DECLARACIÓN JURAMENTADA

Yo David Andrés Dueñas Torres, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

……

David Andrés Dueñas Torres

AGRADECIMIENTOS

Quiero agradecer a Dios, a mis padres, profesores, compañeros y especialmente a mi novia por haberme apoyado a lo largo de toda mi carrera universitaria que ha sido la etapa mas bella de mi vida con amistades que nunca las voy a olvidar y tener una formación profesional de muy alto nivel con conocimientos actuales a la par con la tecnología.

Siempre voy a tener presente a todas las personas que a mi y a mis compañeros nos ayudaron a ser mas profesionales y con buenos principios éticos y morales. Y por ultimo un enorme agradecimiento a mi mejor amigo, Ing. Pedro Román que me apoyo en todo sentido en mis estudios universitarios.

RESUMEN EJECUTIVO

El ausentismo de estándares para manejar de manera adecuada y la falta de un medio de conexión de dos edificaciones de una misma organización crea una dificultad al momento de una adecuada administración de los recursos.

El propósito de esta investigación es la planificación e instalación del nuevo estándar de red para la Universidad Internacional SEK basada en Microsoft Windows 2003 y Centos 5. Con estas plataformas se conseguirá reducir sustancialmente el uso de recursos tecnológicos y una ayuda a los administradores, instaladores y de soporte que brinden servicio en los laboratorios, reduciendo y mejorando la administración.

Mediante esta integración vamos a unificar las dos redes para poder manejar de forma centralizada basado en servidores de dominio en diferentes plataformas con replicación entre ellas.

Un directorio de dominio de código abierto, como principal de nuestra red facilitara la rapidez de la lectura de sus registros de recursos e información de usuarios que se encuentren definidos en el dominio principal, además, permite replicar y recibir replicas de servidores de forma muy sencilla. Muchas aplicaciones tienen interfaces de conexión y se pueden integrar fácilmente, es decir, el directorio activo, tiene un sistema jerárquico de almacenamiento de información, permite múltiples directorios independientes, funciona sobre TCP/IP y SSL, entre otras.

ABSTRACT

The absenteeism of standards to handle of suitable way and the lack of means of connection of two buildings of a same organization create a difficulty at the time of a suitable administration of the resources.

The intention of this investigation is the planning and installation of the new standard networks for the University International SEK based on Microsoft Windows 2003 and Centos 5. With these platforms one will be able substantially to reduce to the use of technological resources and an aid to the administrators, installers and of support that offers service in the laboratories, reducing and improving the administration

By means of this integration we are going to unify the two networks to be able to handle of centralized form based on dominion servers in different platforms with replication among them.

A directory of open source dominion, as main of our network would facilitate the rapidity of the reading of his registries of resources and information of users who are defined in the main dominion, in addition, allows to talk back and to receive replicas of servers of very simple form. Many applications have connection interfaces and they are possible to be integrated easily, that is to say, the directory assets, have a hierarchic system of information storage, allow independent directory manifolds, work on TCP/IP and SSL, among others.

CONTENIDO

INDICE FIGURAS

INDICE TABLAS

INDICE ANEXOS

1. INTRODUCCION

1.1. DETERMINACION DEL PROBLEMA

La falta de integración de redes de datos por diferentes situaciones, plataformas de administrador de redes de diferente tecnología, abierta, propietaria, genera un aislamiento que ocasiona problemas en temas de administración empresarial, seguridades de la red, optimización de recursos.

El aislamiento entre redes de diferentes plataformas es un problema que dificulta una administración y manejo de políticas de usuarios y grupos de trabajos centralizados.

Crear estructuras jerárquicas de dominios y subdominios, facilitando la estructuración de los recursos según su localización o función dentro de la organización es un factor clave para que una organización pueda manejar escalabilidad y capacidad de ampliación.

Debido a una descentralización, no se puede crear varios objetos que manejen los recursos y los usuarios que acceden a la red. A su vez cada uno de estos objetos no tiene propiedades que permitan identificarlos en modo uniforme.

De esta forma, es inconveniente crear recursos, como carpetas compartidas, impresoras de red, y conceder acceso a estos recursos a usuarios. Active Directory y LDAP son repositorios de tipo centralizado que proporciona el control, la administración y la consulta de todos los elementos lógicos de una red y la compatibilidad de estándares entre ellos, como pueden ser usuarios, equipos y recursos.

1.2. JUSTIFICACION E IMPORTANCIA

El integrar redes de diferente plataforma de administración a través de un proceso de planificación e instalación, basado en Directorios Activos es un tema importante para las empresas, instituciones educativas que tengan redes no integradas y es el objetivo fundamental de la investigación y desarrollo del presente trabajo.

Con la unificación, se mejora la posibilidad de que el administrador de una red de datos, configure y administre de forma eficaz diversos bosques, dominios y sitios de la red. Estas mejoras facilitan y hacen que sea más eficaz la administración de grupos de usuarios y equipos en un entorno de dominio.

Las características de seguridad que incluyen nuestras herramientas facilitan la administración de las diversas relaciones de confianza entre grupos y entre dominios. Todas estas se manejan desarrollando políticas según las necesidades de la organización permitiendo mayor confiabilidad y disponibilidad de los recursos de la misma.

Un directorio de dominio de código abierto, como principal de nuestra red facilitara la rapidez de la lectura de sus registros de recursos e información de usuarios que se encuentren definidos en el dominio principal, además, permite replicar y recibir replicas de servidores de forma muy sencilla. Muchas aplicaciones tienen interfaces de conexión y se pueden integrar fácilmente, es decir, el directorio activo, tiene un sistema jerárquico de almacenamiento de información, permite múltiples directorios independientes, funciona sobre TCP/IP y SSL, entre otras.

1.3. DEFINICION DEL TEMA

Integración de redes: Diseño e integración de redes heterogéneas de diferente plataforma de administración usando tecnología de Directorios Activos.

1.4. OBJETIVOS

1.4.1. Objetivo General

Diseñar e integrar redes de diferentes plataformas con tecnología de Directorios Activos.

1.4.2. Objetivos Específicos

1. Proponer el uso de estándares para nomenclatura de nombres de recursos, definición de directorios y aplicaciones.

2. Facilitar la administración centralizada de los recursos de red creando políticas y manejo de los mismos.

3. Establecer un diseño organizando los dominios en árboles.

1.5. DELIMITACION DEL TEMA

La integración de redes de diferente plataforma se limitara a redes que corran bajo software administrador de red Windows 2003 Server y Linux, usando como base tecnológica para la integración, el diseño de Directorio Activo, LDAP.

Como aplicación práctica de la tesis se propondrá la integración de la red de la Universidad Internacional SEK sede Ecuador, entre sus campus de Carcelén y Guápulo mediante un servidor de dominio principal con herramienta de código abierto LDAP y sus dominios hijo con servidores Active Directory.

1.6. MARCO TEORICO

Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios y recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de unión entre los usuarios y los recursos compartidos.[1]

El administrador de la red obtendrá una mayor facilidad debido a la integración de todos los recursos de la red con su respectiva nomenclatura que definirá el tipo y descripción del objeto para poder controlar y compartirlos en la red de su directorio.

La gran mayoría de implementaciones están basados en el estándar X.500, que posteriormente fue la base de LDAP, pero utilizando el modelo TCP/IP en lugar de usar el modelo OSI, adquiriendo especial relevancia en Internet.

Existen numerosas formas de implementación de servicios de directorio de diferentes compañías. Algunos de estos ejemplos son:

- **NIS** Network Information Service protocolo Sun Microsystems.
- **eDirectory**, desarrollado por Novell.
- **Servidor de directorio de Red Hat**
- **Active Directory** el servicio del directorio de Microsoft
- **Open Directory**: el servidor del Mac OS X de Apple.
- **Servidor de directorio de Apache**: Apache Software Fundation
- **Directorio de Internet de Oracle**: (OID) es el servicio del directorio de Oracle Corporation.
- **Servidor de Sun Java System**: Sun Microsystems
- **OpenDS** la nueva generación de servicio de directorio abierto ofrecido por Sun Microsystems.
- **OpenLDAP** está liberada bajo su propia licencia OpenLDAP Public License.

Active Directory tuvo una presentación previa en 1996, y liberada con Windows 2000 Server Edition. Mejorando su administración y funcionalidad en Windows Server 2003 con ventajas adicionales en Windows Server 2003 R2 y Windows Server 2008.

[1] Carter, Gerald "LDAP System Administration". *O'Reilly*. 2003.

El proyecto OpenLDAP se inició en 1998 por Kurt Zeilenga. El proyecto comenzó como un clon de la implementación LDAP de la Universidad de Michigan, entidad donde se desarrolló originalmente el protocolo LDAP y que también actualmente trabaja en la evolución del mismo.[2]

1.6.1. Definición de LDAP

LDAP son las siglas de *Lightweight Directory Access Protocol*. Como su propio nombre indica, es un protocolo ligero para acceder al servicio de directorio. LDAP se ejecuta sobre TCP/IP.[3]

El modelo de información de LDAP está basado en entradas. Una entrada es una colección de atributos que tienen un único y global Nombre Distinguido (DN). El DN se utiliza para referirse a una entrada sin equívocos. Cada atributo de una entrada posee un tipo y uno o más valores.

En LDAP, las entradas están constituidas en una estructura jerárquica en árbol. Usualmente, esta estructura reflejaba los límites geográficos y organizacionales. El árbol también se puede organizar basándose en los nombres de dominio de Internet. Este tipo de nombramiento se está volviendo muy difundido, ya que permite localizar un servicio de directorio haciendo uso de los DNS. LDAP permite controlar que atributos son requeridos y permitidos en una entrada gracias al uso del atributo denominado *objectClass*. El valor del atributo *objectClass* establece que reglas de diseño (*schema rules*) ha de seguir la entrada.

LDAP especifica operaciones para interrogar y actualizar el directorio. Proporciona operaciones para añadir y borrar entradas del directorio, modificar una entrada existente y cambiar el nombre de una entrada. La mayor parte del tiempo, sin embargo, LDAP se utiliza para buscar información almacenada en el directorio. Las operaciones de búsqueda de LDAP admiten buscar entradas que conciertan con algún criterio especificado por un filtro de búsqueda. La información puede ser solicitada desde cada entrada que concuerda con dicho criterio.

---

[2] Maria C. Espana Boquera, “Servicios avanzados de telecomunicación”, 2003.

[3] http://es.wikipedia.org/wiki/OpenLDAP

LDAP provee un mecanismo de autentificación para los clientes, o la confirmación de identidad en un servidor de directorio, facilitando el control de acceso que proteja la información que el servidor posee. LDAP también soporta los servicios de privacidad e integridad.

1.6.2. Definición de Active Directory

Active Directory (AD) es el nombre utilizado por Microsoft para referirse a su implementación de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente protocolo LDAP, DNS, DHCP, kerberos).

Su estructura jerárquica lógica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

La estructura más común es la estructura de árbol, es decir, un dominio puede tener muchos subdominios, los cuáles a su vez pueden poseer más hijos (subdominios), y así sucesivamente.

Estos dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.[4]

Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

A su vez, los árboles pueden integrarse en un espacio común denominado bosque. Para realizar un bosque es necesario crear dos o más árboles (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de "trust" o confianza entre ellos. De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio Active Directory.

[4] http://es.wikipedia.org/wiki/Active_Directory

Su funcionamiento es similar a otras estructuras de LDAP (*Lightweight Directory Access Protocol*), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. La ventaja que presenta esto es la sincronización presente entre los distintos servidores de autenticación de todo el dominio.

Debido a esta centralización, se pueden crear varios objetos que afectarán los recursos y los usuarios que acceden a la red.

A su vez, cada uno de estos objetos tendrá atributos que permiten identificarlos en modo unívoco (por ejemplo, los usuarios tendrán campo "nombre", campo "email", etc., las impresoras de red tendrán campo "nombre", campo "productor", campo "modelo", campo "usuarios que pueden acceder", etc.). Toda esta información queda almacenada en *Active Directory* replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

De esta forma, es posible crear recursos (como carpetas compartidas, impresoras de red, etc.) y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito. Para decirlo en otras palabras, *Active Directory* es un repositorio centralizado que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

Para permitir que los usuarios de un dominio accedan a recursos de otro dominio, Active Directory usa un *trust* (enlace de confianza). El trust es creado automáticamente cuando se crean nuevos dominios. Los límites del trust no son marcados por dominio, sino por el bosque al cual pertenece. Existen trust transitivos, donde los trust de Active Directory pueden ser un acceso directo (une dos dominios en árboles diferentes, transitivo, una o dos vías), bosque (transitivo, una o dos vías), reino (transitivo o no transitivo, una o dos vías), o externo (no transitivo, una o dos vías), para conectarse a otros bosques o dominios que no son de Active Directory. Active Directory usa el protocolo V5 de Kerberos, aunque también soporta NTLM y usuarios Web mediante autenticación SSL / TLS

Las *Confianzas transitivas* son confianzas automáticas de dos vías que existen entre dominios en Active Directory. Se definen como confianzas que fluyen a través de la red,

utilizando servidores de paso para utilizar los recursos de dos árboles no conectados directamente. Esto maximiza las relaciones entre dominios de Windows porque evita poseer exceso de confianza para conectarse con todas las máquinas de la red.

Las *Confianzas explícitas* son aquellas que establecen las relaciones de forma manual para entregar una ruta de acceso para la autenticación. Este tipo de relación puede ser de una o dos vías, dependiendo de la aplicación.

Las Confianzas explícitas se utilizan con frecuencia para acceder a dominios compuestos por ordenadores con Windows NT 4.0.

La *Confianza de acceso directo* es, esencialmente, una confianza explícita que crea accesos directos entre dos dominios en la estructura de dominios. Este tipo de relaciones permite incrementar la conectividad entre dos dominios, reduciendo las consultas y los tiempos de espera para la autenticación.

La *Confianza entre bosques* permite la interconexión entre bosques de dominios, creando relaciones transitivas de doble vía. En Windows 2000, las confianzas entre bosques son de tipo explícito, al contrario de Windows .NET 2003 Server.

Los direccionamientos a recursos de Active Directory son estándares con la Convención Universal de Nombrado (UNC), Localizador Uniforme de Recursos (URL) y nombrado de LDAP.

Cada objeto de la red posee un nombre de distinción (en inglés, Distinguished name (DN)), así una impresora llamada *Imprime* en una Unidad Organizativa (en inglés, Organizational Units, OU) llamada *Ventas* y un dominio *foo.org*, puede escribirse de las siguientes formas para ser direccionado:

- En DN sería C*N=Imprime,OU=Sistemas,DC=uisek,DC=edu,DC=ec*

Donde:

  - CN es el nombre común (en inglés, Common Name)
  - DC es clase de objeto de dominio (en inglés, Domain object Class).

- En forma canónica sería *uisek.edu.ec/Sistemas/Imprime*

Los otros métodos de direccionamiento constituyen una forma local de localizar un recurso

- Distinción de Nombre Relativo (en inglés, Relative Distinguised Name (RDN)), que busca un recuso sólo con el Nombre Común (CN).
- Globally Unique Identifier (GUID), que genera una cadena de 128 bits que es usado por Active Directory para buscar y replicar información

Ciertos tipos de objetos poseen un Nombre de Usuario Principal (en inglés, User Principal Name (UPN)) que permite el ingreso abreviado a un recurso o un directorio de la red. Su forma es *objetodered@dominio*[5]

1.6.3. Integración de LDAP y Active Directory

Hay 2 maneras de conseguir datos de la autentificación (uid/gid) de directorio activo:

- Kerberos + LDAP
- Kerberos + Winbind de Samba

Usar LDAP es mucho más transparente, si el esquema del servidor de Windows puede manejar los usuarios de Unix, que significa que un cambio del esquema necesita ser instalado. Winbind es un poco más no fiable y más lento.

Sin importar la versión de Linux, se utilizara los mismos elementos:

- Kerberos: Winbind utiliza el Kerberos para obtener acceso a Acitve Directory.
- Conmutación de los Servicios de Nombres (Name Service Switch): Éste es un paquete de contenidos construidos en las bibliotecas de Linux que permiten que una aplicación seleccione una fuente para validar las credenciales de la autentificación.
- Proceso de autenticación centralizado (Pluggable Authentication Modules): Esto extiende el mecanismo estándar de la autentificación de la contraseña de Unix para incluir las bases de datos centrales tales como LDAP, Kerberos, Active Directory, etcétera.
- Samba con y sin Winbind: Para la interoperabilidad de Active Directory, debe estar funcionando una versión actual de samba (3.05 o más nuevo).

[5] Stan Reimer, Mike Mulcare, "Active Directory para Microsoft Windows Server 2003: referencia técnica", 2003, 418 p.

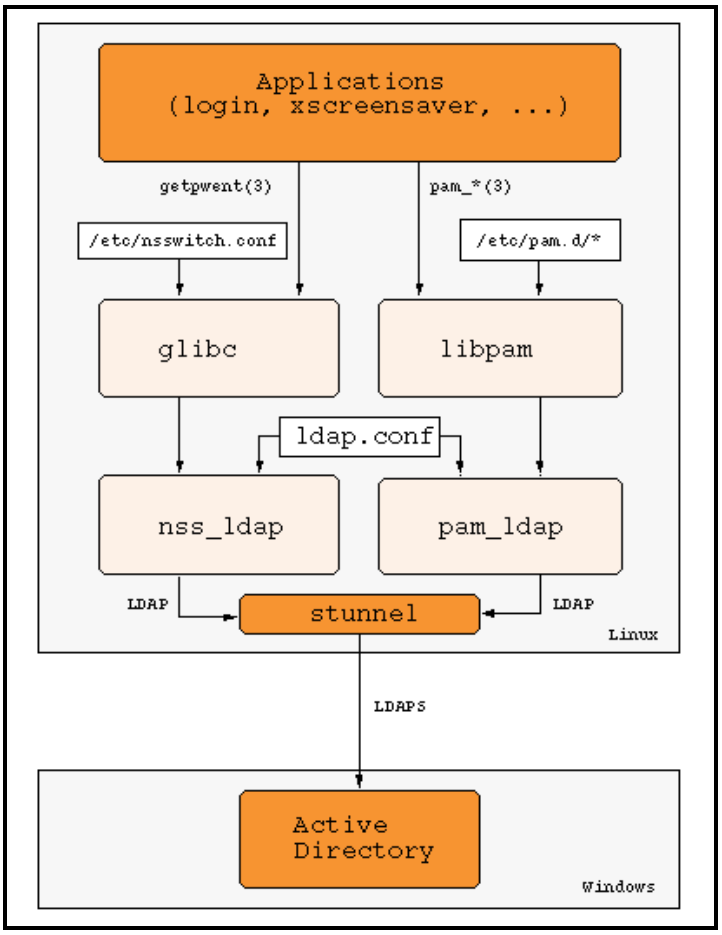


Figura 1: Diagrama de la comunicación client/server con Active Directory

Los paquetes necesarios para el desarrollo de esta tesis son los siguientes:

- **Openldap**.- necesitado para las búsquedas del ldap del cliente
- **cyrus-sasl**.- capa simple de la autentificación y de la seguridad - para el cifrado básico de los lazos y de las búsquedas del ldap. Usted también necesitará cyrus-sasl-gssapi y libgssapi.
- **mit-krb5**.- el Kerberos del MIT.
- **PAM**.- la base del proceso de autentificación centralizado.
- **pam_krb5**.- módulo del PAM del Kerberos.
- **pam_mount**
- **nss_ldap**.- módulo de LDAP para el sistema conocido del interruptor (permite el cambio de dirección de las búsquedas para los usuarios, los grupos, etc. al ldap).
- **nscd**
- **samba**

- **openssl**
- **NTP**.- Utilizaremos a NTP-CLIENTE para la sincronización de tiempo (para el apropiado funcionamiento de Kerberos)

2. DISEÑO DE LA ARQUITECTURA DE RED DE LA UNIVERSIDAD SEK

La Universidad Internacional SEK no cuenta con un dominio para poder tener una administración completa de todos sus recursos y mejorar el uso del ancho de banda.
En esta tesis se va a desarrollar tres servidores de dominio que van estar ubicados de la siguiente manera: un servidor en cada campus que serán configurados con Microsoft Active Directory cada uno, y el servidor principal de dominio tendrá una configuración con OpenLDAP con replicación hacia los servidores secundarios anteriormente señalados.

En la Fig. 2 se indica el diseño de la red de dominio de la Universidad Internacional SEK.

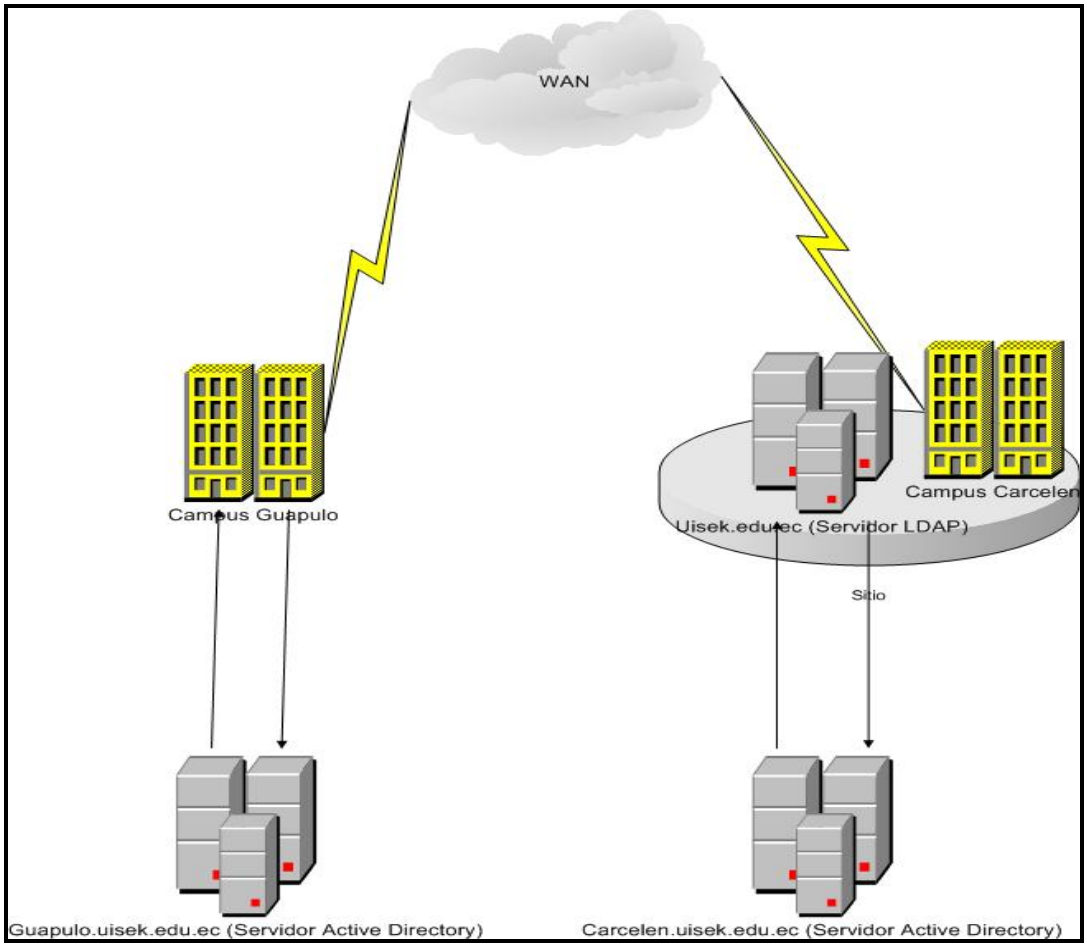


Figura 2: Diseño de red de Dominio Universidad Internacional SEK

2.1. ANTECEDENTES

Actualmente la Universidad Internacional SEK tiene con dos campus; en ninguno de los dos existen un diseño de dominios que permita utilizar políticas de seguridad.

La comunicación física entre los campus se da a través de una Red Privada Virtual (VPN), utilizando la nube de internet.

Los campus Carcelén y Guápulo utilizan con una conexión de internet de 512 kbps. y 1024 kbps. respectivamente, para el establecimiento de la VPN no existe segmentación del canal.

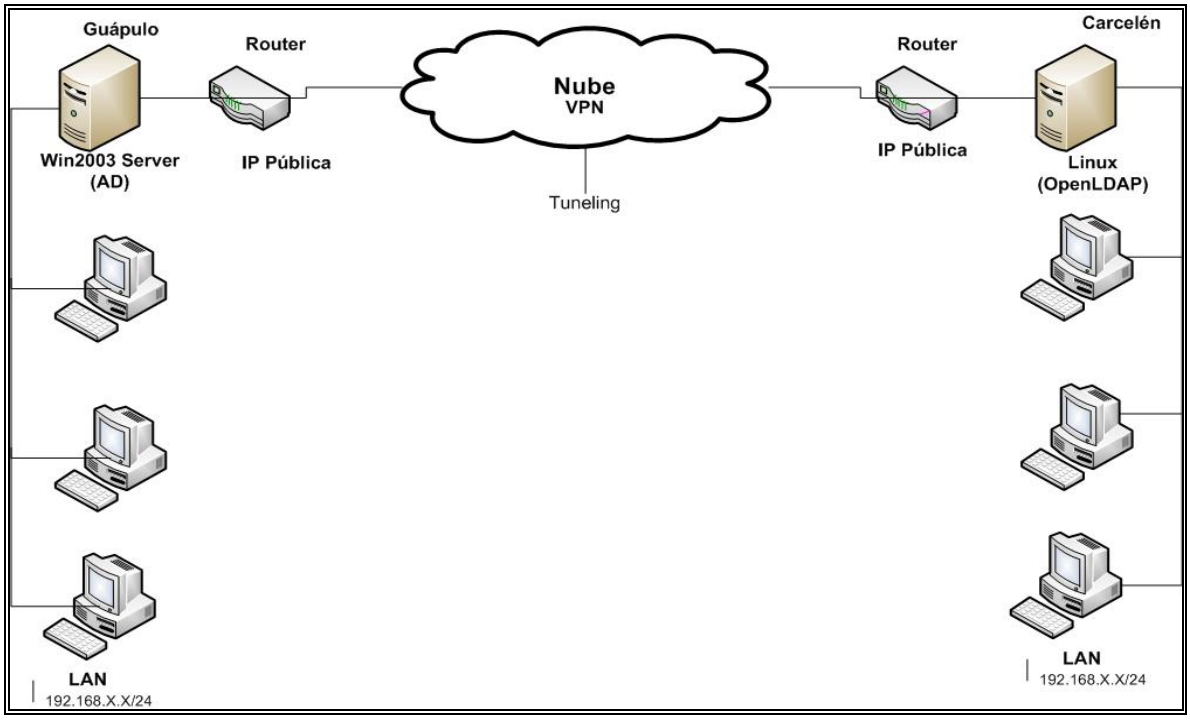


Figura 3: Diseño de red actual Universidad Internacional SEK

2.2. DISEÑO

Se incorporan un servidor en el campus Carcelén con sistema operativo Windows 2003 Server con Active Directory. Se debe instalar en el servidor Guápulo Active Directory y en el servidor Linux de Carcelén OpenLDAP.

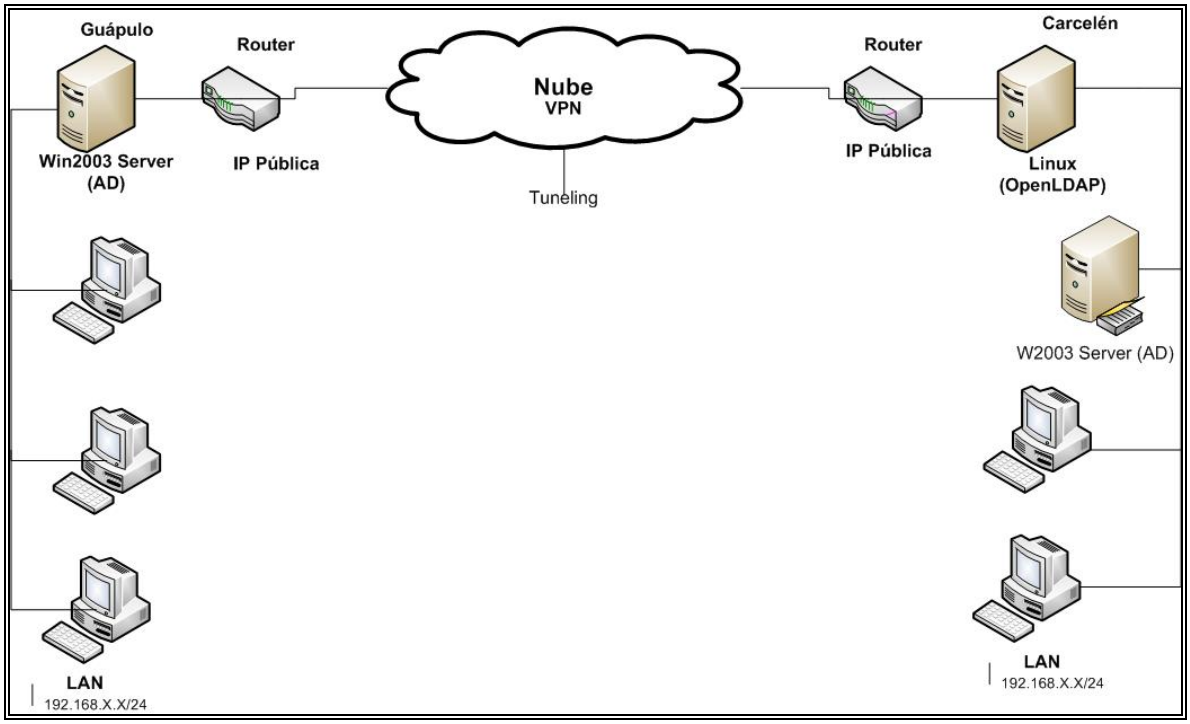


Figura 4: Nuevo Diseño de red de directorio.

Luego de la implementación física, el diseño del forest se detalla a continuación:

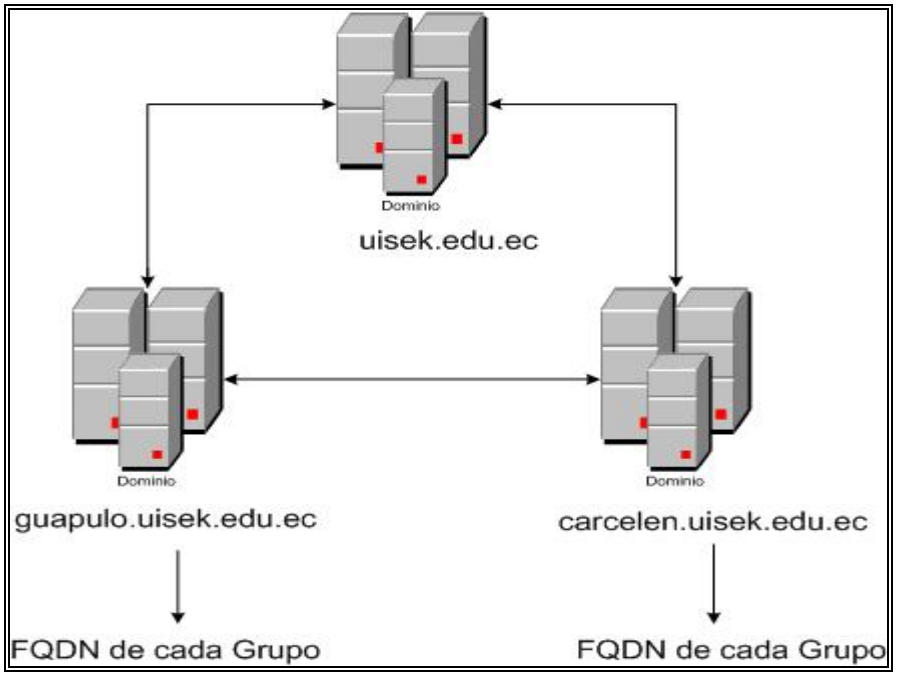


Figura 5: Diseño Forest.

2.3. DISEÑO DE FOREST

Cada dominio del directorio se identifica mediante un nombre DNS de dominio y necesita uno o más controladores de dominio. Si nuestra red necesita más de un dominio, se pueden crear varios fácilmente.

Uno o más dominios que comparten un esquema y un catálogo global comunes se conocen como bosque. Si varios dominios del bosque tienen nombres DNS de dominio contiguos, esa estructura se denomina árbol de dominio.

La Universidad Internacional SEK al momento no cuenta con ningún tipo de topología de directorio, es decir, bosque o árbol. Por lo que es muy importante definir y diseñar una topología para la red.

Se implementara un diseño de Forest que incluirá dos árboles primarios que serán los de cada campus en donde sus recursos y usuarios pertenecerán a su árbol en el dominio dependiendo de la ubicación.

2.4. DISEÑO DE DOMINIO.

Un dominio es un conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

El equipo en el cual reside la administración de los usuarios se llama controlador de dominio y cuando queremos usar un ordenador de dicha red tenemos que poner un nombre de usuario y una contraseña para ser reconocidos por el controlador de dominio y poder usar los recursos compartidos de la red (acceso a Internet, impresoras, software, etc.).

Se dispondrá de un solo dominio principal y dos dominios secundarios, es decir, Guápulo y Carcelén. Mediante este diseño se facilitara la administración teniendo una replica de información entre los dominios, de esta manera el usuario podrá ingresar en cualquiera de los campus con su cuenta y bajo un grupo de políticas.

2.5. NOMBRE DEL SERVICIO DE DIRECTORIO

El Sistema de Nombres de Dominio (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Los árboles de dominio asociados en un bosque comparten el mismo esquema de Active Directory y la información de duplicación y configuración del directorio, pero no comparten un espacio de nombres de dominio DNS contiguo.

La combinación de bosques y árboles de dominio ofrece opciones flexibles para asignar nombres a los dominios. En el directorio se pueden incluir espacios de nombres DNS contiguos y no contiguos.

En la actualidad la Universidad Internacional SEK (Ecuador) posee un DNS uisek.edu.ec registrado en Internet. Debido que servicios como el correo electrónico, Proxy entre otros, mantendremos el nombre de dominio para nuestro servicio de directorio.

2.6. DISEÑO DE LAS UNIDADES ORGANIZACIONALES

Las OU son contenedores lógicos en los que se colocan los usuarios, los grupos, los equipos y otras OU. Sólo pueden contener objetos procedentes del dominio principal. Una OU es la unidad de ámbito más pequeña a la que se puede aplicar una directiva de grupo o una autoridad delegada.

Es posible una relacion de árboles de OU situando a cada árbol como subordinado del anterior. Esta potente posibilidad de Directorio Activo permite delegar tareas de administración a un subconjunto de usuarios dentro de un dominio Windows 2003 Server. La OU proporciona un control granular de la delegación de la gestión de recursos.

El diseño de las unidades organizacionales estará distribuido de la siguiente manera:
Campus Guápulo (guapulo.uisek.edu.ec):

- Administrativo.
- Biblioteca.

- Centro de Cómputo.
- Turismo.
- Wireless.

Campus Carcelén (carcelen.uisek.edu.ec):

- Comunicación.
- Administrativo
- Finanzas.
- Sistemas 1.
- Sistemas 2.
- Wireless.

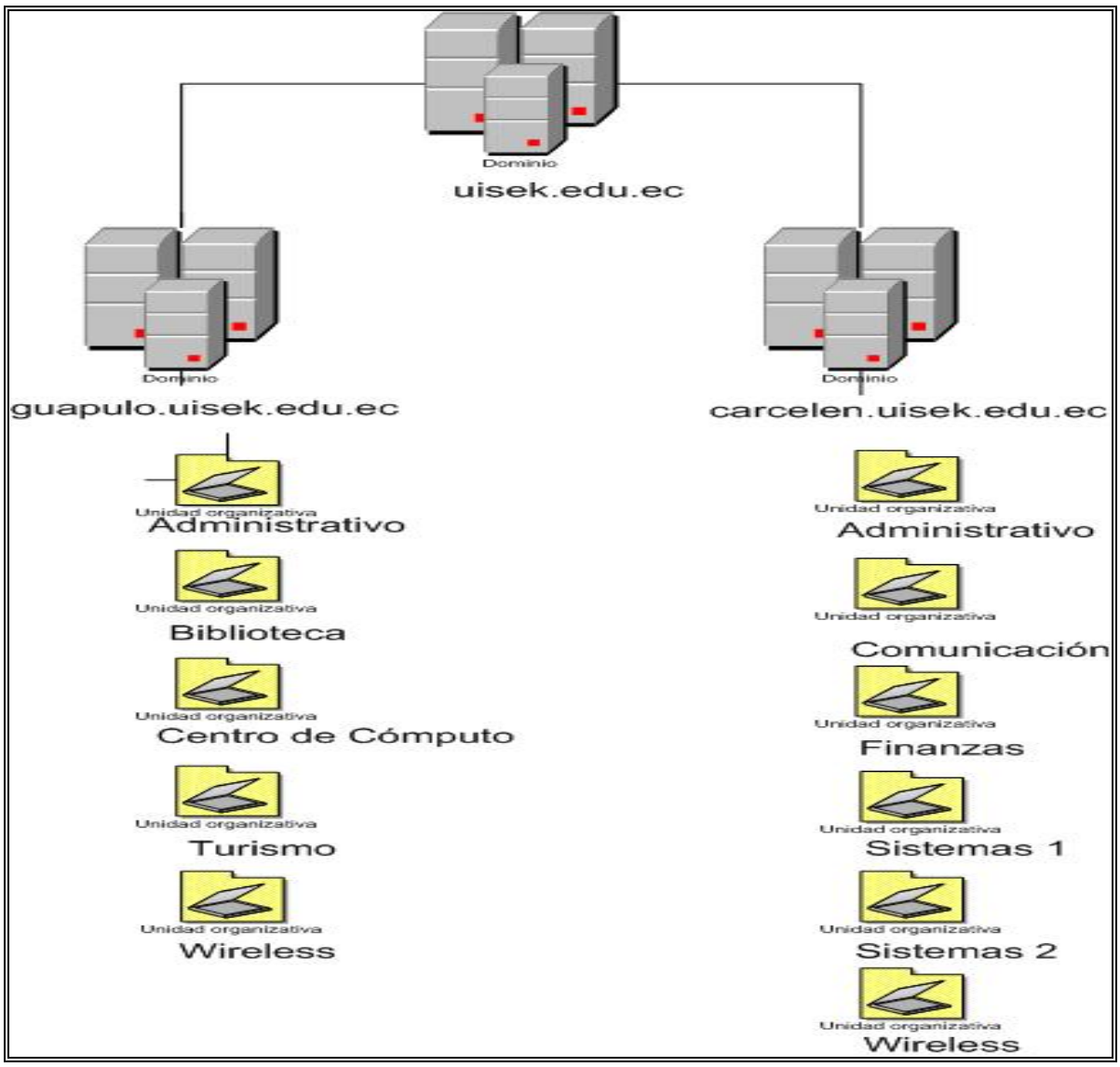


Figura 6: Diseño de Unidades Organizacionales.

Mediante este diseño integraremos las políticas de grupo para cada unidad organizacional y podremos integrar los dos campus en un solo dominio en diferentes plataformas.

2.7. DISEÑO DE LA TOPOLOGIA DE SITIO

La Universidad Internacional SEK dispone de dos redes de 10/100 Mbps., una para cada campus. Las dos redes tienen una red de 512 kbps. en Guápulo y 1024 kbps en Carcelén. La replicación entre los dominios se lo realiza a través del enlace WAN en horarios que no afecta otros servicios de la red.

2.8. DISEÑO DE LA RED DEL CAMPUS GUÁPULO.

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a Internet, e-mail, Chat, juegos), etc.

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI por la ISO, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

En el campus Juan Montalvo ubicado en Guápulo, al nor-este de la ciudad de Quito, se diseña la red bajo el dominio Active Directory como se muestra en la Figura 4. Teniendo una red de clase C (192.168.X.X/24) permitiendo tener 254 hosts o direcciones IPs con su respectivo nombre de dominio, los FQDN (Full Quality Domain Name) de cada uno de ellos se detallan en las tablas 1,2,3,4 y 5.

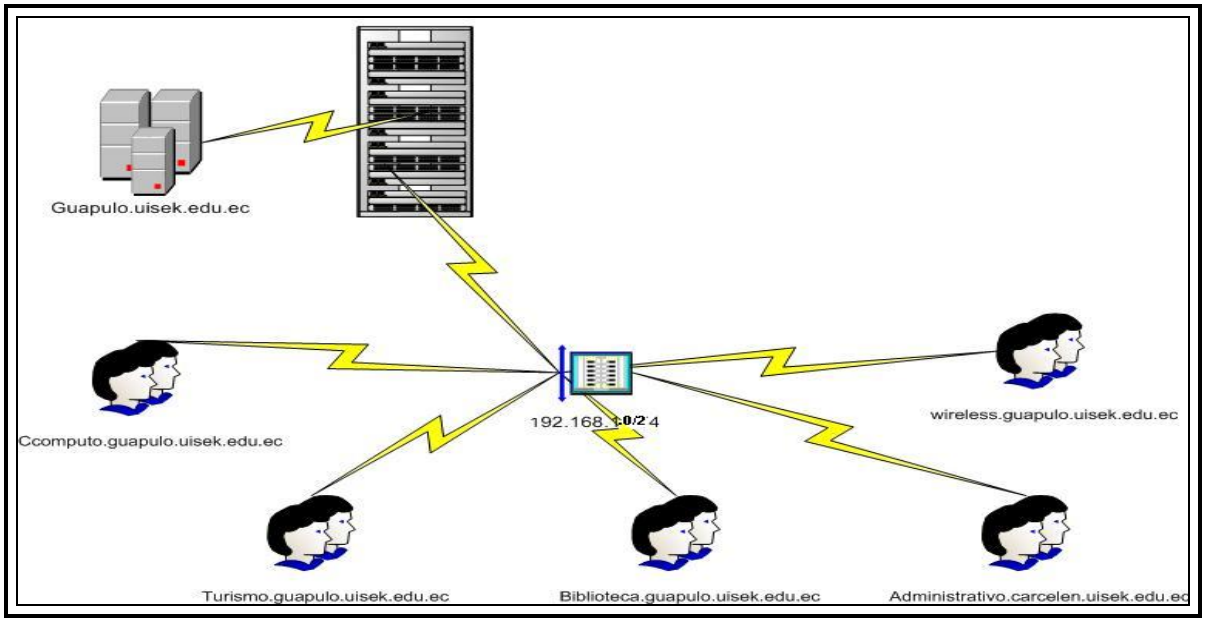


Figura 7: Diseño de la Red Campus Guápulo

Nombre	**Dirección IP**
CComputo01.guapulo.uisek.edu.ec	192.168.X.X
CComputo02.guapulo.uisek.edu.ec	192.168.X.X
CComputo03.guapulo.uisek.edu.ec	192.168.X.X
CComputo04.guapulo.uisek.edu.ec	192.168.X.X
CComputo05.guapulo.uisek.edu.ec	192.168.X.X
CComputo06.guapulo.uisek.edu.ec	192.168.X.X
CComputo07.guapulo.uisek.edu.ec	192.168.X.X
CComputo08.guapulo.uisek.edu.ec	192.168.X.X
CComputo09.guapulo.uisek.edu.ec	192.168.X.X
CComputo10.guapulo.uisek.edu.ec	192.168.X.X
CComputo11.guapulo.uisek.edu.ec	192.168.X.X
<CComputo12.guapulo.uisek.edu.ec	192.168.X.X
CComputo13.guapulo.uisek.edu.ec	192.168.X.X
CComputo14.guapulo.uisek.edu.ec	192.168.X.X
CComputo15.guapulo.uisek.edu.ec	192.168.X.X
CComputo16.guapulo.uisek.edu.ec	192.168.X.X
CComputo17.guapulo.uisek.edu.ec	192.168.X.X
CComputo18.guapulo.uisek.edu.ec	192.168.X.X
CComputo19.guapulo.uisek.edu.ec	192.168.X.X

CComputo20.guapulo.uisek.edu.ec	192.168.X.X
CComputo21.guapulo.uisek.edu.ec	192.168.X.X
CComputo22.guapulo.uisek.edu.ec	192.168.X.X

Tabla 1: Nombres de dominios con sus respectivas IPs del Centro de Cómputo del campus de Guápulo.

Nombre	**Dirección IP**
Turismo01.guapulo.uisek.edu.ec	192.168.X.X
Turismo02.guapulo.uisek.edu.ec	192.168.X.X
Turismo03.guapulo.uisek.edu.ec	192.168.X.X
Turismo04.guapulo.uisek.edu.ec	192.168.X.X
Turismo05.guapulo.uisek.edu.ec	192.168.X.X
Turismo06.guapulo.uisek.edu.ec	192.168.X.X
Turismo07.guapulo.uisek.edu.ec	192.168.X.X
Turismo08.guapulo.uisek.edu.ec	192.168.X.X
Turismo09.guapulo.uisek.edu.ec	192.168.X.X
Turismo10.guapulo.uisek.edu.ec	192.168.X.X
Turismo11.guapulo.uisek.edu.ec	192.168.X.X
Turismo12.guapulo.uisek.edu.ec	192.168.X.X
Turismo13.guapulo.uisek.edu.ec	192.168.X.X
Turismo14.guapulo.uisek.edu.ec	192.168.X.X
Turismo15.guapulo.uisek.edu.ec	192.168.X.X
Turismo16.guapulo.uisek.edu.ec	192.168.X.X

Tabla 2: Nombres de dominios con sus respectivas IPs del Laboratorio de Turismo del campus de Guápulo.

Nombre	**Dirección IP**
Biblioteca01.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca02.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca03.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca04.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca05.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca06.guapulo.uisek.edu.ec	192.168.X.X

Biblioteca07.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca08.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca09.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca10.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca11.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca12.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca13.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca14.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca15.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca16.guapulo.uisek.edu.ec	192.168.X.X
Biblioteca17.guapulo.uisek.edu.ec	192.168.X.X

Tabla 3: Nombres de dominios con sus respectivas IPs de la Biblioteca del campus de Guápulo.

Nombre	**Dirección IP**
Administrativo0x.guapulo.uisek.edu.ec	192.168.X.X – X

Tabla 4: Nombres de dominios con sus respectivas IPs para el personal Administrativo del campus de Guápulo.

Nombre	**Dirección IP**
Wireless01.guapulo.uisek.edu.ec	192.168.X.X
Wireless02.guapulo.uisek.edu.ec	192.168.X.X

Tabla 5: Nombres de dominios con sus respectivas IPs Wireless del campus de Guápulo.

2.9. DISEÑO DE LA RED DEL CAMPUS CARCELÉN

En el campus Miguel de Cervantes ubicado en Carcelén, al nor-oeste de la ciudad de Quito, se diseña la red bajo el dominio Active Directory como se muestra en la Figura 3, En este mismo campus se ubicara el servidor principal, que funciona bajo la plataforma Linux (Centos 5.1) en el cual implementaremos el protocolo LDAP para el acceso de los dos sub-dominios o dominios hijos de los diferentes campus a uisek.edu.ec bajo tecnología OpenLDAP.

Teniendo una red de clase C (192.168.X.X/24) permitiendo tener 254 hosts o direcciones IPs con su respectivo nombre de dominio por cada red, los FQDN (Full Quality Domain Name) de cada uno de ellos se detallan en las tablas 6,7,8,9 y 10.

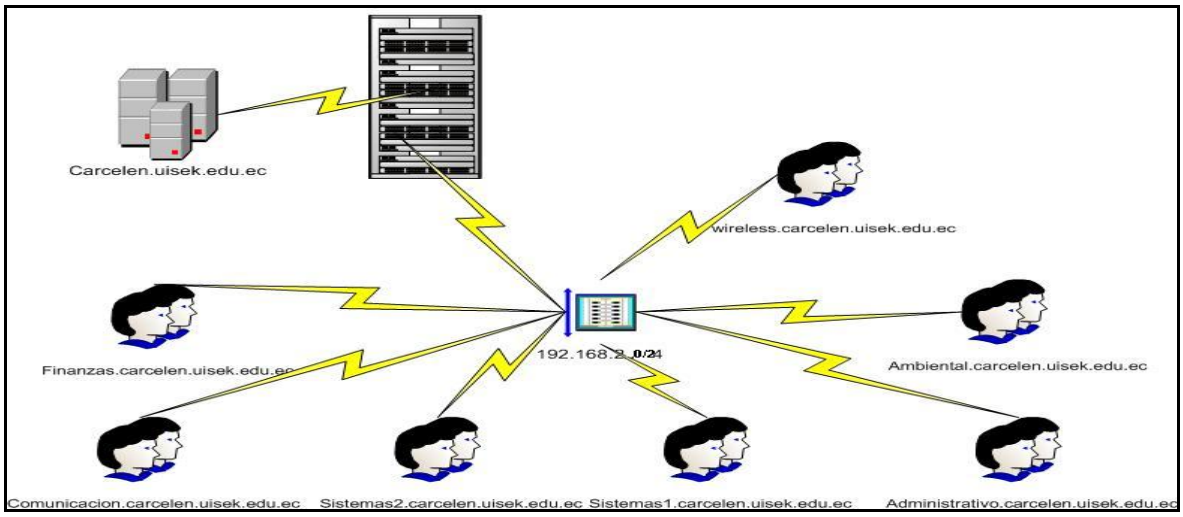


Figura 8: Diseño de la Red Campus Carcelén.

Nombre	**Dirección IP**
Wireless01.carcelen.uisek.edu.ec	192.168.X.X
Wireless02.carcelen.uisek.edu.ec	192.168.X.X
Wireless03.carcelen.uisek.edu.ec	192.168.X.X
Wireless04.carcelen.uisek.edu.ec	192.168.X.X
Wireless05.carcelen.uisek.edu.ec	192.168.X.X
Wireless06.carcelen.uisek.edu.ec	192.168.X.X

Tabla 6: Nombres de dominios con sus respectivas IPs Wireless del campus de Carcelén.

Nombre	**Dirección IP**
Finanzas01.carcelen.uisek.edu.ec	192.168.X.X
Finanzas02.carcelen.uisek.edu.ec	192.168.X.X
Finanzas03.carcelen.uisek.edu.ec	192.168.X.X
Finanzas04.carcelen.uisek.edu.ec	192.168.X.X
Finanzas05.carcelen.uisek.edu.ec	192.168.X.X
Finanzas06.carcelen.uisek.edu.ec	192.168.X.X

Finanzas07.carcelen.uisek.edu.ec	192.168.X.X
Finanzas08.carcelen.uisek.edu.ec	192.168.X.X
Finanzas09.carcelen.uisek.edu.ec	192.168.X.X
Finanzas10.carcelen.uisek.edu.ec	192.168.X.X
Finanzas11.carcelen.uisek.edu.ec	192.168.X.X
Finanzas12.carcelen.uisek.edu.ec	192.168.X.X
Finanzas13.carcelen.uisek.edu.ec	192.168.X.X
Finanzas14.carcelen.uisek.edu.ec	192.168.X.X
Finanzas15.carcelen.uisek.edu.ec	192.168.X.X
Finanzas16.carcelen.uisek.edu.ec	192.168.X.X
Finanzas17.carcelen.uisek.edu.ec	192.168.X.X
Finanzas18.carcelen.uisek.edu.ec	192.168.X.X
Finanzas19.carcelen.uisek.edu.ec	192.168.X.X
Finanzas20.carcelen.uisek.edu.ec	192.168.X.X
Finanzas21.carcelen.uisek.edu.ec	192.168.X.X
Finanzas22.carcelen.uisek.edu.ec	192.168.X.X
Finanzas23.carcelen.uisek.edu.ec	192.168.X.X
Finanzas24.carcelen.uisek.edu.ec	192.168.X.X
Finanzas25.carcelen.uisek.edu.ec	192.168.X.X

Tabla 7: Nombres de dominios con sus respectivas IPs para el Laboratorio de Finanzas del campus de Carcelén.

Nombre:	**Dirección IP:**
Comunicacion01.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion02.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion03.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion04.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion05.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion06.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion07.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion08.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion09.carcelen.uisek.edu.ec	192.168.X.X
Comunicacion10.carcelen.uisek.edu.ec	192.168.X.X

Comunicacion11.carcelen.uisek.edu.ec	192.168.X.X

Tabla 8: Nombres de dominios con sus respectivas IPs para el Laboratorio de Comunicación del campus de Carcelén.

Nombre:	**Dirección IP:**
Sistemas2_01.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_02.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_03.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_04.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_05.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_06.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_07.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_08.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_09.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_10.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_11.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_12.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_13.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_14.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_15.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_16.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_17.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_18.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_19.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_20.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_21.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_22.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_23.carcelen.uisek.edu.ec	192.168.X.X
Sistemas2_24.carcelen.uisek.edu.ec	192.168.X.X

Tabla 9: Nombres de dominios con sus respectivas IPs para el Laboratorio de Sistemas 2.

Nombre:	**Dirección IP:**
Sistemas1_01.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_02.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_03.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_04.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_05.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_06.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_07.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_08.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_09.carcelen.uisek.edu.ec	192.168.X.X
Sistemas1_10.carcelen.uisek.edu.ec	192.168.X.X

Tabla 10: Nombres de dominios con sus respectivas IPs para el Laboratorio de Sistemas 1.

3. DEFINICIÓN DE POLÍTICAS Y ESTÁNDARES DE NOMENCLATURA.

Con la implementación de un solo dominio principal basado en OpenLDAP y los dominios secundarios con Active Directory, tenemos una administración centralizada de usuarios, grupos y aplicaciones. Adicionalmente vamos a encontrar que los usuarios encargados de monitoreo del dominio, servidores y aplicaciones no tendrán la necesidad de ingresar a trabajar en los controladores de dominio, servidores miembros o de aplicaciones u otro equipo que se encuentre dentro de la red de la universidad, garantizando que no tendremos trabajando servidores como estaciones de trabajo, mejorando el rendimiento de estos equipos.

Con la administración centralizada, es posible tener un total control de usuarios, grupos y unidades organizacionales (OU)

El primer punto es la creación de las unidades organizacionales, dentro de estas unidades se crearán usuarios y grupos funcionales (globales).

Dentro de la nueva red es posible tener políticas de seguridad en cualquier nivel como por ejemplo: dominio, controladores de dominio, unidades organizacionales, grupos de usuarios, estaciones de trabajo, subredes, etc.

Según los requerimientos, es posible tener seguridades en cualquier objeto de Windows 2003 integrado al Active Directory y este al dominio principal en OpenLDAP.

Una vez que se han creado las unidades organizacionales, los usuarios y grupos, podremos administrar de mejor manera todos los recursos de red, garantizando el servicio a todos los clientes internos de la organización.

Una vez definidos los recursos, asignaremos permisos a cada recurso y garantizaremos que ningún usuario pueda ingresar a un recurso que no queremos compartir, brindando un mejor servicio para la empresa.

3.1. DOCUMENTO DE ESTÁNDARES PARA SERVIDORES DE DOMINIO

Una correcta administración de la plataforma, se ha establecido un estándar para los servidores creados para los diferentes dominios. Estos estándares contemplan varios puntos como:

- Nombre del servidor
- Tipo de partición de discos
- Requerimientos de Hardware
- Directorios de trabajo
- Servicios
- Software estándar

3.1.1. Nombre del servidor

El nombre de la estación de trabajo o servidor deberá ser único dentro de toda la red de la Universidad Internacional SEK, por este motivo, hemos estructurado el siguiente estándar:

cciiiaaafnn

Donde:

Código	Descripción
cc=	Código de país ISO
Iii=	Código de ciudad IATA
Aaa=	Nombre del Campus
f=	Función que desempeña: M=Mail D=Dominio F=FTP S=SNA Q=SQL H=Home B=Backup L=Cluster Server

	V=Virtual SQL W=Web Server T=MTS Server
nn=	Número secuencial

Tabla 11: Nomenclatura de Servidor

Ejemplo 1, tenemos un servidor de FTP que se encuentra ubicado en el campus de Carcelén en la ciudad de Quito:

ECUIOCARD01

Ejemplo 2, un servidor de Internet / Intranet que se encuentra ubicado en el mismo campus de Carcelén en la ciudad de Quito y además es el primer servidor de este tipo.

ECUIOGUAD01

Según el estándar planteado, podemos tener hasta 99 servidores de una misma aplicación en un único lugar.

3.1.2. Tipo de partición de discos

Todos los servidores de la Universidad Internacional SEK tengan como sistema operativo Windows 2003, deberán tener particiones **NTFS** para los volúmenes de datos de su servidor.

Adicionalmente se deberá respetar la estructura recomendada por los fabricantes de software como son: Sistema Operativo en un volumen y datos en otro volumen.

Tenemos dos volúmenes bien definidos, uno para el sistema operativo y otro para los datos de las aplicaciones.

El sistema operativo deberá tener un arreglo de discos Mirror, el mismo que permite tener una completa redundancia ante cualquier problema o falla.

Los datos, al igual que el sistema operativo se encuentran en un arreglo de discos RAID-5, el mismo que permite mayor acceso y seguridad a la información.

Con esta configuración estamos seguros de que las aplicaciones aquí instaladas serán 100% seguras, no tendremos que solucionar problemas de daños de discos.

Adicionalmente debemos estar seguros de que el volumen destinado para sistema operativo sea solo utilizado por este y que los datos de usuarios sean solo utilizados para esta función. Los core de las aplicaciones deberán estar instaladas en los volúmenes del Sistema Operativo y los datos deberán estar en el volumen de datos.

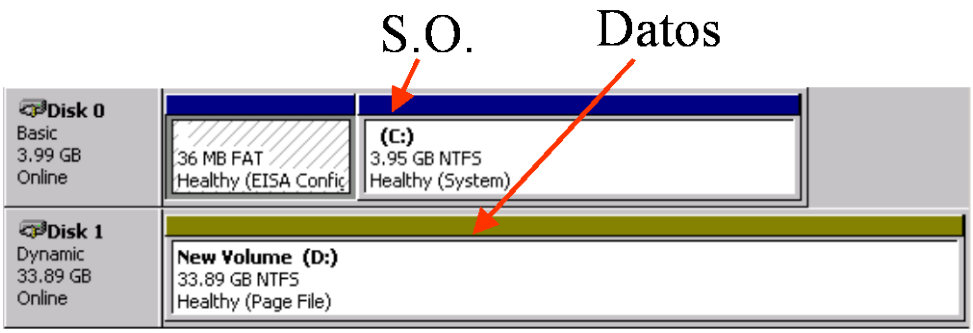


Figura 9: Arreglo de Disco

3.1.3. Requerimientos de Hardware

3.1.3.1. Requerimientos mínimos para Microsoft Windows 2003 Server

- Procesador Pentium Intel de 600 Mhz mínimo
- Soportados un máximo de cuatro procesadores por computador
- 512 MB en RAM
- Partición de sistema mínimo de 2 GB en Mirror
- Partición de datos en RAID-5
- Monitor VGA ó superior
- CD-ROM ó DVD
- Tarjeta de red

3.1.4. Directorios de trabajo

Los directorios de trabajo en los servidores de Windows 2003 Server y UNIX también se encuentran estandarizados y el esquema es el siguiente:

Uso	**Descripción**	**Directorio sugerido**	**Sugerencia nombre de recurso**
Archivo de programas locales	Directorio para instalación de aplicaciones locales	C:\Program Files	-no compartido-
Archivos temporales	Directorio para archivos de uso temporal	C:\Temp	-no compartido-
Archivos de grupo	Directorio para datos de grupo	@:\Group Files*groupname*	Compartido en el nivel del grupo usando el nombre del grupo
Archivos de intercambio	Área de archivos para intercambio entre usuarios	@:\Exchange Files	ExchangeFiles
Archivo de programas compartidos	Archivo de programas para aplicaciones en el servidor	@:\Shared Program Files	SharedProgramFiles
Archivos para Bases de Datos	Directorio de bases de datos	@:\DataBases	Databases
Archivos de usuario	Archivos personales de cada usuario	@\User Files *username*	Compartido a nivel de cada usuario con su nombre
Archivos de distribución	Área para la distribución de archivos	@:\Distribution Files	DistributionFiles
Perfiles de usuario	Perfiles de sistema operativo para	@:\Profiles*user name*	Profiles

	cada usuario		
Directorio de soporte	Contiene archivos para soporte (i386, SPx)	@:\Support Files	SupportFiles

Tabla 12: Estándar de ubicación de Directorios

Donde: @ se debe reemplazar con la letra apropiada para el volumen de datos.

3.1.5. Servicios

A continuación se detalla la lista de servicios que los servidores Windows 2003 Server y UNIX deberán tener configurados para un buen funcionamiento de los equipos.

Services *(GS = Global Infrastructure Server FS = File & Print Server WS = Web Server AS = Application Server)*				
Service	***Description***	***Status***	***Startup***	***Server Role***
Alerter	*Notifies Selected users and computers of Administrative alerts.*	*Started*	*Automatic*	*All*
Application Management	*Provides software installation services such as assign publish and remove.*		*Manual*	*GS*
Clipbook	*Supports Clipbook viewer which Allows pages to been seen by remote Clipbooks.*		*Manual*	*GS(Terminal Server Only)*
COM+Event System	*Provides automatic distribution of events to subscribing COM*	*Started*	*Manual*	*???*

	components.			
Computer Browser	*Maintains an up to date list of the computers on your network and supplies the list to programs that request it.*	*Started*	*Automatic*	*All*
DHCP Client	*Manages network configuration by registering and updating IP addressed and DNS names.*	*Started*	*Automatic*	*All*
Distributed File System	*Manages local volumes distributed across a local or wide area network.*		*Manual*	*None*
Distributed Link Tracking Client	*Sends notifications of files moving between NTFS volumes in a network domain.*	*Started*	*Automatic*	*None*
Distributed Link Tracking Server	*Stores information so that files moved between volumes can be tracked for each volume in the domain.*	*Started*	*Automatic*	*None*
Distributed Transaction Coordinator	*Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.*	*Started*	*Automatic*	*None*
DNS Client	*Resolves and caches*	*Started*	*Automatic*	*All*

	Domain Name System (DNS) names.			
DNS Server	*Answers query and update requests for Domain Name System (DNS) names.*		*Manual*	*None*
Event Log	*Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.*	*Started*	*Automatic*	*All*
Fax Service	*Helps you send and receive faxes*		*Manual*	*None*
File Replication Service	*Maintains file synchronization of file directory contents among multiple servers.*	*Started*	*Automatic*	*GS*
IIS Admin Service	*Allows administration of Web and FTP services through the Internet Information Services snap-in.*	*Started*	*Automatic*	*WS*
Indexing Service			*Manual*	*None*
Internet Connection Sharing	*Provides network address translation, addressing, and name resolution services for All computers on your home network through a dial-up connection.*		*Manual*	*None*

Intersite Messaging	*Allows sending and receiving messages between Windows Advanced Server sites.*	*Started*	*Automatic*	*GS*
IPSEC Policy Agent	*Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.*	*Started*	*Automatic*	*?? Security Dependant*
Kerberos Key Distribution Center	*Generates session keys and grants service tickets for mutual client/server authentication.*	*Started*	*Automatic*	*?? Security Dependant*
License Logging Service				*None*
Local Disk Manager	*Logical Disk Manager Watchdog Service*	*Started*	*Automatic*	*All*
Local Disk Administrative Service	*Administrative service for disk management requests*		*Manual*	*None*
Messenger	*Sends and receives messages transmitted by administrators or by the Alerter service.*	*Started*	*Automatic*	
Net Logon	*Supports pass-through authentication of account logon events for computers in a domain.*	*Started*	*Automatic*	*All*
NetMeeting Remote Desktop Sharing	*Allows authorized people to remotely access your Windows desktop using*		*Manual*	*None*

	NetMeeting.			
Network Connections	*Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.*	*Started*	*Manual*	*All*
Network DDE	*Provides network transport and security for dynamic data exchange (DDE).*		*Manual*	*None*
Network DDE DSDM	*Manages shared dynamic data exchange and is used by Network DDE*		*Manual*	*None*
NT LM Security Support Provider	*Provides security to remote procedure call (RPC) programs that use transports other than named pipes.*		*Manual*	*None*
Performance Logs and Alerts	*Configures performance logs and alerts.*		*Manual*	*None*
Plug and Play	*Manages device installation and configuration and notifies programs of device changes.*	*Started*	*Automatic*	*All*
Print Spooler	*Loads files to memory for later printing.*		*Manual*	*None*
Protected Storage	*Provides protected storage for sensitive data, such as private keys, to prevent access*	*Started*	*Automatic*	*All*

	by unauthorized services, processes, or users.			
QoS RSPV	*Provides network signalling and local traffic control set-up functionality for QoS-aware programs and control applets.*		*Manual*	*None*
Remote Access Auto Connection Manager	*Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.*		*Manual*	*None*
Remote Access Connection Manager	*Creates a network connection.*		*Manual*	*None*
Remote Procedure Call(RPC)	*Provides the endpoint mapper and other miscellaneous RPC services.*	*Started*	*Automatic*	*All*
Remote Procedure Call(RPC) Locator	*Manages the RPC name service database.*	*Started*	*Automatic*	*All*
Remote Registry Service	*Allows remote registry manipulation.*	*Started*	*Automatic*	*??? Depends on Security*
Removable Storage	*Manages removable media, drives, and libraries.*	*Started*	*Automatic*	*None*
Routing and Remote Access	*Offers routing services to businesses in local*		*Disabled*	*None*

	area and wide area network environments.			
RunAs Service	*Enables starting processes under alternate credentials*		*Manual*	*None*
Security Accounts Manager	*Stores security information for local user accounts*	*Started*	*Automatic*	*All*
Server	*Provides RPC support and file, print, and named pipe sharing.*	*Started*	*Automatic*	*All*
Simple Mail Transport Protocol(SMTP)	*Transports electronic mail across a network*		*Manual*	*None*
Smart Card	*Manages and controls access to a smart card inserted into a smart card reader attached to the computer.*		*Manual*	*None*
Smart Card Helper	*Provides support for legacy smart card readers attached to the computer.*		*Manual*	*None*
System Event Notification	*Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.*	*Started*	*Automatic*	*All*
Task Scheduler	*Enables a program to run at a designated time.*		*Manual*	*None*
TCP/IP NetBIOS	*Enables support for*		*Manual*	*None*

Helper Service	*NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.*			
Telephony	*Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.*		*Manual*	*None*
Telnet	*Allows a remote user to log on to the system and run console programs using the command line.*		*Manual*	*None*
Terminal Services	*Provides a multisession environment that Allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.*		*Disabled*	*None*
Uninterruptible Power Supply	*Manages a UPS connected to a computer*		*Manual*	*None*
Utility Manager	*Starts and Configures accessibility tools from one window*		*Manual*	*None*
Windows Installer	*Installs, repairs and removes software according to information*	*Started*	*Manual*	*All*

	in .MSI files.			
Windows Management Instrumentation	*Provides system management information.*	*Started*	*Automatic*	*All*
Windows Management Instrumentation Driver Extension	*Provides systems management information to and from drivers*	*Started*	*Manual*	*???*
Windows Time	*Sets the Computer Clock*	*Started*	*Automatic*	*All*
Workstation	*Provides Network connections and communications*	*Started*	*Automatic*	*All*
World Wide Web Publishing Service	*Provides web connectivity and administration through the Internet Information Service snap-in.*	*Started*	*Automatic*	*Microsoft*

Tabla 13: Lista de Servicios de UNIX y Windows 2003 Server[6]

3.2. Estandarización de nombres de los recursos.

Una correcta administración de usuarios, grupos funcionales, grupos aplicacionales y unidades organizacionales en Windows 2000 y UNIX (OpenLDAP). Estos estándares contemplan varios puntos como:

- Nombres de usuario
- Nombres de grupos globales
- Nombres de grupos aplicaciones
- Unidades organizacionales

[6] Kathy Ivens, Rich Benack, Christian Branson. Windows Server 2003: The Complete Reference, 2003. 1008 p.

3.2.1. Nombres de usuarios

Los nombres para los usuarios se encuentran normados en los estándares del HOST de la Universidad Internacional SEK, por lo que, Active Directory y OpenLDAP deberá acoger este estándar de 8 caracteres.

3.2.2. Nombres de grupos globales

La función principal de este grupo, es la asociación de usuarios con fines comunes, es decir, los usuarios de Telecomunicaciones, los usuarios de Ingeniería, los usuarios de Administrativos, etc. Es claro ver que los usuarios se encuentran agrupados por funciones específicas. Otra función es la portabilidad de los grupos, es decir, podemos tener grupos que necesitan tener recursos en un dominio diferente al que normalmente utilizan.

El estándar propuesto es el siguiente:

Nnnnn.GF

Donde:

Código	Descripción
GF=	Ubicación
Nnnnn=	Nombre claro del grupo

Tabla 14: Estándar de nomenclatura de grupos.

Ejemplo 1, un grupo que pertenece a la Facultad de Comunicaciones deberá llamarse así:

Comunicaciones.carcelen

3.2.3. Nombres de grupos aplicacionales

A diferencia de los grupos globales, la función es de asignar permisos a un recurso o aplicación, a este tipo de grupo se pueden y deben añadir los grupos globales y eventualmente usuarios preferiblemente **no**.

El estándar presentado para este tipo de grupos es el siguiente:

Nnnnnn.GA

Donde:

Código	Descripción
GA=	Ubicación
Nnnnn=	Nombre claro del grupo

Tabla 15: Estándar de nomenclatura para grupos aplicacionales.

Ejemplo 1, la aplicación Office para la Universidad Internacional SEK deberá llamarse así:

Office.carcelen

3.2.4. Unidades organizacionales

Para un mejor manejo de usuarios, grupos, permisos y políticas de seguridad se han definido unidades organizacionales. Estas unidades fueron creadas en forma similar a como se encuentra organizado de forma física de la universidad, es decir, tenemos campus, facultad y laboratorios.

En la raíz de cada uno de los dominios en el Active Directory, se creara una única OU (Unidad Organizacional), llamada Centro de Procesamiento <uisek.edu.ec>, por ejemplo, para el dominio del campus de Carcelén, la OU se llama Centro de Procesamiento UIO.

Dentro de estas unidades se han definido según la necesidad varias nuevas unidades, las mismas que representan las facultades donde se encuentran los laboratorios o hosts.

Los usuarios y grupos funcionales se encontrarán en este último nivel de OU's, con lo que garantizamos que ningún usuario quedará fuera de un grupo o política de seguridad de Windows 2003 Server y UNIX.

4. DISEÑO Y CONFIGURACIÓN DE DOMINIOS

Esta investigación explica cómo crear una infraestructura de red, empezando por la instalación y configuración del sistema operativo Microsoft Windows Server 2003 como un controlador de dominio y OpenLDAP para la plataforma Linux. Esta infraestructura permite conocer y evaluar las dos tecnologías.

4.1. CONFIGURACIÓN DE DOMINIOS DE LOS DIFERENTES CAMPUS.

4.1.1. Configuración del Dominio Secundario guapulo.uisek.edu.ec y carcelen.uisek.edu.ec en Active Directory.

Se necesitará un servidor con dos unidades de disco o con una única unidad pero con dos particiones.

El primer disco o partición contiene Windows Server 2003 y los demás archivos de la infraestructura común, como los paquetes de Windows Installer y los archivos de origen de la aplicación. El segundo disco o partición está reservada para los archivos de registro de Active Directory.

Cada disco o partición debe contener varios gigabytes de información y tener el formato del sistema de archivos NT (NTFS).

Para empezar el procedimiento de instalación, inicie directamente desde el CD de Windows Server 2003. El CD-ROM debe admitir CD de inicio.

El programa de instalación crea las particiones del disco en el equipo que ejecuta Windows Server 2003, da formato a la unidad y copia los archivos de instalación del CD al servidor.

1. Inserte el CD de Windows Server 2003 en la unidad de CD-ROM.

2. Reinicie el equipo. Si se le indica, presione cualquier tecla para iniciar desde el CD. Comenzará entonces la instalación de Windows Server 2003.

3. En la pantalla Programa de instalación, presione ENTRAR.

4. Acepte el contrato de licencia presionando F8.

5. Siga las instrucciones para eliminar todas las particiones del disco existentes. Los pasos exactos variarán según el número y el tipo de particiones que tenga ya el equipo. Siga eliminando particiones hasta que todo el espacio del disco tenga la etiqueta Espacio no particionado.

6. Cuando todo el espacio del disco tenga la etiqueta Espacio no particionado, presione C para crear una partición en el espacio no particionado de la primera unidad de disco (si procede).

7. Si su servidor tiene una única unidad de disco, divida el espacio en disco disponible por la mitad para crear dos particiones de igual tamaño. Elimine el valor predeterminado de espacio total. Escriba el valor de la mitad del espacio en disco total en el símbolo del sistema Crear partición de tamaño (en MB) y presione ENTRAR. (Si su servidor tiene dos unidades de disco, escriba el tamaño total de la primera unidad en este símbolo del sistema.)

8. Cuando haya creado la partición Nueva “uisek”, presione ENTRAR.

9. Seleccione Formatear la partición utilizando el sistema de archivos NTFS <rápido> y, a continuación, presione ENTRAR.

El programa de instalación de Windows Server 2003 dará formato a la partición y copiará los archivos del CD de Windows Server 2003 a la unidad de disco duro. Se reiniciará el equipo y continuará el programa de instalación de Windows Server 2003.

1. El Asistente para la instalación de Windows Server 2003 detecta e instala los dispositivos.

2. En el cuadro de diálogo Configuración regional y de idioma, realice los cambios necesarios para Ecuador.

3. En el cuadro de diálogo Personalice su software, escriba Dominio Guápulo en el cuadro Nombre y UISEK en el cuadro Organización. Haga clic en Siguiente.

4. Escriba la Clave del producto en los cuadros de texto provistos para ello y, después, haga clic en Siguiente.

5. En el cuadro de diálogo Modos de licencia, seleccione el modo de licencia adecuado para la universidad y, a continuación, haga clic en Siguiente.

6. En el cuadro de diálogo Nombre del equipo y contraseña del administrador, escriba el nuevo nombre del equipo GUAPULO UISEK en el cuadro de nombre del equipo y, a continuación, haga clic en Siguiente.

7. En el cuadro de diálogo Configuración de fecha y hora, corrija, si es necesario, la fecha y la hora actuales y, después, haga clic en Siguiente.

8. En el cuadro de diálogo Configuración de red, asegúrese de que la opción Configuración típica está seleccionada y, a continuación, haga clic en Siguiente.

9. En el cuadro de diálogo Grupo de trabajo o dominio del equipo (está seleccionado No de manera predeterminada), haga clic en Siguiente.

10. Se reinicia el servidor y se carga el sistema operativo desde la unidad de disco duro.

El espacio no particionado de la instalación de Windows Server 2003 debe recibir formato para que el sistema operativo pueda tener acceso a él. La administración de discos y particiones se realiza mediante el complemento Administración de equipos de Microsoft Management Console.

1. Presione Ctrl+Alt+Supr e inicie sesión en el servidor como administrador.

2. Haga clic en el botón Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Administración de equipos.

3. Para definir y dar formato al espacio no particionado, haga clic en Administración de discos.

4. Haga clic con el botón secundario del mouse en No asignado en el Disco 1.

5. Para definir una partición, haga clic en Partición nueva y luego en Siguiente para continuar.

6. Seleccione Partición primaria (opción predeterminada) y, a continuación, haga clic en Siguiente para continuar.

7. Haga clic en Siguiente con la opción Tamaño de partición en MB establecida en el valor predeterminado.

8. Para Asignar la letra de unidad siguiente, seleccione L y, a continuación, haga clic en Siguiente para continuar.

9. En Formatear esta partición con la configuración siguiente, haga clic en Dar formato rápido. Haga clic en Siguiente y luego en Finalizar para completar la configuración de la unidad de disco secundaria.

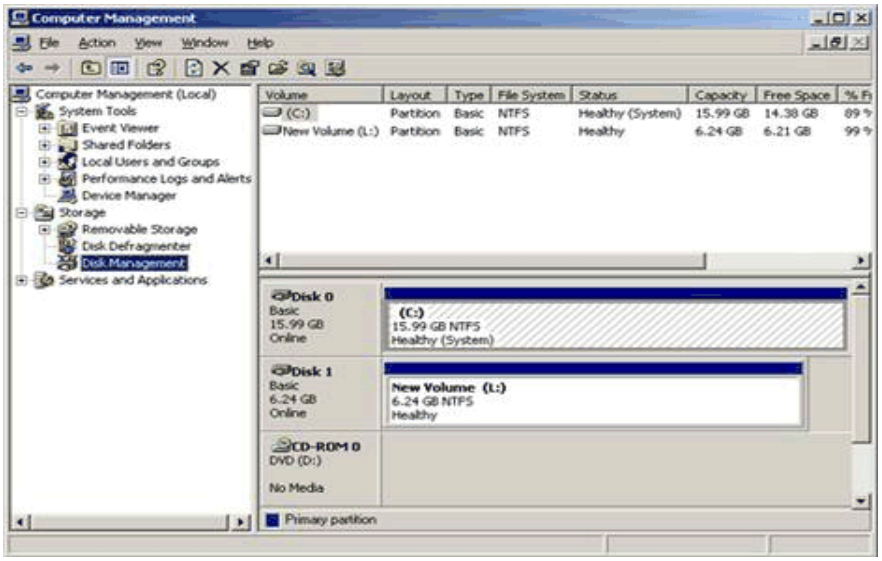


Figura 10: Consola de Administración de Equipos.

10. Cierre la consola de Administración de equipos.

El Servicio de nombres de dominio (DNS) y DCPromo (la herramienta de la línea de comandos que crea DNS y Active Directory) pueden instalarse manualmente o mediante el Asistente para configurar su servidor de Windows Server 2003. En esta tesis se utilizan las herramientas manuales para realizar la instalación.

1. Haga clic en el botón Inicio y en Ejecutar, escriba DCPROMO y, a continuación, haga clic en Aceptar.

2. Cuando aparezca el Asistente para instalación de Active Directory, haga clic en Siguiente para iniciar la instalación.

3. Después de revisar la información de Compatibilidad de sistema operativo, haga clic en Siguiente.

4. Seleccione Controlador de dominio para un dominio nuevo (opción predeterminada) y, a continuación, haga clic en Siguiente.

5. Seleccione Dominio en un nuevo bosque (opción predeterminada) y, a continuación, haga clic en Siguiente.

6. Para Nombre DNS completo, escriba guapulo.uisek.edu.ec y, después, haga clic en Siguiente.

7. Haga clic en Siguiente para aceptar la opción predeterminada Nombre NetBIOS del dominio de GUAPULO. (El nombre NetBIOS proporciona compatibilidad de bajo nivel.)

8. En la pantalla Carpetas de la base de datos y del registro, establezca la Carpeta de registro de Active Directory de forma que apunte a la carpeta \Windows\NTDS y, a continuación, haga clic en Siguiente para continuar.

9. Deje la ubicación de la carpeta predeterminada para Volumen del sistema compartido y, después, haga clic en Siguiente.

10. En la pantalla Diagnósticos de registro de DNS, haga clic en Instalar y configurar el servidor DNS en este equipo. Haga clic en Siguiente para continuar.

11. Seleccione Permisos compatibles sólo con sistemas operativos de servidor Windows Server 2003 (opción predeterminada) y, a continuación, haga clic en Siguiente.

12. Escriba la contraseña para Contraseña de modo de restauración y Confirmar contraseña y, después, haga clic en Siguiente para continuar.

13. Haga clic en Aceptar para confirmar la advertencia de que se va a asignar una dirección IP de forma dinámica a un servidor DNS.

14. Si dispone de varias interfaces de red, seleccione la interfaz de red 192.168.1.0 de la lista desplegable Elegir conexión y, a continuación, haga clic en Propiedades.

15. En la sección Esta conexión utiliza los siguientes elementos, haga clic en Protocolo Internet (TCP/IP) y luego en Propiedades.

16. Seleccione Usar la siguiente dirección IP y, a continuación, escriba 192.168.1.2 para Dirección IP. Presione dos veces la tecla Tab y, después, escriba 192.168.1.1 para Puerta de enlace predeterminada. Escriba 127.0.0.1 para Servidor DNS preferido y, a continuación, haga clic en Aceptar. Haga clic en Cerrar para continuar.

17. Haga clic en Finalizar cuando termine el Asistente para instalación de Active Directory.

18. Haga clic en Reiniciar ahora para reiniciar el equipo.

El mismo procedimiento descrito se aplica para la creación del dominio carcelen.uisek.edu.ec en el campus “Miguel de Cervantes”.

4.2. CREACIÓN Y CONFIGURACIÓN DEL DOMINIO PRINCIPAL

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.[7]

SMB (acrónimo de Server Message Block) Protocolo de red que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows. SMB fue originalmente inventado por IBM, pero la versión más común hoy en día es la modificada ampliamente

[7] http://es.wikipedia.org/wiki/LDAP

por Microsoft. Microsoft renombró SMB a Common Internet File System (CIFS) en 1998 y añadió más características, que incluyen soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo.[8]

OpenLDAP es una implementación libre y open source del protocolo Lightweight Directory Access Protocol (LDAP) desarrollado por el OpenLDAP Project. Está liberada bajo su propia licencia OpenLDAP Public License. LDAP es un protocolo independiente de la plataforma. Muchas distribuciones Linux incluyen el software OpenLDAP para su soporte.[9]

SAMBA es un conjunto de programas, originalmente creados por Andrew Tridgell y actualmente mantenidos por The SAMBA Team, bajo la Licencia Publica General GNU, y que implementan en sistemas basados sobre UNIX® el protocolo SMB. Sirve como reemplazo total para Windows® NT, Warp®, NFS® o servidores Netware®.[10]

Equipamiento lógico requerido.

1. openldap-2.3.27
2. openldap-clients-2.3.27
3. openldap-servers-2.3
4. authconfig-5.3.12
5. samba-common
6. samba-client
7. samba-3.0.
8. smbldap-tools-0.9.1-1

4.2.1. Instalación a través de yum.

Yum -y install openldap openldap-clients openldap-servers authconfig authconfig-gtk samba samba-client samba-common

[8] http://es.wikipedia.org/wiki/CIFS
[9] http://www.alcancelibre.org/staticpages/index.php/SAMBALDAP-CENTOS5
[10] http://www.tutorial-enlace.net/tutorial-Como_configurar_SAMBA-15036.html

4.2.2. Procedimiento

4.2.2.1 Openldap y Autenticación

Copiar el archivo de esquema de samba al directorio de esquemas de openLDAP:

```
cp /usr/share/doc/samba-*/LDAP/samba.schema /etc/openldap/schema/
```

Tabla 16: Copia esquema de Samba.

Editar el fichero **/etc/openldap/slapd.conf** y agregar una línea más para que openLDAP soporte el esquema de samba. El fichero quedaría como lo siguiente:

```
# # See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
```

Tabla 17: Edición archivo slapd.conf

Añadir al final del fichero /etc/openldap/slapd.conf :

database bdb

suffix **"dc=carcelen,dc=edu,dc=ec"**

rootdn **"cn=Administrador,dc=carcelen,dc=edu,dc=ec"**

 # Este password obtenido previamente al digitar slappasswd

rootpw {SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

directory /var/lib/ldap/autenticar

Indices to maintain for this database

#index objectClass eq,pres

#index ou,cn,mail,surname,givenname eq,pres,sub

#index uidNumber,gidNumber,loginShell eq,pres

#index uid,memberUid eq,pres,sub

#index nisMapName,nisMapEntry eq,pres,sub

index objectClass eq

index cn pres,sub,eq

index sn pres,sub,eq

index uid pres,sub,eq

index displayName pres,sub,eq

index uidNumber eq

index gidNumber eq

index memberUID eq

index sambaSID eq

index sambaPrimaryGroupSID eq

index sambaDomainName eq

index default sub

Tabla 18: Ingreso de parámetros de configuración en archivo slapd.conf

Tenemos que configurar los parámetros globales como cliente (NSS), el mismo servidor localhost en **/etc/ldap.conf** :

host 127.0.0.1

base dc=carcelen,dc=edu,dc=ec

Tabla 19: Configuración archivo /etc/ldap.conf

También tenemos que configurar el cliente LDAP en **/etc/openldap/ldap.conf** :

```
HOST 127.0.0.1
BASE dc=carcelen,dc=edu,dc=ec
```

Tabla 20: Configuración archivo /etc/openldap/ldap.conf

Iniciamos el servicio LDAP y configuramos que arranque por defecto:

```
service ldap start
chkconfig ldap on
```

Tabla 21: Inicio servicio ldap

Configuramos la autenticación de Linux con ***authconfig-tui*** :

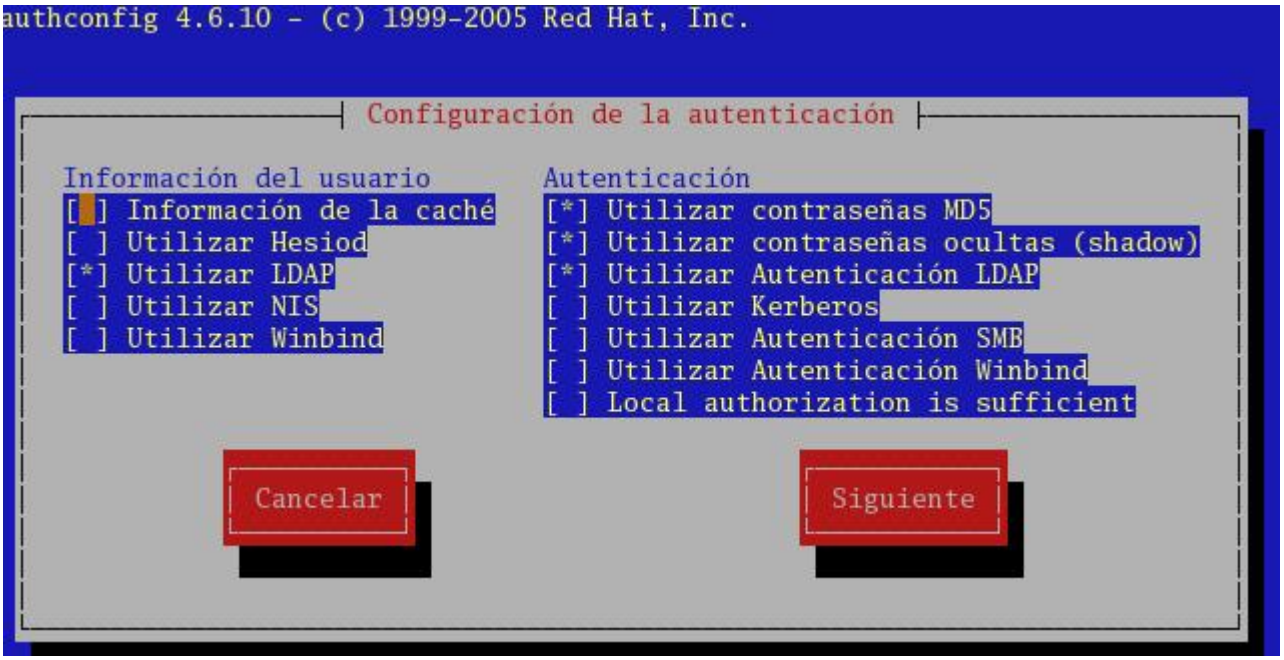


Figura 11: Configuración de la Autenticación.

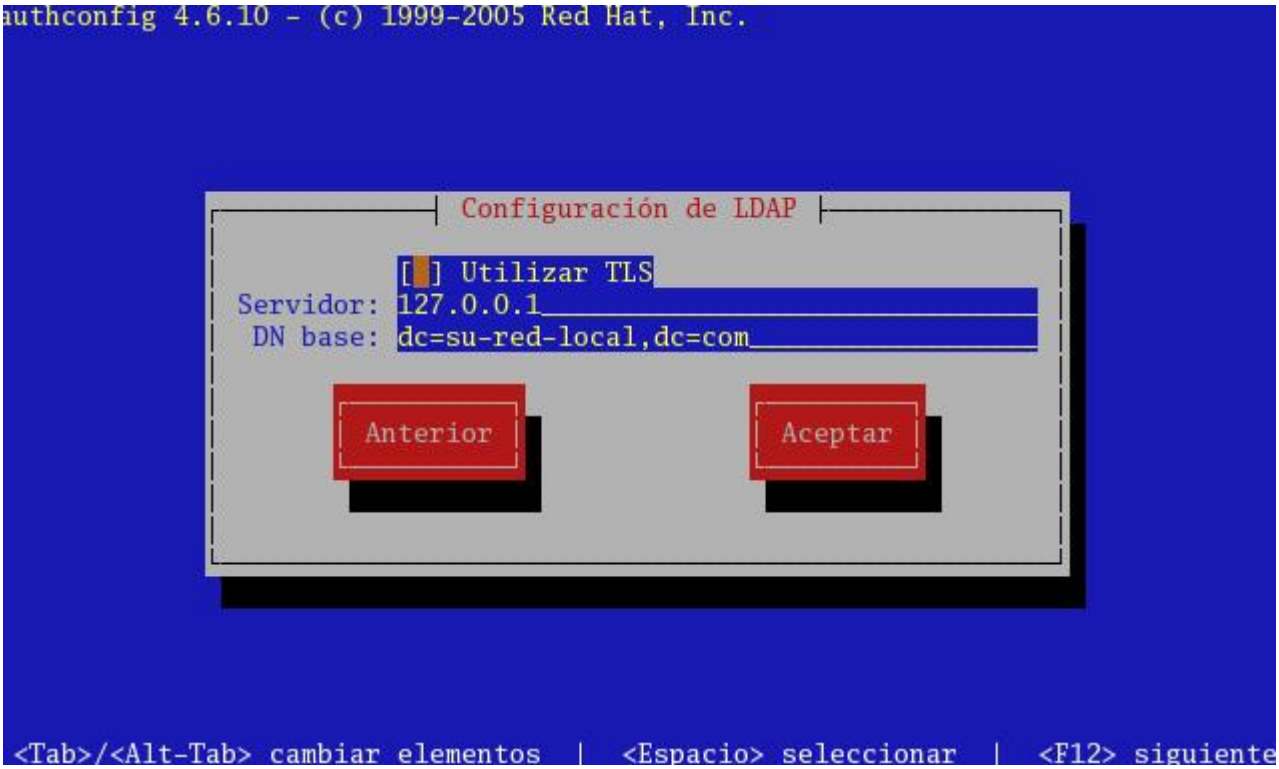


Figura 12: Definir Servidor LDAP.

4.2.2.2 Samba e Integración Ldap

Ahora configuremos Samba en **/etc/samba/smb.conf**

# Samba PDC openLDAP para CentOS 5
workgroup = uisek.edu.ec
server string = Samba Server
netbios name = LINUX

----- Parametros LDAP -----

 # Quien va a ser el usuario administrador del dominio
admin users = Administrator @"Domain Admins"
passdb backend = ldapsam:ldap://localhost

#?Sufijo ldap para todas las entradas siguientes
ldap suffix = dc=carcelen,dc=edu,dc=ec

 # OU de usuarios netbios
ldap user suffix = ou=People

 # OU de Grupos netbios
ldap group suffix = ou=Group

 # Cuentas maquinas netbios
ldap machine suffix = ou=Computers

 # La cuenta administrador openLDAP
ldap admin dn = cn=Administrador,dc=uisek.edu.ec

 # Sincronizacion de cuentas LDAP, NT y LM
ldap passwd sync = yes

 # Agregado de cuentas maquina automáticamente
add machine script = /usr/sbin/smbldap-useradd -w %u

```
#ldap ssl = start tls
#add user script = /usr/sbin/smbldap-useradd -m "%u"
#ldap delete dn = Yes
#delete user script = /usr/sbin/smbldap-userdel "%u"
#add group script = /usr/sbin/smbldap-groupadd -p "%g"
#delete group script = /usr/sbin/smbldap-groupdel "%g"
#add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
#delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
#set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
#ldap replication sleep = 1000 # Tiempo de replicacion entre servidores

# ----- FIN DE PARAMETROS LDAP

# Asegurarse de tener los siguiente parámetros activado de la siguiente
forma:

security = user

encrypt passwords = yes
os level = 65
domain master = yes
preferred master = yes
domain logons = yes
```

Tabla 22: Edición archivo smb.conf

Necesitamos hacer saber a samba cual es el password del usuario *Administrador* de OpenLDAP para que pueda conectarse al directorio:

```
smbpasswd –w password
```

Tabla 23: Configuración de contraseña OpenLDAP con Samba.

Nos indicara el siguiente mensaje y confirmará que samba ya pueda autenticarse en openLDAP:

Setting stored password for "cn=Administrador,dc=carcelen,dc=edu,dc=ec" in secrets.tdb

Testeamos y reiniciamos samba:

Testparm
service smb restart

Tabla 24: Iniciar servicio Samba.

4.2.2.3. Smbldap-tools y repositorios extras.

Por alguna razón el que viene junto con samba no funcionó así que opté por usar el del repositorio DAG.

En nuestro caso instalamos el RPM de http://dag.wieers.com:

wget http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm

Tabla 25: Configuración para el uso de repositorios de DAG

Ahora ya podemos comprobar en */etc/yum.repos.d/rpmforge.repo :*

[rpmforge]
name = Red Hat Enterprise $releasever - RPMforge.net - dag
#baseurl = http://apt.sw.be/redhat/el5/en/$basearch/dag
mirrorlist = http://apt.sw.be/redhat/el5/en/mirrors-rpmforge
#mirrorlist = file:///etc/yum.repos.d/mirrors-rpmforge
enabled = 0
protect = 0
gpgkey = file:///etc/pki/rpm-gpg/RPM-GPG-KEY-rpmforge-dag
gpgcheck = 1

Tabla 26: Comprobación de repositorios.

Deshabilito el repositorio por defecto (enabled=0).

Ahora ya es posible instalar el smbldap-tools :

yum install smbldap-tools --enablerepo=rpmforge

Tabla 27: Instalación de smbldap-tools

Ahora averigüemos el SID de nuestro servidor Samba:

net getlocalsid

Tabla 28: SID Servidor Samba

Nos mostrará un mensaje similar al siguiente y debemos de anotarlo o copiarlo:
SID for domain LINUX is: S-1-5-21-XXXXXXXXXX-XXXXXXXXXX
Procedemos a configurar el acceso smbldap-tools a la BD de openLDAP en */etc/smbldap-tools/smbldap_bind.conf* :

 # password es el password sin cifrar del Administrador openLDAP

*slaveDN="**cn=Administrador,dc=carcelen,dc=edu,dc=ec**"*

*slavePw="**password**"*

*masterDN="**cn=Administrador,,dc=carcelen,dc=edu,dc=ec**"*

*masterPw="**password**"*

Tabla 29: Configuración de acceso de Samba a OpenLDAP

Y la configuración principal en ***/etc/smbldap-tools/smbldap.conf*** :

 # Aquí el SID que copiamos

SID="S-1-5-21-XXXXXXXXXXX-XXXXXXXXXX-XXXXXXX"

 # El nombre del DOMINIO SAMBA workgroup = DOMAIN

sambaDomain=uisek.edu.ec

slaveLDAP="127.0.0.1"

slavePort="389"

masterLDAP="127.0.0.1"

masterPort="389"

Para usar TLS con LDAP

(También usará el puerto 389)

ldapTLS="1"

 # verify="optional"

#cafile="/etc/smbldap-tools/ca.pem"

#clientcert="/etc/smbldap-tools/smbldap-tools.pem"

#clientkey="/etc/smbldap-tools/smbldap-tools.key"

 # Sufijo por defecto a todas las entradas posteriores

suffix="dc=uisek.edu.ec"

 # Usuarios del dominio

usersdn="ou=People,${suffix}"

 # Cuentas Computadoras del dominio

computersdn="ou=Computers,${suffix}"

 # Cuentas Grupo

groupsdn="ou=Group,${suffix}"

 # Si somos un Samba Domain Member Server
idmapdn="ou=Idmap,${suffix}"

 # Importante: el nextUID para calcular el codigo siguiente usuario o grupo
sambaUnixIdPooldn="sambaDomainName=DOMAIN,${suffix}"

scope="sub"
hash_encrypt="SSHA"

crypt_salt_format="%s"

userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"

 # LINUX es el nombre NETBIOS DEL SERVER netbios name = LINUX
userSmbHome="\LINUX\%U"

 # Perfiles
userProfile="\LINUX\profiles\%U"

 # Letra de la unidad para su carpeta personal
userHomeDrive="Z:"

#userScript="logon.bat"

with_smbpasswd="0"

smbpasswd="/usr/bin/smbpasswd"

with_slappasswd="0"

slappasswd="/usr/sbin/slappasswd"

Tabla 30: Configuración de Samba (smb.conf)

Ahora debemos crear la estructura de dominio en openldap con el comando y digitar el password de *Administrator* que es el administrador del dominio:

smbldap-populate -a Administrator

Tabla 31: Estructura de Dominio OpenLDAP

Con un resultado similar al siguiente:

Populating LDAP directory for domain DOMAIN (S-1-5-21-WEÑHFÑIOWEHFIOFMBIJBIOEJTOPBJ)

(using builtin directory structure)

adding new entry: dc=carcelen,dc=edu,dc=ec

adding new entry: ou=People, dc=carcelen,dc=edu,dc=ec

adding new entry: ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: ou=Computers, dc=carcelen,dc=edu,dc=ec

adding new entry: ou=Idmap, dc=carcelen,dc=edu,dc=ec

adding new entry: uid=Administrator,ou=People, dc=carcelen,dc=edu,dc=ec

adding new entry: uid=nobody,ou=People, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Domain Admins,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Domain Users,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Domain Guests,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Domain Computers,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Administrators,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Account Operators,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Print Operators,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Backup Operators,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: cn=Replicators,ou=Group, dc=carcelen,dc=edu,dc=ec

adding new entry: sambaDomainName=DOMAIN, dc=carcelen,dc=edu,dc=ec

Please provide a password for the domain Administrator:
Changing password for Administrator
New password :
Retype new password :

Ahora veremos la asociación de los builtin groups del dominio SAMBA con los grupos openLDAP creados:

```
net groupmap list
```

Tabla 32: Lista de grupos en OpenLDAP

Con un resultado similar al siguiente:
Domain Admins (S-1-5-21-XXXXXXXXXX-XXXXXXXX-512) -> Domain Admins
Domain Users (S-1-5-21-XXXXXXXXXX-XXXXXXXX-513) -> Domain Users
Domain Guests (S-1-5-21-XXXXXXXXXX-XXXXXXXX-514) -> Domain Guests
Domain Computers (S-1-5-21-XXXXXXXXXX-XXXXXXXX-515) -> Domain Computers
Administrators (S-1-5-32-544) -> Administrators
Account Operators (S-1-5-32-548) -> Account Operators
Print Operators (S-1-5-32-550) -> Print Operators
Backup Operators (S-1-5-32-551) -> Backup Operators
Replicators (S-1-5-32-552) -> Replicators

Ahora podemos crear una cuenta de usuario Windows (-a), se le crea una carpeta personal (-m), especificando que no tenga una ruta Profile (opción -F) y le asignamos una contraseña:

```
Smbldap-useradd –a -m -F "" root
smbldap-passwd tesis
```

Tabla 33: Creación de usuario Windows

Reiniciamos samba y ldap:

service ldap restart
service smb restart

Tabla 34: Reinicio de Servicios Samba y LDAP

4.2.3. Uniendo máquinas al dominio del Controlador Primario de Dominio.

En este proceso no es necesario crear cuentas máquinas debido a que agregamos en el archivo **/etc/samba/smb.conf** el script correspondiente salvo posiblemente en plataformas antiguas.

4.2.3.1. Windows 95/98/ME y Windows XP Home

Ya que los sistemas con Windows 95/98/ME y Windows XP Home no incluyen una implementación completa como miembros de dominio, no se requieren cuentas de confianza. El procedimiento para unirse al dominio es el siguiente:

- Acceder hacia Menú de inicio → Configuraciones → Panel de control → Red.
- Seleccione la pestaña → Configuración
- Seleccione → Cliente de redes Microsoft
- Haga clic en el botón de propiedades
- Seleccione → Acceder a dominio de Windows NT y especifique el dominio correspondiente.
- Clic en todos los botones → Aceptar → reinicie el sistema.
- Acceda con un usuario que haya sido creado con smbldap-useradd en el directorio LDAP, o una cuenta de usuario que pertenezca a la OU=Domain Admins

4.2.3.2. Windows 2000/2003 y Windows XP Profesional

- Clic derecho en el icono de → Mi PC.
- Seleccionar → Propiedades
- Haga clic en la pestaña de → Identificación de red → o → Nombre del sistema.
- Clic en el botón → Propiedades.

- Clic en el botón → Miembro de dominio.
- Ingrese el nombre del dominio y el nombre de la máquina y haga clic en el botón → Aceptar.
- Aparecerá un diálogo que preguntará por una cuenta y clave de acceso con privilegios de administración en el servidor. Especifique el usuario: *Administrator* y la clave de acceso que se le asignó.
- Deberá mostrarse un mensaje emergente de confirmación que dice «Bienvenido a carcelen.uisek.edu.ec»
- Reinicie el sistema
- Acceda con un usuario que haya sido creado con smbldap-useradd en el directorio LDAP, o una cuenta de usuario que pertenezca a la OU=Domain Admin.

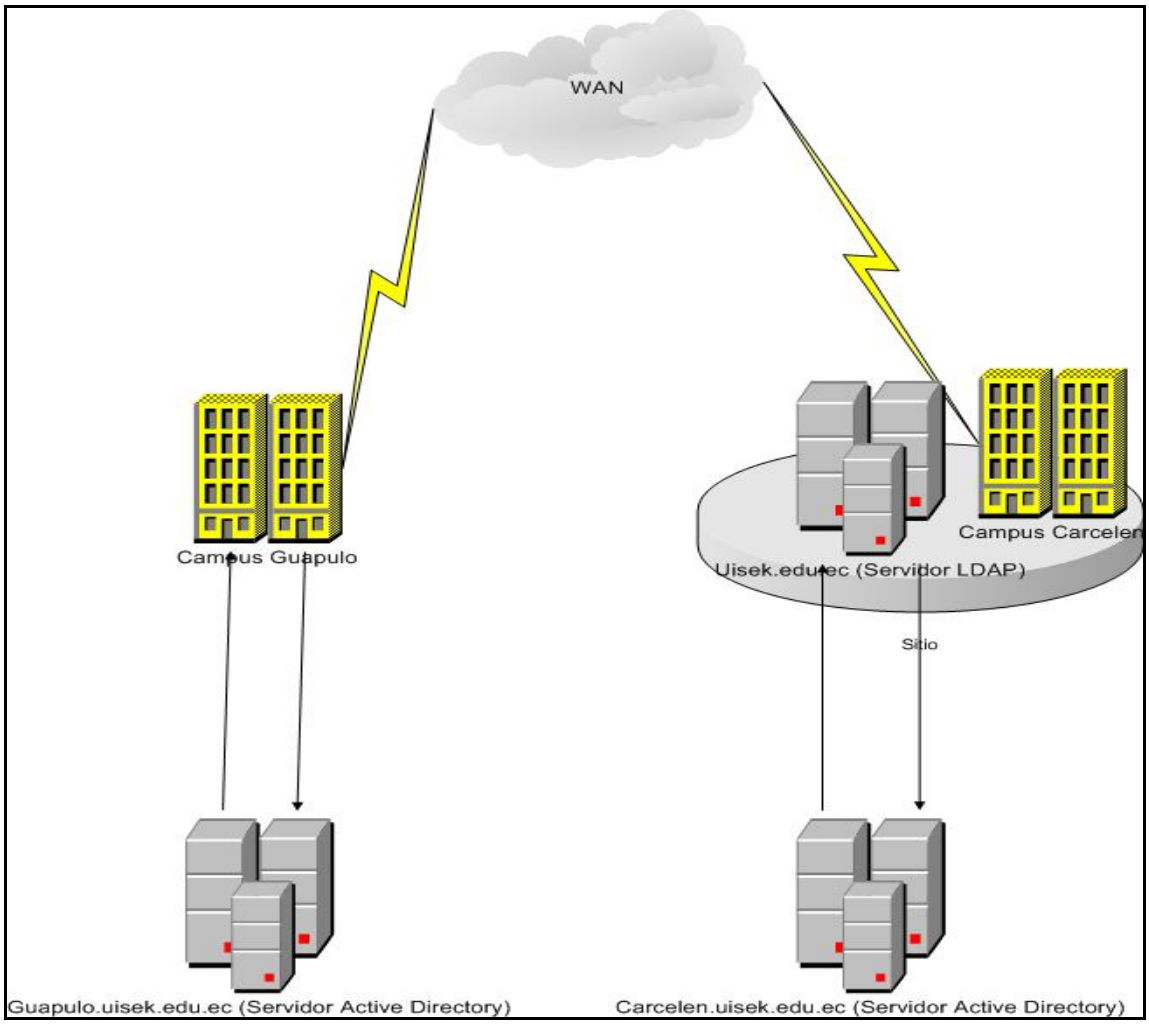


Figura 13: Red Universidad Internacional SEK

4.3. BACKUP ACTIVE DIRECTORY

Realizar backups del Active Directory es una tarea imprescindible entre las tareas de administración de nuestro dominio, sobre todo si este es el único en la red y no esta apoyado por otro controlador adicional.

Para realizar este backup podemos utilizar cualquier utilidad como por ejemplo Ntbackup incorporada en MS WindowsServer. Debemos abrir Ntbackup (desde menú inicio, ejecutar y teclear ntbackup) y seleccionar system state a la hora de realizar un backup.

Una vez seleccionado system state pulsamos iniciar y nos aparecerá un cuadro con opciones avanzadas además de tener la posibilidad de programar el backup para que se realice de forma periódica.

Entre los contenidos del backup de system state esta la base de datos NTDS.dit del Directorio Activo y el contenido del volumen de sistema (SYSVOL), independiente de que el servidor sea controlador de dominio o no, contendrá también los ficheros de arranque (NTLDR, boot.ini, NTDetect.com), el registro y el COM+. Además si se trata de un Windows 2000 o Server 2003 que actué como entidad certificadora se copiara también el almacén de certificados (certificate store).

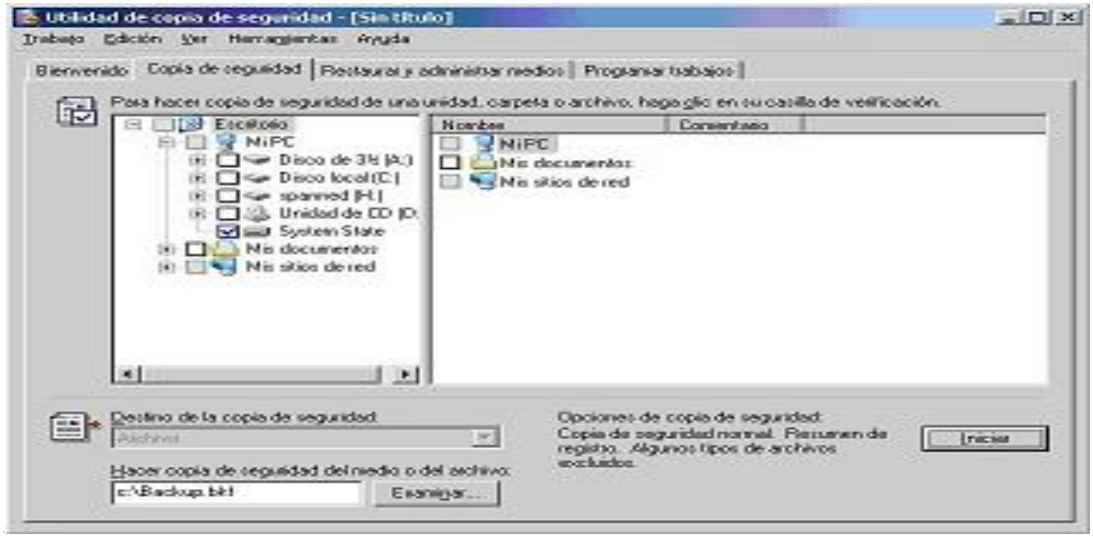


Figura 14: Utilidad de Copia de Seguridad.

4.4. RESTAURACIÓN DE ACTIVE DIRECTORY

El procedimiento de restauración del Directorio Activo, es una tarea delicada de realizar.

Esta restauración depende mucho del número de controladores de dominio en la red.

Básicamente existen 3 tipos de restauraciones:

- **Primaria (primary)**: Este tipo de restauración se realiza cuando tenemos un único Controlador de Dominio.
- **Normal (non-authoritative):** Consiste en restaurar la base de datos del active directory pero de manera que no se replicaran a otros controladores de dominio.
- **Autoritativa (Authoritative restore):** Con este procedimiento los cambios se replicaran a los otros controladores de dominio. Para realizar este procedimiento debemos de realizar primero una restauración no autoritativa y luego mediante la utilidad NTDSUTIL realizar una restauración autoritativa. Este procedimiento se suele realizar cuando queremos restaurar algún complemento del Sistema Operativo como una cuenta de usuario, equipo, DC.

4.4.1. Restauración Normal o No autoritativa

El proceso de realizar los diferentes tipos de restauraciones es similar, a continuación se explica la manera de realizar una restauración normal (No autoritativa) y los diferentes supuestos en los que podemos encontrarnos:

4.4.1.1. El Sistema Operativo arranca pero la base de datos o algún complemento del dominio esta corrupto.

Si nos encontramos en este caso debemos de arrancar el controlador de dominio en modo restauración del SD.

Para arrancar en este modo debemos de mantener pulsada la tecla F8 durante el arranque del sistema y seleccionar la opción arrancar en modo restauración de SD.

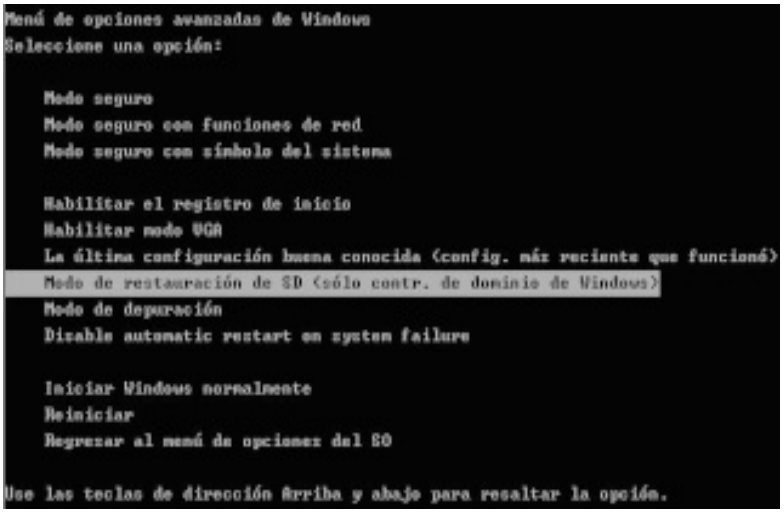


Figura 15: Menú de Opciones Avanzadas de Windows.

Esto nos arrancara el Sistema Operativo en modo recuperación del controlador de dominio y mediante la utilidad Ntbackup nos permitirá restaurar el sistema.

El proceso de restauración mediante el Ntbackup es un wizard donde debemos indicarle la ubicación del backup del system restore así como el modo de restauración:

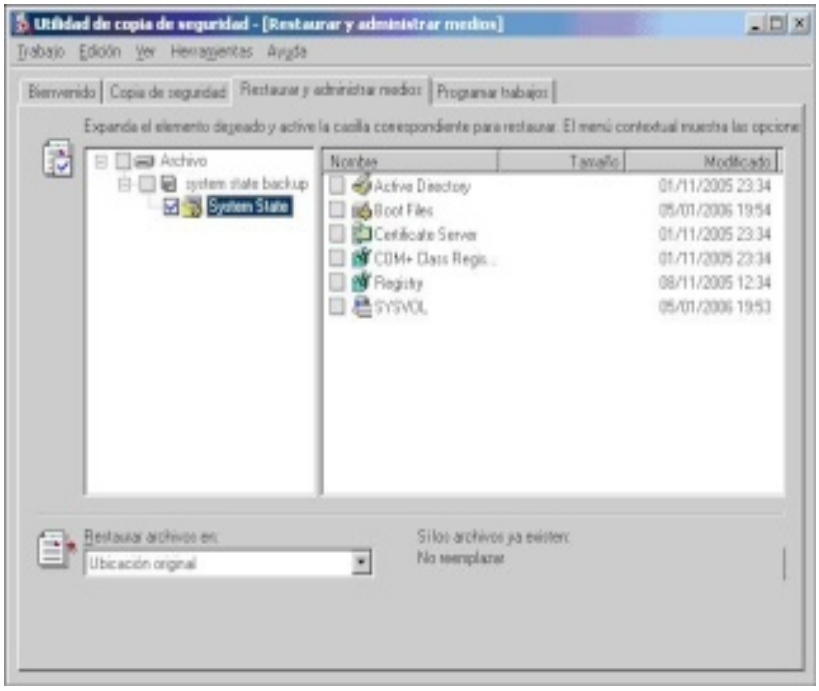


Figura 16: Utilidad de Restauración.

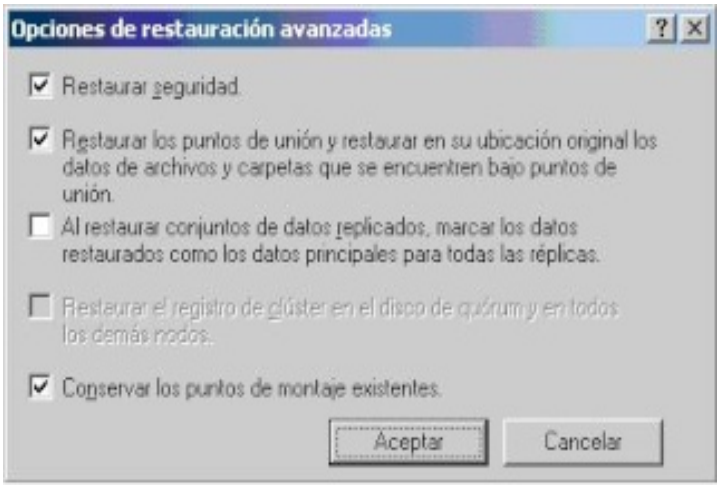


Figura 17: Opciones de Restauración Avanzadas.

4.4.1.2. Si el Sistema Operativo no arranca o esta corrupto.

En el caso de que el S.O. no arranque y no nos permita arrancarlo en modo restauración del SD (Primer supuesto) debemos utilizar un disquete de recuperación del sistema (ASR), este disco se crea desde la utilidad ntbackup. Una vez tenemos el disco creado así como una copia del *System State* debemos arrancar la maquina con un disco de instalación del Sistema Operativo y presionar la tecla f2 cuando nos aparezca la opción de ejecutar el Asistente de recuperación Automatizada:

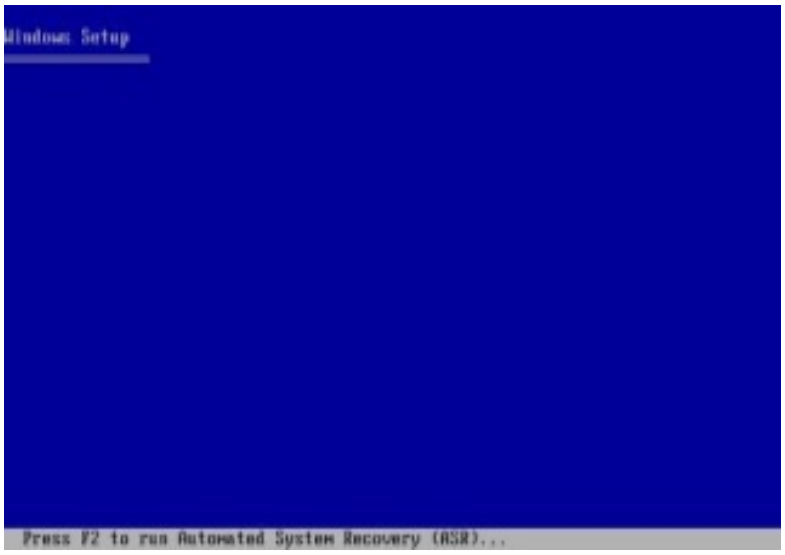


Figura 18: Windows Setup.

En este proceso nos pedirá un disco de recuperación del sistema que debíamos a ver creado previamente desde la utilidad NTBACKUP.

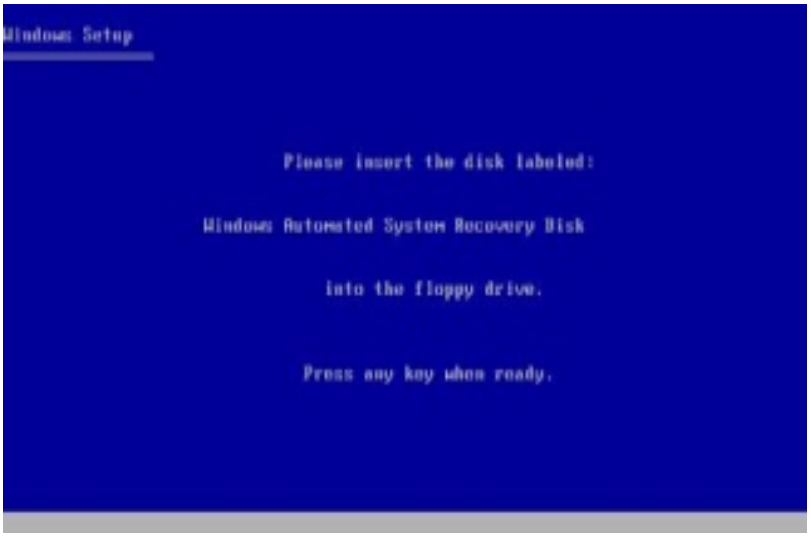


Figura 19: Windows Setup Recuperación.

Una vez insertado el disquete de recuperación nos aparece un asistente para recuperar el system state.

Figura 20: Asistente de Recuperación del Estado del Sistema.

4.4.1.3. Controlador de dominio recién formateado

En el caso que nos encontremos ante un problema de hardware o una situación que conlleve el formateo de la maquina, debemos de realizar la restauración desde el nuevo sistema.

Para realizar este procedimiento debemos de poner a la maquina el nombre del controlador de dominio a restaurar y ejecutar el asistente de ntbackup.

Una vez finalizado el Directorio Activo seria restaurado en la misma maquina.

4.4.2. Restauración autoritativa

Esta restauración se realiza siempre que se quiera que los datos del backup del Controlador de dominio prevalezcan sobre los actuales del dominio, en el caso que fuera el único controlador de dominio no seria necesario pero si existen mas controladores, la información que estamos restaurando es más antigua y no se actualizara salvo que lo forcemos con una restauración autoritativa

Este tipo de restauraciones se suelen hacer cuando borramos de forma accidental algún complemento del directorio (Usuario, Grupo, Controlador de Dominio.)

Para realizar este tipo de restauración debemos de hacer previamente una restauración Normal, como vimos en el tema anterior (arrancando en modo restauración del directorio activo) y tras la restauración sin reiniciar la maquina utilizar el comando NTDSUTIL.

Para realizar una restauración autoritaria completa del Directorio Activo, puede utilizarse el mandato *Restore Database*, sin embargo, es necesario hacerlo con mucha precaución, ya que se perderán todos los cambios realizados desde la última copia de seguridad.

Mediante el comando NTDSUTIL podemos restaurar de forma autoritativa componentes del dominio.

Por ejemplo si quisiéramos restaurar una unidad organizativa llamada sistemas realizaríamos este proceso:

Authoritative restore

Restore subtree

OU=Sistemas,DC=uisek,DC=edu,DC=ec

Quit

Exit

5. MANUAL DE ADMINISTRACIÓN DE LA RED

Las herramientas administrativas de Active Directory y OpenLDAP simplifican la administración del servicio de directorio. Puede utilizar las herramientas estándar o Microsoft Management Console (MMC) para crear herramientas personalizadas centradas en tareas de administración únicas. Puede combinar varias herramientas en una única consola. También puede asignar herramientas personalizadas a administradores individuales con responsabilidades administrativas específicas.

Para los administradores avanzados y los especialistas de soporte técnico de redes, existen muchas herramientas de línea de comandos que pueden utilizar para configurar, administrar y solucionar problemas de Active Directory y OpenLDAP. También puede crear secuencias de comandos que utilicen las Interfaces de servicio de Active Directory (ADSI).

5.1. INICIAR EL COMPLEMENTO DOMINIOS Y CONFIANZAS DE ACTIVE DIRECTORY

1) Haga clic en el botón Inicio, seleccione Todos los programas, Herramientas administrativas y, a continuación, haga clic en Dominios y confianzas de Active Directory. Aparece el complemento Dominios y confianzas de Active Directory, como se muestra en la Figura 18.

Figura 21: Complemento Dominios y confianzas de Active Directory

El Nombre principal del usuario (UPN) proporciona un estilo de nomenclatura fácil de usar para que los usuarios inicien sesión en Active Directory. El estilo del UPN se basa en el estándar RFC 822 de Internet, al que también se hace referencia como dirección de correo. El sufijo UPN predeterminado es el nombre DNS del bosque, que es el nombre DNS del

primer dominio del primer árbol del bosque. El sufijo UPN predeterminado es uisek.edu.ec.

Puede agregar sufijos UPN alternativos, lo que aumenta la seguridad del inicio de sesión. También puede simplificar los nombres de inicio de sesión de usuario si utiliza un solo sufijo UPN para todos los usuarios. El sufijo UPN sólo se utiliza dentro del dominio de Windows Server 2003 y no es necesario que sea un nombre válido de dominio DNS.

Para agregar sufijos UPN adicionales

1) Seleccione Dominios y confianzas de Active Directory en el panel superior izquierdo, haga clic con el botón secundario del mouse en él y, a continuación, haga clic en Propiedades.
2) Especifique cualquier sufijo UPN alternativo en el cuadro Sufijos UPN alternativos y haga clic en Agregar.
3) Haga clic en Aceptar para cerrar la ventana.

5.2. USAR EL COMPLEMENTO USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY

1) Haga clic en el botón Inicio, seleccione Todos los programas, Herramientas administrativas y, a continuación, haga clic en Usuarios y equipos de Active Directory.
2) Expanda uisek.edu.ec haciendo clic en el signo +.

En la Figura 11 se muestran los componentes clave del complemento Usuarios y equipos de Active Directory.

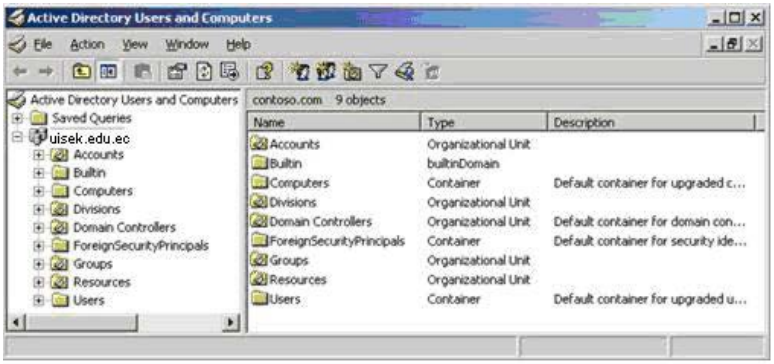


Figura 22: Complemento Usuarios y equipos de Active Directory

5.2.1 Reconocer objetos de Active Directory

Los objetos descritos en la tabla siguiente se crean durante la instalación de Active Directory.

Icono	Carpeta	Descripción
	Dominio	El nodo raíz del complemento representa el dominio que se va a administrar.
	Equipos	Contiene todos los equipos con Windows NT, Windows 2000, Windows XP y Windows Server 2003 que se unen a un dominio. Entre éstos se incluyen los equipos que ejecutan Windows NT versiones 3.51 y 4.0. Si actualiza de una versión anterior, Active Directory migra la cuenta de equipo a esta carpeta. Es posible mover estos objetos.
	Sistema	Contiene información de sistemas y servicios de Active Directory.
	Usuarios	Contiene todos los usuarios del dominio. En una actualización, se migran todos los usuarios del dominio anterior. Al igual que los equipos, se posible mover los objetos de usuario.

Tabla 35: Objetos creados en la instalación de Active Directory

Se puede usar Active Directory para crear los siguientes objetos.

Icono	Objeto	Descripción
	Usuario	Un objeto de usuario es un objeto que es un principal de seguridad en el directorio. Un usuario puede iniciar sesión en la red con estas credenciales y a los usuarios se les puede conceder permisos de acceso.
	Contacto	Un objeto de contacto es una cuenta que no tiene ningún permiso de seguridad. No se puede iniciar sesión como contacto. Los contactos se suelen utilizar para representar a usuarios externos con fines relacionados con el correo electrónico.
	Equipo	Objeto que representa un equipo en la red. Para las estaciones de trabajo y servidores con Windows NT, ésta es la cuenta de equipo.
	Unidad organizativa	Las unidades organizativas se utilizan como contenedores para organizar de manera lógica objetos de directorio tales como usuarios, grupos y equipos, de forma muy parecida a como se utilizan las carpetas para organizar archivos en el disco duro.
	Grupo	Los grupos pueden contener usuarios, equipos y otros grupos. Los grupos simplifican la administración de cantidades grandes de objetos.
	Carpeta compartida	Una carpeta compartida es un recurso compartido de red que se ha publicado en el directorio.
	Impresora compartida	Una impresora compartida es una impresora de red que se ha publicado en el directorio.

Tabla 36: Objetos Active Directory

5.2.2. Agregar una unidad organizativa

Este procedimiento crea una unidad organizativa adicional en el dominio uisek. Tenga en cuenta que se pueden crear unidades organizativas anidadas, y que no hay límite de niveles de anidación.

Para agregar una unidad organizativa

1) Haga clic en el signo + situado junto a Cuentas para expandirlo.

2) Haga clic con el botón secundario del mouse en Cuentas.

3) Seleccione Nuevo y haga clic en Unidad organizativa. Escriba Campus3 como el nombre de la nueva unidad organizativa y, a continuación, haga clic en Aceptar.

5.2.3. Crear una cuenta de usuario

1) Haga clic con el botón secundario del mouse en la unidad organizativa Campus3, seleccione Nuevo y, a continuación, haga clic en Usuario o Usuario nuevo en la barra de herramientas del complemento.

2) Escriba la información del usuario.

3)

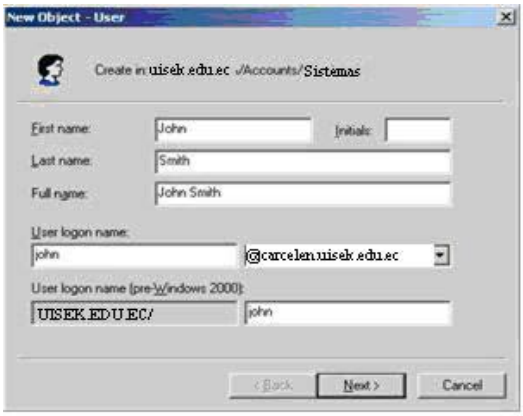


Figura 23: Cuadro de diálogo Usuario nuevo

4) Haga clic en Siguiente para continuar.

5) Escriba password1 en los cuadros Contraseña y Confirmar contraseña y, después, haga clic en Siguiente.

6) Haga clic en Finalizar para aceptar la confirmación en el siguiente cuadro de diálogo.

Para agregar información adicional sobre este usuario

1) Seleccione Campus3 en el panel de la izquierda, haga clic con el botón secundario del mouse en el usuario en el panel de la derecha y, a continuación, haga clic en Propiedades.

2) Agregue más información sobre el usuario en el cuadro de diálogo Propiedades en la ficha General e ingrese la información, a continuación, haga clic en Aceptar. Haga clic en cada ficha disponible y revise la información opcional del usuario que se puede definir.

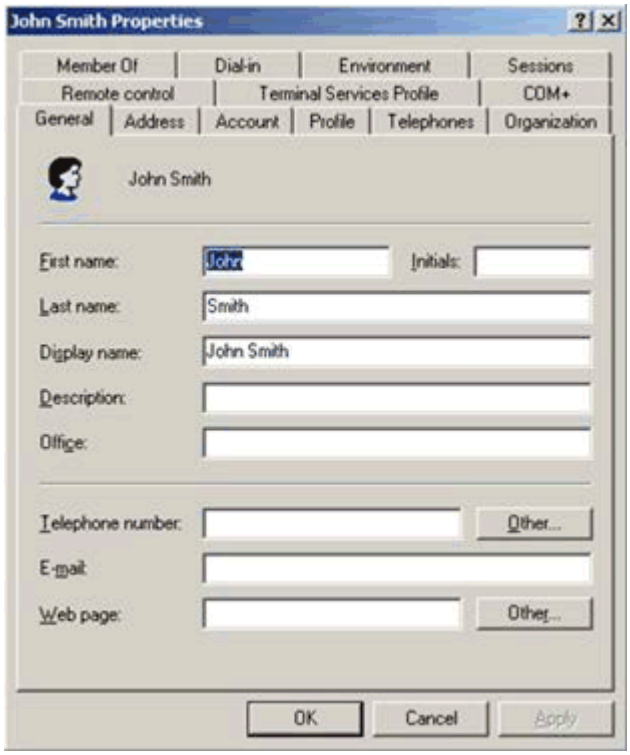
3) 

Figura 24: Información adicional del usuario

5.2.4. Mover una cuenta de usuario

Los usuarios se pueden mover de una unidad organizativa a otra del mismo dominio o de un dominio distinto.

1) Haga clic en la cuenta del usuario en el panel de la derecha, haga clic con el botón secundario del mouse en ella y, después, haga clic en Mover.

2) En la pantalla Mover, haga clic en el signo + situado junto a Cuentas para expandirlo.

3) Haga clic en la unidad organizativa donde lo desea mover y luego en Aceptar.

5.2.5. Crear un grupo

1) Haga clic con el botón secundario del mouse en la unidad organizativa Campus3, haga clic en Nuevo y después en Grupo.

2) En el cuadro de diálogo Nuevo objeto – Grupo, escriba FacultadX para el nombre.

3) Revise el tipo y el ámbito de los grupos disponibles. Mantenga la configuración predeterminada y, a continuación, haga clic en Aceptar para crear el grupo Herramientas.

5.2.6. Agregar un usuario a un grupo

1) Haga clic en la unidad organizativa Campus3 en el panel de la izquierda.

2) Haga clic con el botón secundario del mouse en el grupo Herramientas en el panel de la derecha y, a continuación, haga clic en Propiedades.

3) Haga clic en la ficha Miembros y luego en Agregar.

4) En el cuadro de texto Escriba los nombres de objeto que desea seleccionar, escriba el nombre del usuario y, a continuación, haga clic en Aceptar.

5)

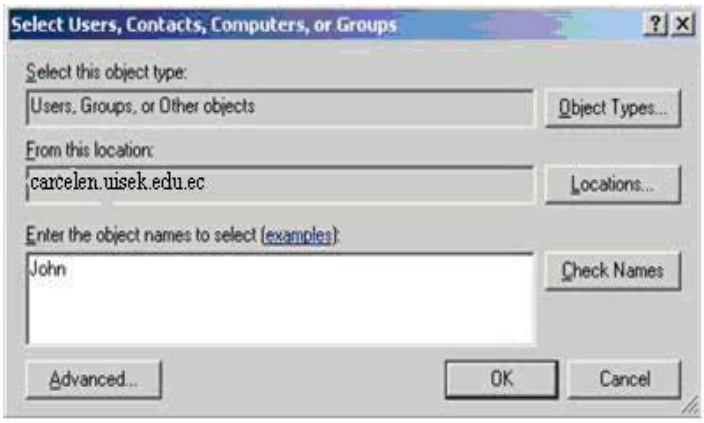


Figura 25: Agregar al grupo de seguridad Herramientas

6) En la pantalla Propiedades de herramientas, compruebe que el nombre de usuario es un miembro del grupo de seguridad y, después, haga clic en Aceptar.

5.2.7. Publicar una carpeta compartida

Para que los usuarios puedan encontrar más fácilmente las carpetas compartidas, puede publicar información sobre dichas carpetas en Active Directory. Cualquier carpeta compartida en la red, incluida una carpeta de Sistema de archivos distribuido (DFS), se puede publicar en Active Directory. Cuando se crea un objeto de carpeta compartida en el directorio, la carpeta no se comparte automáticamente. Éste es un proceso que consta de dos pasos: en primer lugar se debe compartir la carpeta y después publicarla en Active Directory.

1) Utilice el Explorador de Windows para crear una nueva carpeta en uno de los volúmenes del disco.

2) En el Explorador de Windows, haga clic con el botón secundario del mouse en la carpeta y, a continuación, haga clic en Propiedades. Haga clic en Compartir y después en Compartir esta carpeta.

3) En la pantalla Propiedades de especificaciones de ingeniería, escriba ES en el cuadro Nombre del recurso y, a continuación, haga clic en Aceptar. Cierre el Explorador de Windows cuando termine. De forma predeterminada, el grupo integrado Todos tiene

permisos en esta carpeta compartida. Puede cambiar el permiso predeterminado haciendo clic en el botón Permisos.

Publicar la carpeta compartida en el directorio

1) En el complemento Usuarios y equipos de Active Directory, haga clic con el botón secundario del mouse en la unidad organizativa, seleccione Nuevo y, a continuación, haga clic en Carpeta compartida.
2) En la pantalla Nuevo objeto – Carpeta compartida, escriba el Nombre.
3) En el cuadro Ruta de acceso de red, escriba \\uisek.edu.ec\ES y haga clic en Aceptar.
4) Haga clic con el botón secundario del mouse y, después, haga clic en Propiedades.
5) Haga clic en Palabras clave. Para Valor nuevo, escriba un nombre y, a continuación, haga clic en Agregar para continuar. Haga clic dos veces en Aceptar para finalizar.

5.2.8. Publicar una impresora

Puede publicar también información sobre impresoras compartidas en Active Directory. Utilice Usuarios y equipo de Active Directory para publicar manualmente información sobre impresoras compartidas.

El subsistema de impresión propaga de forma automática al directorio los cambios realizados en los atributos de la impresora (ubicación, descripción, carga de papel. etc.).

1) Haga clic en el botón Inicio, en Impresoras y faxes y, después, haga doble clic en Agregar impresora. Aparece el Asistente para agregar impresoras. Haga clic en Siguiente.
2) Haga clic en Impresora local conectada a este equipo, desactive la casilla de verificación Detectar e instalar mi impresora Plug and Play automáticamente y, a continuación, haga clic en Siguiente.
3) En la lista desplegable Usar el puerto siguiente, haga clic en la opción ARCHIVO: (Imprimir a archivo) y después en Siguiente.
4) En el panel de resultados Fabricante, haga clic en Genérico. En el panel de resultados Impresoras, haga clic en Genérico / sólo texto. Haga clic en Siguiente para continuar.
5) En la página Dar un nombre a su impresora, cambie el nombre de la impresora por Imprimir a archivo y, después, haga clic en Siguiente.
6) En la página Compartir impresora, cambie el Nombre del recurso por ImpresoraArchivo y, a continuación, haga clic en Siguiente.

7) Para Ubicación en la página Ubicación y comentario. Haga clic en Siguiente para continuar.

8) Haga clic en Siguiente para imprimir una página de prueba y, después, haga clic en Finalizar para completar la instalación.

9) Cuando se le indique, escriba Impresión de prueba como nombre del archivo para la página de prueba de la impresora. Cuando termine, haga clic en Aceptar.

La impresora se publica automáticamente en Active Directory.

Publicar una impresora manualmente mediante la secuencia de comandos pubprn.vbs

1) Haga clic en el botón Inicio y luego en Ejecutar. Escriba cmd en el cuadro de texto y, después, haga clic en Aceptar.

2) Escriba cd \ windows\ system32 y presione ENTRAR.

3) Escriba cscript pubprn.vbs prserv1 "LDAP://ou=cuentas,dc=uisek.edu,dc=ec" y, después, presione ENTRAR.

4) Cierre la ventana.

5.2.9. Administrar objetos de equipo

Los objetos de equipo de Active Directory se pueden administrar directamente desde el complemento Usuarios y equipos de Active Directory. Administración de equipos es un componente que sirve para ver y controlar numerosos aspectos de la configuración del equipo. Administración de equipos combina varias utilidades de administración en un único árbol de consola, lo que proporciona un fácil acceso a las propiedades administrativas y herramientas de los equipos locales o remotos.

1) En el complemento Usuarios y equipos de Active Directory, haga clic con el botón secundario del mouse en uisek.edu.ec y, después, haga clic en Conectar con el dominio.

2) Haga clic en Examinar y luego en el signo + situado junto a uisek.edu.ec. Haga doble clic en carcelen.uisek.edu.ec y, a continuación, haga clic en Aceptar.

3) Expanda carcelen.uisek.edu.ec haciendo clic en el signo + y, después, haga clic en Controladores de dominio.

4) Haga clic con el botón secundario del mouse y, después, haga clic en Administrar. El sistema se puede administrar ahora de forma remota.

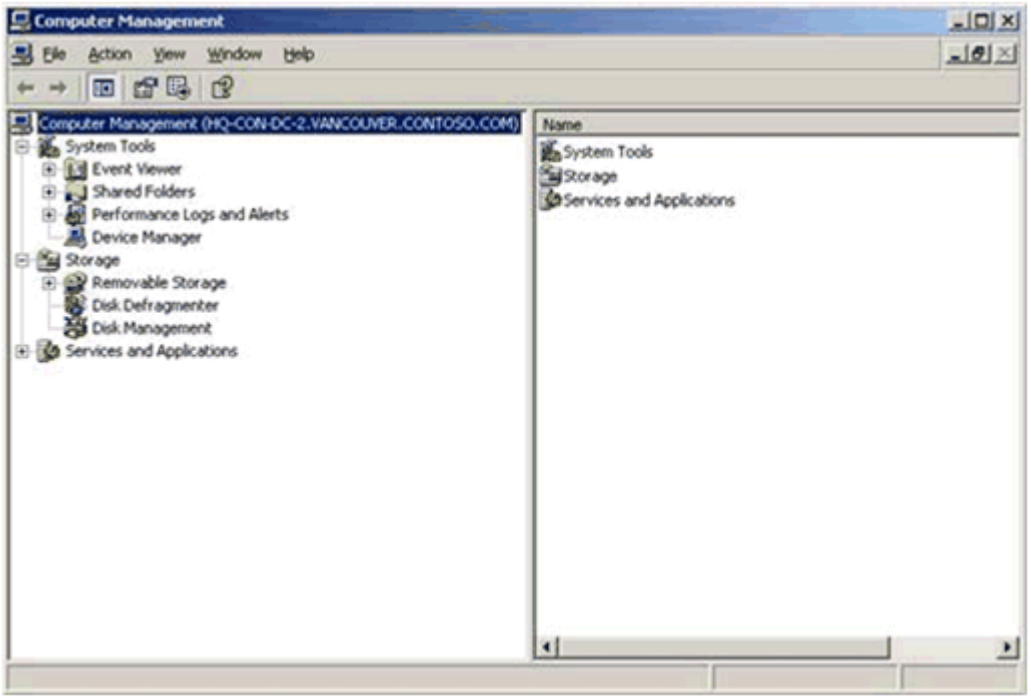


Figura 26: Administrar un equipo de forma remota

5) Cierre la ventana Administración de equipos.

5.2.10. Grupos anidados

Los grupos anidados permiten proporcionar acceso a los recursos a toda la empresa o a todo el departamento con un mantenimiento mínimo. Colocar cada grupo de cuentas de equipo en un único grupo de recursos de toda la empresa no es una solución eficaz, ya que para ello es necesario crear y mantener un gran número de vínculos de pertenencia.

1) En el complemento Usuarios y equipos de Active Directory, haga clic con el botón secundario del mouse en carcelen.uisek.edu.ec y, después, haga clic en Conectar con el dominio.

2) Haga clic en Examinar y luego en uisek.edu.ec. Haga clic dos veces en Aceptar para finalizar.

3) Expanda uisek.edu.ec y, después, expanda la unidad organizativa Cuentas.

4) Cree un nuevo grupo haciendo clic con el botón secundario del mouse en Ingeniería, seleccionando Nuevo y haciendo clic en Grupo. Escriba Sistemas y, a continuación, haga clic en Aceptar.

5) Haga clic con el botón secundario del mouse en el grupo Sistemas y, después, haga clic en Propiedades.

6) Haga clic en la ficha Miembros y luego en Agregar.

7) En el cuadro Escriba los nombres de objeto que desea seleccionar, y a continuación, haga clic en Aceptar.
8) Haga clic de nuevo en Aceptar. Se crea un grupo anidado.

5.2.11. Filtrar una lista de objetos

Filtrar la lista de objetos devueltos desde el directorio le permite administrar el directorio de forma más eficaz. La opción de filtrado permite restringir los tipos de objetos devueltos al complemento.

1) En el complemento Usuarios y equipos de Active Directory, haga clic en Ingeniería bajo la unidad organizativa Cuentas.
2) Haga clic en el menú Ver y luego en Opciones de filtro.
3) Haga clic en el botón de opción Mostrar sólo los siguientes tipos de objetos, seleccione Usuarios y, después, haga clic en Aceptar.
4) Expanda Cuentas y, a continuación, haga clic en Ingeniería para comprobar los resultados del filtro.
5) Quite el filtro.

5.2.12. Seguridad

La posible pérdida de datos o beneficios resultante de un ataque malintencionado en un sistema informático puede ser devastadora para una organización. Con el objetivo de ayudarle a proteger los datos y sistemas de su empresa contra las ubicuas amenazas de código malintencionado que representan los gusanos, virus y ataques, es fundamental que aplique medidas de seguridad para reducir la exposición de los activos empresariales.

Los controladores de dominio en la red constituyen el eje del servicio de directorio de Active Directory. Contienen toda la información de las cuentas de usuario, sin la que los usuarios no pueden iniciar sesión en la red para obtener acceso a los recursos que necesitan para realizar su trabajo.

Debido a esta información incluida en los controladores de dominio y el papel fundamental que desempeñan en todos los entornos, se convierten en objetivos lógicos de ataques malintencionados. Por este motivo, debe colocar los controladores de dominio en la ubicación más segura posible, se deben mantener al día con las últimas actualizaciones de

seguridad y es recomendable deshabilitar servicios innecesarios para evitar que queden expuestos a gusanos, virus y ataques malintencionados:

- Servicios DHCP
- Servicios WINS
- Servicios de impresión
- Servicios de certificados
- Servicios IAS
- Servicio Programador de tareas

5.3. SEGURIDAD ADMINISTRAR OPENLDAP

5.3.1. LDAP en modo SSL/TLS

El inicio de la operación StartTLS en un servidor LDAP, establece la comunicación TLS (Transport Layer Security, o Seguridad para Nivel de Transporte) a través del mismo puerto 389 por TCP. Provee confidencialidad en el transporte de datos e protección de la integridad de datos. Durante la negociación, el servidor envía su certificado con estructura X.509 para verificar su identidad. Opcionalmente puede establecerse la comunicación. La conexión a través del puerto 389 y 636 difiere en lo siguiente:

1. Al realizar la conexión por puerto 636, tanto el cliente como el servidor establecen TLS antes de que se transfiera cualquier otro dato, sin utilizar la operación StatTLS.
2. La conexión a través de puerto 636 debe cerrarse al terminar TLS.

RSA Rivest Shamir Adleman, es un algoritmo para el ciframiento de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el Instituto Tecnológico de Michigan (MIT). RSA es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

X.509 es un estándar ITU-T (estandarización de Telecomunicaciones de la International Telecommunication Union) para infraestructura de claves públicas (PKI, o Public Key Infrastructure).

OpenSSL es una implementación libre, de código abierto, de los protocolos SSL (Secure Sockets Layer) y TLS (Transport Layer Security). [11]

5.3.2. Generando clave y certificado.

cd /etc/openldap/cacerts

La creación de la clave y certificado para OpenLDAP requiere utilizar una clave con algoritmo RSA de 1024 octetos y estructura x509.

```
openssl req -x509 -nodes -newkey rsa:1024 \
-days 730 -out slapd.crt -keyout slapd.key
```

Tabla 37: Creación de clave y certificado para OpenLDAP.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit RSA private key
.............++++++
.++++++
writing new private key to 'uisek.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
```

[11] Gerald Carter, LDAP System Administration, 2003, 294 p.

State or Province Name (full name) [Berkshire]:Quito
Locality Name (eg, city) [Newbury]:Ecuador
Organization Name (eg, company) [My Company Ltd]:Universidad
Internacional SEK
Organizational Unit Name (eg, section) []:Carcelen
Common Name (eg, your name or your server's hostname) []:
Uisek.edu.ec
Email Address []:webmaster@uisek.edu.ec

Tabla 38: Clave y Certificado para OpenLDAP

El certificado solo será válido cuando el servidor LDAP sea invocado con el nombre definido en el campo Common Name. Es decir, solo podrá utilizarlo cuando se defina uisek.edu.ec como servidor LDAP con soporte SSL/TLS.

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario ldap:

```
chown ldap.ldap /etc/openldap/cacerts/slapd.*
chmod 400 /etc/openldap/cacerts/slapd.*
```

Tabla 39: Creación de permisos de lectura para los ficheros de claves y certificados.

5.3.3. Parámetros de /etc/openldap/slapd.conf.

Se deben descomentar los parámetros TLSCACertificateFile, TLSCertificateFile y TLSCertificateKeyFile estableciendo las rutas hacia el certificado y clave. Opcionalmente se puede descomentar la directiva referral para indicar el URI (Uniform Resource Identifier o Identificador Uniforme de Recursos) del servicio de directorio superior como ldaps en lugar de ldap.

```
TLSCACertificateFile /etc/openldap/uisek/slapd.crt
```

```
TLSCertificateFile /etc/openldap/uisek/slapd.crt
TLSCertificateKeyFile /etc/openldap/uisek/slapd.key
referral    ldaps://midominio.org
```

Tabla 40: Edición archivo slapd.conf para uso de autentificación TLS

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **ldap**.

```
service ldap restart
```

Tabla 41: Reinicio servicio ldap

6. PRUEBAS Y RESULTADOS

A continuación se detalla todos los pasos y detalles de la ejecución de cada uno en una prueba que realizamos para determinar el funcionamiento de esta tesis. Se utilizaron dos servidores de dominio, uno tiene instalado Active Directory y el otro OpenLDAP. Los clientes fueron maquinas Windows XP.

6.1. PROBANDO SERVIDOR LDAP

Primero verificamos que tenemos nuestros paquetes siguientes instalados en el sistema:

- openldap-2.2.13
- openldap-clients-2.2.13
- openldap-servers-2.2.
- authconfig-4.6.10

Mediante la siguiente instrucción:
rpm –q openldap openldap-clients openldap-servers authconfig
Para poder tener una mejor organización vamos a crear un directorio donde solo tendrá permisos el usuario y grupo ldap:
mkdir /var/lib/ldap/autenticar
chmod 700 /var/lib/ldap/autenticar
chown ldap.ldap /var/lib/ldap/autenticar

Creamos la clave de acceso como administrador o Manager depende como lo hayamos definido al servidor ldap:
slappasswd

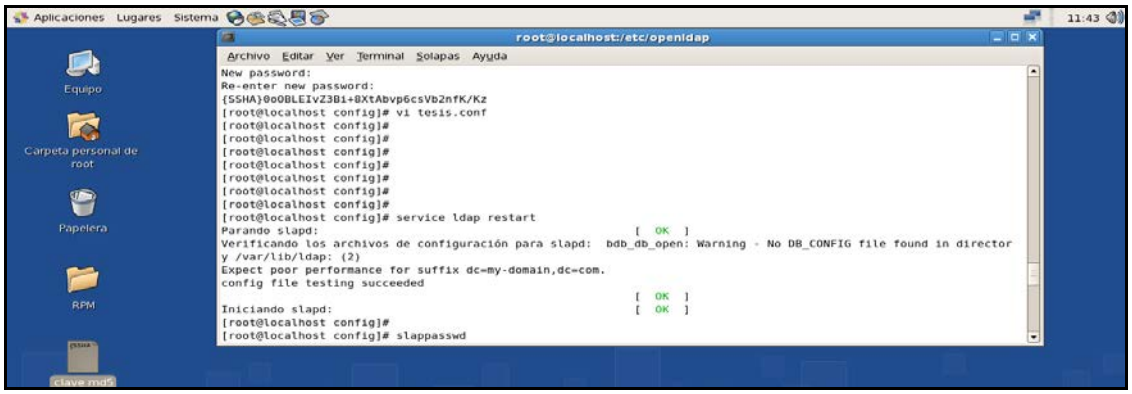


Figura 27: Contraseñas Administrador LDAP

Obtendremos nuestra clave encriptada que debemos copiarla para poder usarla después: *{SSHA}KNFCWNJ9WEU2WHF2U90JFE290*

Verificamos nuestro archivo **/etc/openldap/slapd.conf**

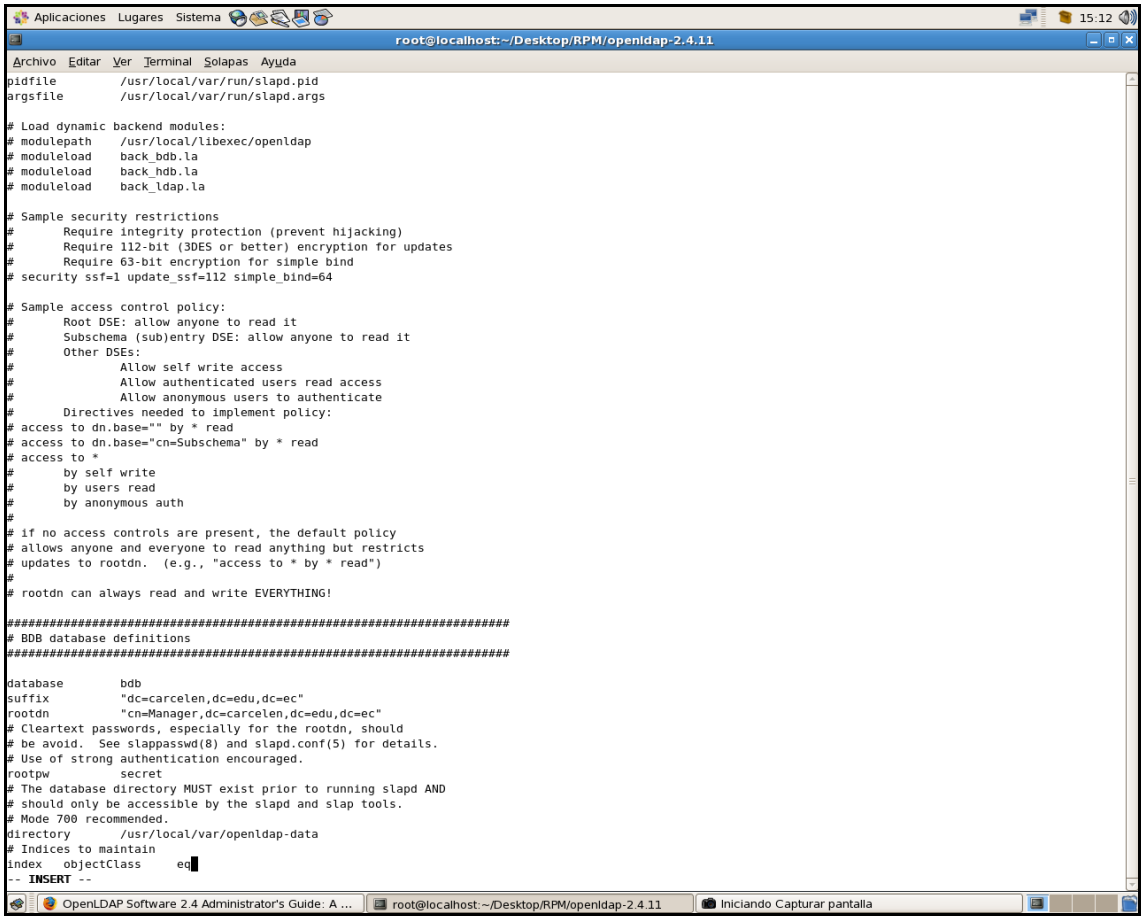


Figura 28: Editar archivo /etc/openldap/sldap.conf

Iniciamos el servicio ldap.

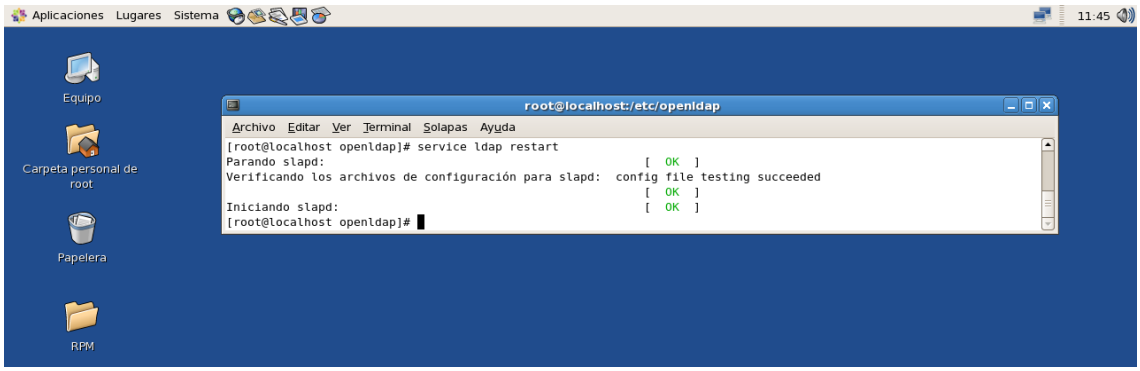


Figura 29: Inicio servicio ldap

A continuación hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio. Genere un fichero base.ldif del siguiente modo:

/usr/share/openldap/migration/migrate_base.pl > base.ldif

Procedemos a insertar la información mediante comandos:

ldapadd -x -W -D 'cn=Administrador, dc=carcelen, dc=edu, dc=ec' -h 127.0.0.1 -f base.ldif

6.2. COMPROBACIÓN DE ACCESO CON LA NUEVA CUENTA EN UN SISTEMA WINDOWS XP

Los pasos que se siguieron en estas pruebas son:

6.2.1. Conexiones de Red e Internet

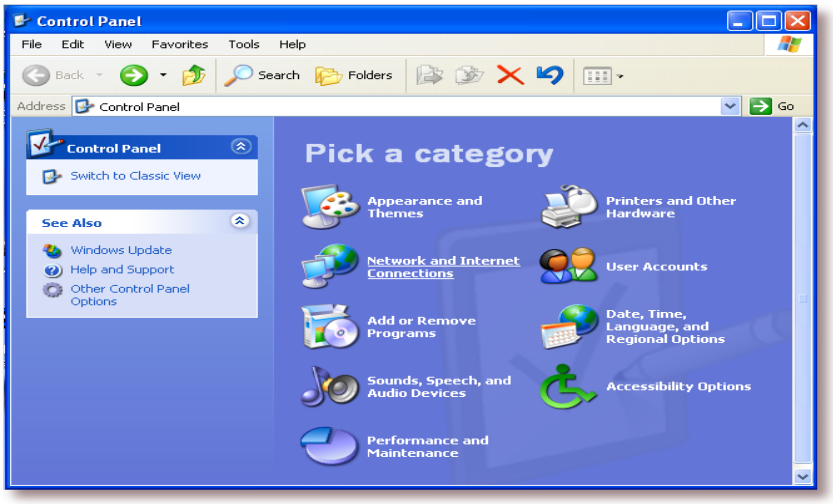


Figura 30: Panel de Control

Acceda a la opción “Conexiones de Red e Internet” del *Panel de Control* (Inicio -> Configuración -> Panel de Control -> Conexiones de Red e Internet).

6.2.2. Conexiones de Red

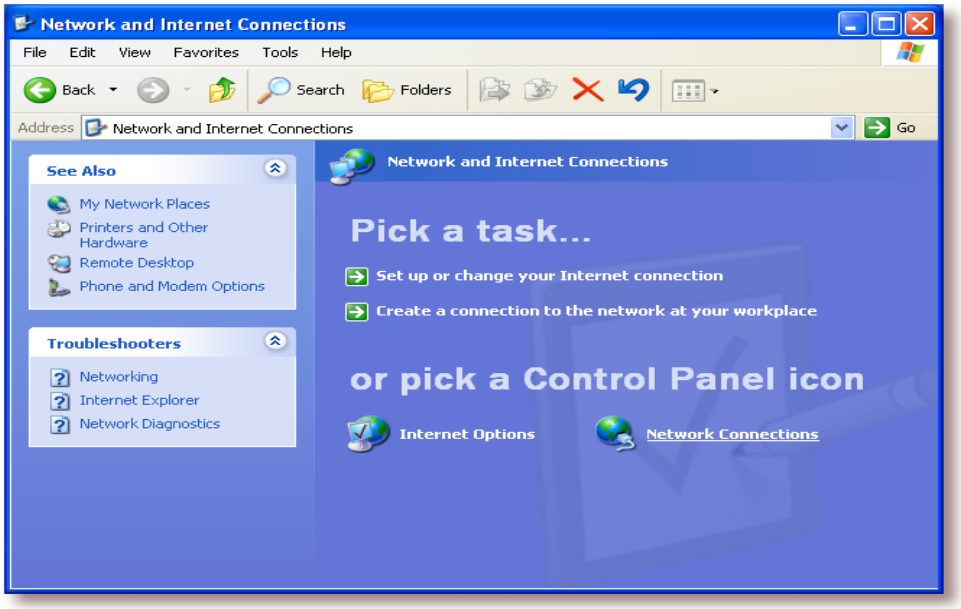


Figura 31: Conexiones de Red

Pulse sobre “Conexiones de Red”.

6.2.3. Identificación de Red

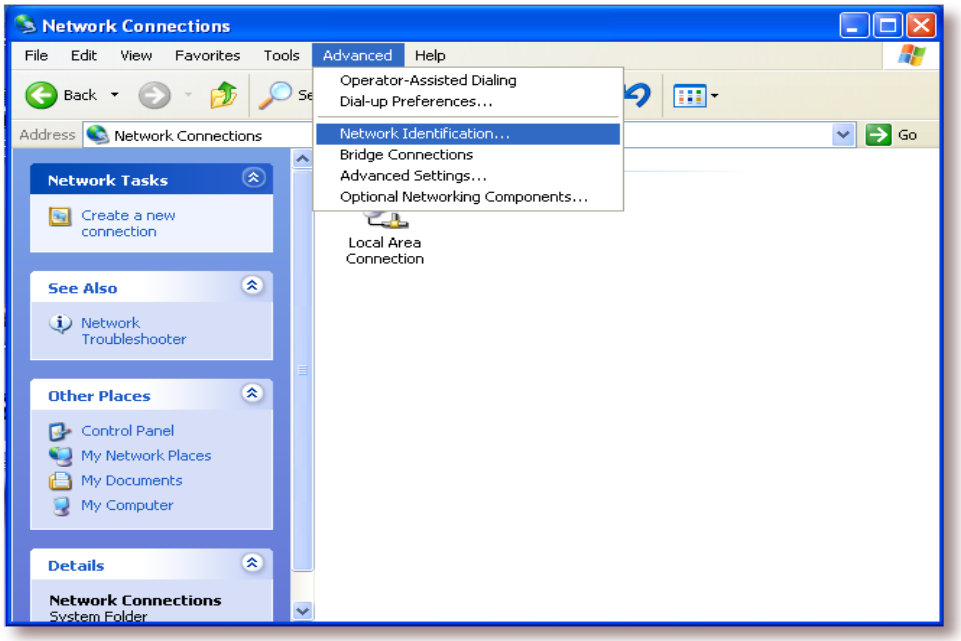


Figura 32: Identificación de Red

Pulse sobre el menú *Avanzado*, opción “Identificación de Red...”

6.2.4. Propiedades del Sistema

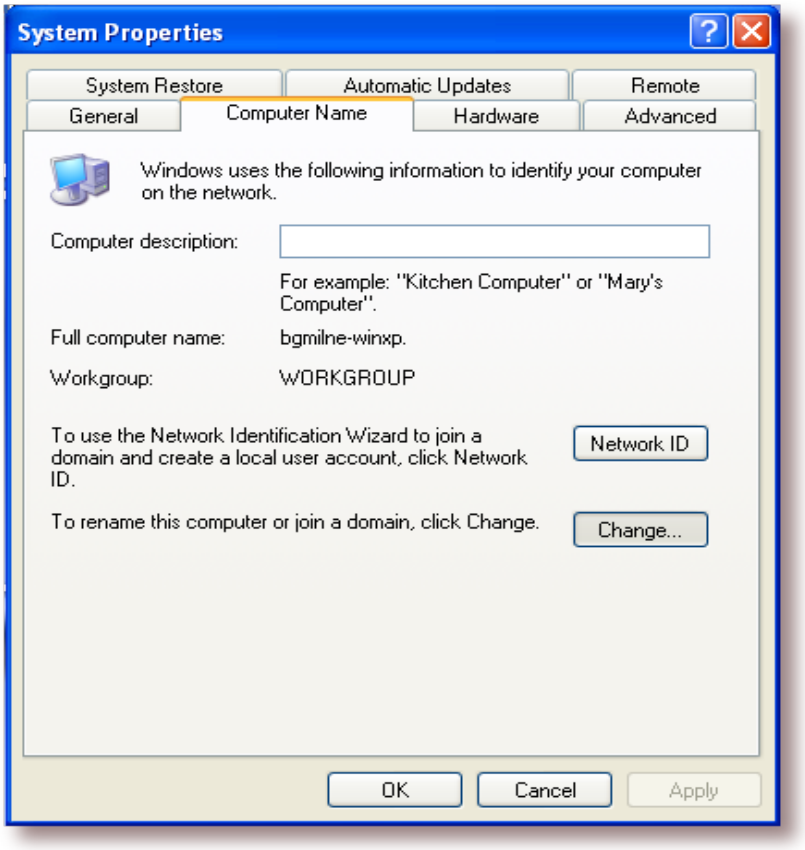


Figura 33: Propiedades del Sistema

Pulse sobre el botón “Cambiar...”

6.2.5. Selección del Dominio

Figura 34: Ingreso a Dominio

Seleccione la opción “Dominio”, teclee carcelen.edu.ec y finalmente, pulse sobre el botón *Aceptar*.

6.2.6. Cuenta del dominio

Figura 35: Cuenta de Dominio

Teclee la cuenta del usuario “root” de OpenLDAP y pulse sobre el botón *Aceptar*.

Bienvenida al dominio

Figura 36: Mensaje de Bienvenida

Si todo ha ido bien, se dará la bienvenida al dominio.

6.3. HERRAMIENTA DE ADMINISTRACION DE LDAP

Las capturas de pantalla que se muestran a continuación mostrarán los pasos que hay que seguir para añadir un usuario al sistema:

6.3.1. URL donde está instalado LAM

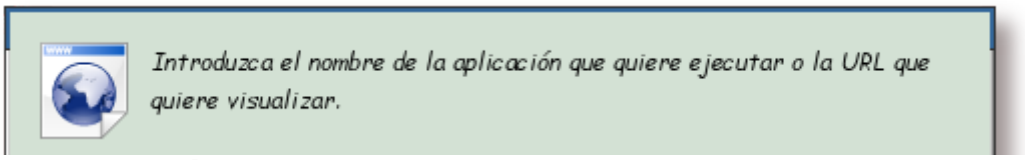


Figura 37: Ingreso de URL.

6.3.2. Aviso acerca del certificado del servidor Web

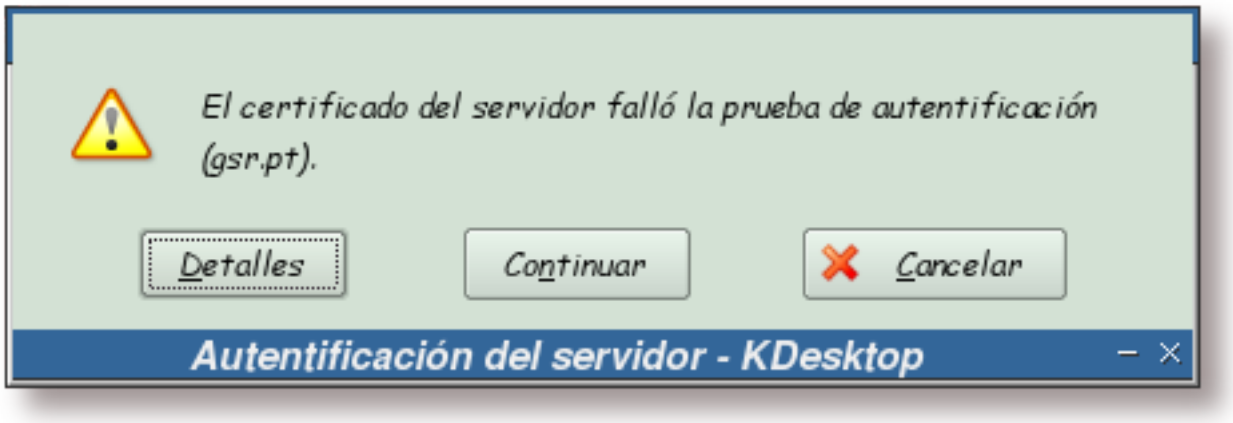


Figura 38: Certificado del Servidor Web

Si ha configurado correctamente el servidor Web, a la hora de acceder a la aplicación LAM por el protocolo *http,* Apache le tendría que redireccionar a la misma dirección, pero bajo el protocolo *https* Esto es lo que ha ocurrido en esta pantalla, Apache ha redirigido la petición realizada (http://192.168.2.12/lam/) hacia el protocolo *https*. Por este motivo, y debido a que la entidad certificadora que se ha creado es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

6.3.3. Información SSL

Se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado.

6.3.4. Período de aceptación del certificado

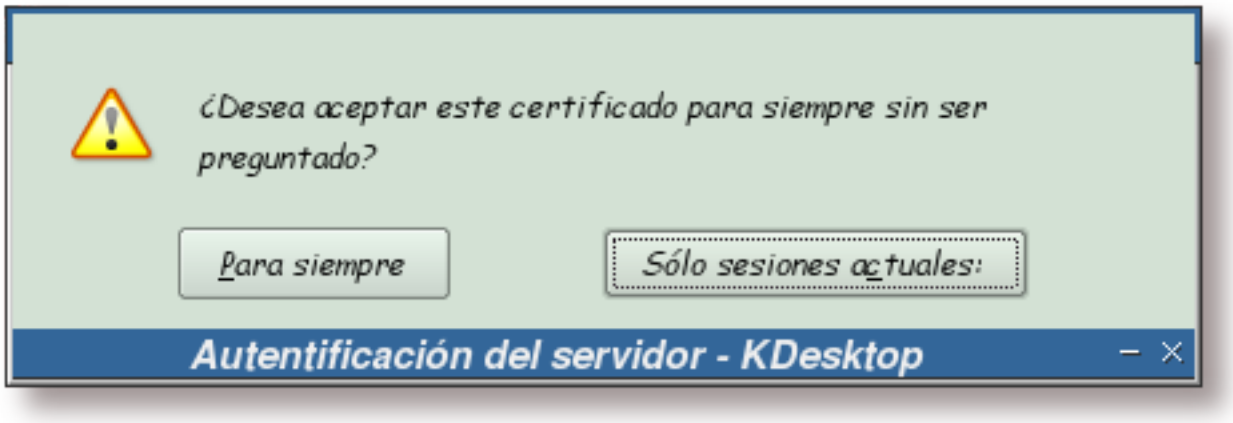


Figura 39: Aceptación de Certificado

6.3.5. Ingreso en LAM

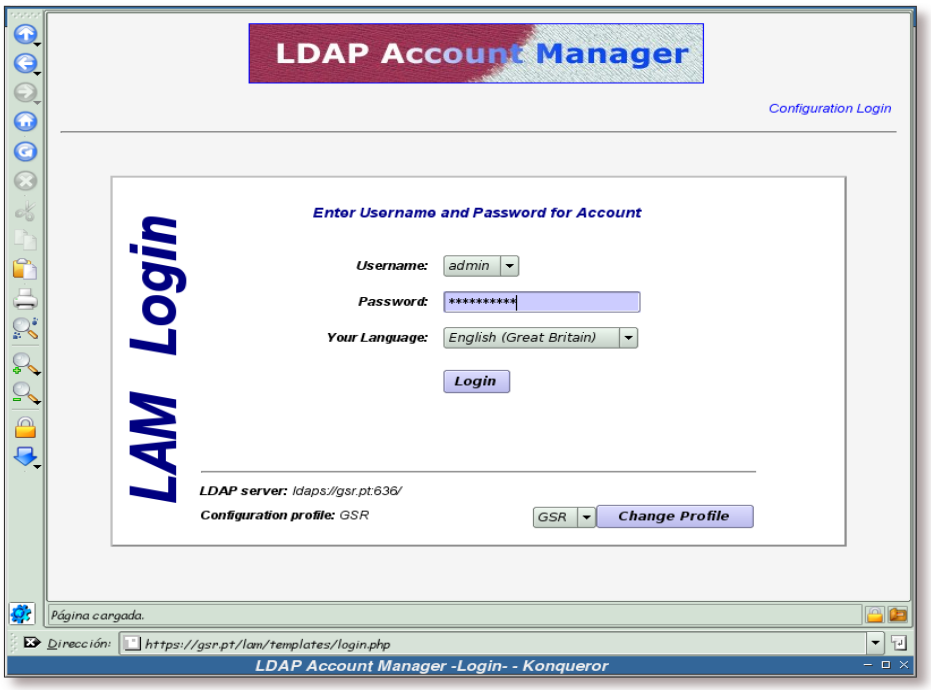


Figura 40: Ingreso a LDAP Account Manager

Si no está seleccionado, elija el perfil *GSR* y pulse sobre: *Change Profile*. Una vez seleccionado el perfil adecuado, escriba la clave del administrador del directorio LDAP y pulsar sobre *Login*.

6.3.6. Edición de perfiles

Figura 41: Edición de Perfiles

La sección predeterminada, tras el ingreso en la herramienta, es la gestión de usuarios. Antes de añadir usuarios, se creará un nuevo perfil de usuarios, personalizado para el sistema. Para proceder a la edición de perfiles, se ha de pulsar sobre el enlace *Profile Editor*.

6.3.7. Edición de un perfil de usuario

Figura 42: Edición de un perfil de usuario.

En el cuadro de *User Profiles* se selecciona la opción *Create a new User Profile* y se pulsa sobre el botón *Submit*.

6.3.8. Opciones de las cuentas

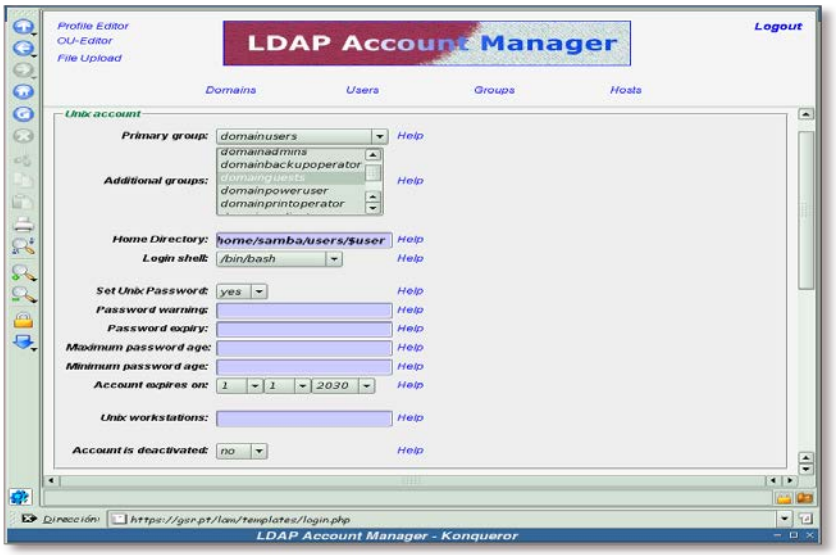


Figura 43: Opciones de las cuentas.

El cuadro destinado a las cuentas Unix (*Unix account*) permite configurar una serie de opciones comunes a todos los usuarios, como son:

- *Primary group*: selección del grupo principal de los usuarios, por defecto será el grupo *domainusers*.
- *Additional groups*: selección del grupo o grupos adicionales para los usuarios, a mayores se seleccionará el grupo *domainguest*.
- *Home Directory*: localización del home de los usuarios. La ruta donde se establecerán los archivos personales de cada usuario será: `/home/samba/users/$user`, donde la variable *$user* se sustituirá por el nombre del usuario a la hora de su creación.
- *Login shell*: se establece la shell *bash* como shell por defecto para los usuarios.
- *Account expires on*: se establece la fecha en la cual la cuenta va a caducar. Se ha fijado en el máximo disponible por la aplicación.

Figura 44: Unix Account

En el cuadro destinado a las cuentas de Samba (*Samba account*) especifique la ruta al directorio home (*todoscsi**$user*) y la ruta al directorio para los perfiles móviles de los usuarios (*todoscsi**profiles**$user*). Al igual que en las cuentas Unix, la variables *$user* se sustituirá por el nombre del usuario a la hora de crear una nueva cuenta.

El campo *Profile name* se rellena con el nombre del perfil que se quiere crear, en este caso: *GSR*.

Para continuar, pulse sobre el botón *Save*.

6.3.9. Perfil guardado

Figura 45: Perfil Guardado

Esta pantalla informa de que el perfil *GSR* se ha guardado correctamente.

Se pulsa sobre el enlace *Users* para proceder a la adición de un nuevo usuario.

6.3.10. Creación de un nuevo usuario

Figura 46: Creación de un nuevo usuario.

Se pulsa sobre el botón: *New user* para comenzar el proceso de creación de un nuevo usuario.

6.3.11. Selección del perfil

Figura 47: Selección de Perfil.

Antes de comenzar a completar los campos con los datos del nuevo usuario, se ha de seleccionar el perfil anteriormente creado, *GSR*. Una vez seleccionado, se pulsa sobre el botón: *Load Profile*.

6.3.12. Datos generales

Figura 48: Datos Generales

Con el perfil *GSR* cargado, sólo se han de completar los campos: *Username* con el nombre que va a tener el usuario en el sistema, *First name* con el nombre real del usuario, *Last*

name con el primer apellido del usuario y, opcionalmente, el campo *Gecos* con una descripción del usuario.

Para continuar, se ha de pulsar sobre el botón *Unix*.

6.3.13. Datos generales Adicionales

Figura 49: Datos Generales Adicionales

Antes de acceder a la información sobre Unix, la aplicación completa automáticamente el campo *UID number* y sustituye las variables *$group* y *$user* por sus valores reales en el campo *Home directory*.

Pulsando en este momento, nuevamente, sobre el botón *Unix* se accederá a la información sobre Unix para el usuario.

6.3.14. Propiedades sobre Unix

Figura 50: Propiedades Unix

En esta pantalla se completa la clave que tendrá el usuario, campos *Password* y *Repeat password*.

Seguidamente pulse sobre el botón: *Samba*.

6.3.15. Propiedades sobre Samba

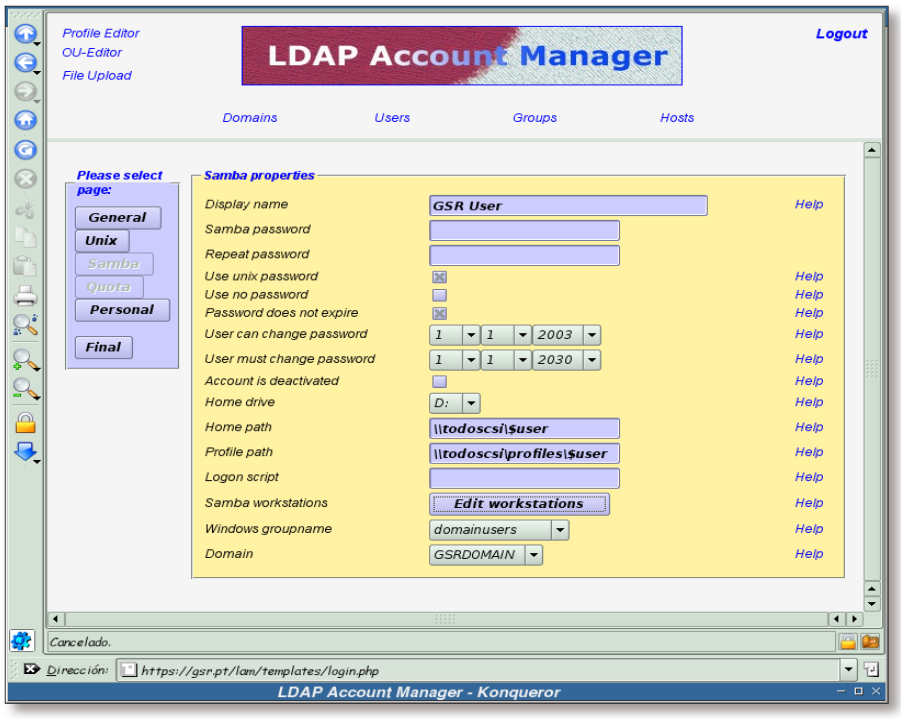


Figura 51: Propiedades Samba

En esta pantalla se completa el campo *Display name*, de forma que ilustre quien es el usuario de la cuenta.

Una vez realizado esto, pulse sobre el botón *Personal*.

Antes de acceder a la información personal, la aplicación sustituye las variables *$group* y *$user* por sus valores reales en los campos *Home path* y *Profile path*.

Vuelva a pulsar sobre el botón *Personal*.

6.3.16. Propiedades personales

Figura 52: Propiedades Personales.

Se pulsa sobre el botón *Final* para continuar.

6.3.17. Creación del usuario

Figura 53: Creación de usuario.

Para completar la creación del usuario, se ha de pulsar sobre el botón *Create Account*.

6.3.18. Usuario creado

Figura 54: Usuario Creado

Esta pantalla indica que el usuario se ha creado satisfactoriamente, se va a comprobar accediendo a la lista de usuarios, para ello pulse sobre el botón *Back to user list*.

6.3.20. Lista de usuarios

Figura 55: Lista de usuarios.

Se puede comprobar en esta pantalla que el usuario *gsruser* ya se encuentra en el directorio LDAP.

6.4. CONSOLA DE MANEJO DE POLITICAS DE GRUPO

Las políticas de grupo de Directorio Activo de Windows 2003 Server, nos permiten controlar y limitar el comportamiento de los usuarios al acceder los recursos los equipos y la red. Las políticas de grupo se definen en dos secciones: la primera que modifica la configuración de clientes o servidores y la segunda que configura el ambiente para los usuarios.

La sección “Computer Configuration” permite configurar entre otras cosas los “security settings” de los equipos, esto incluye: Account policies (password policy y account lockout policy), Local Policies (audit policy, user rights y security options), Event Log, System Services, configuración del registry y File System, etc. Adicionalmente permite la configuración de ciertas funciones de diferentes productos, así como el poder publicar aplicaciones para su instalación. Esta parte de la política se aplica por equipo en el momento que este inicia su sesión de red.

La sección de “User Configuration” permite configurar diferentes aspectos del ambiente de Windows, tales como acceso al control panel, o la configuración de red, instalación de software, configuración del escritorio (fondo, protector de pantalla, etc.), configuración del Internet Explorer, las opciones disponibles en los menús, etc. Esta parte de la política se aplica por usuario, al momento en que este se firma en una computadora con su cuenta y contraseña del dominio.

Las políticas de grupo pueden definirse a nivel Sitio (Site), a nivel Dominio y a nivel Unidad Organizacional (OU). Las políticas a nivel dominio afectan a todos objetos (usuarios y/o equipos) dentro de un dominio. Las políticas a nivel OU afectan solo a los usuarios y/o equipos que se encuentren contenidos en dicha OU. Las OU’s pueden estar anidadas, las políticas se heredan hacia los niveles inferiores de OU’s. En estos casos si existe la misma política definida en múltiples niveles se aplica la política más cercana a los objetos, a menos de que explícitamente especifique lo contrario. No se recomienda utilizar políticas a nivel de sitios, a menos de que sea totalmente indispensable, ya que en un sitio donde existan múltiples dominios puede degradar el proceso de firma (logon) del usuario.

Al definir políticas a diferentes niveles hay que tener en cuenta que a un usuario o equipo le son aplicadas todas estas políticas. Un numero grande de políticas de grupo, que apliquen a un usuario, pueden degradar de forma significativa el proceso de firma (logon) del usuario a la red. Es posible filtrar las políticas de grupo por Grupo de Seguridad de Windows 2000/XP, aplicando la política solo al grupo de usuarios definido y evitando el tiempo de proceso a los otros usuarios.

También es posible deshabilitar una de las dos secciones de una política de grupo, en caso de que no existan políticas definidas en la sección. Esto ahorra tiempo de proceso de la política al "saltarse" la sección, mejorando el tiempo de firma a la red de los usuarios o equipos.

La Consola de Gestión de Políticas de Grupo (GPMC) permite la administración basada en políticas. El administrador puede implantar de forma efectiva los parámetros de seguridad, aplicar de forma necesaria las políticas de TI y distribuir software adecuadamente dentro de un dominio o un rango de unidades organizativas (OU).

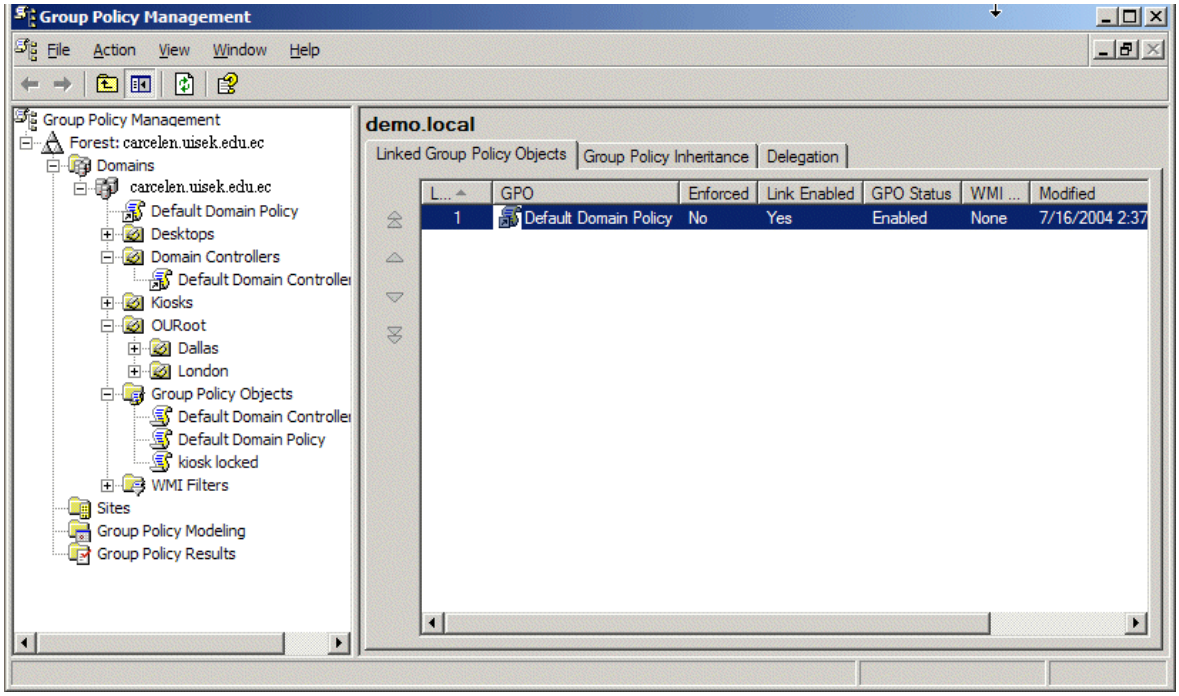


Figura 56: Consola de Gestión de Políticas de Grupo.

La creación de nuestras políticas de grupo se la realiza de la siguiente manera:

- Iniciamos con la creación de las unidad organizativas y sus usuarios:

  Campus Guápulo (guapulo.uisek.edu.ec):

  - Administrativo.
    - Los usuarios son los detallados en la Tabla 4.
  - Biblioteca.
    - Los usuarios son los detallados en la Tabla 3
  - Centro de Cómputo.
    - Los usuarios son los detallados en la Tabla 1.
  - Turismo.
    - Los usuarios son los detallados en la Tabla 2.
  - Wireless.
    - Los usuarios son los detallados en la Tabla 5.

  Campus Carcelén (carcelen.uisek.edu.ec):

  - Comunicación.
    - Los usuarios son los detallados en la Tabla 8.
  - Finanzas.
    - Los usuarios son los detallados en la Tabla 7.
  - Sistemas 1.
    - Los usuarios son los detallados en la Tabla 10.
  - Sistemas 2.
    - Los usuarios son los detallados en la Tabla 9.
  - Wireless
    - Los usuarios son los detallados en la Tabla 6.

6.4.1. Aplicar las directivas de equipo

A los equipos de las OUs desde el Directorio Activo hacemos los pasos siguientes:

- Seleccionamos la OU y después creamos la directiva de grupo y le aplicamos los derechos.

- En la seguridad le aplicaremos las directivas al grupo sistemas, después empezamos a ingresar los equipos a este grupo, para aplicar las directivas sin reiniciar podemos usar en equipos XP el comando **gpupdate** desde el ejecutar y reiniciar los equipos Windows 2000 porque para ellos solo se usan unas llaves de registro pero para no tener problemas con estas mejor se reinicia el equipo y las directivas se aplicaran.

De la misma forma realizaremos otras políticas de grupo que serian muy importantes para la universidad, es decir:

- Bloquear acceso a Panel de Control.
- Impedir modificación del papel tapiz.
- Impedir instalación, modificación o eliminación de programas adicionales.
- Bloquear las propiedades de la Red.
- Establecer horarios de uso del computador.
- Y otras políticas que pueden ser necesarias según el requerimiento del tipo de usuario.

6.5. RESULTADOS

6.5.1 Instalación

En la instalación y configuración del servidor Windows Server 2003 no presento ningún tipo de problema. Esto se lo pudo verificar al momento de acceder desde un cliente con un usuario credo en Active Directory y se verifico que todas las políticas se encontraban correctas.

En cambio, en el servidor ldap se produjo en conflicto de base de datos al momento de iniciar el servicio ldap:

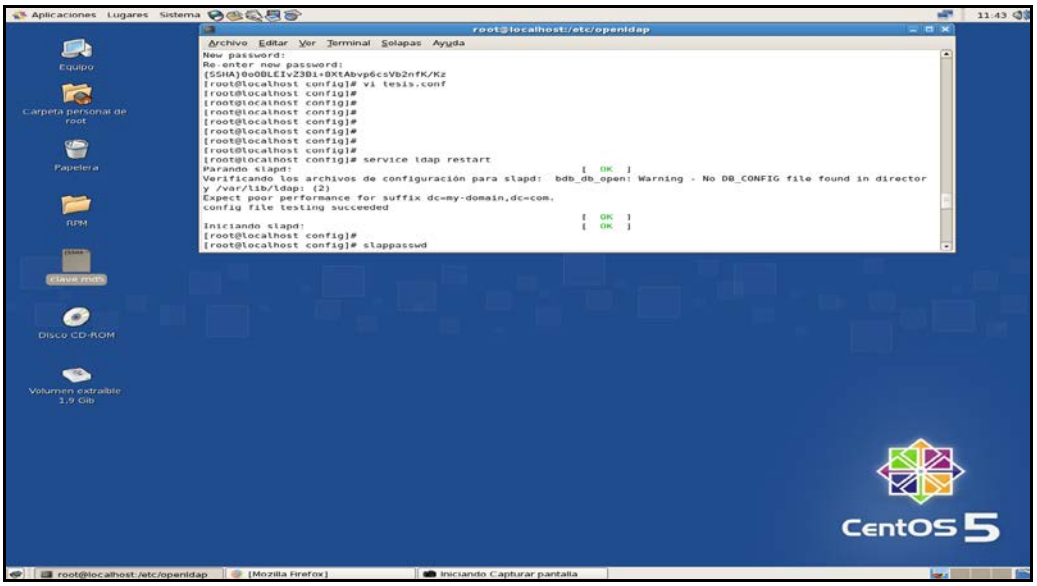


Figura 57: Problema Inicio de Servicio LDAP

Esto se soluciono al utilizar el archivo sample.conf (ejemplo) de configuración de base de datos que se encuentra en la carpeta de OpenLDAP y modificarla a nuestros requerimientos.

```
#cd /etc/openldap
#cp DB_CONFIG.example DB_CONFIG
#mv DB_CONFIG /var/lib/ldap/
```

Figura 58: Cambios base de datos de ldap

Al final pudimos iniciar nuestro servicio ldap sin ningún tipo de conflicto.

6.5.2. Integración

A medida que se agregan, modifican o suprimen miembros de un grupo, únicamente se replican las modificaciones, mediante esta información que se encuentra en los tres servidores de directorio logramos integrar y realizamos las pruebas.

Mediante keberos para autentificación y LDAP para autorización obtenemos la integración de los diferentes dominios y sus unidades organizacionales. Las pruebas realizadas nos permitieron poder ver equipos del dominio carcelen.uisek.edu.ec en el dominio guapulo.uisek.edu.ec y de la forma contraria con un resultado positivo de integración.

6.5.3 Acceso a Recursos.

- Compartir una carpeta en un equipo en Guápulo o Carcelén (este equipo debe estar en guapulo.uisek.edu.ec o carcelen.uisek.edu.ec).
- En un equipo en Carcelén, podremos ingresar al dominio guapulo.uisek.edu.ec.
- Si están bien establecidas las relaciones de confianza se podrán observar los recursos, caso contrario, nos solicitara una clave de acceso. Es preferible que el ingreso sea de forma transparente.
- La misma prueba se debe realizar en sentido contrario.

Luego debemos ingresar con una cuenta al dominio uisek.edu.ec y acceder a los recursos de los dos dominios.

CONCLUSIONES

- Es sumamente necesario e importante mantener una nomenclatura estándar para poder mantener un orden y una política de uso ya que esta nos puede ayudar a la administración de los servicios de la red.

- El tener una administración centralizada de dos redes mediante cualquier tipo de enlace o plataforma facilita notablemente la administración de los recursos teniendo como apoyo unas políticas establecidas.

- La importancia al diseño de la red es muy significativo, ya que es una base muy importante para poder crear nuestra organización en nuestro dominio con sus diferentes tipos de objetos según la Universidad Internacional SEK lo demande en un futuro.

- El servicio ldap, el que fue usado para la implementación del servidor de dominio basado en una plataforma Linux depende de muchas librerías y configuraciones lo que pueda dar un entrono de dificultad al momento de instalar o administrar.

- Se pueden definir muchas políticas de seguridad para todos nuestros miembros de nuestro servidor de dominios, pero estas políticas son un poco más complejas de ser aplicadas en ldap.

- El servidor Windows 2003 con Active Directory tiene una mejor manera de administrar los usuarios y sus diferentes permisos y políticas dentro de el y su interacción con el servidor ldap es segura ya que manejan el mismo protocolo que es ldap, por lo tanto, la replicación se lleva a cabo sin ningún problema entre ellos.

- Salvaguardar toda la información tanto de aplicaciones como de usuarios, manteniendo centralizada toda la información. Manteniendo un solo dominio, podremos administrar fácilmente todo tipo de objetos de Windows como servidores, estaciones de trabajo, colas de impresión, usuarios y grupos, así como aplicaciones, bases de datos y correo electrónico, etc.

- Dentro de Windows 2003 es posible tener políticas de seguridad en cualquier nivel como por ejemplo: dominio, controladores de dominio, unidades organizacionales, grupos de usuarios, estaciones de trabajo, etc. Según los requerimientos, es posible tener seguridades en cualquier objeto de Windows 2003 integrado al Active Directory.

- Todo cambio que se haga en cualquiera de los dos servidores principales (LDAP y Active Directory) se verá inmediatamente reflejado entre ellos por la replicación que manejan los dos, es decir, tendremos una gran ventaja ya que se puede tener una administración centralizada y realizar cambios dependiendo el nivel en que se realice los cambios su efectos se verán reflejados en el mismo momento.

RECOMENDACIONES

- Enfocar mediante un plan estratégico de tecnología más recursos para el área de informática de la Universidad Internacional SEK en todas sus secciones con el fin de obtener servicios que pueden ser usados de mejor manera por parte de las personas que lo conforman.

- Centralizar los servicios de los dos campus mediante cualquier medio para obtener una mejor administración y planes para renovar la tecnología que le puede generar una fortaleza a la universidad.

- Administrar el servicio de ldap mediante software ya que este lo puede ayudar a no cometer inconsistencias en el momento de realizar cualquier cambio y generar otro tipo de configuración que puede generar errores en el desempeño del servidor.

- Mantener el servicio de replicación, según los cambios que se realiza se puede determinar el tiempo que será necesario para realizar. Es muy importante determinar este tiempo para no hacer uso de nuestro enlace continuamente ya que lo podríamos necesitar para servicios de mayor prioridad.

- Centralización en la administración de los servidores mejoraría el desempeño de los mismos para no tener atrasos o congestiones de conexión.

- Para proporcionar protección adicional para el esquema de Active Directory, recomiendo quitar todos los usuarios del grupo Administradores de esquema y agregar un usuario al grupo sólo cuando sea necesario realizar cambios en el esquema. Una vez realizado el cambio, quitar el usuario del grupo.

- Hacer una copia de seguridad de los datos de todos los volúmenes y de los datos del estado del sistema al mismo tiempo.

- Mantener al menos tres copias de los medios. Guardar como mínimo una copia fuera de la universidad, en un entorno correctamente controlado.

- El acceso físico a un servidor constituye un elevado riesgo de seguridad. El acceso físico de un usuario no autorizado a un servidor podría dar como resultado el acceso a datos no autorizados o la modificación e instalación de hardware o software diseñado para violar la seguridad. Para mantener un entorno seguro, se debe limitar el acceso físico a todos los servidores y al hardware de red.

- Optimizar el rendimiento mejorando la configuración del sistema y la carga de trabajo para corregir el rendimiento con una supervisión para evaluar los resultados de dicha optimización.

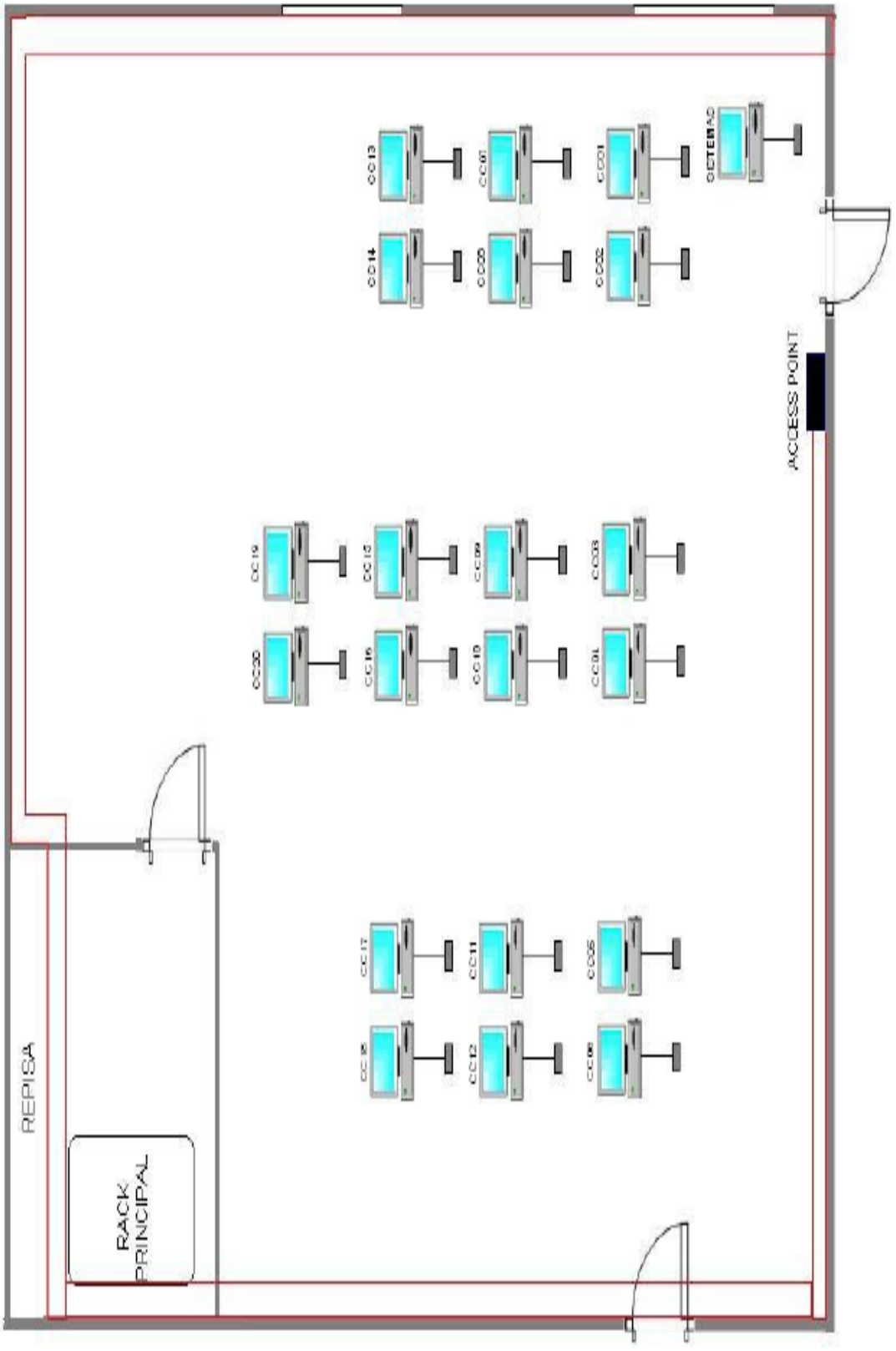
BIBLIOGRAFÍA

- W. Wahl, T. Howes, and S. Kille. Lightweight directory access protocol (v3), rfc 2251, 1997.
- M. Bauer. Authenticate with ldap, part iii. Linux Journal, (113), September 2003.
- http://www.openldap.org
- Information about installing, configuring, running and maintaining an ldap (lightweight directory access protocol) server on a linux machine. http://www.tldp.org/HOWTO/LDAP-HOWTO/
- M. Kershaw. Linux-powered wireless hot spots. Linux Journal, (113), Sep 2003.
- S. Vugt. InDepth: The Lightweight Directory Access Protocol. LinuxJournal, 2001.
- Gerald Carter, LDAP System Administration, 2003, 294 p.
- Véronique Cottin, Active Directory: Los servicios de Directorio Windows 2000, 2002, 447 p.
- Jill Spealman, José Daniel Sánchez Navarro, Kurt Hudson, Melissa Craft; Planning, Implementing, and Maintaining a Microsoft Windows Server 2003, 2004, 1166 p.
- Tom Jackiewicz, Deploying OpenLDAP, 2004, 311 p.
- Martín-Bejarano Sánchez, José Antonio, Integración de los servicios de autenticación en un directorio OpenLDAP, 2005, 341 p.
- Butcher, Matt; Mastering OpenLDAP: Configuring, securing, and integrating directory services, 2007, 467 p.
- Gerald Carter, Jay Ts, Robert Eckstein; Samba, 2008, 528 p.
- Tim Howes, Mark Smith; LDAP: Programming Directory-enabled Applications with Lightweight, 1997,462 p.
- http://www.ldapman.org/
- http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-ldap-auth
- Timothy A. Howes, Tim Howes, Mark C. Smith, Gordon S. Good; Understanding and deploying LDAP directory services, 2003, 899 p.
- Clayton Donley; LDAP, 2002, 654
- Brian Arkills; Ldap Directories Explained: An Introduction and Analysis, 2003, 432 p.

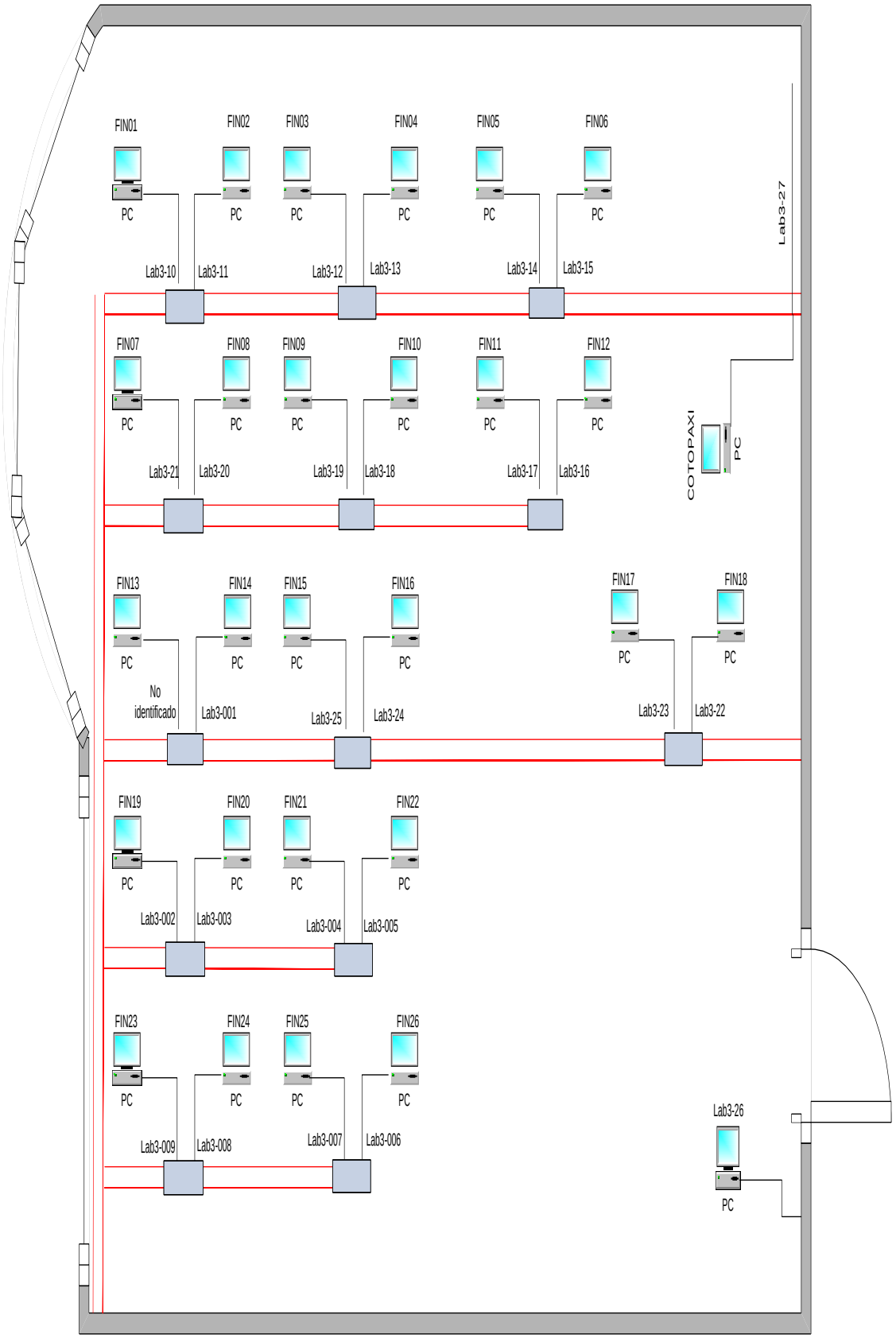
- Antonio Salavert Casamor; Los protocolos en las redes de ordenadores, 2003, 165 p.
- Stan Reimer, Mike Mulcare; Active Directory para Microsoft Windows Server 2003: referencia técnica, 2003, 418 p.
- Véronique Cottin; Active Directory: Los servicios de Directorio Windows 2003, 2002, 447 p.
- Jean-Francois Apréa; Active Directory con Windows Server 2003, 2005, 359 p.
- Gustavo Gabriel Poratti; Windows Server 2003, 2004, 376 p.
- William R. Stanek; Microsoft Windows Server 2003: manual del administrador, 2003, 738 p.
- Robert Williams, Mark Walla; La Biblia de Windows Server 2003, 2004, 1024 p.
- José Luis Raya, J Raya, José Luis Raya Cabrera, Laura Raya González, Laura Raya; Windows Server 2003: instalación y configuración avanzada, 2004, 775 p.
- Charlie Russel, Sharon Crawford, Jason Gerend, Antonio García Cordero, Carolina López Martínez, Luis Miguel Sánchez Brea, Fernando Sáenz Pérez; Guía completa de Microsoft Windows Server 2003, 2003, 1243 p.
- Dee-Ann Leblanc; La Biblia de Administración de Sistemas Linux, 2001, 864 p.
- Tony Bautts, Terry Dawson, Gregor N. Purdy; Linux Network Administrator's Guide, 2005, 338 p.
- http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/domcntrl.mspx
- http://gentoo-wiki.com/HOWTO_Authenticate_from_Active_Directory_using_OpenLDAP
- http://www.securityfocus.com/infocus/1563
- http://www.windowsnetworking.com/articles_tutorials/Authenticating-Linux-Active-Directory.html
- http://crysol.inf-cr.uclm.es/node/370
- http://blogs.technet.com/opineda/
- http://www.activedir.org/

ANEXOS

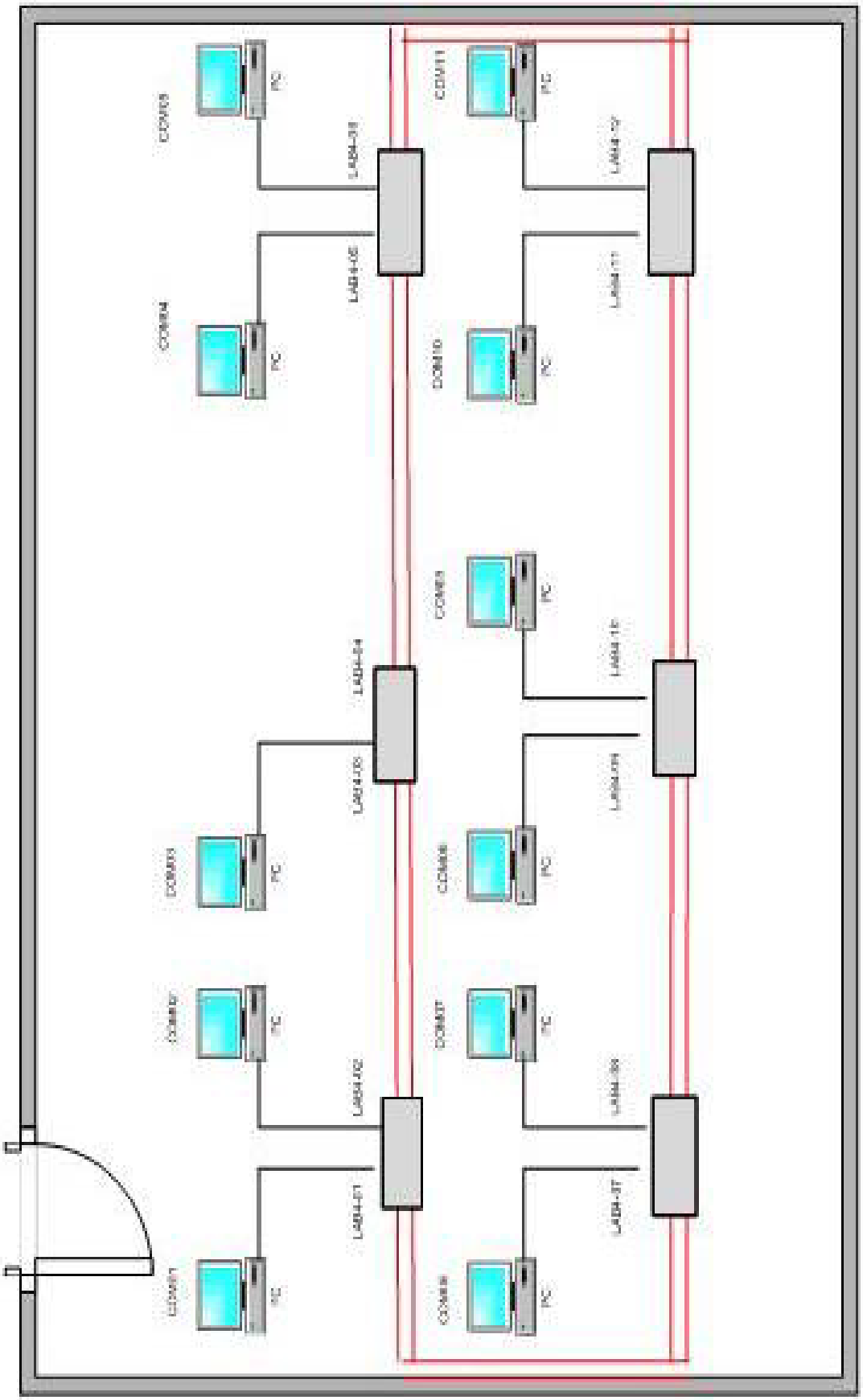
Anexo 1: Diagrama de Red campus Guápulo



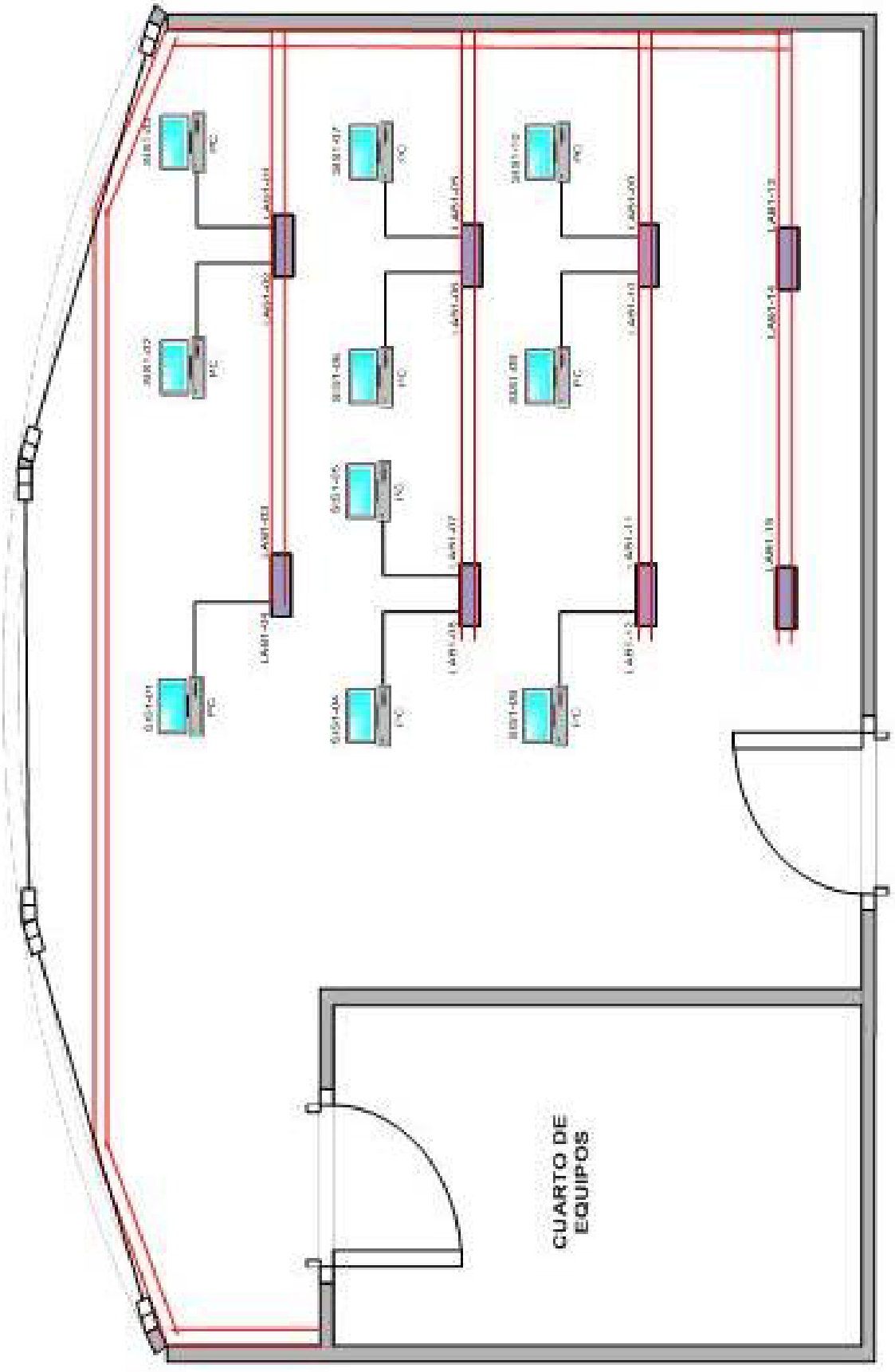
Anexo 2: Diagrama de Red Laboratorio de Finanzas campus Carcelén



Anexo 3: Diagrama de Red Laboratorio de Comunicación campus Carcelén



Anexo 4: Diagrama de Red Laboratorio de Sistemas 1 campus Carcelén



Anexo 5: Diagrama de Red Laboratorio de Sistemas 2 campus Carcelén