00623
16

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO.

FACULTAD DE CONTADURIA Y ADMINISTRACION.

"IMPLEMENTACION DE UNA INTRANET PARA LOS LABORATORIOS DE LA FACULTAD DE CONTADURIA Y ADMINISTRACION"

DISEÑO DE UN SISTEMA PARA UNA ORGANIZACION

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

PRESENTA:

RAFAEL EUGENIO MENDOZA TORRES

ASESOR:

L.A. SALVADOR MEZA BADILLO

MEXICO, D.F. 2003

A

AGRADECIMIENTOS

A Dios por darme la oportunidad de lograr una de las metas más importantes de mi vida.

A mis Padres Noemí y Artemio, a los que les debo no solo el ser sino todo lo que he logrado, gracias por sus desvelos, sacrificios, consejos, sin los cuales no hubiera sido posible cumplir uno de mis anhelos, él convertirme en Profesionista, por esto y mas les estoy eternamente agradecido, rogándoles que compartan este triunfo que no solo es mío si no también de ustedes.

A mi Asesor L.A. Salvador Meza Badillo, quien siempre tuvo tiempo para escucharme y orientarme a pesar de sus múltiples actividades, que más que un Maestro es un amigo. Mi más profundo agradecimiento, cariño y respeto.

A Tere quien con su amor y cariño me motivo para salir adelante en este proyecto, cristalizando uno de mis anhelos, el de ser un Profesionista. Gracias por esto y más.

D

A Carmen y Nohemí, a quienes agradezco todo su apoyo, que fue una contribución enorme para este proyecto.

A Frida y Diego a quienes dejo este proyecto como constancia de que con trabajo y esfuerzo se pueden cristalizar nuestras metas, esperando que un futuro me superen profesionalmente que estoy seguro así será.

E

A Juan y Luis quienes gracias a su amistad, consejos y apoyo me orientaron en los momentos más difíciles, ya que sin ellos no me hubiera sido posible terminar mi carrera.

A Erick gracias por tus invaluables consejos, pero sobre todo por tu amistad, no solo como amigos sino también como colegas.

A mis familiares y amigos que me apoyaron a lo largo de mi carrera.

A aquellas personas que aunque físicamente no están aquí, están en mi corazón, estando seguro de que me felicitarían y animarían.

+ Abuelita Lucha
+ Tío Jorge
+ Tío Julio

G

Al Honorable Jurado por su valiosa intervención.

A mi querida Universidad, la cual seguirá siendo la cuna de los hombres más importantes de nuestro País.

INDICE.

INTRODUCCIÓN.

Debido al rápido desarrollo de nuevas tecnologías de sistemas de información y al creciente desarrollo de nuevas computadoras, surge la necesidad de migrar a plataformas nuevas que presentan características mejoradas, mejor rendimiento, más seguridad, etc.

El caso de los sistemas operativos, ha tenido una evolución muy amplia, desde MS-dos hasta Windows XP, linux, unix, etc., estos sistemas están en actualización, sobre todo en el caso de los sistemas operativos para servidor, los cuales se han desarrollado de manera amplia ofreciendo diferentes características que los identifican.

En el caso de los laboratorios de la Facultad de Contaduría y Administración, se ha trabajado sobre sistemas basados en Windows 95, Windows 98se y Windows 2000 los cuales no contaban con ningún tipo de restricción para los usuarios, originando daños en el software tanto en el sistema operativo como en los paquetes instalados, instalación del software no autorizado, etc.

Tomando en cuenta esta problemática, se plantea el objetivo de este proyecto así como la implementación de las herramientas necesarias, para llevarlo acabo.

CAPITULO I

MARCO CONCEPTUAL.

1.1 OBJETIVOS.

Objetivo General

- Implementar políticas de seguridad informatica para los usuarios de los laboratorios de computo.

Objetivos Específicos

- Implementar políticas de seguridad informática a través de un perfil de usuario.

- Implementar un servidor para montar el dominio y los servicios necesarios para su correcto funcionamiento.

- Diseñar un dominio por donde los usuarios sé logearan para aplicarles las políticas de seguridad.

- Crear grupos de usuarios y cuentas de usuario para la administración de los laboratorios.

1.2 CENTRO DE INFORMATICA DE LA FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN.

La Universidad Nacional Autónoma de México, nuestra Máxima Casa de Estudios, es una de las instituciones educativas más importantes de nuestro país ya que cuenta con un amplio reconocimiento tanto a nivel nacional como internacional. Dentro de la Universidad se encuentran diversas Facultades, Escuelas, Institutos, Colegios dependencias entre otras, una de ellas es la Facultad de Contaduría y Administración.

Esta surge por la necesidad de dotar de profesionales en las áreas contable y administrativa, desde su fundación la Facultad ha sufrido cambios en su estructura, ubicación, recursos, instalaciones, etc.

La historia de la Facultad en orden cronológico es la siguiente:

- En el año de 1894 surge la Escuela Superior de Comercio y Administración.

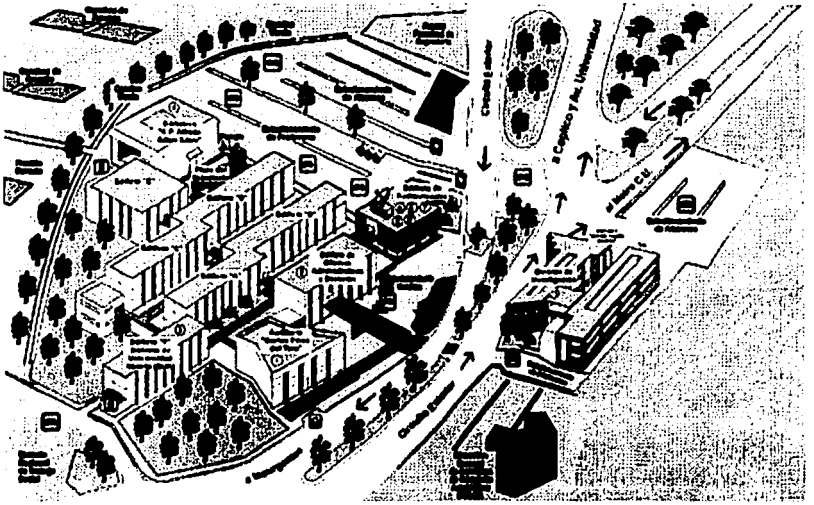
- Para 1929, una porción de esta escuela, se integro al Campus Universitario como parte de la Esuela Nacional de Derecho y Ciencias Sociales.

- Liverpool 66 en la Colonia Juárez fue la casa de esta escuela desde 1945, y actualmente se encuentra albergada ahí la División de Educación Continua.

- Hacia 1955, la escuela se traslada a Ciudad Universitaria, en el ala de Humanidades, actualmente la Facultad de Economía.

- El Consejo Universitario autorizo la creación de la División de Posgrado en 1965, y se decide darle la categoría de Facultad.

- La facultad se establece en el edificio que conocemos actualmente en el año de 1968.



- Durante 1972 surge el proyecto para formar un Centro de Procesamiento de Datos para la facultad, el cual llevo el nombre de Servicios de Informática de la Facultad de Contaduría y Administración (SIFCA).

- A partir de 1980 se conoce como el Centro de Informática de la Facultad de Contaduría y administración (CIFCA).

- En 1985 surge la licenciatura en Informática en la FCA y queda a cargo de la coordinación de Informática, ubicada en el edificio del centro de Informática.

- La primera computadora que se adquirió para la facultad fue en 1987.

- En 1992 se inauguraron 3 redes Novell Netware en el laboratorio 1, ubicado en la planta baja del edificio de la biblioteca, así como en las salas A , B , y C del edificio de Posgrado.

- Durante 1993 se remodelaron las 3 salas de audiovisuales ubicadas en la planta baja de la biblioteca con el fin de instalar otros 3 laboratorios de cómputo.

- A partir de 1994, la FCA ya contaba con laboratorios de cómputo para alumnos, profesores y personal administrativo.

- En 1995 se conecto la FCA al Backbone de la RedUNAM, a través de 480 metros de fibra óptica desde el edificio f hacia la Dirección General de Servicios de Computo Académico (DGSCA).

- Actualmente se cuenta con más de 1500 servicios de red distribuidos en toda la Facultad, así como en el Posgrado, y sus extensiones en la División de Educación Continua (DEC), y el Campus de Juriquilla en Querétaro.

- Se cuenta con 9 laboratorios en licenciatura y con 3 en el Posgrado.

1.3 OBJETIVO DEL CENTRO DE INFORMATICA.

Promover, orientar y difundir las acciones que en materia de docencia e investigación se llevan acabo en el ámbito de la Informática, así como apoyar a la Facultad en los sistemas administrativos que requiere.

1.4 MISION.

Proporcionar servicios de computo y telecomunicaciones a la comunidad de la Facultad, así como fomentar los vínculos con organismos externos, establecer normas y políticas en materia de tecnología informática y telecomunicaciones que permitan automatizar y hacer mas eficientes las actividades de la institución.Ademas de difundir la cultura computacional a la comunidad de la facultad, así como investigar, desarrollar e integrar tecnologías innovadoras.

1.5 FUNCIONES.

- Coordinar a los alumnos, profesores, investigadores y empleados administrativos para el uso del equipo de cómputo en las salas de la Facultad, así como el servicio de impresión.

- Analizar y diseñar propuestas para el desarrollo e implantación de nuevas tecnologías en el área de Informática académica, de investigación y desarrollo.

- Administrar cuentas de alumnos, profesores y personal administrativo dentro de los servidores de la FCA.

- Administrar los servicios electrónicos de acceso a Internet, garantizando la seguridad en la transferencia de información.

- Proporcionar mantenimiento preventivo y correctivo a los equipos de cómputo y periféricos, así como soporte técnico y soporte de telecomunicaciones a la comunidad de la FCA.

- Análisis y diseño de sistemas de información para el personal administrativo y académico de la Facultad.

- Resguardar y dar seguimiento a los contratos y convenios celebrados con los diferentes proveedores de equipos de cómputo de la Facultad.

- Diseño y mantenimiento de la pagina Web y servicios de Internet de la Facultad.

- Diseñar, editar, digitalizar textos o imágenes para colocarlos en las páginas Web de la FCA.

- Administrar la infraestructura de la red de cómputo de la FCA, su instalación y mantenimiento de la misma, según las normas establecidas por la DGSCA.

- Garantizar la eficiencia y calidad de los servicios proporcionados hacia los usuarios de la FCA.

CAPITULO 2

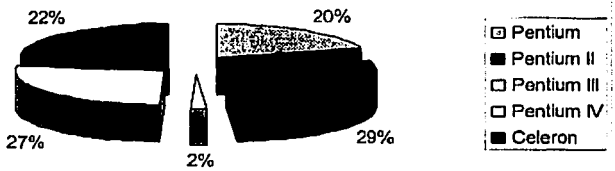
MARCO PROBLEMATICO.

2.1 INFRAESTRUCTURA DE LOS LABORATORIOS DE LA FCA.

El equipo de cómputo[1] con el que cuenta la FCA para el área de laboratorios es el siguiente:

Pentium	Pentium II	Pentium III	Pentium IV	Celeron
81	113	6	107	89

EQUIPO DE COMPUTO DE LOS LABORATORIOS DE LA FCA.



[1] Estadísticas proporcionadas por el Departamento de Hardware actualizadas al mes de Julio del 2002.

Como se puede observar el la grafica el 56% del equipo de computo de los laboratorios corresponde a equipos Pentium II y Pentium IV, y un 22% a equipos celeron, lo cual nos da una idea de la caracteristicas de lo equipos.

De estos equipos cuentan con los sistemas operativos siguientes:

- Windows 98SE®
- Windows 2000 Profesional®

Como se puede ver en la grafica, el 65% de lo equipos cuentan con Windows98se y el 35% con Windows 2000 Profesional, tomando en consideración que los equipos con Windows 98 cumplen las caracteristicas minimas para trabajar con Windows 2000 Profesional.

2.2 INFRAESTRUCTURA EN MATERIA DE TELECOMUNICACIONES.

La red es un elemento clave en las actividades diarias de la FCA, ya que por media de ella se obtiene, distribuye, maneja y administra la información generada y utilizada por todo el personal de la Facultad, así como de los usuarios externos a ella.

La FCA cuenta con un enlace de fibra óptica a 10Mbps tendido desde la DGSCA hasta la planta baja del edificio F, donde se encuentra el switch principal el cual distribuye el servicio de red hacia el interior de la Facultad.

Internamente se cuenta con un Backbone de fibra óptica que viene desde el switch principal hacia los edificios E, Biblioteca, Coordinaciones, Auditorio, Audiovisuales edificios de Posgrado e Investigación y a partir de ahí, a través de switches y concentradores (hubs), se proporciona servicio de red (datos y video) a todas la áreas de la FCA, haciendo mención que la red es ethernet.

A nivel de direccionamiento IP, RedUNAM es una red de clase B (132.248.0.0), y las subredes creadas para todas sus instituciones son de clase C con mascara de 24 bits (132.248.x.0).

A la FCA le fueron asignados 5 segmentos de red por el Centro de Información de la Red de la UNAM (NIC), distribuidos de la siguiente manera:

Segmento de Red	IP's	Utilización
132.248.18.0	253	Servidores, Equipos de Red y equipos que requieren una conexión permanente.
132.248.128.0	253	Reservado a un servidor DHCP con el objetivo de proporcionar direcciones IP dinámicas a los usuarios.
132.248.158.0	253	Segmento dedicado a dar servicio a lo equipos de la DEC.
132.248.179.0	50	Segmento dedicado a dar servicio a los equipos de Juriquilla.
132.248.164.0	253	Reservado a un servidor DHCP con el objetivo de proporcionar direcciones IP dinámicas a los usuarios.

El crecimiento de la Red ha propiciado que las tareas de mantenimiento y administración de la misma se hayan visto afectadas debido a la elevada cantidad de usuarios conectados.

DIAGRAMA DE RED DE LA FCA.

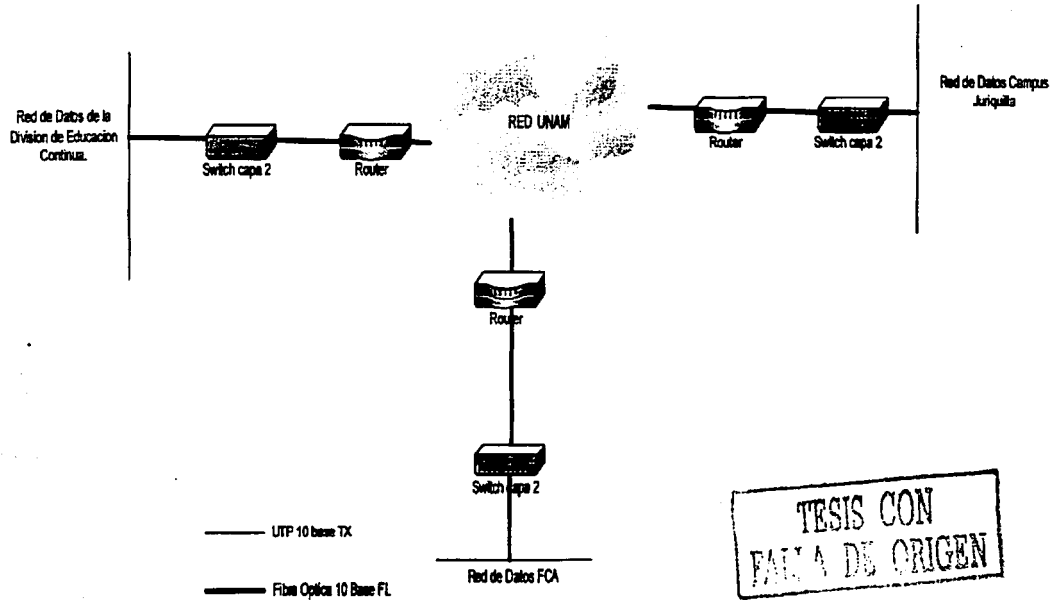
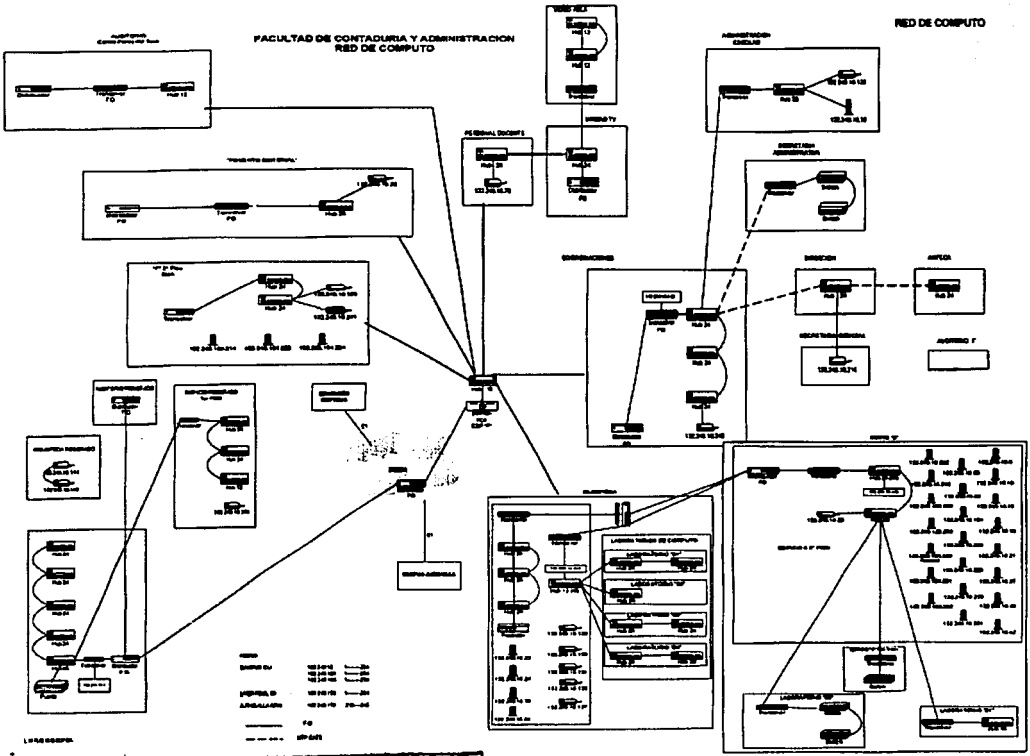


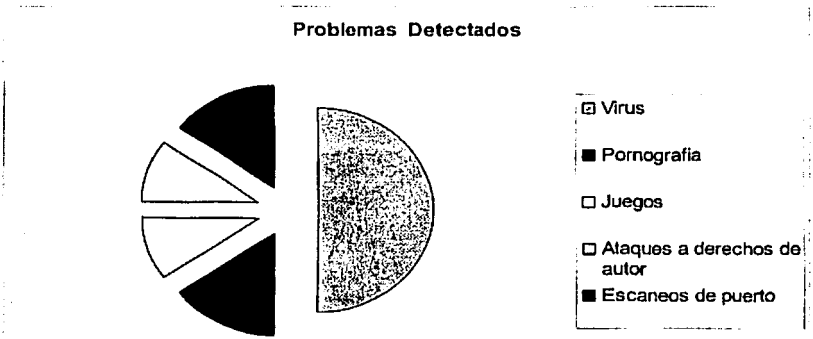
DIAGRAMA FISICO DE LA RED DE LA FCA.



2.3 SITUACION ACTUAL DE LOS LABORATORIOS DE LA FCA.

Actualmente los laboratorios de la FCA no cuentan con una política de seguridad establecida, ya que tienen conexión directa a Internet sin que se le aplique algún tipos de restricción, además en un principio en los equipos con Windows 2000 Profesional®, se les estaba dando acceso a los alumnos con la clave de administrador, dándoles los privilegios para modificar cualquier configuración de el sistema, así como para cambiarle las contraseñas de acceso.

Dentro los principales problemas detectados se muestran en la siguiente grafica:



Como se observa en la grafica, los problemas menos frecuentes son la pornografía, los juegos, los ataques a lo derechos de autor y los escaneos de puerto, estos últimos relacionados también con virus, el problema más frecuente detectado son los ataques por virus, ya que los usuarios bajan archivos sin ninguna precaución aundado a esto se ha detectado que los servidores sociales instalan software para bajar mp3, videos, juegos, etc, ocasionando t tambien la infeccion del equipo.

Dentro de los ataques de vidrus mas frecuentes detectados se tienen los siguientes:

- Nimda
- W32.Opaserv
- W32 bugbear
- Code Red
- Etc.

Ocasionando que se reciban reportes como el siguiente:

Fecha: Wed, 6 Nov 2002 14:33:30 -0600 (CST)
De: "Abuse RedUNAM" <spam@unam.mx>
A: sameza@server.contad.unam.mx, loromero@server.contad.unam.mx
Asunto: Problemas de Seguridad [132.248.164.228] Primer Aviso

"Reporte del gusano W32.Opaserv o W32.Bugbear"

Buen día.

Hemos recibido uno o mas correos indicando que el equipo cuya dirección IP se indican en el subject de este correo esta haciendo escaneos a maquinas de otra institución u organización, de acuerdo al comportamiento presentado y los puertos por donde se están haciendo dichos escaneos, es probable que la dirección IP mencionada este infectada por el gusano W32.Opaserv o el W32.Bugbear.

Para poder dar solución a este problema le recomendamos visitar las siguientes direcciones:

- W32.Opaserv o Win32.Opasoft

http://www.unam-cert.unam.mx/
http://www.f-secure.com/v-descs/opasoft.shtml
http://www.cert.org/
http://vil.nai.com/vil/content/v_99729.htm
http://www.sophos.com/virusinfo/analyses/w32opaserva.html

- W32.Bugbear

http://www.unam-cert.unam.mx/
http://vil.nai.com/vil/content/v_99728.htm
http://www.f-secure.com/v-descs/tanatos.shtml
http://www.sophos.com/virusinfo/analyses/w32bugbeara.html
http://www.trendmicro-la.com/vinfo/WORM_BUGBEAR_A.html

Le pedimos revisar este problema y notificarnos a la cuenta abuse@unam.mx en cuanto quede resuelto con el fin de enviar las notificaciones necesarias en caso de que ya se haya filtrado su IP o alguna subred de la UNAM.

Para solicitar asesoria pueda acudir a:

- UNAM-CERT Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Computo Jefe del Departamento: Juan Carlos Guel López
E-Mail:seguridad@seguridad.unam.mx
http://www.asc.unam.mx/
Tel: 56 22 81 69 Fax: 56 22 80 43

Le enviaremos cada unos de los correos recibidos con el subject: Opaserv-Worm "[direccion IP]".

Gracias por su colaboración, reciba un cordial saludo.
Atte.Isabel Guzmán

Centro de Información R e d U N A M	Network Information Center NIC - RedUNAM
http://www.nic.unam.mx/	NIC-mail :
Subdirección de Redes DTD - DGSCA - UNAM	TEL: (+52 5) 622 81 10 Fax: (+52 5) 622 85 88

Otro problema presentado es que tanto los profesores y usuarios que llegan a utilizar el software de los laboratorios este no este disponible por daños en el mismo sobre todo para los profesores que utilizan este software como parte de su materia, ocasionando atrasos tanto en su clase como en los alumnos.

2.4 DIAGNOSTICO.

Como se puede ver dada la problemática presentada anteriormente se llego a lo siguiente:

- Los laboratorios no cuentan con políticas de seguridad adecuadas en cuanto a lo que es el sistema operativo y la red.

- Una gran parte de usuarios y servidores sociales hacen mal uso del equipo esto es instalando software para bajar música, videos, juegos, ocasionando con esto un consumo excesivo de espacio en disco duro y la infección del equipo con virus.

- Los usuarios accedan a los equipos con claves de administrador provocando que no tengan ninguna restricción de el equipo y puede modificar cualquier configuración, ocasionando daños al sistema operativo, así como cambiando contraseñas.

- Se empezaron a implementar políticas de manera local, pero dado el número de equipos y el tiempo que se llevaba hacer esto resultaba complicado para el personal de telecomunicaciones ya que solo eran 2 personas las que lo implementaban y además tenían otras actividades dentro del área misma.

- Se dañaba, modificaba o desinstalaba, el software utilizado tanto por los profesores como por los alumnos.

2.5 PROPUESTA TECNOLOGICA.

WINDOWS 2000 ADVANCED SERVER®.

La opción mas viable en este caso es la implementación de un servidor Windows 2000 Advanced Server para que lo usuarios inicien sesión a través de el.

La idea es que cuando los usuarios inicien sesión a través del servidor se les apliquen políticas de seguridad las cuales les restringirán entre otras cosas modificar las configuraciones del equipo.

Destacando las siguientes características:

- Costo reducido debido a un convenio con Microsoft gracias al cual se donaron las licencias de Windows 2000 en sus versiones Profesional, Server, Advanced Server.
- Se cuenta con equipos configurados con Windows 2000 Profesional®.
- La mayoría de los equipos con Windows 98 SE® cumplen los requisitos mínimos para instalar Windows 2000 Profesional®.
- Las políticas de acceso a los equipo se aplicarían por medio del servidor y no de manera local.
- Fácil administración debido a que el personal de telecomunicaciones esta capacitado para el manejo de Windows 2000 ®.

CAPITULO 3

MARCO METODOLOGICO.

3.1 WINDOWS 2000.

Un sistema operativo es un programa que le da significado y orden a las aplicaciones para interactuar con el hardware de la computadora. Un sistema operativo administra cuatro aspectos claves de la operación de una computadora:

- Administración del hardware: El sistema operativo le da a la computadora la habilidad de comunicarse con dispositivos periféricos como la impresora o el Mouse.

- Administración del software: El sistema operativo provee de un mecanismo para iniciar los procesos que requiere un programa como un procesador de texto o dibujo.

- Administración de memoria: Al sistema operativo le corresponde ubicar a cada aplicación en su espacio de memoria sin que afecte el funcionamiento de las demás aplicaciones y de la memoria en si.

- Administración de datos: El sistema operativo administra los archivos almacenados en los discos duros y otros dispositivos de almacenamiento. Habilita a las aplicaciones para crear y abrir archivos, transferir datos entre dispositivos y ejecutar tareas administrativas de documentos como borrar o renombrar.

El sistema operativo coordina la interacción entre la computadora y las aplicaciones que se ejecutan en ella. Controla el flujo de datos y provee la interfaz grafica del usuario (GUI), significa que interactúa con la computadora. La GUI es un camino grafico intuitivo para los usuarios que contiene los comando para el sistema operativo al igual que en un ambiente basado en línea de comando pero con la ventaja que representa.

Windows 2000 provee de un conjunto de herramientas para asistir y simplificar las tareas administrativas y la configuración de las computadoras clientes. Windows 2000 provee de capacidades avanzadas para la automatización de muchas de estas tareas y así minimizar los costos. La familia de sistemas operativos Windows 2000 consta de las siguientes versiones:

- Microsoft Windows 2000 Profesional.
- Microsoft Windows 2000 Server.
- Microsoft Windows 2000 Advanced Server.
- Microsoft Windows 2000 Data Center Server.

3.2 CARACTERISTICAS DE WINDOWS 2000.

El sistema operativo Windows 2000 cuenta con las siguientes características:

- **Multitarea**: la multitarea habilita al usuario ejecutar múltiples aplicaciones de manera simultánea en el mismo sistema. El número de aplicaciones que el usuario puede ejecutar simultáneamente y del rendimiento cuando se están ejecutando depende de la memoria del sistema.

- **Soporte a la memoria**: Para funcionar cada aplicación que se ejecuta en Windows 2000 requiere cierto espacio de memoria.Para el soporte multitarea y para aplicaciones de grandes requerimientos de memoria, Windows 2000 provee soporte hasta 64 GB de memoria.

- **Escalabilidad para multiprocesamiento simétrico**: el multiprocesamiento simétrico(SMP) es una tecnología que permite a un sistema operativo utilizar múltiples procesadores de manera simultanea para improvisar rendimiento al sistema reduciendo el tiempo de transacción.Dependiendo de le versión, Windows 2000 provee soporte SMP hasta para 32 procesadores.

- **Plug and Play**: Con Windows 2000 es sencillo instalar dispositivos Plug and Play. Esto es que se pueda conectar y utilizar inmediatamente sin necesidad de ejecutar un procedimiento de instalacion.Una vez conectado el dispositivo, Windows 2000 automáticamente identifica el componente agregado y completa la configuración.

- **Clustering**: El sistema operativo de Windows 2000 provee de habilidad para agrupar un numero de computadoras independientes para ejecutar juntas un set común de aplicaciones.Este grupo aparece como un sistema único para el

cliente y la aplicacion.Si el grupo es llamado clustering, el grupo de computadoras es llamado clusters.Este arreglo de maquinas evita cualquier punto de falla.Si una computadora se "cae" otra de grupo provee los mismos servicios en su lugar.

- **Características del sistema de archivos**:El sistema de archivos NTFS es recomendado para utilizar con Windows 2000, ya que provee las siguientes características:
  - *Recuperación del sistema de archivos.
  - *Particionamiento para grandes tamaños.
  - *Seguridad.
  - *Compresión.
  - *Disk quotas.

  Además de que se pueden utilizar los sistemas de archivos FAT y FAT32.

- **Quality of Service (QoS)**: En Windows 2000, quality of service es un set de requerimientos de servicios que debe contener la red para asegurar un adecuado nivel de servicio para la transmisión de datos.Utilizando QoS se puede controlar como el ancho de banda es utilizado para las aplicaciones.

- **Servicio de terminal**: El servicio de terminal provee de acceso remoto al escritorio del servidor a través de un emulador de terminal. Un emulador de terminal es una aplicación que le permite acceder a una computadora remota como si físicamente estuviera ubicado en ella.Utilizando este servicio se pueden ejecutar aplicaciones clientes en el servidor así la computadora cliente funciona como terminal mas que como un sistema independiente.

Las características de cada versión de Windows 2000 son:

- Windows 2000 Profesional: Es un sistema operativo de escritorio que incorpora las características de Windows 98 y que se construye sobre la plataforma de Windows NT 4.0 .Incluye una interfaz de usuarios simplificada, la funcionalidad Plug and Play, administración poderosa y soporte para un rango de dispositivos de hardware.

- Windows 2000 Server: Es una edición estándar de la familia de Windows 2000 Server.Contiene todas las características del Profesional y es ideal para organizaciones pequeñas –medianas.Esta versión de Windows 2000 trabaja bien para servidores de archivos e impresión.

- Windows 2000 Advanced Server: Contiene toda la funcionalidad de Windows 2000 además de incrementar escalabilidad y disponibilidad del sistema.Escalabilidad es la habilidad de incrementar el poder de procesamiento incrementado, esta funcionalidad se provee a través de clusters de múltiples servidores.Estos servidores proveen de poder de procesamiento adicional si uno de los servidores sale de disponibilidad.

- Windows 2000 Datacenter Server: Contiene toda la funcionalidad de Windows 2000 advanced server mas soporte para memoria adicional y CPU'S por computadora. Esta diseñado para datawarehouse, transacciones en línea y simulaciones en gran escala, puede soportar mas de 100,000 usuarios de manera simultánea. Soporta sistemas SMP con 32 procesadores y 64 GB de memoria física.

3.3 SERVICIOS DE DIRECTORIO ACTIVO (ACTIVE DIRECTORY).

Windows 2000 introduce el directorio activo, un servicio de directorio que es seguro, distribuido, esta separado en particiones y duplicado.

Un directorio es una estructura jerárquica de información que guarda datos acerca de objetos en la red.El Active Directory proporciona a los usuarios de red acceso a recursos en cualquier parte de la red utilizando una sola conexión.Tambien proporciona a los administradores un punto único de administración para todos los objetos de la red que se pude organizar en una estructura intuitiva y jerárquica, además de proporcionar los siguientes beneficios:

Consultas: El Active Directory genera un catalogo global que pueden usar los usuarios y administradores para encontrar cualquier objeto en la red, utilizando cualquier atributo de ese objeto.Por ejemplo, puede encontrar un usuario por su primer nombre, apellido, alias de correo electrónico, etc. Las PC's que estén ejecutando un cliente soportado por el active directory proporcionan opciones de menú que le permiten al cliente consultar el catalogo global para obtener información.

Administración mejorada: Una lista mejorada de control de acceso (ACL), o permisos, controla que usuarios pueden ver y acceder a los objetos en el active directory.Una ACL de un objeto enumera que usuarios pueden ver o utilizar el objeto y que acciones especificas se pueden realizar sobre ese objeto.Se puede otorgar acceso específicamente a cada atributo individual de un objeto.
La seguridad del active directory soporta tanto herencia como delegación de autoridad.La herencia permite que se copie el conjunto de permisos de un objeto especifico a todos sus objetos hijos.Los administradores pueden delegar autoridad y

otorgar derechos administrativos específicos para contenedores y subárboles a otros individuos y grupos.

Información sobre seguridad: Para proporcionar mecanismos mas fuertes y efectivos de seguridad, interoperabilidad con entidades externas tales como Internet y compatibilidad con los clientes existentes, Windows 2000 Server soporta una variedad de protocolos de seguridad de red.
Kerberos versión 5, un estándar de seguridad de Internet, es el protocolo preestablecido para la autenticación de red en Windows 2000 Server, También se soportan los siguientes:

*Protocolos basados en clave pública, incluyendo Secure Sockets Layer 3.0
*Autenticación de contraseña distribuida.
*Protocolo de Windows NT LAN Manager (NTLM) que utiliza Windows NT versión 4.0 y anteriores.

Duplicación: Dentro de cada dominio, se duplica el directorio en cada servidor que este ejecutando el active directory.Si el dominio contiene varios servidores de active directory (Conocidos también como controladores de dominio), se duplica el directorio a varios servidores. Cada uno de estos guarda y mantiene una copia completa del directorio del dominio.Los beneficios de la duplicación incluyen tolerancia a fallos, balance de carga y rendimiento mejorado.
El Active directory utiliza la duplicación multimaestra, que le permite cambiar información en cualquier servidor que contenga el directorio y copiar automáticamente los cambios a otros servidores.

Particiones de información: Con el active directory, el directorio de cada dominio guarda información solo acerca de los objetos ubicados en ese dominio, en lugar de utilizar un almacén masivo. El active directory permite el uso de varias particiones de directorio para la escalacion de compañías muy pequeñas a muy grandes.

Facilidad de ampliación del directorio: El active directory es totalmente ampliable, esto significa que puede añadir tipos de objetos nuevos al directorio y atributos nuevos a tipos de objetos existentes utilizando ya sea la herramienta del administrador de esquema del active directory o escribiendo un programa.

Integración con DNS: El active directory utiliza el sistema de nombres de dominios (DNS), un conjunto de protocolos y servicios que se utiliza a través de Internet y otras redes de TCP/IP. DNS proporciona registro de nombres y servicios de resolución de nombres a dirección, que permite la identificación de conexión de PC's y usuarios en redes TCP/IP.Dns permite el uso de nombres "amigables" de estructura jerárquica, por ejemplo DNS permites que se refiera a una PC por medio del un nombre como por ejemplo www.fca.unam.mx, en vez de poner la dirección ip de el equipo.
El active directory implementa un modelo de nombres de dominios y objetos basado en el sistema de nombres de dominio. Los nombres de dominio de Windows 2000 corresponden a los nombres preestablecidos del dominio DNS. También esta soportado el DNS dinámico, que permite a los servidores actualizar las base de datos DNS Mientras ejecutan el sistema operativo, El DNS dinámico se describe en el documento RFC 2136.

Interoperacion con otros directorios: El active directory soporta otros estándares de la industria, tales como la versión 2 y 3 del Lightweight Directory Access Protocol (LDAP), la interfaz del proveedor de servicios de nombres(NSPI) y el protocolo de transferencia de hipertexto (HTTP).LDAP es el protocolo central del Active directory, es un protocolo de servicio de directorio estándar de la industria que permite al active directory compartir información con cualquier otro servicio de directorio que soporte LDAP. Al soportar esos estándares, el active directory puede ampliar sus servicios a través de varios espacios de nombres y lidiar con información y recursos ubicados en Internet, otros sistemas operativos u otros directorios.

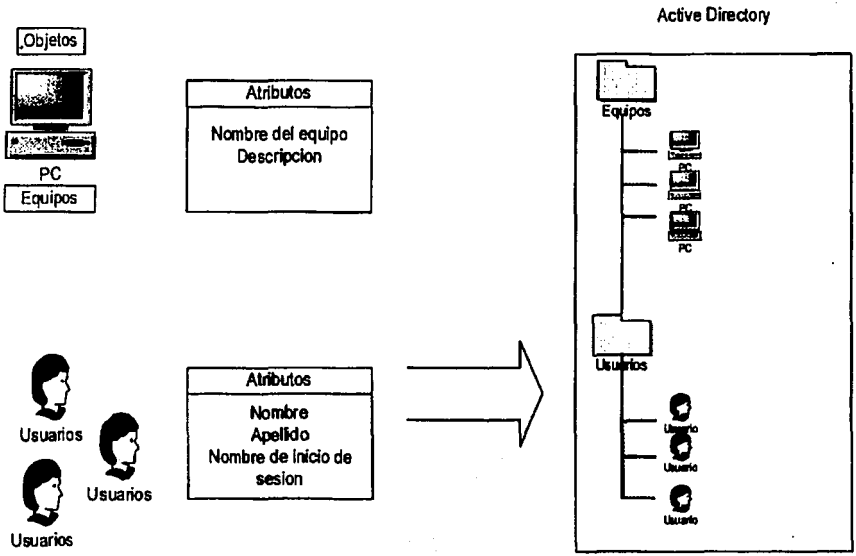
TECNOLOGIAS SOPORTADAS POR ACTIVE DIRECTORY.

TECNOLOGIA	FUNCION	REFERENCIA
DHCP	Administración de las direcciones IP de la red	RFC 2131
DNS, Dinamy Update	Administración de los Hostname	RFC 2052 y 2136
SNTP	Servicio de distribución de tiempo	RFC 1769
LDAP	Cliente de acceso a directorios	RFC 2251
LDAP'C	Directorio API's	RFC 1823
LDAP Stara Interchange Format (LDIF)	Sincronización de Directorio	Internet Engineering Task Force (IETF) Draft
LDAP	Esquema del Directorio	RFC 2247, 2252 y 2256
Kerberos 5	Autentificación	
X.509 v3 Certificates	Autentificación	ISO X.509
TCP/IP	Transporte de Red	RFC 791 y 793

3.4 ESTRUCTURA DE ACTIVE DIRECTORY.

Active Directory proporciona un método para el diseño de la estructura de directorios que corresponda a las necesidades de la organización.

Active Directory almacena información sobre los recursos de la red, al igual que sobre todos los servicios que permiten que la información se encuentre disponible y sea útil. Los recursos almacenados en el directorio, como pueden ser, datos de usuarios, impresoras, servidores, bases de datos, grupos, equipos, y directivas de seguridad, se denominan objetos.



Un objeto es un conjunto de atributos, diferenciado por un nombre, que representa un recurso de red.

Los atributos de los objetos son características de los objetos del directorio, por ejemplo, los atributos de una cuenta de usuario pueden incluir los nombres y apellidos del usuario, departamento y dirección de correo electrónico.
En Active Directory, los objetos se pueden organizar en clases, que son agrupaciones lógicas de objetos. Algunos ejemplos de clases de objetos son las cuentas de usuarios, grupos, equipos dominios y unidades organizacionales (OU-Organizational Unit).

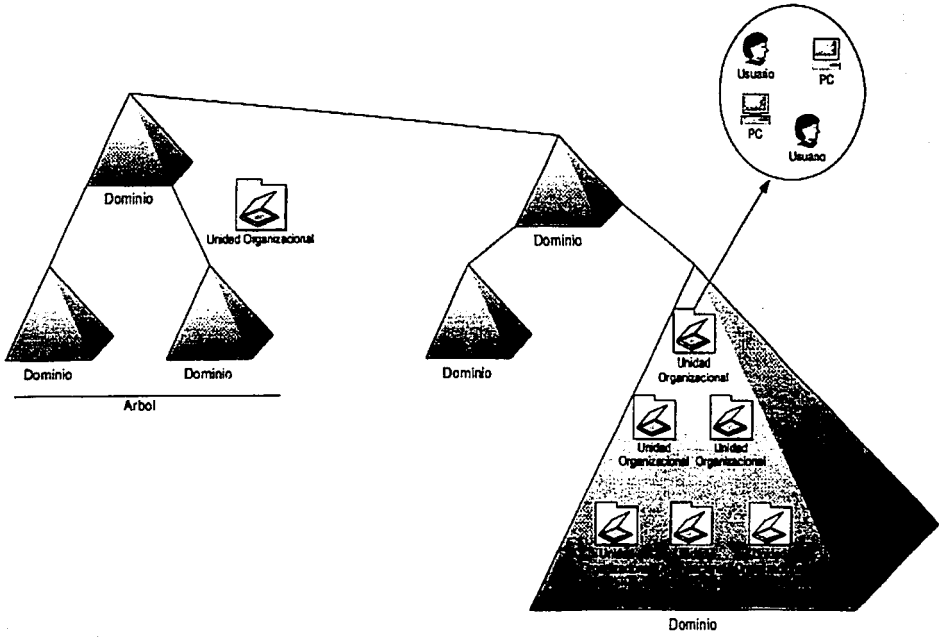
3.5 COMPONENTES DE ACTIVE DIRECTORY.

Active Directory utiliza componentes para construir una estructura de directorio acorde con las necesidades de una organización. Las estructuras lógicas de la organización se representan en los siguientes componentes: Dominio, Unidades Organizacionales, Árboles y Bosques. La estructura física de una organización esta representada por los siguientes componentes: Sitios y Controladores de Dominio. Active Directory separa completamente la estructura física de la lógica.

ESTRUCTURAS LOGICAS.

En Active Directory, los recursos se organizan en una estructura lógica que refleja la estructura lógica de una organización. Agrupar recursos lógicamente permite encontrar unos recursos por su nombre en lugar de por su localización física, por el hecho de agrupar recursos lógicamente, Active Directory hace transparente la estructura física a los usuarios.

DIAGRAMA ESTRUCTURA JERARQUICA LOGICA.



Bosque

DOMINIOS.

La unidad central de la estructura lógica de Active Directory es el dominio, que puede almacenar millones de objetos. Los objetos que se almacenan en un dominio son aquellos que se consideran "interesantes" para la red. Los objetos "interesantes" son productos que los miembros de la comunidad de la red necesitan para realizar su trabajo: impresoras, documentos, direcciones de correo electrónico, bases de datos, usuarios, y otros recursos. Todos los objetos de la red existen en un dominio, y cada dominio almacena información exclusivamente sobre los objetos que contiene.

Agrupar objetos en uno o mas dominios permite a la red reflejar la organización de la empresa, los dominios comparten las siguientes caracteristicas:

- Todos los objetos de la red pueden estar dentro de un dominio, aunque cada dominio almacena información referida exclusivamente a los objetos que contiene.

- Un dominio es un límite de seguridad, las Listas de Control de Acceso (ACL) controlan el acceso a los objetos del dominio, las ACL contienen los permisos asociados con los objetos que controlan los usuarios que pueden acceder aun objeto, así como los tipos de acceso que pueden realizar.

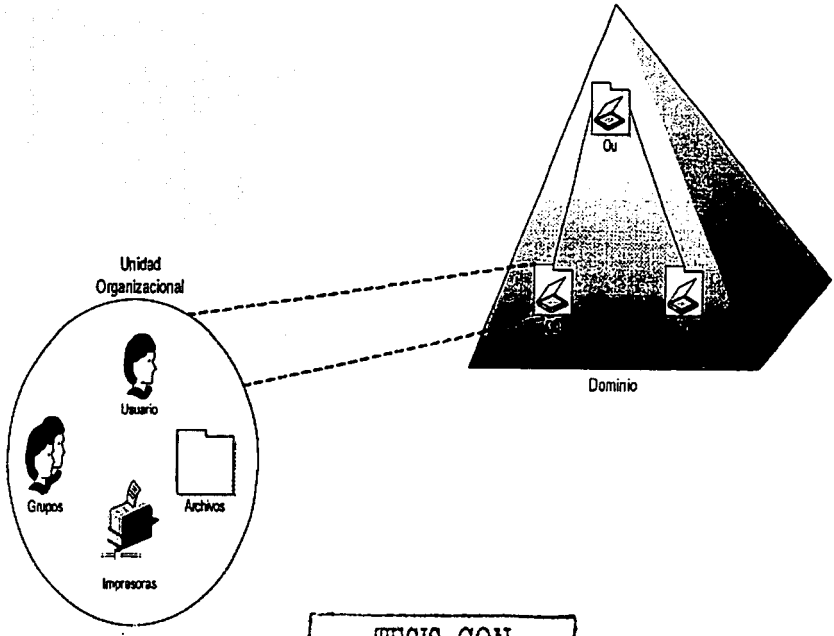
UNIDADES ORGANIZACIONALES.

Una Unidad Organizacional (OU-Organizational Unit) es un contenedor que se utiliza para organizar objetos dentro de un dominio en grupos administrativos lógicos que reflejan la estructura funcional de una organización. Una OU puede contener objetos tales como cuentas de usuario, grupos, equipos impresoras, aplicaciones, archivos compartidos, etc. y otras OU del dominio.

La jerarquía de una OU dentro de un dominio es independiente de la estructura jerárquica de la OU de otros dominios, cada dominio puede implementar su propia jerarquía de OU.

Las Ou pueden proporcionar una forma de manejar las tareas administrativas, ya que representan el punto de vista más pequeño de delegación para las autoridades administrativas, esto proporciona un método para delegar la administración de recursos y usuarios.

UTILIZACION DE UNIDADES ORGANIZACIONALES.



ÁRBOLES.

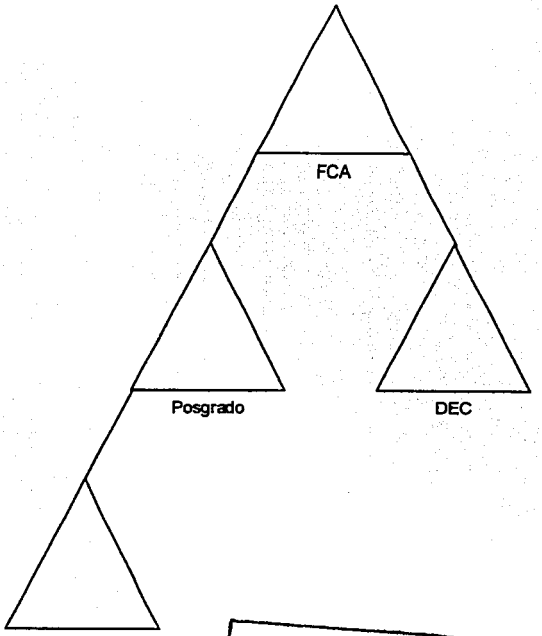
Un árbol es una agrupación o una ordenación jerárquica de uno o más dominios de Windows 2000 que se pueden crear añadiendo uno o más dominios secundarios a un dominio principal existente. Los dominios en un árbol comparten un espacio de nombres contiguo y una estructura jerárquica de nombre, los árboles comparten las siguientes características:

- Acorde con los estándares del Sistema de Nombres de Dominio (DNS), el nombre de dominio de un dominio secundario es el nombre relativo de ese nombre secundario agregado a ese dominio secundario agregado al nombre del dominio principal.

- Todos los dominios dentro de un mismo árbol comparten un esquema común, que es una definición formal de todas las clases de objeto que se pueden almacenar en el desarrollo de Active Directory.

- Todos los dominios dentro de un mismo árbol comparten un catalogo global que es el deposito central de información de los objetos del árbol.

ARBOL DE DOMINIO.



BOSQUES.

Un bosque es una agrupación o configuración jerárquica de uno o mas árboles de dominio distintos y completamente independientes entre si. Por consiguiente, los bosques tienen las siguientes características:

- Todos los árboles de un bosque comparten un esquema en común.

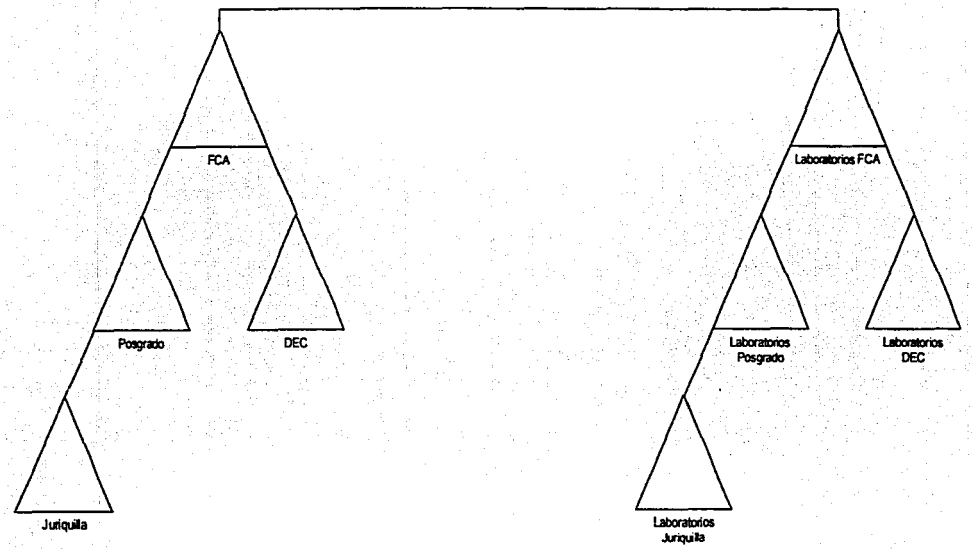
- Los árboles de un bosque tienen diferentes estructuras de nombre de acuerdo con sus dominios.

- Todos los dominios de un bosque comparten un catalogo común global.

- Los dominios de un bosque operan independientemente, pero el bosque permite la comunicación a lo largo de toda la organización.

- Existe una relación transitiva de confianza bidireccional entre los dominios y los árboles de dominio.

BOSQUE DE ÁRBOLES DE DOMINIO.



ESTRUCTURAS FISICAS.

Los componentes físicos de Active Directory son los sitios y los controladores de dominio, utiliza estos componentes para desarrollar una estructura de directorio que refleje la estructura física de una organización.

SITIOS.

Un sitio es una combinación de una o más subredes que utilizan direcciones IP conectadas por un enlace rápido y de alta fiabilidad que permite agrupar la mayor cantidad de tráfico posible. Típicamente un sitio tiene los mismos límites que una red de área local (Lan), cuando se agrupan subredes en una red, se deben combinar solamente aquellas subredes que tengan conexiones rápidas, fiables y baratas.

CONTROLADORES DE DOMINIO.

Un controlador de dominio es un equipo con Windows 2000 Server o Advanced Server que almacena una copia del directorio de dominio, dado que un dominio puede contener uno o más controladores de dominio, todos los controladores de dominio en un dominio tienen una copia completa de la porción de dominio del directorio.

Las funciones de un controlador de dominio son las siguientes:

- Cada controlador de dominio almacena una copia completa de toda la información de Active Directory para ese dominio, administra los cambios y replica esos cambios a otros controladores de dominio del mismo dominio.

- Los controladores de dominio de un dominio replican todos los objetos del dominio entre ellos, cuando se realiza una acción que provoca la actualización de Active Directory, se realiza en realidad un cambio en uno de los controladores de dominio, en ese caso, ese controlador de dominio replica el cambio a los demás controladores de dominio del dominio.

- Los controladores de dominio replican inmediatamente ciertas actualizaciones urgentes, tales como la eliminación de una cuenta de usuario.

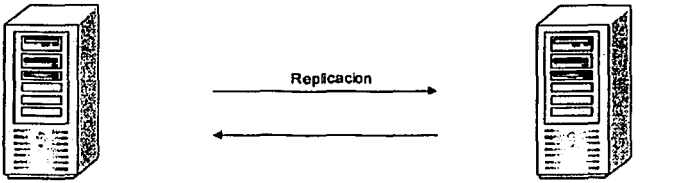
- Active Directory utiliza replicación multimaestro, en la cual ningún controlador de dominio es el maestro, en lugar de eso, todos los controladores de dominio de un dominio son iguales y contienen una copia de la base de datos del directorio en la que pueden escribir. Los controladores de dominio pueden mantener información diferente durante cortos espacios de tiempo hasta que todos los controladores de dominio han sincronizado los cambios.

- El hecho de tener más de un controlador de dominio provoca tolerancia a fallos. Si un controlador de dominio esta desconectado o falla otro controlador de dominio puede proporcionar todas las funciones necesarias.

- Los controladores de dominio administran todas las facetas de las interacciones de los usuarios en un dominio, como puede ser la localización de los objetos de Active Directory y la validación de los intentos de inicio de sesión por parte de los usuarios.

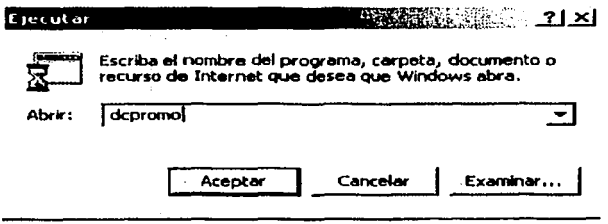
3.6 PROPUESTA.

Se propone la instalación de un controlador de dominio primario y su respaldo en un controlador secundario, esto en caso de que ocurra una falla en el controlador primario, entonces entrara en función el controlador secundario, ambos controladores de dominio estarán replicados conforme el siguiente diagrama.

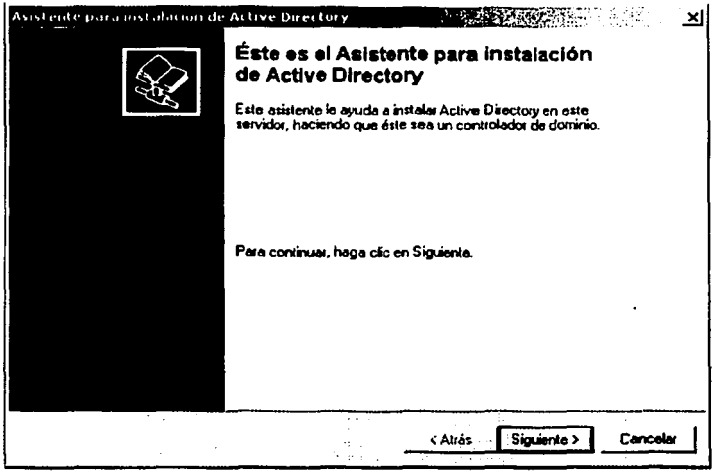


Para instalar active directory se seguirán los siguientes pasos:

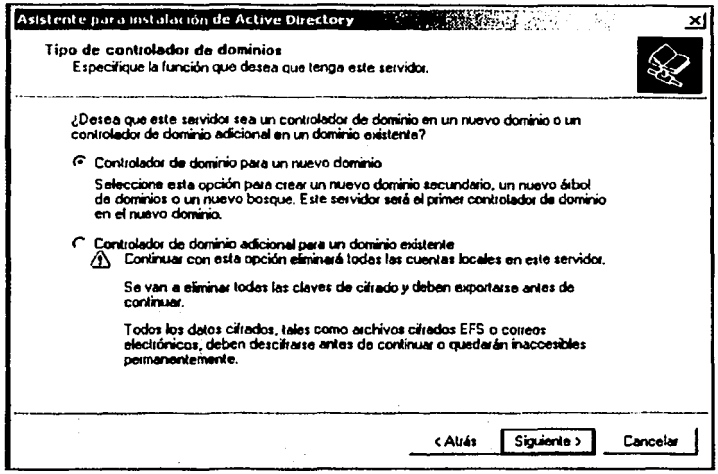
- Ir al menú inicio, ejecutar escribir la siguiente instrucción: dcpromo.



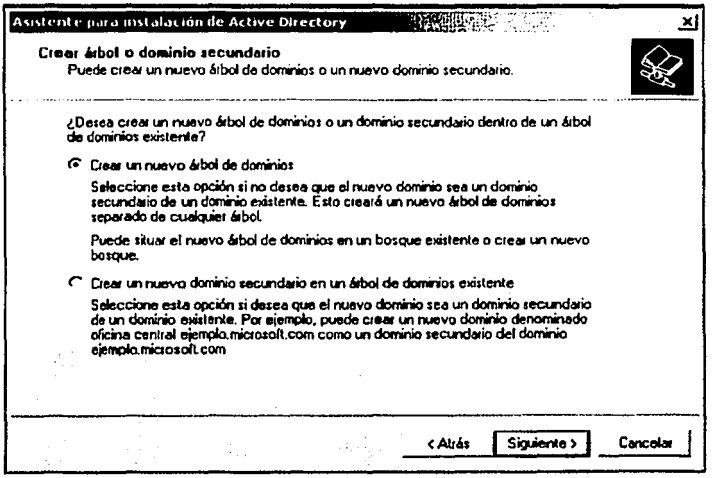
• Esta instrucción mandara a llamar al asistente de instalación de active directory y nos mostrara la siguiente pantalla.



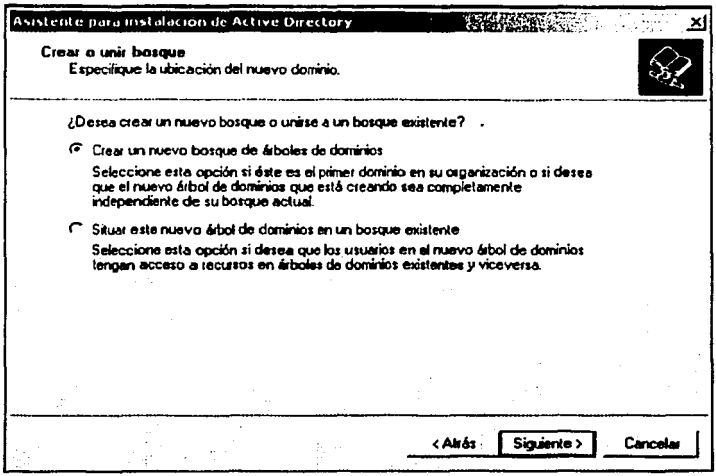
•Al dar clic en siguiente nos preguntara que deseamos hacer, si se va a instalar un nuevo controlador de dominio o si se va a agregar un controlador de dominio para uno existente, en este caso seleccionaremos la opción de un controlador de dominio nuevo.



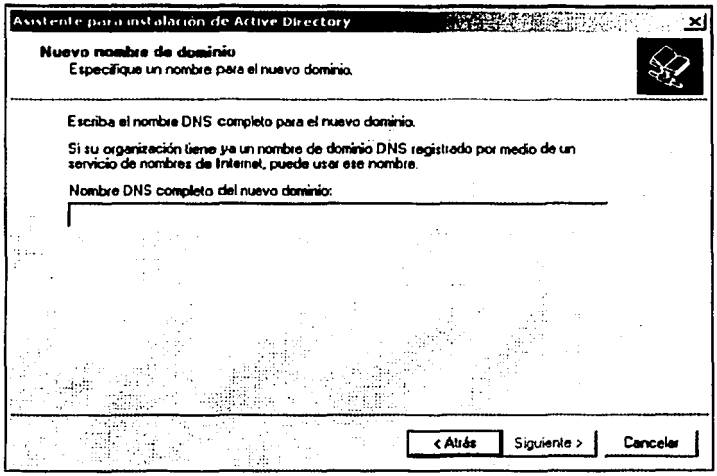
• Posteriormente se nos preguntara si vamos a crear un nuevo árbol de dominio o si se va a crear un nuevo árbol para un dominio existente, como vamos a levantar un dominio nuevo, se va a crear un árbol nuevo.



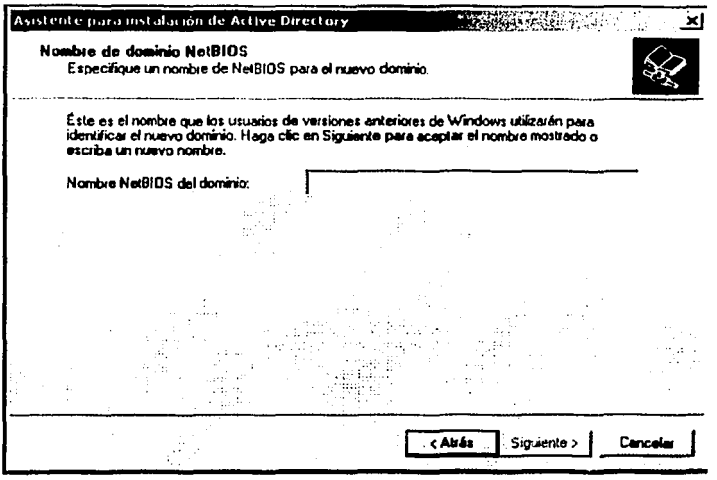
•Igualmente nos preguntara lo mismo sobre el bosque de árboles de dominio, y la opción a escoger será crear un nuevo bosque de árboles de dominio.



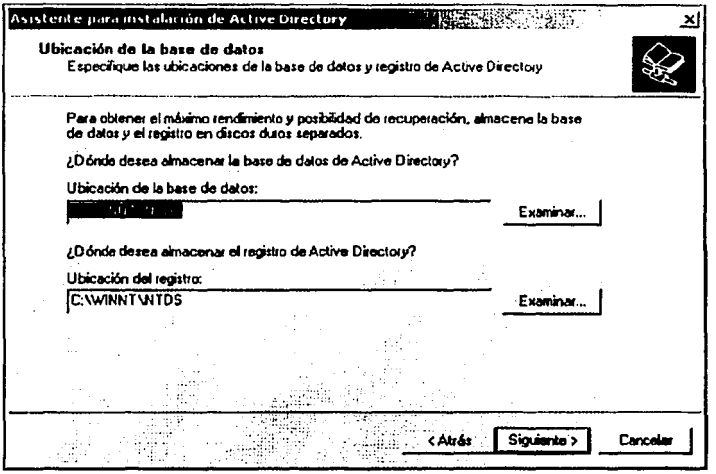
•Los siguiente será asignar un nombre de dns al dominio, en este caso le asignamos el nombre de laboratorios.



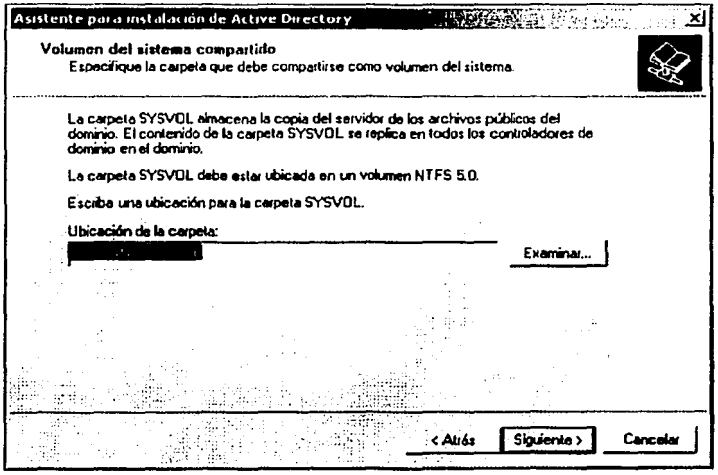
•Posteriormente se le asignara el nombre netbios del dominio, lo cual servirá para localizar al equipo en la red local.



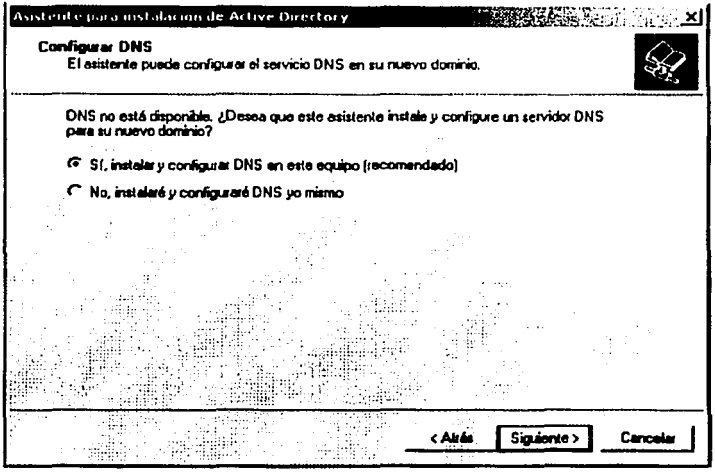
•Posteriormente se nos preguntara donde se desea almacenar la base de datos de active directory dejamos la opción por default que es C:\WINNT\NTDS.



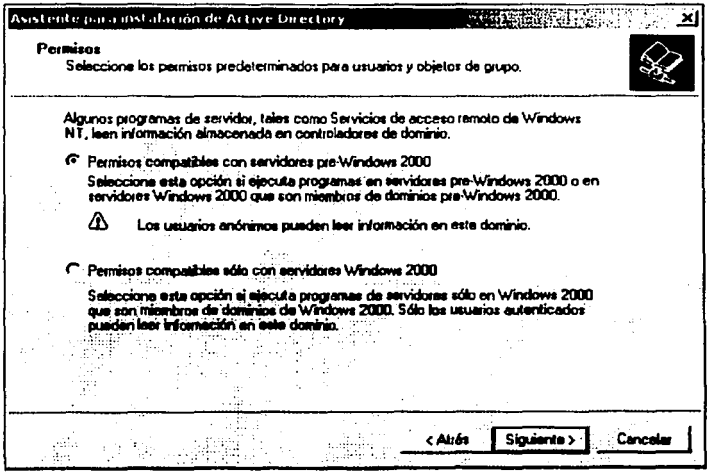
•Una vez que damos siguiente se nos preguntara don de se van a guardar los archivos públicos del dominio, la ruta donde se almacenaran estos es C:WINNT\SYSVOL.



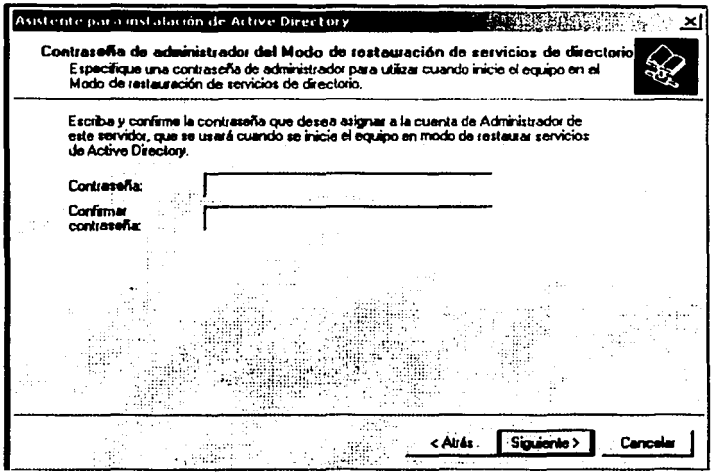
•Se nos preguntará si deseamos instalar y configurar los DNS, seleccionamos la opción si y damos clic en siguiente.



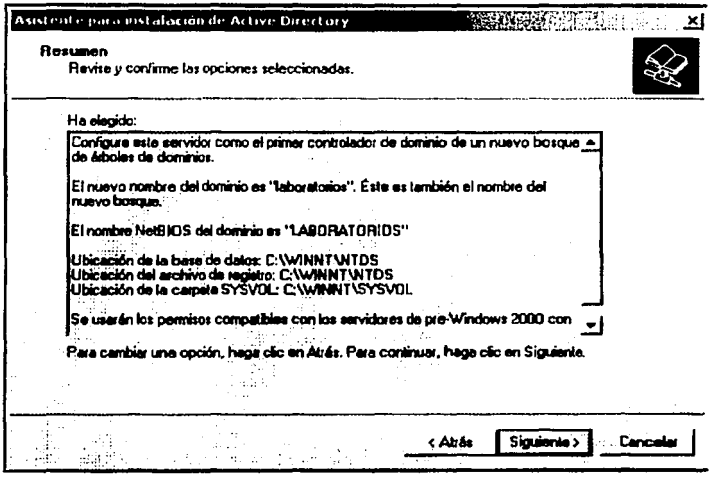
•Posteriormente se nos preguntara si deseamos la compatibilidad con servidores pre windows2000, esto por si se ejecutan programas en servidores pre windows2000, seleccionaremos la opción de solo servidores Windows 2000, ya que los clientes son Windows 2000.



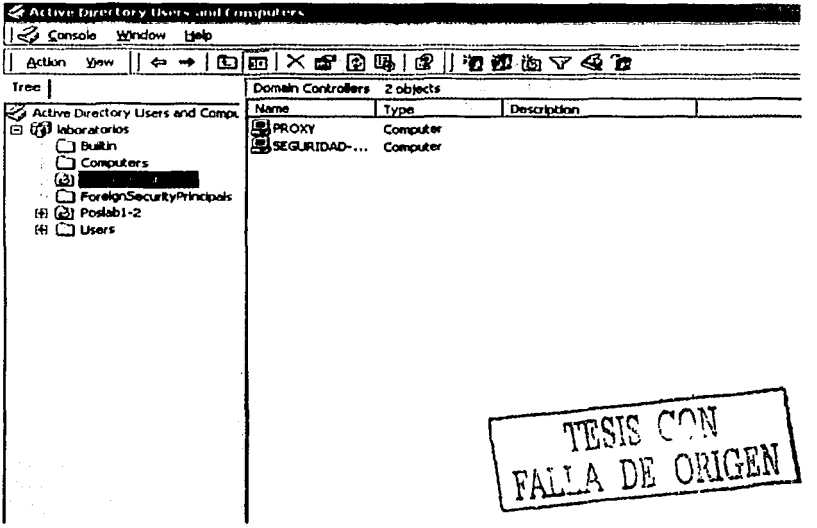
•Se nos pedirá también un password para el administrador del dominio.



•Con esto se finaliza la instalación de active directory.

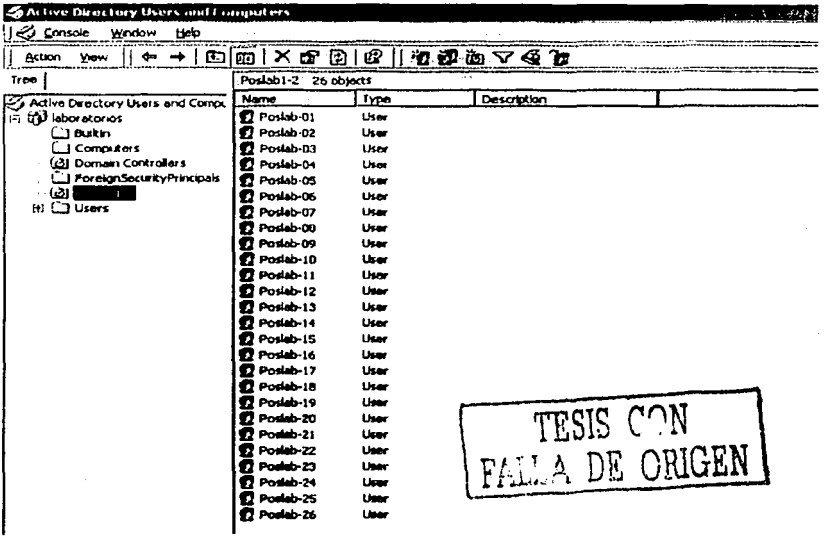


Una vez instalados los dos controladores de dominio con sus respectivos DNS, Active Directory en sus herramientas de administración de usuarios y computadoras(active directory users and computers)a la cual accederemos por medio del menú inicio programas, herramientas administrativas, lo presentara de la siguiente forma:

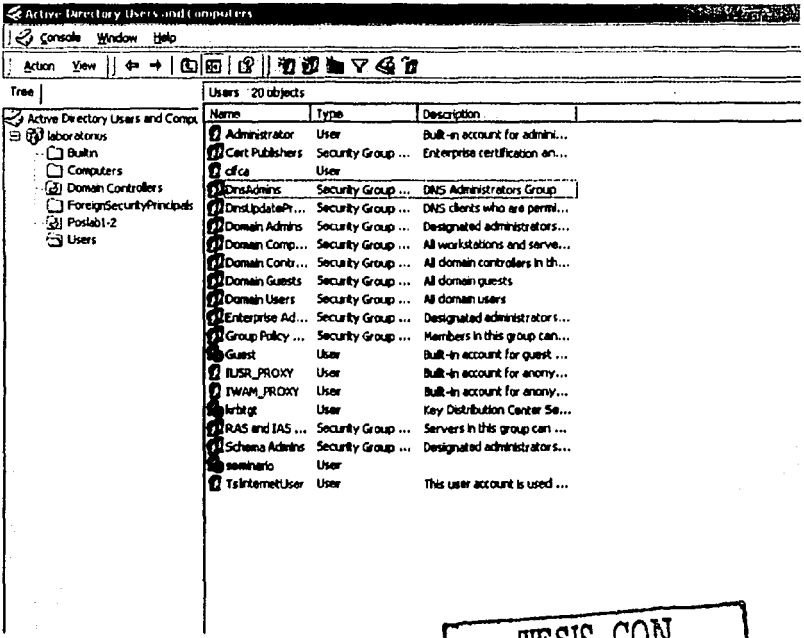


Como se pude observar en la imagen del lado izquierdo aparece el dominio principal, donde nos despliega una serie de carpetas, dentro de la carpeta domain controlers aparecen dos equipos, en este ejemplo llamados Proxy y seguridad-laboratorios, los cuales son los controladores de dominio, seguridad-laboratorios es el equipo que tiene el dominio principal y Proxy es donde esta el domino secundario, ambos dominios replicándose entre si.

Una vez instalados ambos controladores de dominio se procederá a la creación de la unidad organizacional, en este caso se creo una unidad organizacional para administrar los laboratorios 1 y 2 de Posgrado con sus respectivas cuentas de usuario.



Como se puede ver de lado izquierdo aparece la unidad organizacional (OU)Poslab1-2 y en el lado derecho aparecen las cuentas de los usuarios y el tipo de cuenta que es, además de que también se tienen las cuentas que el sistema genera .



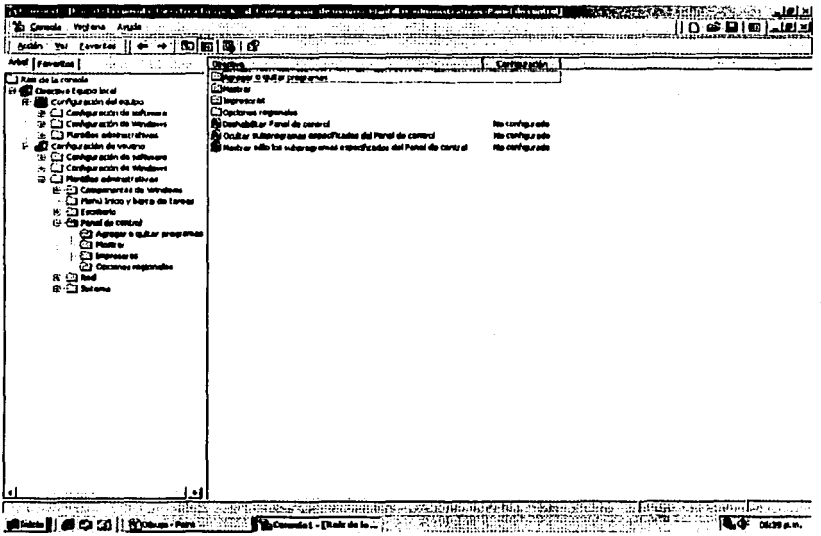
POLITICAS DE GRUPO.

Las políticas de grupo son colecciones de parámetros de configuración de equipos y usuarios que pueden vincularse a equipos, sitios, dominios y unidades organizacionales para definir el comportamiento de los escritorios de los usuarios.

Para tener un mejor control de los usuarios s propone crear una unidad organizacional por cada laboratorio, con el fin de facilitar su rápida ubicación y administración, como se ejemplifico anteriormente se tiene un a OU del laboratorio 1 y 2 de Posgrado.

Con estas políticas se crearan restricciones a los usuarios para evitar que modifiquen las configuraciones del equipo, para evitar problemas que se generan cuando los usuarios cambian la configuración del equipo, sobre todo la configuración de la red.

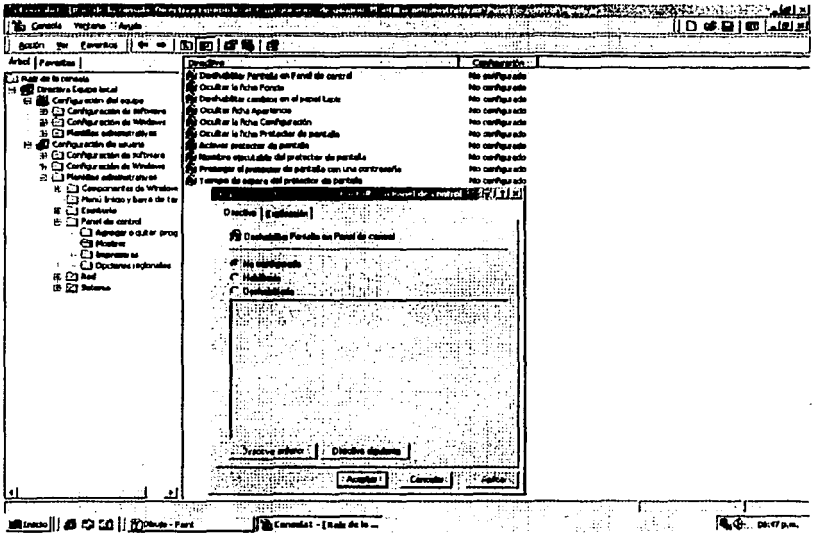
Un ejemplo de políticas nos lo muestra la siguiente imagen:



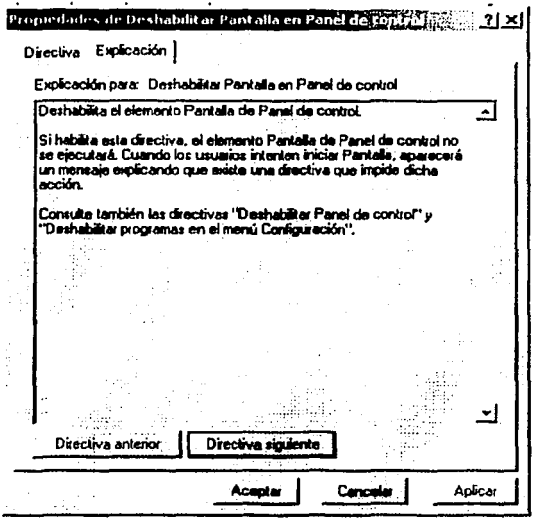
En esta imagen se pude apreciar que de el lado derecho donde se encuentran lo que son las plantillas administrativas, don de vienen políticas ya preestablecidas, aparecen distintas carpetas, se elegirá una dependiendo de la política que vayamos a aplicar, en este caso se presenta las de el panel de control, donde de el lado derecho se muestra las políticas disponibles para el panel de control, se seleccionara una y se aplicara, para evitar que los usuarios pueden hacer una modificación.

Como ejemplo de administración de políticas tenemos lo siguiente: se va a deshabilitar el panel de control para que los usuarios no puedan desinstalar algún programa ni modificar alguna configuración del hardware o del sistema.

Nos vamos a lo que son las plantillas administrativas a la parte que dice panel de control, seleccionamos la carpeta mostrar y seleccionamos la política que dice deshabilitar panel de control, nos aparecerá los siguiente



Posteriormente si queremos una explicación de lo que trata la política, basta dar un clic en la pestaña que dice explicación para tener la función de la política.

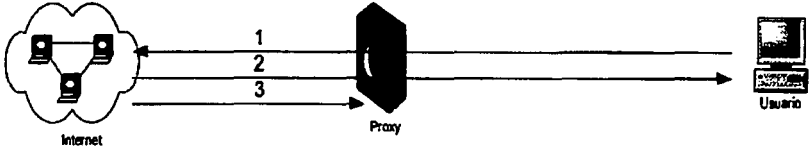


PROXY.

Para este proyecto se cuenta asociado un Proxy basado en linux red hat versión 8 implem,entado por el Departamento de telecomunicaciones el cual restringirá el acceso a páginas no autorizadas como por ejemplo paginas pornográficas, descarga de software no autorizado.

El funcionamiento del Proxy se muestra en el siguiente diagrama.

FUNCIONAMIENTO DEL PROXY.



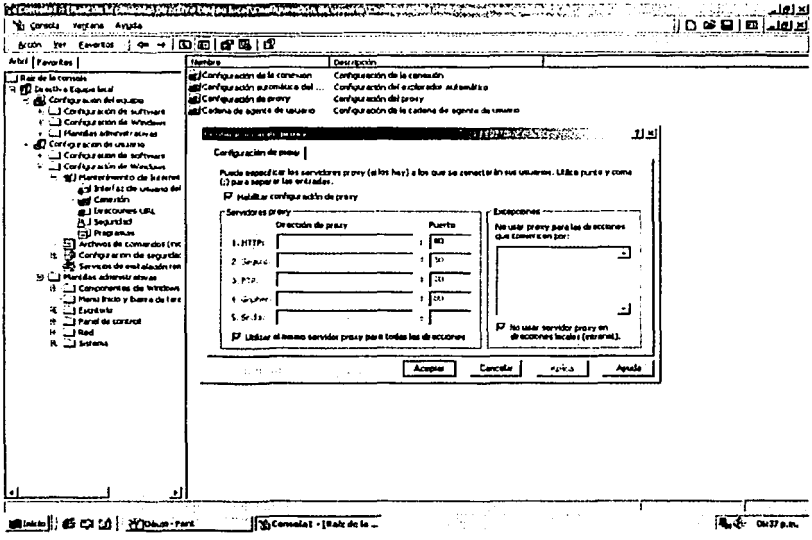
1.- El cliente hace una petición a un servidor Web para visualizar cierta página, como ejemplo www.fca.unam.mx, la petición pasa a través del Proxy, el cual busca si se encuentra dentro de la lista de sitios no permitidos.

2.-Al no encontrarlo dentro de la lista de sitios no permitidos autoriza la petición de el cliente y este puede visualizar la pagina.

3.- En caso de que el cliente solicitara una petición a www.xxx.com ocurre el paso 1, al encontrarlo dentro de la lista de sitios no permitidos no autoriza la visualización de la pagina.

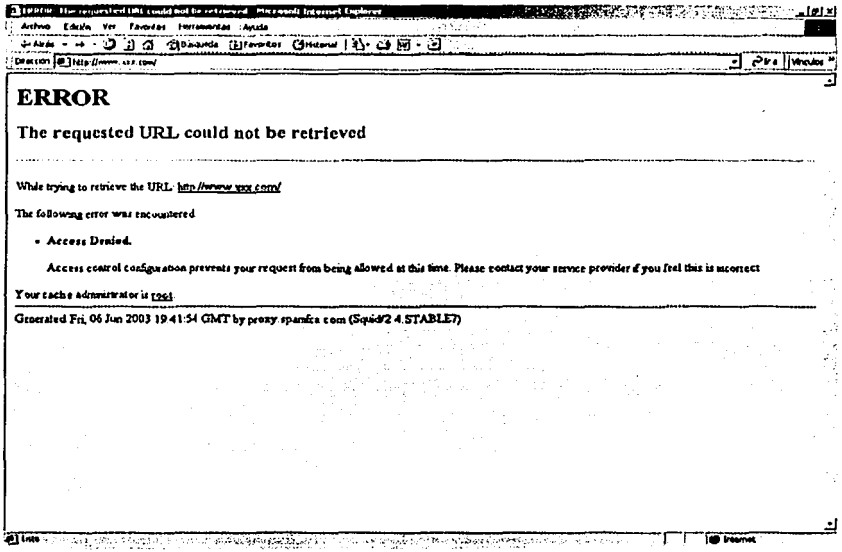
La configuración de la política donde se incluirá el Proxy se configura de la siguiente manera:

Dentro de las directivas de usuario en la configuración de Windows se seleccionara la carpeta mantenimiento de Internet, de ahí se seleccionara la carpeta conexión y dentro de las opciones que se presentan seleccionaremos configuración del Proxy, la cual nos presentara la siguiente ventana.



en la cual colocaremos la dirección IP del Proxy, así como el puerto.

Cuando el usuario trate de acceder a una página prohibida le aparecerá el siguiente mensaje



Una vez que se tienen definidas las políticas que se implementaran, se procederá a la creación de un perfil de usuario, el cual abarcara desde restricciones en la configuración del hardware del equipo, así como restricciones en el sistema operativo.

El perfil propuesto es el siguiente:

Hardware

Política	Función
Habilitar el password del Bios	Evitar que los usuarios puedan modificar cualquier configuración del hardware, así como de los demás dispositivos físicos.
Deshabilitar el booteo de CD y disquete	Evitar que el usuario pueda dañar el sistema operativo, así como prevenir que pueda utilizar cualquier programa para franquear contraseñas.

En cuanto a las políticas de Active Directory aplicadas por medio del dominio estarán las siguientes:

Política	Función
Restricción para agregar complementos en la consola de administración de Microsoft.	Evitar que el usuario pueda crear restricciones y aplicarlas al equipo, ocasionando que pueda bloquearse el acceso al mismo, o alguna de las funciones.
Remover Ejecutar del menú inicio	Evitar que el usuario pueda ejecutar comandos no autorizados.
Remover red y conexiones telefónicas.	Evitar que el usuario pueda modificar la

	configuración de la red.
Remover propiedades del menú contextual de mi PC	Evitar que el usuario pueda modificar alguna opción como lo son los perfiles de hardware, perfiles de usuario o cambiar la identificación de red del equipo.
Deshabilitar el Panel de Control	Evitar que el usuario pueda desinstalar software y componentes de Windows.
Deshabilitar el protector de pantalla protegido con contraseña.	Evitar que el usuario ponga contraseña a los protectores de pantalla.
Prohibir el acceso a las propiedades de la configuración Lan	Evitar que el usuario pueda modificar la configuración establecida, así como agregar o quitar protocolos de red.
Prohibir el acceso al asistente para conexión de red.	Evitar que el usuario pueda crear conexiones que puedan crear conflicto en los servidores.
Deshabilitar bloqueo del equipo.	Evitar que el usuario deje bloqueado el equipo.
Deshabilitar cambiar password.	Evitar que el usuario cambie la contraseña de usuario, con el fin de proteger los equipos.
Habilitación de Proxy para todos los usuarios.	Evitar que los usuarios pueden acceder a pagina pornográficas, de juegos, etc.
Deshabilitar el escritorio activo.	Evitar que los usuarios puedan poner cualquier imagen como fondo de escritorio.

Se recomienda las deshabilitacion de los siguientes servicios:

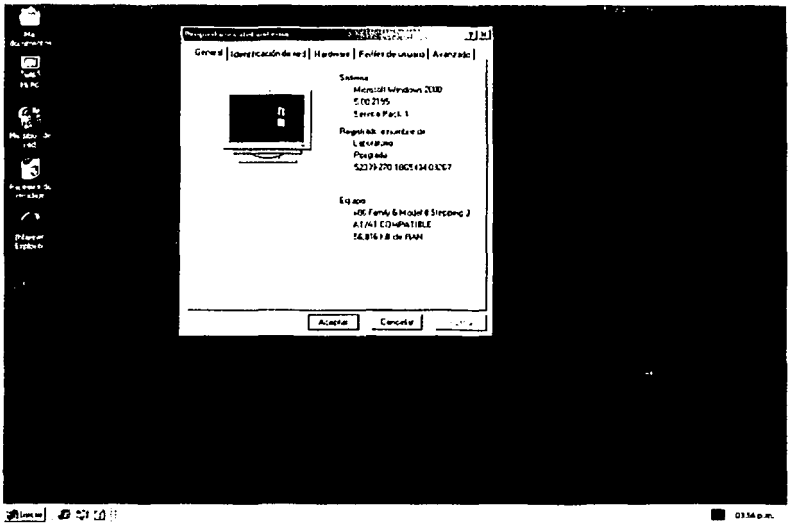
- Mensajero.

Para hacer que un cliente pueda logearse al dominio se tiene que realizar lo siguiente:

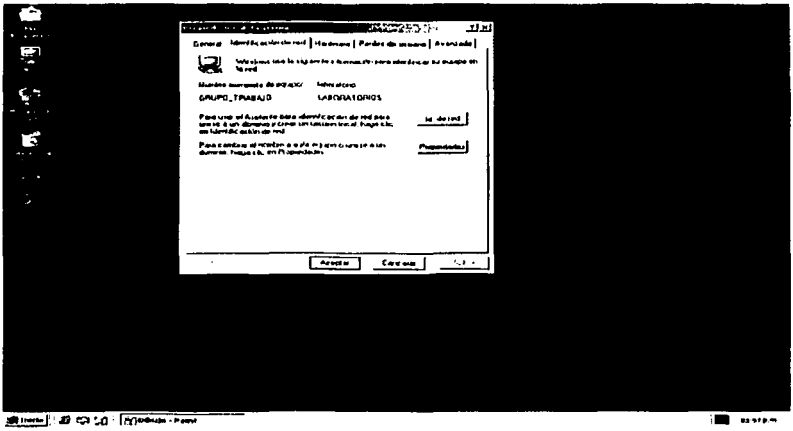
- Solicitar la cuenta con el administrador del dominio.

Una vez que se tiene la cuenta y la contraseña, en el cliente se realizara lo siguiente:

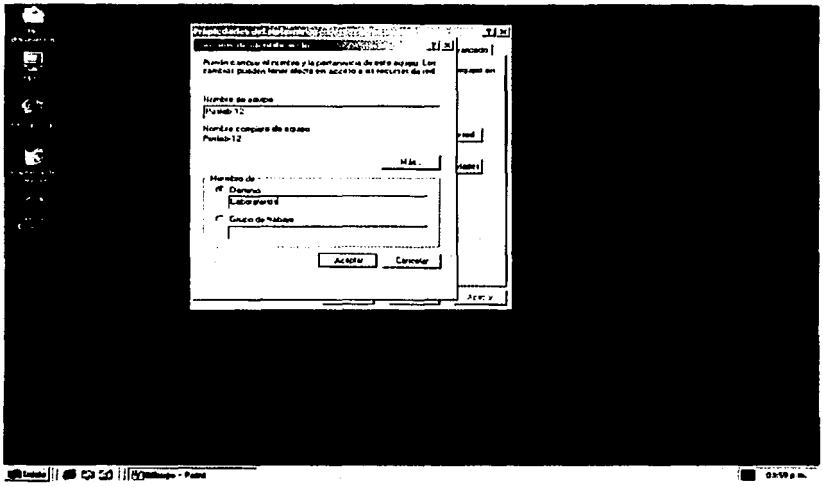
- En Mi PC se dará un clic derecho y se seleccionar propiedades.
- Una vez en propiedades seleccionaremos la pestaña de identificación de red.



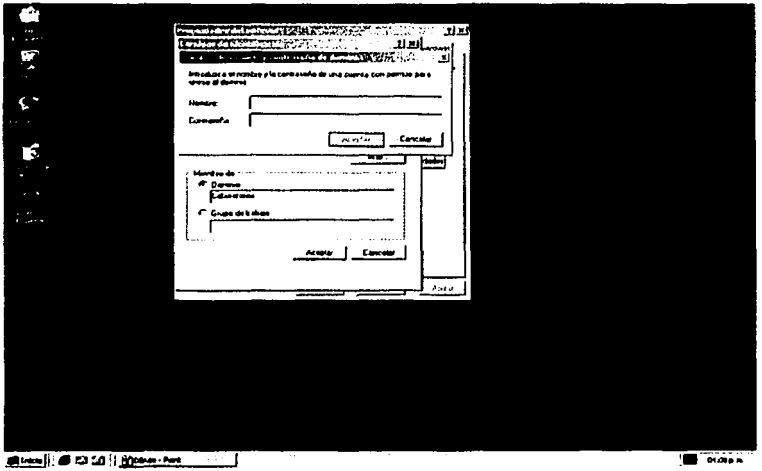
- Una vez en la opción de identificación de red seleccionaremos la opción propiedades.



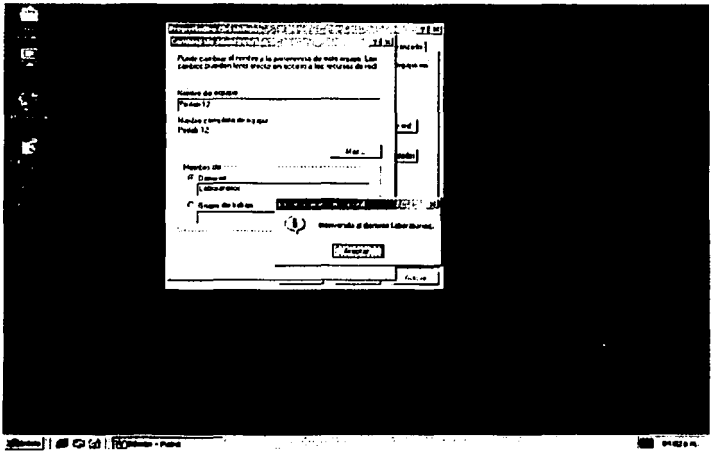
- Una vez que seleccionamos la opción propiedades aparecer la opción de nombre del equipo, donde se colocar el nombre del equipo, y en la opción donde dice miembro de, se seleccionara la opción dominio y el nombre del dominio es Laboratorios.



- Una vez colocados los datos antes mencionados, se dará un clic en aceptar y se nos pedirá el nombre de usuario y la contraseña del mismo.

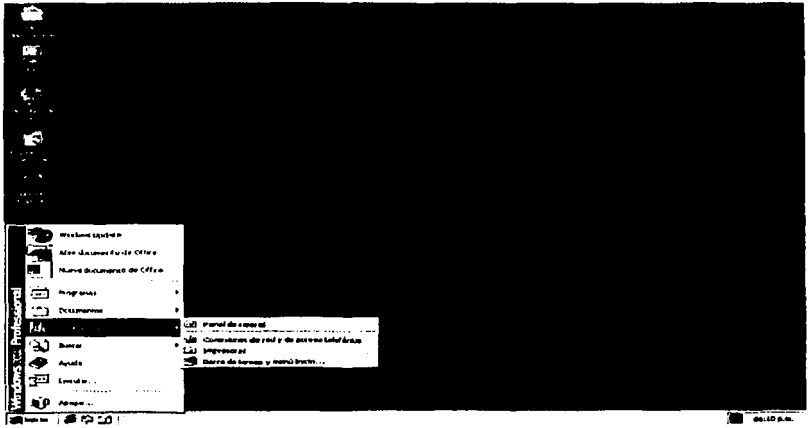


- Ya validados los datos nos aparecerá un mensaje de bienvenida.



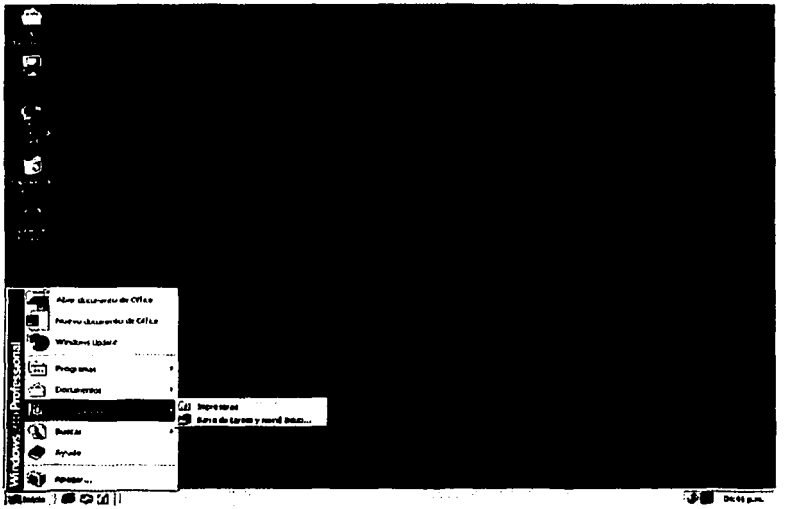
- Damos aceptar y reiniciaremos el equipo para que los cambios tengan efecto.

Antes de logear la PC con el dominio no se tenía ninguna política aplicada, como lo muestra la siguiente imagen:



Aquí podemos apreciar que están el panel de control, el asistente para redes y acceso telefónico, y la opción ejecutar.

Una vez que se han aplicado el perfil de usuario del domino se vera lo siguiente:



Desaparece el panel de control, el asistente para redes y acceso telefónico, así como la opción ejecutar.

3.7 TCO (COSTO TOTAL DE PROPIEDAD).

El TCO *(total cost of ownership)* es un modelo integral que ayuda a los administradores de sistemas empresariales a comprender y controlar los costos presupuestales (directos) y no presupuestales (indirectos) en los que incurre la propiedad y uso de un componente de tecnología durante todo su ciclo de vida. Un buen modelo de TCO ayuda a resaltar cuestiones actuales, justificar la necesidad de cambios y a generar una retroalimentación progresiva acerca de la administración del costo.

APLICACIÓN DE UN MODELO DE TCO.

El modelo TCO del GartnerGroup es uno de los esquemas más completos para calcular el costo total de la propiedad (TCO). Al emplearlo con las nuevas herramientas de computación desarrolladas por GartnerGroup (TCO Manager for Distributed Computing and TCO Analyst for Distributed Computing), una compañía puede simular un TCO típico para clase de negocio o industria particular, comparar los costos reales contra los típicos y simular una variedad de planes de mejoramiento. Existen más de 70 áreas detalladas dentro de las siete categorías principales de costo del Modelo TCO.

El modelo TCO de GartnerGroup utiliza dos principales categorías para organizar los costos:

Costos (presupuestados) directos: que son el capital, honorarios, costos de mano de obra generados por el departamento, o por el personal de sistemas

contratado para prestar servicios y soluciones para la organización. Dichos costos incluyen los gastos de capital, administración de sistemas, soporte, costos de trabajo de desarrollo, honorarios externos, adquisiciones, capacitación, viajes, mantenimiento, soporte y honorarios de comunicación. Los costos directos buscan regular y capturar todos los gastos directos relacionados con los clientes, servidores, periféricos y la red dentro de un ambiente de computación distribuida.

Costos indirectos (sin presupuestar): evalúan el capital y la eficiencia de administración del área de sistemas cuando brinda servicios requeridos por los usuarios finales. Si la administración y las soluciones en sistemas son eficientes, es menos probable que los usuarios finales tengan necesidad de buscar apoyo, tanto por sí mismos como en línea, o de tener tiempos muertos. Si la administración y las soluciones son ineficientes, los usuarios finales tendrán que invertir más tiempo en soporte, ya sea que ellos mismos resuelvan sus problemas o que busquen asesoría, y esto tendrá un impacto en la organización, pues generará más tiempo muerto.

Esas categorías utilizadas en el Modelo TCO GartnerGroup tienen los siguientes componentes:

Costos directos (presupuestados) – miden los gastos directos hechos por una organización en el área de sistemas (capital, mano de obra y honorarios).

- Hardware y software – gastos de capital y honorarios por renta de servidores, computadoras cliente (tanto de escritorio como portátiles), periféricos y el sistema de red

- Administración – la red directa, el sistema y el personal administrativo encargado del manejo del almacenamiento, horas y costos de actividad, así como los honorarios por servicios profesionales externos.

- Soporte – el número de horas y costo del departamento de soporte técnico, mediciones de desempeño del departamento de soporte técnico, honorarios y trabajo de capacitación, adquisiciones, viajes, contratos de mantenimiento/soporte y mano de obra indirecta.

- Desarrollo – el diseño de la aplicación, desarrollo, verificación y documentación, incluyendo el desarrollo de nuevas aplicaciones, personalización y mantenimiento.

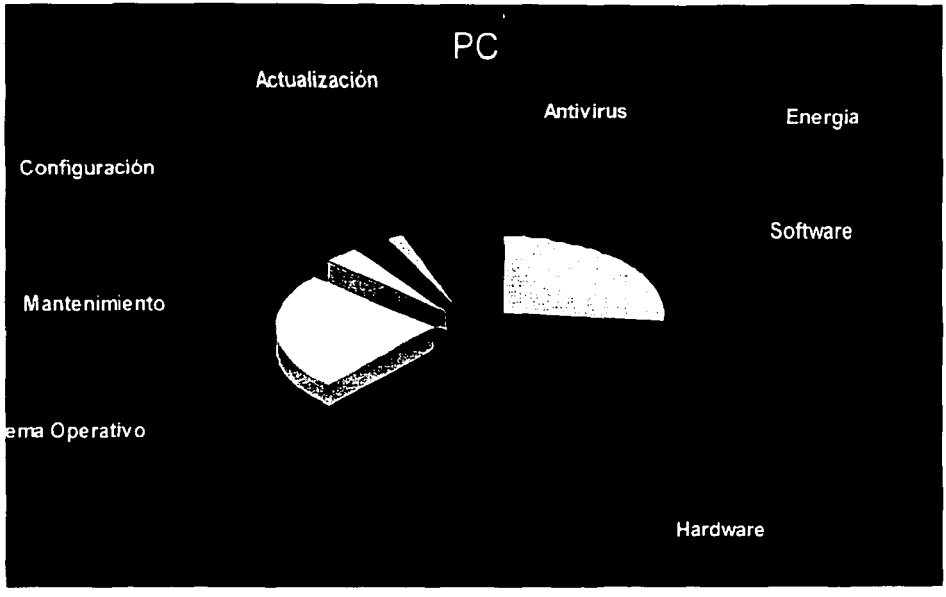
- Cuotas de comunicaciones– los gastos de comunicación entre computadoras a través de las líneas arrendadas, acceso remoto, acceso al servidor, así como los gastos WAN asignados.

Costos indirectos (no presupuestados) – mide el capital y eficiencia de la administración del área de sistemas sobre los servicios prestados a los usuarios finales.

- Usuario final del área de sistemas – el costo que absorben los usuarios finales al buscar soporte por sí mismos o con sus compañeros de trabajo, en lugar de depender de los canales de soporte del área de sistemas, capacitación formal de los usuarios finales, aprendizaje casual (capacitación informal) y desarrollo individual de aplicaciones.

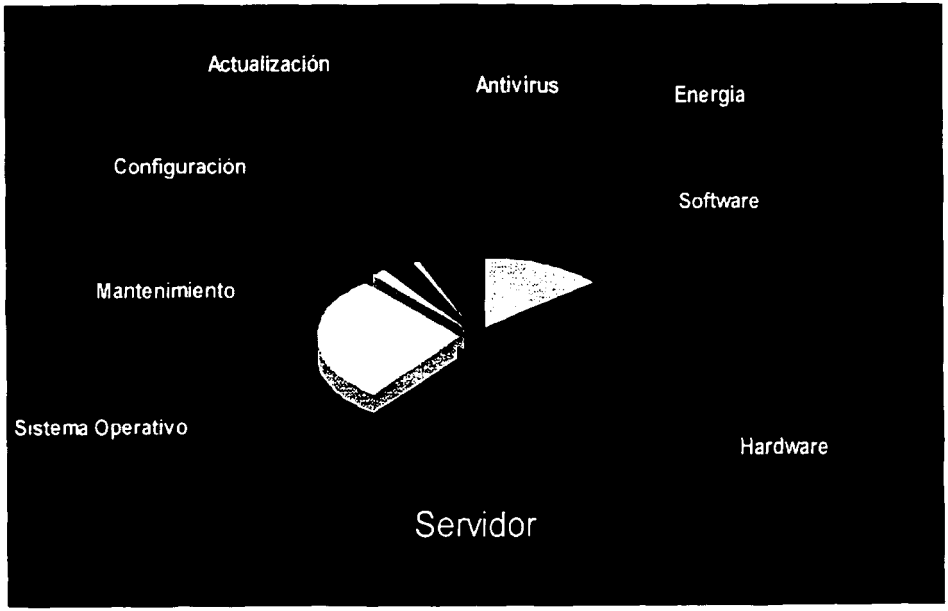
Tiempo sin sistema – la pérdida de productividad ocasionada por la falta de disponibilidad (planeada o inesperada) del sistema de red, del sistema o de las aplicaciones, evaluada en términos de salarios perdidos (productividad perdida).

TCO POR PC.



	Software	Hardware	Sistema Operativo	Mantenimiento	Configuración	Actualización	Antivirus	Energia
Pesos	3900	5000	3600	500	400	250	800	3.08

TCO POR SERVIDOR.



	Software	Hardware	Sistema Operativo	Mantenimiento	Configuración	Actualización	Antivirus	Energia
Pesos	3900	13000	8000	500	800	250	1600	7.08

CONCLUSIONES.

El desarrollo e implementación de este proyecto redujo los reportes recibidos por el CERT-UNAM.

Esto se logró gracias al diseño e implementación de las herramientas, como fue el Active Directory y de los perfiles de usuario.

La razón principal del uso de la plataforma Windows 2000 se debe a la amplia infraestructura de operación de red y servicios de directorio proporcionados por Windows, estas características explicadas dentro de la estructura de este proyecto fueron la parte fundamental del mismo así como la implementación de la herramienta y contar con una red basada en su mayoría con Windows 2000.

Uno de los puntos contemplados para la elección de la plataforma fue el TCO(Costo Total de Propiedad), que es donde se va a tomar en cuenta el costo por el uso de un componente tecnológico durante su ciclo de vida, el TCO por implementar este proyecto es bajo, dado que el personal del área de Telecomunicaciones esta capacitado para el manejo de dicha plataforma, reduciendo así de gran manera el costo por capacitación, y en lo que respecta al mantenimiento el costo es reducido ya que el sistema automáticamente avisa cuando se requiere una actualización.

Cuestiones como la seguridad del sistema se tomaron en cuenta y van implícitas con el mismo sistema operativo.

Los laboratorios de computo que son parte importante de nuestra vida académica, tendrán con la implementación de este proyecto una mejor administración y control de los mismos, logrando así una mayor eficiencia y cumpliendo al máximo su objetivo que es el de apoyar a los académicos y a los alumnos.

GLOSARIO

Glosario.

A

Acl Véase lista de control de acceso.

Active Directory Servicio de directorio de Windows 2000 Server y Advanced Server. Almacena información de objetos de una red y facilita el acceso a la misma a los usuarios y administradores. Active Directory concede a los usuarios acceso a cualquiera de los recursos permitidos de la red utilizando un único proceso de acceso. Proporciona a los administradores de la red una vista jerárquica e intuitiva de la red y un único punto de administración de todos los objetos de la red.

Atributo Información que indica si un archivo es de solo lectura, oculto, listo para archivo (copia de seguridad), comprimido o cifrado y si su contenido se debería indicar para realizar una búsqueda rápida.

Autenticación Proceso por el que un sistema valida la información de acceso de un usuario. El nombre de usuario y su contraseña se comparan con la lista de autorizaciones. Si el sistema detecta que coinciden se concede un acceso que abarca la lista de permisos especificados

para dicho usuario. Cuando un usuario accede a una cuenta de un equipo con Windows 2000 Profesional, la autenticación se produce en la estación de trabajo. Cuando el usuario accede a una cuenta de dominio, la autenticación la realiza cualquier servidor de dicho dominio.

B

Backbone Parte de una red que actúa como una ruta primaria para el tráfico que, con mayor frecuencia, proviene de otras redes y se destina a las mismas.

C

Catalogo Global Controlador de dominio que contiene una replica parcial de cada dominio en Active Directiory. Un catalogo global contiene una replica de todos los objetos en Active Directory, pero con un numero limitado de atributos de cada objeto. El catalogo global almacena los atributos que se utilizan con mayor frecuencia el las operaciones de búsqueda (como el nombre y apellidos de un usuario) y los atributos necesarios para ubicar la replica completa del objeto. El sistema de replica de

Active Directory construye el catalogo global incluyen el conjunto base definido por Microsoft. Un administrador puede definir propiedades adicionales para adaptarlo a las necesidades de su instalación.

Concentrador (HUB) Véase Hub.

Controlador de dominio En Windows 2000 Server y Advanced Server, un equipo que ejecuta Windows 2000 Server o Advanced Server y administra el acceso de usuarios a la red, lo que incluye el acceso, autenticación y acceso al directorio y recursos compartidos.

Cuenta de usuario Registro que consiste en toda la información que define un usuario de Windows 2000.Incluye el nombre del usuario y su contraseña para el acceso, los grupos a los que pertenece la cuenta del usuario y los derechos y permisos para utilizar el equipo y la red y acceder a sus recursos. Para Windows 2000 Profesional y servidores miembro, las cuentas de usuario se administran con la consola de Usuarios locales y grupos. Para los controladores de dominio de Windows 2000 Server y Advanced Server las cuentas de usuario se administran con la consola usuarios y equipos de Active Directory.

D

DHCP Véase Protocolo de configuración dinámica de host.

Dirección IP Dirección de 32 bits para identificar un nodo en un conjunto de redes Ip. Cada nodo de un conjunto de redes de IP debe tener una dirección única, que consta de un identificador de red y un identificador de host. Una dirección se suele representar en notación decimal con puntos, con el valor decimal de cada octeto separado por puntos, por ejemplo 132.248.18.50.

DNS Véase Sistema de nombres de dominio.

Dominio Una colección de equipos que define el administrador de una red que comparten una base de datos directorio común. Un dominio tiene un nombre único y proporciona acceso a las cuentas de usuario y grupos centralizadas mantenidas por el administrador del dominio. Cada dominio tiene sus propias directivas y relaciones de seguridad con otros dominios y representa una frontera de seguridad de una red de equipos con Windows 2000.

E

Ethernet Especificación de Red de Área Local (Lan) de banda base, inventada por Xerox Corporation y desarrollada

conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes ethernet utilizan CSMA/CD y se ejecutan en una serie de tipos de cable a 10, 100 y 1000 Mbps. Ethernet se asemeja a la serie de estándares IEEE 802.3.

H

Hub Dispositivo que sirve como centro de una red con topología en estrella y conecta las estaciones finales. En ethernet e IEEE 802.3, un repetidor multipuesto ethernet, a veces denominado concentrador.

K

Kerberos V5 Un protocolo de seguridad estándar de Internet para manejar la autenticación de usuarios o la identidad de un sistema. Con Kerberos V5, las contraseñas se envían cifradas por las líneas de las redes, no como texto plano.

L

Lista de control de acceso Mecanismo para limitar el acceso a la información, a ciertos elemento o a ciertos controles, según la identidad del usuario o su pertenencia a determinados grupos predeterminados. El control de acceso lo suele

utilizar el administrador del sistema para controlar el acceso de los usuarios a los recursos de la red, tales como servidores, directorio y archivos, y se suele implantar mediante la concesión de permisos a los usuarios y los grupos para acceder a objetos concretos.

O

Objeto Una entidad como un archivo, una carpeta, una carpeta compartida, una impresora o un objeto de Active Directory descrito por un conjunto de atributos distintos, cada uno con un nombre.

P

Protocolo de configuración dinámica de host Protocolo del servicio de Protocolo de control de Transmisión/Protocolo de Internet (TCP/IP) que ofrece la configuración de concesión dinámica de direcciones IP de host y distribuye los parámetros de configuración a los clientes de red. DHCP proporciona una configuración de red TCP/IP segura, fiable y simple, previene los conflictos de direcciones y ayuda a conservar el uso de direcciones IP cliente de la red. DHCP usa un modelo

cliente/servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes con DHCP pueden solicitar y obtener temporalmente una dirección IP de un servidor de DHCP durante el proceso de inicio de red.

Protocolo de control de transmisión/Protocolo de Internet Conjunto de protocolos de red usados en Internet para la comunicación a través de redes compuestas por arquitecturas de distinto hardware y distintos sistemas operativos.TCP/IP incluye estándares sobre como se comunican los equipos y convenios sobre la conexión de redes y del enrutamiento del trafico.

Proxy Es un servidor muy particular que se encarga de centralizar el tráfico entre Internet y una red independiente, de manera que evita que cada una de las computadoras que conforman esa red independiente dispongan de manera innecesaria una conexión directa a Internet. Además utiliza mecanismos de seguridad como (firewall) que evita accesos no autorizados desde Internet hacia la red independiente.

R

Replicación Proceso de copia de los datos de un almacén de datos o un sistema de archivos a múltiples equipos para sincronizar los datos. Active Directory proporciona replicación multimaestro del directorio entre los controladores de dominio dentro de un dominio dado. Las replicas del directorio en cada controlador del dominio se pueden modificar. Ello permite que la actualización se aplique a cualquier replica de un dominio dado. El servicio de replicación copia automáticamente los cambios de una replica dada al resto de replicas.

Replicación multimaestra Un modelo de replicación en que cualquier controlador de dominio acepta y replica los cambios de directorio en cualquier otro controlador de dominio. Difiere de otros modelos de replicación en que un equipo guarda la única copia modificable del directorio y el resto guardan copias de respaldo.

Router Dispositivo de la capa de red que usa una o mas métricas para determinar cual es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red que contiene las actualizaciones de enrutamiento.

S

Servidor Equipo que proporciona recursos compartidos a los usuarios de red.

Servicio de directorio Proporciona los métodos para almacenar datos de directorio y ponerlos disponibles a los usuarios y administradores. Por ejemplo, Active Directory almacena información sobre cuentas de usuarios, como nombres, contraseñas, números de teléfono y otros, y permite a los usuarios autorizados en la misma red acceder a esta misma información.

Sistema de nombres de dominio Un servicio de nombres jerárquico, estático, para los host del Protocolo de control de transmisión/Protocolo de Internet (TCP/IP).El administrador de la red configura el DNS con la lista de nombres de host y direcciones IP, permitiendo a los usuarios de las estaciones de trabajo configuradas para hacer peticiones al DNS especificar un sistema remoto por su nombre en lugar por su dirección IP.

Switch Dispositivo de red que filtra, direcciona y difunde tramas con base en la dirección de destino de cada trama.

T

TCP/IP Véase Protocolo de control de transmisión/Protocolo de Internet

U

Unidad organizacional Un objeto contenedor de Active Directory usado con dominios. Las UO son contenedores lógicos en los que se pueden situar usuarios, grupos, equipos y otras UO. Puede contener objetos solo de su dominio principal. Una UO es el menor ámbito en el que se puede aplicar una directiva de grupo o delegar autoridad.

BIBLIOGRAFIA

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN.

L.A. SALVADOR MEZA BADILLO
ASESOR DE PROYECTO DE TITULACION
"IMPLEMENTACION DE UNA INTRANET PARA LOS LABORATIORIOS DE LA FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN"

Por este medio hago a usted la entrega del proyecto para titulación "Implementación de una Intranet para los laboratorios de la Facultad de contaduría y administración, el cual incluye:

- Servidor Windows 2000 Advanced Server.
- Password de administrador.
- Manuales de seguridad y mantenimiento.
- Manual de administrador.
- Disco compacto con documentación del proyecto.

Las pruebas fueron realizadas satisfactoriamente y se encuentra en funcionamiento.

Ciudad Universitaria, D.F. 15 de Agosto del 2003.

Salvador Meza B

L.A. Salvador Meza Badillo