protocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware que corresponde a una determinada dirección IP.

AD: Acitve Direcrtory, es el nombre que micrososft refiere como la seguridad de una red distribuida de computadores.

DNS: Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

DCHP: Es un protocolo de red que permite a los equipos de una red, obtener la dirección IP automáticamente.

Ethernet: Es el nombre de una tecnología de redes de computadoras de área local basada en tramas de datos.

Frame Relay: Es un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor.

Ftp: File Transfer Protocol (Protocolo de Transferencia de Ficheros) es el ideal para transferir grandes bloques de datos por la red.

Gpmc: Nueva herramienta de administración para manejar la Política de grupo:. Conjunto de objetos utilizables en las secuencias de comandos.

GPO: Group Policy Object, Directivas de Grupo.

http: Hyper Text Transfer Protocol, es el protocolo usado en cada transacción de la Web (WWW).

IP: Protocolo de Internet no orientado a conexión usado tanto por el origen como el destino.

ICMP: Internet Control Message Protocol es el subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP).

Ipconfig: El comando de red ipconfig nos permite ver la dirección IP, la máscara de red y la puerta de enlace que están asignados a nuestra tarjeta de red, este comando solo está disponible en sistemas Microsoft Windows.

Nslookup: Comando que ayuda a la comprobación del correcto funcionamiento dns.

NetBios: Engloba un conjunto de protocolos de nivel de sesión.

OSI: Open System Interconection, lanzado en 1984 fue el modelo de red descriptivo creado por ISO.

OU: Unidad Organizativa, son contenedores de objetos pertenecientes a Active Directory.

P2P: Se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red.

Ping: Se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco.

Ram: Memoria de acceso aleatorio. Es una memoria en la que se puede tanto leer como escribir información.

RCP: Copia archivos entre una computadora y un sistema rshd, servicio remoto shell (demonio).

Router: Es un dispositivo hardware o software de interconexión de redes de computadoras.

RTP: Real-time Transport Protocol ,Protocolo de Transporte de Tiempo real.

Snmp: El Protocolo Simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SMTP: Simple Mail Transfer Protocol, o protocolo simple de transferencia de correo electrónico.

SID: Los identificadores de seguridad, son valores numéricos que identifican usuarios o grupos.

Tracert: Traceroute es una herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host (punto de red) a otro.

TCP/IP: Protocolo de control de transmisión / Protocolo de Internet, permite la transmisión de datos entre redes.

Telnet: es el nombre de un protocolo que sirve para acceder mediante una red a otra máquina.

Tftp: Trivial File Transfer Protocol a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red.

TTL: Tiempo de vida de un paquete en la red.

UDP: User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas.

Unix: Es un sistema operativo portable, multitarea y multiusuario.

Wins: Windows Internet Naming Service es un servidor de nombres de Microsoft para NetBIOS.

Ambato, 25 de Enero de 2007

Ingeniero
Telmo Viteri
DIRECTOR ESCUELA DE SISTEMAS PUCESA
Presente

De mi consideración:

Por la presente tengo a bien informarle que se ha procedido a la validación del trabajo de disertación del señor: Álvaro Fabián Villacrés Barrera, titulado: "Implementación de un Controlador de Dominio basado en la plataforma Windows 2003 Server en la Pontificia Universidad Católica del Ecuador Sede Ambato en el periodo 2006-2007", el mismo que se encuentra concluido y presta servicio en el Centro de Cómputo de la PUCESA.

Atentamente,

Ing. Diego Santacruz Abril
Administrador Centro de Cómputo
Pucesa

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUTO

PONTIFICIA
UNIVERSIDAD
CATOLICA
DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPU
BIBLIOTECA VIRTU
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telef: 593 3 2416 220
Telefax: 593 3 2411 868 ext. 10
webmaster@pucesa.edu.ec
Ambato - Ecuador
www.pucesa.edu.ec

Ambato, 25 de Enero de 2007

Ingeniero
Telmo Viteri
DIRECTOR ESCUELA DE SISTEMAS PUCESA
Presente

De mi consideración:

Por la presente tengo a bien informarle que se ha procedido a la validación del trabajo de disertación del señor: Nelson Eduardo Cortez Garzón, titulado: "Implementación de un Controlador de Dominio basado en la plataforma Windows 2003 Server en la Pontificia Universidad Católica del Ecuador Sede Ambato en el periodo 2006-2007", el mismo que se encuentra concluido y presta servicio en el Centro de Cómputo de la PUCESA.

Atentamente,

Ing. Diego Santacruz Abril
Administrador Centro de Cómputo
Pucesa

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUTO

PONTIFICIA
UNIVERSIDAD
CATOLICA
DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUTO
BIBLIOTECA VIRTUAL
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telef: 593 3 2416 220
Telefax: 593 3 2411 868 ext. 102
webmaster@pucesa.edu.ec
Ambato - Ecuador
www.pucesa.edu.ec

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 14 de noviembre de 2006

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

La presente es portadora de un saludo cordial y a la vez informarle que se ha procedido a la validación del trabajo de disertación del señor: Álvaro Fabián Villacrés Barrera, titulado: "Implementación de un Controlador de Dominio basado en la plataforma Windows 2003 Server en la Pontificia Universidad Católica del Ecuador Sede Ambato en el periodo 2006 – 2007", encontrando que el mencionado trabajo esta concluido a cabalidad, cumpliendo los objetivos trazados y funcionando plenamente en el Centro de Cómputo de la PUCESA.

Se destaca en el trabajo el servicio que está prestando en el control y adecuada administración de los recursos del Centro de Cómputo, la versatilidad y perspectivas futuras que este proyecto presenta dentro de la Institución.

Recalco además la utilidad del sistema instalado en la PUCESA, por su alto contenido técnico.

Atentamente,

Ing. Santiago Acurio M.
COORDINADOR ACADÉMICO
ESCUELA DE INGENIERIA DE SISTEMAS

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 14 de noviembre de 2006

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

La presente es portadora de un saludo cordial y a la vez informarle que se ha procedido a la validación del trabajo de disertación del señor: Nelson Eduardo Cortez Garzón, titulado: "Implementación de un Controlador de Dominio basado en la plataforma Windows 2003 Server en la Pontificia Universidad Católica del Ecuador Sede Ambato en el periodo 2006 – 2007", encontrando que el mencionado trabajo esta concluido a cabalidad, cumpliendo los objetivos trazados y funcionando plenamente en el Centro de Cómputo de la PUCESA.

Se destaca en el trabajo el servicio que está prestando en el control y adecuada administración de los recursos del Centro de Cómputo, la versatilidad y perspectivas futuras que este proyecto presenta dentro de la Institución.

Recalco además la utilidad del sistema instalado en la PUCESA, por su alto contenido técnico.

Atentamente,

Ing. Santiago Acurio M.
COORDINADOR ACADÉMICO
ESCUELA DE INGENIERIA DE SISTEMAS