Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Juan Gerardo Tunay Vásquez
Asesorado por el Ing. Daniel Oswaldo Pérez Ramírez

Guatemala, octubre de 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JUAN GERARDO TUNAY VÁSQUEZ
ASESORADO POR EL ING. DANIEL OSWALDO PÉREZ RAMÍREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Floriza Felipa Avila Pezquera
EXAMINADOR	Ing. Marlon Antonio Pérez Turk
EXAMINADORA	Inga. Sonia Yolanda Castañeda
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha abril de 2011.

Juan Gerardo Tunay Vásquez

Guatemala 13 de marzo del 2012

Ingeniera
Norma Ileana Sarmientos
Directora Unidad EPS
Facultad de Ingeniería
USAC

Respetable Ingeniera Sarmientos:

Por este medio hago de su conocimiento que he revisado el trabajo final de graduación del estudiante **Juan Gerardo Tunay Vásquez** carné **No. 199615654** titulado **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"**, y a mi criterio, el mismo cumple con los objetivos propuestos para su desarrollo, dando por aprobado el informe final.

Agradeciendo su atención a la presente, aprovecho la oportunidad para suscribirme.

Atentamente,

Daniel Oswaldo Pérez Ramírez
Ingeniero en Ciencias y Sistemas
Asesor del Proyecto

Ingeniero en Ciencias y Sistemas
Colegiado No. 7467

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

UNIDAD DE EPS

Guatemala, 15 de mayo de 2012.
REF.EPS.DOC.715.05.2012.

Inga. Norma Ileana Sarmiento Zeceña de Serrano
Directora Unidad de EPS
Facultad de Ingeniería
Presente

Estimada Ingeniera Sarmiento Zeceña.

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (E.P.S) del estudiante universitario de la Carrera de Ingeniería en Ciencias y Sistemas, **Juan Gerardo Tunay Vásquez** Carné No. **199615654** procedí a revisar el informe final, cuyo título es **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA".**

En tal virtud, **LO DOY POR APROBADO**, solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Inga. Floriza Felipa Avila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas

Universidad de San Carlos de Guatemala
SUPERVISOR (A) DE EPS
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

FFAPdM/RA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

UNIDAD DE EPS

Guatemala, 15 de mayo de 2012.
REF.EPS.D.511.05.2012.

Ing. Marlon Antonio Pérez Turk
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Perez Turk.

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA",** que fue desarrollado por el estudiante universitario **Juan Gerardo Tunay Vásquez** carné No. **199615654** quien fue debidamente asesorado por el Ing. Daniel Oswaldo Pérez Ramírez y supervisado por la Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Directora apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Inga. Norma Ileana Sarmiento Zeceña de Serrano
Directora Unidad de EPS

NISZ/ra

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 30 de Mayo de 2012

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **JUAN GERARDO TUNAY VÁSQUEZ,** carné **1996-15654,** titulado: **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TESIS

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación titulado ***"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA",*** *presentado el estudiante JUAN GERARDO TUNAY VÁSQUEZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 15 de octubre 2012

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.512.2012

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA LA ADMINISTRACIÓN DE LOS LABORATORIOS SAE/SAP DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**, presentado por el estudiante universitario: **Juan Gerardo Tunay Vásquez,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, octubre de 2012

/cc

ACTO QUE DEDICO A:

Dios	Por su ayuda y compañía, llenando mi existencia de seguridad, alegría y esperanza en los momentos de bonanza como de dificultad.
Mis padres	Marcos Tunay y María Teresa Vásquez, por su amor incondicional y apoyo en cada etapa de mi vida. Mostrándome valores como el trabajo, la perseverancia y el respeto por medio de su ejemplo.
Mis hermanos	Sara Julieta y Marco Vinicio, por su cariño, apoyo y aliento a no desistir de mis sueños.
Mi esposa	Yesenia Rodríguez, por su amor y compartir mis sueños a lo largo de mi carrera.
Mis hijos	Andrea Abigail y José Javier, por ser fuente de mi alegría, ilusión y lucha.
Mis amigos	Carlos Ramírez, Nelson Santos, Luis Téllez, Álvaro Méndez, Milton López, Rodely Navarro por su amistad y ayuda a lo largo de la carrera.
Mi asesor	Ing. Daniel Oswaldo Pérez Ramírez, por compartir sus importantes conocimientos que sirvieron como guía la para elaboración del proyecto.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ADSL	Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional.
ARP	Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware.
Backbone	Principales conexiones troncales de Internet.
Bit	Dígito del sistema de numeración binario que puede ser representado por 0 o 1.
Bridge	Dispositivo para la interconexión de redes locales.
Broadcast	Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.
Buffer	Es una ubicación de la memoria en un disco o en un instrumento digital reservada para el almacenamiento temporal de información digital.

Caché	Memoria más pequeña y rápida, la cual almacena copias de datos ubicados en la memoria principal que se utilizan con más frecuencia.
CNAME	Nombre canónico. Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio.
Códec	Describe una especificación desarrollada en software, hardware o combinación de ambos, capaz de transformar un archivo con un flujo de datos a una señal.
CRM	Modelo de gestión de toda la organización, basada en la orientación al cliente.
Datagrama	Es la estructura interna de un paquete de datos.
DNS	Traducción de nombre inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
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.

Framework	Conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.
GHZ	El hercio es la unidad de frecuencia del sistema internacional de medidas. El gigahercio (GHZ) es un múltiplo de la unidad de medida de frecuencia hercio y equivale a 1.000.000.000 hercios.
Host	Computadora conectada a una red, que proveen y utilizan servicios de ella.
ICMP	Protocolo de control y notificación de errores del protocolo de Internet.
Internet	Es la red de redes que permite la conexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.
Intranet	Red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.
IP	Número que identifica a cada dispositivo dentro de una red.

IPV4	Protocolo de Internet Protocol versión 4.
Kernel	Núcleo de un sistema operativo.
LDAP	Protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
Led	Componente electrónico semiconductor que emite luz.
MAC	Identificador de 48 bits que se corresponde de forma única con una interfaz de red.
MBPS	Megabit por segundo. Es una unidad que se usa para cuantificar un caudal de datos.
Modelo OSI	Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.
NIC	*Network Interface Card*, tarjeta de red.
Nodo	Se refiere a un punto de intersección en el que confluyen dos o más elementos de una red de comunicaciones.

Protocolo	Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.
Proxy	Programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A.
Rack	Soporte metálico destinado alojar equipamiento electrónico, informático y de comunicaciones.
RAM	Memoria de acceso aleatorio. Memoria desde donde el procesador recibe las instrucciones y guarda los resultados.
RARP	Protocolo utilizado para resolver la dirección IP de una dirección hardware dada.
Router	Dispositivo de hardware para interconexión de red de ordenadores que opera a nivel de red.
Script	Conjunto de instrucciones que permiten la automatización de tareas creando pequeñas utilidades.
SMTP	Protocolo simple de transferencia de correo.

Switch	Dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Interconecta dos o más segmentos de red.
TCP/IP	Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.
Topología de red	Se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.
UDP	Protocolo de nivel de transporte basado en el intercambio de datagramas.

RESUMEN

Hoy en día las ciencias han avanzado de tal manera que han ido emergiendo una serie de necesidades tecnológicas, entre ellas están la necesidad de compartir recursos, almacenar y analizar grandes cantidades de datos, aunado a esto se encuentra el hecho de que los usuarios y las organizaciones puedan estar distribuidos geográficamente.

Una red es un sistema donde los elementos que lo componen (por lo general computadoras) son autónomos y están conectados entre sí por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos.

La administración de redes informáticas son un conjunto de acciones cuyo objetivo primordial es mantener la red operativa, eficiente, y segura.

La administración de la red debe por tanto conseguir:

- La resolución de problemas en el menor tiempo posible.
- Hacer uso eficiente de todos los recursos de la red: programas, impresoras.
- Convertir la red lo más segura posible, protegiéndola contra intrusos.
- Controlar cambios y actualizaciones en la red y su software para minimizar las interrupciones en el servicio a los usuarios.

OBJETIVOS

General

Diseñar e implementar un sistema de red sólido para satisfacer de manera eficiente los requerimientos de los usuarios, mejorar el servicio, disponibilidad, estabilidad, seguridad y escalabilidad de la red a través del sistema de planeación, diseño y mantenimiento.

Específicos

1. Realizar el análisis de la forma en que trabaja actualmente la institución.

2. Realizar un inventario de los recursos de hardware y software con los que se cuente.

3. Identificar los problemas recurrentes que se presentan dentro de los laboratorios mediante la observación y la entrevista al personal.

4. Investigar herramientas tecnológicas que se ajusten a la solución del problema.

5. Diseñar, implementar y documentar el sistema en sí.

6. Capacitar a los usuarios responsables de los laboratorios para el uso del sistema.

INTRODUCCIÓN

Las conexiones por red permiten a los empleados de una empresa colaborar entre sí y con empleados de otros lugares u otras empresas. Posibilitan el contacto de maneras nuevas, a la vez que lo estrechan más de lo que jamás habría cabido imaginar, entre personas de la oficina o de cualquier punto geográfico. Si la empresa está conectada por una red, nadie está lejos de nadie.

Las redes de área local (LAN, del inglés Local Area Network) hacen posible, por ejemplo, que todos los trabajadores de una oficina compartan el uso de una impresora.

Disponer del software adecuado, también sirve para compartir archivos, colaborar en proyectos y enviar mensajes instantáneos o de correo electrónico de forma simultánea. Las redes de área extensa (WAN, del inglés Wide Area Network) son LAN más amplias. Conectan varias redes locales, por lo general para larga distancia.

Administrar una red informática debe favorecer mecanismos para identificación y autenticación de usuarios, autorizar acceso a los recursos y confidencialidad de datos.

Con este trabajo se pretende desarrollar un sistema de red que optimice el uso de los recursos de la institución y establecer políticas administrativas para los usuarios con el fin de tener segura la red y facilitar su administración.

1. MARCO TEÓRICO

1.1. Redes de computadoras

"Una red de computadoras o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos y ofrecer servicios".[1]

"La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones".[2]

"La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en 7 capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a 4 capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares".[3]

[1] Tanenbaum. Redes de computadoras. p. 3
[2] Tanenbaum. p. 3 - 4.
[3] Tanenbaum. Redes de computadoras. p. 38 - 39.

1.1.1. Clasificación de las redes[4]

Las redes de computadoras se clasifican por su tamaño, es decir la extensión física en que se ubican sus componentes. Dicha clasificación determinará los medios físicos y protocolos requeridos para su operación.

1.1.1.1. Por alcance

- Red de área personal o PAN (personal area network), es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

- Red de área local o LAN (local area network), es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión.

- Una red de área de *campus* o CAN (campus area network), es una red de computadoras que conecta redes de área local a través de un área geográfica limitada.

- Una red de área metropolitana (metropolitan area network o MAN, en inglés), es una red de alta velocidad que da cobertura en un área geográfica extensa.

- Las redes de área amplia (wide area network, WAN), son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como satélites o cables interoceánicos.

[4] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 17 de febrero de 2012.

- Una Red de área local virtual (Virtual LAN, VLAN), es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de *broadcast* en la capa de enlace de datos, a pesar de su diversa localización física.

1.1.1.2. Por tipo de conexión[5]

- Medios guiados

    - El cable coaxial se utiliza para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.

    - El cable de par trenzado es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.

    - La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

[5] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 17 de febrero de 2012.

- Medios no guiados
    - Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

    - Red por infrarrojos. Las redes por infrarrojos nos permiten la comunicación entre dos nodos, usando una serie de *leds* infrarrojos para ello.

    - Red por microondas, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802,11 y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo).

1.1.1.3. Por relación funcional[6]

- Cliente-servidor, es una arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

- Peer-to-peer, es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

[6] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 17 de febrero de 2012.

1.1.1.4. Por tecnología[7]

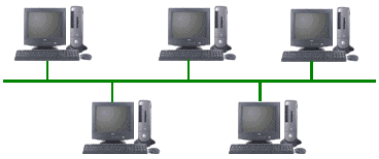
- Red Point-To-Point, es aquella en la que existe multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en algunos casos, máquinas intermedias (*routers*) que establezcan rutas para que puedan transmitirse paquetes de datos.

- Red *Broadcast*, se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo.

1.1.1.5. Por topología[8]

- La red en bus se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o *backbone*) al cual se conectan los diferentes dispositivos.

Figura 1. **Topología en bus**



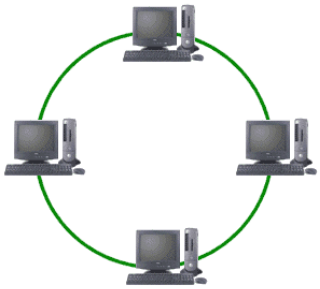
Fuente: http://www.monografias.com/trabajos53/topologias-red/topologias-red2.shtml. Consulta: 21 de febrero de 2012.

[7] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 21 de febrero de 2012.

[8] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 21 de febrero de 2012.

- En una red en anillo cada estación está conectada a la siguiente y la última está conectada a la primera.

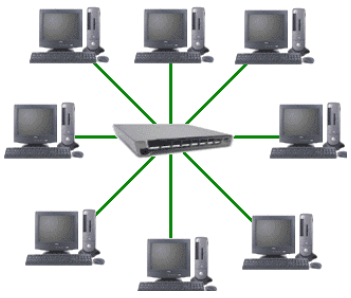
Figura 2. **Topología en anillo**



Fuente: http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml. Consulta: 21 de febrero de 2012.

- En una red en estrella las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

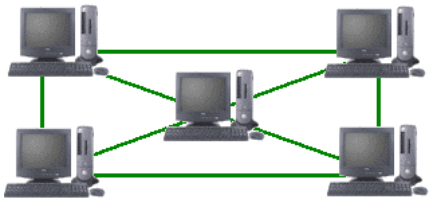
Figura 3. **Topología en estrella**



Fuente: http://www.monografias.com/trabajos53/topologias-red/topologias-red2.shtml. Consulta: 21 de febrero de 2012.

- En una red en malla cada nodo está conectado a todos los otros.

Figura 4. **Topología en malla**



Fuente: http://www.monografias.com/trabajos53/topologias-red/topologias-red2.shtml. Consulta: 21 febrero de 2012.

- En una red en árbol los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

Figura 5. **Topología en árbol**

Fuente: http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtm. Consulta: 21 de febrero de 2012.

- En una red mixta se da cualquier combinación de las anteriores.

1.1.1.6. Por la direccionalidad de los datos[9]

- *Simplex* o unidireccional: un equipo terminal de datos transmite y otro recibe.

- *Half-dúplex* o bidireccional: sólo un equipo transmite a la vez. También se llama semidúplex.

- *Full-dúplex*: ambos pueden transmitir y recibir a la vez una misma información.

1.1.1.7. Por grado de autenticación[10]

- Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

- Red de acceso público: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal.

1.1.1.8. Por grado de difusión

- Una intranet, es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma

[9] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 21 de febrero de 2012.
[10] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 21 de febrero de 2012.

privada, esto es, que no comparte sus recursos o su información con redes ilegítimas.

- Internet, es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

1.1.1.9. Por servicio o función[11]

- Una red comercial proporciona soporte e información para una empresa u organización con ánimo de lucro.

- Una red educativa proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.

1.1.2. Protocolo de redes

Las computadoras, aunque inteligentes, no son seres humanos que pueden, gracias a su capacidad de juicio, establecer una comunicación organizada en la que la información fluye apropiada y ordenadamente, de modo que representa una sesión coherente y significativa de intercambio de información. Además, a diferencia de las personas que efectúan una conversación, los mensajes distorsionados no tienen sentido alguno para las máquinas, por lo cual éstas necesitan de reglas rápidas y estrictas de procedimiento para hacer frente a cualquier eventualidad.

[11] "Red de Computadoras", http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes. Consulta: 21 de febrero de 2012.

Por estas razones, se necesita establecer una serie de lineamientos de comunicación cuya función específica sirva para gobernar el intercambio ordenado de datos a través de la red y para suministrar la corrección de errores en la información incomprensible. Este conjunto de reglas de operación constituye el protocolo de comunicación.

En un principio los protocolos fueron sencillos, pero a medida que las organizaciones crecieron y las redes de datos se volvieron más sofisticadas y difundidas, la logística y circuitería de soporte de comunicaciones se hicieron extraordinariamente complejas. Fue necesario, entonces, desarrollar protocolos más sofisticados para este tipo de redes. Se crearon así los protocolos de capas, cuyo diseño está basado en la filosofía de la programación estructurada. El principio de esta disciplina consiste en dividir todo el trabajo de un sistema de información en funciones, módulos o capas más pequeñas para simplificar el diseño y facilitar el control del sistema.

"El objetivo de los protocolos de capas es definir todas las funciones de telecomunicaciones y separarlas en conjuntos (capas) de subfunciones. Cada capa realiza una tarea distinta y autosuficiente, pero depende de las capas inferiores. Así, las tareas complejas emplearían varias capas, mientras que las sencillas requerirían sólo algunas. La función simple de cada capa implicaría la realización simple de circuitería y logística siendo independiente de las funciones de otras capas. De esta manera se podrían cambiar las funciones o la realización de una capa funcional con el mínimo impacto sobre la logística y la circuitería de las otras capas".[12]

Son varios los protocolos que cooperan para gestionar las comunicaciones, cada uno de ellos cubre una o varias capas del modelo OSI

[12] HERRERA PÉREZ, Enrique, "Tecnologías y redes de transmisión de datos", p. 41.

(*Open System Interconnection*); la realidad, es que para establecer la comunicación entre dos equipos terminales de datos se emplea más de un protocolo, es por esta razón que se suele hablar no de protocolos aislados, sino que al hacer mención de alguno de ellos, se sobreentiende que se está hablando de una pila de protocolos.

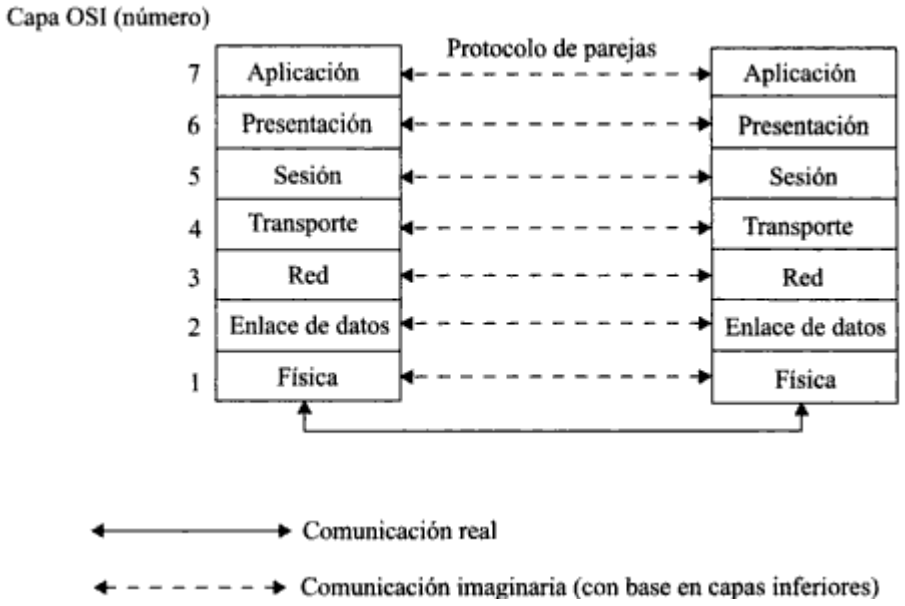
1.1.2.1. Modelo de referencia OSI[13]

El modelo de interconexión de sistemas abiertos, es el ejemplo típico o patrón de los protocolos de capas. Pero no es en sí mismo un protocolo (o conjunto de protocolos), sino más bien la definición cuidadosa de las capas funcionales para la conformación de todos los protocolos modernos. El objetivo es establecer estándares mundiales de diseño para todos los protocolos de datos de telecomunicaciones con la idea de que todos los equipos que se fabriquen sean compatibles.

El principio del modelo OSI, es el de los protocolos de capas. Mientras las capas interactúen de manera aparejada y la interfaz entre la función de una capa y su capa inmediata superior e inferior no se afecten, no es importante la forma como se lleve a cabo la función de esa capa individual. OSI subdivide la función de comunicación de datos en cierto número de subfunciones de capas aparejadas como se ilustra en la siguiente figura. En total se definen 7 capas.

[13] HERRERA PÉREZ, Enrique, "Tecnologías y redes de transmisión de datos", p. 42.

Figura 6. **Modelo de interconexión de sistemas abiertos (OSI)**



Fuente: HERRERA PÉREZ, Enrique, “Tecnologías y redes de transmisión de datos”, p. 42.

Cada capa del modelo OSI se puede considerar como un programa o proceso en una máquina que se comunica con el proceso correspondiente en otra máquina. Las leyes que rigen esta conversación para determinada capa constituyen el protocolo de esa capa. Un protocolo contiene los siguientes elementos principales:

- Sintaxis: define el formato de los datos y los niveles eléctricos de las señales.

- Semántica: define la información de control para la coordinación y el manejo de errores.

- Base de tiempo: establece la sincronización del receptor y el transmisor para la detección adecuada de los *bits*. También define el acoplamiento de velocidades y las secuencias de paquetes de datos.

Las funciones de las capas individuales de modelo OSI se definen completamente en los estándares ISO (ISO 7498); en resumen, son las siguientes:

- Capa física (capa 1). Se encarga del establecimiento y la liberación del enlace físico y de la transmisión de los datos sobre dicho enlace. Especifica los requerimientos eléctricos, mecánicos y de procedimiento para tal fin. Ejemplos de requerimientos de cada tipos son los siguientes:

    - Eléctricos: niveles de voltaje para los bits, base de tiempo para las señales, forma de conectores, impedancia, etcétera.

    - Mecánicos: tipos de conectores, forma de conectores, conexión con el medio, etcétera.

    - De procedimiento: transmisión síncrona y asíncrona, transmisión *dúplex* y *semidúplex*, uso de cada pin de un conector.

- Capa de enlace de datos (capa 2). Se encarga de asegurar la confiabilidad de la transmisión entre nodos adyacentes de los datos considerando un canal ruidoso. Entre las principales funciones específicas que realiza para este fin están: organizar los datos (paquetes) que recibe de la capa superior en tramas, agregar redundancia a la trama para la detección de errores, regular el tráfico mediante *buffer*, agregar banderas para indicar comienzo y fin de mensajes.

- Capa de red (capa 3). Es responsable del establecimiento de conexiones a través de una red real determinando la combinación apropiada de enlaces individuales que se necesita y controlando el flujo de datos entre nodos. Sus funciones específicas son: establece rutas de un nodo fuente a un nodo destino para transmitir los paquetes, direcciona los nodos intermedios en la ruta de los paquetes, ensambla los mensajes que recibe de la capa de transporte en paquetes y los desensambla en el otro extremo, realiza control de flujo y de error, reconoce prioridad en los mensajes y los envía con la prioridad asignada y ofrece servicios de conectividad para enlazar redes por medio de enrutadores.

- Capa de transporte (capa 4). Controla la integridad de un extremo al otro del mensaje. Esto significa que al recibir información de la capa de red, la capa 4 verifica que la información esté en el orden adecuado y revisa si existe información duplicada o extraviada. Si la información recibida está en desorden, lo cual es posible en redes grandes cuando se encaminan las tramas, la capa de transporte corrige el problema y transfiere la información a la capa de sesión en donde se le dará un proceso adicional.

- Capa de sesión (capa 5). Se encarga de iniciar, mantener y terminar la conexión llamada sesión (diálogo entre dispositivos). Las funciones que realiza son las siguientes: controla el diálogo entre dispositivos (quién transmite, cuándo, por cuánto tiempo, por enlace *semidúplex* o *dúplex*, etc.), sincronización (restablece la comunicación si ocurre una ruptura del enlace sin perder datos), etcétera.

- Capa de presentación (capa 6). Se encarga de negociar una técnica mutuamente establecida para la codificación y puntuación de los datos

(sintaxis), así como de cualquier conversión que se necesite entre los formatos de código o arreglo de datos para que la capa de aplicación reciba el tipo que reconoce. Las funciones que realiza esta capa son: compresión de datos, encriptado de datos (para dar seguridad a la transmisión), transformación sintáctica del conjunto de carácteres, formato de desplegado de datos, organización de archivos, etcétera.

- Capa de aplicación (capa 7). Se encarga de suministrar servicios de transferencia de datos al usuario, es decir, al programa de aplicación.

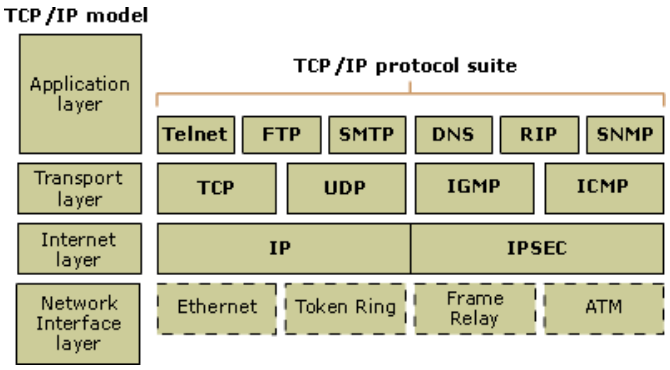
1.1.2.2. Modelo de referencia TCP/IP[14]

TCP/IP está basado en un modelo de referencia de cuatro niveles. Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo.

Tal como se muestra en la siguiente ilustración, cada nivel del modelo TCP/IP, corresponde a uno o más niveles del modelo de referencia Interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*) de siete niveles, propuesto por la Organización internacional de normalización (ISO, *International Organization for Standardization*).

[14] http://technet.microsoft.com/es-es/library/cc786900%28WS.10%29.aspx. Consulta: 23 de febrero de 2012.

Figura 7. **Niveles del modelo TCP/IP**



Fuente: http://technet.microsoft.com/es-es/library/cc786900%28WS.10%29.aspx. Consulta: 23 de febrero de 2012.

Los tipos de servicios realizados y los protocolos utilizados en cada nivel del modelo TCP/IP se describen con más detalle a continuación.

- Capa interfaz de red (enlace). Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.

- Capa Internet (red). Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre *hosts* y a través de redes. Realiza el enrutamiento de los datagramas IP. Protocolos que utiliza: IP, ICMP, ARP, RARP.

- Capa de transporte. Permite administrar las sesiones de comunicación entre equipos *host*. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos. Protocolos que utiliza: TCP, UDP, RTP.

- Capa de aplicación. Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red. Protocolos que utiliza: HTTP, *Telnet*, FTP, TFTP, SNMP, DNS, SMTP y otros protocolos de aplicación.

1.1.3. Componentes básicos de una red[15]

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (*hosts*) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

1.1.3.1. Software

- Sistema operativo de red: permite la interconexión de ordenadores para poder acceder a los servicios y recursos. En muchos casos el sistema operativo de red es parte del sistema operativo de los servidores y de los clientes, por ejemplo en Linux y Microsoft Windows.

[15]http://es.wikipedia.org/wiki/Red_de_computadoras#Componentes_b.C3.A1sicos_de_las_redes. Consulta: 23 de febrero de 2012.

- Software de aplicación: en última instancia, todos los elementos se utilizan para que el usuario de cada estación, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correos electrónicos, etc.

1.1.3.2. Hardware

- Tarjeta de red: para lograr el enlace entre las computadoras y los medios de transmisión, es necesaria la intervención de una tarjeta de red, o NIC (*Network Card Interface*), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (*Media Access Control*), que consta de 48 bits (6 bytes).

1.1.3.3. Dispositivos de usuario final

- Computadoras personales: son los puestos de trabajo habituales de las redes.

- Terminal: muchas redes utilizan este tipo de equipo en lugar de puestos de trabajo para la entrada de datos. Este tipo de terminales, trabajan unido a un servidor, que es quien realmente procesa los datos y envía pantallas de datos a los terminales.

- Electrónica del hogar: las tarjetas de red empezaron a integrarse, de forma habitual, en muchos elementos habituales de los hogares: televisores, equipos multimedia, proyectores, videoconsolas, teléfonos celulares, libros electrónicos, etc., e incluso en electrodomésticos.

- Servidores: son los equipos que ponen a disposición de los clientes los distintos servicios. Algunos tipos comunes de servidores son:
    - Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.

    - Servidor de impresión: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión.

    - Servidor de correo: almacena, envía, recibe, encamina y realiza otras operaciones relacionadas con los correos electrónicos para los clientes de la red.

    - Servidor *proxy*: permite administrar el acceso a Internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web, basándose en contenidos, origen/destino, usuario, horario, etc.

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

    - Servidores para los servicios de red: estos equipos gestionan aquellos servicios necesarios propios de la red y sin los cuales no

se podrían interconectar, al menos de forma sencilla. Algunos de esos servicios son: servicio de directorio para la gestión de los usuarios y los recursos compartidos, *Dynamic Host Configuration Protocol* (DHCP) para la asignación de las direcciones IP en redes TCP/IP, *Domain Name System* (DNS) para poder nombrar los equipos sin tener que recurrir a su dirección IP numérica, etc.

- Servidor de base de datos: permite almacenar la información que utilizan las aplicaciones de todo tipo, guardándola ordenada y clasificada y que puede ser recuperada en cualquier momento y en base a una consulta concreta.

- Servidor de aplicaciones: ejecuta ciertas aplicaciones. Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente.

1.1.3.4. Dispositivos de red

Los equipos informáticos descritos necesitan de una determinada tecnología que forme la red en cuestión. Según las necesidades se deben seleccionar los elementos adecuados para poder completar el sistema. Por ejemplo, si queremos unir los equipos de una oficina entre ellos debemos conectarlos por medio de un conmutador o un concentrador, si además hay varios portátiles con tarjetas de red *Wi-Fi* debemos conectar un punto de acceso inalámbrico para que recoja sus señales y pueda enviarles las que les correspondan, a su vez el punto de acceso estará conectado al conmutador por un cable.

Los elementos de la electrónica de red más habituales son:

- Conmutador o *switch*
- Enrutador o *router*
- Puente de red o *bridge*
- Puente de red y enrutador o *brouter*
- Punto de acceso inalámbrico o WAP (*Wireless Access Point*)

1.2. Servidor[16]

Un servidor, es una computadora que suele ser más potente que una computadora promedio. Está diseñado específicamente para proporcionar información y software a otras computadoras que estén conectadas a él por medio de una red.

1.2.1. ¿Para qué están diseñados los servidores?

Están diseñados para manejar cargas de trabajo más grandes y más aplicaciones, pues utilizan hardware específico para que la productividad sea mayor y el tiempo de inactividad, menor.

1.2.2. ¿Cuándo necesito un servidor?

Comience haciéndose estas preguntas para comprender cuándo es el momento de invertir en un servidor:

[16] http://www1.la.dell.com/content/topics/segtopic.aspx/es/dell-server-basics-buy-guide?c=cl&l=es&cs=clbsdt1. Consulta: 23 de febrero de 2012.

- ¿Usa dos o más computadoras en su empresa? Al almacenar y organizar los datos en una ubicación central, puede acceder a los archivos y compartirlos.

- ¿Tiene personal móvil? Las empresas con personal móvil definitivamente necesitan un servidor. Sus empleados pueden conectarse de manera remota a la red de la empresa y acceder a la información y a los recursos, independientemente de dónde se encuentren.

- ¿Sus empleados comparten documentos entre varias computadoras? Si es así, existe el riesgo de perder archivos importantes, sin mencionar la multiplicidad de versiones de documentos vitales.

- ¿Puede darse el lujo de perder archivos y datos valiosos? ¿Puede reemplazarlos o restaurarlos? Un servidor puede ayudarlo a organizar los datos y contribuye a proteger la empresa contra la pérdida y el daño en los archivos. Puede respaldar la información desde el servidor en un sistema de respaldo y recuperación dedicado a ello.

- ¿Necesita compartir el acceso a los periféricos, como las impresoras y máquinas de fax? Los servidores dan acceso a estos periféricos a toda la oficina.

1.2.3. ¿Por qué necesito un servidor?

Al invertir en un servidor:

- Los empleados pueden compartir las herramientas de software y el acceso a las bases de datos de la empresa dentro y fuera de las instalaciones.

- Puede controlar el acceso a la información confidencial (por ejemplo, registros financieros e información del personal), almacenándola lejos de las miradas curiosas.

- Puede agregar plataformas con facilidad, como software de administración de las relaciones con los clientes (CRM) y programas de contabilidad, que le permiten programar reuniones grupales, compartir información y administrar clientes y proveedores.

1.2.4. ¿Qué tipo de servidor necesito?

El servidor que escoja debe reflejar la cantidad y el tipo de aplicaciones que desea ejecutar en él. Debe saber cuántos usuarios (clientes) tendrá. Muchas aplicaciones comunes (como la de los servidores de impresión y el uso compartido de documentos de Office, como archivos de Word y Excel) tienen exigencias tan bajas de procesamiento que un único servidor de bajo costo puede alcanzar para manejar toda la empresa con facilidad. Otras tareas, como el alojamiento de bases de datos o bibliotecas de imágenes de gran tamaño, requieren más potencia de procesamiento además de discos duros rápidos y con mucho espacio, con las correspondientes conexiones de red de gran capacidad. Puede escoger de los siguientes tres tipos de servidores:

- Servidores en torre. Son los servidores más básicos del mercado. Los servidores en torre son ideales para las pequeñas empresas que:

    - Tienen un espacio limitado y necesitan un procesamiento centralizado sin llegar a requerir una sala de datos.
    - Necesitan poder realizar un monitoreo y un mantenimiento más sencillos de los recursos en red.
    - Desean reducir la susceptibilidad a las intrusiones y los ataques a través de una ubicación central.

- Servidores en *rack*. Estos sistemas apilan los servidores en *racks* de la misma manera en que un organizador de CD apila los CD. Es una opción que ahorra espacio pero es más adecuada para las empresas que:

    - Desean maximizar el espacio en un centro de datos centralizado.
    - Necesitan flexibilidad para combinar servidores que se correspondan con las aplicaciones y cargas de trabajo.
    - Requieren almacenamiento dedicado de gran tamaño interno para el servidor.

- Servidores *blade*. Estos sistemas constituyen los servidores más compactos de los tres. Toman su nombre de la palabra en inglés que significa hoja debido a su forma delgada. Pueden instalarse muchos servidores *blade* de manera vertical en un único gabinete, para compartir ciertos componentes de hardware como las fuentes de alimentación. Consolidar una infraestructura de servidores tradicional en gabinetes para *blades* que ahorran espacio y energía significa:

- Más procesamiento
- Menos espacio
- Menos energía
- Menos tiempo y dinero para la administración

1.2.5. Configuración de hardware para servidores

Los servidores usan la misma arquitectura básica o configuración que una computadora. Sin embargo, un servidor tiene características de hardware mejoradas, como: varios procesadores de varios núcleos, opciones más rápidas de memoria para brindar un rendimiento mayor de las aplicaciones, varios discos duros para contar con más capacidad para los datos y con redundancia, tarjetas de red especializadas.

- Tarjeta madre del sistema. La tarjeta madre del sistema, que también se conoce como placa madre, es la tarjeta de circuitos principal de la computadora, a la que se conectan todos los otros componentes del servidor. Los principales componentes de la tarjeta madre del sistema incluyen el procesador, que contiene unos circuitos llamados *chipset*, la memoria, las ranuras de expansión, una controladora de discos duros y puertos de entrada/salida (E/S) para los dispositivos como teclados, mouse e impresoras.

- Procesador. El procesador, es el cerebro del servidor. La velocidad y la cantidad de procesadores de un servidor repercuten enormemente en la capacidad del servidor para admitir aplicaciones. Los procesadores cambian constantemente, por lo que puede resultar difícil determinar cuál es el adecuado para una aplicación. Debe tener en cuenta tres características principales al seleccionar un procesador.

- Velocidades del reloj. Representan la velocidad con la que funciona el procesador que típicamente se mide en *gigahertz* (GHz). Por lo general, cuanto más rápido, mejor: los servidores con velocidades más altas tienen un mejor rendimiento.

- Cantidad de núcleos. Cantidad de procesadores físicos dentro del procesador en sí. Hoy en día, la mayoría de las CPU poseen dos o cuatro núcleos. Al contar con varios núcleos, los servidores que ejecutan muchas aplicaciones pueden realizar tareas múltiples de una mejor manera.

- Tamaño de la *caché*. Cada procesador tiene una memoria de alta velocidad integrada que se encuentra directamente sobre y cerca de la unidad central de procesamiento (CPU). Las cachés de mayor tamaño reducen la frecuencia que necesita la CPU para obtener datos de la memoria del sistema que se encuentra fuera de la CPU.

- Memoria. Cuando se abre un archivo o documento, el servidor necesita un lugar para mantener un seguimiento temporal de ese archivo. Usa *chips* especializados de alta velocidad llamados memoria de acceso aleatorio o RAM. La RAM está diseñada para el acceso rápido y recuerda enseguida dónde se almacena el archivo en el sistema de discos duros permanentes.

- Almacenamiento o sistema de discos duros. Los discos duros brindan a su servidor una gran biblioteca con todos los archivos a los que accede. El tamaño y tipo de sistemas de discos duros dependen de cuántos datos es necesario almacenar.

- Almacenamiento interno. Los discos duros de los servidores están diseñados especialmente para el acceso rápido y para brindar la posibilidad de agregar muchos discos duros en el interior. Con el tiempo, es posible que deba agregar más discos duros y conectar sistemas de discos duros externos.

- RAID. Del inglés *Redundant Array of Independent Disks* o arreglo redundante de discos independientes: combina discos duros en un único sistema de almacenamiento lógico de gran tamaño que escribe los datos en más de un disco para brindar más confiabilidad.

- Controladora de red. La conexión de red es una de las partes más importantes de cualquier servidor. La controladora de red maneja las entradas y el tráfico de los clientes de la organización.

- Fuente de alimentación. Dado que un servidor suele tener más dispositivos que una computadora típica, requiere una fuente de alimentación más grande (generalmente, de 300 vatios).

1.2.6. Software para servidores

Los requisitos del sistema operativo y del software de aplicaciones de un servidor difieren de los de una computadora. Un servidor puede compartir mejor los datos de varias personas de forma segura y reduce los cuellos de botella.

- Autenticación centralizada. Uno de los más grandes beneficios de un servidor es que puede alojar un directorio central de usuarios. Contiene los nombres de usuario y las contraseñas de todos los empleados de la

empresa. Todos los sistemas de escritorio de la red se conectan al servidor, lo que permite que los usuarios inicien sesión en cualquier computadora de la red con su nombre de usuario y contraseña. Sus archivos y configuraciones aparecerán como si estuvieran frente a su propia computadora.

- Uso compartido de archivos. El directorio central de usuarios también puede usarse para permitir o denegar el acceso a ciertos archivos. El servidor de una empresa pequeña normal tiene recursos compartidos de archivos disponibles que contienen los archivos personales de los usuarios, además de los archivos compartidos a los que pueden acceder otros usuarios cuando resulta necesario.

- Aplicaciones centralizadas. Pueden ejecutarse desde el servidor aplicaciones empresariales adicionales, como un inventario o aplicaciones de administración de los recursos para los clientes, y los empleados pueden usarlas manteniendo la seguridad de los datos en el almacenamiento redundante del servidor

- Respaldo de datos. Uno de los servicios más importantes que presta un servidor es el respaldo de los datos críticos para la empresa. En caso de una falla catastrófica, un incendio o una inundación, estos datos pueden marcar la diferencia entre continuar con las operaciones o cerrarlas para siempre. El software de respaldo que se ejecuta en el servidor hace copias del sistema operativo y los archivos del servidor en cinta o en otro dispositivo de almacenamiento externo.

1.3. Windows Server 2003[17]

En los últimos tiempos se ha producido un gran crecimiento de las redes corporativas basadas en servidores de tecnología Windows NT, Windows *2000* y actualmente Windows 2003. Este crecimiento se ha producido debido a varios factores, siendo fundamental el despliegue generalizado, como plataforma de clientes de la red, de máquinas basadas en los procesadores de Intel con sistemas operativos de Microsoft. La utilización de servidores basados en Windows 2003/2000/NT en entornos como el anterior, permite un buen aprovechamiento de las posibilidades que pueden ofrecer la red corporativa. Windows 2003/2000/NT es una plataforma bastante adecuada para el despliegue de Intranets.

1.3.1. Servicios DHCP

DHCP (*Dynamic Host Configuration Protocol*), son las siglas que identifican a un protocolo empleado para que los *hosts* (clientes) en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de *broadcast*, la característica del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos *hosts* en una red evitando en gran medida los posibles errores humanos.

1.3.1.1. Ventajas

- Una configuración segura y fiable evitando los errores de configuración que se provocan por la necesidad de escribir valores manualmente en cada equipo. Así mismo, DHCP ayuda a evitar los conflictos de

[17] GARCÍA GARCÍA, Rafael, "Gestión y administración de Windows Server 2003", p. 20.

direcciones que causan las direcciones IP previamente asignadas que se utilizan para configurar un equipo nuevo en la red.

- La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y reconfigurar los equipos de la red. Así mismo, el proceso de renovación de concesiones de DHCP ayuda a garantizar que en las situaciones en que sea necesario actualizar a menudo la configuración de los clientes (como en el caso de usuarios con equipos móviles o portátiles que cambian frecuentemente de ubicación).

1.3.1.2. Funcionamiento

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

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

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

Básicamente el servicio DHCP funciona de la siguiente forma. Existe un programa servidor en un *host* de la red que escucha las solicitudes de los clientes y que en su configuración almacena tablas de posibles direcciones IP a otorgar además del resto de la información. Cuando un cliente requiere del servicio, envía una solicitud en forma de *broadcast* a través de la red. Todos los servidores alcanzados por la solicitud responden al cliente con sus respectivas propuestas, éste acepta una de ellas haciéndoselo saber al servidor elegido, el cual le otorga la información requerida. Esta información se mantiene asociada al cliente mientras éste no desactive su interfaz de red o no expire el plazo del contrato (*lease time*).

El plazo del contrato o renta, es el tiempo en que un cliente DHCP mantiene como propios los datos que le otorgó un servidor. Éste se negocia como parte del protocolo entre el cliente y el servidor. Una vez vencido el plazo del contrato el servidor puede renovar la información del cliente, fundamentalmente su dirección IP, y asignarle otra nueva o extender el plazo, manteniendo la misma información. El cliente puede solicitar también la renovación o liberación de sus datos.

A continuación se enumeran los principales mensajes que se intercambian como parte del protocolo DHCP y para que se emplea cada uno:

- *DHCPDISCOVER*: mensaje de *broadcast* de un cliente para detectar los servidores.

- *DHCPOFFER*: mensaje de un servidor hacia un cliente con una oferta de configuración.

- *DHCPREQUEST*: mensaje de un cliente a un servidor para:

- Aceptar la oferta de un servidor determinado y rechazar las otras
- Confirmar la exactitud de la información asignada antes del reinicio del sistema
- Extender el contrato de una dirección IP determinada

- *DHCPPACK*: mensaje del servidor hacia un cliente para enviarle la configuración asignada excluyendo la dirección IP que ya fue aceptada.

- *DHCPNAK*: mensaje del servidor al cliente para indicar que la dirección que tiene asignada es incorrecta (por ejemplo, cuando el cliente cambia de subred) o que el contrato ha expirado.

- *DHCPDECLINE*: mensaje del cliente para el servidor indicando que aún está usando una dirección determinada.

- *DHCPRELEASE*: mensaje del cliente para el servidor para indicar que renuncia a la dirección otorgada y cancela lo que queda del contrato establecido anteriormente.

- *DHCPINFORM*: mensaje del cliente para el servidor para pedir sus parámetros de configuración excluyendo la dirección IP que ya tiene asignada.

Un servidor de DHCP puede identificar a cada cliente a través de dos formas fundamentales:

- La dirección MAC (*Media Access Control*) de la tarjeta de red del cliente
- Un identificador que le indique el cliente

Aunque la idea central del servicio DHCP es la dinamicidad de las direcciones IP asignadas, no se excluye la posibilidad de utilizar direcciones fijas para algunos *hosts* que por sus características lo requieran.

1.3.2. Servicio DNS

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

Por ejemplo, la mayoría de los usuarios prefieren un nombre fácil de utilizar como www.upm.es para localizar un equipo (como un servidor Web o de correo electrónico) en la red. Un nombre sencillo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los servicios de nombres como DNS proporcionan una forma de asignar estos nombres sencillos de los equipos o servicios a sus direcciones numéricas.

1.3.2.1. Nombres de dominio

El Sistema de Nombres de Dominio (DNS) especifica elementos comunes a todas las implementaciones de software relacionadas con DNS, entre los que se incluyen:

- Un espacio de nombres de dominio DNS, que especifica una jerarquía estructurada de dominios utilizados para organizar nombres.

- Los registros de recursos, que asignan nombres de dominio DNS a un tipo específico de información de recurso para utilizar cuando se registra o se resuelve el nombre en el espacio de nombres.

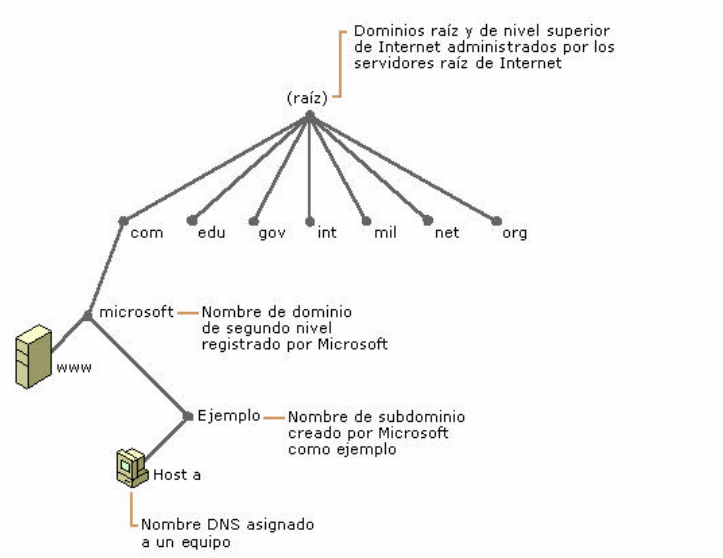
- Los servidores DNS, que almacenan y responden a las consultas de nombres para los registros de recursos.

- Los clientes DNS, que consultan a los servidores para buscar y resolver nombres de un tipo de registro de recursos especificado en la consulta.

1.3.2.2. Espacio de nombres de dominio DNS

El espacio de nombres de dominio DNS, como se muestra en la siguiente figura, se basa en el concepto de un árbol de dominios con nombre. Cada nivel del árbol puede representar una rama o una hoja del árbol. Una rama es un nivel donde se utiliza más de un nombre para identificar una colección de recursos con nombre. Una hoja representa un nombre único que se utiliza una vez en ese nivel para indicar un recurso específico.

Figura 8. **Ejemplo de espacio de nombres de dominio**



Fuente: GARCÍA, Rafael. Microsoft Windows 2003. p. 71.

El gráfico anterior muestra cómo Microsoft es la autoridad asignada por los servidores raíz de Internet para su propia parte del árbol del espacio de nombres de dominio DNS en Internet. Los clientes y los servidores DNS usan las consultas como el método fundamental para resolver los nombres en el árbol como información específica de los tipos de recurso. Los servidores DNS proporcionan esta información a los clientes DNS en las respuestas a las consultas, quienes, a continuación, extraen la información y la pasan al programa solicitante para resolver el nombre consultado.

1.3.2.3. Delegación

Como ya se ha expresado anteriormente una de las ventajas fundamentales de la estructura distribuida del DNS es la descentralización de su administración. El mecanismo que permite resolver un nombre completamente es la delegación. La organización propietaria de un dominio puede dividir éste en varios subdominios y delegar a su vez todo lo concerniente al mantenimiento de la información relacionada y su accesibilidad, a cada uno de estos subdominios. Los dominios de segundo nivel pueden dividirse también en otros subdominios continuando el mecanismo de delegación.

1.3.2.4. Servidores de nombres de dominio

Los programas encargados de agrupar y mantener disponible la información asociada a un espacio de nombres de dominio se conocen como servidores de nombres de dominio. Estos servidores usualmente administran la información referente a una parte del dominio, la cual se conoce como zona.

Entonces se dice que el servidor tiene autoridad sobre la zona. El mismo servidor puede estar autorizado para varias zonas. Una zona se diferencia de un dominio en que ésta no necesariamente incluye la información asociada a los subdominios de éste, aunque puede hacerlo. En este último caso no se produce la delegación a los subdominios incluidos por parte del servidor del dominio padre. Algunos de los tipos de servidores de nombres que existen son:

- Maestros: almacena los registros de las zonas originales y tienen la autoridad de un cierto espacio de nombres donde buscan respuestas concernientes a dicho espacio de nombres.

- Esclavo: responde también a las peticiones que provienen de otros servidores de nombres y que se refieren a los espacios de nombres sobre los que tiene autoridad.

Un servidor de nombres puede ser primario para unas zonas y secundario para otras. Existe un conjunto de servidores de nombres de dominio que controlan el dominio raíz y conocen todos los servidores autorizados para los dominios de primer nivel. Estos servidores son claves en el proceso de resolución de nombres de dominio.

1.3.2.5. Estructura de la base de datos del DNS

A cada nombre de dominio en el DNS se le pueden asociar varias informaciones. Para los nombres de dominio asociados a un *host*, la principal información es su número IP, pero también se le pueden hacer corresponder varios alias, indicar una descripción de la máquina (procesador y sistema operativo), etc. Los registros más importantes son:

- El registro SOA. SOA significa *Start Of Authority* e informa que todos los registros de recursos que le siguen están autorizados a dicho dominio. Los datos asociados con un registro SOA son los siguientes:

    - *Origin*: es el nombre canónico del servidor de nombres primario para este dominio, y generalmente se da como absoluto, es decir, con un punto al final.

    - *Contact*: es el nombre de la persona responsable para este dominio. Es parecido a una dirección de correo electrónico normal,

a excepción que la arroba se remplaza con un punto. También termina con un punto.

- *Serial*: es un número que indica la versión del archivo de zona, y debe ser incrementado cada vez que el archivo se modifique. Es importante porque los servidores secundarios solicitan el registro SOA en ciertos intervalos, para verificar el serial. Si éste ha cambiado, entonces transfieren el archivo completo para actualizarse. Una práctica muy común es utilizar la fecha en el formato aammdd y agregarle dos dígitos más para los cambios que se hacen al archivo en el mismo día. De tal manera, un serial típico podría ser 2001032201.

- *Refresh*: es el intervalo, en segundos, para las revisiones que hacen los servidores secundarios del registro SOA, con el fin de verificar si la información del dominio ha cambiado. El valor típico es de una hora (3 600).

- *Retry*: es el tiempo, en segundos, que un servidor secundario debe esperar para reintentar una conexión por *refresh* que ha fallado. El valor recomendado es de 10 minutos (600 segundos).

- *Expire*: si un servidor secundario no ha podido comunicarse con su servidor primario para verificar que no haya habido cambios a la zona (mediante su registro SOA), descartará la información que tiene después de este período dado en segundos. El valor típico es de 42 días, o sea 3 600 000.

- *Minimum*: este es el número de segundos empleado en los registros del archivo que no especifican su campo ttl (*time to live*).

- El registro A. Este registro sirve para asociar un nombre de máquina con una dirección IP. El único dato para este tipo de registro es la dirección IP en su forma estándar xxx.xxx.xxx.xxx. Debe haber sólo un registro A por cada dirección IP en el archivo, aunque es posible asignarle a una máquina más de una dirección mediante varios registros A.

- El registro NS. Mediante un registro NS es posible designar un servidor que deberá responder para todas las peticiones que involucren un determinado subdominio. Esto es importante porque permite delegar la asignación de nombres y facilita el manejo de dominios complejos.

- El registro PTR. Un registro PTR se utiliza para relacionar una dirección IP con un nombre de máquina, exactamente al revés que un registro tipo A. Estos registros aparecen en los archivos de zonas para la resolución inversa. En cada registro sólo aparece una fracción de la dirección IP: la dirección se completa porque a cada nombre que no termina en un punto se le agrega el origen. Los nombres de máquinas aparecen siempre en los registros PTR en su forma canónica, es decir, con el dominio completo.

- El registro MX. Los registros MX sirven para anunciar a los programas de intercambio de correo, una máquina que se encarga de administrar el correo de un determinado dominio.

- El registro CNAME. Este registro sirve para asignarle un nombre alternativo o alias a una máquina. Todos estos tipos de datos se conocen como *Resource Records* (RR) y se asocian a los nombres de dominios.

1.3.3. Directorio activo

El Directorio Activo, es el servicio de directorio en una red Windows 2000 y Windows Server 2003. Un servicio de directorio, es un servicio de red donde se almacena la información de los recursos de la red para hacer más fácil la accesibilidad a las aplicaciones y a los usuarios. El servicio de directorio proporciona una manera consistente de nombrar, describir, localizar, acceder, administrar y asegurar la información los recursos. El Directorio Activo proporciona la funcionalidad al servicio de Directorio, incluyendo los medios de centralizar, administrar y controlar los accesos a los recursos de la red.

El Directorio Activo produce que la topología de la red física y los protocolos sean transparentes para que los usuarios de una red puedan acceder a los recursos sin tener que saber dónde están situados esos recursos o cómo están conectados físicamente. El Directorio Activo organiza el directorio en secciones que permiten almacenar un gran número de objetos. Como resultado, el Directorio Activo puede expandirse tanto como requiera la organización, desde un servidor con cientos de objetos hasta cientos de servidores con millones de objetos.

La seguridad está integrada en el Directorio Activo mediante la autenticación del inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión en la red, los administradores pueden administrar datos del directorio y de la organización en cualquier punto de la red, y los usuarios autorizados de la red pueden tener acceso a recursos en

cualquier lugar de la red. La administración basada en directivas facilita la tarea del administrador incluso en las redes más complejas El Directorio Activo también incluye:

- Un conjunto de reglas, el esquema, que define las clases de objetos y los atributos contenidos en el directorio, así como las restricciones y los límites en las instancias de estos objetos y el formato de sus nombres.

- Un catálogo global que contiene información acerca de cada uno de los objetos del directorio. Esto permite a los usuarios y administradores encontrar información del directorio con independencia de cuál sea el dominio del directorio que realmente contiene los datos.

- Un sistema de índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar y encontrar los objetos y sus propiedades.

- Un servicio de replicación que distribuye los datos del directorio por toda la red. Todos los controladores de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio para su dominio. Cualquier cambio en los datos del directorio se replica en todos los controladores del dominio.

- Compatibilidad con el software de cliente del Directorio Activo, lo que permite que muchas de las características de Windows 2000 Professional o Windows XP Professional también estén disponibles en los equipos que ejecutan Windows 95, Windows 98 y NT Server 4.0.

Ventajas que ofrece el Directorio Activo:

- Reduce el coste de propiedad (TCO). Las políticas de grupo con el Directorio Activo permiten configurar entornos de trabajo e instalar aplicaciones desde una consola administrativa. Esto reduce el tiempo que se necesita en ir a cada equipo para configurar e instalar aplicaciones.

- Administración simplificada. Proporciona una localización simple de la información almacenada como recursos y usuarios. Esto simplifica la administración y hace más fácil a los usuarios encontrar los recursos a través de la red. Además, elimina la dependencia con las ubicaciones físicas ya que permite un único punto de administración.

- Administración flexible. Permite delegar los permisos sobre usuarios y equipos a otros usuarios o grupos.

- Escalabilidad. En Windows NT 4.0, los dominios tienen un límite claro de hasta 40 000 objetos. Aún así se tienen que crear muchos dominios en una organización grande. Un dominio con Directorio Activo puede contener millones de objetos.

- Protocolo basado en estándar. El acceso al Directorio Activo se lleva a cabo a través del protocolo de acceso a Directorio *Lightweight* (LDAP). Las aplicaciones usan LDAP mejor que los protocolos propietarios para acceder y cambiar la información en el Directorio Activo.

1.3.3.1. Directorio Activo y DNS

El Directorio Activo utiliza DNS para las siguientes funciones:

- Resolución de Nombres. DNS proporciona la resolución de nombres traduciendo los nombres de los *host* a direcciones IP.

- Definición del Espacio de Nombres. El Directorio Activo usa DNS para nombrar a los dominios. Los nombres de los dominios de Windows 2000 y Windows Server 2003 son nombres de dominio DNS.

- Localización del componente físico del Directorio Activo. Para hacer *logon* en la red y ejecutar las peticiones del Directorio Activo, un equipo debe primero localizar un controlador de dominio para proceder a la autentificación de *logon*.

1.3.3.2. Estructura lógica

Directorio Activo, es una estructura arbolada jerárquica que agrupa, de menor a mayor, los siguientes componentes:

- Objetos
- Objetos contenedores
- Unidades organizativas
- Dominios
- Árboles
- Bosques

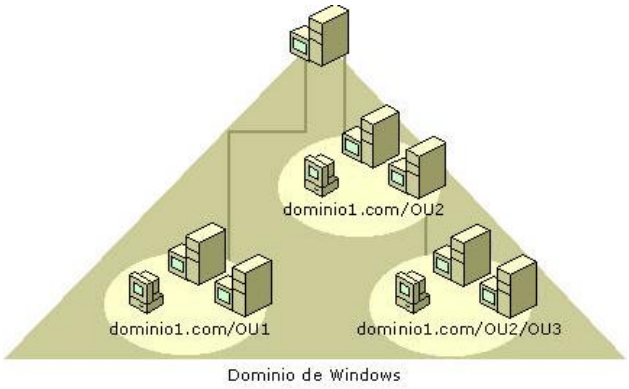
1.3.3.2.1. Objetos y contenedores

Un objeto puede ser la representación de un sistema, un usuario, un recurso, un servicio, etc. Cada tipo tiene sus propios atributos característicos del tipo de objeto. Un objeto Usuario necesita tener definidos ciertos atributos propios: nombre del usuario, los datos personales, etc. Por su parte, otro tipo de objeto, por ejemplo, el objeto Sistema, tendrá diferentes atributos: la dirección IP, el nombre del ordenador, etc. Cada objeto en el Directorio Activo tiene una identidad única. Los objetos se pueden mover y renombrar, pero su identidad nunca cambia.

1.3.3.2.2. Unidades organizativas

Las unidades organizativas, son contenedores del Directorio Activo en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas. Una unidad organizativa no puede contener objetos de otros dominios. Una unidad organizativa es el ámbito o unidad más pequeña a la que se pueden asignar configuraciones de Directiva de grupo o en la que se puede delegar la autoridad administrativa. Con las unidades organizativas, puede crear contenedores dentro de un dominio que representan las estructuras lógicas y jerárquicas existentes dentro de una organización. Esto permite administrar la configuración y el uso de cuentas y recursos en función de su modelo organizativo.

Figura 9. **Ejemplo de unidades organizativas dentro de un dominio**



Fuente: GARCÍA, Rafael. Microsoft Windows 2003. p. 115.

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

1.3.3.2.3. Dominios

Un dominio constituye un límite de seguridad. El directorio incluye uno o más dominios, cada uno de los cuales tiene sus propias directivas de seguridad y relaciones de confianza con otros dominios. Los dominios ofrecen varias ventajas:

- Las directivas y la configuración de seguridad (como los derechos administrativos y las listas de control de accesos) no pueden pasar de un dominio a otro.

- Al delegar la autoridad administrativa en dominios o unidades organizativas desaparece la necesidad de tener varios administradores con autoridad administrativa global.

- Los dominios ayudan a estructurar la red de forma que refleje mejor la organización.

- Cada dominio almacena solamente la información acerca de los objetos que se encuentran ubicados en ese dominio. Al crear particiones en el directorio, Directorio Activo puede ampliarse y llegar a contener una gran cantidad de objetos.

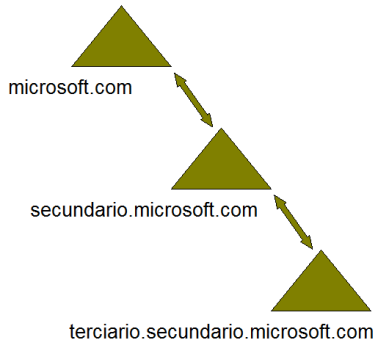
Para crear un dominio, debe promover uno o más equipos que ejecuten Windows 2000 Server o Windows Server 2003 a controladores de dominio. Cada dominio debe tener al menos un controlador de dominio.

1.3.3.2.4. Árboles

Todos los dominios que comparten el mismo dominio raíz forman un espacio de nombres contiguo llamado árbol. El primer dominio de un árbol de dominio se denomina dominio raíz. Los dominios adicionales del mismo árbol de dominio son dominios secundarios. Un dominio que se encuentra inmediatamente encima de otro dominio del mismo árbol se denomina dominio principal del dominio secundario.

En la siguiente figura, secundario.microsoft.com, es un dominio secundario de microsoft.com y dominio principal de secundario2.secundario.microsoft.com. El dominio microsoft.com es el dominio principal de secundario.microsoft.com. Además, es el dominio raíz de este árbol.

Figura 10. **Ejemplo de árbol de dominios**



Fuente: GARCÍA, Rafael. Microsoft Windows 2003. p. 116.

Los dominios de Windows 2000 y Windows Server 2003 que forman parte de un árbol están unidos entre sí mediante relaciones de confianza transitivas y bidireccionales. Dado que estas relaciones de confianza son bidireccionales y transitivas, un dominio de Directorio Activo recién creado en un bosque o árbol de dominio tiene establecidas inmediatamente relaciones de confianza con todos los demás dominios en ese bosque o árbol de dominio. Estas relaciones de confianza permiten que un único proceso de inicio de sesión sirva para autenticar a un usuario en todos los dominios del bosque o del árbol de dominio.

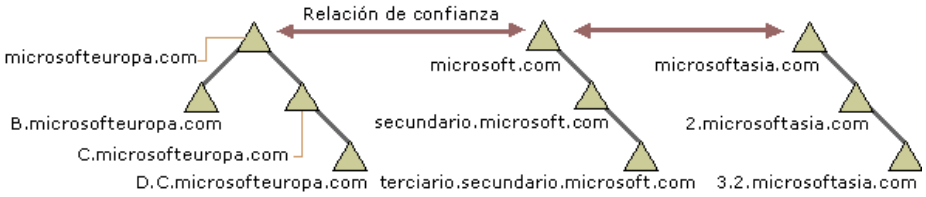
Sin embargo, esto no significa que el usuario, una vez autenticado, tenga permisos y derechos en todos los dominios del árbol de dominio. Dado que un

dominio es un límite de seguridad, los derechos y permisos deben asignarse para cada dominio.

1.3.3.2.5. Bosques

Un bosque está formado por varios árboles de dominio. Los árboles de dominio de un bosque no constituyen un espacio de nombres contiguo. Por ejemplo, aunque dos árboles de dominio (microsoft.com y microsoftasia.com) pueden tener ambos un dominio secundario denominado soporte, los nombres DNS de esos dominios secundarios serán soporte.microsoft.com y soporte.microsoftasia.com. Es evidente que en este caso no existe un espacio de nombres contiguo.

Figura 11. **Ejemplo de bosques de dominios**



Fuente: GARCÍA, Rafael. Microsoft Windows 2003. p. 117.

Sin embargo, un bosque no tiene ningún dominio raíz propiamente dicho. El dominio raíz del bosque es el primer dominio que se creó en el bosque. Los dominios raíz de todos los árboles de dominio del bosque establecen relaciones de confianza transitivas con el dominio raíz del bosque. En la figura anterior, microsoft.com es el dominio raíz del bosque. Los dominios raíz de los otros árboles de dominio (microsofteuropa.com y microsoftasia.com) tienen establecidas relaciones de confianza transitivas con microsoft.com.

Al utilizar bosques y árboles de dominio se obtiene la flexibilidad que ofrecen los sistemas de espacios de nombres contiguos y no contiguos. Esto puede ser útil, por ejemplo, en el caso de compañías que tienen divisiones independientes que necesitan conservar sus propios nombres DNS.

1.3.3.3. Estructura física

En el Directorio Activo, la estructura lógica está separada de la estructura física. La estructura lógica se usa para organizar los recursos de la red y se usa la estructura física para configurar y administrar el tráfico de red. La estructura física del Directorio Activo está compuesta por *sites* y controladores de dominio.

Esta estructura define dónde y cuándo ocurrirá el tráfico de *logon* y de replicación. Entender los componentes de la estructura física del Directorio Activo es importante para optimizar el tráfico de red y el proceso de *logon*. Esta información ayudará a resolver problemas con los *loggins* y con la replicación.

1.3.3.3.1. Sitio

Un sitio, es la combinación de una o más subredes IP conectadas en enlaces de alta velocidad. Esta definición permite configurar el acceso al Directorio Activo y la topología de replicación para que Windows 2000 y/o Windows Server 2003 utilicen los enlaces más eficientes y sincronice el tráfico de replicación y de *logon*. Se crean Sitios por dos razones importantes:

- Optimizar el tráfico de replicación.

- Posibilitar a los usuarios conectarse con controladores de dominio usando una posible conexión de alta velocidad.

Los Sitios mapean la estructura física de la red al igual que los dominios mapean la estructura lógica de la correlación. La estructura física y lógica del Directorio Activo son independientes una de la otra lo cual tiene las siguientes consecuencias:

- No hay correlación entre la estructura física de la red y su estructura de dominio.

- El Directorio Activo permite múltiples dominios en un solo sitio al igual que múltiples Sitios en un solo dominio.

Sitios y Servicios del Directorio Activo permite especificar la información de los Sitios. El Directorio Activo utiliza esta información para determinar el mejor modo de utilizar los recursos de la red disponibles. Esto aumenta la eficacia de los siguientes tipos de operaciones:

- Solicitudes de servicio. Cuando un cliente solicita un servicio a un controlador de dominio, éste la dirige a un controlador de dominio del mismo sitio, si hay alguno disponible. La selección de un controlador de dominio que esté conectado correctamente con el cliente que formuló la solicitud facilita su tratamiento.

- Replicación. Los sitios optimizan la replicación de información del directorio. La información de configuración y de esquema del directorio se distribuye por todo el bosque y los datos del dominio se distribuyen entre todos los controladores de dominio del dominio. Al reducir la replicación de forma estratégica, igualmente se puede reducir el uso de la red. El Directorio Activo replica información del directorio dentro de un sitio con mayor frecuencia que entre sitios. De esta forma, los controladores de

dominio mejor conectados, es decir, aquellos que con más probabilidad necesitarán información especial del directorio, son los que primero reciben las replicaciones.

1.3.3.3.2. Controladores de dominio

Los controladores del dominio, son equipos que ejecutan Windows 2000 Server, Advanced Server o Datacenter Server, o bien, Windows Server 2003 Standard Edition, Enterprise Edition y Datacenter Edition donde se almacena una copia del directorio. También administra los cambios del directorio y los replica a otros controladores de dominio del mismo dominio. Los controladores de dominio almacenan los datos de directorio administra el proceso de *logon* de los usuarios, autentificación y búsquedas del directorio. Un dominio puede tener uno o más controladores de dominio.

Una organización pequeña que utilice una red de área local (LAN) puede necesitar nada más que un solo dominio con dos controladores de dominio para proporcionar la adecuada disponibilidad y tolerancia a fallos mientras que una compañía grande con muchas localizaciones geográficas necesitará uno o más controladores de dominio en cada localización para proporcionar también una adecuada disponibilidad y tolerancia a fallos requerido.

El Directorio Activo utiliza la replicación *multi-master*, en la que ningún controlador de dominio es el controlador de dominio maestro. En lugar de eso, todos los controladores de dominio contienen una copia del directorio. Cualquier controlador de dominio puede almacenar una copia del directorio con información diferente durante cortos períodos de tiempo hasta que todos los controladores de dominio realicen una sincronización de los cambios hechos en el Directorio Activo.

1.3.3.4. Administración de usuarios y grupos

Una cuenta, es un registro con toda la información necesaria para definir un usuario, grupo o equipo en Windows Server 2003. Una cuenta de usuario incluye la contraseña y nombre de usuario necesarios para iniciar una sesión, los grupos a los que pertenece la cuenta del usuario y los derechos y permisos que tiene el usuario para utilizar el equipo y la red, y tener acceso a sus recursos. En Windows Server 2003 que se comportan como servidores miembro, las cuentas de usuario y grupo se administran con usuarios y grupos locales. En los controladores de dominio de Windows Server 2003, las cuentas de usuario, grupos y equipos se administran con usuarios y equipos de Microsoft Active Directory.

Una cuenta de usuario o de equipo hace posible:

- Autenticar la identidad de la persona o equipo que se conecta a la red
- Controlar el acceso a los recursos del dominio
- Auditar las acciones realizadas utilizando la cuenta

1.3.3.4.1. Administración de cuentas y grupos locales

Usuarios y grupos locales es una herramienta que se puede usar para administrar los usuarios y grupos locales. Está disponible en equipos donde se ejecutan los siguientes sistemas:

- Clientes que utilicen Microsoft Windows 2000 Professional o Windows XP Professional.

- Servidores miembro que ejecuten cualquiera de los productos de las familias Microsoft Windows 2000 Server o Windows Server 2003.

- Servidores independientes que ejecuten cualquiera de los productos de las familias Microsoft Windows 2000 Server o Windows Server 2003.

Los usuarios y los grupos tienen importancia en la seguridad de sistemas Windows XP, Windows 2000 y Windows Server 2003 porque, al asignarles derechos y permisos, se puede limitar la capacidad de los usuarios y los grupos para llevar a cabo ciertas acciones. Un derecho autoriza a un usuario a realizar ciertas acciones en un equipo, como efectuar copias de seguridad de archivos y carpetas, o apagar un equipo. Un permiso es una regla asociada con un objeto (normalmente un archivo, carpeta o impresora) que regula los usuarios que pueden tener acceso al objeto y de qué manera.

1.3.3.4.2. Administración de cuentas y grupos en el Directorio Activo

Las cuentas de usuario y de equipo del Directorio Activo representan una entidad física como una persona o un equipo. Las cuentas de usuario y de equipo (así como los grupos) se denominan principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asignan automáticamente identificadores de seguridad. Los objetos con identificadores de seguridad pueden iniciar sesiones en la red y tener acceso a los recursos del dominio.

Cuando se establece una confianza entre un dominio de Windows Server 2003 de un bosque específico y un dominio de Windows Server 2003 que se

encuentra fuera de ese bosque, se puede conceder a los principales de seguridad del dominio externo el acceso a los recursos del bosque.

1.3.3.5. Directivas de grupo

En el sistema operativo Windows Server 2003, las políticas de grupo definen las configuraciones para usuarios, grupos de usuarios y ordenadores. Puede crear una configuración específica de escritorio para cualquier grupo particular de usuarios. Estas configuraciones de políticas de grupo que usted crea se encuentran en el Objeto de políticas de grupo (GPO) que a su vez está asociado con objetos seleccionados del Directorio Activo tales como sitios, dominios o unidades organizativas.

Se denominan Directivas de grupo al conjunto de valores de configuración utilizados por el administrador para gestionar objetos que actúan durante la inicialización y la finalización de los equipos y durante el inicio de la sesión y el final de la sesión de los usuarios.

Por medio de estas directivas, el administrador controla los entornos de trabajo de los usuarios del dominio y el comportamiento de un objeto determinado. Las Directivas de grupo se pueden utilizar para administrar las características que incluye la familia Microsoft Windows Server 2003, tales como instalación de software, plantillas administrativas, redirección de carpetas, configuración de seguridad, secuencias de comandos (inicio o apagado, e inicio de sesión o cierre de sesión) y mantenimiento de Internet Explorer.

El administrador de las directivas de grupo puede definir, por ejemplo, los programas que se visualizarán en el escritorio de los usuarios, las opciones del menú Inicio de cada usuario, los archivos que copiarán en la carpeta Mis

Documentos, el acceso a los archivos y a las carpetas. Las directivas de grupo también pueden influir en los permisos que se otorgan a las cuentas de usuarios y de grupos.

Las directivas de grupo afectan a usuarios y a equipos. Las directivas de grupo de usuario se activan en el momento que el usuario inicia su sesión, mientras que, por su parte, las directivas de grupo de equipo se activan en el inicio del sistema. Las directivas de grupo constan de varios componentes configurables. El primero son las plantillas administrativas, que definen las directivas basadas en el registro. Las plantillas administrativas ofrecen información de la directiva para los elementos que aparecen bajo la carpeta plantillas administrativas en el árbol de la consola del editor de objetos de directivas de grupo. Los componentes principales de directivas de grupo son los siguientes:

- Instalación de software: asigna las aplicaciones a los usuarios.

- Administrar la directiva basada en el Registro con las plantillas administrativas. La Directiva de grupo crea un archivo con valores del registro que se escriben en la parte usuario o equipo local de la base de datos del registro.

- Secuencia de comando: especifica las secuencias de comandos para el inicio y el apagado de los ordenadores, así como para los eventos de inicio y cierre de sesión de los usuarios.

- Redirección de carpetas: ubica en la red las carpetas especiales como Mis documentos o las carpetas de aplicación específicas.

- Configuraciones de seguridad: configura la seguridad de los usuarios, de los ordenadores y de los dominios.

1.3.3.5.1. Configuración de directiva de grupo

En la raíz del espacio para el nombre del editor de políticas de grupo hay dos nodos principales: configuración del ordenador y configuración del usuario. Estas son las carpetas principales que utiliza para configurar ambientes de escritorio específicos y para aplicar las Políticas de grupo en los ordenadores y usuarios en la red.

- Las configuraciones de la computadora incluyen políticas que especifican el comportamiento del sistema operativo, la apariencia del escritorio, la configuración de las aplicaciones, las aplicaciones asignadas, las opciones de implementación de archivo, las configuraciones de seguridad y los *scripts* de iniciar y apagar el ordenador.

- Las configuraciones del usuario incluyen toda la información específica del usuario tal como el comportamiento del sistema operativo, las configuraciones de escritorio, las configuraciones de aplicaciones, aplicaciones asignadas y publicadas, opciones de implementación de archivos, configuraciones de seguridad y *scripts* de conexión y desconexión de usuarios.

Además de aplicar esa configuración a equipos y usuarios cliente, puede aplicarla a servidores miembros y controladores de dominio en el ámbito de un bosque del Directorio Activo. Dentro de la configuración del ordenador y de la configuración del usuario existen las siguientes carpetas:

- Plantillas administrativas. Bajo esta carpeta se almacena la información de directivas basada en el registro.

    - Sistema (*System.adm*): controla características como el escritorio, las conexiones de red, las carpetas compartidas y el panel de control.

    - Internet Explorer (*Inetres.adm*): permite configurar características como las zonas de seguridad, la configuración de *proxy*, las búsquedas y los archivos temporales de Internet.

    - Reproductor de Windows Media (*Wmplayer.adm*): controla características como la configuración de *proxy*, *códec* y el *búfer* de red.

    - NetMeeting (*Conf.adm*): permite controlar características como compartir aplicaciones, audio, vídeo y charla.

    - Windows Update (*Wuau.adm*): permite configurar características como las actualizaciones automáticas de software a través de Internet.

- Configuración del software. Contiene los valores de configuración de software que se aplican a todos los usuarios que inician sesión en el equipo. Esta carpeta contiene la configuración de instalación de software y puede incluir otros valores de configuración procedentes de proveedores independientes de software.

- Configuración de Windows. Contiene los valores de configuración de Windows que se aplican a todos los usuarios que inician sesión en el equipo. Esta carpeta también contiene los siguientes elementos: configuración de seguridad y secuencias de comandos.

1.3.3.5.2. Objetos de directiva de grupo

Los valores de configuración de la directiva de grupo se almacenan en objetos de directiva de grupo (GPOs, group policy objects). Se puede tener un grupo de directivas de grupo contenidas en un objeto GPO asociado a un sitio, dominio o a una unidad organizativa, y, por otra parte, el mismo objeto GPO se puede aplicar a varios sitios, dominios o unidades organizativas.

Existen dos clases de objetos GPO:

- Objetos de tipo local: en cada equipo de Windows Server 2003 hay un único objeto de directiva local y es un subconjunto del objeto de directiva no local. Los valores se pueden sobrescribir con los valores no locales.

- Objetos de directiva no local. Estos objetos se almacenan en el controlador de dominio, en el Directorio Activo y, en caso de conflictos, tienen prioridad sobre el objeto de grupo local.

Todos los equipos que ejecutan Windows XP Professional, Windows XP 64-Bit Edition o los sistemas operativos Windows Server 2003, tienen exactamente un objeto de directiva de grupo. Éste se almacena en raíz Sistema\System32\GroupPolicy. Los objetos de directiva de grupo, excepto el objeto de directiva de grupo local, son objetos virtuales. La información de configuración de directivas de un GPO se almacena en dos ubicaciones:

- Contenedor de directivas de grupo, es un contenedor del Directorio Activo que almacena propiedades de GPO, incluida la información de la versión, el estado de GPO y una lista de componentes que tienen valores de configuración el GPO.

- Plantilla de directiva de grupo, es una estructura de directorio en el sistema de archivos que almacena directivas basadas en plantillas administrativas, opciones de configuración de seguridad, archivos de secuencias de comandos e información respecto a las aplicaciones disponibles para Instalación de software de directiva de grupo. La plantilla de directiva de grupo se encuentra en la carpeta de volumen del sistema (*Sysvol*), en la subcarpeta \Directivas de su dominio.

1.3.3.5.3. Herencia de directiva de grupo

Las directivas se pueden heredar de contenedores (sitios, dominios o unidades organizativas) padres a contenedores hijos. No obstante si se establece una directiva a nivel de carpeta hija, esta directiva reemplaza a la directiva que le puede llegar por herencia.

Cuando existen directivas a nivel de contenedor padre y directivas particulares a nivel de contenedor hijo (es decir, además de las directivas heredadas del contenedor padre), las directivas del contenedor hijo son acumulativas, salvo que se produzca alguna incompatibilidad. En tal caso, se cumple la directiva a nivel de contenedor hijo.

Las directivas son heredables pero el mecanismo de herencia se puede bloquear para evitar que un contenedor hijo reciba las directivas que hay definidas en el contenedor padre. Por contrapartida, así como se puede

bloquear la herencia también es posible bloquear el reemplazo de una directiva definida a un nivel superior por otra directiva, no compatible, definida a nivel inferior. En caso de conflicto, esta opción tiene prioridad sobre la opción del bloqueo de herencia.

1.4. Seguridad de Interconexión de redes

La seguridad de redes, es un nivel de seguridad que garantiza que el funcionamiento de todos los equipos de una red sea óptimo y que todos los usuarios de estos equipos posean los derechos que les han sido concedidos.

1.4.1. Conceptos de seguridad[18]

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

[18]http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf, p. 1. Consulta: 6 de marzo de 2012.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

1.4.1.1. ¿Cuál puede ser el valor de los datos?

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Cuando hablamos del valor de la información nos referimos, por ejemplo, a qué tan peligroso es enviar la información de mi tarjeta de crédito a través de Internet para hacer una compra, en una red gigantesca donde viajan no únicamente los 16 dígitos de mi tarjeta de crédito sino millones de datos más , gráficas, voz y vídeo.

De hecho, este tema es complejo. Algunos expertos opinan que se corre más peligro cuando se entrega una tarjeta de crédito al empleado de un restaurante o cuando se la emplea telefónicamente para efectivizar alguna compra.

El peligro más grande radica no en enviar la información sino una vez que esta información, unida a la de miles de clientes más, reposa en una base de datos de la compañía con las que se concretó el negocio. Con un único acceso

no autorizado a esta base de datos, es posible que alguien obtenga no únicamente mis datos y los de mi tarjeta, sino que tendrá acceso a los datos y tarjetas de todos los clientes de esta compañía.

1.4.1.2. Seguridad global

El concepto de red global incluye todos los recursos informáticos de una organización, aún cuando estos no estén interconectados.

De manera que, seguridad global es mantener bajo protección todos los componentes de una red global. Al fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad.

Por ejemplo, permite que se determine exactamente lo que debe hacer cada uno y cómo debe hacerlo, y, también las desviaciones que se pueden producir. De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene. Para realizar esto, lo más usado, y que da muy buenos resultados es hacer grupos de trabajo en los cuales se informen los fines, objetivos y ganancias de establecer medidas de seguridad, de tal manera que los destinatarios finales se sientan informados y tomen para sí los conceptos. Este tipo de acciones favorece, la adhesión a estas medidas.

1.4.1.3. Impacto en la organización

La implementación de políticas de seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. ¿Cómo pueden impactar si se implementan para hacer más seguro el sistema? En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativa.

Por otro lado, al poner en funcionamiento una nueva norma de seguridad, ésta traerá una nueva tarea para la parte técnica (por ejemplo, cambiar los derechos a algo de algunos usuarios) y administrativamente, se les deberá avisar por medio de una nota de los cambios realizados y en qué les afectará.

1.4.1.4. Implementación

La implementación de medidas de seguridad, es un proceso técnico administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la implementación de estas medidas. Será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen. También, es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

De todo lo expuesto anteriormente, resulta claro que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

1.4.2. Firewall[19]

Un sitio pequeño puede tener acceso a Internet a través de cable módem, una línea ADSL o, a menudo, a través de una conexión PPP a una cuenta de acceso telefónico. El equipo conectado directamente a Internet es el centro de las cuestiones de seguridad. Si se dispone de un equipo o una red de área local (LAN, Local Area Network) pequeña de equipos conectados, el centro de un sitio pequeño será la máquina que tiene la conexión directa a Internet. Esta máquina será la máquina firewall.

El término firewall (cortafuegos o servidor de seguridad) tiene varios significados dependiendo de su implementación y de su propósito. Utilizaremos el término firewall para referirnos a la máquina conectada a Internet. Aquí es donde se implementarán las directivas de seguridad. La tarjeta de interfaz de red externa de la máquina firewall es el punto de conexión, o pasarela, a Internet. El objetivo de un firewall es proteger lo que hay en el lado del usuario de esta pasarela de los que hay al otro lado.

Una configuración simple de firewall suele recibir el nombre de firewall bastión, debido a que es la principal línea de defensa contra cualquier ataque desde el exterior. Todas las medidas de seguridad se implementan desde este

[19] ZIEGLER, Robert L., "Firewall Linux, Guía Avanzada", p. 3.

defensor de su entorno. En consecuencia, es el que hace todo lo posible para proteger el sistema. Es el primer y único bastión de defensa.

Detrás de esta línea de defensa se encuentra el equipo o el grupo de equipos del usuario. El propósito de la máquina firewall puede ser simplemente servir como punto de conexión a Internet para otras máquinas de la LAN. Quizá detrás de este firewall, se ejecuten servicios privados locales, como una impresora compartida o un sistema de archivos compartido.

En algún momento, se querrán ofrecer servicios propios a Internet. Una de las máquinas podría estar albergando un sitio web propio para Internet. La configuración y objetivos particulares determinarán las directivas de seguridad.

El propósito del firewall, es hacer cumplir unas determinadas directivas de seguridad. Estas directivas reflejan las decisiones que se han tomado sobre qué servicios de Internet deben ser accesibles a los equipos, qué servicios se quieren ofrecer al exterior desde los equipos, qué servicios se quieren ofrecer a usuarios remotos o sitios específicos y qué servicios y programas se quieren ejecutar localmente para uso privado. Todas directivas de seguridad están relacionadas con el control de acceso y uso autenticado de servicios privados o protegidos y de programas y archivos en los equipos.

1.4.3. Netfilter/iptables[20]

Netfilter, es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es

[20] http://es.wikipedia.org/wiki/Netfilter/iptables. Consulta: 8 de marzo de 2012.

también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

El componente más popular construido sobre Netfilter es iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de *log*. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

Iptables, es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre iptables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de iptables tales como el connection tracking system o sistema de seguimiento de conexiones, que permite encolar paquetes para que sean tratados desde espacio de usuario. iptables es un software disponible en prácticamente todas las distribuciones de Linux actuales.

1.4.3.1. Resumen de operación

Iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica qué paquetes la cumplen (*match*) y un objetivo que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red

que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la política de destino de la cadena dicta qué hacer con el paquete.

Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se denomina *implicit target* RETURN o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas.

En iptables, las reglas se agrupan en cadenas. Una cadena, es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos. Cada regla puede desechar el paquete de la cadena, con lo cual otras cadenas no serán consideradas. Una cadena puede contener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno, va a continuar en la primera cadena. No hay un límite respecto de cuán anidadas pueden estar las cadenas. Hay tres cadenas básicas (INPUT, OUTPUT y FORWARD: ENTRADA, SALIDA y REENVÍO) y el usuario puede crear tantas como desee. Una regla puede ser simplemente un puntero a una cadena.

1.4.3.2. Tablas

Hay tres tablas ya incorporadas, cada una de las cuales contiene ciertas cadenas predefinidas. Es posible crear nuevas tablas mediante módulos de

extensión. El administrador puede crear y eliminar cadenas definidas por usuarios dentro de cualquier tabla. Inicialmente, todas las cadenas están vacías y tienen una política de destino que permite que todos los paquetes pasen sin ser bloqueados o alterados.

- Filter table (Tabla de filtros): esta tabla es la responsable del filtrado (es decir, de bloquear o permitir que un paquete continúe su camino). Todos los paquetes pasan a través de la tabla de filtros. Contiene las siguientes cadenas predefinidas y cualquier paquete pasará por una de ellas:

    - INPUT *chain* (Cadena de ENTRADA): todos los paquetes destinados a este sistema atraviesan esta cadena (y por esto se la llama algunas veces LOCAL_INPUT o ENTRADA_LOCAL).

    - OUTPUT *chain* (Cadena de SALIDA): todos los paquetes creados por este sistema atraviesan esta cadena (a la que también se la conoce como LOCAL_OUTPUT o SALIDA_LOCAL).

    - FORWARD *chain* (Cadena de REDIRECCIÓN): todos los paquetes que meramente pasan por este sistema para ser encaminados a su destino recorren esta cadena.

- Nat table (Tabla de traducción de direcciones de red): esta tabla es la responsable de configurar las reglas de reescritura de direcciones o de puertos de los paquetes. El primer paquete en cualquier conexión pasa a través de esta tabla; los veredictos determinan como van a reescribirse todos los paquetes de esa conexión. Contiene las siguientes cadenas redefinidas:

- PREROUTING *chain* (Cadena de PRERUTEO): los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de ruteo local, principalmente para DNAT (destination-NAT o traducción de direcciones de red de destino).

- POSTROUTING *chain* (Cadena de POSRUTEO): los paquetes salientes pasan por esta cadena después de haberse tomado la decisión del ruteo, principalmente para SNAT (source-NAT o traducción de direcciones de red de origen).

- OUTPUT *chain* (Cadena de SALIDA): permite hacer un DNAT limitado en paquetes generados localmente.

- Mangle table (Tabla de destrozo): esta tabla es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio. Todos los paquetes pasan por esta tabla. Debido a que está diseñada para efectos avanzados, contiene todas las cadenas predefinidas posibles:

  - PREROUTING *chain* (Cadena de PRERUTEO): todos los paquetes que logran entrar a este sistema, antes de que el ruteo decida si el paquete debe ser reenviado (cadena de REENVÍO) o si tiene destino local (cadena de ENTRADA).

  - INPUT *chain* (Cadena de ENTRADA): todos los paquetes destinados para este sistema pasan a través de esta cadena.

- FORWARD *chain* (Cadena de REDIRECCIÓN): todos los paquetes que exactamente pasan por este sistema pasan a través de esta cadena.

- OUTPUT *chain* (Cadena de SALIDA): todos los paquetes creados en este sistema pasan a través de esta cadena.

- POSTROUTING *chain* (Cadena de POSRUTEO): todos los paquetes que abandonan este sistema pasan a través de esta cadena.

1.4.3.3. Destinos de regla

El destino de una regla puede ser el nombre de una cadena definida por el usuario o uno de los destinos ya incorporados ACCEPT, DROP, QUEUE, o RETURN (aceptar, descartar, encolar o retornar, respectivamente). Cuando un destino es el nombre de una cadena definida por el usuario, al paquete se lo dirige a esa cadena para que sea procesado (tal como ocurre con una llamada a una subrutina en un lenguaje de programación).

Si el paquete consigue atravesar la cadena definida por el usuario sin que ninguna de las reglas de esa cadena actúe sobre él, el procesamiento del paquete continúa donde había quedado en la cadena actual. Estas llamadas entre cadenas se pueden anidar hasta cualquier nivel deseado.

Existen los siguientes destinos ya incorporados:

- ACCEPT (aceptar): este destino hace que netfilter acepte el paquete. El significado de esto depende de cuál sea la cadena realizando esta aceptación. Un paquete que se acepta en la cadena de ENTRADA se le

permite ser recibido por el sistema (*host*), un paquete que se acepta en la cadena de SALIDA se le permite abandonar el sistema y un paquete que se acepta en la cadena de REDIRECCIÓN se le permite ser encaminado (*routing*) a través del sistema.

- DROP (descartar): este destino hace que netfilter descarte el paquete sin ningún otro tipo de procesamiento. El paquete simplemente desaparece sin ningún tipo de indicación al sistema o aplicación de origen, de que fue descartado en el sistema de destino. Esto se refleja en el sistema que envía el paquete a menudo, como un *communication timeout* (alcance del máximo tiempo de espera en la comunicación), lo que puede causar confusión, aunque el descarte de paquetes entrantes no deseados se considera a veces una buena política de seguridad, pues no da ni siquiera el indicio a un posible atacante de que el sistema destino existe.

- QUEUE (encolar): este destino hace que el paquete sea enviado a una cola en el espacio de usuario. Una aplicación puede usar la biblioteca libipq, también parte del proyecto netfilter/iptables, para alterar el paquete. Si no hay ninguna aplicación que lea la cola, este destino es equivalente a DROP.

- RETURN (retorno): hace que el paquete en cuestión deje de circular por la cadena en cuya regla se ejecutó el destino RETURN. Si dicha cadena es parte de otra, el paquete continuará por la cadena superior como si nada hubiera pasado. Si por el contrario la cadena es una cadena principal (por ejemplo la cadena INPUT), al paquete se le aplicará la política por defecto de la cadena en cuestión (ACCEPT, DROP o similar).

Hay muchos destinos de extensión disponibles. Algunos de los más comunes son:

- REJECT (rechazo): este destino tiene el mismo efecto que 'DROP', salvo que envía un paquete de error a quien envió originalmente. Se usa principalmente en las cadenas de ENTRADA y de REDIRECCIÓN de la tabla de filtrado. El tipo de paquete se puede controlar a través del parámetro '*--reject-with*'. Un paquete de rechazo puede indicar explícitamente que la conexión ha sido filtrada (un paquete ICMP filtrado administrativamente por conexión), aunque la mayoría de los usuarios prefieren que el paquete indique simplemente que la computadora no acepta ese tipo de conexión (tal paquete será un paquete *tcp-reset* para conexiones TCP denegadas, un *icmp-port-unreachable* para sesiones UDP denegadas o un *icmp-protocol-unreachable* para paquetes no TCP y no UDP).

- LOG (bitácora): este destino lleva un log o bitácora del paquete. Puede usarse en cualquier cadena en cualquier tabla, y muchas veces se usa para análisis de fallos.

- ULOG: este destino lleva un *log* o bitácora del paquete, pero no de la misma manera que el destino LOG. El destino LOG le envía información al log del núcleo, pero ULOG hace multidifusión de los paquetes que coincidan con esta regla a través de un *socket* netlink, de manera que programas del espacio de usuario puedan recibir este paquete conectándose al *socket*.

- DNAT: este destino hace que la dirección (y opcionalmente el puerto) de destino del paquete sean reescritos para traducción de dirección de red.

Mediante la opción '*--to-destination*' debe indicarse el destino a usar. Esto es válido solamente en las cadenas de SALIDA y PRERUTEO dentro de la tabla de *nat*.

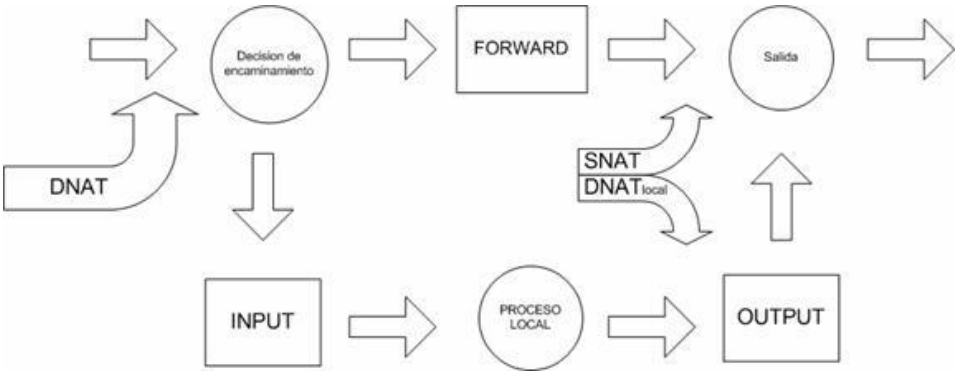
- SNAT: este destino hace que la dirección (y opcionalmente el puerto) de origen del paquete sean reescritos para traducción de dirección de red. Mediante la opción '*--to-source*' debe indicarse el origen a usar. Esto es válido solamente en la cadena de POSRUTEO dentro de la tabla de *nat* y, como DNAT, se recuerda para todos los paquetes que pertenecen a la misma conexión.

- MASQUERADE: esta es una forma especial, restringida de SNAT para direcciones IP dinámicas, como las que proveen la mayoría de los proveedores de servicios de Internet (ISP) para *módems* o línea de abonado digital (DSL). En vez de cambiar la regla de SNAT cada vez que la dirección IP cambia, se calcula la dirección IP de origen a la cual hacer NAT fijándose en la dirección IP de la interfaz de salida cuando un paquete coincide con esta regla. Adicionalmente, recuerda cuales conexiones usan MASQUERADE y si la dirección de la interfaz cambia, todas las conexiones que hacen NAT a la dirección vieja se olvidan.

1.4.3.4. Diagrama iptables

Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete y tiene que decidir qué hacer con él. El kernel lo que hace es, dependiendo si el paquete es para la propia máquina o para otra, consultar las reglas del firewall y decidir qué hacer con el paquete.

Figura 12. **Dirección de un paquete que llega al kernel con iptables**



Fuente: http://www.pello.info/filez/firewall/iptables.html. Consulta: 8 de marzo de 2012.

2. INVESTIGACIÓN PRELIMINAR

2.1. Reseña historia del SAE/SAP

Desde octubre de 1997 se creó la unidad académica de Servicio de Apoyo al Estudiante (SAE) y de Servicio de Apoyo al Profesor (SAP), llamada por sus siglas SAE-SAP y con el aval de Junta directiva de la Facultad de Ingeniería y posteriormente del Consejo Superior Universitario, ha venido ejecutando el presente proyecto de prestación de servicios de capacitación en el área de informática con el objetivo primordial de fortalecer a esta unidad y generar recursos para su sostenibilidad. Este proyecto ha permitido también contribuir a apoyar de manera significativa la actividad académica que se ha prestado a usuarios clasificados de la siguiente manera:

- Usuario TIPO A: estudiantes, catedráticos, investigadores y personal administrativo de la Facultad de Ingeniería.

- Usuario TIPO B: estudiantes, catedráticos, investigadores y personal administrativo de otras facultades.

- Usuario TIPO C: sector externo a la USAC:
    - OG's
    - ONG's
    - Organismos internacionales
    - Industria privada
    - O cualquier organización externa a la USAC

En julio de 2006, aprovechando el inicio de una nueva administración, después de evaluar lo actuado y analizar las fortalezas y debilidades de los procedimientos utilizados a la fecha, consideramos ideal el poder retroalimentar el presente proyecto e iniciar acciones que permitan darle mejor eficiencia a los servicios que el SAE/SAP ofrece, utilizando la infraestructura legal que la misma Universidad pone a disposición de las unidades académicas.

2.2. Servicios que presta el SAE/SAP

Los servicios que presta el departamento SAE/SAP a los usuarios son los siguientes:

- Préstamo gratuito de equipo con servicio de Internet y servicio de uso de programas de ofimática (Word, Excel, PowerPoint, Access), diseño asistido por computadora para dibujo en dos y tres dimensiones (Autocad), programas para el análisis y diseño de edificios (Etabs), y otros.

- Se imparten cursos como Excel, PowerPoint, Access, Word, Visio, WinQSB, Project, Autocad, etc. En su mayoría los usuarios pertenecen a la comunidad de ingenieril de la Usac, como requisito y parte de su formación profesional de las diferentes carreras de la facultad de ingeniería.

- Se realizan capacitaciones a personal administrativo de las diferentes unidades académicas de la Universidad de San Carlos de Guatemala.

- Se realizan capacitaciones a todo nivel para estudiantes de colegios e institutos así como para otras universidades del país.

- Capacitación a estudiantes de la carrera de Ingeniería en Sistemas en temas afines a su carrera.

- Se sirve como laboratorios para los cursos de la carrera de Ingeniería en Sistemas, para los cursos de Introducción a la programación 1 e Introducción a la programación 2.

- Se ofrecen cursos de lenguaje de programación (Java, Microsoft .NET), cursos de ingeniería de software (ISE, SQM, SA).

2.3. Laboratorios

El departamento SAE/SAP cuenta con varios laboratorios distribuidos en los diferentes niveles del edificio T-3 de la facultad de ingeniería, siendo éstos los siguientes:

- Laboratorio de Geomática, ubicado en el primer nivel del edificio T-3 que cuenta con 30 equipos de cómputo para impartir cursos o capacitación de usuarios.

- Laboratorio Plaza Korea ubicado en el segundo nivel del edificio T-3 con 20 equipos disponibles. Este laboratorio es de uso exclusivo para préstamo gratuito de equipos con acceso a internet y uso de programas como Word, Access, Autocad, etc.

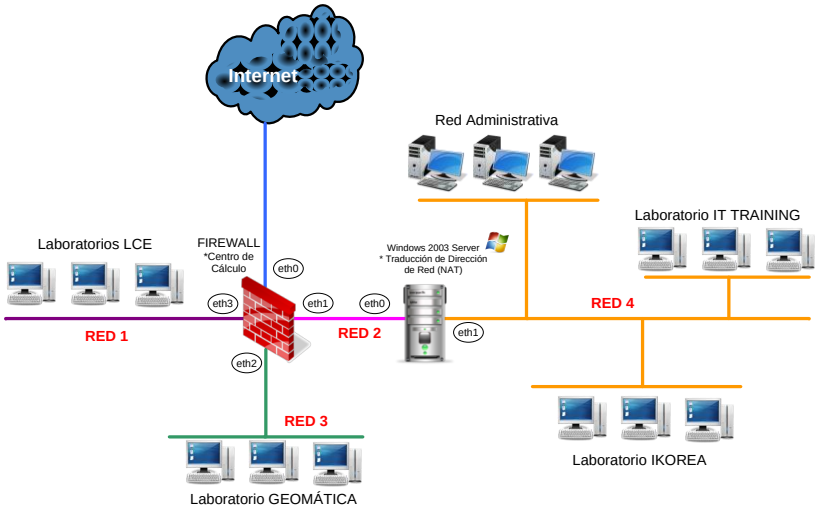
- Laboratorio IT Training, ubicado también en el segundo nivel del edificio T-3 con 25 equipos disponibles. Utilizado para impartir cursos o capacitación de usuarios.

- Laboratorios LCE (Laboratorio de Cómputo Estudiantil) ubicados en el tercer nivel del edificio T-3. Estos a su vez se dividen en dos laboratorios, LCE 301 y LCE 302 correspondientes al salón 301 y 302 respectivamente. Cada laboratorio cuenta con 35 equipos de cómputo para impartir cursos o capacitación de usuarios.

- Laboratorio del cuarto nivel del edificio T-3 que cuenta con 18 equipos de cómputo para impartir cursos o capacitación de usuarios.

- Laboratorios ITCoE ubicados también en el cuarto nivel del edificio T-3, distribuidos en 3 laboratorios con 20 equipos disponibles cada uno.

Figura 13. **Diseño actual de red del departamento SAE/SAP**



Fuente: elaboración propia.

3. FASE DE ANÁLISIS

3.1. Determinación de requerimientos

Involucra las actividades encaminadas a obtener las características necesarias que deberá poseer nuestro nuevo sistema de red, para comprender cómo trabaja y dónde es necesario efectuar mejoras en la implementación. Se destacan tres fases:

- Anticipación de requerimientos
- Investigación de requerimientos
- Especificación de requerimientos

3.1.1. Anticipación de requerimientos

Se han previsto algunas características que deben reunir el diseño e implementación del nuevo sistema de red para los laboratorios del SAE/SAP.

3.1.1.1. Escalabilidad

Es de suma importancia que el diseño del sistema de red pueda ofrecer la habilidad de extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

En base a información obtenida dentro de la Facultad de Ingeniería se sabe que el departamento SAE/SAP empezó a funcionar con un área administrativa y un solo laboratorio con aproximadamente 20 equipos de cómputo. Sin embargo, en la actualidad cuenta con aproximadamente 8 laboratorios y aproximadamente 190 equipos de cómputo. Además, que se han agregado otros servicios que en sus inicios no estaban contemplados, como el ofrecer servicio de internet gratuito a sus usuarios, o el servicio de red inalámbrica del departamento.

3.1.1.2. Compatibilidad de Hardware y Software

Otro factor a tomar en cuenta es la compatibilidad de hardware y software en la implementación del nuevo sistema de red, ya que tanto los protocolos de red, los sistemas operativos y las aplicaciones se deben ajustar a la naturaleza de los servicios que presta actualmente el departamento SAE/SAP a todos sus usuarios.

3.1.1.3. Costo implementación

Se hará uso de todos los recursos disponibles tanto de hardware como de software con los que cuenta el departamento SAE/SAP, es decir, equipos de trabajos, servidores, *switch*, *hub*, *rack*, *Access point*, licencias de sistemas operativos, licencias de software de aplicaciones, licencias de antivirus, etc., con la finalidad de optimizar todos los recursos que tengamos a la mano y evitar al mínimo generar costos de implementación.

3.1.2. Investigación de requerimientos

Para poder brindar una solución que satisfagan las necesidades de la institución, se toman en cuenta dos métodos para captación de información:

- Entrevistas
- Observación

3.1.2.1. Método de entrevista

Se hizo uso de la entrevista a 5 encargados de los diferentes laboratorios de la institución para obtención de información. Las entrevistas se realizaron en horario de labores del personal y en un lapso de tiempo no mayor a 30 minutos.

El modelo de la entrevista realizada a los encargados del departamento SAE/SAP fue el siguiente:

- ¿Los laboratorios se encuentran dentro de un mismo segmento de red?
- ¿La red administrativa y la red de laboratorios se encuentran en segmentos de redes diferentes?
- ¿Qué tipo de sistema operativo utilizan los equipos?
- ¿Cuentan con el uso de servidores dentro de los laboratorios?
- ¿Cuentan con software de antivirus?

- ¿Mencione al menos 3 problemas recurrentes que considere que impidan ofrecer un buen servicio a los usuarios?

- ¿Tienen políticas para el control de usuarios y recursos dentro de la red actual?

- ¿La configuración de las direcciones IP de red de los equipos se realiza de forma manual o dinámica?

- ¿Qué servicios pretende ofrecer en un futuro inmediato el departamento SAE/SAP?

- ¿Cuenta con algún sistema de firewall dentro de los laboratorios?

3.1.2.2. Método de observación

La observación se realizó durante una semana en un horario de 7:00 a 20:00 horas, tomando en cuenta la afluencia de los usuarios a los laboratorios, el tipo de servicio que requerían, el rol de los encargados y tipo recurrente de problemas al cual el usuario estaba expuesto.

Se tomó de muestra el laboratorio PLAZA KOREA ubicado en el segundo nivel del edificio T-3 de la facultad de ingeniería, debido a que es el laboratorio con más afluencia de usuarios.

3.1.2.3. Resultados obtenidos

A continuación, basándose en la información obtenida mediante el método de entrevista realizado al personal encargado de la administración de los laboratorios SAE/SAP, se obtuvieron las siguientes respuestas.

3.1.2.3.1. Entrevistas

Resultados obtenidos en la pregunta: ¿Los laboratorios se encuentran dentro de un mismo segmento de red?

- Todos los entrevistados respondieron que los laboratorios se encuentran en redes diferentes.

Resultados obtenidos en la pregunta: ¿La red administrativa y la red de laboratorios se encuentran en segmentos de redes diferentes?

- Se constató que la red de equipos administrativos se encuentra en la misma red que los equipos del laboratorio Plaza Korea.

Resultados obtenidos en la pregunta: ¿Qué tipo de sistema operativo utilizan los equipos?

- Todos los entrevistados coincidieron que el sistema operativo utilizado dentro de los laboratorios es la plataforma Microsoft Windows.

Resultados obtenidos en la pregunta: ¿Cuentan con el uso de servidores dentro de los laboratorios?

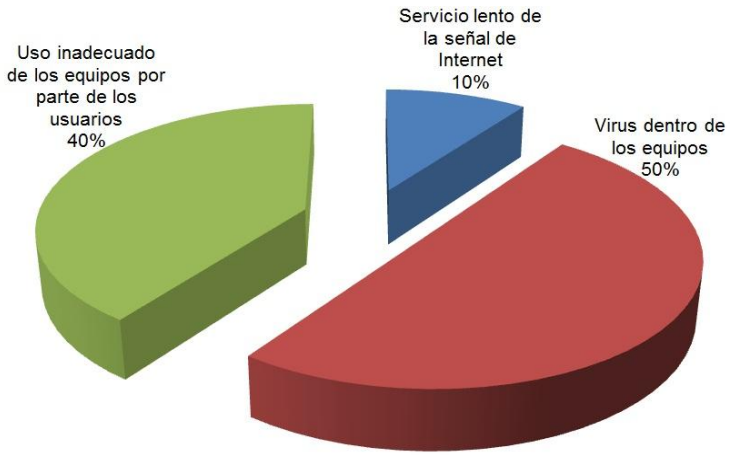
- Los entrevistados respondieron que tienen instalado un servidor Windows 2003 en el laboratorio Plaza Korea, que realiza la traducción de direcciones de red (NAT) el cuál es un mecanismo utilizado para intercambiar paquetes entre redes diferentes (configurado para poder tener acceso a Internet). Los demás laboratorios tienen acceso a Internet directamente.

Resultados obtenidos en la pregunta: ¿Cuentan con software de antivirus?

- Si cuentan con software antivirus, específicamente Avast en su versión gratuita.

Resultados obtenidos en la pregunta: ¿Mencione al menos 3 problemas recurrentes que considere que impidan ofrecer un buen servicio a los usuarios?

Figura 14. **Problemas relevantes con el servicio de los laboratorios**



Fuente: elaboración propia.

- Tabulando los datos obtenidos de la pregunta anterior, se determinó tres problemas recurrentes y relevantes:

    - Se estableció que el 50 por ciento de los problemas con los equipos corresponden a la infección de virus dentro los sistemas de cómputo que corrompen archivos del sistema y de aplicaciones.

    - Un 40 por ciento al uso inadecuado de los equipos, por ejemplo: acceso y daño a los archivos del sistema Windows, desinstalación de programas, instalación de programas y configuración del equipo sin autorización de los encargados (cambio de dirección de red de las interfaces de red, des habilitación de la interfaz de red, cambio de configuraciones de los navegadores, eliminación de archivos, etc.).

    - Y un 10 por ciento a problemas con la señal de Internet.

Resultados obtenidos en la pregunta: ¿Tienen políticas para el control de usuarios y recursos dentro de la red actual?

- Mencionaron que no hay ninguna política de control de usuarios y recursos de la red.

Resultados obtenidos en la pregunta: ¿La configuración de las direcciones IP de red de los equipos se realiza de forma manual o dinámica?

- La configuración de las direcciones de red de las interfaces de red se realizan manualmente.

Resultados obtenidos en la pregunta: ¿Qué servicios pretende ofrecer en un futuro inmediato el departamento SAE/SAP?

- Implementación de un servidor Web para la realización de los exámenes de computación para ingresar a la facultad de ingeniería.

Resultados obtenidos en la pregunta: ¿Cuenta con algún sistema de firewall dentro de los laboratorios?

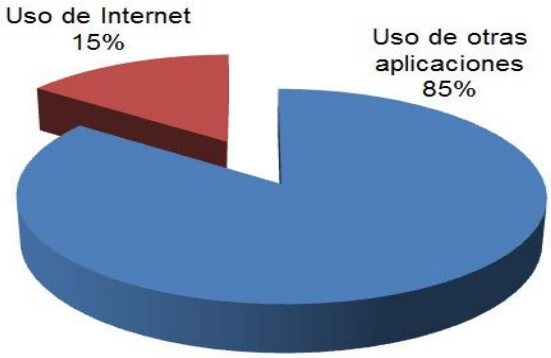
- No, no hay ningún firewall instalado en los laboratorios.

3.1.2.3.2. Observaciones

- En promedio se atienden a 245 usuarios por día en el laboratorio Plaza Korea, tomando de referencia la asignación de 1 hora por usuario en horario de 7:00 a 19:00 horas en los 20 equipos de cómputo disponibles.

- El 85 por ciento del servicio requerido es el uso de Internet, mientras que el 15 por ciento es utilizado para uso de otras aplicaciones como Word, PowerPoint, AutoCad, Access, etc.

Figura 15. **Porcentaje de uso de tipo de servicio Plaza Korea**



Fuente: elaboración propia.

- El 85 por ciento de los usuarios pertenecen a la Facultad de Ingeniería, el 10 por ciento a otras unidades académicas de la Universidad de San Carlos y un 5 por ciento a usuarios externos a la universidad como estudiantes o profesores de nivel medio.

Figura 16. **Tipo de usuarios que utilizan servicios en la Plaza Korea**

Fuente: elaboración propia.

3.1.3. Especificación de requerimientos

En base a la recopilación de la información de datos mediante la observación y las entrevistas realizadas al personal de los laboratorios, se describen las características que nuestro nuevo sistema de red debe proveer:

3.1.3.1. Administración simplificada de usuarios y recursos

Creación de un Servidor de Directorio para la creación de usuarios, grupos de usuario, equipos, grupos de equipos, delegación de permisos, delegación de servicios que puedan permitir la administración centralizada de todos los recursos de la red entre los diferentes laboratorios.

Mediante el uso del servicio de Directivo Activo de Windows 2003 Server podremos almacenar la información de los recursos de la red para hacer más fácil la accesibilidad a las aplicaciones, el hardware y los usuarios. Con este esquema de implementación la escalabilidad no es un problema debido a que los dominios tienen un límite claro de hasta 40 000 objetos. Un factor a tomar en cuenta sería el ancho de banda que se proporcione a la institución por el departamento de redes de la facultad de ingeniería.

3.1.3.2. Control sobre usuarios

Creación de políticas de grupo (GPO) que definirán las configuraciones sobre usuarios y grupos de usuarios. Actualmente los usuarios que se utilizan dentro de los laboratorios cuentan con permisos de administrador, cuenta que por defecto crea Windows a sus usuarios.

El usuario tipo administrador tiene todo el control sobre el sistema operativo, es decir, tiene permisos para ver, ejecutar, instalar y borrar todo sin ningún tipo de restricción.

Algunas ventajas de utilizar usuarios limitados o no administradores se describen a continuación:

- Evitar que algún virus o archivo infectado dentro del equipo o de la red tenga el control total sobre el sistema operativo de un usuario que esté utilizando cuenta de administrador.

- Evitar que personas por descuido o malintencionadas modifiquen, borren, instalen o desinstalen aplicaciones de software.

- Evitar que los usuarios modifiquen las configuraciones de hardware como cambio de direcciones IP o deshabilitar interfaces de red, cambio de idioma de teclado, deshabilitar dispositivos de audio, etc.

También se crearán políticas para delegar el uso de recursos o servicios a determinados usuarios. Por ejemplo: usuarios que por la naturaleza del servicio requieran acceso a Internet, uso de impresora, uso de carpeta específica o aplicación.

3.1.3.3. Instalación de aplicaciones

Actualmente la institución cuenta con aproximadamente 190 equipos de cómputo, sin embargo, esta cifra podría aumentar. A medida que aumenta la cantidad de equipos la administración de los mismos se volverá más difícil sino

se cuentan con políticas adecuadas para el mantenimiento, configuración e instalación de aplicaciones.

Como solución a lo expuesto anteriormente, se instalará un servidor de DHCP para la administración de y configuración de direcciones de red de forma dinámica dentro de los equipos. Algunas ventajas que nos ofrece este servicio son:

- Una configuración segura y fiable de direcciones IP, que evita los errores de configuración que se provocan por la necesidad de escribir valores manualmente en cada equipo.

- Evita los conflictos de direcciones que causan las direcciones IP previamente asignadas que se utilizan para configurar un equipo nuevo en la red.

- Reduce significativamente el tiempo necesario para configurar y reconfigurar los equipos de la red.

- Utilización de reservas IP para equipos que por alguna razón necesiten que se les asigne la misma dirección de red, como por ejemplo los equipos de la Plaza Korea, los cuales utilizan el programa Ghetto para control de tiempo de los usuarios.

Con relación a las aplicaciones del sistema operativo, se crearán directivas de grupo para la administración de instalación de software, plantillas administrativas, redirección de carpetas, configuración de seguridad, secuencia de comando y mantenimiento de navegadores Web, entre otros.

3.1.3.4. Implementar políticas para la seguridad de la red

En base a la información suministrada por el personal de la institución y mediante la observación se pudo determinar lo siguiente:

- Los laboratorios de la institución se encuentran en segmentos de red diferente (no pueden compartir recursos de entre ellos).

- La red administrativa se encuentra en la misma red que los equipos de los laboratorios de Plaza Korea e IT Training, lo cual en ningún caso es recomendable por razones de seguridad. Los equipos de la red administrativa contienen información de suma importancia para la institución, como por ejemplo: almacenamiento de notas de cursos, información financiera, datos personales de los trabajadores, exámenes para las pruebas específicas de computación, etc.

- Como se mencionó anteriormente, los usuarios de los laboratorios trabajan con una cuenta administrador, delegando todo el control del sistema operativo.

- A corto plazo se pretende implementar un Servidor Web, para la realización de las pruebas específicas de computación.

Las estrategias a utilizar son las siguientes:

- Colocar los laboratorios dentro de un mismo segmento de red. Con la ayuda del administrador de red de la facultad de ingeniería, reconfigurar la red de área local virtual (VLAN), debido a que en realidad las redes de

los laboratorios están separadas lógicamente dentro de una misma red física.

- Instalar un Servidor Windows 2003 con el servicio de Directorio Activo dentro de la red de los laboratorios. Esto nos proporcionará la creación, el control, delegación de permisos o servicios a usuarios, administración de la configuración de equipos, permisos sobre carpetas, aplicaciones, etc.

- Separar la red administrativa de la red de los laboratorios. Se implementará un firewall de software que administre el tráfico de paquetes entre los distintos segmentos de la red. El sistema operativo a utilizar será una distribución de Linux, más específicamente Ubuntu Server en su versión 11.10. Nuestro firewall a implementar tendrá las siguientes características:

    - El equipo firewall tendrá 3 interfaces de red. Una interfaz que tendrá comunicación con la red de laboratorios, la otra tendrá comunicación con la red administrativa y la última comunicación con la red perimetral o zona desmilitarizada (DMZ, demilitarized zone).

    - Se configurará iptables que es el componente más popular construido sobre netfilter el cual es un framework disponible en el núcleo de Linux que nos permite interceptar y manipular paquetes de red en nuestro servidor firewall.

    - La zona desmilitarizada o DMZ (demilitarized zone), es una red local que se encuentra entre la red interna (red administrativa) de la organización y la red externa (red de laboratorios e Internet). En

esta red se colocarán los servidores Web, de correo electrónico o de base de datos, los cuales ofrecen servicio tanto a la red exterior como a la red interior.

- Las conexiones de la red interna (administrativa) están permitidas para el exterior (Internet).

- Las conexiones de red interna hacia la zona desmilitarizada están permitidas.

- Las conexiones de red externa hacia la zona desmilitarizada están permitidas.

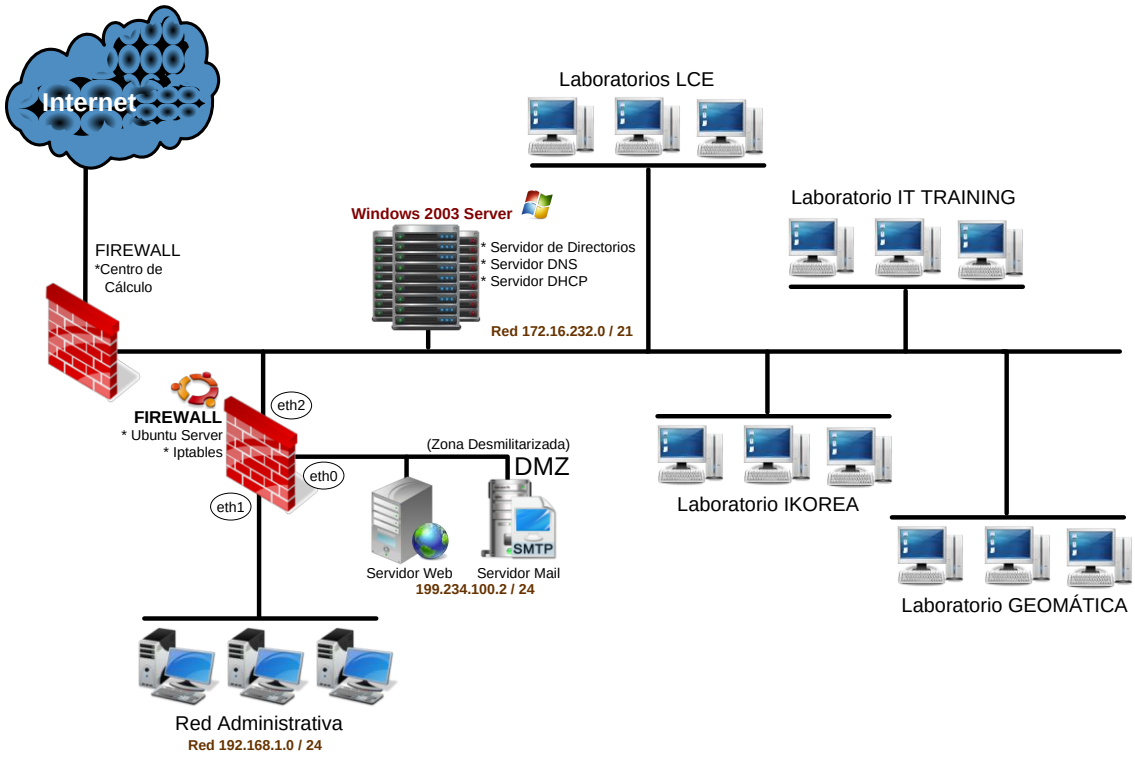
- Las conexiones de la red externa hacia la red administrativa no están permitidas.

El objetivo principal es que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

4. FASE DE DISEÑO

Con base a los requerimientos planteados anteriormente, se presenta a continuación el diseño del sistema de red de los laboratorios SAE/SAP que cubre las necesidades que se determinaron en la fase de análisis.

Figura 17. **Diseño del sistema de red propuesto como solución al Departamento SAE/SAP**



Fuente: elaboración propia.

4.1. Descripción de los elementos del diseño

- El sistema contará con tres segmentos de red, una red para los laboratorios, una red para la zona desmilitarizada y la red administrativa respectivamente.

- Dentro de la red de laboratorios se instalará un único servidor proporcionando los servicios de Directorio Activo, DHCP y DNS. El sistema operativo del servidor es un Windows Server 2003 Enterprise Edition.

- Mediante la instalación y configuración del Directorio Activo del Servidor de la red de laboratorios se administrará la creación, modificación, eliminación, configuración y asignación de permisos sobre los recursos de la red (estos pueden ser usuarios, equipos, carpetas, archivos, etc.).

- Se creará un dominio con el nombre de saesap.ingenieria.usac.edu.gt que constituirá un límite de seguridad para todos los equipos dentro de la red de laboratorios.

- Se crearán políticas de grupo a unidades organizativas dentro del dominio del Directorio Activo.

- La asignación de direcciones IP de las interfaces de red se realizará dinámicamente por medio del servicio DHCP instalado y configurado en el servidor.

- Se utilizarán reservas IP para equipos que por la función de su servicio requieran la misma dirección IP, como por ejemplo los equipos de la

Plaza Korea que utilizan un programa de control de tiempo. Este servicio también es proporcionado por el DHCP.

- Se instalará un equipo con el sistema operativo Ubuntu Server versión 11.04 y se configurarán los IPTABLES que controlarán el tráfico de red.

- El Servidor Ubuntu Server también servirá para separar la red de laboratorios, la red administrativa y la red de la zona desmilitarizada utilizando 3 interfaces de red una asignada a cada red respectivamente.

- En la red de laboratorios se ubicarán los equipos que prestarán servicios a los usuarios ajenos al personal de la institución.

- Dentro de la red administrativa se ubicarán todos los equipos del personal de la institución, como la administradora de la institución, secretarias, profesores, instructores y encargados de los laboratorios.

- En la red desmilitarizada o DMZ se ubicarán los servidores que proporcionarán servicios tanto a usuarios externos como usuarios internos. Los servicios que comúnmente se encuentran en esta área son los de Servidor Web, Servidor de Correo o Servidor de Base de Datos. Es importante mencionar que actualmente no se cuenta con ninguno de éstos servicios, sin embargo, como parte de la solución del proyecto se dejó implementada ésta característica en el sistema.

4.2. Diseño de plan de dominio

Los servidores donde se ejecuta Windows 2003 que contienen una base de datos con los objetos del dominio y que realizan la función de autenticación se denominan controladores de dominio. Las siguientes son algunas consideraciones a tomarse en cuenta para el diseño de la estructura de dominios:

- Alcance de la administración y políticas: cada dominio tiene un grupo de administradores de dominio. Los administradores de dominio tienen el control total sobre cada objeto del dominio y estos derechos sólo son válidos dentro del dominio y no se propagan a otros dominios. Así también la Política de grupo (Group Policy Object, GPO) asociada con un dominio no se propaga automáticamente a otros dominios del bosque.

- Capacidad de la base de datos SAM (Administración de Cuentas de Seguridad): en versiones anteriores de Microsoft Windows NT Server, la base de datos SAM tenía una limitación práctica de aproximadamente 40,000 objetos por dominio. El Directorio Activo puede llegar a usar fácilmente millones de objetos por dominio.

- Diferenciar los nombres de dominio de la Internet y de la Intranet: si la organización SAE/SAP decide denominar a un dominio en la Intranet como saesap.ingenieria.usac.edu.gt, no debería crear un dominio en Internet que también se llame saesap.ingenieria.usac.edu.gt, ya que si un usuario de saesap.ingenieria.usac.edu.gt se conecta a la Intranet y a la Internet a la vez, seleccionaría el dominio que conteste primero durante la búsqueda del sitio.

Para determinar el esquema de dominios que mejor se ajuste a los requerimientos de SAE/SAP, es necesario recordar que entre las necesidades de la institución está el manejar un entorno centralizado con configuraciones homogéneas a lo largo de toda la red.

Así también las tareas de administración deben ser sencillas (cada dominio adicional supone una carga administrativa). Por lo tanto, se ha definido implementar un esquema de un solo dominio el cuál consolidará todos los recursos y cuentas de usuario del negocio.

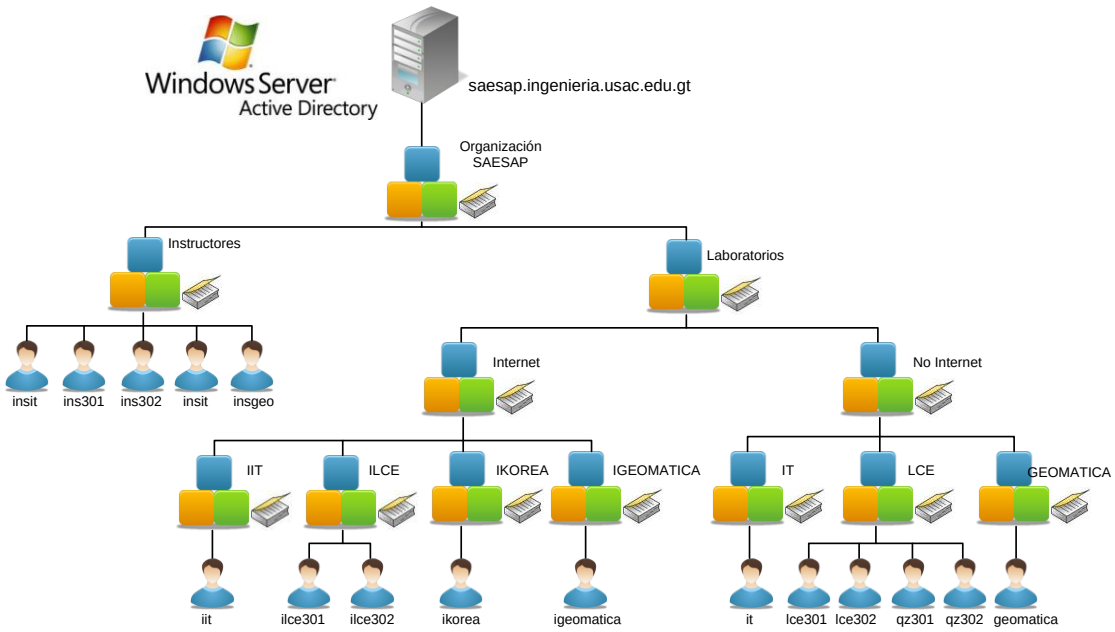
En relación al nombre de dominio se creará con el nombre de saesap.ingenieria.usac.edu.gt sin ningún problema debido a que Internet se encuentra el nombre saesap.ingenieria-usac.edu.gt.

4.3. Diseño del plan de unidades organizativas

De acuerdo a las necesidades de la organización y a los recursos de los cuales se dispone, se ha considerada como la estructura más adecuada, una estructura compuesta de varios niveles, la misma que está orientada a facilitar la administración y aplicación de políticas.

Se ha definido implementar un esquema de unidades organizativas basada en funciones de trabajo de la organización sin importar la ubicación geográfica.

Figura 18. **Diseño de unidades organizativas**



Fuente: elaboración propia.

4.4. Diseño del plan de políticas

Se ha definido implementar una plantilla básica de políticas orientadas especialmente al control de usuarios. Se ha identificado claramente 4 tipos de usuarios dependiendo de su función, pero podrían ser más. Se muestran algunas políticas en la tabla adjunta que se consideran de mayor importancia para administrar de forma correcta los recursos de la red.

Tabla I. **Clasificación de usuarios SAE/SAP según su función**

Usuario	**Panel de Control**	**Acceso Internet**	**Instalar Programas**	**Acceso a MS-DOS**	**Acceso a Quiz4Win**
Instructor	✓	✓	✓	✓	**X**
Internet	**X**	✓	**X**	**X**	**X**
No Internet	**X**	**X**	**X**	**X**	**X**
Examen Computación	**X**	**X**	**X**	**X**	✓

Fuente: elaboración propia.

4.5. Diseño del servicio DHCP

Se implementará un servidor DHCP dentro de la institución para asignar direcciones IP a las interfaces de red de los equipos de los laboratorios.

En lo referente a los rangos de exclusión se ha definido excluir únicamente las direcciones 172.16.232.1 a la 172.16.232.19 con máscara 21, para equipos dedicados como servidores o cámaras de seguridad.

Se ha considerado utilizar reservas de direcciones IP para los equipos del laboratorio KOREA, por la razón que éstos hacen uso de un programa especial para control de tiempo de usuario sobre los equipos, y es necesario asignarles la misma dirección IP a las interfaces de red.

4.6. Diseño de la zona desmilitarizada

Se implementará una zona desmilitarizada o DMZ por sus siglas en inglés, que será una zona entre la red de laboratorios y la red administrativa. En esta zona se encuentran generalmente los servidores *Web,* de base de datos o de correo electrónico. Actualmente la institución no cuenta con éstos servicios, sin embargo, se dejará prevista.

La creación de la DMZ será posible mediante la implementación de un firewall que será un equipo de cómputo normal con las siguientes características:

- Sistema operativo: Ubuntu Server versión 11.04
- Red: 3 interfaces (red laboratorios, red administrativa y DMZ)
- Configuración de IPTABLES (administración del tráfico de paquetes entre redes)

4.7. Elementos disponibles para el funcionamiento del sistema

Se realizó un inventario de todos los recursos disponibles y necesarios para la implementación del sistema mediante una clasificación de los elementos tanto de hardware, software e infraestructura de red.

4.7.1. Hardware

Hardware, corresponde a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

4.7.1.1. Servidores

- Servidor Microsoft Windows Server 2003 Enterprise Edition
  - Equipo: computadora marca DELL modelo PowerEdge 2950
  - Procesador: Intel Xeon doble núcleo de 3.0 GHZ
  - Memoria: 4 GB
  - Disco duro: 500 GB
  - Unidad: quemadora de DVD

- Ubuntu Server 11.04
  - Equipo: computadora marca COMPAQ
  - Procesador: *Pentium* 4 de 2.0 *GHZ*
  - Memoria: 1 GB
  - Disco duro: 40 GB
  - Unidad óptica: CD-ROM de 52X

4.7.1.2. Estaciones de trabajo

Son todos los equipos de cómputo utilizados dentro del departamento SAE/SAP. En una red de computadoras, es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red.

- Microsoft Windows XP Professional Edition
    - Procesador: Intel Core 2 Duo
    - Memoria: 1 GB
    - Disco duro: 80 GB
    - Dispositivos ópticos: Grabadora de CD

4.7.1.3. Estructura de red

Se refiere a la organización e interconexión entre grupos de ordenadores y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información.

- Todas las terminales y los servidores deberán contar con tarjetas de red 10/100, un cableado estructurado UTP categoría 5 y conectores RJ-45.

- *Switch* de 16 puertos 10/100 base T o superior.

4.7.2. Software

Se refiere al equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

4.7.2.1. Software propietario

Es cualquier programa informático en el que el usuario final tiene limitaciones para usarlo, modificarlo o distribuirlo, o cuyo código fuente no está disponible por un acuerdo de licencia.

- Software requerido
    - Microsoft Windows Server 2003 Enterprise Edition (para servidor)
    - Microsoft Windows XP Professional Edition (para estaciones de trabajo)

- Software existente
    - Microsoft Windows Server 2003 Enterprise Edition
    - Microsoft Windows XP Professional Edition.

4.7.2.2. Software libre

Es cualquier programa de computación cuya licencia garantiza al usuario acceso al código fuente del programa y lo autoriza a ejecutarlo con cualquier propósito, modificarlo y redistribuir tanto el programa original como sus modificaciones.

- Software requerido
    - Sistema Operativo Ubuntu Server 11.04

- Software disponible
    - Sistema Operativo Ubuntu Server 11.04

5. IMPLEMENTACIÓN DEL DISEÑO

5.1. Servidor de Directorio

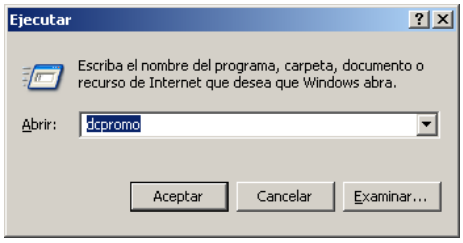
El servidor de directorio contiene una aplicación o conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de la red, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.

5.1.1. Instalación

Se procede a instalar el sistema operativo Microsoft Windows Server 2003 Enterprise Edition sobre el servidor DELL PowerEdge 2950, encargado de la organización y administración de los recursos de la red como de los usuarios.

- Se comienza haciendo clic en el menú inicio, elegir la opción ejecutar, digitar la palabra dcpromo y hacer clic en aceptar.

Figura 19. **Ventana comando ejecutar**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

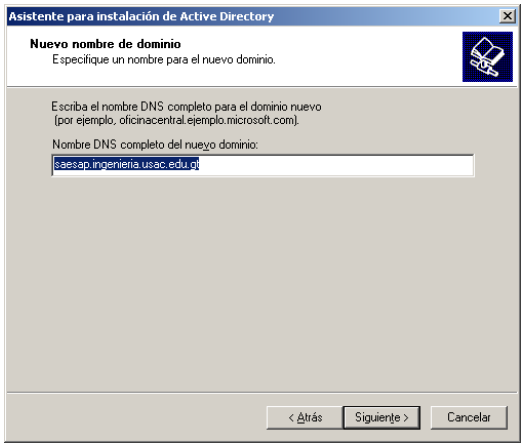
- Presionar clic en las siguientes dos pantallas que aparecen.

- Seleccionar controlador de dominio para un dominio nuevo y presionar siguiente.

- Seleccionar dominio en un nuevo bosque y presionar siguiente.

- En la siguiente pantalla se ingresa el nombre completo del dominio. En nuestro caso dejamos saesap.ingenieria.usac.edu.gt. En el nombre del BIOS colocar SAESAP.

Figura 20. **Asistente instalación Active Directory**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

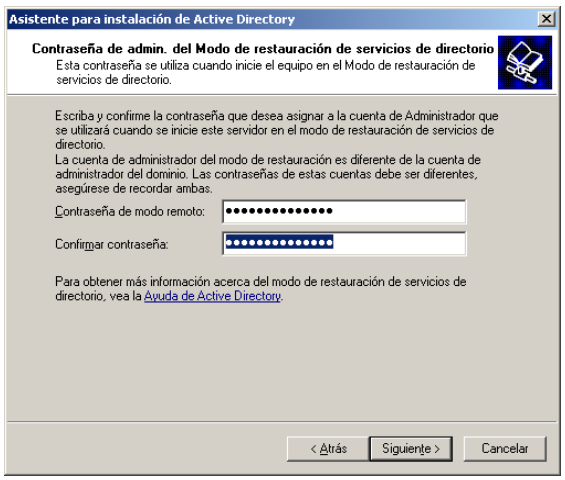
- Tanto las carpetas donde se almacenarán la base de datos, los registros del Active Directory y el volumen del sistema compartido las dejaremos con las direcciones que aparecen como predeterminadas.

- En este punto se debe tener configurada y activa al menos una interfaz de red con una dirección de red estática y presionamos la opción siguiente.

- Seleccionar la opción permisos compatibles sólo con sistemas operativos de servidor Windows 2000 o Windows Server 2003.

- Se colocará una contraseña a la cuenta Administrador que se utilizará únicamente cuando se inicie el servidor en modo de restauración de servicios de directorio (a esta opción se ingresa presionando la tecla F8 antes de cargue nuestro sistema operativo). Nota: La cuenta de administrador del modo de restauración es diferente de la cuenta de administrador de dominio.

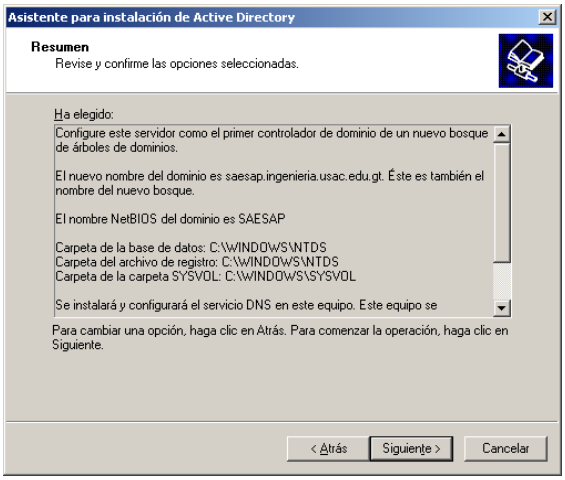
Figura 21. **Contraseña de administrador del modo de restauración**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Se muestra un resumen de la configuración de nuestro Active Directory antes de proceder a instalar.

Figura 22. **Resumen de la instalación de Active Directory**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.2. Creación de unidades organizativas

Se crean las unidades organizativas que son contenedores de Active Directory en los que se puede colocar usuarios, grupos, equipos y otras unidades organizativas.

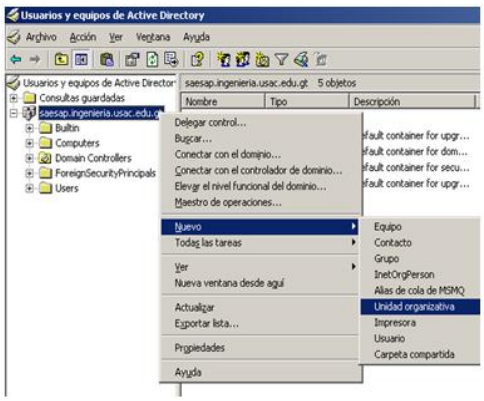
- Se procede abrir la opción usuarios y equipos de Active Directory seleccionando inicio, todos los programas, herramientas administrativas.

Figura 23. **Selección de usuarios y equipos de Active Directory**

Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Sobre el nombre del dominio presionar clic derecho, seleccionar la opción Nuevo y luego Unidad Organizativa. En la siguiente pantalla colocar el nombre de la unidad organizativa.

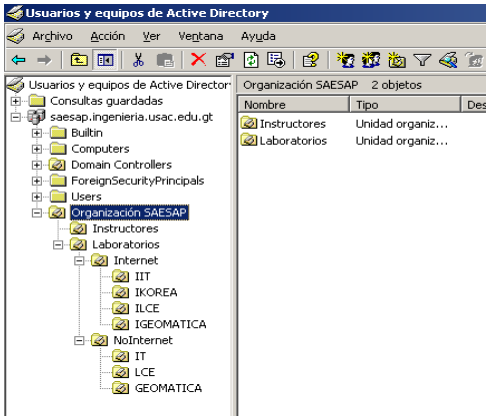
Figura 24. **Creación de unidad organizativa**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Se realizan los mismos pasos del inciso anterior para crear todas las unidades organizativas de la organización SAESAP.

Figura 25. **Resumen de unidades organizativas del SAE/SAP**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

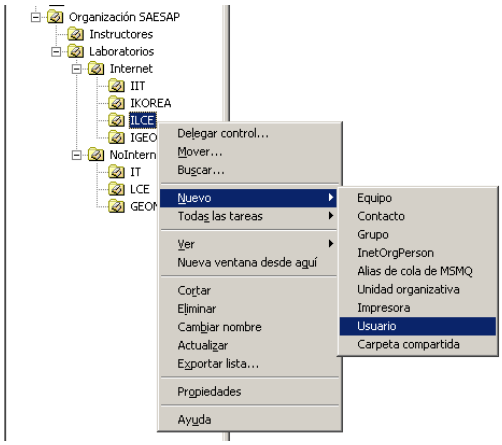
5.3. Usuarios del Servidor de Directorios

Son todos aquellos usuarios disponibles dentro del sistema que harán uso de los recursos y servicios provistos por el servidor de directorio en base a la función de cada usuario.

5.3.1. Creación de usuarios

- Se crea el usuario ilce301 dentro de ILCE. Clic derecho sobre ILCE, seleccionar Nuevo y a continuación la opción Usuario.

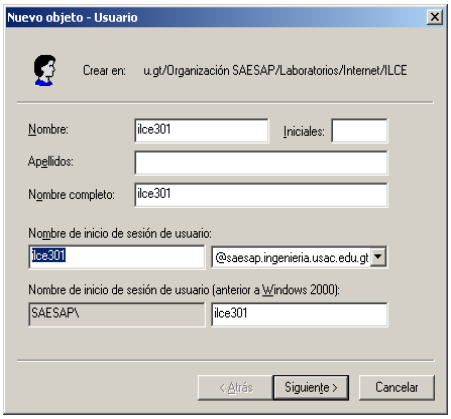
Figura 26. **Creación de usuario**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Ingrese la información relacionada al usuario y presione el botón siguiente.

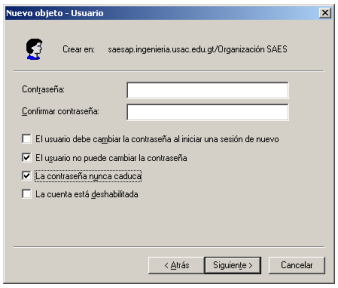
Figura 27. **Ingreso de información del usuario**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Se le pide ingresar la contraseña del usuario. Dejar la contraseña vacía y seleccionar las opciones para que el usuario no pueda cambiar la contraseña y que la contraseña nunca caduca. A continuación aparecerá una nueva pantalla y se presiona la opción finalizar.

Figura 28. **Ingreso y configuración de contraseña de usuario**

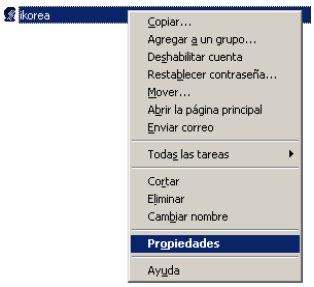


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.3.2. Inicio de sesión de usuarios por equipo

- Seleccionar el usuario elegido dentro de los usuarios del Active Directory, se presiona clic derecho sobre el mismo y se elige propiedades.

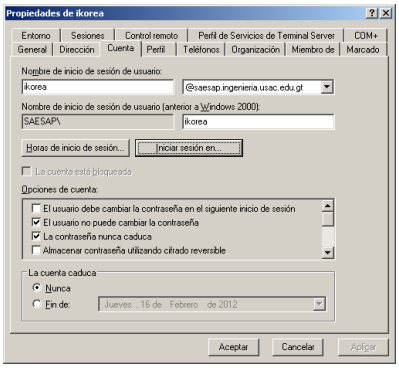
Figura 29. **Propiedades del usuario**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En la nueva ventana se selecciona la pestaña con la opción cuenta y se presiona el botón iniciar sesión en.

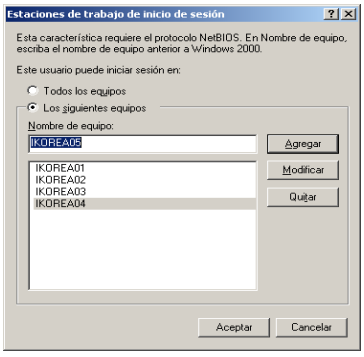
Figura 30. **Configuración de cuenta de usuario**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Se selecciona el o los equipos donde se permite que dicho usuario pueda iniciar su sesión como lo muestra la siguiente figura.

Figura 31. **Estaciones de trabajo de inicio de sesión**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.4. Políticas de grupo

Un objeto de directiva de grupo (Group Policy Object, GPO), es un conjunto de una o más políticas del sistema. Cada una de las políticas del sistema establece una configuración del objeto al que afecta. Por ejemplo, tenemos políticas para: establecer título de Internet, ocultar Panel de Control, ocultar Área de Notificaciones, deshabilitar el intérprete de comandos para DOS, etc.

5.4.1. GPMC

Para la administración de políticas de grupo se utilizará la herramienta denominada Consola de Administración de Directivas de grupo (GPMC) de Microsoft, que ayuda a los administradores a administrar la organización de una forma más rentable al mejorar la capacidad de administrar y aumentar la productividad.

5.4.1.1. Descarga e instalación GPMC

- Descargar el paquete de Windows Installer (.MSI) GPMC de la siguiente dirección: http://www.microsoft.com/downloads/es-es/details.aspx?familyid=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=es

- Se presiona doble clic en el paquete gpmc.msi y, a continuación, presionar clic en la opción siguiente.

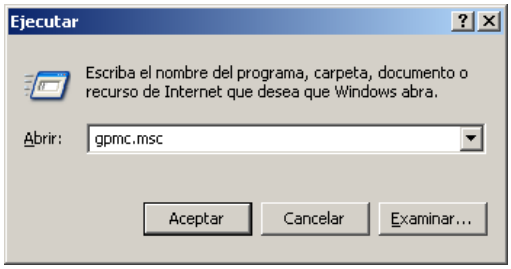
- Se selecciona la opción Acepto para aceptar el Contrato de licencia de usuario final y, a continuación, presionar clic en la opción siguiente.

- Se presiona clic en finalizar para completar la instalación de GPMC.

5.4.2. Crear políticas de grupo utilizando GPMC

- En la barra de tareas del escritorio de Windows seleccionar el menú inicio, elegir la opción ejecutar, escribir gpmc.msc y presionar aceptar.

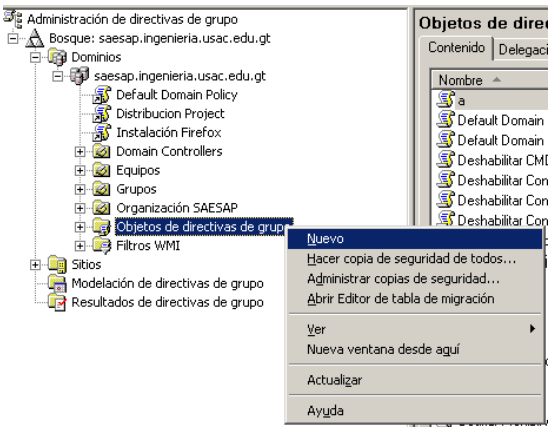
Figura 32. **Ejecutar consola de administración de directivas de grupo**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Elija el dominio, clic derecho sobre la opción Objetos de directiva de grupo, presione clic en Nuevo y asigne un nombre a la política.

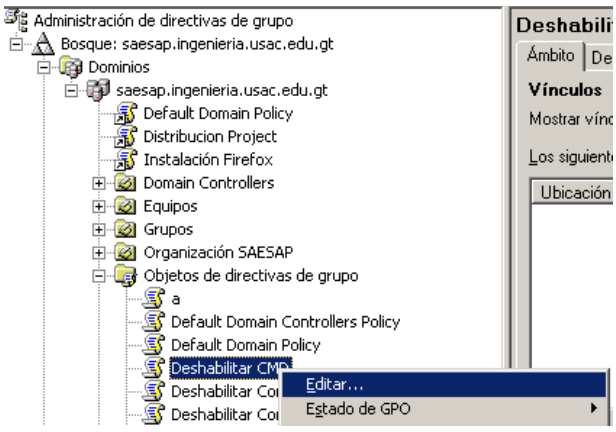
Figura 33. **Creación de política de grupo**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Una vez creada la política, clic derecho sobre la misma y elija editar.

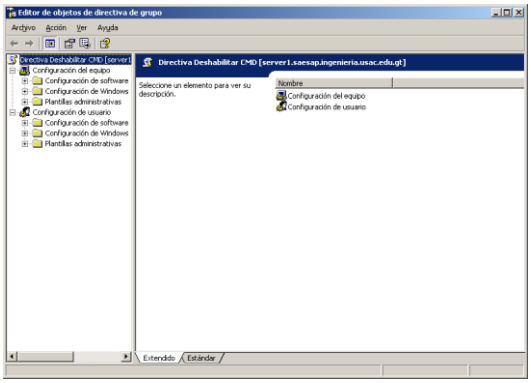
Figura 34. **Selección de política de grupo creada**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En esta pantalla se define la política en sí, en base a la necesidad de la organización. Por ejemplo, deshabilitar el comando MS-DOS, colocar un fondo de pantalla específico, ocultar unidad D, deshabilitar opciones del navegador como Internet Explorer, etc.

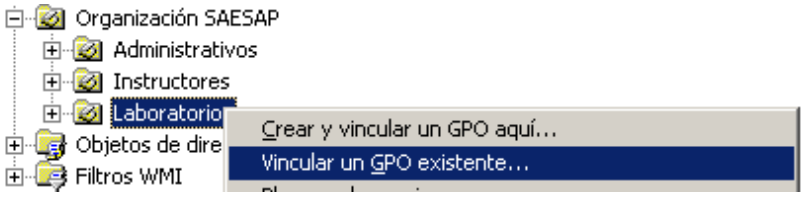
Figura 35. **Definir política de grupo**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Dentro del dominio seleccione la unidad organizativa donde se aplicará la política de grupo creada anteriormente y elegir la opción vincular un GPO existente.

Figura 36. **Vincular una política de grupo a una unidad organizativa**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.5. Servidor DHCP

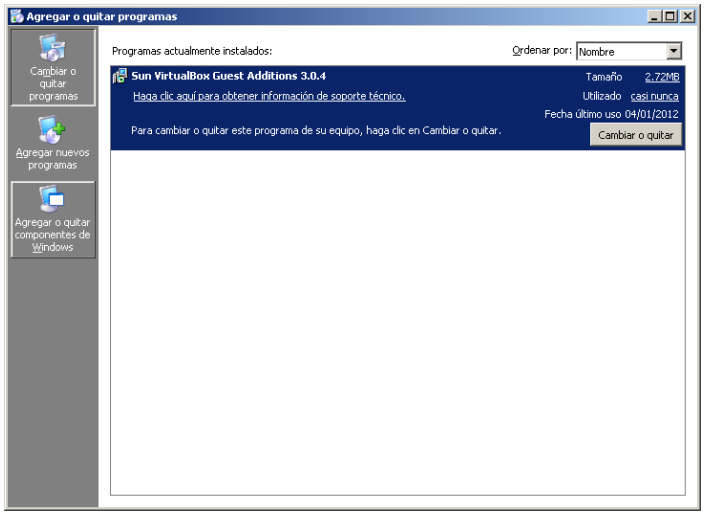
Es un protocolo de red que permitirá a los usuarios de una red IP obtener sus parámetros de configuración automáticamente. Generalmente posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

5.5.1. Instalación servidor DHCP

- Haga clic en Inicio, en configuración y, a continuación, en Panel de control.

- Haga doble clic en Agregar o quitar programas y, después, haga clic en Agregar o quitar componentes de Windows.

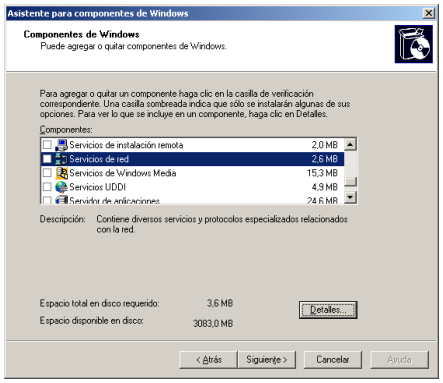
Figura 37. **Agregar o quitar programas**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En el asistente para componentes de Windows, haga clic en servicios de red en el cuadro componentes y, después, en detalles.

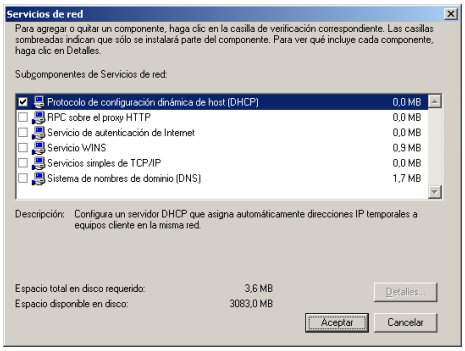
Figura 38. **Asistente para componentes de Windows**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Active la casilla de verificación Protocolo de configuración dinámica de *host* (DHCP) si no está ya activada y, después, haga clic en Aceptar.

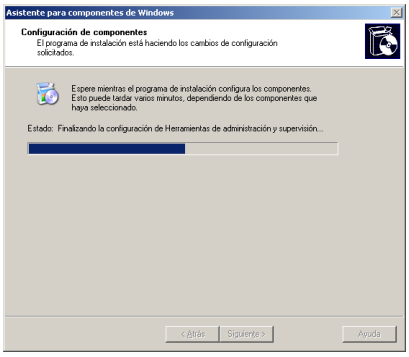
Figura 39. **Servicios de red**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En el asistente para componentes de Windows, haga clic en siguiente para iniciar la instalación. Cuando se le pida, introduzca el disco de instalación de Windows Server 2003 en la unidad de CD-ROM. El programa de instalación copiará al equipo el servidor DHCP.

Figura 40. **Asistente para componentes de Windows**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Cuando termine el programa de instalación, haga clic en finalizar.

Figura 41. **Finalización asistente componentes de Windows**

Fuente: Microsoft Windows Server 2003 Enterprise Edition.

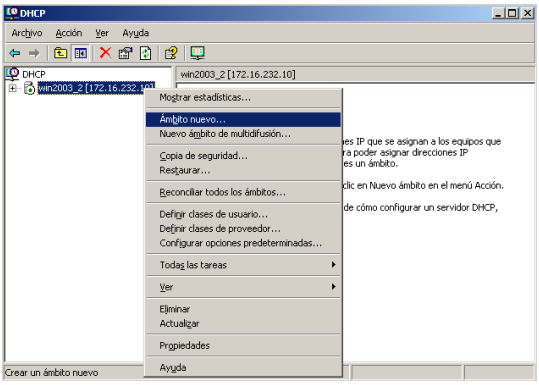
5.5.2. Configuración servidor DHCP

Una vez instalado el servidor DHCP, se creará un ámbito (un intervalo de direcciones IP válidas que se pueden conceder a los clientes de DHCP). Cada servidor DHCP del entorno debe tener al menos un ámbito que no se superponga con ningún otro del servidor DHCP de su entorno. En Windows Server 2003, los servidores DHCP dentro de un dominio de Active Directory deben estar autorizados para impedir que se pongan en conexión servidores DHCP falsos y autoricen a otro servidor DHCP.

- Haga clic en Inicio, Herramientas administrativas y, a continuación, haga clic en DHCP.

- En el árbol de la consola, haga clic con el botón secundario del *mouse* (ratón) en el servidor DHCP en el que desee crear el ámbito DHCP y, a continuación, haga clic en Ámbito nuevo.

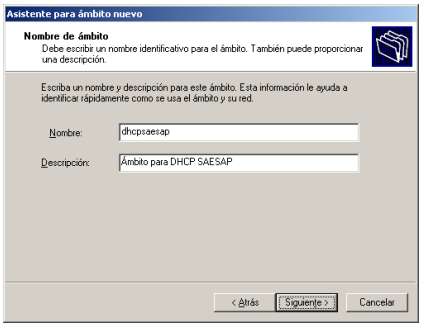
Figura 42. **Selección de ámbito nuevo**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En el Asistente para ámbito nuevo, haga clic en siguiente, y escriba un nombre y una descripción para el ámbito. Haga clic en Siguiente.

Figura 43. **Asistente para el ámbito nuevo**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

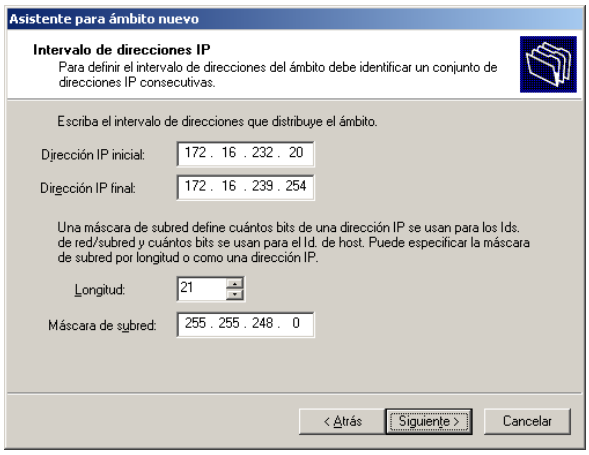
- Escriba el intervalo de direcciones que pueden concederse como parte de este ámbito. La dirección de red provista al departamento SAESAP por parte del Administrador de Red de la Facultad de Ingeniería es la siguiente: 172.16.232.0/21. En base a la máscara de subred se pudo establecer lo siguiente:

Tabla II. **Resumen de direcciones de red SAE/SAP**

Dirección IP de Red	172.16.232.0
Primera dirección IP válida	172.16.232.1
Última dirección IP válida	172.16.239.254
Dirección IP de *Broadcast*	172.16.239.255
Total de *Host* disponibles	2046 *Host*

Fuente: elaboración propia.

Figura 44. **Intervalo de direcciones IP**

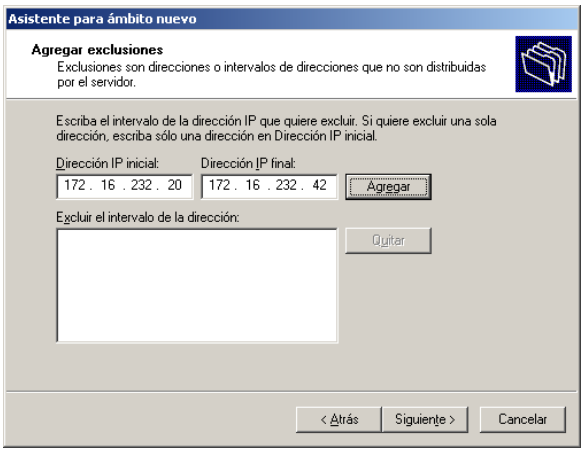


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- La máscara de subred se genera automáticamente. Si desea utilizar una máscara de subred diferente, escríbala. Haga clic en siguiente.

- Escriba todas las direcciones IP que desee excluir del intervalo especificado. Esto incluye todas las direcciones que puedan haberse asignado estáticamente a varios equipos de la organización. Se les asignará IP estáticas mediante el uso de Reservas del servidor DHCP, debido a que el programa que controla el tiempo de usuarios necesita direcciones IP fijas.

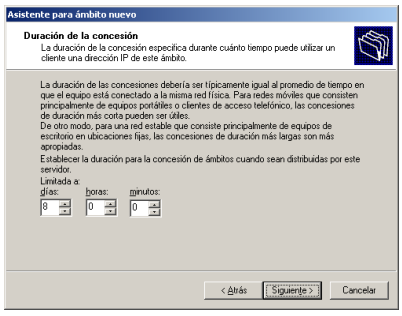
Figura 45. **Exclusión de intervalo de direcciones IP**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Escriba el número de días, horas y minutos que deben transcurrir antes de que caduque la concesión de una dirección IP de este ámbito. Esto determina el período que un cliente puede tener una dirección concedida sin renovarla. Haga clic en siguiente.

Figura 46. **Duración de concesión de direcciones IP**

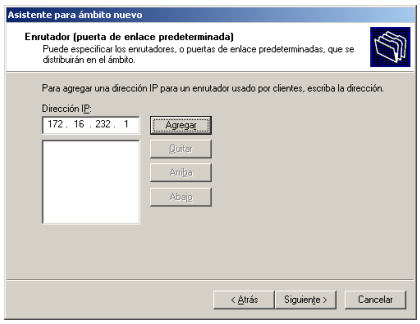


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Haga clic en configurar estas opciones ahora y en Siguiente para extender el asistente de manera que configure valores para las opciones de DHCP más comunes.

- Escriba la dirección IP de la puerta de enlace predeterminada que deben utilizar los clientes que obtienen una dirección IP de este ámbito. Haga clic en Agregar para agregar la dirección de puerta de enlace predeterminada a la lista y, a continuación, haga clic en siguiente.

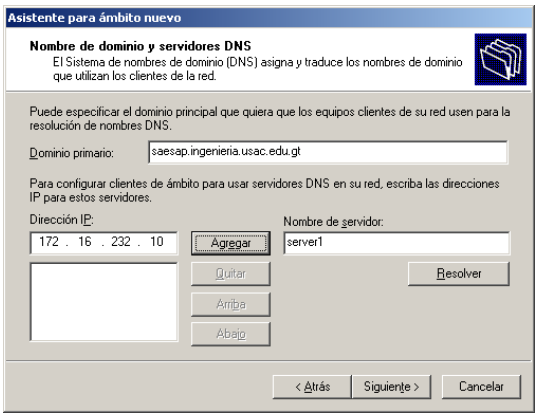
Figura 47. **Configuración de puerta de enlace determinada**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Escriba el nombre de su servidor DNS y haga clic en Resolver para asegurarse de que el servidor DHCP puede ponerse en contacto con el servidor DNS y determinar su dirección. Después, haga clic en Agregar para incluir ese servidor en la lista de servidores DNS asignados a los clientes DHCP. Haga clic en siguiente.

Figura 48. **Nombre de dominio y servidores DNS**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Haga clic en Activar este ámbito ahora para activar el ámbito y permitir que los clientes obtengan concesiones del mismo. Haga clic en siguiente y, después, haga clic en finalizar.

5.6. Reservas IP

Con las reservas de clientes es posible reservar una dirección IP específica, para que la utilice de forma permanente un cliente DHCP.

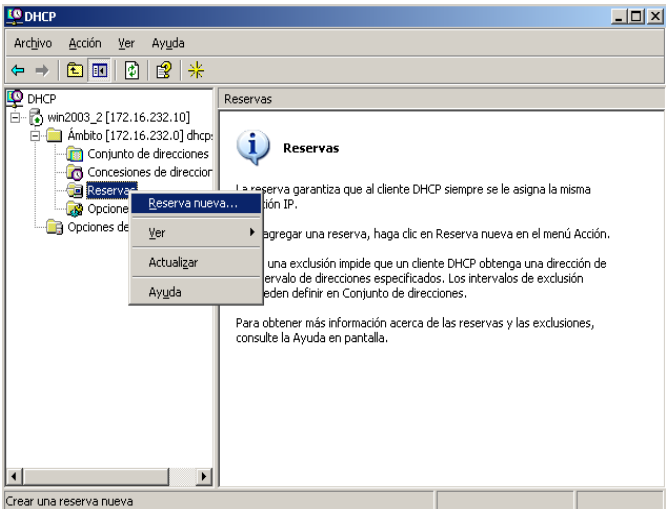
Para la creación de reservas IP es imprescindible conocer la dirección MAC de cada interfaz de red de los equipos del laboratorio Plaza Korea.

5.6.1. Configuración de reservas IP

- Haga clic en Inicio, Herramientas administrativas y, a continuación, haga clic en DHCP.

- Expanda las opciones de la carpeta Ámbito creada con anterioridad. Seleccionar la opción Reservas, clic derecho sobre la misma y presionar sobre la opción reserva nueva.

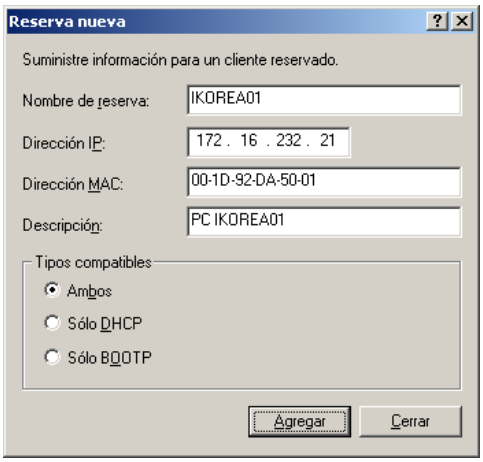
Figura 49. **Selección de reserva nueva**



Fuente: Microsoft Windows Server 2003 Enterprise Edition

- Ingrese la información que se le solicita para crear la reserva IP. Tome en cuenta que la dirección IP está relacionada a la dirección MAC del equipo. Por ejemplo, en la gráfica que a continuación se muestra, estamos indicando lo siguiente: el equipo que tenga la dirección MAC 00-1D-92-DA-50-01 en su interfaz de red, asígnele la dirección IP 172.16.232.21. Repita ésta operación para registrar las reservas necesarias.

Figura 50. **Configuración de reserva nueva**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

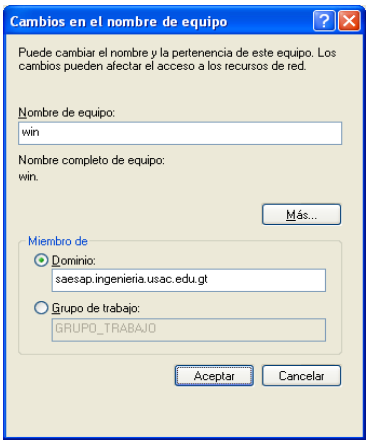
5.7. Agregando equipos al dominio

- Recuerde que para agregar equipos al dominio, deberá tener privilegios de administrador en el equipo cliente. Clic en el botón de Inicio, clic derecho sobre el icono mi pc y seleccionar propiedades.

- Seleccione la pestaña nombre de equipo, y clic sobre el botón cambiar.

- En el área de Miembro de seleccione la opción Dominio y escriba correctamente el nombre del dominio creado en nuestro servidor de directorio.

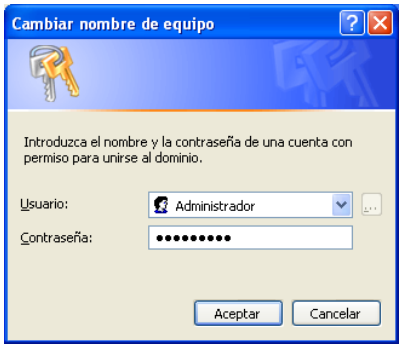
Figura 51. **Configuración de ingreso de equipo al dominio SAE/SAP**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- A continuación se le pedirá que ingrese el nombre de usuario y contraseña no del equipo local, sino, de una cuenta del servidor de directorios con permiso para unirse al dominio.

Figura 52. **Autenticación para unirse al dominio**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

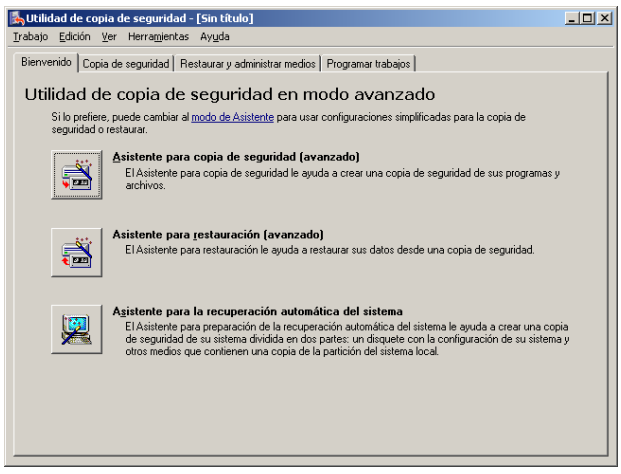
- Si los datos ingresados han sido autenticados correctamente, aparecerá un mensaje indicando que el equipo se ha unido al dominio. Tome en cuenta que éste proceso deberá repetirlo por cada equipo que desee unir al dominio. Por último, se le pedirá que reinicie el equipo para que todos los cambios se realicen correctamente.

5.8. Copia de seguridad servidor de directorios

- Clic en el botón Inicio, seleccione la opción ejecutar, escriba la palabra ntbackup para ejecutar la utilidad de copia de seguridad de nuestro servidor y presione aceptar.

- Seleccione la opción asistente para copia de seguridad (avanzado) y luego presione el botón siguiente.

Figura 53. **Utilidad de copia de seguridad Directorio Activo**

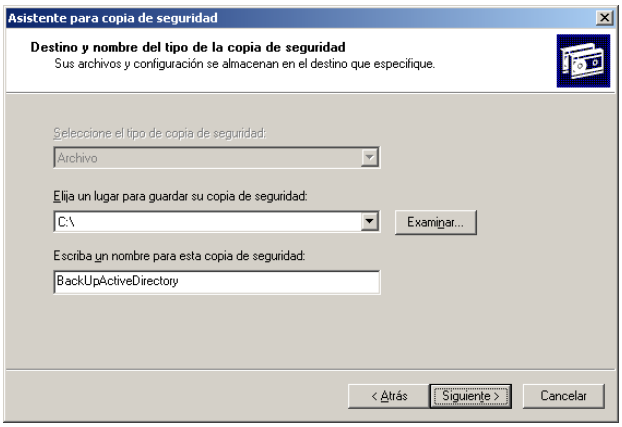


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- En la siguiente pantalla seleccionar Hacer copia de seguridad de los datos de estado del sistema y presionamos siguiente.

- Definir la ubicación y el nombre del archivo que contendrá la copia de respaldo.

Figura 54. **Destino y nombre de la copia de seguridad Directorio Activo**

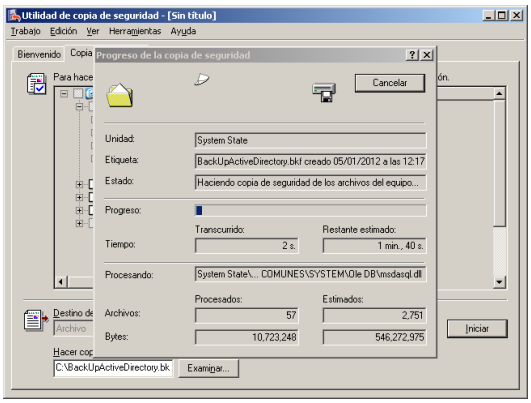


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Mostrará un resumen de la finalización del asistente para la copia de seguridad. Presionar el botón finalizar para que inicie la operación.

- Se observará el progreso de la copia de seguridad.

Figura 55. **Progreso de la copia de seguridad**

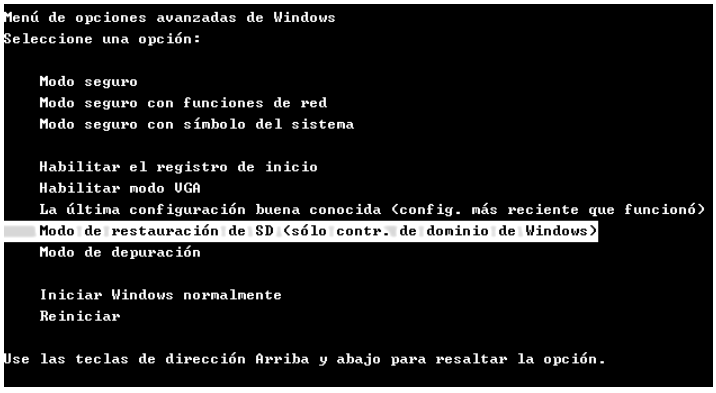


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.9. Restaurar copia de seguridad servidor de directorios

- Iniciar el servidor en modo de restauración (sólo controlador de dominio de Windows) presionando la tecla F8 antes que cargue el sistema operativo.

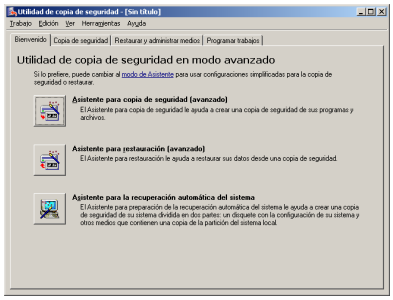
Figura 56. **Modo de restauración controlador de dominio**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Clic sobre el botón Inicio, seleccionar el comando Ejecutar, escribir la palabra ntbackup, presionar Aceptar y dentro de la nueva ventana seleccionar asistente para restauración (avanzada).

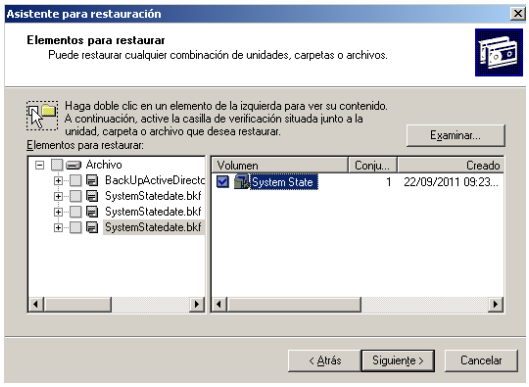
Figura 57. **Utilidad de copia de seguridad modo avanzado**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Seleccionar la ubicación y nombre del archivo de copia de seguridad. Presionar el botón siguiente para la restauración.

Figura 58. **Asistente para restauración del Directorio Activo**

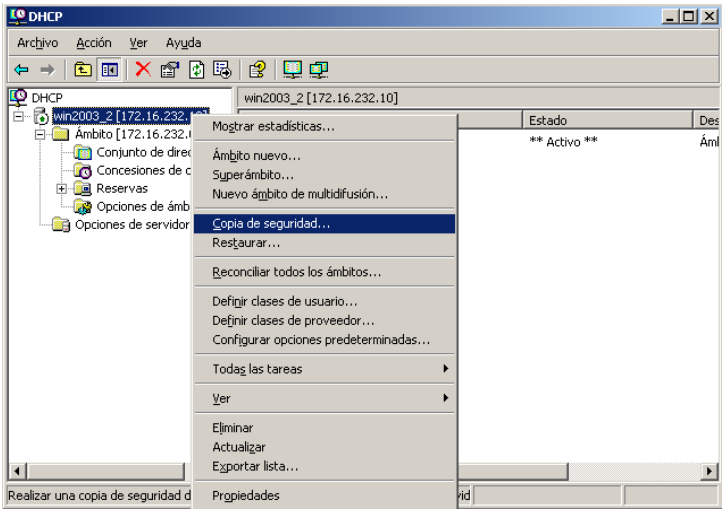


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.10. Copia de seguridad servidor DHCP

- Seleccionar botón de Inicio, en herramientas administrativas seleccionar la opción DHCP. Clic derecho sobre el icono del servidor DHCP y elegir la opción copia de seguridad.

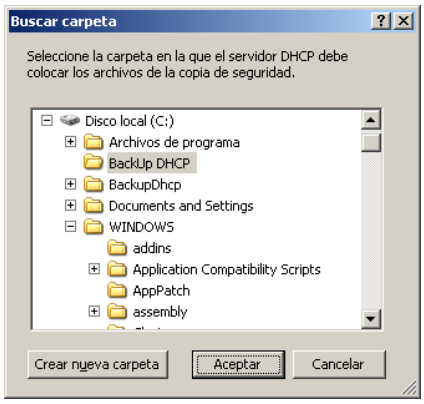
Figura 59. **Copia de seguridad servidor DHCP**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Elegir la ubicación y nombre del archivo que contendrá la copia de respaldo del servidor DHCP y presionar aceptar.

Figura 60. **Ubicación y nombre de la copia de seguridad del DHCP**

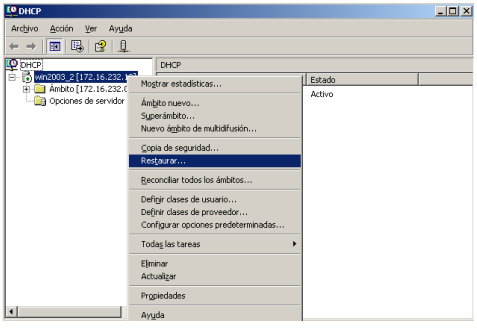


Fuente: Microsoft Windows Server 2003 Enterprise Edition.

5.11. Restaurar copia de seguridad servidor DHCP

- Seleccionar botón de Inicio, en herramientas administrativas seleccionar la opción DHCP. Clic derecho sobre el icono del servidor DHCP y elegir la opción restaurar.

Figura 61. **Restauración de copia de seguridad del DHCP**



Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Seleccionar la ubicación y nombre del archivo que contiene la copia de seguridad y presionar aceptar.

Figura 62. **Ubicación y selección de copia de seguridad del DHCP**

Fuente: Microsoft Windows Server 2003 Enterprise Edition.

- Al momento de restaurar la copia de seguridad se le informará que el servicio DHCP se reiniciará. Al finalizar se habrá concluido con el proceso de restauración.

5.12. Zona desmilitarizada o DMZ

Se refiere a la red local que se ubica entre la red interna de la organización y la red externa, generalmente Internet. El objetivo es que las conexiones de la red interna y la red externa a la zona desmilitarizada estén permitidas, mientras que las conexiones desde la zona desmilitarizada solo se permitan a la red externa.

5.12.1. Instalación firewall (Ubuntu 11.10)

- Inserte el disco de instalación del servidor Ubuntu y elija el idioma de la instalación.

- A continuación elegir la opción Instalar Ubuntu Server y presionar enter.

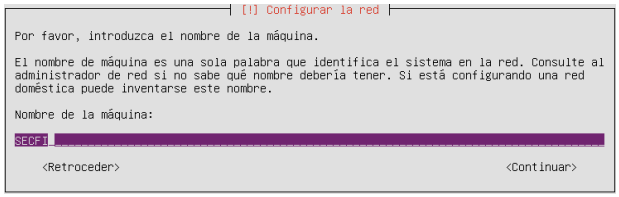
Figura 63. **Instalación de Ubuntu Server**

Fuente: Ubuntu Server 11.10.

- Seleccione la ubicación que se utilizará para fijar su zona horaria.

- Ingrese el nombre del equipo como se identificará dentro de la red.

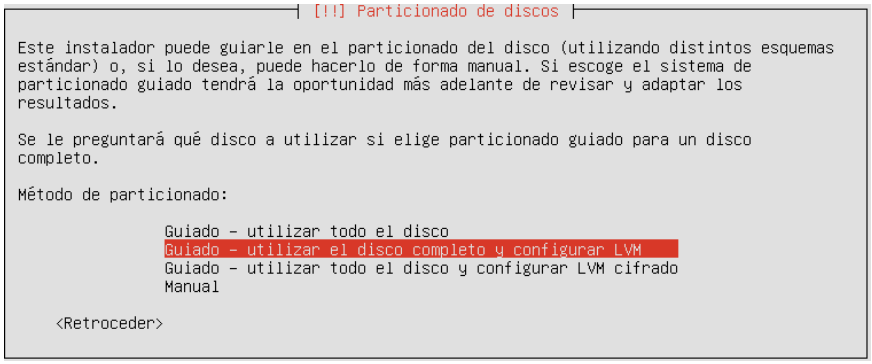
Figura 64. **Configuración de red Ubuntu Server**



Fuente: Ubuntu Server 11.10.

- Para partición del disco duro elegir guiado – utilizar el disco completo y configurar LVM según sea el caso.

Figura 65. **Partición de discos Ubuntu Server**



Fuente: Ubuntu Server 11.10.

- Se le pedirá que confirme la forma de partición del disco.

- Iniciará el proceso de instalación del sistema operativo en el equipo.

- En la siguiente pantalla se le pedirá que elija los programas que se instalarán en su Servidor Ubuntu. En particular sólo instalaremos el OpenSSH Server ya que IPTABLES viene por defecto en el Kernel de Linux.

Figura 66. **Selección de programas Ubuntu Server**

Fuente: Ubuntu Server 11.10.

- Al final mostrará un mensaje indicando que la instalación se ha completado. Retire el disco de instalación y reinicie su equipo.

5.12.2. Configuración interfaces de red

- Para editar el archivo de configuración de las interfaces de red dentro de Ubuntu ingresar el siguiente comando desde una terminal con privilegios de administrador: *sudo nano /etc/network/interfaces*.

- Asignar las direcciones de red a cada interfaz tomando en cuenta su máscara y su dirección de red.

Tabla III. **Configuración de interfaces de red Ubuntu Server**

```
auto lo
iface lo inet loopback

# Red Laboratorios SAESAP
auto eth0
iface eth0 inet static
address   172.16.232.11
netmask  255.255.248.0
gateway   172.16.232.1
network    172.16.232.0

# Red DMZ (Servidor Web)
auto eth1
iface eth1 inet static
address   199.234.100.1
netmask  255.255.255.0
network    199.234.100.0

# Red Administrativa
auto eth2
iface eth2 inet static
address   192.168.1.1
netmask  255.255.255.0
network    192.168.1.0
```

Fuente: elaboración propia.

- Guardar el archivo presionando Ctrl + X.

- Reiniciar los servicios de red mediante el siguiente comando desde una terminal: *sudo /etc/init.d/networking restart* para que se realicen los cambios.

5.12.3. Configuración de IPTABLES

- Ingresar el siguiente comando con privilegios de administrador desde una terminal: *sudo nano /home/firewall.sh* (si no existe el archivo lo crea). La ubicación del archivo es arbitraria. Se abrirá un editor de texto (*nano*), en el cuál escribiremos lo siguiente:

Tabla IV. **Configuración de IPTABLES Ubuntu Server**

```
#!/bin/bash
## FLUSH De Reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -P INPUT  ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

#usado para el nateo
echo 1 > /proc/sys/net/ipv4/ip_forward

# Todo lo que venga por el exterior (INTERNET) y vaya al puerto 80 lo redirigimos a una máquina interna
```

Continuación de la tabla IV.

```
iptables -t nat -A PREROUTING -i eth0 -d 172.16.232.11/255.255.248.0 -p tcp --dport 80 -j DNAT --to 199.234.100.2:80

# Todo lo que venga por el exterior (RED INTERNA) y vaya al puerto 80 lo redirigimos a una máquina interna
iptables -t nat -A PREROUTING -i eth0 -s 172.16.232.0/255.255.248.0 -d 172.16.232.11/255.255.248.0 -p tcp --dport 80 -j DNAT --to 199.234.100.2:80
#iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 22 -j DNAT --to 172.16.100.2:22

# Todo lo que venga de la Red Administrativa y vaya al puerto 80 lo redirigimos a una máquina interna
iptables -t nat -A PREROUTING -i eth2 -s 192.168.1.0/255.255.255.0 -d 172.16.232.11/255.255.248.0 -p tcp --dport 80 -j DNAT --to 199.234.100.2:80

# El localhost se deja
/sbin/iptables -A INPUT -i lo -j ACCEPT

# Al firewall tenemos acceso desde la red Local
iptables -A INPUT -s 192.168.1.0/24 -i eth2 -j ACCEPT

# Enmascaramiento de la Red Administrativa y la DMZ para salir a Internet
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 199.234.100.0/24 -o eth0 -j MASQUERADE



# Permitimos el Paso del Área Administrativa a la BDD SQL
iptables -A FORWARD -s 192.168.1.0/24 -p tcp --sport 1433 -d 199.234.100.2/24 -j ACCEPT

iptables -A FORWARD -s 199.234.100.2/24 -p tcp --sport 1433 -d 192.168.1.0/24 -j ACCEPT
```

Continuación de la tabla IV.

```
# Cerramos acceso de la DMZ a la LAN
#iptables -A FORWARD -s 199.234.100.0/24 -d 192.168.1.0/24 -j DROP

# Cerramos acceso de la DMZ al propio Firewall
iptables -A INPUT -s 199.234.100.0/24 -i eth1 -j DROP

# Cerramos el rango de puerto bien conocido
iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 1:1024 -j DROP

# Cerramos el puerto de Gestión del Webmin
iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 10000 -j DROP

# Fin del Script
```

Fuente: elaboración propia.

- Presionar la tecla Ctrl + X para cerrar y guardar el archivo firewall.sh.

- Ejecutar el archivo firewall.sh que administrará el tráfico de red de nuestro firewall. Dentro de una terminal escribir el siguiente comando: *sudo ./home/firewall.sh* para activar las reglas.

CONCLUSIONES

1. Las redes informáticas dentro de las organizaciones hoy en día, se han convertido en parte vital de ellas, pues es una herramienta necesaria para compartir recursos e información como también asegurar la confiabilidad y la disponibilidad de la información.

2. Con la implementación de un servidor DHCP se ha logrado obtener una configuración segura y fiable de direcciones IP a los equipos, evitando errores de configuración o conflictos de direcciones IP.

3. La utilización del servidor DHCP redujo significativamente el tiempo necesario para configurar y reconfigurar las direcciones IP de los equipos.

4. El uso de un Directorio Activo reduce el costo de propiedad, debido a que permite configurar entornos de trabajo e instalar aplicaciones desde una consola administrativa.

5. El Directorio Activo proveyó una administración simplificada, mediante una localización simple de la información almacenada como recursos y usuarios.

6. El uso de políticas de grupo fue de vital importancia para administrar los entornos de trabajo de los usuarios del dominio y el comportamiento de sus recursos.

7. La implementación de políticas de seguridad ayudó a concientizar a los usuarios de la importancia y la sensibilidad de la información y sus servicios, los cuales favorecen el desarrollo de la organización y su buen funcionamiento.

8. El uso de un firewall de software hizo posible el control del tráfico de información entre redes y protección de la información contra cualquier ataque desde el exterior.

RECOMENDACIONES

1. Se le insta que el personal involucrado en la administración y monitoreo del sistema Windows 2003 sea previamente capacitado, para aprovechar las características implementadas y conseguir una óptima funcionalidad.

2. Durante el análisis e implementación del sistema se pudo apreciar al menos cuatro encargados debido a la cantidad de los laboratorios. Por tal razón se propone que la administración se realice de forma centralizada.

3. Se recomienda a tener una mentalidad abierta al uso de tecnologías de pago como de Open source, evaluar sus bondades y tomar las mejores decisiones que se ajusten a sus recursos con que cuenta sean éstos de hardware, software o económicos.

4. Se recomienda reemplazar todos los conectores RJ45 de los cables de red que llegan a los equipos de cómputo de los laboratorios del primer nivel (Geomática) y los del tercer nivel (LCE). También se insta a realizar una verificación de los conectores RJ45 en el resto de los laboratorios para evitar problemas de conectividad.

5. De implementar una red inalámbrica, se recomienda crear una red nueva, instalando otra interfaz de red en el servidor firewall y realizar las configuraciones necesarias de los IPTABLES, debido a que es más insegura que una red cableada.

BIBLIOGRAFÍA

1. ALTADILL IZURA, Pello Xabier. *Iptables manual práctico*. [en línea] <http://www.pello.info/filez/firewall/iptables.html>. [Consulta: 6 de marzo de 2012].

2. GARCÍA GARCÍA, Rafael. *Gestión y administración de Windows Server 2003*. [en línea] <http://es.scribd.com/doc/48055164/Manual-de-Gestion-y-Administracion-Windows-Server-2003>. [Consulta: 27 de febrero de 2012].

3. HERRERA PÉREZ, Enrique. *Tecnologías y redes de transmisión de datos*. [en línea] <http://books.google.com.gt/books?id=2zzUqp-Jp-oC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. [Consulta: 24 de febrero de 2012].

4. NETFILTER. *Netfilter/iptables*. [en línea] <http://es.wikipedia.org/wiki/Netfilter/iptables>. [Consulta: 8 de marzo de 2012].

5. REDES INFORMÁTICAS. *Redes de computadoras*. [en línea] <http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_las_redes>. [Consulta:17 de febrero de 2012].

6. SEGURIDAD REDES. *Manual de seguridad en redes*. [en línea] <http://www.librosintinta/biblioteca/ver-pdf/www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf.htx>. [Consulta: 6 de marzo de 2012].

7. SERVIDORES. *Fundamentos de los servidores*. [en línea] <http://www1.la.dell.com/content/topics/segtopic.aspx/es/dell-server-basics-buy-guide?c=cl&l=es&cs=clbsdt1>. [Consulta: 23 de febrero de 2012].

8. TCP/IP. *El modelo TCP/IP*. [en línea] <http://technet.microsoft.com/es-es/library/cc786900%28WS.10%29.aspx>. [Consulta: 23 de febrero de 2012].

9. UBUNTU SERVER. *Meeting Minimum Hardware Requirements*. [en línea] <https://help.ubuntu.com/11.04/installation-guide/i386/minimum-hardware-reqts.html>. [Consulta: 9 de marzo de 2012].

10. WINDOWS 2003 SERVER. *Requisitos del sistema windows 2003 server*. [en línea] <http://technet.microsoft.com/es-es/windowsserver/bb430827>. [Consulta: 10 de marzo de 2012].

11. ZIEGLER, Robert L. *Firewalls Linux, Guía Avanzada*. [en línea] <http://www.abebooks.com/servlet/BookDetailsPL?bi=8611570934&searchurl=an%3Drobert%2Bl%2Bziegler>. [Consulta: 8 de marzo de 2012].