

## **CAPITULO III**

### **3. PROPUESTA FACTIBLE**

#### **3.1. DESARROLLO DEL SERVIDOR LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”) EN WINDOWS 2003**

Para el desarrollo de la implementación del servidor LDAP, se propuso brindar una alternativa a los docentes y estudiantes de Ingeniería en informática y Sistemas Computacionales con este tipo de recurso, el mismo que va a facilitar la administración de parte de los educadores a sus educandos, con el Active Directory correctamente configurado, un buen rastreador de crackers y hackers que posee el Windows 2003 Server Enterprise Edition.

Es necesario de la misma manera dar a notar que este sistema operativo puede almacenar en su visor de sucesos todas las actividades de los usuarios con sus respectivos grupos de trabajo dentro del bosque de administración.

Está actividad se la ha realizado en un Servidor de Windows 2003 Server Enterprise Edition por las bondades que este tiene y más aun aprovechando el recursos del Campus Agreement con que cuenta la Universidad Técnica de Cotopaxi, las practicas se desarrollaron en una Computadora personal con procesados Core 2 duo de 1.8 Ghz, con 1GB de memoria RAM y un disco duro de 160GB. Estos apenas son el

requerimiento mínimo que debe tener un Servidor ya que lo ideal sería trabajar en un servidor que contenga como mínimo dos Procesadores de 2GHz, 8 GB de memoria RAM y 2 discos duros de 250GB de preferencia Hot Swap(Cambio en caliente).

### **3.1.1. ANALISIS DEL SOFTWARE**

#### **3.1.1.1. Descripción del Sistema Operativo**

**Microsoft Windows** (conocido simplemente como *Windows*) es un sistema operativo con interfaz gráfica para computadoras personales cuyo propietario es la empresa Microsoft. Las distintas versiones de Windows, las cuales ofrecen un entorno gráfico sencillo desde la versión Windows 95. Se ha convertido en el sistema operativo más utilizado en el mundo. Por ésta razón, la mayoría de las empresas fabricantes de hardware y software en el mundo tienden a desarrollar sus aplicaciones basadas en dicho sistema. El común uso de éste sistema operativo se debe a que la mayoría de las computadoras incluyen éste sistema instalado por defecto. Esto causa cierta controversia, ya que es visto por ciertas personas, como un método monopolista de Microsoft, ya que obliga al cliente a comprar una licencia de Microsoft, al mismo tiempo que compra la máquina.

Windows ha incorporado a través de sus diferentes versiones varias herramientas que se han convertido en estándares internacionales, como por ejemplo, el sistema de archivos FAT. Windows incorpora, entre otro software, herramientas como Internet Explorer y el Reproductor de Windows Media. Estas herramientas se han convertido con el tiempo en las más usadas, especialmente Internet Explorer, debido a que vienen instaladas por defecto en dicho sistema operativo.

Windows es utilizado principalmente en computadoras personales existiendo también diferentes versiones para servidores y dispositivos móviles.<sup>1</sup>

**Windows Server 2003** es un sistema operativo de la familia Windows de la marca Microsoft para servidores que salió al mercado en el año 2003. Está basada en tecnología NT y su versión del núcleo NT es la 5.2.

En términos generales, Windows Server 2003 se podría considerar como un Windows XP modificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor, por ejemplo, la interfaz gráfica denominada *Luna* de Windows XP viene desactivada y viene con la interfaz clásica de Windows. Sin embargo, es posible volver a activar las

---

<sup>1</sup> Tomado de los sitios web: [www.linuxparatodos.com/index.html](http://www.linuxparatodos.com/index.html), [www.linux.mx/historiadkernel.php](http://www.linux.mx/historiadkernel.php), [www.linux.es/definiciones.jhtml](http://www.linux.es/definiciones.jhtml), [www.proyectolinux.ar](http://www.proyectolinux.ar).

características mediante comandos *services.msc*. En internet existen varios trucos para hacerlo semejante a Windows XP.

### 3.1.1.2. Alcances

De las características más importantes que pueden ser consideradas como alcances son:

- Sistema de archivos NTFS:
  1. cuotas
  2. cifrado y compresión de archivos, carpetas y no unidades completas.
  3. permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo unix
- Gestión de almacenamiento, backups... incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.
- Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware.
- ActiveDirectory Directorio de organización basado en LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”), permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.
- Autenticación Kerberos5
- DNS con registro de IP's dinámicamente

- Políticas de seguridad

## **Servidores**

Los servidores que maneja Windows 2003 son:

- Servidor de archivos
- Servidor de impresiones
- Servidor de aplicaciones
- Servidor de correo (SMTP/POP)
- Servidor de terminal
- Servidor de Redes privadas virtuales (VPN) (o acceso remoto al servidor)
- Controlador de Dominios (mediante Active Directory)
- Servidor DNS
- Servidor DHCP
- Servidor de Streaming de Video
- Servidor WINS

### **Servidor de Impresión**

Teniendo ya en cuenta que para activar el servidor de impresión en Windows Server 2003 tiene que tener instalado el Windows Server, luego implementar una red cliente servidor y configurar la impresora en las PC y esta listo para que la pueda utilizar, ya sea del servidor o de una "PC hija "

### **Mejoras Respecto Windows 2000 Server**

Diferencias principales con Windows 2000 server

1. Durante la instalación arranca con el mínimo de servicios activados para no comprometer la seguridad del sistema
2. Mejoras en el manejo de políticas de seguridad
3. Active Directory ya no utiliza NetBIOS sino que es necesaria la presencia de un DNS que soporte Service Records (detección de servicios ofrecidos por una máquina a través de un DNS)

### **Versiones**

Actualmente existen cuatro versiones de Windows 2003, aunque todas ellas cuentan a su vez con versiones de 32 y 64 bits (excepto Web Edition). Las versiones son:

- **Web Edition** Diseñado para los servicios y el hospedaje Web.
- **Standard Edition** El más versátil de todos, ofrece un gran número de servicios útiles para empresas de cualquier tamaño.
- **Enterprise Edition** Para empresas de mayor tamaño que la *Standard Edition*.
- **Datacenter Edition** Para empresas que requieran bases de datos más escalables y un procesamiento de transacciones de gran volumen.

### **3.1.1.3. Limitaciones**

Como todo programa de informática siempre encontramos problemas o limitaciones las mismas que pueden ser:

Windows Server 2003, es un sistema operativo denominado propietario es decir su licencia tiene dueño y este es Microsoft, además cuentan con la tecnología de activación de producto lo que significa que deben activar su copia de Windows Server 2003 antes de utilizarlo. Algunos servidores nuevos comprados con Windows Server 2003 pre-instalado también requieren la activación. Si su organización utiliza licencias de Windows Server 2003 por volumen como Open License, Select License, o Enterprise Agreement, entonces no es necesario activar estas licencias, pero este tipo de licencias son compradas con los equipos o responden al contrato que tenga la empresa o institución con la empresa Microsoft.

La Activación de Producto Microsoft es una tecnología de antipiratería diseñada para verificar que el software es legal. La meta de la activación del producto es reducir una forma de piratería conocida como copia casual. La activación también ayuda a proteger contra la clonación de discos duros. La activación es rápida, simple, discreta, y mantiene su privacidad.

Microsoft se compromete a la protección de la propiedad intelectual y la reducción en la piratería de software. Todos en la económica no sólo el fabricante del software es herido por la piratería incluso el revendedor, el proveedor de soporte, y usted, el usuario. El software de Microsoft

auténtico le asegura un software de calidad superior y libre de virus. El software pirata no lo hace.

La activación del producto trabaja verificando que la llave del producto de un programa de software no se utilice en un número mayor de computadoras al que está especificado en la licencia.

Debe utilizar la llave del producto para instalar el software y entonces se transformará en un número de ID de instalación.

Mediante un asistente de activación usted proporcionará a Microsoft su número de ID de instalación mediante una transferencia segura sobre Internet o vía telefónica. Una ID de confirmación será enviada a su servidor para activar el producto.

El número de ID de instalación incluye una encriptación del la ID del producto y un digido del hardware. No son requeridos datos personales. El ID de confirmación es simplemente un código de desbloqueo de una instalación de Windows Server 2003 en particular.

#### **3.1.1.4. Requisitos del Sistema Operativo**

Los requisitos para la instalación de Windows 2003 Server tiene que ver mucho con las distintas versiones que este sistema operativo tiene así por ejemplo:

### **Windows Server 2003 Standart edition**

- Procesador a 133 Mhz, recomendado 550 Mhz o superior, soporta hasta 4 procesadores en un servidor
- 128 megabytes (MB) de memoria RAM, recomendado 256MB, máximo 4 GB
- Entre 1.25 y 2 GB de espacio en Disco duro
- Unidad de CDROM o DVD ROM
- VGA o hardware que soporte consola de redireccionamiento, soporta Súper VGA a 800 \*600 recomendado una resolución mayor.

### **Windows Server 2003 Enterprise edition**

- Procesador a 133 Mhz basado en x86, 733 Mhz para itanium hasta 8 procesadores basados en la versión 32 bits o 64 bits.
- 128 megabytes (MB) de memoria RAM, máximo 32 GB para pcs x86 con 32 bits y 64GB para pcs basadas en itanium con 64 bits.
- 1.5 de espacio en el disco duro para pcs basado en x86 y 2 GB para pcs basados en itanium, un espacio adicional si lo está instalando sobre una red
- Unidad de CDROM o DVD ROM
- VGA o hardware que soporte consola de redireccionamiento
- La versión de 64bits es compatible solo con sistema Intel de 64bits basado en itanium y no puede instalarse en sistema de 32 bits.

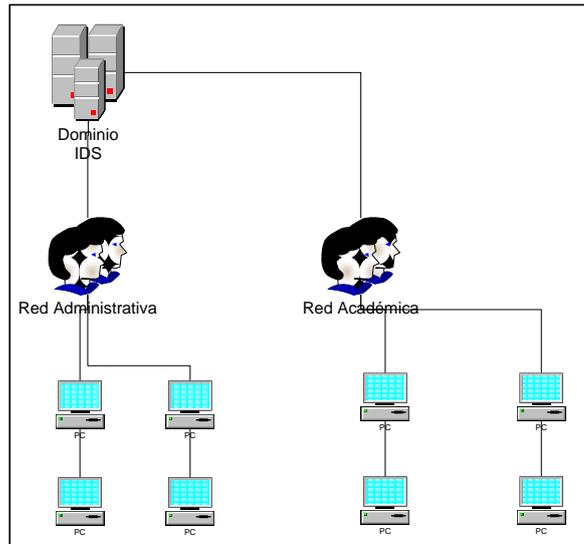
### **Windows Server 2003 datacenter edition**

- Procesador a 400 Mhz basado en x86, 733 Mhz para itanium.
- 512 megabytes (MB) de memoria RAM, recomendado 1GB.
- 1.5 de espacio en el disco duro para pcs basado en x86 y 2 GB para pcs basados en itanium.
- Requiere 8 procesadores y soporta hasta 64 procesadores.

Las otras versiones de Windows Server 2003 necesitan de las mismas características pero tienen algunos trabajos en especifico. Las versiones de Enterprise y datacenter de 64 bits no pueden ser instaladas en maquinas de 32 bits.

#### **3.1.1.5. Identificación de Grupos de trabajo**

Para la determinación de grupos de trabajo debemos tener en claro que siendo la universidad una institución donde se encuentran claramente definidas las funciones, es decir la primera Administrativa y la otra la académica, siendo las dos importantes pero sobre todo la función de la administrativa es más delicada la documentación que genera, en cambio la académica va a ser siempre el manejo de laboratorios o la utilización de redes inalámbricas, en este último caso no genera información al contrario sino más bien es un servicio que brinda la universidad a sus estudiantes y profesores.



**Gráfico 3.1:** Grupos de trabajo UTC  
**Fuente:** La Investigadora

### 3.1.1.6. Identificación de usuarios

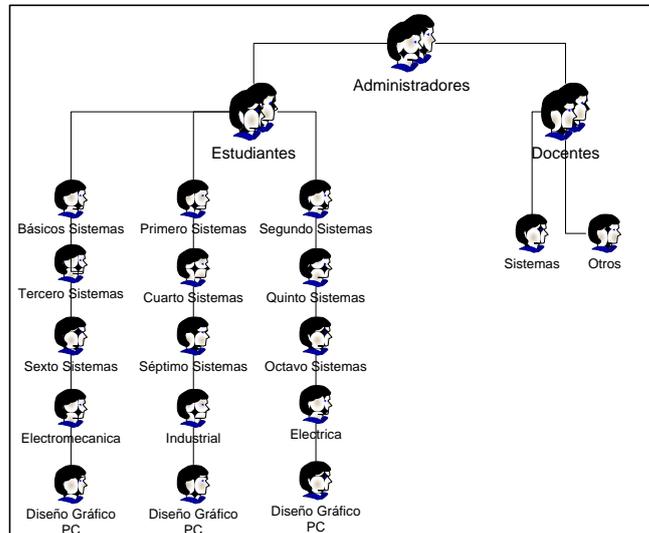
La identificación de usuarios de las redes de la Universidad se lo realiza de acuerdo a las funciones que desempeñan ya que de esta manera se garantiza la optimización del ancho de banda.

Claramente dentro de la Universidad y particularmente en el área académica se tiene 2 tipos de usuarios los mismos que son los estudiantes los mismos que se les asigna privilegios para poder acceder a sus respectivos grupos de curso y podrán realizar:

- Instalación de software educativo
- Desinstalación del mismo software
- Acceder a su cuenta
- Escritorio remoto dentro de su grupo de trabajo.

Los docentes cuentan con los mismos privilegios más el de administración de las actividades que los estudiantes puedan

realizar esto es acceso al servidor de Windows 2003 Server con los privilegios de Administrador.

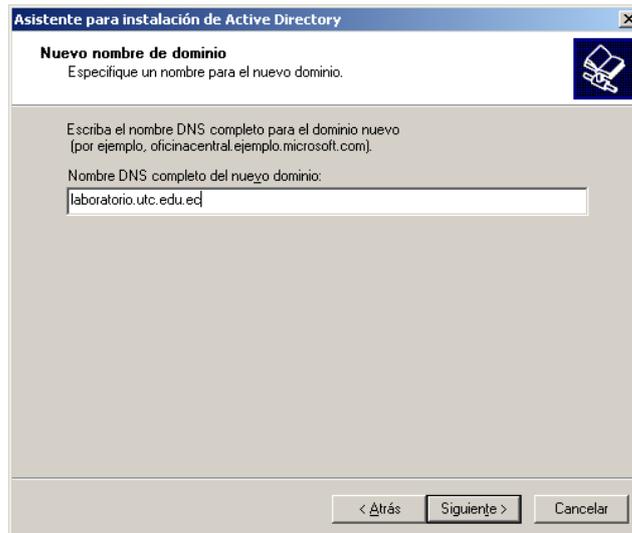


**Gráfico 3.2:** Usuarios Área Académica UTC  
**Fuente:** La Investigadora

### 3.1.2. DISEÑO DEL SERVIDOR LDAP (“LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL”)

#### 3.1.2.1. Diagramas de árboles jerárquicos

En la grafica 3.2 se pudo observar la distribución en forma de árbol de cómo puede quedar las configuraciones de los servidores el mismo que debe ser ubicado dentro de un laboratorio de sistemas, ya que de esta manera se va a garantizar de que los usuarios puedan tener privilegios para instalar/ desinstalar software, acceder o restringir a estudiantes su utilización, es decir todo esto va en beneficio directo de los administradores de las salas de laboratorio de la Universidad y particularmente al laboratorio de Windows 2003 Server y compatibles.



**Gráfico 3.3:** Dominio planteado para la Investigación  
**Fuente:** La Investigadora

### **3.1.2.2. Puertos de asignación para el Servidor LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”)**

Los puertos asignados en un servidor LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”) tienen mucho que ver con los servicios que se encuentren habilitados de acuerdo al perfil que tengan los usuarios o los grupos de trabajo, como se pudo observar en un punto anterior en el árbol jerárquico.

### **3.1.3. FUNCIONALIDAD DEL SERVIDOR LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”)**

#### **3.1.3.1. Descripción del contenido del servidor**

Un servidor LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”) es básicamente un servidor de dominio con la configuración de todos los usuarios dentro de éste, tienen que soportar el DNS(Domain Name Server), que es muy importante

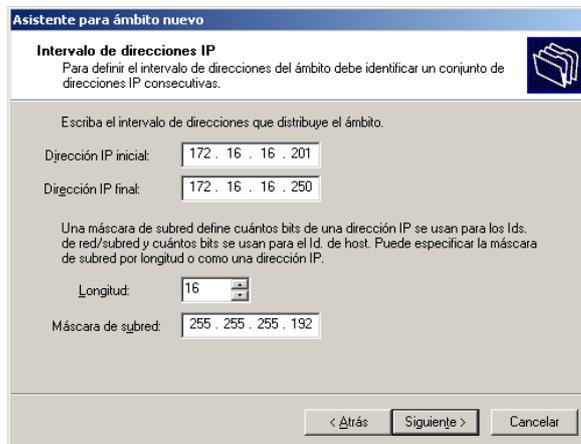
cuando se cuenta con una conexión a Internet para que nos pueda resolver todos los nombres de la red.



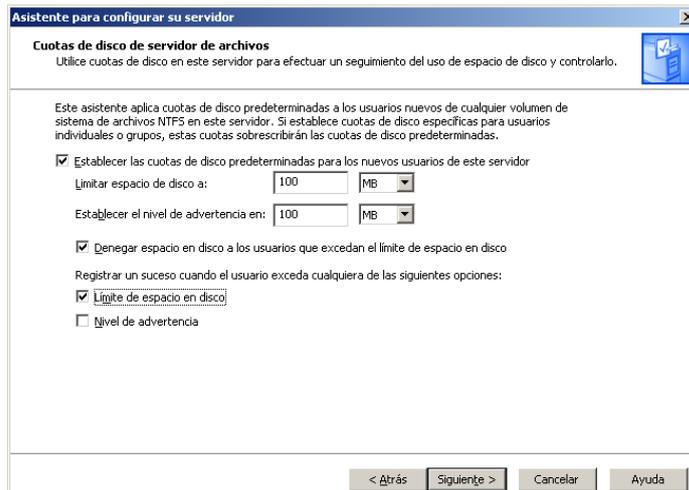
**Gráfico 3.4:** Dominio y Direcciones IP Asignadas para el servidor  
**Fuente:** La Investigadora

Además de esto que es la base fundamental ya que todos los usuarios deben acceder resolviendo su usuario y contraseña contra el servidor es importante tener un servidor de DHCP para la configuración de las direcciones IP automáticas, es importante notar que el DHCP debe resolver muy bien las IP automáticas de dirección inversa.

**Gráfico 3.5:** Intervalos asignados en el DHCP  
**Fuente:** La Investigadora



Al tener una gran base de datos el servidor de tener compartido el privilegio de ser un servidor de archivos e impresiones los mismos que van a ser base fundamental en la Base de datos del servidor.



**Gráfico 3.6:** Dominio y Direcciones IP Asignadas para el servidor  
**Fuente:** La Investigadora

En base a lo manifestado deben tener al menos 5 puertos los mismos que deben ser controlados por un servidor de Base de datos, que por compatibilidad debería ser SQL Server, o en su defecto el Oracle con configuraciones para Servidores Microsoft.

### 3.1.3.2. Contenido del software

Como se pudo observar a lo largo de las configuraciones del servidor **LDAP** (**"LIGHTWEIGHT DIRECTORY ACCES PROTOCOL"**) ("Lightweight Directory Acces Protocol"), en español Protocolo Ligero de Acceso a

Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

En este trabajo se utilizó inicialmente como un Front-end, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos.

La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos, Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo.

Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta.

Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer

requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

Finalmente se puede deducir que un LDAP (“LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL”) es un sistema gestor de una base de datos (Database Management System ó DBMS) de Oracle, Microsoft, o de Open source como MySQL es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.

Un servidor LDAP (“LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL”) es usado para procesar peticiones (queries) a un directorio. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento.

En otras palabras, LDAP (“LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL”) es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.

### 3.1.3.3. Mapa de la Configuración

Una vez que se realizo todas las configuraciones al servidor Windows 2003 Server, debemos realizar la creación del directorio de:

- Usuarios
- Grupos de Trabajo
- Controladores de Dominio

La creación de usuarios se lo debe realizar de forma normal es decir que no debe contener atributos especiales ya que los Grupos o los controladores de dominio van a ser quines tengan los privilegios para poder realizar una u otra actividad.

Como se puede observar en la siguiente grafica el usuario siempre va a tener el dominio que hace referencia el controlador de dominio o el domain controller, hay que tener en cuenta que en nuestro caso se le denomino **laboratorio.utc.edu.ec** este dominio también podría ser tomada en cuenta para lo que es correo electrónico, y algunas otras actividades.

Incluso los Administradores, docentes todos son creados de una misma manera ya que sus atributos no van a estar personalizados.

Nuevo objeto - Usuario

Crear en: laboratorio.utc.edu.ec/Users

Nombre: Mirian Iniciales:

Apellidos: Herrera

Nombre completo: Mirian Herrera

Nombre de inicio de sesión de usuario:  
mherrera @laboratorio.utc.edu.ec

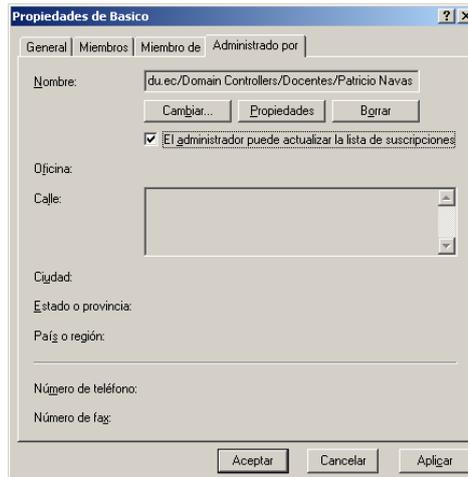
Nombre de inicio de sesión de usuario (anterior a Windows 2000):  
LABORATORIO\ mherrera

< Atrás Siguiente > Cancelar

**Gráfico 3.7:** Creación de usuarios  
**Fuente:** La Investigadora

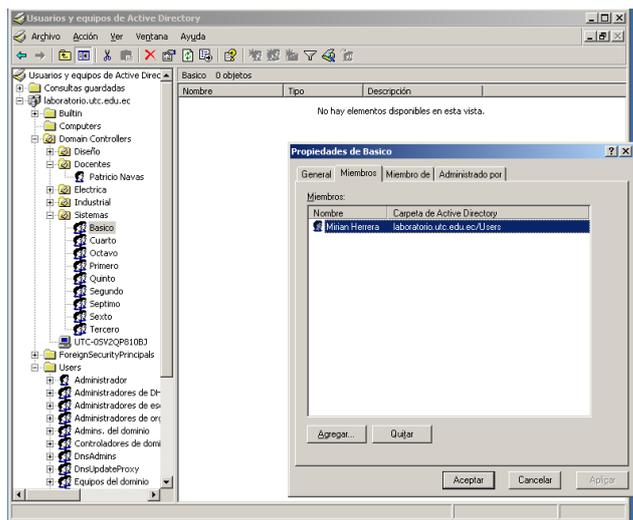
Una vez creados todos los usuarios que conformaran el directorio del servidor LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”) se procede a crear los grupos de trabajo donde va a contener los usuarios con los privilegios que pueden tener de acuerdo a sus perfiles, dentro del árbol de jerarquías van a contener los **DOMAIN CONTROLLERS**, que son los que contienen todas las configuraciones que los equipos clientes van a contener.

Los grupos de trabajo son contenedores y en donde se almacenan todos los usuarios con los respectivos privilegios que tienen los clientes que van acceder a la red y servidores que conformen los dominios.



**Gráfico 3.8:** Creación y configuración de Grupos  
**Fuente:** La Investigadora

En la grafica se puede ver que los controladores de dominio son los administradores del grupo denominado Docentes y este a su vez contiene al usuario Patricio Navas, de esta manera el árbol de directorios final quedaría de la siguiente manera:



**Gráfico 3.9:** Árbol de usuarios  
**Fuente:** La Investigadora

El árbol de usuarios creada detalla con lo anteriormente manifestado, lo que se consigue con esto cumplir con lo planificado en el proyecto de grado.

## **VERIFICACION DE LA HIPOTESIS**

Al iniciar el anteproyecto de tesis previo la obtención del título de Ingeniera en Informática y Sistemas Computacionales se planteó como Hipótesis:

La implementación de un servidor LDAP permitirá mejorar las seguridades en la red y ser un aporte valido en la formación de nuevos profesionales de Sistemas.

Basándose en esta hipótesis se desarrollo el proyecto cumpliéndose a cabalidad con lo planteado ya que el desarrollo de esta investigación ha permitido realizar pruebas en seguridades de la información, y sobre todo permitir flexibilizar el uso de las computadores de los laboratorios de sistemas, pero todo esto supuso un pequeño detalle que la implementación del servidor ldap ocasiona un conflicto con el IDS(Sistema de Detección de Intrusos) ya que el Tipping Point de 3com que equipa la Universidad genera su propio dominio y DNS lo que la aplicación de otro Dominio genera conflictos de autenticación de logeo y passwords.

La implementación se la debe realizar en un servidor de Windows 2003 el mismo que se debe encontrar independientemente de las VLAN de la Universidad ya que esto supone un aporte valioso a la formación de los futuros profesionales de Sistemas de esta prestigiosa Universidad.