UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DOMINIO PARA LA ADMINISTRACIÓN CENTRALIZADA DE RECURSOS DE CÓMPUTO

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

AGUILAR MACIEL MARCO ANTONIO

CORTES JUÁREZ JULIO CÉSAR

DIRECTORA DE TESIS:
MA. JAQUELINA LÓPEZ BARRIENTOS
(2013)

ÍNDICE

Índice de Tablas

Índice de Figuras

Introducción

Uno de los principales objetivos del módulo de redes y seguridad de la carrera de Ingeniería en Computación, es implementar las mejores prácticas y herramientas necesarias para garantizar la seguridad ya sea física o informática de los bienes, por ello los académicos se esfuerzan por demostrar de manera real a los alumnos cómo se implementan dichas prácticas, mecanismos y herramientas de seguridad con el material y espacio disponibles. De esta forma, gran parte de lo expuesto en las clases de teoría, se implementa a cierta escala en el Laboratorio de Redes de Datos y Seguridad.

Así, haciendo un análisis de la forma de operar del laboratorio, se ha observado que uno de los inconvenientes que se presentan es la administración de las cuentas tanto de usuarios como de los equipos de cómputo. Al estar operando bajo el modelo "grupo de trabajo" (infraestructura implementada actualmente) cada computadora tiene su propia base de datos de administración de cuentas de seguridad, a consecuencia de esto, la administración de las cuentas se lleva acabo de manera descentralizada (debe administrarse y configurarse cada equipo y cuenta individualmente), por lo que no se admite una configuración automática para todas las PCs al mismo tiempo. También se ha notado que a pesar de las reglas del laboratorio, su red no es del todo segura, ya que todas las cuentas de los equipos de cómputo son de tipo "administrador local" y éstas pueden ser vulneradas al suplantar identidades.

La actualización de los equipos de cómputo y las labores de mantenimiento, representan tareas adicionales para los administradores debido a que no existe una configuración unificada para el acceso sus recursos, como por ejemplo carpetas de trabajo, servicios y control de acceso a los equipos.

De esta manera se ha detectado que el principal problema en el laboratorio es mantener los equipos operando adecuadamente durante el semestre debido a los inconvenientes ya mencionados, además de los desperfectos causados por los estudiantes o usuarios y al carga administrativa generada a lo largo de cada semestre, por lo que mantener eficazmente la operación del laboratorio durante el semestre representa una labor muy ardua.

Para solucionar lo anterior, se propone contribuir con la implementación de un dominio, el cual contendrá las herramientas necesarias para realizar las labores de administración centralizada de la infraestructura de cómputo del Laboratorio de Redes de Datos y Seguridad.

Así, el objetivo del presente trabajo de tesis es: Instrumentar un dominio para Administración Centralizada de Recursos de Computo, con el fin de simplificar las tareas administrativas, reducir el número de problemas presentados en el uso de los equipos de cómputo para garantizar el uso correcto y seguro de las actividades impartidas en el laboratorio, así como mejorar los servicios de éste de tal forma que los problemas que llegaran a presentarse sean resueltos de manera clara y oportuna.

Para alcanzar el objetivo mencionado, se ha desarrollado el presente trabajo en 3 capítulos, donde el primero de ellos contiene definiciones básicas de redes y administración, cabe mencionar que son importantes para entender algunos conceptos que se usarán durante el desarrollo del presente trabajo para así poder tener un mayor entendimiento en los capítulos posteriores.

En el capítulo 2 se hace un análisis de requerimientos del laboratorio de redes y seguridad de la Facultad de Ingeniería, así como también se detalla el escenario actual identificando tanto el software como el hardware disponible y necesario para poder realizar las prácticas que desarrollarán los alumnos, también se encontrarán una serie de preguntas realizadas a la administradora del laboratorio las cuales se consideran necesarias para identificar la problemática y así poder hacer finalmente el análisis de factibilidades para poder disminuir los problemas principales previamente identificados. Con este capítulo se pretende brindar un panorama actual de estado del laboratorio para poder identificar áreas de oportunidad para mejoramiento del mismo.

La instrumentación de un dominio se desarrollará en el capítulo 3 como solución a los inconvenientes identificados esto es, seleccionando, definiendo e implementando las herramientas que mejor se adecuan para dicha solución, se explica de manera general desde la instalación del sistema operativo seleccionado y así como las funciones necesarias para dicha instrumentación, al final de este capítulo se encuentra una fase de pruebas donde se identificaron algunos problemas y la solución de los mismos. Este capítulo aporta soluciones a diversos problemas especificados en el tema anterior.

Finalmente una vez terminada la instrumentación del dominio, en las conclusiones se reflejan las consecuencias más importantes del presente trabajo así como también se realizan algunas recomendaciones como aporte adicional con el fin de mejorar los servicios ofrecidos en el laboratorio, aprovechar al máximo la solución implementada y que así el laboratorio de redes y seguridad de la Facultad pueda crecer en infraestructura en un futuro cercano.

Capítulo 1
Conceptos Básicos

En este primer capítulo se verán los conceptos básicos necesarios para comprender este trabajo de tesis

1.1Definiciones

Redes de Datos

Una red de computadoras es un conjunto de computadoras (y generalmente terminales) conectados mediante una o más vías de transmisión que usan un protocolo en común. (Behrouz, 2002)

De este modo ahora surge la pregunta ¿qué son las vías de transmisión y los protocolos?

Medios o Vías de Transmisión

El ambiente físico usado para conectar miembros de una red se denomina medio.

Los medios de la red facilitan la comunicación al proporcionar un ambiente para que la comunicación tenga lugar. Los medios de una red se presentan en dos amplias categorías: cables e inalámbricos. Ejemplos del medio cable son el cable de par trenzado, el cable coaxial y la fibra óptica. Ejemplos del medio inalámbrico son las ondas de radio y radiación infrarroja. (Behrouz, 2002)

Ventajas de las Redes de Datos:

Las Redes de datos presentan diversas ventajas de entre las cuales se destacan las siguientes (Black, 1997):

- Las organizaciones modernas de hoy en día suelen estar dispersas geográficamente, y sus oficinas están situadas en diversos puntos de un país e incluso en diferentes lugares del mundo. Muchas computadoras y terminales de cada una necesitan intercambiar información y datos. Las redes proporcionan la posibilidad de que dichas computadoras puedan intercambiar toda esa información y los programas necesarios a todo el personal de la empresa.

- Las redes de computadoras permiten compartir recursos, por ejemplo, una impresora o algún otro dispositivo.

- Las redes también pueden facilitar la función crítica de tolerancia ante fallos. En el caso de que una computadora falle, otra puede asumir sus funciones y su carga de trabajo. Esta posibilidad es de especial importancia, por ejemplo, en sistemas de publicación de páginas Web, algunas empresas emplean más de un servidor para atender las solicitudes hacia su página, entonces en caso de que falle algún servidor, otro puede tomar su carga de trabajo.

- Entre las ventajas más importantes que ofrecen las redes de computadoras se encuentran: permitir el compartir recursos e información, permitir un entorno de trabajo flexible y la tolerancia a fallos en funciones críticas

Topologías de Red

Hay muchos tipos diferentes de redes de computadoras. Las diferencias entre ellas se fundamentan usualmente en la perspectiva. Por ejemplo, las redes de computadoras son frecuentemente clasificadas según el área geográfica que abracan, por sus topologías o el tipo de rutas de comunicación que usan y la manera en que los datos son transmitidos a lo largo de esta ruta.

En este caso se comienza definiendo las redes por su topología.

La topología establece la forma (en cuanto a conectividad física) de la red. El termino topología se utiliza en geometría para describir la forma de un objeto. El diseño de una red tiene tres objetivos al establecer la topología de la misma (Black, 1997):

- Proporcionar la máxima fiabilidad a la hora de establecer el tráfico (por ejemplo, mediante encaminar alternos).
- Encaminar el tráfico utilizando la vía de coste mínimo entre los terminales (no obstante, a veces no se escoge la vía de coste mínimo porque otros factores, como la fiabilidad, pueden ser más importantes).
- Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo.

De este modo, para cumplir con los objetivos antes mencionados, se tienen 5 topologías que son las más comunes y usadas:

1. **Topología de Árbol:** Una topología de árbol es una configuración jerárquica (Figura 1.1). Ella consiste en un nodo raíz o núcleo que está conectado a nodos o núcleos de segundo nivel. Esos dispositivos de segundo nivel están conectados a dispositivos de tercer nivel, y así sucesivamente. (Black, 1997)

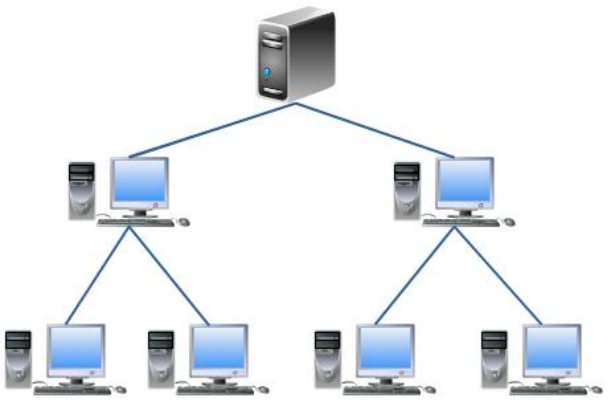

Figura 1. 1 *Topología de árbol. La jerarquía comienza en un nodo raíz y se ramifica hacia más nodos.*

2. **Topología en Bus:** En esta topología un cable largo actúa como canal que conecta todos los dispositivos en la red. Los nodos se conectan al bus mediante cables de conexión. (Black, 1997)

Figura 1. 2 *Topología en Bus, un único cable se conecta a cada uno de los dispositivos de red*

3. **Topología en Estrella**: Una característica clave de una red en estrella es la presencia de un equipo o núcleo central de procesamiento, que sirve como centro de cableado para todos los demás nodos. (Black, 1997)

Figura 1. 3 *Topología típica en estrella.*

4. **Topología en Anillo**: En una configuración de anillo, todos los nodos están conectados al mismo anillo (Figura 1.4), que sirve como el medio compartido. Las redes basadas en anillos pueden diseñarse físicamente como una estrella. Al diseño de estrella se le llama formalmente anillo lógico sobre una estrella física, y al diseño en simple bucle se le llama bucle se le llama formalmente anillo lógico sobre anillo físico. (Black, 1997)

Figura 1. 4 *Topología en anillo. La comunicación se da mediante un token*

5. **Topología en Malla**: En la topología de malla (Figura 1.5) cada nodo en la red está conectado a todos los demás (todos conectados con todos). (Black, 1997)

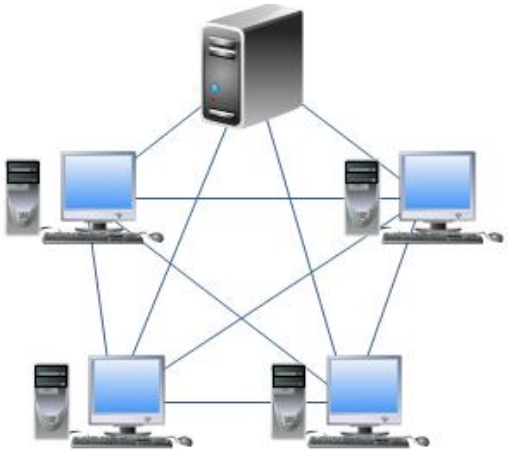

Figura 1. 5 *Topología en malla. Todos los dispositivos de red están interconectados con cada uno de los dispositivos pertenecientes a la red.*

Clasificación de las Redes de Datos

Un criterio alternativo para la clasificación de las redes es su escala, es decir, la distancia que hay entre sus nodos (Tanenbaum, 1994). Las redes se clasifican de acuerdo a su extensión geográfica, dicha clasificación se muestra en la tabla 1.1

Tabla 1. 1 Redes de datos según su extensión geográfica

Distancia entre Nodos:	Nodos ubicados en el mismo:	Ejemplo
1 m	Metro cuadrado	Red personal
10 m	Cuarto	Red Local
100 m	Edificio	Red Local
1 Km	Campus	Red Local
10 Km	Ciudad	Red de Área Metropolitana
100 km	País	Red de Área Amplia
1000 km	Continente	Red de Área Amplia
10,000 km	Planeta	Internet

Las Redes de Área Personal (**PAN**) están destinadas para una sola persona. Por ejemplo, una red que conecta una computadora con su ratón, teclado e impresora, es una red personal.

Redes de Área Local (**LAN**) por sus siglas en inglés LAN, Local Area Network, son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo impresoras) e intercambiar información.

Las redes LAN están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño anteriormente descritos. Esto también simplifica la administración de la red. LA velocidad de transferencia de información de estas redes es de entre 10 y 1000 Mbps

Los medios por los que se comunican los dispositivos en una red LAN son propiedad de la organización que las utiliza. Las compañías proveedoras de Internet o telefonía no son sus propietarias ni se ocupan de su mantenimiento.

La Red de Área Metropolitana (**MAN**) por sus siglas en inglés MAN, Metropolitan Area Network, abarca una ciudad. El ejemplo más conocido de una red MAN es la red de televisión por cable disponible en muchas ciudades. Generalmente se trata de un conjunto de redes LAN dispersas por la ciudad. Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL (Digital Subscriber Line), WDM (Wavelenght Division Modulation), ISDN, E1/T1, PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas. Maneja velocidades de entre 50 y 100 Mbps.

Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguen entre redes LAN y WAN.

Las Redes de Área Amplia (**WAN**) por sus siglas en inglés Wide Area Netwok, son aquellas que proporcionan un medio de transmisión a lo largo de grandes extensiones geográficas (por lo general más de 100 km). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo. Maneja velocidades de transferencia de información de 19.2 Kbps a 622 Mbps.

Ejemplos de las redes WAN incluyen a la red de datos de servicios digitales integrados (ISDN), el frame relay, el servicio de datos conmutados multimegabit (SMDS) y las redes de transferencia asíncrona (ATM).

La Red de Área Global (GAN) se refiere a un conjunto interconectado de redes WAN que cubren todo el planeta. Por ejemplo, muchos negocios tales como los bancos, tienen operaciones en gran cantidad de países en todo el mundo. La conexión de esas localizaciones de negocios individuales forman a la red GAN.

Modelo de Referencia OSI

El modelo OSI (en español Interconexión de Sistemas Abiertos), fue creado por la ISO en 1984 con el objetivo de posibilitar la interoperabilidad de varias redes patentadas y heterogéneas, además de fungir como modelo de referencia para la creación de futuros estándares de protocolos de redes (Stallings, 2004).

Describe cómo se transfiere la información desde una aplicación de software en una computadora a través del medio de transmisión hasta una aplicación de software en otra computadora. OSI es un modelo conceptual compuesto de siete capas; en cada una de ellas se especifican funciones de

red particulares. Cada capa es razonablemente individual, por lo que las tareas asignadas a cada capa se pueden implementar de manera independiente. Esto permite que las soluciones ofrecidas por una capa se puedan actualizar sin afectar a las demás.

Las capas del modelo OSI son las siguientes:

- Capa 7: Capa de Aplicación
- Capa 6: Capa de Presentación
- Capa 5: Capa de Sesión
- Capa 4: Capa de Transporte
- Capa 3: Capa de Red
- Capa 2: Capa de Enlace de Datos
- Capa 1: Capa Física

Cada capa consta de partes: una de definición de servicio, que define el tipo de servicio que la capa proporciona, y una especificación de protocolo, que detalla las reglas que rigen la implementación de un servicio en particular.

Las siete capas del modelo de referencia OSI se pueden dividir en dos categorías: Capas Superiores y Capas Inferiores.

Las capas Superiores tienen que ver con la aplicación y en general están implementadas sólo en software. La capa superior, la de aplicación, es la más cercana al usuario final. Tanto los usuarios como los procesos de la capa de aplicación interactúan con la aplicación de software que contiene un componente de comunicación.

Las capas inferiores manejan lo concerniente a la transferencia de datos. Las capas física y de enlace de datos se encuentran implementadas en hardware y software. En general las otras inferiores están implementadas en software. La capa física, es la más cercana al medio de transmisión de la red física, es la responsable de colocar la información en el medio de transmisión.

Modelo de referencia TCP/IP

El modelo de referencia TCP/IP tiene sus orígenes en la red de computadoras ARPANET, una red de investigación respaldada por el DoD. Con el paso de los años, esta red conectó a las universidades e instalaciones gubernamentales mediante líneas telefónicas alquiladas, posteriormente se agregaron redes satelitales y de radio, motivo por el cual los protocolos existentes tuvieron problemas para interactuar con las nuevas redes. De este modo la necesidad de comunicar a todas aquellas redes da como resultado el origen de una nueva arquitectura de referencia, el modelo TCP/IP (Stallings, 2004).

En la figura 1.6 se puede observar una imagen comparativa entre los dos modelos:

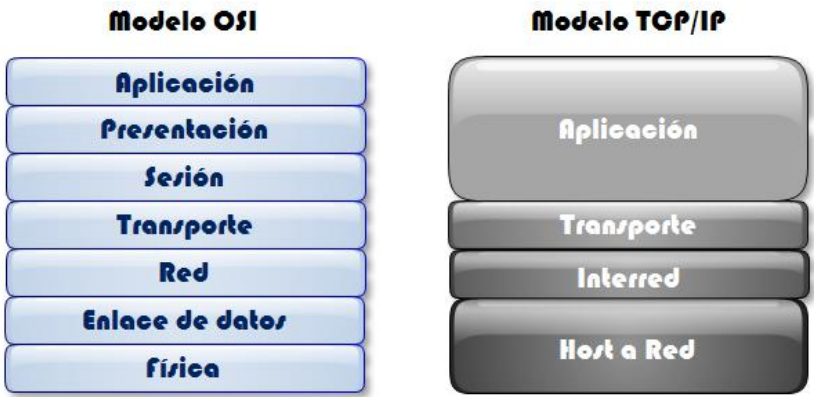

Figura 1. 6 *Comparación entre el modelo TCP/IP y el modelo OSI*.

Administración de Redes de Datos

La administración está definida como el proceso de planificación, organización, dirección y control del trabajo de los miembros de una organización o institución, así como de usar los recursos disponibles para alcanzar las metas establecidas. Cabe señalar que los objetivos pueden ser múltiples y muy variados.

Así, al analizar la definición del concepto puro de administración, se puede encontrar para este trabajo de tesis una definición acorde con el tópico según el autor Heriberto Olguín (Olguin, 1997), que dice lo siguiente: "La administración de redes de datos es el proceso de controlar redes de datos complejas para maximizar su eficiencia y productividad".

De este modo, se observa a la administración de redes como una herramienta indispensable hoy por hoy para el buen funcionamiento de y desempeño de las organizaciones e instituciones donde exista al menos una red de datos. Cabe señalar que en nuestros días casi todas las instituciones y organizaciones manejan o tienen en sus instalaciones de trabajo una red de datos, ya sea de pequeño, mediano o gran tamaño; de ahí viene en gran medida la importancia de mantener la red de datos funcional y optima mediante su administración.

Ventajas de la Administración de Redes:

Se pueden obtener múltiples ventajas para la institución con una correcta implementación y administración de las redes de datos, entre las ventajas se pueden observar las siguientes:

- Con una correcta administración es posible reducir considerablemente el tiempo de respuesta para la solución de cualquier tipo de problemas, esto gracias a las herramientas y procedimientos con que se cuentan.

- Con una correcta centralización de los recursos de cómputo se ofrece un enfoque completo, ya que desde un mismo sitio se tiene el control tanto del software como el hardware, así como los dispositivos de comunicación (equipos de telecomunicaciones como el switch, etc.).

- Una de las partes importantes en una correcta administración de las redes de datos son sus procedimientos, los cuales se basan en una serie de políticas que conllevan al cumplimiento y resolución de algún problema que llegara a presentarse.

- Otra ventaja es poder administrar el rendimiento de la red para proporcionar un diagnóstico del estado en el que se encuentra la misma así como de los sistemas que la conforman, esto con el fin de tomar acciones preventivas ante posibles eventualidades, o acciones correctivas ante un problema presente en el momento.

- Al tener un control y administración centralizada, la tendencia es unificar la información de la organización o institución, esto permite un acceso rápido a la información para permitir con ello la toma de decisiones en forma conjunta, basándose en las políticas y procedimientos para la solución de los problemas, brindando así un mejor servicio.

- Además de lo anterior, se puede tener la capacidad de planear el crecimiento de la red y de sus sistemas con una visión amplia a futuro.

Otro punto a resaltar es que en muchas organizaciones e instituciones el manejo de la información es un factor crítico para el desarrollo de sus actividades, por tal motivo, aprovechar todas las ventajas y beneficios de una red de datos es una tarea fundamental.

Objetivo de la Administración de Redes de Datos:

Entre los principales objetivos por el cual es necesario tener una administración de las redes de datos en general se tienen las siguientes:

- Asegurar un servicio de operación, soporte y mantenimiento óptimo a los usuarios de la red para que reciban el servicio con la calidad que se espera en la organización o institución. Esto se logra gracias a que se cuentan con las herramientas necesarias para tomar las acciones pertinentes

- Planeación estratégica y táctica de las operaciones y mantenimiento de la red y de sus servicios. Esto nos proporciona información de los requerimientos faltantes y disponibles para poder realizar un presupuesto a futuro.

- Ayudar al personal de ingeniería a enfrentar las complejidades de la red y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios.

- Otro objetivo muy importante y que se muestra como una ventaja al tener una administración centralizada de la red de datos, es la administración de la seguridad tanto de los recursos de la red y sus sistemas, como de la información que circula por ella.

De este modo se observan los objetivos de la administración de redes de datos, que la tendencia es tener un control total centralizado para proveer un máximo desempeño de las funciones y servicio de la red con un mínimo de administración y costo.

Modelos y Protocolos de Administración de Redes

Haciendo un poco de historia, en la década de 1980 se vivió una gran expansión en el área de la implementación de las redes de datos. Esto, debido a que las empresas se percataron de los beneficios en los costos y el aumento de la productividad creadas por el uso de la tecnología de red, pero también a mediados de la misma década, comenzaron a suscitarse problemas al ampliar las redes existentes debido al uso de las nuevas tecnologías de red y sus productos que generalmente presentaban problemas de compatibilidad.

Los problemas asociados con la expansión de la red afectaban tanto a la administración diaria de la red y a la planificación estratégica que se hacía para su crecimiento sustentable. Cada nueva tecnología de red adquirida necesitaba su propio conjunto de expertos, por lo que la necesidad de personal solo para la gestión de redes grandes y heterogéneas desembocó en problemas de administración y gastos innecesarios para las organizaciones, creado una crisis para muchas de ellas. De este modo surgió la necesidad urgente para la administración automatizada de la red, así, comenzaron a surgir los modelos de administración para responder a toda la problemática.

La tabla 1.2 relaciona los modelos de administración de red y sus principales características para un mejor discernimiento de todos ellos.

Tabla 1. 2 Comparativa Modelos de Administración de Red

Modelo de Administración	Órgano responsable	Tipo de Administración	Utilización
Modelo Básico de Administración de Redes	ISO	Fallas, configuraciones, desempeño, confiabilidad, seguridad.	Estructura conceptual para la administración de redes populares.
TMN	ITU-T	Admón. de Empresas, Admón. de Servicios, Admón. de Redes y Admón. de los elementos de red.	Estructura conceptual para muchos servicios de Proveedores de Sistemas de Admón. de redes.
TOM	TMN (TeleManagement Forum)	Redes y sistemas, desarrollo de servicios y operaciones, atención al usuario	Utilizado en los procesos de negocios utilizados por los proveedores de servicios.
eTOM	TMN (TeleManagement Forum)	Redes y sistemas, desarrollo de servicios y operaciones, atención al usuario	Versión mejorada y actualmente usada del modelo TOM.
OAM&P	Proveedores de Servicio	Operación, Mantenimiento, Administración, aprovisionamiento.	Utilizado en redes de grandes proveedores de servicios. Se utiliza para grandes redes.
FCAPS	ISO	Fallas, configuraciones, desempeño, confiabilidad, seguridad.	Estructura conceptual para la administración de redes populares.

Del mismo modo, la tabla 1.3 relaciona los protocolos de administración de red y sus principales características.

Tabla 1. 3 Comparativa de protocolos de administración de red

Protocolo de Administración	Órgano responsable	Tipo de Administración	Utilización
SNMP	IETF	Desempeño, fallos	Ampliamente utilizado en redes de datos, especialmente en redes basada en TCP/IP.
CMIP/CMIS	ISO	Desempeño, configuraciones	Desarrollo limitado, basado en redes en el modelo OSI.
CORBA	OMG	Cómputo Distribuido	Inter operatividad entre sistemas abiertos

Con esto, se tienen elementos para poder elegir un modelo de administración según sean nuestras necesidades, o se pueden elegir uno y acoplarlo a nuestros requerimientos específicos.

1.2 Grupos de Trabajo.

Definiendo un grupo de trabajo, se refiere a un grupo de computadoras interconectadas que comparten datos y recursos (impresoras, scanner y otros dispositivos) (Microsoft, Dominio, grupo de trabajo y grupo en el hogar, s.f.).

En un grupo de trabajo toda la seguridad es administrada localmente en cada equipo. Cada máquina cuenta localmente con una lista de usuarios autorizados y con las contraseñas correspondientes. Es decir, se tiene un tipo de administración descentralizada ya que cada equipo es autónomo y no depende de un servidor porque tanto la autenticación como la autorización sobre los recursos se ejecutan localmente en cada equipo de cómputo.

1.2.1 Ventajas de los Grupos de Trabajo

Dentro de las ventajas que existen al utilizar una red en grupo de trabajo son las siguientes:

- Es fácil de diseñar e implementar y no requiere mayor conocimiento que cableado y creación de usuarios y recursos compartidos simples. En este sentido solo basta tener conectados nuestros equipos de cómputo a nuestro switch o router convencional.
- Está pensado en redes pequeñas y de fácil acceso al público donde la seguridad de los datos no se vea involucrada. La seguridad no importa mucho dado que se trata generalmente de una red doméstica.
- No se necesitan de servidores para realizar la autenticación.
- Es más barato utilizar un grupo de trabajo ya que los sistemas operativos de tipo servidor son más costosos que los sistemas operativos cliente.
- Su administración es sencilla.

1.2.2 Desventajas de los grupos de Trabajo

Aun con sus ventajas, los grupos de trabajo ofrecen serios inconvenientes a las personas que buscan tener una mejor administración de la red y seguridad. Entre los problemas más destacados siguientes:

- La SAM (Security Account Manager) debe administrarse y configurarse en cada uno de los equipos involucrados.

- Si se realiza algún cambio en uno de los equipos de cómputo, éste deberá ser actualizado y realizado en los demás equipos de cómputo.

- No es una red muy segura, ya que maneja cuentas de administrador local y estas pueden ser vulneradas al suplantar identidades y accesos.

- Algunos recursos compartidos pueden ser difíciles de localizar para los usuarios.

- Los recursos se comparten con un grupo limitado de colaboradores.

1.3 Servicios de Directorio

Un Directorio es una Base de Datos Distribuida que puede contener información acerca de personas, aplicaciones informáticas, organismos o empresas, etc., (Lightweight Directory Access Protocol (LDAP), s.f.)

El concepto de servicio de directorio no dista mucho de lo que es un directorio convencional, la mayoría de las personas ha utilizado en algún momento algún tipo de directorio, desde la guía telefónica hasta cualquier revista que contenga la programación televisiva. Utilizando estos ejemplos de la vida diaria se puede presentar el Directorio, y sus principales características.

1.4 Protocolo de DAP

DAP (Directory Access Protocol): El *Protocolo de Accesos al Directorio* fue el primer protocolo creado para establecer la comunicación entre un cliente y un servidor utilizando el servicio de directorio, pero debido a que DAP es un protocolo que trabaja sobre la capa de aplicación, tanto el cliente como el servidor debían implementar completamente el modelo OSI, además de otros inconvenientes en la implementación no permitieron al protocolo tener el uso deseado. Utiliza un protocolo de cliente servidor para la comunicación.

1.5 Protocolo de LDAP

El Protocolo Ligero de Acceso al Directorio (Lightweight Directory Access Protocol) es la versión mejorada del protocolo DAP, este protocolo surge como alternativa al protocolo DAP, ya que dicho protocolo presentaba algunas dificultades en la implementación, fue pensado originalmente para tener un accesos sencillo y rápido a los directorios basados en X.500 pero posteriormente LDAP hace algunas modificaciones basadas en DAP para crear un protocolo más consistente así como más fácil de adoptar en la implementación.

Una de los principales cambios es que LDAP utiliza TCP/IP en lugar de los protocolos OSI. Además, TCP/IP requiere menos recursos y una mayor disponibilidad.

Como se comenta, el modelo de LDAP es mucho más simple y elimina opciones e instrucciones que eran poco usadas en estándar X.500 (DAP). De este modo, LDAP es más fácil de comprender por lo que su implementación se vuelve más fácil.

Otra característica y diferencia es que LDAP representa la información mediante cadenas de caracteres en lugar de complicadas estructuras ASN.1 (Abstract Syntax Notation One) como DAP.

1.6 Dominio

Un Dominio es una agrupación de equipos de cómputo en torno a un servidor centralizado (o varios) que guarda una lista de objetos (usuarios, computadoras, impresoras, etc.) y de nivel de acceso de cada uno. (Microsoft, Dominio, grupo de trabajo y grupo en el hogar, s.f.)

El dominio utiliza los conceptos de grupo de trabajo y de los servicios de directorio, ya que como se mencionó antes, coloca los recursos en una única estructura organizativa (un servicio de directorio), de esta forma a los usuarios se les concede privilegios de conectarse a un dominio en lugar de conectarse a servidores independientes, como en el caso de un grupo de trabajo.

Los servidores que forman parte de un dominio muestran sus servicios a los usuarios y estos pueden conectarse a aquellos a los que se les ha concedido permiso. Así, se pueden observar los recursos del dominio de una mejor manera que en un grupo de trabajo.

1.6.1 Características de Dominios

Entre las características más distintivas de los dominios se observan las siguientes:

- Está conformado por objetos (usuarios, computadoras, impresoras), por naturaleza es más seguro que un grupo de trabajo debido a que sus contraseñas son cifradas y son monitoreadas constantemente por el Servidor de Dominio el cual centraliza la seguridad y administración de los recursos de la red.

- Uno o más equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y los permisos de todos los equipos del dominio. Así resulta más sencillo efectuar cambios, ya que éstos se aplican automáticamente a todos los equipos.

- Si dispone de una cuenta de usuario en el dominio, puede iniciar sesión en cualquier equipo del dominio sin necesidad de disponer de una cuenta local en dicho equipo.

- Probablemente solo podrá hacer cambios limitados a la configuración de un equipo porque los administradores de red con frecuencia desean garantizan un nivel de homogeneidad entre los equipos.

- Un dominio puede incluir miles de equipos.

- En un dominio esta implementado el concepto de directorio.

1.6.2 Ventajas de los Dominios

Dentro de las principales ventajas que tienen los dominios, se hace mención de las siguientes:

- Maneja una Base de Datos, la cual centraliza toda la información de las cuentas de los usuarios de la red y la mantiene segura a través del uso de distintos protocolos como LDAP y Kerberos.

- Las Cuentas ya no se encuentran almacenadas en la cuenta SAM, sino en la Base de Datos del Servidor.

- Gestiona y controla redes demasiado grandes y extensas.

- Al crear una cuenta de usuario, esta solo es realizada en el Controlador de Dominio (Domain Controller) y los equipos cliente se conectan a ella sin necesidad de crear ninguna cuenta en el equipo local.

- Los equipos pueden encontrarse en diferentes redes locales.

1.6.3 Desventajas

Así como presentan ventajas los Dominios sobre los grupos de trabajo, también tienen algunos pequeños inconvenientes como los siguientes:

- La cuenta SAM queda desactivada mientras la PC se encuentra conectada a un dominio
- Requiere conocimientos básicos de Protocolos, Direccionamiento de Números IP

- Está basado en reglas y lo primero que se debe hacer es diseñar la red antes de implementarla, incluyendo los servicios, la política de seguridad, etc.

- Si el dominio falla, toda la red replicara las fallas a las estaciones de trabajo.

1.7 Árbol

Se le denomina árbol a un conjunto de dominios y la relación de confianza que existe entre ellos con la finalidad de compartir recursos entre ellos, es decir al primer dominio de un árbol de dominio se le conoce como dominio raíz, y así todos los dominios que comparten el mismo dominio raíz formaran un nombre de espacios contiguo y será llamado árbol. (Microsoft, Active Directory Services and Windows 2000 or Windows Server 2003 Domains , 2007)

1.8 Bosque

El bosque se define de árboles de dominio donde existe una relación entre sí, puede que no exista un nombre de espacio contiguo entre los árboles dominios para formar un bosque pero sí existe esa relación de confianza entre los dominios raíz de cada árbol de dominio para poder crear o extender el bosque. (Microsoft, Active Directory Services and Windows 2000 or Windows Server 2003 Domains , 2007)

1.9 Relación de confianza

La relación de confianza se presenta cuando un dominio puede autenticar a usuarios de otro dominio. Para que se presente dicha relación de confianza debe existir un dominio en el que se confía y un dominio que confía. (Microsoft, Introducción a los Servicios de dominio de Active Directory, 2007)

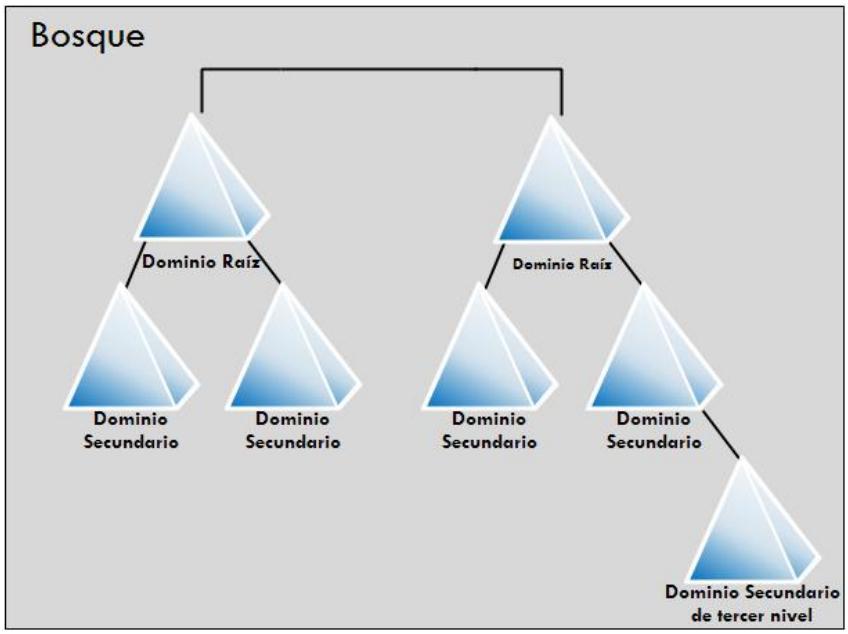

Figura 1. 7 ***Estructura de dominio, cualquiera de los dominios raíz dependiendo de la configuración puede ser el dominio raíz del bosque.***

1.10 Tipos de Servidores en un Dominio

En el dominio, al implementar el modelo cliente-servidor coloca los recursos en un servidor para que puedan ser accedidos por los equipos cliente, en este sentido un servidor de un dominio puede actuar de las siguientes maneras:

- **Controlador Principal de Dominio:** Es un servidor en donde se almacena la copia maestra de la base de datos del directorio, es decir, donde se guardan los datos de grupos, usuarios, etc., del dominio.

- **Controlador de Reserva de Dominio:** Es otro servidor en donde se almacena una copia de seguridad de la base de datos del directorio, generalmente esta copia es replicada por el controlador de principal de dominio cada determinado tiempo.

- **Servidor Independiente:** Es otro tipo de servidor que participa en el dominio con distintas finalidades, pueden ser desde compartir recursos, hasta albergar una base de datos o un sitio Web, etc., puede tener distintas funciones.

1.11 Servicio de DNS

DNS (Sistema de nombres de Dominio) es un sistema que permite la resolución de los nombre de dominio a direcciones IP y viceversa, es decir resuelve direcciones alfanuméricas (Ej.

www.unam.mx) a direcciones IP (132.248.10.44) y de IP a direcciones alfanuméricas. La utilidad de hacer esa resolución de nombres es porque resulta más fácil a una persona recordar una dirección alfanumérica que recordar una IP.

El DNS es una base de datos jerárquica distribuida la cual contiene información asociada a servicios o recursos conectados a Internet o a una red privada resolvieron la dirección o nombre a una IP. (Davies, 2003)

Un host de red necesariamente debe tener una dirección DNS con la finalidad de poder localizar a otro host en cualquier punto de la red, si un host hace una petición de resolución de nombre, el DNS hará la búsqueda llegando hasta el nodo raíz si es necesario e ir descendiendo en el árbol dependiendo del número de etiquetas que contenga las cuales están separadas por puntos, hasta encontrar el host destino (Figura 1.8).

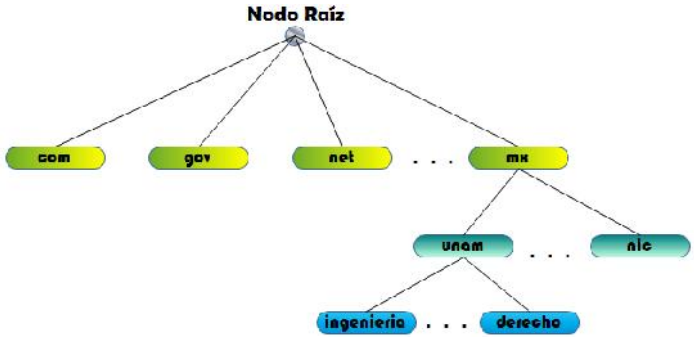

Figura 1. 8 *Localización del dominio ingenieria.unam.mx, la jerarquía más alta es la etiqueta del extremo derecho.*

1.12 Servicios de DHCP

DCHP (Protocolo de Configuración Dinámica de Host) es un protocolo de red que permite a un cliente de una red poder tomar sus parámetros de red automáticamente, es decir el servicio de DCHP asignará automáticamente los parámetros de red a cada uno de los clientes de la red. Un cliente pide una petición y el servidor recibe el mensaje y envía un mensaje de respuesta al cliente donde viene información sobre la configuración y el tiempo de vencimiento de la misma, después, el DCHP mantiene un registro de las direcciones que ha prestado para evitar repeticiones. (Davies, 2003)

La configuración que puede proveer un DCHP es: la dirección IP, dirección del servidor de DNS, puerta de enlace, Máscara de subred, tiempo máximo de espera de ARP, etc.

1.13 Seguridad en un Dominio

La seguridad en un dominio es un tema bastante importante y demasiado amplio. Para preservar la funcionalidad y salud de la red y el dominio es imprescindible seguir una serie de

recomendaciones y buenas prácticas de implementación tanto de reglas como de herramientas de seguridad.

Casi todos los esfuerzos de seguridad, a nivel de normas y del cumplimento de las mismas, están dirigidos a denegar el acceso a usuarios no autorizados. Si bien se trata de un objetivo muy sensato, es muy común que muchas de las infracciones las perpetren usuarios no autorizados, no obstante, no es el único objetivo de la seguridad.

1.14 Seguridad en Redes de Datos

Se puede entender y definir como seguridad al conjunto de acciones y herramientas para preservar y proteger algo que se considere importante, además se observa que la seguridad es una característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo que pudiese presentarse.

Acercando un poco más la definición a tópico de ésta tesis, se puede decir que la seguridad en redes de datos es mantener bajo protección los recursos y la información de la red, a través de procedimientos basados en mecanismos y políticas de seguridad tales que permitan el control de lo actuado.

Para lograr el objetivo de la definición planteada anteriormente se tienen que considerar previamente las siguientes cuestiones:

- ¿Qué se quiere proteger?
- ¿De qué se quiere proteger?

Una vez establecidas las respuestas a estas preguntas se puede elegir una manera de realizar acciones destinadas a la protección de nuestros bienes, para ello se hace uso de mecanismos de seguridad.

1.15 Mecanismos de Seguridad

Los mecanismos de seguridad son herramientas o controles que buscan preservar una serie de principios que son considerados básicos en la seguridad:

- **Integridad**: La integridad hace referencia la certeza de que la información no ha sido alterada, borrada, reordenada, copiada, etc., durante un proceso de transmisión.

- **Confidencialidad**: La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos.

- **Disponibilidad**: La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Además de los principios básicos, existen otros como "el no repudio" que se refiere a probar la participación de las partes en una comunicación bloqueo, previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido); y la autenticación que se refiere al proceso de detectar y comprobar la identidad de una entidad de seguridad mediante el examen de las credenciales del usuario y la validación de las mismas consultando a una autoridad determinada.

Los mecanismos utilizados para preservar lo anterior son:

- Aplicaciones
- Físicos
- Buenas Prácticas
- Reglas
- Estándares

Dentro de estos mecanismos se puede hacer uso de herramientas de control de acceso (ejemplo: sensores biométricos), métodos de autenticación (ejemplo: kerberos), cifrado de datos (ejemplo: métodos de criptografía simétrica y asimétrica con AES o DES), seguir los estándares internacionales (ejemplo: estándar 802.XX de redes inalámbricas), el cumplimiento de las políticas internas de la organización o institución, seguir las recomendaciones del fabricante en la implementación y configuración de herramientas de software, y el aseguramiento físico del área de trabajo.

1.16 Kerberos

Como se menciona con anterioridad, uno de los mecanismos de seguridad utilizados es el uso de herramientas de control de acceso y autenticación, en el caso de un dominio esta tarea es de gran importancia para preservar los principios de seguridad de la información. Una herramienta que ayuda en esta tarea es kerberos.

Kerberos es un protocolo de autenticación de red que permite que dos o más computadoras dentro de una red puedan comunicarse de una manera segura mediante criptografía de claves simétricas con la finalidad de no estar enviando las credenciales de usuario por la red.

Los objetivos principales de Kerberos son:

- Impide que las contraseñas sean enviadas a través de la red
- Centraliza la autenticación de usuarios, en una base de datos de usuarios única para toda la red.

Capítulo 2

Análisis de Requerimientos y Alternativas de Solución

Para proponer una solución unificada a los distintos problemas de administración de los equipos de cómputo del Laboratorio de Redes y Seguridad, se realizó un análisis y evaluación de las distintas situaciones que producen los problemas, esto con la finalidad de brindar un diagnóstico para resolver estas problemáticas.

2.1 Laboratorio de Redes de Datos y Seguridad.

El laboratorio de Redes y Seguridad de la Facultad de Ingeniería es un aula dedicada a la práctica y adquisición de conocimientos relacionados con las redes de datos y seguridad informática. Está ubicado en el Anexo de Ingeniería en el Edificio de Posgrado en el primer piso. Sus instalaciones se muestran en la figura 2.1

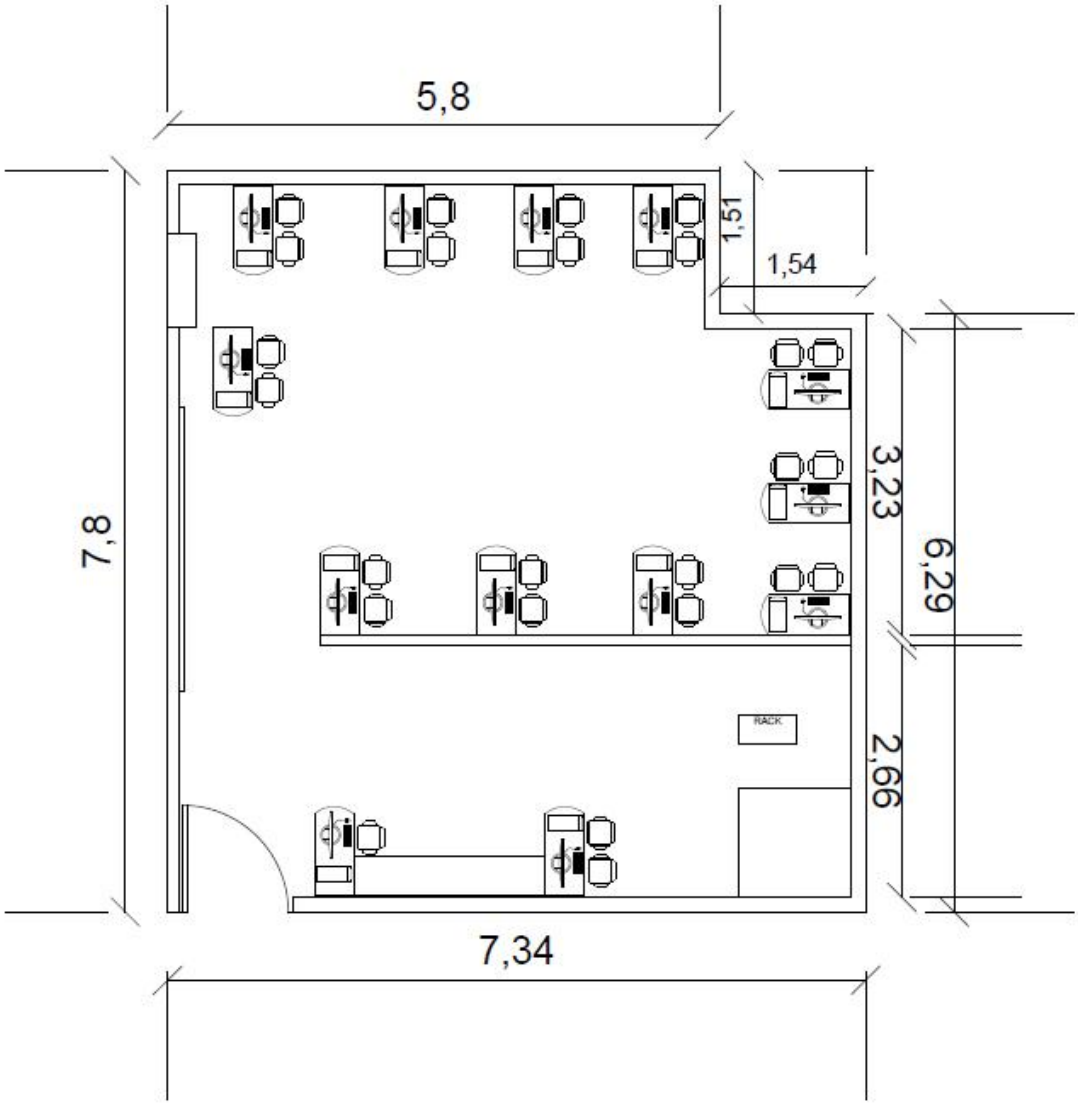

Figura 2. 1 Plano del Laboratorio de Redes y Seguridad de FI.

En sus instalaciones se imparten las asignaturas de laboratorio de Redes de Datos y Administración de Redes de Datos de la carrera de Ingeniería en Computación. En este laboratorio muchos alumnos cursan materias cada semestre, a los cuales se les proporciona un equipo de cómputo por parejas para realizar una serie de prácticas a lo largo del semestre.

El objetivo primordial del laboratorio según la página oficial del laboratorio (http://redyseguridad.fi-p.unam.mx) es el siguiente:

> "*Proveer una plataforma de trabajo en hardware y software a los estudiantes y profesores del área de redes de computadoras.*
> *Apoyar al alumno en el desarrollo de habilidades analíticas y funcionales para la creación, implantación, mantenimiento y administración de redes de computadoras mediante el seguimiento de las prácticas de las distintas materias del área.* "

Para la realización de las prácticas es indispensable instalar software necesario y configurarlo para efectuar las actividades solicitadas en cada una de ellas. El software instalado en los equipos de cómputo es el siguiente:

- Windows XP
- Linux-Debian
- Vecsim
- Office
- Avast
- Process Modeler
- Packet Tracer
- Crypto Forge
- AxCrypt
- MG-SOFT MIB Browser
- Opnet IT GURU
- Wireshark
- Asterisk
- X-Lite Softphone
- SSH
- Apache
- Open SSL
- Java JDK
- Joomla
- PHPMyAdmin
- MySQL

La Red de Datos del laboratorio cuenta en sus instalaciones con una red de Datos estructurada tanto cableada como inalámbrica. Dentro de su infraestructura cuenta con el equipo cómputo y telecomunicaciones listado en Tabla 2.1.

Tabla 2. 1 Equipo de Laboratorio de Redes y Seguridad

Cantidad	Descripción
2	Computadora Dell 170L Pentium 4 256 MB en RAM Monitor DELL E173FPc
3	Computadora HP DC5850 Dual Core 1.75 GB en RAM Monitor HP L1710
1	Computadora COMPAQ 7550 Monitor COMPAQ KB-0311
1	Computadora Dell GX260 Monitor Dell e551
2	Computadora Dell GX270 Pentium 4 640 MB en RAM Monitor Dell M783s
1	Computadora COMPAQ Presario SR1220LA Monitor COMPAQ 7550
1	Computadora HP DX5150MT Athlon 2 GB en RAM Monitor HP L1710
1	Computadora HP D220M Monitor HP 5500
1	Servidor HP Proliant DL160 G5 Monitor Dell E5510
1	Servidor DELL PowerEdge 1800 Xeon 2.79 GHz, 1GB Ram, 100 GB disco Duro

Además, todo el semestre es necesario brindar soporte a los equipos para mantenerlos funcionales durante las clases y prácticas.

Tiene un total de 10 equipos de cómputo dedicados a los alumnos para la realización de prácticas de las materias antes mencionadas, además en sus instalaciones se cuenta con equipo de telecomunicaciones como: un Switch CISCO, un Router Linksys, un Patch Panel, un par de servidores y algunos dispositivos móviles de profesores, ayudantes, estudiantes de servicio social.

2.2 Análisis del Problema.

Para realizar el análisis e identificación de la problemática en el laboratorio se utilizó la técnica de estudio “Entrevista”, la cual se llevó a cabo con la M.C. Cintia Quezada Reyes, administradora del laboratorio, ya que como administradora cuenta con una visión más cercana de las necesidades y problemas del laboratorio.

1.- ¿Qué servicios provee la red del laboratorio?

Dentro de los servicios que provee el laboratorio a sus usuarios tenemos el acceso a Internet, el uso de las computadoras para la realización de prácticas del laboratorio para las asignaturas de Redes de datos y Administración de redes; y también se lleva a cabo el curso de CISCO CCNA dentro de sus instalaciones.

2.- ¿A cuántos usuarios se le brindan estos servicios?

Aproximadamente cada semestre 410 alumnos, debido a que es un laboratorio, los estudiantes pueden intercambiar las computadoras que ocupan y así mismo, cada semestre son distintos usuarios.

3.- ¿Considera que la red de datos del Laboratorio es propensa a ataques de servicios?

Sí, no hay una seguridad al 100%, por ende es factible que existan esos ataques.

4.- ¿Cuál es el servicio que propicia más problemas?

El acceso a Internet, pues se depende de la red implementada en UNICA, si no hay acceso, el laboratorio tampoco lo tiene. Esta situación puede provocar retardos en la realización de las prácticas debido a que en ocasiones es necesario revisar algún sitio de Internet o descargar algún archivo.

5.- ¿Cuáles son los problemas más frecuentes? (Red lenta, IP´s repetidas, Servicios con respuestas lentas, saturación de servicios, los servicios se caen o fallan, otros a especificar)

Una de las principales problemáticas a las que se enfrenta el laboratorio en su uso, es la modificación en la configuración del sistema operativo, principalmente sobre Linux, ya que en algunas prácticas es requerido hacer algunas modificaciones al hardware del equipo como la tarjeta de Red. Esto provoca que los alumnos dentro de su curiosidad modifiquen archivos de configuración o borren archivos, carpetas o software sin querer del sistema operativo. Esta clase de modificación desemboca en no poder usar el equipo de cómputo y provoca retrasos en la elaboración de las prácticas durante las clases, por lo que corregir este tipo de problemas de manera rápida y eficiente es necesaria

Otro evento presentado usualmente es la presencia de malware, que si no es atendido a tiempo el problema puede desencadenar el bloqueo de la dirección IP. Estos problemas provocan una denegación del servicio de cómputo para realizar la práctica a algunos alumnos tomando clase.

6.- ¿Ha detectado algún ataque a la red de datos del Laboratorio o a algún servicio?

Sí, durante mi gestión en el semestre 2012-2 hubo una ataque provocado por malware instalado en 2 de los equipos del laboratorio. Este malware provocó el envío de paquetes saturando la red,

llegando incluso puede provocar una denegación del servicio de Internet. Este tipo de ataques se ha detectado que se presenta debido a la introducción de memorias USB infectadas en los equipos.

7.- ¿Qué tipo de vulnerabilidades y ataques ha identificado?

Durante mi gestión sólo se han detectado problemas de Malware que se han atendido oportunamente. De esta forma podemos identificar que una vulnerabilidad es que al ser un laboratorio, los estudiantes acceden a los equipos de cómputo con cuenta de administrador, esto provoca que al introducir memorias USB, el malware que puedan traer consigo afecte a los equipos.

Otro ataque es la modificación de los archivos de configuración del sistema operativo LINUX, provocando que el equipo no pueda ser utilizado correctamente durante las prácticas.

8.- Actualmente, ¿con qué medidas de seguridad cuentan en el Laboratorio?

Actualmente se cuenta con las siguientes medidas de seguridad: en las computadoras se tiene Antivirus y Firewall. En el laboratorio se tiene un reglamento y el uso de buenas prácticas con base en dicho reglamento, controles de acceso físico y lógicos.

En el control de accesos físico la puerta principal con doble chapa y un registro de entrada de cada usuario del laboratorio.

Para el control a los equipos se tienen 3 tipos de cuentas con diferentes privilegios, adicionalmente el laboratorio está dividido en 2 secciones: El Área Académica y el Área de Profesores. Al Área Académica tienen accesos los estudiantes y usuarios en general, al Área de Profesores solo pueden acceder profesores, estudiantes realizando su servicio social y tesistas. De esta forma en el Área Académica las computadoras tienen cuentas llamadas “Administrador”, “Estudiantes” y “Cisco” con contraseñas de administrador local en el equipo, pero estas cuentas no disponen de privilegios en servidor ni en las computadoras colocadas en el Área de Profesores.

En el Área de Profesores donde se ubica el servidor se cuenta con una cuenta especial de super usuario utilizada únicamente en dicho servidor y conocida solo por la administradora del laboratorio.

9.-En caso de alguna falla, ¿Cuánto tiempo tardan en promedio el solucionarlo?

Cundo se llega a presentar alguna falla se trata de corregir inmediatamente, el objetivo es que si la falla es muy grave se tarde menos de 24 horas en resolverlo. Esto es fundamental para el funcionamiento del laboratorio debido a que está en funcionamiento continúo por las clases que se imparten, así que en caso de fallo de algún equipo, si no se corrige oportunamente provoca el retraso en las prácticas para los alumnos.

10.- ¿Cree que es suficiente para proteger a la red de datos de los ataques?

Los más detectados sí, pero no son los únicos, recordar que no hay una seguridad total. Con esto no se descarta una actualización de algunos sistemas y la implementación de algunos mecanismos de seguridad adicionales a los que ya existen para aumentar el control sobre el laboratorio y poder brindar un mejor servicio corrigiendo algunos problemas.

11.- ¿Cree usted que sería útil tener un Dominio en el Laboratorio?

Sí, porque ayudaría a aumentar el nivel de seguridad pensando en las necesidades actuales del laboratorio y su desarrollo a futuro. Creo que puede proveernos de varios beneficios para automatizar ciertas tareas y tener una mejor administración del laboratorio con una menor carga de trabajo, lo que se traduciría en un laboratorio más eficiente.

2.3 Identificación de requerimientos.

Con las preguntas planteadas anteriormente se observa que el esquema de la red puede ser mejorado en muchos aspectos:

- Seguridad
- Funcionalidad
- Rendimiento
- Administración

Al revisar el escenario, se identifica que entre los principales problemas de los que adolece el laboratorio están los siguientes:

1. Desconfiguración del Sistema Operativo: Las computadoras usadas en el laboratorio de redes y seguridad son para uso educativo, es decir los estudiantes hacen uso de las mismas para realizar prácticas de las materias de Redes de Datos y Administración de Redes, con el fin de reafirmar sus conocimientos vistos en las clases de teoría, estas computadoras tienen instalado 2 sistemas operativos: Windows XP y Linux Debian. En algunas prácticas se requiere hacer algunas modificaciones a la configuración del sistema operativo, como por ejemplo asignación o cambio de IP's, compartir archivos mediante la red, instalación de Software, etc. En la mayoría de los casos se requiere el uso de cuentas de administrador local para poder realizar dichas modificaciones, esto conlleva a correr riesgos ya que un equipo se puede infectar por malware mediante un dispositivo USB o algún archivo descargado de la red o una modificación del mismo ya sea accidental o intencionalmente y por consiguiente es difícil detectar alguna falla de una manera rápida si es que el equipo aún puede utilizarse o se tenga que recurrir a reinstalar los sistemas operativos en el peor de los caso. Cabe señalar que sí un equipo del laboratorio deja de funcionar afectaría a los estudiantes directamente ya que no podrán realizar sus prácticas de manera óptima y se pudiera perder el objetivo principal de las mismas.

2. Modificación del funcionamiento normal del software instalado: Cada equipo cuenta con el software necesario para poder realizar actividades específicas dentro del laboratorio, la mayoría de las veces es instalado por el encargado del laboratorio, debido a la manipulación de los programas instalados en ocasiones se llega a desconfigurar y es más fácil desinstalar y reinstalar el software, generalmente suele ser muy justo el tiempo ya que existen alumnos de otro grupo de alumnos esperando a realizar la práctica que le corresponde y sí el equipo tiene problemas con sus programas instalados puede llegar a retrasar e inclusive cancelar la práctica para ese par de alumnos que hacen uso de ese equipo en particular, por lo cual deben integrarse por lo menos con otros 2 compañeros para realizar la práctica lo cual conlleva a que sean muchas personas manipulando una sola computadora y no todos obtengan el mismo nivel de conocimiento. Entre el software instalado se encuentra: CryptoForge, NetBeans, Opnet, PacketTracer, WireShark, MIB Browser.

3. Insuficiencia de tiempo para administrar todos los equipos: Este problema se presenta comúnmente, ya que el administrador del laboratorio tiene un tiempo reducido para la administración debido a las múltiples actividades que se le presentan dentro de la Facultad, como por ejemplo las actividades en la docencia en cada uno de los grupos asignados. Entre las actividades están dar clase, revisar tareas, exámenes, proyectos, etc., por lo que en ocasiones es difícil y complicado llevar la administración de los equipos del laboratorio de una manera descentralizada, ya que se toma más tiempo en revisar cada una de las computadoras.

4. Alta susceptibilidad a ataques informáticos por parte de los usuarios del laboratorio: Como cualquier equipo de cómputo se está expuesto a ataques de malware ya sea accidental o malintencionados al introducir memorias USB infectadas o al navegar o descargar programas no permitidos desde Internet ya que no existe una restricción de los sitios que se visitan ni de archivos que se descargan.

5. Falta de identificar a los usuarios responsables de cada equipo de cómputo por clase: Debido a que no se utilizan perfiles de usuario, las cuentas utilizadas siempre son las mismas, por lo tanto no se lleva un control sobre que usuarios hacen el uso del equipo, es decir se crea una cuenta restringida y una con privilegios de administrador en cada uno de los equipos, si se llega a presentar algún problema es difícil restaurar un perfil sobre todo si se trata del administrador, las cuentas con privilegios de administrador pueden manipular el equipo sin restricciones, si el perfil se daña es difícil restaurarlo, o crear algún otro, generalmente se reinstala el equipo por lo cual se requiere de mucho tiempo.

6. Utilización del equipo de cómputo para actividades no permitidas durante la clase: Debido a que no se tiene una restricción del equipo, los alumnos pueden hacer uso indebido del equipo como por ejemplo las actividades de ocio entre ellas están la instalación y/o

ejecución de software no permitido como juegos, navegar en páginas no permitidas como lo son las redes sociales (Facebook, Hi5, Twitter, MSN, etc.), con contenido multimedia como Youtube, etc.

7. Un alto tiempo de respuesta para la resolución de problemas técnicos en los equipos de cómputo: Como ya se mencionó anteriormente, el tiempo para poder restablecer un equipo es muy corto ya que las clases en laboratorios casi son continuas, un equipo podría no estar disponible hasta en un par de horas tiempo en el que se reinstala el sistema operativo y el software necesario para realizar alguna actividad en el mismo.

8. Nulo control de seguridad al compartir archivos: Los equipos no tienen un control estricto de con quién o con qué equipo compartirán archivos o carpetas. Para hacerlo se requiere agregar al equipo local cada cuenta de los usuarios de cada computadora para poder compartir de forma segura, o simplemente se omite la autenticación, hecho que provoca que se corra el riesgo de que los equipos se contagien de virus o malware desencadenando que el solucionar dicho problema sea tardado.

2.4 Alternativas de solución.

Una vez identificados todos los problemas del laboratorio, se llegó a la conclusión de que con este trabajo de tesis se pueden resolver los siguientes puntos:

1. Desconfiguración del Sistema Operativo.
2. Modificación del funcionamiento normal del software instalado.
3. Alta susceptibilidad a ataques informáticos por parte de los usuarios del laboratorio.
4. Un alto tiempo de respuesta para la resolución de problemas técnicos en los equipos de cómputo
5. Nulo control de seguridad al compartir archivos.

Este tipo de problemática corresponde a los equipos de cómputo y al servicio de administración de estos. Por ello, con este trabajo de Tesis se pretende mejorar estas situaciones. Los puntos que no son abarcados son problemas de seguridad física que si bien se pueden mejorar, no son del alcance de este trabajo.

2.5 Análisis de factibilidades

Para proponer una solución unificada a los distintos problemas de administración de los equipos de cómputo del Laboratorio de Redes y Seguridad, se realizó un análisis y evaluación de las distintas situaciones que producen los problemas, así como de la factibilidad de resolverlos con el equipo disponible.

Para mejorar la red del laboratorio de la Facultad de Ingeniería se propone la implementación de un Dominio, esto ya que se adecua para resolver varios problemas detectados en la entrevista y en análisis hecho del funcionamiento del laboratorio:

- Al tener un dominio en la red, es posible administrar tanto equipos de cómputo, usurarios y otros recursos como impresoras de manera centralizada, esto ahorra un gasto en tiempo de administración de la red.

- Con cuentas de usuario individuales es posible administrar la seguridad sobre los equipos de cómputo por grupos de seguridad conformados por los alumnos de cada clase, con esto el manejo de los permisos es altamente personalizable, lo que provee a la red de un entorno más seguro. Además, brinda la posibilidad de un mejor manejo y aplicación para compartir recursos y archivos de una forma más óptima.

- Con cuentas de usuario individuales a los alumnos, es posible tener un registro de los eventos sucedidos en los equipos, esto con la finalidad de contar con información suficiente sobre los posibles responsables del mal funcionamiento de un equipo de cómputo.

- Para prevenir la desconfiguración del sistema operativo (SO) se propone limitar los privilegios de los usuarios, esto por medio de las Políticas de Grupo (Group Policy) de Windows Server. Esto es a cierto nivel, ya que hay que tomar en consideración que como laboratorio es imprescindible que los alumnos realicen algunos cambios a los equipos para algunas prácticas.

- Para evitar problemas en la instalación y utilización del software, se propone distribuirlo vía red y administrarlo centralmente por el servidor con Políticas de Grupo (Group Policy). Esto hace más eficiente y rápido el formateo de los equipos y la puesta en marcha de estos para su uso en clase.

- Para realizar una instalación más eficiente del Sistema Operativo (SO) en los equipos utilizados por los alumnos, se propone distribuirlo vía red, el cual es posible administrar centralmente también haciendo uso también de las Políticas de Grupo, sin afectar los demás sistemas operativos instalados.

Capítulo 3
Instrumentación del Dominio

3.1 Selección de Herramientas

La selección de herramientas se lleva a cabo para poder lograr un diseño como el que se plantea en la figura 3.1. Este diseño es el propuesto para ayudar al laboratorio a contrarrestar los problemas identificados.

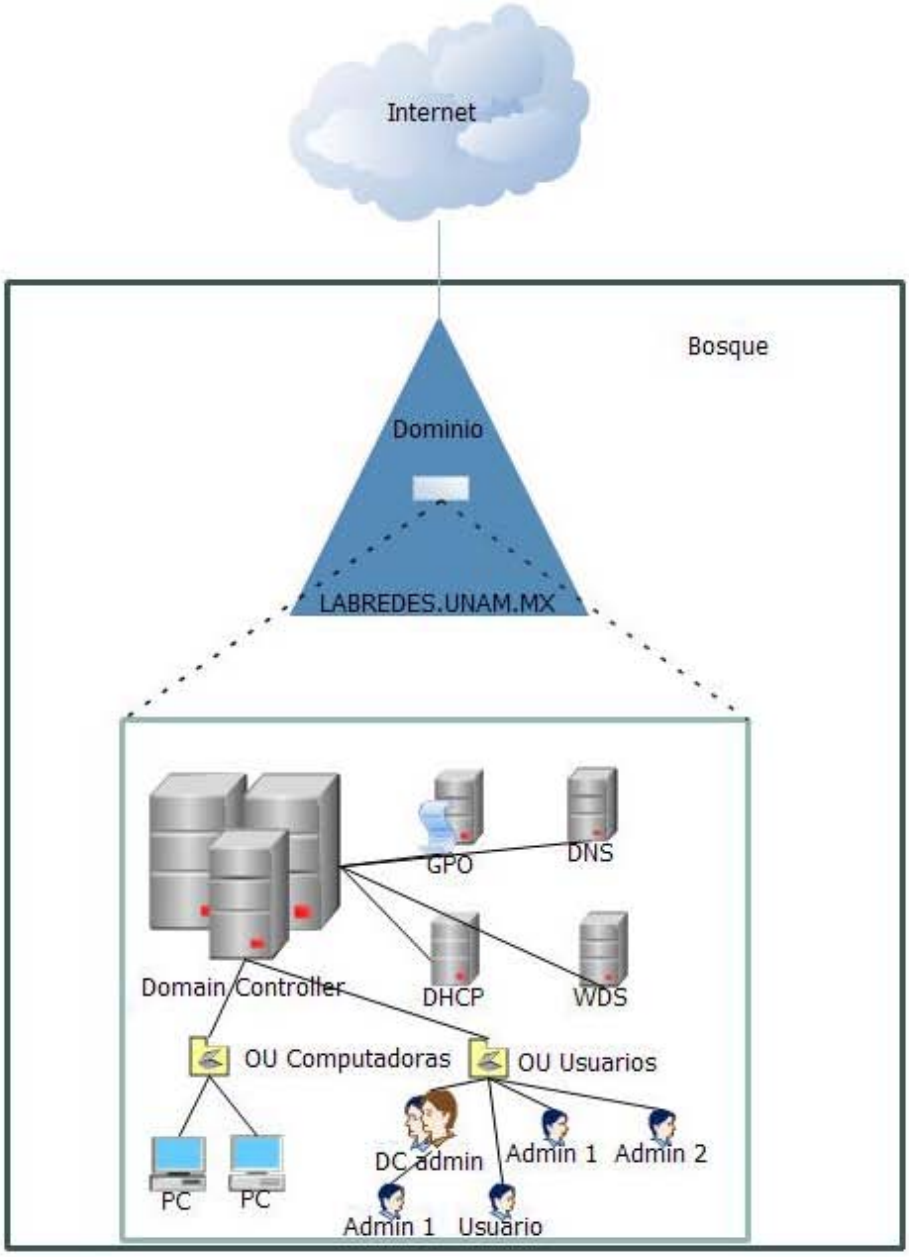

Figura 3.1 *Diagrama de la infraestructura a implementar*

Otra vista de la propuesta es la que se observa en la figura 3.2.

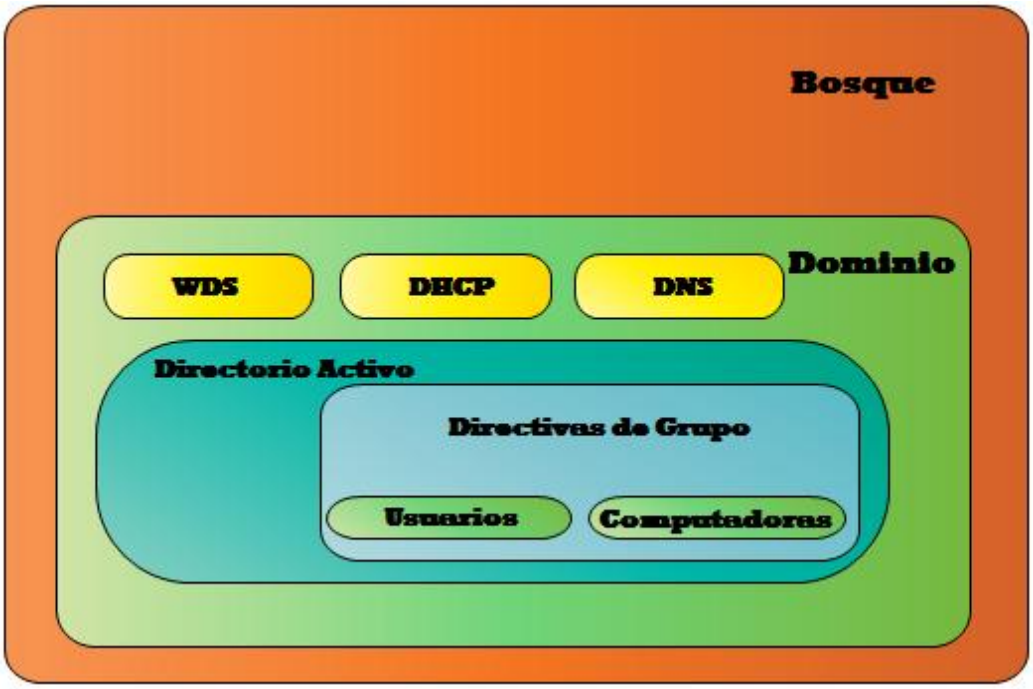

Figura 3.2 *Diagrama de Bloques de la Infraestructura a implementar*

Una vez revisado el diseño a implementar se procede con la elección de las herramientas que conformarán la infraestructura del dominio.

3.2 Sistema Operativo

Existen tres alternativas a la hora de elegir un sistema operativo para un servidor Web: Microsoft, Unix y Linux.

Para este trabajo de tesis se ha elegido el sistema operativo “Windows Server 2008” en su versión “Standard Edition”. Debido a las ventajas de utilizar este sistema operativo entre las que destacan las siguientes:

- Su implementación proporcionan en primer lugar una completa integración de todos los servicios que se escojan (los servicios Web IIS que interactúan con servidores de correo Exchange, bases de datos con SQL Server, virtualización con Hyper V, así como con nuevos entornos de desarrollo como la tecnología .NET) por ejemplo.
- Además de lo anterior los productos de Microsoft proporcionan una interfaz de manejo, configuración y administración que es relativamente sencilla de utilizar, por lo que la

inversión en tiempo y desgaste en horas hombre es menor, y por tanto esto se ve reflejado en el costo de mantener funcionando la arquitectura

- Ofrece un ambiente seguro y de fácil administración.

- Provee de varias herramientas de soporte, y de bastante información de soporte en línea en su sitio oficial.

- Proporciona más control sobre la infraestructura de red, lo que permite centrarse en necesidades críticas.

- Otra ventaja más de escoger las soluciones de Microsoft es que el costo de la mayoría de los productos es ajustado, en este caso es una alternativa muy viable debido al convenio que hay entre dicha empresa y la UNAM. Con este convenio, Microsoft proporciona gran parte de sus productos para poder ser utilizados en ambientes académicos sin ningún costo.

- Está diseñado para ofrecer una plataforma de virtualización de cargas de trabajo.

- Permite el alojamiento confiable de aplicaciones y servicios Web.

- La más reciente versión Windows Server 2008 R2, incluye nuevas funcionalidades que permiten la automatización de muchas tareas, así como una poderosa consola de línea de comandos llamada “PowerShell”.

Con el sistema operativo existe la posibilidad de agregar varias herramientas las cuales se muestran en la tabla 3.1 según la versión del sistema operativo que se instale, dadas las necesidades del laboratorio para este trabajo se eligió e instaló la versión “Standard Edition”.

Tabla 3. 1 Roles disponibles por versión de sistema operativo

KEY: ○ = Not Available ◉ = Partial/Limited ✔ = Full

Server Role	Enterprise	Datacenter	Standard	Itanium	Web	Foundation	HPC
Active Directory Certificate Services	✔	✔	◉ 1	○	○	◉ 1	◉ 1
Active Directory Domain Services	✔	✔	✔	○	○	✔	✔
Active Directory Federation Services	✔	✔	○	○	○	○	○
Active Directory Lightweight Directory Services	✔	✔	✔	○	○	✔	○
Active Directory Rights Management Services	✔	✔	✔	○	○	✔	○
Application Server	✔	✔	✔	✔	○	✔	○
DHCP Server	✔	✔	✔	○	○	✔	✔
DNS Server	✔	✔	✔	○	✔	✔	✔
Fax Server	✔	✔	✔	○	○	✔	○
File Services	✔	✔	◉ 2	○	○	◉ 2	◉ 2
Hyper-V	✔	✔	✔	○	○	○	✔
Network Policy and Access Services	✔	✔	◉ 3	○	○	◉ 5	◉ 3
Print and Document Services	✔	✔	✔	○	○	✔	○
Remote Desktop Services	✔	✔	◉ 4	○	○	◉ 6	◉ 4
Web Services (IIS)	✔	✔	✔	✔	✔	✔	✔
Windows Deployment Services	✔	✔	✔	○	○	✔	✔
Windows Server Update Services (WSUS)	✔	✔	✔	○	○	✔	✔

HPC Edition is limited in use to running clustered HPC applications or providing job scheduling services for HPC applications.

1 Limited to creating Certificate Authorities – no other ADCS features (NDES, Online Responder Service). See ADCS role documentation on TechNet for more information.

2 Limited to 1 standalone DFS root.

3 Limited to 250 RRAS connections, 50 IAS connections and 2 IAS Server Groups.

4 Limited to 250 Remote Desktop Services Gateway connections.

5 Limited to 50 RRAS connections, 10 IAS connections.

6 Limited to 50 Terminal Service Gateway connections.

Para realizar la instrumentación del dominio se debe de tener la arquitectura adecuada con los siguientes servicios andando:

- Servidor con un Controlador de Dominio (Domain Controller)
- Servidor con un DHCP
- Servidor con un DNS

Cabe señalar que un dominio puede albergar otros servicios además de los anteriores como lo ilustra la figura 3.3.

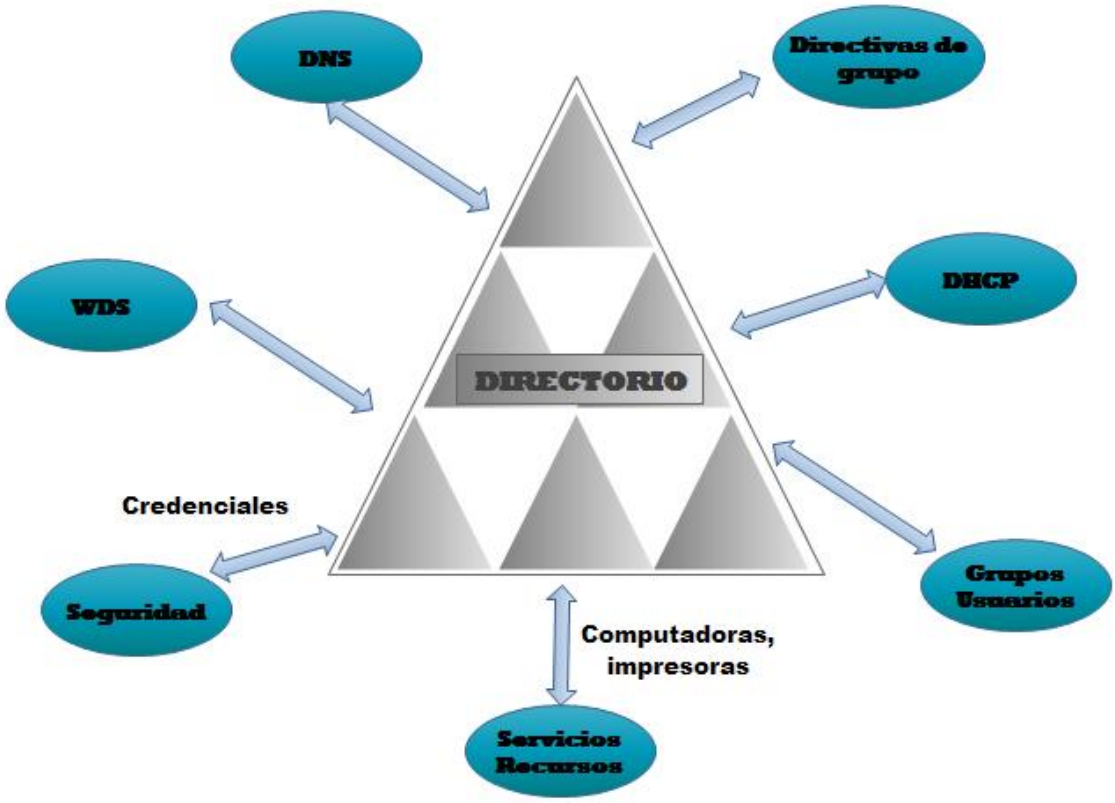

Figura 3.3 *Recursos y Servicios del dominio*

3.3 Directorio Activo

Dentro del Controlador de Dominio (DC) se encuentra la parte medular del Dominio, la cual es el servicio de directorio.

Algunas opciones para la implementación del servicio de directorio con LDAP que pueden ser ocupadas, entre las principales están las siguientes:

- Microsoft Active Directory
- Novell Directory Services
- Open LDAP
- Red Hat Directory Server
- Apache Directory Server

De entre estas opciones se ha elegido la versión de Microsoft, llamada **Active Directory**, esto debido a que ofrece varias ventajas sobre otras versiones del mercado:

- Active Directory es un producto posicionado en el mercado, demostrado así por sus más de 10 años, lo que hace que sea un producto probado y es estable.
- Es fácil de instalar ya que tiene un asistente que facilita su implementación con las herramientas necesarias para su funcionamiento (Kerberos, Directivas de grupo, Ldap, entre otras), es decir se trata de una solución integral. Un ejemplo esquemático y simplificado de esto es el de la figura 3.4.
- Los productos de Microsoft desde su desarrollo están pensados para convivir con el resto de sus otros productos (compatibilidad para la administración del sistema operativo)
- La UNAM y la Facultad de Ingeniería tiene convenios con Microsoft por lo cual el licenciamiento es gratuito.
- Con una sola licencia del sistema operativo Windows Server 2008, se puede hacer uso de los todos los demás roles disponibles (DNS, DHCP, WDS, ISS, FTP, etc.) sin costo extra.
- El Soporte de Microsoft es bastante amplio con muchos sitios y foros.
- Es una solución escalable y su posible migración a versiones superiores no es complicada.
- Provee de una administración centralizada.
- Permite la delegación de la administración.
- Reduce la carga de la Administración.

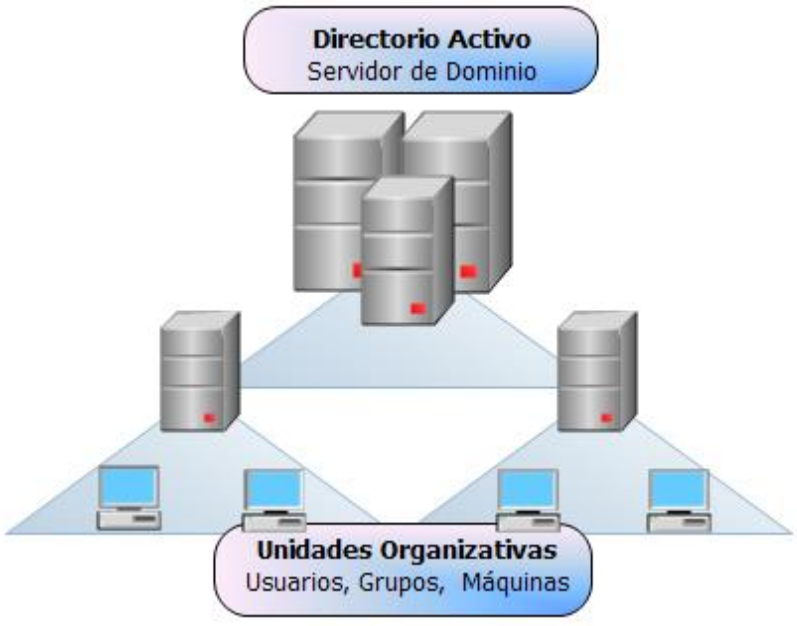

Figura 3.4 *Esquema del Servicio de Active Directory*

3.4 Servidor de Sistema de nombres (DNS)

El servidor de DNS es una base de datos jerárquica y distribuida que contiene asignaciones de nombres de dominio DNS a varios tipos de datos, tales como direcciones IP. Con Windows Server 2008, el nuevo servicio de servidor DNS incluye una nueva carga de zona de fondo, mejoras para la compatibilidad con IPv6, compatibilidad para controladores de dominio de sólo lectura (RODC) y la capacidad de alojar nombres globales de una sola etiqueta.
Por integración y las siguientes características se ha elegido el servicio de DNS integrado a Windows, que mejoran el rendimiento del servidor o agregan una nueva funcionalidad:

- Proporciona la carga de zonas en segundo plano: Los servidores DNS que alojan grandes zonas DNS almacenadas en Servicios de dominio de Active Directory (AD DS) pueden responder con mayor rapidez a las consultas de los clientes al reiniciarse ya que ahora los datos de zona se cargan en segundo plano.

- Tiene compatibilidad con el protocolo IP versión 6 (IPv6): El servicio Servidor DNS es ahora totalmente compatible con las direcciones largas de la especificación IPv6.

- Tiene compatibilidad con controladores de dominio de solo lectura (RODC): La función Servidor DNS en Windows Server 2008 ofrece zonas de solo lectura principales sobre RODC.

- Ocupa nombres globales individuales: La zona llamada “GlobalNames” ofrece resolución de nombres de etiqueta única para grandes redes de empresa que no utilizan el Servicio de nombres Internet de Windows (WINS). La zona GlobalNames es útil cuando no resulta práctico el uso de sufijos de nombres DNS para ofrecer resolución de nombres de etiqueta única.

- Lista global de consultas bloqueadas: los clientes de protocolos como el protocolo WPAD (detección automática de Proxy Web) y el protocolo ISATAP (Intra-site Automatic Tunnel Addressing Protocol) que se basan en la resolución de nombres DNS para resolver nombres de host conocidos son vulnerables a usuarios malintencionados que usan la actualización dinámica para registrar equipos host como si fueran servidores legítimos. La función de servidor DNS en Windows Server 2008 proporciona una lista global de consultas bloqueadas que ayuda a reducir esta vulnerabilidad.

3.5 DHCP

Es sabido que todos los dispositivos en una red basada en TCP/IP deben tener una dirección IP para tener acceso a la red y sus recursos. Sin DHCP, direcciones IP para equipos nuevos o que se mueven de una subred a otra deben configurarse manualmente; o las direcciones IP que se quitan de la red deben ser reclamadas también manualmente, todo esto genera carga de trabajo innecesaria.
Con el servicio de DHCP, todo este proceso está automatizado y administrado de forma centralizada.

El servidor DHCP almacena la información de configuración en una base de datos que incluye:

- Parámetros de configuración de TCP/IP válidos para todos los clientes de la red.
- Direcciones IP válidas, se mantienen en un grupo de asignación a clientes, así como excluir direcciones.
- Direcciones reservadas de IP asociadas con determinados clientes DHCP. Esto permite la asignación coherente de una única dirección IP a un único cliente DHCP.
- La duración de la concesión o la longitud de tiempo para el que se puede utilizar la dirección IP antes de que se requiere una renovación de concesiones.

En Windows Server 2008, el servicio servidor DHCP proporciona las siguientes ventajas:

- **Configuración de direcciones IP fiables**. DHCP minimiza los errores de configuración causados por configuración manual de la dirección IP, como, por ejemplo, errores tipográficos, o solucionar los conflictos causados por la asignación de una dirección IP a más de un equipo al mismo tiempo.

- **Administración de red reducida**. DHCP incluye las siguientes características para reducir la administración de red:

    - Configuración de TCP/IP centralizada y automatizada.

    - La capacidad para definir configuraciones de TCP/IP desde una ubicación central.

    - La capacidad para asignar una gama completa de valores de configuración de TCP/IP adicionales por medio de las opciones de DHCP.

    - El manejo eficiente de los cambios de dirección IP para los clientes que deben actualizarse con frecuencia, tales como los de los equipos portátiles que se mueven a ubicaciones diferentes en una red inalámbrica.

    - El reenvío de mensajes DHCP iniciales mediante el uso de un agente de retransmisión DHCP, lo que elimina la necesidad de un servidor DHCP en cada subred.

3.6 WDS

El WDS o “Servicios de implementación de Windows de Windows Server 2008” es una versión actualizada y rediseñada de herramienta anterior llama “Servicios de instalación remota (RIS)”. El WDS permite implementar sistemas operativos Windows, en especial Windows Vista, Windows 7 y Windows Server 2008. A pesar de esto no excluye al sistema operativo XP.
WDS requiere de la previa instalación y configuración de las herramientas Active Directory, DHCP y DNS. El WDS admite la implementación de imágenes en formato .wim y .vhd. Es posible usarlo para configurar equipos nuevos mediante una instalación basada en red. Esto significa que no es necesario estar físicamente presente en cada equipo ni tampoco instalar cada sistema operativo directamente desde un CD o DVD.

Servicios de implementación de Windows ofrece las siguientes ventajas en cuanto a instalación e implementación:

- Reduce la complejidad de las implementaciones y los costos asociados a procesos de instalación manual ineficaces (inversión de tiempo y mano de obra).
- Permite la instalación basada en red de los sistemas operativos Windows, como Windows Vista, Windows 7, Windows XP y Windows Server 2008.
- Implementa imágenes de Windows en equipos que no tienen sistema operativo.
- Admite entornos mixtos que incluyen Windows Vista, Windows Server 2008, Microsoft Windows XP y Microsoft Windows Server 2003.
- Proporciona una solución completa para la implementación de sistemas operativos Windows en equipos cliente y servidores.
- Usa tecnologías de configuración de Windows Server 2008 estándar, como Windows PE, archivos .wim e instalación basada en imagen.

3.7 Instrumentación del Dominio

Para la implementación es necesario considerar que el servidor cumpla los siguientes requisitos de hardware que se presentan en la tabla 3.2:

Tabla 3. 2 Requisitos de Hardware Windows Server 2008 R2

Componente	Requisito
Procesador	Mínimo: 1 GHz (procesador x86) o 1.4 GHz (procesador x64). Nota: se requiere un procesador Intel Itanium 2 para Windows Server 2008 para sistemas basados en Itanium
Memoria	Mínimo: 512 MB RAM Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (Enterprise Datacenter) Máximo (sistemas de 64 bits): 8 GB (Foundation) o 32 GB (Standard) o 2 TB (sistemas basados en Enterprise, Datacenter e Itanium)
Requisitos de espacio en disco	Mínimo (sistemas de 32 bits): 20 GB o más Mínimo (sistemas de 64 bits): 32 GB o más Foundation: 10 GB o más
Pantalla	Super VGA (800 × 600) o monitor de mayor resolución
Otros	Teclado y Mouse de Microsoft o dispositivo compatible

*Nota: Los requisitos actuales variarán con base en la configuración del sistema, las aplicaciones y características que se deseen instalar. El rendimiento del procesador depende no sólo de la frecuencia de reloj del procesador sino del número de núcleos y el tamaño del caché del procesador. Los requisitos de espacio en disco para la partición del sistema son aproximados. Los sistemas operativos basados en Itanium y x64 varían de estos estimativos de tamaño de disco. Se puede requerir espacio en disco disponible adicional si realiza la instalación sobre una red.

Por otro lado los requisitos para que los equipos cliente del laboratorio puedan soportar la instalación vía red son los siguientes:

- Memoria RAM de 512 MB como mínimo
- Procesador de
- Disco duro con 10 GB de espacio libre mínimo
- Compatibilidad con tecnología PXE

Nota: Todos los datos utilizados en esta sección de instrumentación no son reales, son datos y configuraciones demostrativos para ilustrar el trabajo realizado.

El equipo con el que se cuenta en el laboratorio listado en el capítulo 1 dispone de los requisitos mínimos para poder llevar a cabo la instalación y configuración de las herramientas necesarias para el dominio.

Después de considerar lo anterior se recomienda seguir estos pasos para preparar el equipo servidor.

• Se realiza una comprobación de la compatibilidad de aplicaciones: Como ayuda con esta tarea, se utiliza el Kit de herramientas de compatibilidad de aplicaciones de Microsoft. Aunque se utiliza principalmente para proporcionar información de compatibilidad sobre las aplicaciones de red, también puede utilizarlo con el fin de prepararse para Windows Server 2008.

• Desconectar los dispositivos SAI (UPS, o alimentación eléctrica): Si tiene conectado un sistema de alimentación ininterrumpida (SAI o UPS) al equipo de destino, desconecte el cable serie antes de ejecutar el programa de instalación. El programa de instalación intenta detectar automáticamente los dispositivos conectados a los puertos serie y los equipos SAI (UPS) pueden causar problemas en el proceso de detección. En el caso del laboratorio no existe dispositivos de esta naturaleza, por lo que se puede omitir este paso, pero es necesario hacer mención para futuras ocasiones en las que se pudiesen agregar estos dispositivos a la infraestructura del laboratorio.

• Realizar una copia de seguridad del servidor: Las copias de seguridad deben incluir todos los datos y toda la información de configuración que necesita el equipo para funcionar. Cuando realice las copias de seguridad, no olvidar incluir las particiones de arranque y del sistema, así como los datos del estado del sistema. Otra forma de realizar copias de seguridad de la información de configuración es crear un conjunto de copia de seguridad para la recuperación automática del sistema.

• Ejecutar la Herramienta de diagnóstico de memoria de Windows: Se debe ejecutar esta herramienta para probar la memoria de acceso aleatorio (RAM) del equipo. Con esta acción se comprueba el estado y la capacidad disponible de la memoria RAM.

• Revisar si es necesario proporcionar los controladores de almacenamiento masivo: Si el fabricante proporciona un archivo de controlador independiente, guárdelo en un disquete, CD, DVD o unidad flash USB (bus serie universal) en el directorio raíz del medio o en una de las

siguientes carpetas: amd64 para los equipos basados en x64, i386 para los equipos de 32 bits o ia64 para los equipos basados en Itanium. Para proporcionar el controlador durante la instalación, en la página de selección de disco, haga click en Cargar controlador (o presione F6). Puede buscarse el controlador o dejar que el programa de instalación lo busque en el medio. En el caso del laboratorio el disco de instalación ya cuenta con los controladores necesarios para poder realizar la instalación sin problemas.

• Tomar en cuenta que el Firewall de Windows está activado de manera predeterminada. Las aplicaciones de servidor que deben recibir conexiones de entrada no solicitadas generarán errores hasta que cree reglas de entrada del firewall que las admitan. Para este caso no existe inconveniente.

Una vez revisado los puntos anteriores satisfactoriamente se procede con la instalación introduciendo el disco en el servidor, con esto al encender el servidor comienza el proceso de carga de los archivos de instalación.

Posteriormente aparecerá un asistente que guía durante el proceso de instalación como se ilustra en la figura 3.5.

Figura 3.5 *Pantalla inicial del asistente de instalación.*

Con este asistente se debe elegir el idioma y la configuración personal.

Posteriormente se solicita la clave del producto la cual se debe fue proporcionada por el laboratorio de Microsoft de la Facultad de Ingeniería.

Hecho lo anterior se elige la versión de instalación que en este trabajo es “Instalación completa” como se muestra en la figura 3.6.

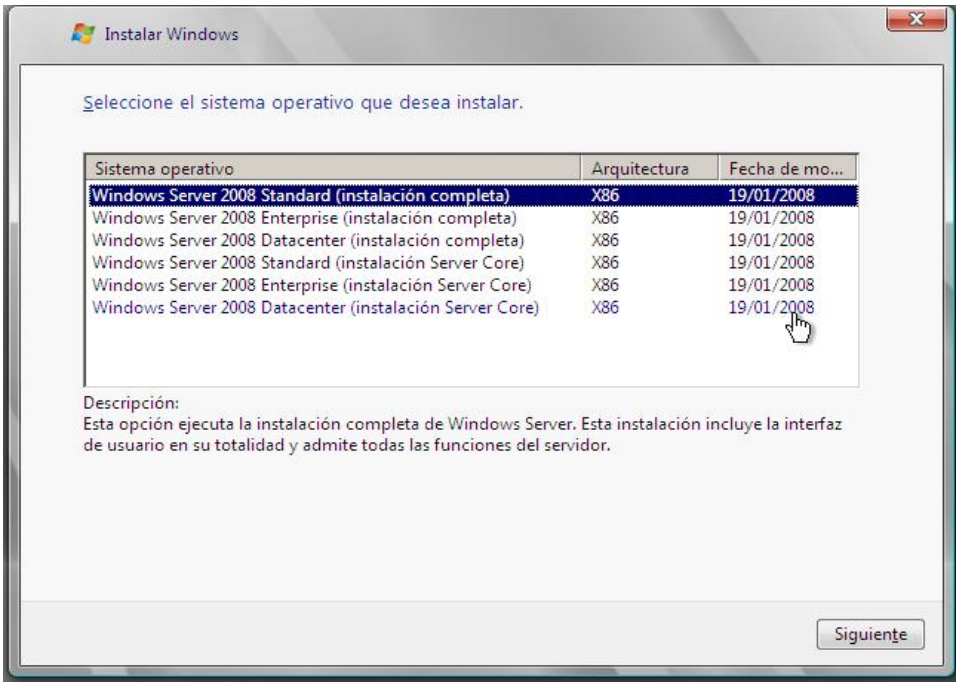

Figura 3. 6 *Pantalla de selección de versión de Sistema Operativo*

Se aceptan los términos de la licencia del Sistema operativo y se elige la opción de "Instalación Personalizada (Avanzada)".

Se elige la unidad de almacenamiento para el sistema operativo y se procede con la instalación.

Por último, al inicio del sistema operativo se definen una contraseña para el usuario administrador local en la pantalla 3.7.

Figura 3. 7 *Pantalla de definición de contraseña*

Después de la instalación del sistema operativo es necesario realizar la configuración del servidor con los siguientes parámetros que ilustran la figura 3.8 y 3.9:

Nombre del Servidor: Hera

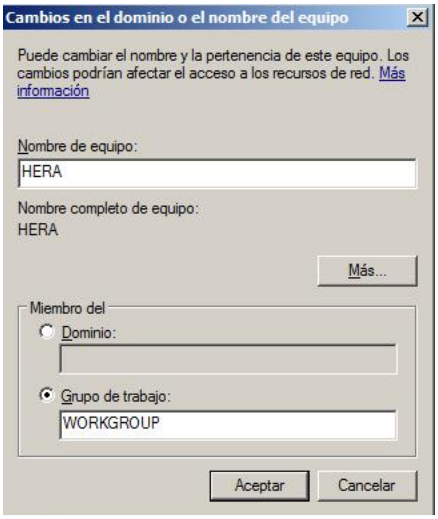

Figura 3. 8 *Pantalla de definición del nombre del servidor*

Parámetros de Red Fijos:

- Dirección IP fija (192.168.2.132)
- Máscara de red (255.255.255.0)
- una puerta de enlace o Gateway (192.168.2.254)
- y un par de servidores de DNS (172.16.100.1), en este caso los datos del DNS y el Gateway son iguales debido a este servidor proveerá de dichos servicios.

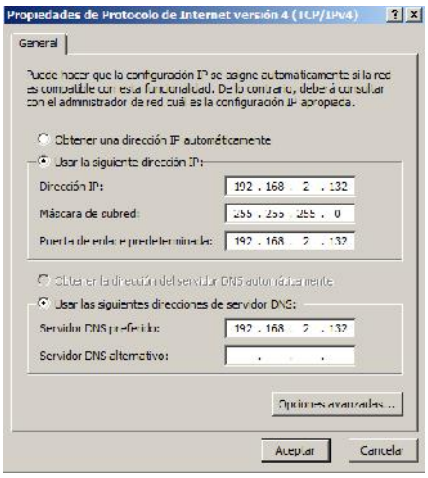

Figura 3. 9 *Parámetros de red*

Cabe señalar que se recomienda ampliamente antes de instalar cualquier rol de Windows Server, instalar todas las actualizaciones del sistema operativo por lo cual los parámetros de red,

específicamente el servidor de DNS se tendrá que usar los DNS de la UNAM para poder tener conexión a Internet. Esto se hace con la finalidad de contar con las herramientas más actualizadas.

3.8 Active Directory y DNS

Posteriormente se requiere la instalación del servicio de directorio llamado "Active Directory" que es el pilar fundamental de la instrumentación de un dominio. Es posible instalar el rol de servidor DNS (Servidor de Sistema de nombres) cuando se instala el rol Servicios de dominio de Active Directory (AD DS). Éste es el método preferido para instalar el rol de servidor DNS debido a que se ahorra tiempo en la instalación ya que desde el mismo asistente es posible realizar la instalación del servicio de DNS, además de que el asistente combina automáticamente dichos servicios para trabajar conjuntamente sin necesidad de realizar configuraciones posteriores ahorrando valioso tiempo.

3.8.1 Instalar Nuevo Bosque

Para instalar un bosque nuevo a través de la interfaz de Windows se siguen los siguientes pasos:

1. Abrir el "Administrador de servidores. Presionar click en **Inicio**, en **Herramientas administrativas** y, a continuación click en **Administrador de servidores**.
2. Luego en la ventana **Resumen de roles**, dar click en **Agregar roles**.
3. Es necesario revisar la información de la página **Antes de comenzar** y, a continuación, presionar click en **Siguiente**.
4. En la página **Seleccionar roles de servidor**, se requiere activar la casilla **Servicios de dominio de Active Directory** y luego click en **Siguiente**.
5. Revisar la información de la página **Servicios de dominio de Active Directory** y, a continuación presionar click en **Siguiente**.
6. En la página **Confirmar selecciones de instalación** (figura 3.10), para luego dar click en **Instalar**.

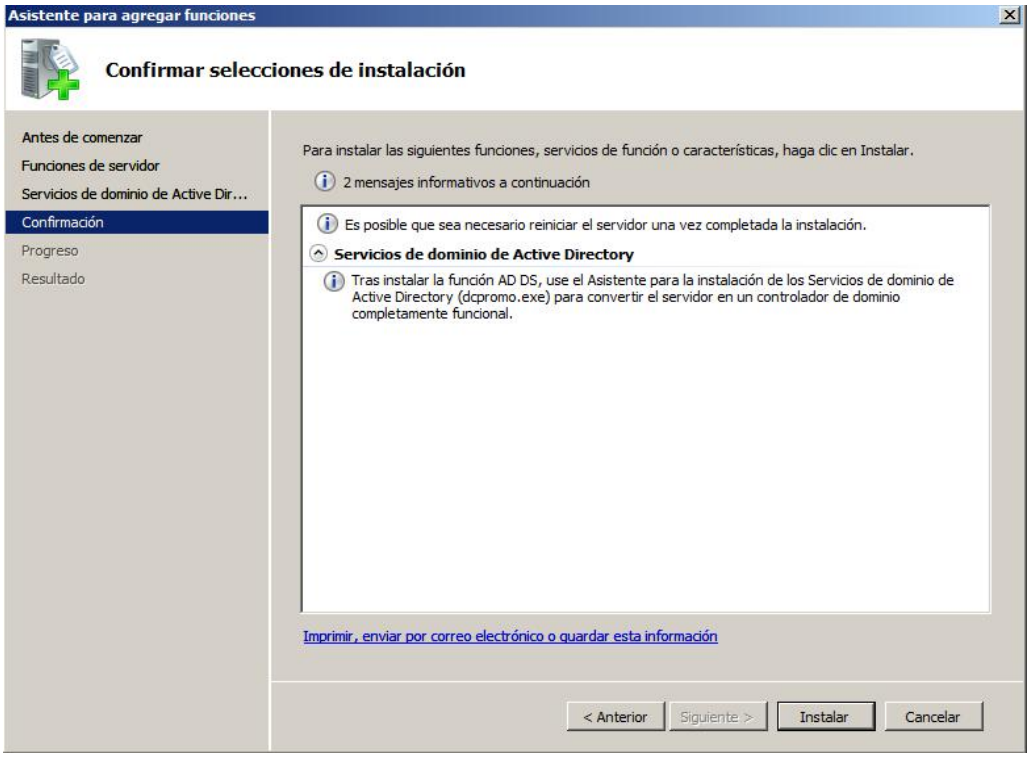

Figura 3. 10 *Asistente de Instalación de Active Directory*

7. En la página **Resultados de la instalación**, hacer click en **Cierre este asistente e inicie el Asistente para la instalación de Servicios de dominio de Active Directory (dcpromo.exe** figura 3.11**)**.

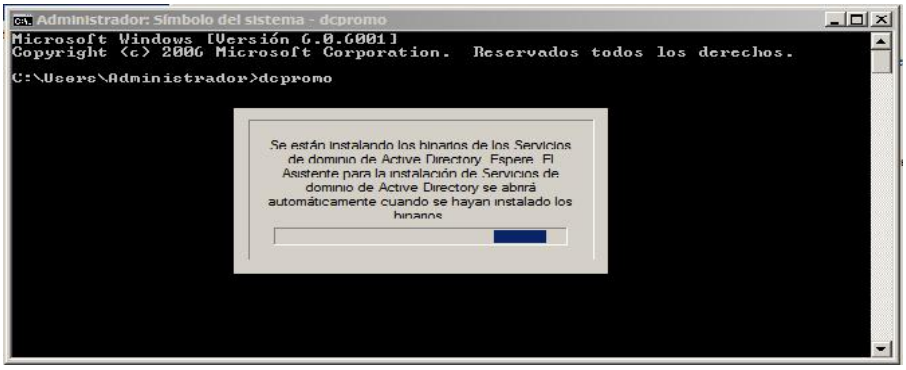

Figura 3. 11 *Instalación por medio de línea de comandos con DCPROMO*

8. En la página **Asistente para la instalación de los Servicios de dominio de Active Directory**, dar click en **Siguiente**.

9. En la página **Compatibilidad de sistema operativo**, se observa la advertencia sobre la configuración de seguridad predeterminada para los controladores de dominio de Windows Server, por lo que solo es necesario hacer click en **Siguiente**.

10. En la página **Elegir una configuración de implementación**, dar click en **Crear un dominio nuevo en un bosque nuevo**. Un bosque se refiere a una estructura jerárquica que alberga a uno o varios árboles de dominio, los cuales comparten un mismo esquema, configuración y catalogo global. Para este caso como no existe otro domino se crea un nuevo bosque con un nuevo dominio.

11. En la página se **asigna un nombre al dominio raíz del bosque** (figura 3.12), se requiere escribir el nombre completo del Sistema de nombres de dominio (DNS) para el dominio raíz del bosque. Para este trabajo el domino recibe el nombre de **LABREDES.UNAM.MX** (figura 3.12)

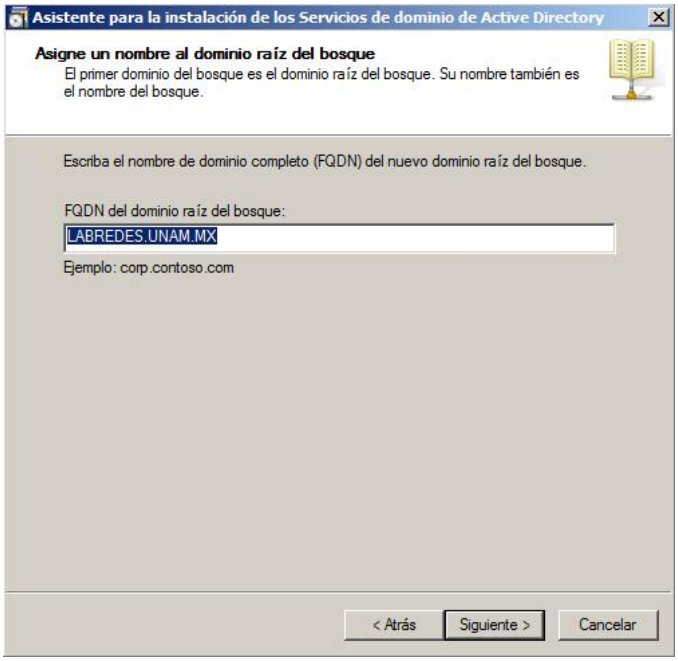

Figura 3. 12 *Pantalla de asignación del nombre del bosque*

12. En la página **Establecer el nivel funcional del bosque**, se elige el nivel funcional del bosque que hospeda los controladores de dominio, es decir se elige si el nuevo dominio tendrá interacción con dominio de versiones anteriores de Windows como Dominios creados en Windows 2000, Windows Server 2003 o solo tendrá interacción con dominio creados en Windows Server 2008. Para este caso que pretende instalar un bosque nuevo se elige **Windows Server 2008**, después se da click en **Siguiente**.

13. En la página **Opciones adicionales del controlador de dominio**, la opción **Servidor DNS** está seleccionada de manera predeterminada, por lo que se puede crear la infraestructura DNS del bosque durante la instalación de AD DS. En este caso se instalará también el servicio de DNS. Al presionar el botón de siguiente nos aparecerá una venta de advertencia (figura 3.13), la cual nos indica en resumen que no está instalado un servidor de DNS por lo no puede crear una delegación, así que solo basta con presionar siguiente.

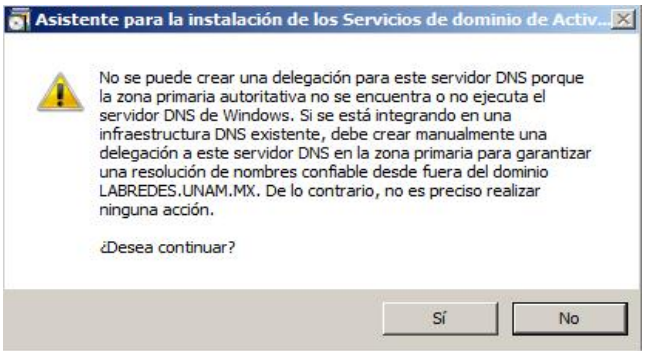

Figura 3. 13 *Advertencia de instalación del DNS*

En la página **Ubicación de la base de datos, los archivos de registro y SYSVOL** (figura 3.14), se muestran el volumen y las ubicaciones de las carpetas donde se encuentran el archivo de la base de datos, los archivos de registro del servicio de directorio y los archivos SYSVOL y, a continuación, estas rutas se recomienda no modificarlas ya que muchas de las herramientas que se integran con el Directorio Activo y DNS ocupan estas rutas predeterminadas. En caso de modificarlas es necesario tenerlas muy presentes al momento de agregar nuevas herramientas que se integren con estos servicios como el caso del servicio de WDS. Esta cuestión puede generar conflictos en futuras implementaciones por lo que la recomendación es no modificar estas rutas, y en caso de hacerlo registrarlas en un documento para su posterior consulta. Estas últimas dos ventanas son las concernientes a la instalación del servicio de DNS, por lo que la terminar la instalación también quedará instalado en el servidor.

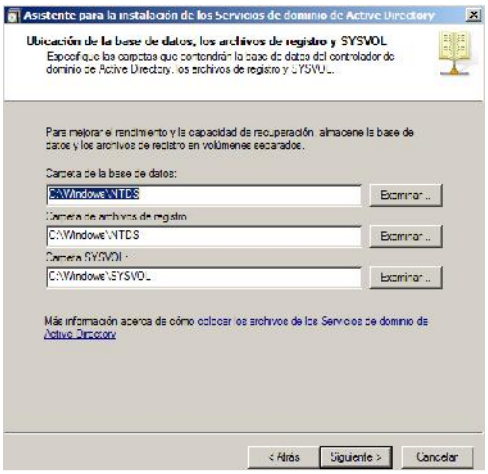

Figura 3. 14 *Ubicación de la base de datos, los archivos de registro y SYSVOL*

14. En la página **Contraseña de admón. del modo de restauración de servicios de directorio** (figura 3.15), se escribe la contraseña de modo de restauración. Esta contraseña se usa para iniciar AD DS en el modo de restauración del servicio de directorio para tareas que se deben realizar sin conexión. Dado que esta contraseña no es usada comúnmente se recomienda tenerla registrada en algún sitio seguro.

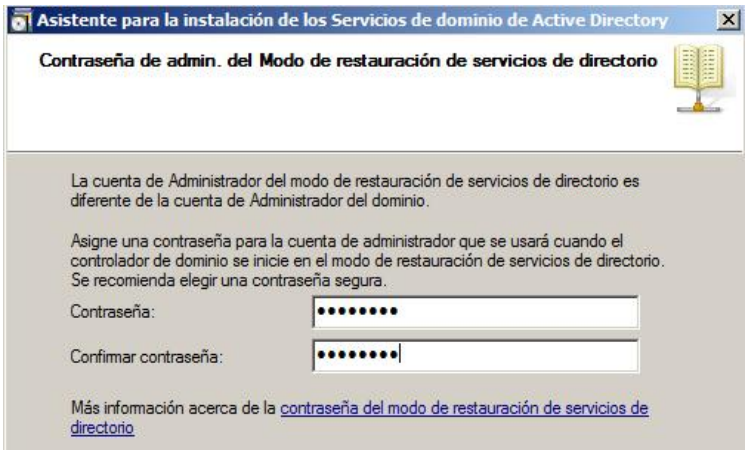

Figura 3. 15 *Contraseña de admón. del modo de restauración de servicios de directorio*

15. En la página **Resumen**, revise las selecciones realizadas. Haga click en **Atrás** para cambiar cualquier selección, si fuera necesario.

Para guardar la configuración seleccionada en un archivo de respuesta que pueda usar para automatizar operaciones posteriores de Active Directory, haga click en **Exportar configuración**. Escriba el nombre del archivo de respuesta y, a continuación, haga click en **Guardar**.
Cuando esté seguro de que las selecciones realizadas son las correctas, haga click en **Siguiente** para instalar AD DS.

16. Activar la casilla **Reiniciar al completar** como se muestra en la figura 3.16 para que el servidor se reinicie automáticamente o puede reiniciar el servidor para completar la instalación de AD DS cuando se le pida que lo haga.

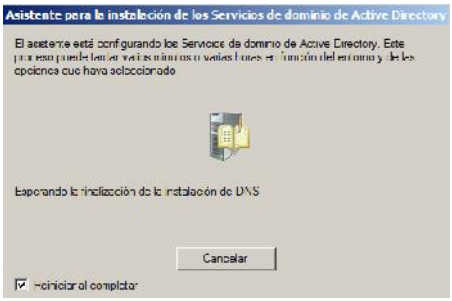

Figura 3. 16 *Pantalla de instalación de DNS final*

De esta forma quedan instalados los servicios de Directorio Activo y DNS. Ahora se requiere configurar el Servicio de DNS ya que algunos parámetros no quedan definidos por defecto, para ello se siguen los siguientes pasos:

1.- Crear la Zona de Búsqueda inversa: para realizar este proceso se debe de abrir desde "**INICIO / Herramientas Administrativas/ DNS"** la consola de Administración de este servicio

2.-En la nueva ventana mostrada (figura 3.17) se expande el árbol dando click sobre el servidor "**Hera**" y se presiona click derecho sobre "**Zonas de búsqueda inversa**"

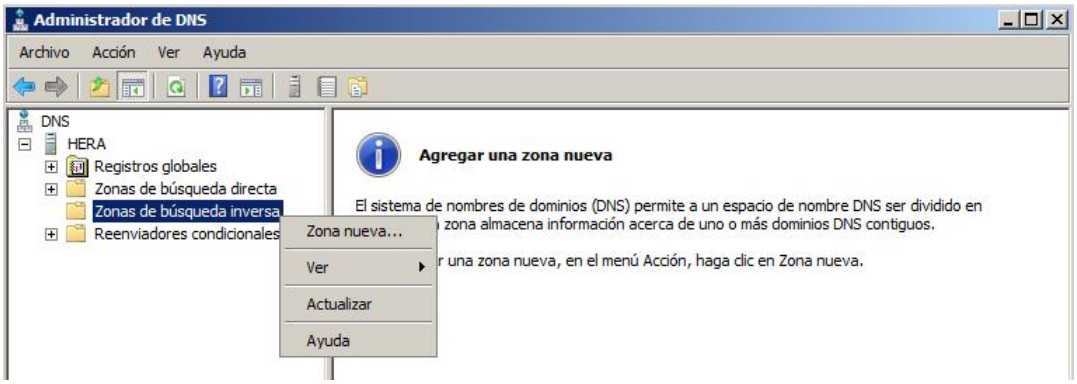

Figura 3. 17 *Consola del Administrador de DNS*

3.- Lo anterior despliega un asistente para la creación de la zona de búsqueda inversa. A continuación se solicita el tipo de zona a crear, en este punto se selecciona la opción "**Zona Principal**" y se mantiene activada la casilla "Almacenar la zona en Active Directory" se presiona el "**Siguiente**".

4.- El siguiente paso es definir cómo se quiere replicar los datos, para ello se selecciona la opción "**Para todos los servidores DNS en este dominio"** y se presiona **siguiente.**

5.- Después en la ventana **Nombre de la zona de búsqueda** se debe elegir el protocolo para el cual funcionará esta zona, que en este caso será **IPv4** y se presiona **siguiente**.

6.- Después se solicita definir el Id de red, este Id hace referencia a las direcciones IP abarcadas por la zona de búsqueda, para este caso se definen las IPs abarcadas de las subredes 0 a 255 colocando solo los dos primeros octetos como se muestra en la figura 3.18.

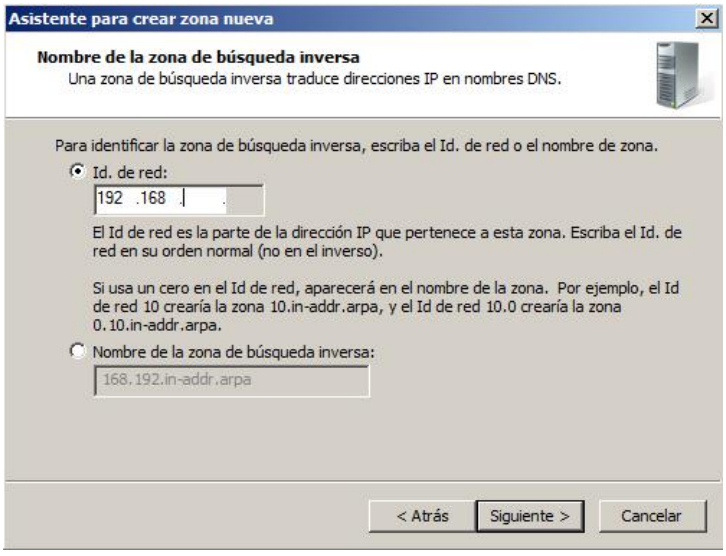

Figura 3. 18 *Asistente para crear una zona nueva*

Posteriormente en la ventana de Actualización dinámica se selecciona el tipo de actualizaciones dinámicas de nuevos equipos del dominio que albergará la zona de búsqueda, para este caso se elige la opción **Permitir solo actualizaciones dinámicas seguras**, y se presiona **Siguiente**.

7.- Por último se muestra un resumen de la configuración hecha durante la instalación, por lo que basta con presionar **Finalizar**.

8.- Después de crearla zona de búsqueda inversa, es necesario Revisar la configuración de la tarjeta de red (figura 3.19): esta acción es necesaria ya que por defecto el asistente de instalación del directorio activo y de la Zona de búsqueda inversa definen la IP **127.0.0.1** como se muestra en la figura 3.20 como Servidor DNS preferido esta IP. Por este motivo se debe sustituir la IP anterior por la IP del servidor, que para este trabajo es **192.168.2.132.** Cabe aclarar que se coloca esta dirección IP ya que este Servidor Controlador de Dominio es el que será el Servidor de DNS, por esta razón se coloca la misma IP que la del Servidor.

Figura 3. 19 *Parámetros de configuración del DNS*

Con lo anterior queda configurada y terminada la instalación de los servicios de Directorio activo y DNS.

3.8.2 Fase de pruebas después de la instalación

Para poder corroborar que la instalación de las herramientas anteriores fue exitosa, se deben seguir los siguientes pasos:

1.- Para el Directorio activo basta abrir la consola de administración del Active Directory en la ruta **Inicio / Herramientas Administrativas / Usuarios y Equipos de Active Directory**.

2.- Con esto aparecerá la consola de administración, dentro de ella se extiende el árbol presionando dos veces el dominio "**LABREDES.UNAM.MX**" y luego sobre Users. Dentro de esta Unidad
Organizativa (OU) se encuentran los usuarios del dominio incluyendo al administrador del dominio.

3.- Si se puede visualizar lo anterior, está correctamente instalado el servicio Directorio Activo.

Ahora se requiere crear una estructura para albergar a los usuarios y a los equipos de cómputo del laboratorio de redes. Para ello se presiona click derecho sobre el dominio y seleccionar Nuevo / Unidad Organizativa y la nombramos “LAB REDES” y presiona aceptar como lo ilustra la figura 3.20.

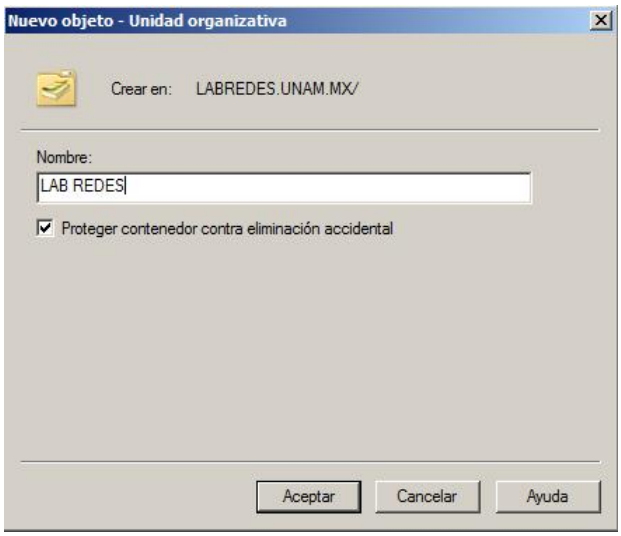

Figura 3. 20 *Pantalla de creación de una nueva OU*

En esta unidad organizativa representada por una carpeta se albergarán todos los objetos del laboratorio, es decir, las cuentas de usuario y equipos. Dentro de esta OU se repite el proceso anterior y se crean dos nuevas OU´s llamadas “**Equipos**” y “**Usuarios**”. Con esto se crea una estructura como la mostrada en la figura 3.21.

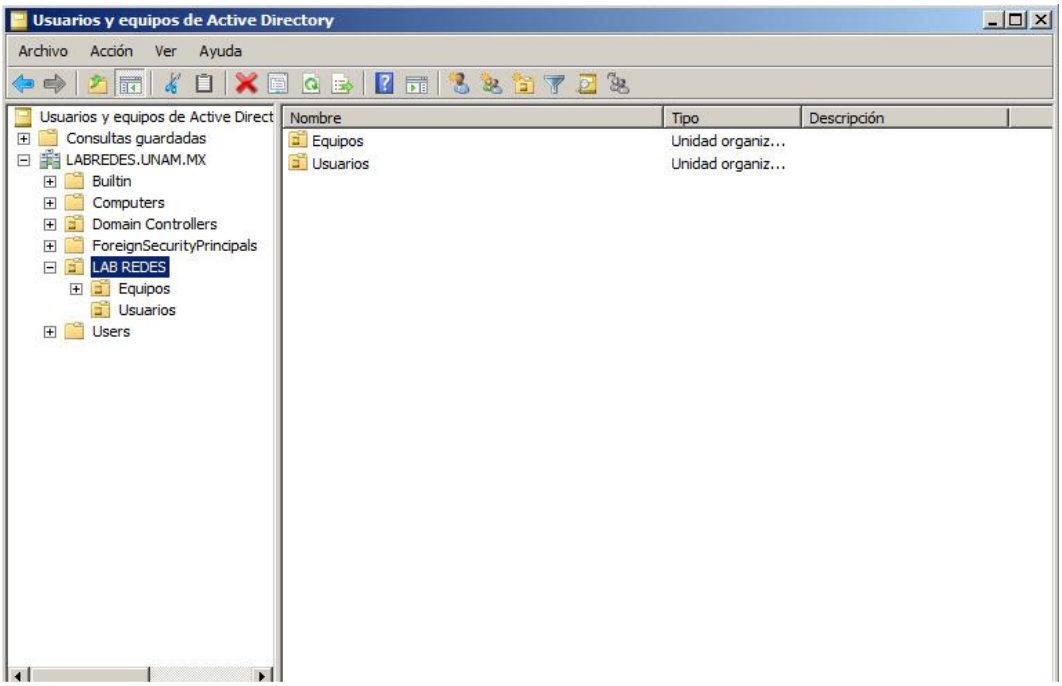

Figura 3. 21 *Consola de Administración de Usuarios y Equipos de Active Directory*

Finalizado lo anterior se procede con la revisión del funcionamiento del servicio de DNS.

Para ello se sigue el siguiente procedimiento:

1.- Se abre una consola de Símbolos del sistema y se escribe el comando “nslookup”, el resultado mostrará algo similar a lo de la figura 3.22.

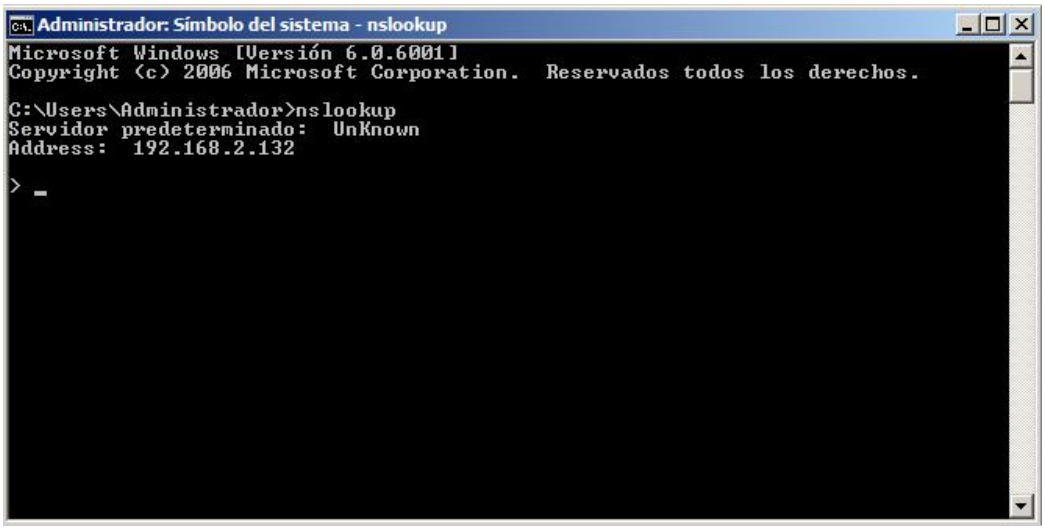

Figura 3. 22 *Prueba con el comando “nslookup”*

En este caso el resultado esperado debiera ser el nombre del servidor complementado por el nombre del domino completo (**hera.labredes.unam.mx**) y la dirección IP del servidor (**192.168.2.132**). Sin embargo, dado que el servicio de DNS fue recién configurado nuevamente por el asistente este resultado no aparece durante la prueba.

Es necesario tener presente que en este caso se requiere hace uso de los siguientes comandos:

1.- Se escribe el comando **exit** para salir del comando anterior.

2.- Se escribe el comando **ipconfig /flushdns** para borrar el registro de DNS incompleto del servidor.

3.- Se escribe el comando **ipconfig /registerdns** para registrar nuevamente el servidor en el DNS.

4.- Se prueba nuevamente el servicio de DNS escribiendo el comando **nslookup**, si el procedimiento se ha realizado correctamente se debe apreciar el resultado comentado anteriormente.

5.- Ahora se procede a probar la configuración de búsqueda inversa escribiendo la IP del servidor, si esta correcta la configuración el resultado debe ser el nombre completo del servidor y su IP. Del mismo modo se prueba escribiendo ahora el nombre del servidor esperando el mismo resultado.

Con estas pruebas realizadas como se muestra en la figura 3.23, es posible decir con certeza que la instalación y configuración de los servicios de Directorio y DNS han sido correctas.

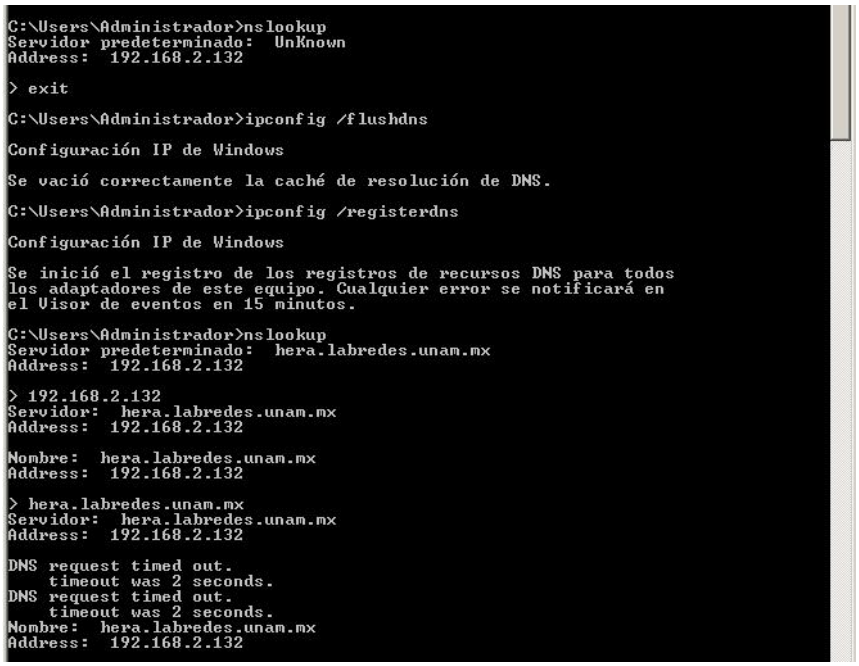

Figura 3. 23 *Comprobación del funcionamiento del DNS*

3.9 Servicio de Nombres Internet de Windows (WINS)

El servicio de Nombres Internet de Windows (WINS) es un servicio de resolución y registro de nombres de equipos que asigna nombres NetBIOS de equipo a direcciones IP de computadoras con sistema operativo Windows. Cuando se implementa WINS en la red, los usuarios finales pueden tener acceso a los recursos de red mediante los nombres de los equipos, en lugar de hacerlo únicamente a través de direcciones IP que generalmente son difíciles de recordar. Además, el software y otros servicios que se deseen instalar en los equipos y otros dispositivos pueden realizar solicitudes de nombres en el servidor WINS para resolver los nombres en direcciones IP más fácilmente.

Para la instalación solo se siguen los siguientes pasos:

1. Dar click en **Inicio, Herramientas administrativas, Administrador del servidor** y, a continuación, se presiona **Características**.

2. En **Seleccionar Características**, hacer click en **Agregar Características,** dar click en **Siguiente,** seleccionar **Servidor WINS** y, a continuación **Siguiente**.

3. A continuación se muestra una ventana indicando que el servicio se instalará, se presiona **Instalar**.

4. Con lo anterior comenzará la instalación, al finalizar solo es necesario cerrar el asistente. No requiere configuración adicional.

3.9.1 Fase de pruebas después de la instalación

Para corroborar el funcionamiento de este servicio es necesario dirigirse a un equipo cliente. Una vez en el equipo cliente se abre las ventana de **Propiedades de Conexión de Área Local** presionando doble click sobre el icono de red y eligiendo la opción **Propiedades**. Aquí se selecciona la opción **Protocolo Internet (TCP/IP)**.

En la ventana que aparece se elige la opción **Obtener una dirección IP automáticamente** y la opción **Obtener una dirección del servidor de DNS automáticamente**.

Luego se presiona el botón de **Opciones Avanzadas**, dentro de esta nueva ventana se elige la pestaña llamada **WINS**.

En esta ventana se presiona el botón de **Agregar** y se escribe la dirección del servido WINS, que para este caso es **192.168.2.132** y luego se presiona **Aceptar** hasta cerrar las opciones de configuración.

Finalmente se comprueba que el equipo está obteniendo una resolución de nombres a IP abriendo una consola de **Símbolos del sistema** y escribiendo el comando **nslookup nombre_servidor,** en este caso **HERA** como se muestra en la figura 3.24.

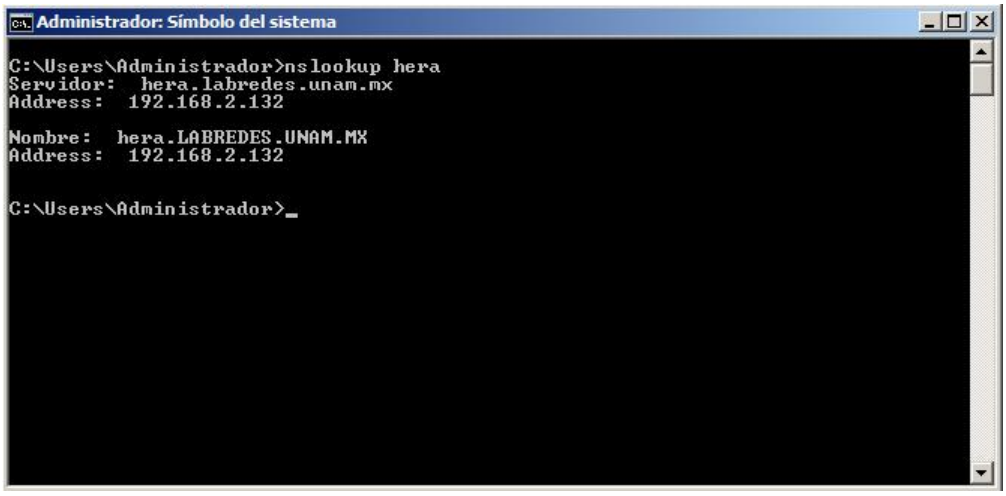

Figura 3. 24 *Comando para la resolución de nombres "nslookup"*

Dado que el equipo cliente resuelve satisfactoriamente esta solicitud se puede afirmar que la instalación y configuración fue exitosa.

Las pruebas de este servicio no son necesarias ya que los resultados están muy ligados al servicio de DNS, por lo que en caso de observar una falla en el servicio de DNS se requiere revisar únicamente que la dirección IP del servidor de WINS sea la correcta en los equipos cliente.

3.10 Servicio de DHCP

Para instalar el servidor DHCP se procede siguiendo los siguientes pasos:

1. Dar click en **Inicio, Herramientas administrativas, Administrador del servidor** y, a continuación, se presiona **Funciones**.

2. En **Resumen de roles**, click en **Agregar roles,** dar click en **Siguiente,** seleccionar **Servidor DHCP** y, a continuación **Siguiente**.

3. Seguidamente aparecerá una introducción del servidor de DHCP con información relevante acerca de su funcionamiento y características, por lo que solo basta con presionar **Siguiente**.

4. Posteriormente el asistente solicita elegir una tarjeta de red para brindar el servicio de DHCP a los clientes, en este punto se selecciona la única disponible (**192.168.2.132**) y se presiona **Siguiente**.

5. Después se solicita especificar el dominio y la dirección IP del servidor DNS para el cual estará disponible el servicio. Para este trabajo se define el dominio **LABREDES.UNAM.MX** y la dirección IP **192.168.2.132** del DNS, antes de presionar el botón de **Siguiente**, se presiona el botón de **Validar** para corroborar la dirección IP.

6. El siguiente paso es configurar el servidor de WINS, la opción predeterminada es la cual indica que "**No se requiere WINS…**", pero para este trabajo se habilita la opción la cual indica que "**Sí requiere WINS…**". Esta opción es utilizada ya que los clientes XP utilizan este servicio para facilitar el trabajo del DNS y del DHCP en conjunto. Se escribe la dirección IP del servidor de WINS que para esta tesis es el mismo servidor con IP **192.168.2.132**

7. Se requiere también agregar un rango de direcciones IP que será utilizado por los equipos cliente, a este rango de IP´s se le conoce como "**Ámbito**", para ello se presiona **Agregar**. Con esto se desplegará una nueva venta en la que se solicita el nombre del ámbito, la dirección IP inicial así como la final, una máscara de subred, la puerta de enlace, Tipo de subred y una casilla para activar o deshabilitar el ámbito. Estos datos son proporcionados conforme se muestra en la figura 3.25. Después sólo se presiona el botón de **Aceptar**.

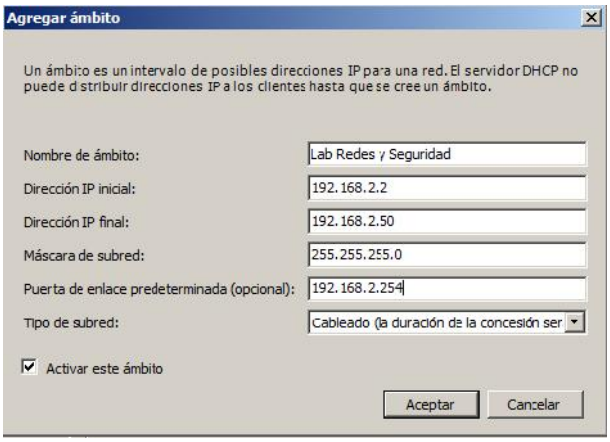

Figura 3. 25 *Venta para crear un nuevo rango de IPs en el DHCP*

8. Se continúa con el asistente y con ello se solicita la configuración del DHCP para el protocolo IPv6. Para el caso del laboratorio, dado que aún no se cuenta con infraestructura para soportar direcciones de este tipo aún se deshabilita el uso de este protocolo con el DHCP. Esto no quiere decir que después de realizar esta configuración en un futuro no se pueda cambiar dicha configuración, se puede realizar la actualización de este protocolo si se necesita en un futuro pero de manera manual dentro de la consola de administración del DHCP.

9. A continuación se solicita una cuenta con privilegios para poder ejecutar dicho servicio, para este caso se habilita la casilla "**Usar Credenciales actuales**" ya que se está trabajando con una cuenta con privilegios de administrador.

10. De esta forma continuando se muestra una ventana con el resumen de la configuración hecha durante el asistente por lo que solo basta presionar **Instalar** (figura 3.26) y posteriormente **Cerrar** para terminar con la instalación.

Las opciones de servidor que deben estar activas deben ser:

- 006 (DNS Servers): 192.168.2.132
- 044: Wins/NBSNS Servers: 192.168.2.132
- 046: Wins/NBSNS Node Type: 0x2

Estas opciones se aplicaran de forma global a cualquier ámbito que se cree en el dominio, cabe aclarar que aún faltan las opciones de WDS, pero estas se agregan una vez instalada la función de Servicios de Implementación de Windows (WDS).

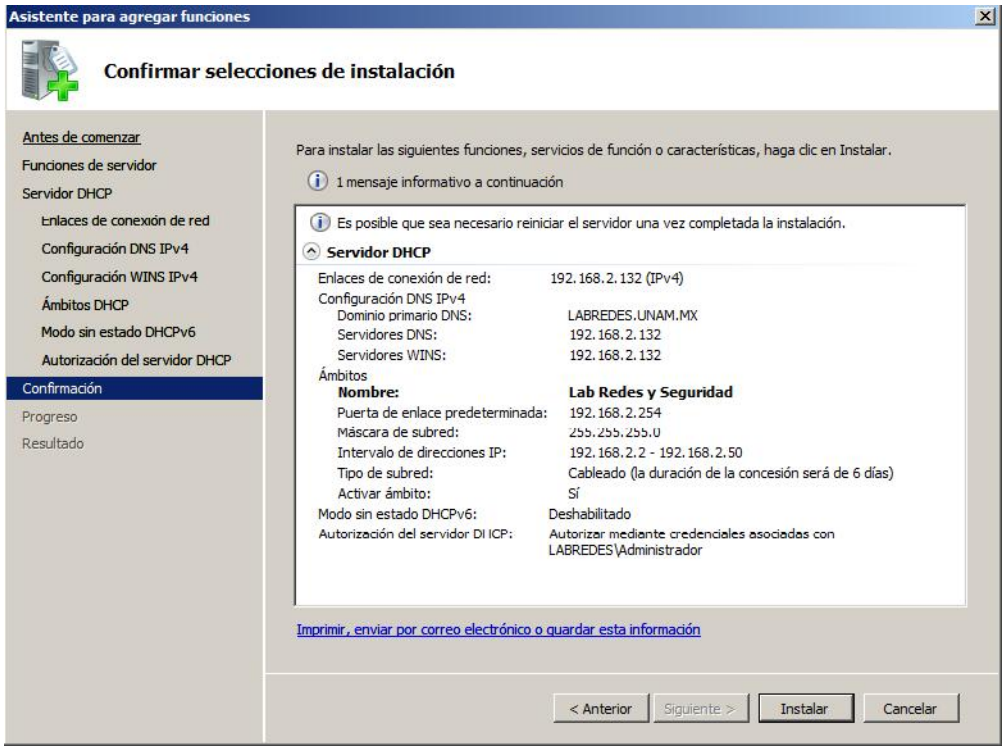

Figura 3. 26 *Resumen de datos de configuración del Asistente del Instalación para el DHCP*

3.10.1 Fase de pruebas después de la instalación

El siguiente paso es probar la configuración de instalación creando una nueva reservación en la consola de DHCP.

Para ello se siguen los pasos que se listan a continuación:

1.- Dar click en **Inicio, Herramientas administrativas, DHCP** para que aparezca la consola de Administración. En esta nueva ventana se selecciona y expande el servidor con el nombre de dominio mostrado en el árbol.

2.- Dentro de este existen dos opciones a elegir para crear nuevos elementos, una llamada **IPv4** y otra con **IPv6**. Estos nombres hacen referencia al tipo de protocolo de red que ocupan los equipos clientes dentro de la red, para el caso de este trabajo se utilizará siempre **IPv4**. Se expande el árbol nuevamente y se expande adicionalmente la opción **Ámbito**.

3.-Dentro del árbol desplegado se presiona click derecho sobre la opción Reserva y se elige la opción Nueva reserva.

4.- Con esto aparecerá una nueva ventana solicitando los datos del equipo a registrar, dentro de estos datos se debe colocar el Nombre de la reservación del equipo individual, la dirección IP para el equipo, la cual debe estar dentro del rango creado durante el proceso de instalación, la dirección MAC del equipo (previamente obtenido del equipo cliente mediante el comando

IPCONFIG en la consola de símbolos del sistema) y una descripción del equipo con la finalidad de poder identificarlo de una manera sencilla en caso de ocurrir algún problema. Todo se llena como el caso de la figura 3.27.

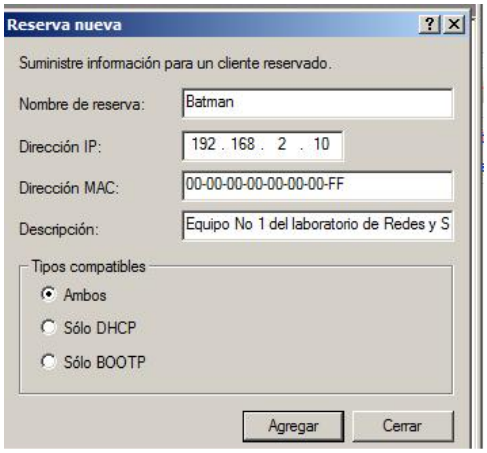

Figura 3. 27 *Venta de creación de una nueva reservación de IP en el DHCP*

Este procedimiento se repite para cada uno de los equipos del laboratorio cuidando el copiar correctamente las direcciones MAC de cada equipo como lo ilustra la figura 3.28.

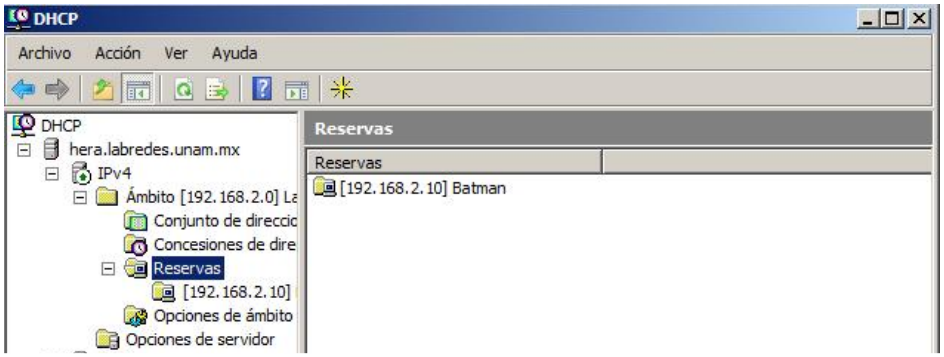

Figura 3. 28 *Consola de Administración del DHCP con una reservación creada*

Para probar esta configuración es necesario seguir los pasos:

- Dirigirse al equipo cliente, una vez ahí se abren las **Propiedades** de la tarjeta de red.
- Se deben colocar los parámetros fijos en la opción de TCP-IPv4 presionando doble click sobre esta opción.
- En la nueva ventana que aparece se elige la opción **Obtener una dirección IP automáticamente** y la opción **Obtener una dirección del servidor de DNS automáticamente**.

- Luego se presiona el botón de **Opciones Avanzadas**, dentro de esta nueva ventana se elige la pestaña llamada **Configuración de IP** (figura 3.29).

Figura 3. 29 *Venta de Configuración avanzada de TCP/IP*

1. En esta ventana se debe visualizar el mensaje **DHCP Habilitado**.

2. Finalmente se comprueba que el equipo está obteniendo la dirección IP abriendo una consola de **Símbolos del sistema** y escribiendo el comando **IPCONFIG** como se muestra en la figura 3.30**.** El resultado esperado es la IP escrita en el servidor, en la consola de administración del DHCP como se muestra en la Figura 3.30.

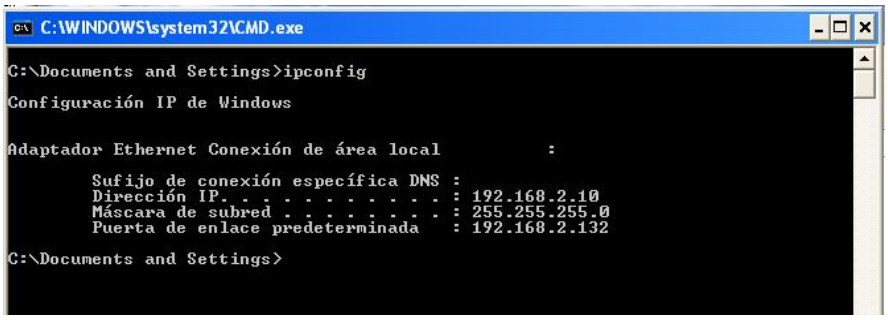

Figura 3. 30 *Comando "ipconfig" para la visualización de parámetros de tarjeta de red*

Con esto queda comprobado el funcionamiento del servidor de DHCP en el equipo cliente.

3.11 Instalación de WDS

Después de instalar las herramientas anteriores se procede a instalar los **Servicios de implementación de Windows** (WDS) mediante el Asistente para tareas de configuración inicial, Administrador del servidor o la línea de comandos.

- Para instalar la función mediante el Asistente para tareas de configuración inicial, dar click en **Agregar funciones** en la pantalla de inicio **Tareas de configuración inicial**. Luego se presiona **Siguiente** y después **Servicios de implementación de Windows.**

- Para instalar la función con el Administrador del servidor, haga click en **Agregar funciones** dentro del panel **Resumen de funciones**. Haga click en **Siguiente** y, a continuación seleccione **Servicios de implementación de Windows**.

Durante el proceso de instalación, se deben elegir los dos servicios listados:

- **Servidor de transporte**. Esta opción ofrece un subconjunto de la funcionalidad de Servicios de implementación de Windows, que contiene sólo los principales componentes de red.

- **Servidor de implementación**. Esta opción ofrece la funcionalidad completa de Servicios de implementación de Windows, que puede usar para configurar e instalar de forma remota sistemas operativos Windows. Con esta opción, es posible crear y personalizar imágenes para después, utilizarlas con la finalidad de volver a crear imágenes de los equipos.

Posteriormente solo basta presionar Instalar y luego cerrar para terminar con la instalación.

3.11.1 Configuración

Para configurar este servicio se abre la consola de **Servicios de implementación de Windows**.

1. En esta consola se selecciona el dominio LABREDES.UNAM.MX con click derecho y se presiona configurar servidor. Esto abrirá un nuevo asistente.

2. En este nuevo asistente se presiona Siguiente.

3. Después se solicita una ruta donde se alojarán los archivos de instalación para su distribución remota. Para este caso la ruta es **E:\Remote install**.

4. Posteriormente en la ventana de **Opción DHCP 60** (figura 3.31), se seleccionan las dos opciones **No escuchar en el puerto 67**, y la opción **Configurar la opción DHCP 60 como "PXEClient"** y se presiona **Siguiente.**

Figura 3. 31 *Ventana de Opción DHCP 60*

5. En la ventana **Configuración inicial del servidor PXE** se debe elegir la forma en la que este servicio estará funcionando, para este trabajo de tesis se elige la opción **Responder solo a los equipos conocidos**. De esta forma solo los equipos registrados en el Directorio Activo y con una reservación en el servidor de DHCP podrán ser atendidos por este servicio para la instalación remota del sistema operativo.

6. Con lo anterior queda finalizada la configuración, se deshabilita la casilla **Agregar Imágenes al servidor** por lo que solo resta presionar **Finalizar**.

7. Colocar el CD de instalación de Windows Server 2008 y en la consola de **Servicios de implementación de Windows**, ir a los servidores, buscar la opción de imágenes de arranque, agregar una imagen de arranque, se seleccionará desde la ruta del **CD, …\sources\ boot.wim**, en este momento se contará con una imagen de arranque.

3.11.2 Captura de imagen para la distribución vía red.

Para capturar una imagen de sistema operativo, primero se debe crear una imagen de captura, basta con dar click en una imagen de arranque y seleccionar la opción de Crear imagen de arranque de captura como se ilustra en la figura 3.32.

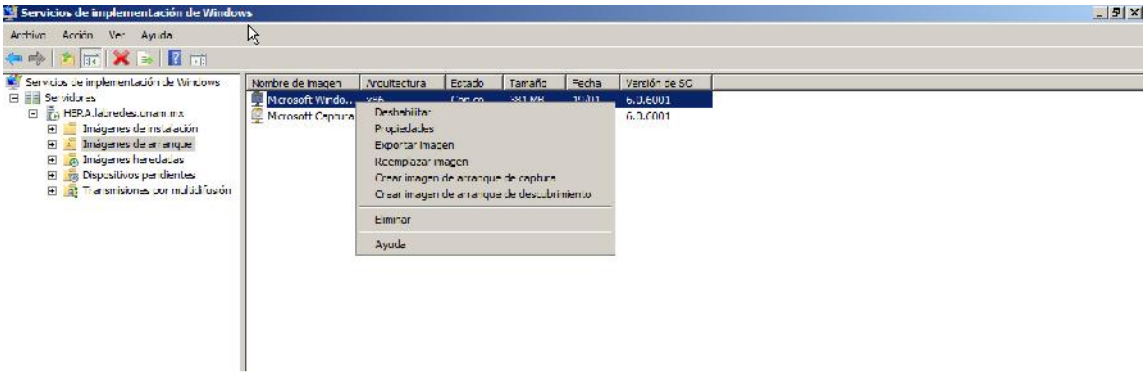

Figura 3. 32 *Consola de WDS, captura de imagen de arranque.*

1- Instalar el sistema operativo (XP) con todas sus actualizaciones en un equipo cliente que ya disponga de una IP asignada mediante DHCP.

2- Desde el disco de instalación del sistema operativo XP, obtener la carpeta de sysprep y copiarla en la raíz del equipo a capturar, dentro de sysprep se creará otra carpeta adicional donde se copiarán todos los drivers de los equipos disponibles.

3- Preparar el archivo Sysprep.inf para adecuarlo al dominio, se le preguntaran datos como nombre, organización, serial, configuración regional, contraseña del administrador, si se desea ingresar a dominio una vez instalado, etc.

4- Ejecutar el comando de sysprep para empaquetar nuevamente el sistema operativo, haciendo una instalación mínima y generalizando, reiniciar el equipo.

5- Reiniciar el equipo mediante la tarjeta de Red, generalmente presionando la tecla f12 (figura 3.-33), obtener los datos del equipo, como el GUID y darlo de alta en el directorio activo, si el equipo está dado de alta, entrará al menú de selección de imágenes, es decir podrá seleccionar la opción de capturar una imagen o instalar el sistema operativo.

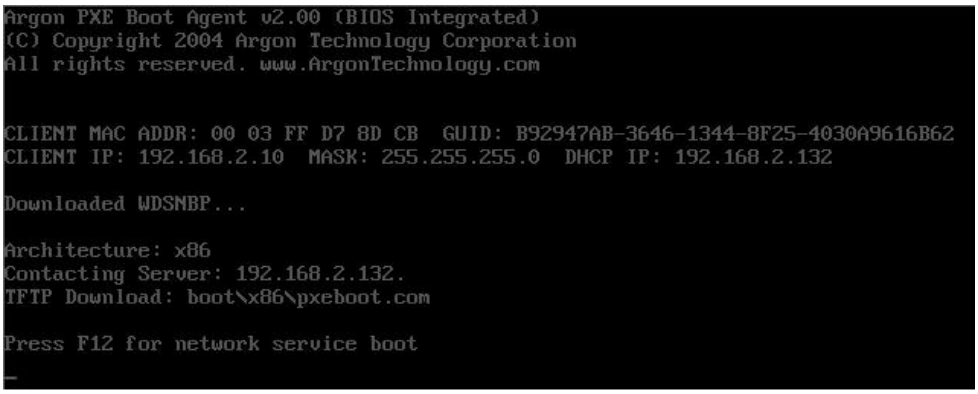

Figura 3. 33 *Boot mediante la tarjeta d red con la tecla F12*

6- Seleccionar la imagen de captura y proporcionar los datos solicitados tal como usuario y contraseña, se recomienda iniciar el equipo con un dispositivo de almacenamiento externo donde se guardará la imagen del sistema operativo, una vez que se han colocado los datos, se comenzará la captura del sistema operativo, y el archivo generado estará listo para subirlo al servidor para su distribución.

7 -Subir la imagen capturada al servidor de implementación de Windows (figura 3.34), ya sea durante el proceso de captura o directamente en el servidor WDS con el medio externo donde se almacenó la imagen de captura, teniendo el cuidado de poner los datos como el nombre y descripción de la imagen para tener todo ordenado de una manera limpia y entendible.

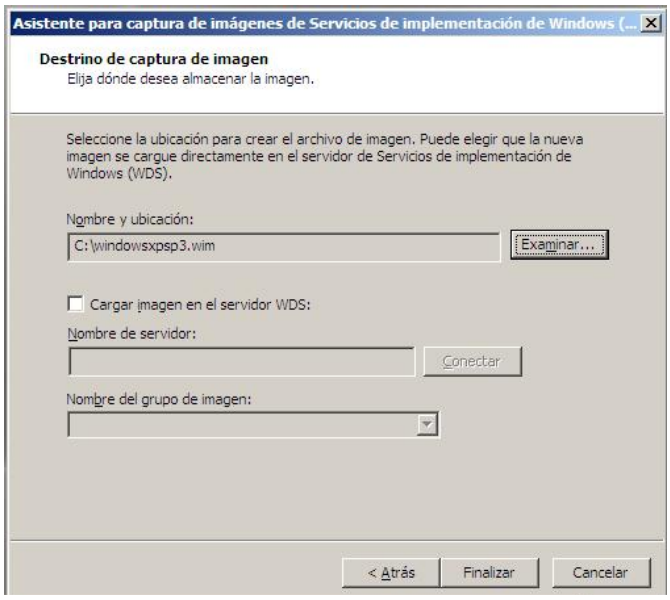

Figura 3. 34 *Destino de captura de la imagen creada*

8- Dar de alta todos los equipos en el directorio activo que se les instalará la imagen del sistema operativo que se encuentra en el WDS.

3.11.3 Fase de pruebas después de la instalación

Después de que se ha realizado la captura de la imagen para su distribución vía red por medio del servidor, se procede a revisar que esta imagen sea listada en los equipos clientes usando el servicio de WDS.

Para probar el correcto funcionamiento de las imágenes de instalación de sistema operativo es necesario hacer lo siguiente:

1. Encender los equipos y arrancar inicializando la tarjeta de red, para los equipos de laboratorio es con la tecla f12, se obtendrán los parámetros de red que se le asignaron desde el DHCP

2. Seleccionar la imagen “Instalación de Windows”, insertamos las credenciales que se usarán para la implementación del sistema operativo.

3. Seleccionar la imagen a instalar (figura 3.35), la partición donde se instalará el sistema operativo, evitando afectar la partición de Linux.

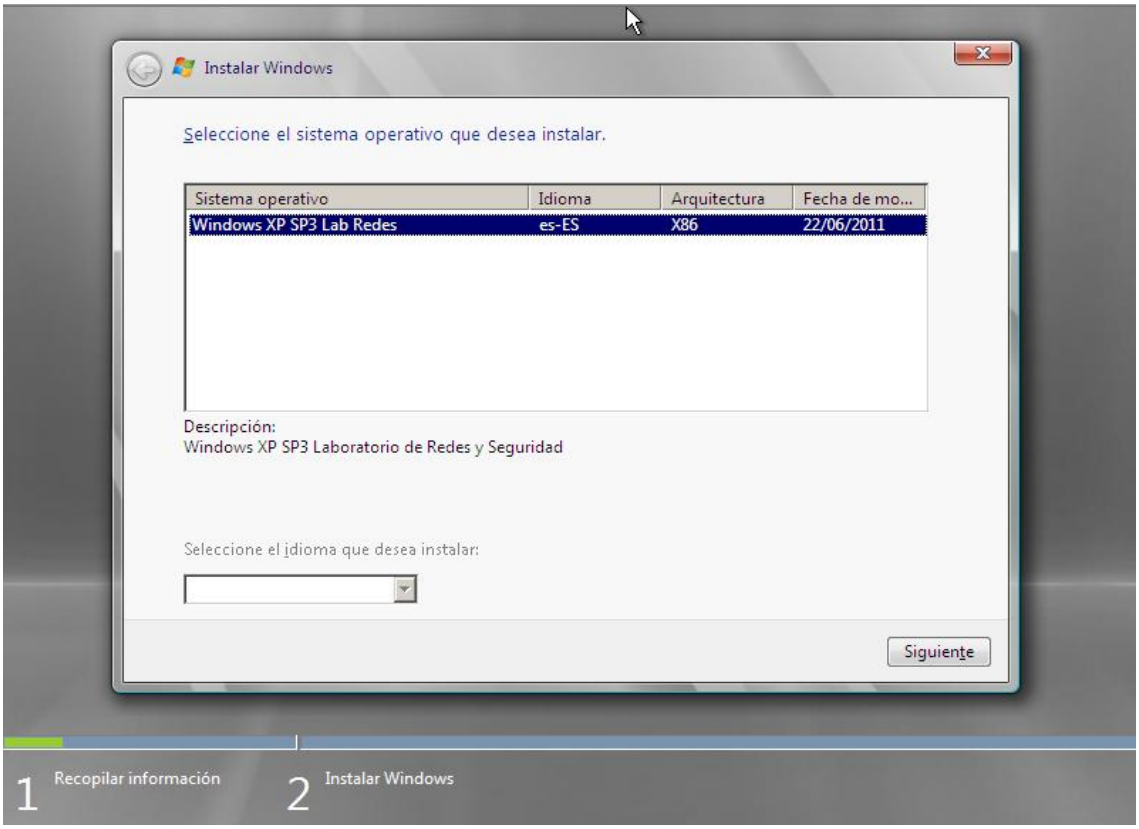

Figura 3. 35 *Selección de la imagen de instalación*

4. Comenzará la instalación y al terminar pedirá la configuración del teclado una vez eligiendo dicha configuración, el equipo estará listo para su uso.

3.12 Creación de directivas de grupo por medio de Group Policy Object (GPO´s)

Las directivas de grupo (GPO´s) según la información de Microsoft son un conjunto de políticas o reglas que son posibles aplicar a una serie de objetos del dominio como usuarios y/o equipos con

el fin de prohibir, ayudar o permitir a estos realizar cambios, ejecutar programas, acceder a ciertos recursos etc.

Las directivas se dividen en dos grupos principalmente, las directivas de configuración de equipo y las directivas de configuración de usuario, las cuales tienen un claro ámbito de aplicación:

- **Directivas de configuración de equipo**: Estas afectan a los equipos o sistemas operativos Windows, se aplican durante la carga del sistema operativo y se actualizan en intervalos de 90 a 120 minutos.
- **Directivas de configuración de usuario**: Afectan solo a las cuentas de usuario del dominio, se aplican durante el proceso de inicio de sesión y se actualizan en intervalos de 90 a 120 minutos.

Como se muestra en la tabla 3.3, se puede apreciar las diferencias entre estos dos grupos

Tabla 3. 3 Diferencias entre directivas de Usuario y de Equipo

Tipo de Ámbito	Ejecución	Tiempo de Actualización
Equipos de la red	Durante la carga del sistema operativo	Intervalos de 90 a 120 min.
Usuarios (objeto)	Durante el inicio de sesión	Intervalos de 90 a 120 min.

Para la instalación se sigue el proceso:

3.12.1 Directiva de Fondo de Escritorio equipos cliente

1. Se abre la consola de Administración de Directivas de grupo desde INICIO, Herramientas Administrativas.
2. Se expande el árbol del domino LABREDES.UNAM.MX, y se selecciona la **OU LAB REDES** como se muestra en la figura 3.36. En este espacio es posible elegir y delimitar el alcance de las reglas o políticas implementadas gracias al uso de las OU´s (unidades organizativas). Esto es posible ya que cada regla creada es ligada a una o varias OU´s dependiendo de la necesidad de su aplicación. En el caso del laboratorio se cuenta con dos OU´s, una dedicada a las cuentas de usuario y otra más para los equipos de cómputo. A continuación se describe el proceso para la creación de la primera regla, la cual define el fondo de escritorio para todos los equipos del laboratorio. Con esta regla se pretende tener un ambiente homogéneo y específicamente educativo apto para la impartición de las clases prácticas.

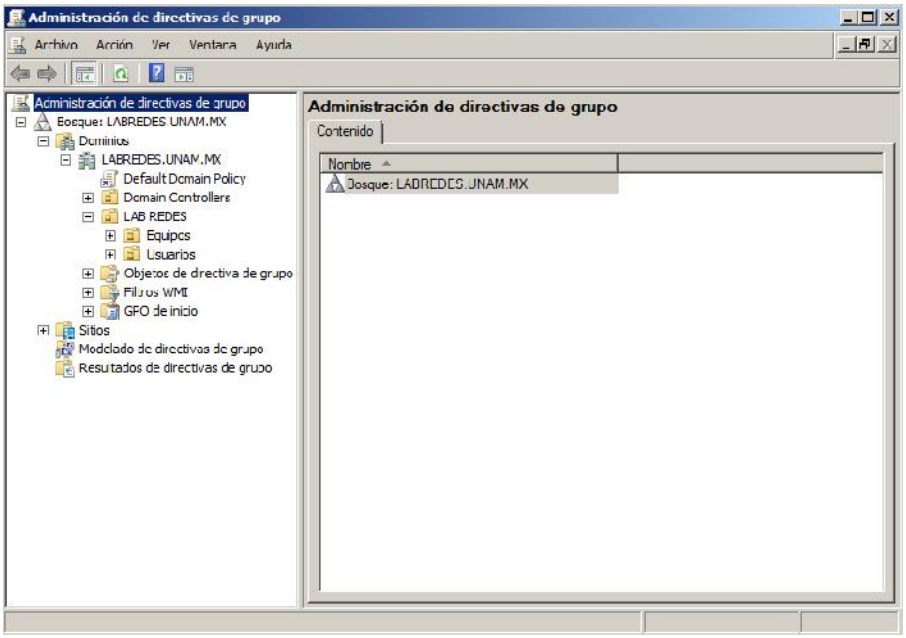

Figura 3. 36 *Consola de Administración de directivas de grupo*

3. Se elige la OU llamada **Equipos** para que en esta se aplique la directiva de seguridad presionando click derecho y seleccionando la opción **Crear una GPO en este dominio y ligar aquí**. A continuación se solicitará el nombre, se coloca **Wallpaper Lab Redes** y **Aceptar**.

4. Con lo anterior ahora se listará la regla recién creada del lado derecho de la consola, por lo que se presiona click derecho sobre ella y se elige **Editar**.

5. Ahora en la nueva ventana **Editor de administración de directivas de grupo** (figura 3.37) se puede apreciar grandes grupos, Configuración del equipo y configuración de usuario. En este caso se sigue la ruta **Configuración de usuario\ Plantillas administrativas: … \Escritorio \ Escritorio.**

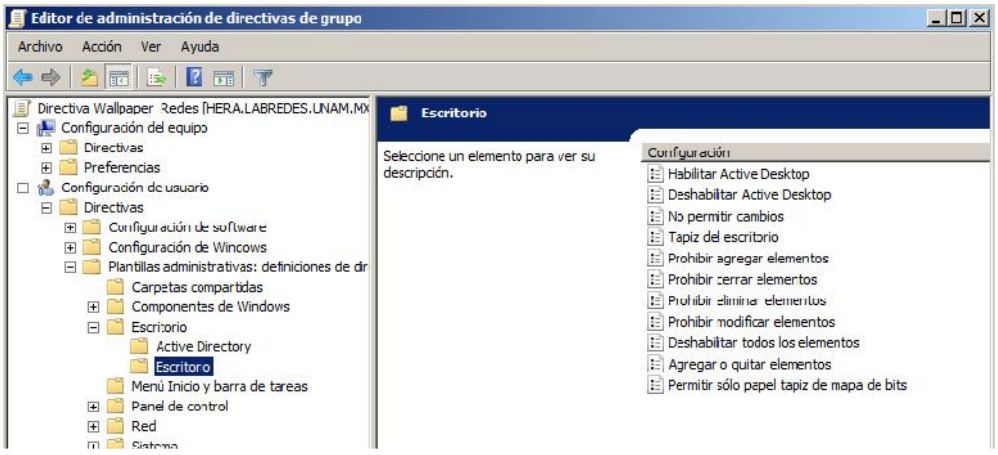

Figura 3. 37 *Editor de administración de directivas de grupo*

6. Del lado derecho se podrá apreciar las opciones para modificar, en este caso se selecciona la opción **Tapiz del escritorio**.

7. Aquí se coloca la ruta de la imagen para ser distribuida. Esta imagen debe estar colocada en una carpeta compartida para ser utilizada por los equipos cliente. En este caso se encuentra en la ruta **\Hera\wallpaper$.** Se selecciona la casilla de **Habilitar** y se presiona **Aceptar**.

8. Finalmente se cierra la ventana y con ello queda aplicada la directiva de seguridad.

3.12.2 Directiva de página de Internet

Para la definición de la página inicio del navegador predeterminado se sigue el mismo procedimiento anterior para la creación de la directiva de seguridad sobre la misma OU utilizada en el caso anterior, es decir, **Equipos**. La edición de la directiva se lleva a cabo mediante los siguientes pasos:

1. La ruta en la que se encuentra esta propiedad configurable dentro del árbol es: **Configuración de Usuario \ Directivas \ Configuración de Windows \ Mantenimiento de Internet Explorer \ Direcciones URL**.

2. Dentro de esta ruta se encuentra la opción Direcciones URL Importantes, se selecciona esta opción para ingresar en la ventana de configuración de esta propiedad.

3. Posteriormente se habilita la casilla de "**Personalizar URL de la página principal**" y se coloca la dirección de la página del laboratorio de redes y seguridad de la Facultad de Ingeniería como lo ilustra la figura 3.38.

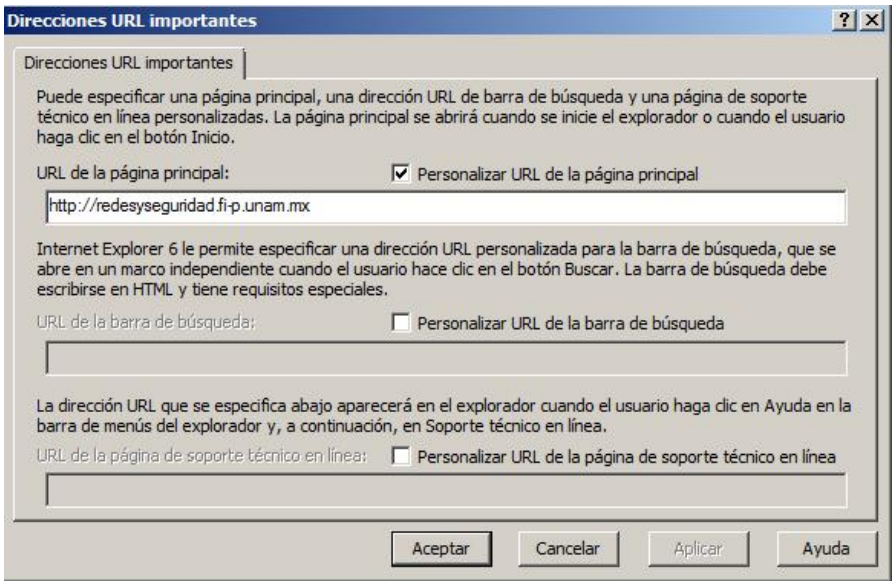

Figura 3. 38 *Pantalla de Direcciones URL importantes*

4.- Posteriormente de la lista mostrada en el árbol, se elige la opción **Seguridad**, en esta opción se restringe el uso de ciertos sitios de Internet como Youtube y Facebook.

5. Para ello una vez elegida la opción de Seguridad, del lado derecho del panel se selecciona la opción Zona de seguridad y clasificación de contenido.

6. Al presionar dos veces esta opción se despliega la una ventana con la configuración de esta opción, en esta ventana en la opción llamada **Zonas de seguridad y privacidad** (figura 3.39), en ella se marca la casilla **Importar la configuración…** y se presiona el botón de **Modificar configuración**.

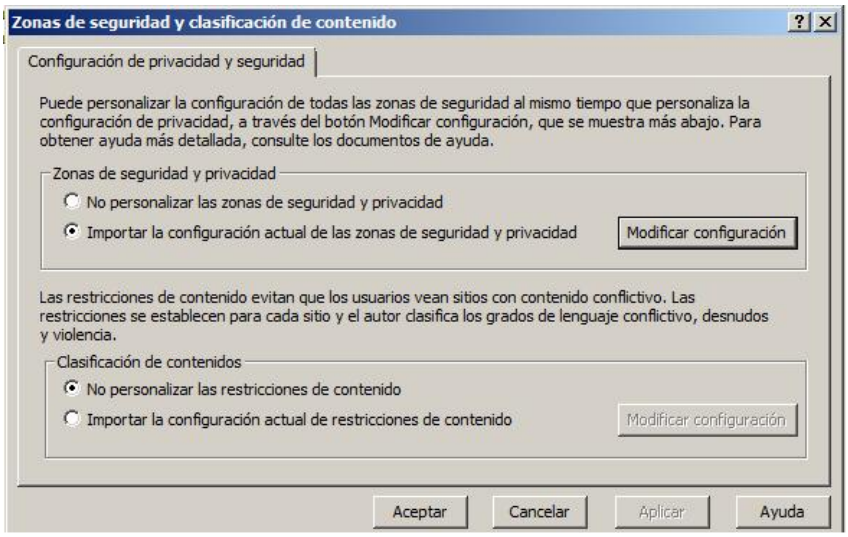

Figura 3. 39 *Zonas de seguridad y clasificación de contenido*

7.- En la nueva ventana se elige la opción **Sitios Restringidos** y se presiona el botón **Sitios**. Es en esta parte donde se coloca la lista de sitios restringidos que no contienen material adecuado para el uso del laboratorio como se ilustra en la figura 3.40.

Figura 3. 40 *Definición de Sitios restringidos*

8.- La última configuración con respecto del navegador se encuentra en la opción llamada **Interfaz de usuario del explorador** colocada en el árbol del panel izquierdo de la consola.

9.- Aquí se elige la opción llamada **Título del explorador**, y aquí se configura la leyenda colocada en el navegador al iniciarse, de esta manera la leyenda es "***Laboratorio de Redes y Seg***". El motivo de no contener el nombre completo es la restricción del número de caracteres en esta opción. Esto se ilustra en la figura 3.41.

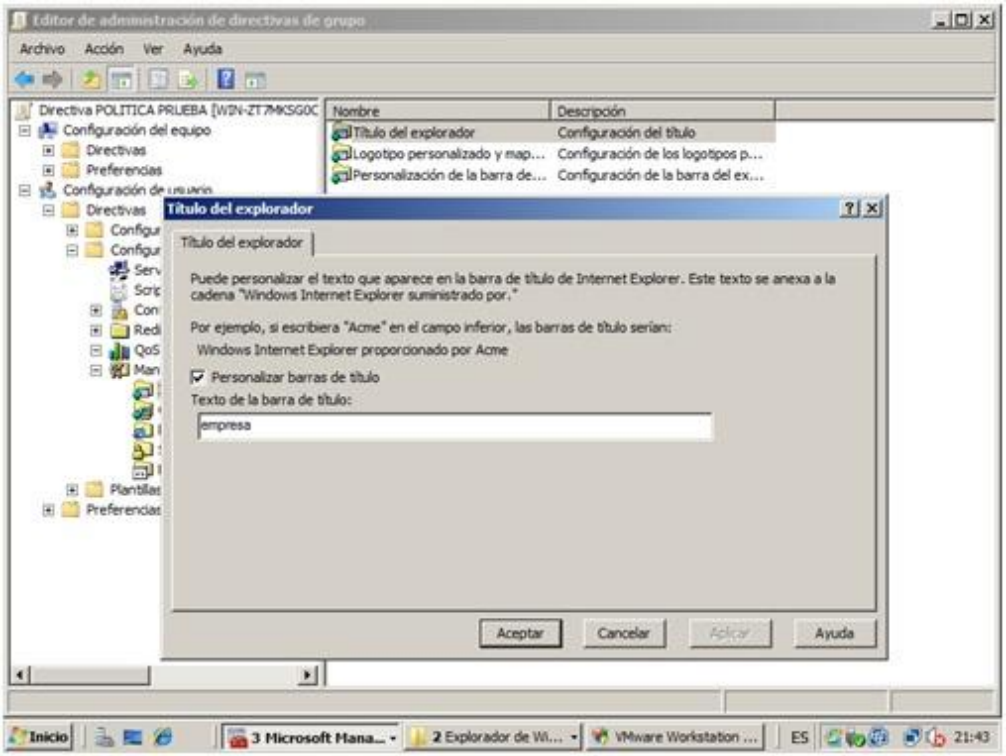

Figura 3. 41 *Definición del Título del navegador de Internet*

10.- Se Aceptan nuevamente los cambios en todas las ventanas pendientes y se cierra la ventana de edición de la directiva de grupo. Con esto queda configurada la política para el uso del navegador

3.12.3 Directiva para la asignación del Administrador Local

Para esta última directiva de seguridad es necesario crear un grupo de seguridad dentro de la OU Usuarios. Para ello se Abre la consola de **Usuarios y Equipos de Active Directory**, en el dominio se busca la ubicación de la OU **LAB REDES** y dentro **Usuarios**.

Se presiona click derecho sobre esta OU y se elige la opción **Nuevo\ Grupo**. Ahí se coloca el nombre del grupo, para este caso llamado **Local Admin** con las opciones mostradas en la figura 3.42.

Se abren las **Propiedades** de este nuevo grupo creado con click derecho, en este sitio se abre la pestaña de **Miembros** y se presiona **Agregar**. En la nueva ventana que se muestra se deben agregar todos los usuarios que serán administradores locales de los equipos cliente. Para este caso se coloca la cuenta de Administrador (no confundir con la cuenta de administrador de dominio) y

Cisco. En caso de requerir agregarse una cuenta más a los administradores locales de los equipos cliente basta con agregar dicha cuenta en este grupo del mismo modo.

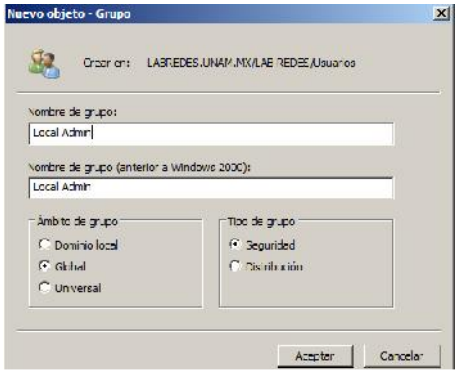

Figura 3. 42 *Creación de un nuevo objeto de tipo Grupo*

Una vez realizada la creación del grupo de seguridad se crea entonces una directiva de seguridad nueva como las anteriores.

Para la edición de esta directiva se sigue en el árbol del panel derecho de la ventana "**Editor de Administración Directivas de grupo**" la siguiente ruta:

Configuración de Equipo\ Directivas\ Configuración de Windows\ Configuración de Seguridad\ Grupos Restringidos

En **Grupos Restringidos** se presiona click derecho y se elige **Agregar** grupo. A continuación solicita un nombre para este grupo, para este trabajo se colocó **Administradores Locales.**

En la nueva ventana se solicita los miembros de este grupo, en esta sección se presiona Agregar y se coloca el nombre del grupo creado recientemente llamado **Local Admin**. En la parte inferior solicita colocar el nombre del grupo al que pertenecerá, en esta sección se presiona agregar y se coloca al grupo llamado **Usuarios de Escritorio Remoto**. Este grupo es el encargado de brindar los privilegios de administrador en el equipo local a todas las cuentas que se coloquen en el grupo **Local Admin** del Active Directory.

Se presiona Aceptar y con esto concluye la edición de la directiva. Como lo ilustra la Figura 3.43

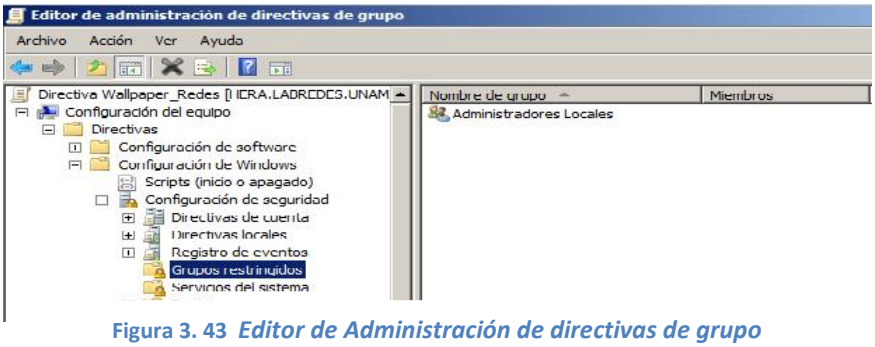

Figura 3. 43 *Editor de Administración de directivas de grupo*

3.12.4 Directiva para la asignación de Software

Para crear una nueva directiva de grupo se sigue el mismo procedimiento hecho en las directivas anteriores.

1. Posteriormente se edita la directiva de grupo, seleccionando la directiva y dando click derecho para elegir la opción "**Editar"**.

2. Se abrirá la ventana del Editor de Administración de directivas de grupo, en dicha ventana del Editor de Administración de directivas de grupo ir a la ruta "**Configuración del equipo \Directivas\ Configuración de Software\ Instalación de software"**.

3. En esta ruta se presiona click derecho dentro del panel de navegación derecho y seleccionar "**Nuevo"**, y posteriormente se elige la opción "**Paquete"**

4. En la venta que se despliega, se coloca la ruta UNC donde se encuentran los archivos de instalación MSI del programa que se desea asignar y se presiona "**Aceptar"**. Cabe señalar que la carpeta debe tener permisos para compartir el contenido con los usuarios del dominio.

5. Se elige el archivo correspondiente a la arquitectura que se desea asignar (x86 o x64), en la ventana de **"Implementar Software"** seleccionar la opción **"Asignada"** y presiona **"Aceptar"** como se ilustra en la figura 3.44.

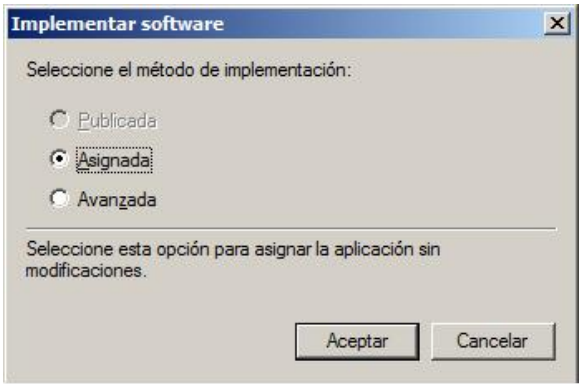

Figura 3. 44 *Selección del método de implementación del software*

6. Posteriormente se observa que ya se ha creado un punto de publicación de **"Software Asignado"**, en el paquete dar click derecho sobre "**Propiedades"**. En la ventana desplegada, ir a la pestaña "**Implementación"** y dar click en "**Opciones Avanzadas".**

7. En la ventana de **"Propiedades"**, ir a la pestaña **"Implementación"** y dar click en **"Opciones avanzadas"**.

8. En **“Opciones Avanzadas”** habilitar la casilla **“Omitir el idioma al implementar este paquete”**, así como la casilla **“Hacer que esta aplicación de 32-bit x86 esté disponible para los equipos Win64”** como se ilustra en figura 3.45.

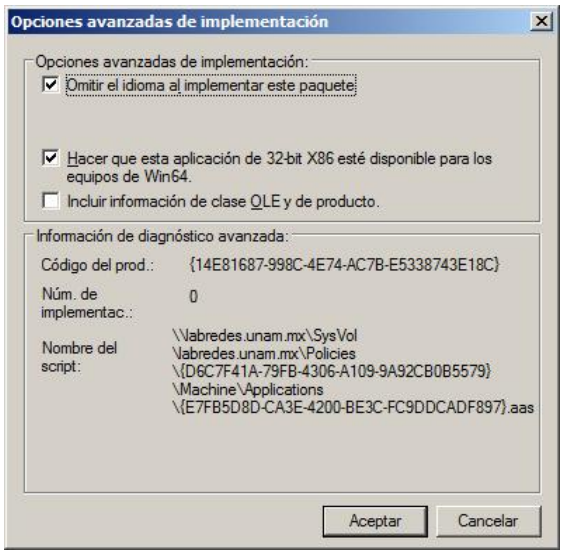

Figura 3. 45 *Venta de Opciones Avanzadas de implementación*

Con lo anterior quedará lista la política de para su asignación a la OU correspondiente.

3.12.5 Directiva para la publicación de Software

Para crear una nueva directiva de grupo se sigue el mismo procedimiento hecho en las directivas anteriores.

1. Posteriormente se edita la directiva de grupo, seleccionando la directiva y dando click derecho para elegir la opción “**Editar”**.

2. Se abrirá la ventana del Editor de Administración de directivas de grupo, en dicha ventana del Editor de Administración de directivas de grupo ir a la ruta “**Configuración de usuario \Directivas\ Configuración de Software\ Instalación de software”**.

3. En esta ruta se presiona click derecho dentro del panel de navegación derecho y seleccionar “**Nuevo”**, y posteriormente se elige la opción “**Paquete”**

4. En la venta que se despliega, se coloca la ruta UNC donde se encuentran los archivos de instalación MSI del programa que se desea asignar y se presiona “**Aceptar”**. Cabe señalar que la carpeta debe tener permisos para compartir el contenido con los usuarios del dominio.

5. Se elige el archivo correspondiente a la arquitectura que se desea asignar (x86 o x64), en la ventana de **"Implementar Software"** seleccionar la opción **"Publicada"** y presiona **"Aceptar"**.

6. Posteriormente se observa que ya se ha creado un punto de publicación de **"Software Asignado"**, en el paquete dar click derecho sobre "**Propiedades"**. En la ventana desplegada, ir a la pestaña "**Implementación"** y habilitar la casilla **"Instalar automáticamente esta aplicación mediante activación por extensión de archivo"** como se muestra en la figura 3.46.

7. Posteriormente se presiona el botón **"Opciones avanzadas"**.

8. En **"Opciones Avanzadas"** habilitar la casilla **"Omitir el idioma al implementar este paquete"**, así como la casilla **"Hacer que esta aplicación de 32-bit x86 esté disponible para los equipos Win64"**.

Con esto se termina la creación de la política para publicar el software en el menú de **"Instalar/Desinstalar Software"** del Panel de Control de los equipos cliente. El siguiente paso es la asignación de dicha política sobre la OU requerida que para este caso es la de equipos del laboratorio.

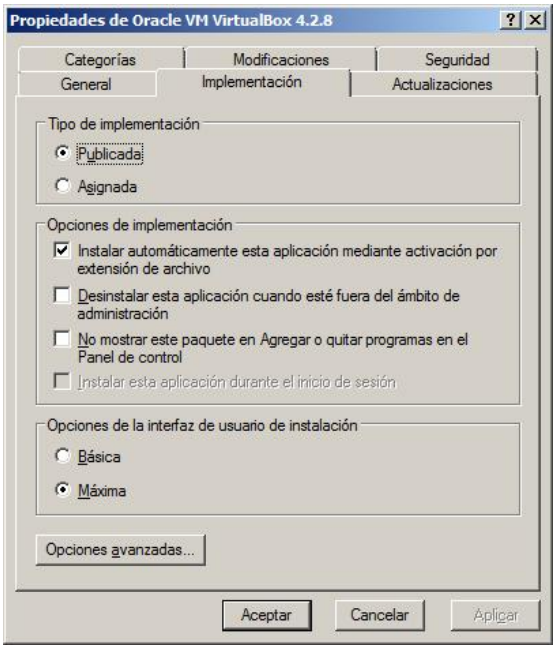

Figura 3. 46 *Venta de Propiedades del Software Publicado*

3.14 Fase de pruebas en producción

La implementación del dominio junto con todos los servicios tales como: Controlador de Dominio, DNS, DHCP, WDS Captura y distribución de sistema operativo, Directivas de Grupo asignación de un papel tapiz así como la asignación y publicación de software quedaron implementados de una manera satisfactoria, se realizaron pruebas en cada una de las fases, es decir se probó que funcionara correctamente el controlador de dominio, el DHCP, la distribución de sistema operativo, etcétera.

Posteriormente, se realizó la liberación de toda la instrumentación de la solución propuesta. En este periodo de tiempo de producción surgieron algunas dudas o inconvenientes por parte de los profesores administradores de la red, a los cuales se les dio una solución casi inmediata. Estos problemas se listan a continuación:

1. Dudas sobre la asignación y publicación software (Virtual box concretamente).

Para la resolución de este evento, se tuvo una constante comunicación por correo electrónico con la profesora responsable del laboratorio, la finalidad era despejar todas las dudas o inquietudes por lo cual se enviaron manuales sobre la publicación y la asignación de software. Estos manuales explican las diferencias entre la publicación y la asignación de software, así como los pasos detallados con imágenes en cada uno de los mismos. La solución final fue instalar el software de manera local en cada uno de los equipos ya que el tener equipos al dominio no implica que no se pueda instalar software de manera local tal y como se ha hecho anteriormente al dominio.

2. Problemas para compartir carpetas mediante la red.

Otro problema al que se enfrentó la administradora del laboratorio fue con respecto a las directivas de seguridad, también con problemas al intentar compartir recursos y carpetas. Debido a la problemática se acudió personalmente al laboratorio para revisar cuál era la fuente del problema. Se encontró que ninguno de los equipos tomaba los parámetros de red por DHCP, razón por la cual, ningún equipo cliente tenía comunicación con el servidor de dominio ni con ninguno de los servicios que éste ofrece. Este problema se corrigió habilitando la opción de tomar parámetros de red por DHCP ya que todo sugiere una modificación de la configuración impuesta inicialmente en los equipos del laboratorio. Se resolvió el problema y se le explicó al personal que estaba en ese momento cuales eran dichos parámetros si es que se deseaba una configuración manual, así como también se procedió a dar una explicación sobre los permisos NTFS de Windows usados para los archivos y para compartir carpetas mediante la red, del mismo modo se les recomendó a los usuarios utilizar las cuentas de dominio creadas previamente, ya que tampoco eran utilizadas.

3. Desinstalación de Wireshark.

Se notificó el problema una vez instalado el software de wireshark, al próximo reinicio se desinstalaba en todos los equipos, esto se corrigió instalando una nueva versión de Wireshark en

el servidor, ya que la versión tenía un conflicto con la que se instalaba de manera local, se recomienda actualizar periódicamente las versiones del software alojadas en el servidor para evitar conflictos de este tipo. Algunos programas pueden instalarse sólo en ciertos perfiles o se instalan en todos los perfiles de usuario, pero esta opción depende del desarrollador de dichos programas, es por eso que en algunos casos no se ve reflejados los cambios de software, aunque el software está instalado en el equipo no se crean los accesos directos en el menú de programas y escritorio.

4. Problema con las particiones lógicas.

Uno de los problemas más difíciles encontrados durante la puesta en marcha del proyecto fue la incapacidad de instalar correctamente el sistema operativo en los equipos del laboratorio. Si bien las pruebas hechas en un entorno virtual con las mismas condiciones fueron exitosas, no ocurrió lo mismo con la instalación real. El principal inconveniente por cual se presentó este problema fue debido a que las computadoras del laboratorio cuentan con dos sistemas operativos instalados en el mismo disco duro del equipo (Windows XP y Linux Fedora) pero en distintas particiones. Para poder tener funcionando los equipos en este modo anteriormente se realizaba la instalación del OS Windows XP y posteriormente el OS Fedora, ya que durante la instalación del Fedora se instala una herramienta propia de Linux llamada GRUB, esta herramienta permite seleccionar el sistema operativo durante el arranque del equipo. El objetivo de la implementación del servicio de WDS fue la distribución del OS XP sin afectar al OS Fedora, por ello se buscó la manera de que el WDS funcionará a pesar de tener un OS distinto de Windows en el equipo. En la fase de pruebas en máquinas virtuales este entorno se reprodujo satisfactoriamente, pero las condiciones en las pruebas en fase de producción las condiciones no se reprodujeron igual, situación que causo conflicto con la reinstalación de los equipos utilizando el WDS. Después de una exhaustiva búsqueda e investigación de dicho problema así como múltiples pruebas, se encontró que herramienta “GRUB” del OS Fedora cambia las propiedades de las particiones del disco duro, situación que causa conflicto durante la instalación vía red del Windows XP con la herramienta de WDS implementada.

Habiendo realizado lo más difícil del problema, es decir la identificación del problema, la resolución fue una tarea sencilla de realizar. Para resolver esta situación es necesario ejecutar una serie de comandos de MSDOS previos a la instalación del Windows XP en la ventana de selección de imagen, durante el proceso para la instalación vía red. En estos comandos se cambia la propiedad de la partición que aloja al OS Windows XP para que sea una partición de tipo “Primaria o principal” que este “Activa” con se muestra en la figura 3.47. Una vez hecho esto se procede con la instalación normal del OS Windows XP.

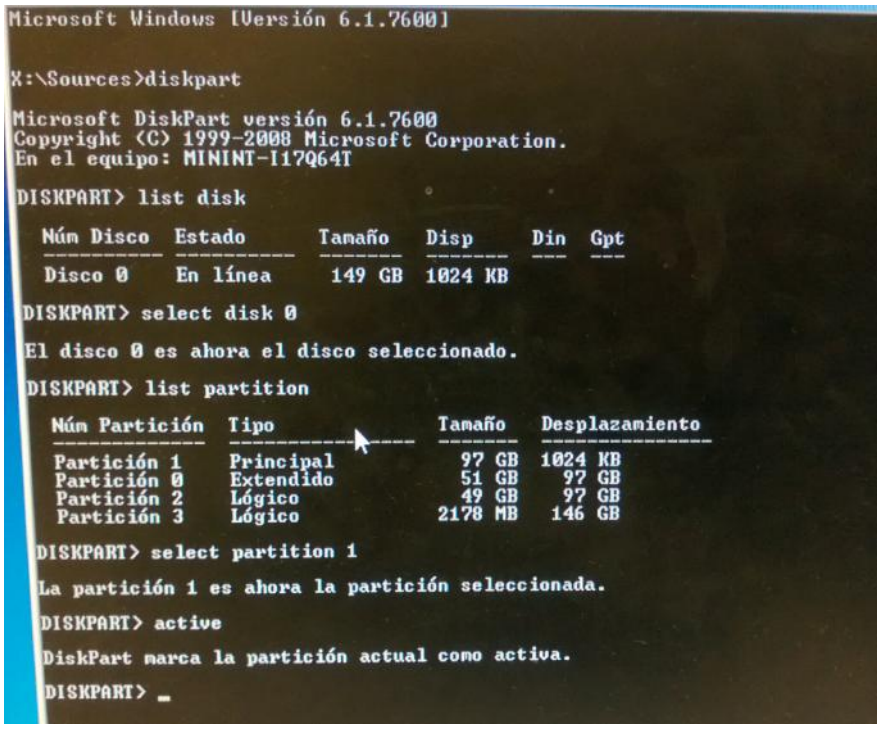

Figura 3. 47 *Instrucción para definir una Partición como "Principal" y "Activa"*

Con este cambio es posible realizar una instalación limpia sobre la partición del OS XP sin afectar la partición del OS Fedora.

5. Problema con los drivers de audio.

Otra situación encontrada y problemática fue la instalación dañada del OS XP. Esta situación se veía reflejada al arranque del OS, una vez encendido el equipo se reiniciaba constantemente. Después de revisiones extensas se encontró que los drivers de audio de los equipos provocaban dicha situación. Al realizarse la instalación automática del equipo, éste tomaba el controlador de audio equivocado lo cual provocaba el colapso del equipo durante el inicio. Cabe señalar que esta situación se presentó ya que los equipos del laboratorio no son homogéneos, por lo cual la imagen de instalación contaba con todos los drivers de audio de cada modelo de computadora del laboratorio, esto provoca que si un equipo durante su instalación no encuentra el driver correspondiente al modelo del equipo intente utilizar uno genérico o en el peor de los casos no tome ninguno. El driver genérico que sea instalado puede no funcionar adecuadamente provocando el colapso del equipo. Para solucionar este problema se optó por remover los drivers de audio de todos los equipos y colocarlos en una carpeta compartida distinta para poder instalados manualmente. Con esto nos aseguramos que la instalación del OS XP de todos los equipos del laboratorio sea satisfactoria y sin errores.

6. Problema con la visualización de las imágenes de instalación.

Una situación inusual que nunca se nos había presentado fue que después de muchas pruebas e imágenes de OS XP creadas y puestas en el servidor de WDS, algunas al ser tratar de ser utilizadas en los equipos cliente durante el proceso de reinstalación vía red, no se lograban visualizar para ser seleccionadas y utilizadas en los equipos. Nos topamos con imágenes que solo eran visibles en ciertos computadoras pero en otras no.

Después de un tiempo encontramos que se tenía un problema con la instancia del servidor de WDS la cual sirve para colocarle dentro las imágenes de OS para que sean vistas y utilizadas por las demás computadoras del dominio. El resultado del análisis y las pruebas concluyen que el hecho de realizar muchas pruebas con las imágenes colocadas en la instancia y la colocación de varias de ellas indiscriminadamente en la instancia provoca un funcionamiento errático y le provoca fallos a la instancia del WDS.

La solución de dicho problema una vez identificado fue sencilla, borrar la instancia creada anteriormente y crear una nueva instancia a la cual solo se le colocaron las imágenes necesarias para instalación del OS en los equipos del laboratorio.

7. Problema con los drivers que no están firmados digitalmente.

Un hecho relacionado con el problema número 5 fue darse cuenta de que varios drivers como los de video de los equipos no están firmados digitalmente. Esta situación se ve reflejada durante la instalación ya que provoca que algunos de los drivers de cada equipos no se instalen de un inicio como el caso de los drivers de audio o el driver de video durante la fase de booteo vía red. Más claramente se observó que durante el booteo vía red, la imagen que se muestra para el proceso de instalación del OS no tiene la resolución ni la combinación de colores adecuada. Esta situación es provocada una que el driver de video no es utilizado, y no es utilizado porque no está firmado digitalmente por el fabricante.

Esta situación solo se presenta en ciertos equipos de la marca DELL, pero no representa un problema para realizar la tarea de reinstalación de las computadoras, por esta situación no fue necesario realizar cambio alguno, pero se presentó como un hecho inusual que merecía una revisión para determinar sus efectos y alcance de afectación para el funcionamiento del proyecto puesto en marcha.

8. Problema para distribuir todo el Software a los equipos de laboratorio.

La imagen distribuida para la reinstalación del OS XP de los equipos contiene cierto software necesario para las prácticas, debido a que la imagen crece en tamaño en la medida que se le agregan programas se decidió dejarle solo algunos programas necesario que no sufren cambios como el packet tracer. Los programas faltantes se omitieron en esta modalidad debido a varias situaciones: el software es demasiado pesado como el office 2007, el software sufre constantes

actualizaciones vía Internet como el navegador Google Chrome o no se cuenta con la licencia correspondiente del software.

Para solventar esta situación se contemplaron otras opciones más: la publicación del software en el menú de Agregar/Quitar Programas, la asignación de software por medio de políticas (esto para el caso del office concretamente) y el compartir el software mediante una carpeta compartida en el servidor.

La primera y segunda opción la cual consiste en publicar el software en el panel de control y la de asignar el software para su instalación al inicio o el apagado del equipo presentan ciertos inconvenientes. La desventaja más grande para estas propuestas es que los programas que se deseen publicar o asignar deben ser obtenidos en su versión de archivo msi (archivo de instalación nativo de Windows alterno al exe), ya sea desde la página del fabricante o creado por medio de otras herramientas de terceros. Esto supone un costo mayor al beneficio obtenido. Otra desventaja es que varios programas como el navegador reciben actualizaciones constantemente lo que conlleva más trabajo para actualizar el software almacenado en el servidor para su distribución.

Por ello se optó por el compartir el software desde una carpeta en una ruta del servidor.

Solo en el caso del Office se optó por realizar una instalación por medio de la asignación de una política, esto para poder automatizar la instalación de esta herramienta bastante ocupada.

Para hacer una comparativa que ilustre la situación anterior y la situación del laboratorio se muestra a continuación una comparación de riesgos basados en las vulnerabilidades y el nivel de impacto de estas al funcionamiento del laboratorio en las figuras 3.48 y 3.49.

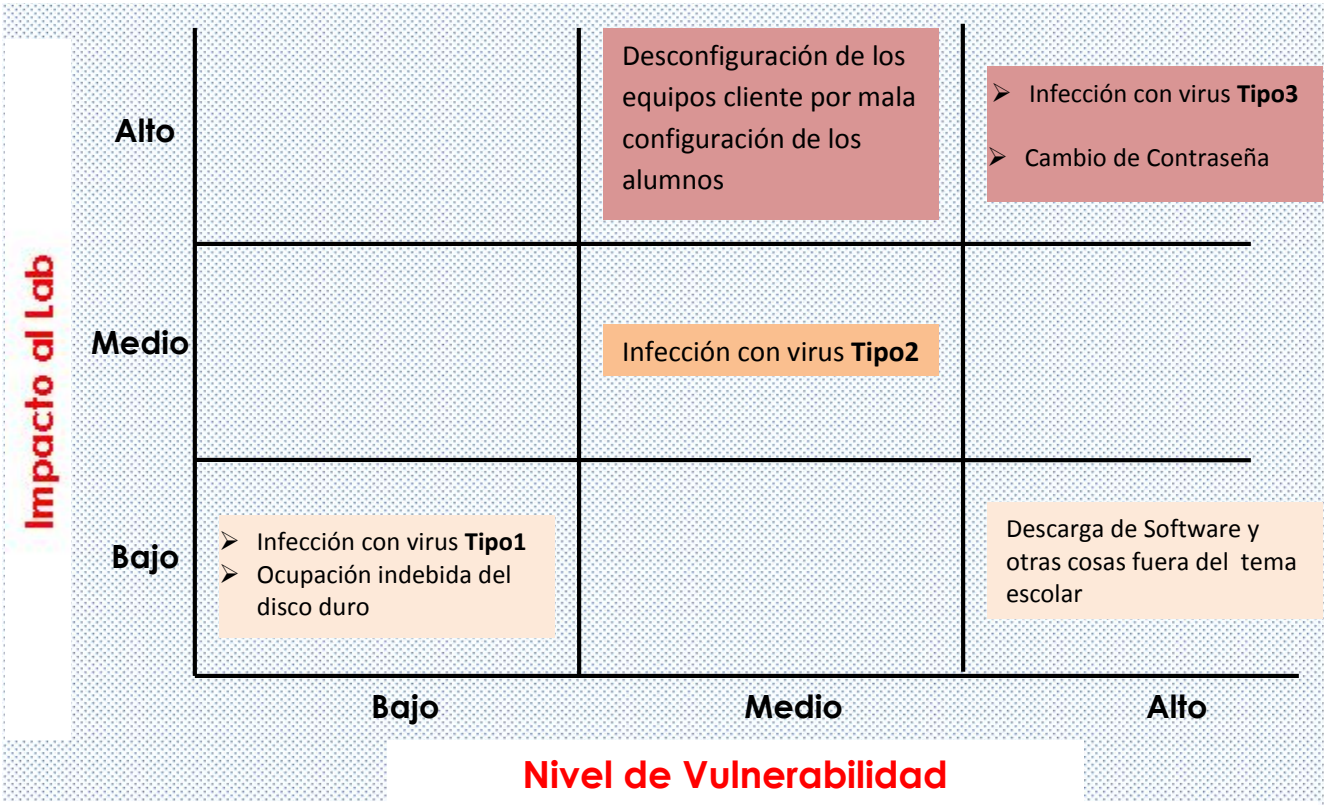

Figura 3. 49 *Diagrama de Riesgo Antes de la instrumentación del Dominio*

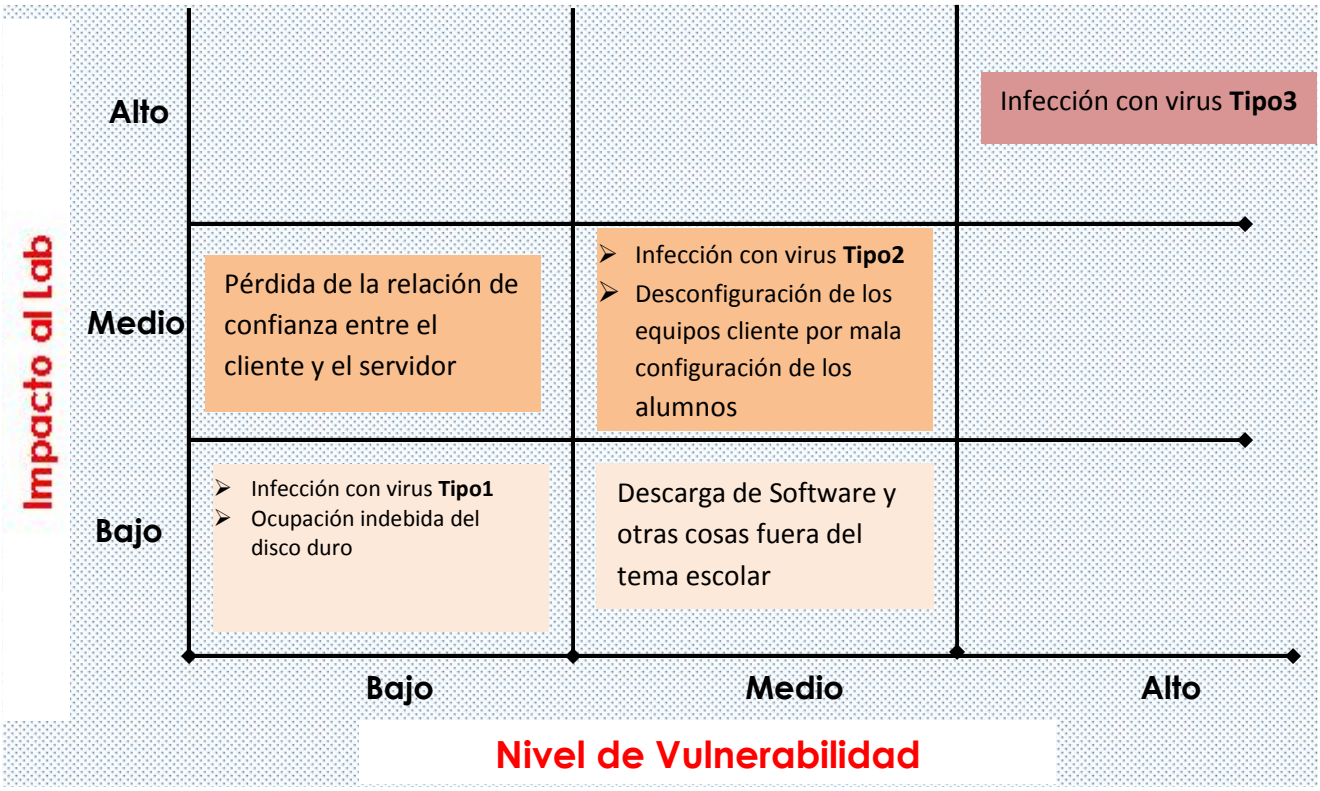

Figura 3. 48 *Diagrama de Riesgo Después de la instrumentación del Dominio*

La definición de los efectos causada por los virus listados en los diagramas anteriores es la siguiente:

- **Virus Tipo 1:** Son aquellos que no afectan el funcionamiento del equipo, trabajan ocultamente sin realizar grandes perjuicios en el equipo. Ejemplo virus replicador de carpetas básicas como “Mis Documentos”

- **Virus Tipo 2:** Son los virus que pueden llegar afectar el funcionamiento del equipo y no permitir la realización de las prácticas. Ejemplo virus que oculta iconos del escritorio y otras carpetas.

- **Virus Tipo 3**: Son todos aquellos virus y malware que inutiliza el uso del equipo por daños directos al sistema operativo o la cuenta con la que se trabaja. Este tipo de malware es el más perjudicial

Como se puede observar la implementación del dominio modifico varios aspectos funcionales de la red, por este motivo el diagrama de riesgo del estado anterior al estado actual cambia significativamente.

Conclusiones

4. Conclusiones

Con base en el objetivo de este trabajo de tesis el cual consistía en la disminución de la carga de trabajo y mantenimiento de los equipos para los encargados del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería, por medio de una administración centralizada se puede constatar que fue alcanzado satisfactoriamente. Esto se logró cabalmente ya que con la implementación del dominio y la herramienta de WDS se redujo considerablemente el tiempo de instalación del sistema operativo de los equipos. Esta tarea fue optimizada para poder dedicarle más tiempo a otras cuestiones importantes del laboratorio como la elaboración de prácticas.

A lo largo de la implementación y la fase de pruebas en producción se detectaron algunos errores no previstos mismos que fueron corregidos lo más pronto que fue posible. Esta situación nos brindó la posibilidad de ver otras necesidades del laboratorio que no se tenían contempladas. Así mismo, con la instrumentación se detectaron algunos nuevos problemas menores que son propios de un dominio, como el desconocimiento del funcionamiento de un dominio por parte de los administradores.

Otro de los beneficios contemplados en el objetivo inicial fue que se ayudó considerablemente a reducir tiempo en la configuración del sistema operativo ya que ahora se cuenta con una imagen del sistema operativo, personalizada con todo lo necesario para realizar las prácticas.

Otro aspecto que cabe resaltar, es que se ayudó a garantizar un mejor y correcto uso de los equipos de cómputo optimizando la manera de compartir recursos y así como la restricción de acceso a sitios como lo son redes sociales, con esto se logró un uso más adecuado de los equipos para actividades meramente académicas durante las clases prácticas. Cabe señalar que un beneficio adicional, que muestra al laboratorio como un espacio dedicado al estudio, fue la colocación de un fondo de pantalla estándar con los logos de la facultad para todos los equipos, con esto se logró tener un ambiente homogéneo y de carácter formal acorde con lo que representa este laboratorio de aprendizaje.

En general el uso de este tipo de herramientas empresariales a nivel académico resultó muy útil para cumplir con los objetivos planteados para mejorar la gestión y administración del Laboratorio de Redes y Seguridad. Como perspectiva a futuro se propone actualizar los equipos de cómputo para poder realizar una actualización del sistema operativo a Windows 7 o más reciente, cambio que conlleva la actualización de algunas características implementadas en el servidor como por ejemplo: agregar el archivo de instalaciones distendidas para versiones de Windows Vista o posterior, la forma en cómo agregar los drivers a dichas imágenes para diferentes arquitecturas, crear e implementar scripts con PowerShell de forma nativa, también, a futuro se recomienda instalar el servicio de IIS para las publicaciones WEB, colocar toda la infraestructura en un servidor con virtualización, así como la virtualización de escritorios mediante Hyper V, también puede implementar un clúster para almacenamiento o balanceo de carga, instalar el servicio de accesos y directivas de redes con la finalidad de poder implementar RADIUS para la administración de la red inalámbrica usando las cuentas de usuario del dominio como método de autenticación. Todas estas mejoras son posibles en un futuro realizando algunos cambios pero muy factibles de realizar debido a que se han sentado las bases para ello con la infraestructura instrumentada.

Cabe resaltar que uno de los problemas que se observó y se resolvió durante la fase de pruebas en producción fue el incorrecto funcionamiento de la herramienta WDS. El problema radicaba en que se iniciaron las pruebas en un ambiente virtual, y algunos elementos usados en esta fase se utilizaron en la fase de producción para poder realizar más ágilmente el proceso de implementación. Este problema tomo tiempo para poder ser resuelto debido al desconocimiento de las causas, con esto comprobamos que la definición del problema y sus causas es la parte más importante para poder solucionar un problema. Una vez encontrado y resuelto el problema de raíz se llegó a la conclusión de que no es recomendable utilizar elementos de ambientes virtuales en ambientes reales y mucho menos en ambientes productivos. Esta fue una gran lección que se aprendió sobre el trabajo, situación que no se comenta en ninguna documentación y son situaciones y enseñanzas que son adquiridas con la experiencia.

Particularmente gracias a este trabajo de tesis, fue posible poner en práctica las habilidades y conocimientos adquiridos tanto en la Facultad como en el trabajo en el Instituto de Ingeniería de la UNAM, esto nos permitió apoyar, con nuestros conocimientos y herramientas, al crecimiento y desarrollo del laboratorio de Redes y Seguridad de la Facultad de Ingeniería.

Es gratificante poder observar que el fruto del trabajo que se desarrolló, está en marcha, siendo usado por los alumnos de la carrera de Ingeniería en Computación del módulo Redes y Seguridad de esta facultad para su beneficio y el de los profesores de las asignaturas que se imparten en este laboratorio.

Bibliografía

Bibliografía

Bibliografía

2012, A. (s.f.). *Las Políticas de Grupo en Windows Server 2008*. Recuperado el 03 de 2012, de http://asir1012.wikispaces.com/Las+Pol%C3%ADticas+de+Grupo+en+Windows+Server+2008

Anderson, J., & Breyer, J. (1996). *Microsoft Windows NT Server, Resource Guide.* Washington: Microsoft Press.

Anderson, J., Breyer, J., & Costantini, P. (1996). *Microsoft Windows NT Server resource kit : technical information and tools for the support professional : for Windows NT Server version 4.0.* Microsoft.

Behrouz, A. F. (2002). *Transmision de datos y redes de comunicaciones.* Madrid: McGraw-Hill Interamericana.

Black, U. (1997). *Reses de Computadoras.* México: Alfaomega.

Bragg, R. (2003). *Designing Security for a Microsoft Windows Server 2003 Network.* Microsoft Press.

Calzada, R. (07 de 2011). *Introducción al Servicio de Directorio.* Obtenido de http://www.rediris.es/ldap/doc/ldap-intro.pdf

Carretero, J., & García, F. (2001). *Sistemas Operativos una visión aplicada.* Madrid: McGraw-Hill, deposito legal 2001 .

casewise. (s.f.). Recuperado el 03 de 2011, de http://www.casewise.com/etom

Chadwick, D. (1996). *Understanding X.500 - The Directory*. Recuperado el 04 de 2011, de http://sec.cs.kent.ac.uk/x500book/

Davies, J. (2003). *Microsoft windows server 2003 : TCP/IP protocols and services technical reference.* Madrid ; México: McGraw-Hill Interamericana.

Degler, S., & Dennis, J. (1999). *Guía avanzada administracion de sistemas Linux.* Madrid: Prentice Hall.

Farrow, R. (1991). *Unix system security : How to protect your data and prevent intruders.* Massachusetts : Mexico : Addison-wesley.

Historia de Sistemas Operativos por Red. (09 de 2005). Recuperado el 02 de 2011, de Osmosis Latína: http://www.osmosislatina.com/diversos/mas_facil.htm

Holme, D., & Ruest, N. (2008). *Configuring Windows Server 2008, Active Directory.* Microsoft Press.

Instalación del rol de servidor DHCP. (s.f.). Recuperado el 11 de 2011, de http://technet.microsoft.com/es-es/library/cc732075.aspx

JAVVIN NETWORK MANAGEMENT & SECURITY. (s.f.). Recuperado el 03 de 2011, de http://www.javvin.com/protocolCMIP.html

Lightweight Directory Access Protocol (LDAP). (s.f.). Recuperado el 05 de 2011, de RFC: http://www.rfc-base.org/rfc-4512.html

Martínez, P. (12 de 2011). *Windows Server 2008 r2*. Recuperado el 04 de 2012, de http://blog.soporteti.net/windows-server-2008/windows-server-2008-r2-repaso-a-las-directivas-de-grupo-especial-teoria/

Microsoft. (01 de 2005). *Introducción a Directiva de grupo*. Recuperado el 04 de 2012, de http://technet.microsoft.com/es-es/library/cc779964(WS.10).aspx

Microsoft. (21 de 2006). *Introducción técnica a los servicios de seguridad de Windows Server 2003*. Recuperado el 08 de 2011, de http://www.microsoft.com/spain/windowsserver2003/technologies/security/securityoverview.aspx

Microsoft. (17 de 2007). *Active Directory Services and Windows 2000 or Windows Server 2003 Domains* . Recuperado el 12 de 2011, de http://support.microsoft.com/default.aspx?scid=kb;en-us;310996

Microsoft. (04 de 2007). *Introducción a los Servicios de dominio de Active Directory*. Recuperado el 08 de 2011, de http://technet.microsoft.com/es-es/library/cc731053(v=ws.10).aspx

Microsoft. (05 de 2008). *Introducción a Servicios de implementación de Windows*. Recuperado el 12 de 2011, de http://technet.microsoft.com/es-es/library/cc770667(v=ws.10).aspx

Microsoft. (2009). *Microsoft Windows ServerCasos de Éxito*. Recuperado el 07 de 2011, de http://www.microsoft.com/spain/compare/analyses/veritest_reliability.mspx

Microsoft. (01 de 2009). *Pasos para instalar AD DS*. Recuperado el 12 de 2011, de http://technet.microsoft.com/es-es/library/cc754438(v=ws.10).aspx

Microsoft. (01 de 2009). *Use Administrative Templates*. Recuperado el 04 de 2012, de http://technet.microsoft.com/en-us/library/c9a96203-875b-4fed-be87-ff092cf7bd88.aspx

Microsoft. (04 de 2010). *Introducción técnica a Windows Server 2008*. Recuperado el 07 de 2011, de http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx

Microsoft. (s.f.). *Configuración del rol de servidor DHCP*. Recuperado el 12 de 2011, de http://technet.microsoft.com/es-mx/library/cc732584.aspx

Microsoft. (s.f.). *Dominio, grupo de trabajo y grupo en el hogar*. Recuperado el 10 de 2011, de http://windows.microsoft.com/es-MX/windows-8/domain-workgroup-homegroup-what-is-difference

Microsoft. (s.f.). *Dynamic Host Configuration Protocol*. Recuperado el 12 de 2011, de http://technet.microsoft.com/es-es/network/bb643151

Microsoft. (s.f.). *Herramientas de implementación de Windows*. Recuperado el 01 de 2012, de http://technet.microsoft.com/es-ar/windows/hh147630.aspx

Microsoft. (s.f.). *Instalación de un servidor DNS*. Recuperado el 12 de 2011, de http://technet.microsoft.com/es-es/library/cc725925.aspx

Microsoft. (s.f.). *Introducción a DHCP*. Recuperado el 06 de 2011, de http://technet.microsoft.com/es-es/library/cc731166(v=ws.10).aspx

Microsoft. (s.f.). *Introducción a DNS*. Recuperado el 10 de 2011, de http://technet.microsoft.com/es-es/library/cc730775.aspx

Microsoft. (s.f.). *Introducción a Servicios de implementación de Windows*. Recuperado el 02 de 2012, de http://technet.microsoft.com/es-es/library/cc770667(v=ws.10).aspx

Microsoft. (s.f.). *Qué es DHCP?* Recuperado el 10 de 2011, de http://technet.microsoft.com/es-es/library/dd145320(v=ws.10).aspx

Microsoft. (s.f.). *Servidor DNS de Microsoft en el entorno de producción - beneficios.* Recuperado el 11 de 2011, de http://support.microsoft.com/kb/555993/es

Microsoft. (s.f.). *Windows Server 2003: Security and Protection*. Recuperado el 09 de 2011, de http://technet.microsoft.com/en-us/library/dd582586%28WS.10%29.aspx

NET IQ. (s.f.). Recuperado el 06 de 2011, de eDirectory: http://www.novell.com/products/edirectory/fsd/whatis.html

Network Dicctionary, OAM. (s.f.). Recuperado el 03 de 2011, de http://www.networkdictionary.com/telecom/oam.php

Northrup, T., & Mackinn, J. (2008). *Configuring Windows Server 2008, Network Infrastructure.* Microsoft Press.

Olguin, H. (1997). *Organización y Administración de Centros de Cómputo.* México: UNAM Fac de Ingeniería.

OPEN LDAP. (s.f.). Recuperado el 06 de 2011, de http://www.openldap.org/

Parker, T. (1992). *Aprendiendo TCP/IP en 14 días.* México: PRICE-HALL HISPANOAMERICANA SA.

Russel, C. (2003). *Microsoft Windows Server 2003 Administrator´s Companion.* Microsoft Press.

Sheldon, T. (1991). *Novell Netware, The Complete Reference.* Madrid: Osborne/Mcgraw-Hill.

Stallings, W. (2004). *Comunicaciones y redes de computadores.* Madrid: Prentice Hall.

Súarez, J. M. (11 de 3 de 2004). *Curso Open LDAP.* Recuperado el 2011, de http://www.redes-linux.com/manuales/openldap/curso_openldap.pdf

Tanenbaum, A. S. (1994). *Redes de computadoras.* México: Pearson Educación de México.

Telecomunications, TOM. (s.f.). Recuperado el 03 de 2011, de http://www.networkdictionary.com/telecom/TOM.php

Tuttle, S., & Ehlenberger, A. (s.f.). *Understanding LDAP, Design and Implementation.* Recuperado el 08 de 2011, de http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf

Ventajas y desventajas del servidor DHCP en Windows Server 2008. (05 de 2011). Recuperado el 11 de 2011, de http://blogdeingmar.wordpress.com/2011/03/23/ventajas-y-desventajas-del-servidor-dhcp-en-windows-server-2008/

Villalón, A. (07 de 2002). *Seguridad En Unix y Redes Autor: .* Obtenido de http://lucas.hispalinux.es/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf

Windows ServerCompare. (10 de 2007). Recuperado el 05 de 2011, de http://www.microsoft.com/windowsserver/compare/windows-server-vs-red-hat-linux.mspx

Wyatt, A. (1998). *Aprendiendo Windows NT Server.* México: Prentice Hall.

X500 Standard. (s.f.). Recuperado el 04 de 2011, de http://www.x500standard.com/

ZYTRAX. (s.f.). Recuperado el 06 de 2011, de LDAP for Rocket Scientists: http://www.zytrax.com/books/ldap/

Apéndice

Script del SYSPREP

```
;SetupMgrTag
[Unattended]
   OemSkipEula=Yes
   InstallFilesPath=C:\sysprep\i386
   TargetPath=\WINDOWS
   OEMPnPDriversPath =
drivers\lan\dell;drivers\lan\dell\PRO1000\;drivers\lan\dell\PRO100;drivers\system\dell;drivers\vi
deo\compaq;drivers\video\dell;drivers\video\hp;drivers\lan\hp;drivers\audio\hp;drivers\system\
dell;drivers\audio;drivers\net;drivers\audio\compaq;drivers\audio\dell
[GuiUnattended]
   AdminPassword="Contraseña definida por el Usuario"
   EncryptedAdminPassword=NO
   OEMSkipRegional=1
   TimeZone=30
   OemSkipWelcome=1
[UserData]
   ProductKey="Serial del Sistema operativo"
   FullName="Laboratorio de Redes y Seguridad"
   OrgName="FI, UNAM"
   ComputerName=
   ProductID=
[TapiLocation]
   CountryCode=52
   AreaCode=55
   LongDistanceAccess="9"
[Identification]
   JoinDomain="Escribir el dominio al que se unirá"
   DomainAdmin="usuario"
   DomainAdminPassword="Contraseña de cuenta de dominio con privilegios para ingresar el
equipo a dominio"

[Networking]
   InstallDefaultComponents=Yes

[Branding]
   BrandIEUsingUnattended=Yes

[Proxy]
   Proxy_Enable=0
   Use_Same_Proxy=0

[RegionalSettings]
   LanguageGroup=1
   Language=0000080a
```

Script para Agregar un usuario al grupo de administradores locales en una computadora

```
on error resume next

Dim DomainName
Dim UsersAccount
Dim AdminsAccount
Dim ITAccount

Set net = WScript.CreateObject("WScript.Network")
local = net.ComputerName
DomainName = "LABREDES"
UsersAccount = "Domain Users"
AdminsAccount = "Enterprise Admins"
ITAccount = "LabAdmins"

set group = GetObject("WinNT://"& local &"/Users")
group.Add "WinNT://"& DomainName &"/"& UsersAccount &""
set group = GetObject("WinNT://"& local &"/Usuarios")
group.Add "WinNT://"& DomainName &"/"& UsersAccount &""
set group = GetObject("WinNT://"& local &"/Administrators")
group.Add "WinNT://"& DomainName &"/"& AdminsAccount &""
set group = GetObject("WinNT://"& local &"/Administradores")
group.Add "WinNT://"& DomainName &"/"& AdminsAccount &""
set group = GetObject("WinNT://"& local &"/Administrators")
group.Add "WinNT://"& DomainName &"/"& ITAccount &""
set group = GetObject("WinNT://"& local &"/Administradores")
group.Add "WinNT://"& DomainName &"/"& ITAccount &""

Set objSysInfo = CreateObject("ADSystemInfo")
```

Script para la Asignación del Office 2007

```
setlocal

REM Declarando las variables


set ProductName=Enterprise
set DeployServer=\\hera\software$\asignado\Office_2007
set ConfigFile=\\hera\software$\asignado\Office_2007\Enterprise.WW\config.xml
set LogLocation=\\hera\software$\asignado\Office_2007\LogFiles

IF NOT "%ProgramFiles(x86)%"=="" (goto ARP64) else (goto ARP86)

:ARP64
reg query
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Microsoft\Windows\CurrentVersion\Uninst
all\%ProductName%
if NOT %errorlevel%==1 (goto End)

:ARP86
reg query
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\%ProductNam
e%
if %errorlevel%==1 (goto DeployOffice) else (goto End)

REM If 1 returned, the product was not found. Run setup here.
:DeployOffice
start /wait %DeployServer%\setup.exe /config %ConfigFile%
echo %date% %time% Setup ended with error code %errorlevel%. >>
%LogLocation%\%computername%.txt

:End

Endlocal
```

Glosario

.NET

Plataforma de Microsoft para el desarrollo de aplicaciones.

AD DS:

De las siglas en inglés *Active Directory Domain Services* (servicio de directorio Active Directory), es el servicio de directorio de Microsoft que permite la gestión de forma segura de la información de usuarios, computadoras y dispositivos de red y así como facilitar el uso compartido de los recursos entre usuarios.

AMD64:

Es una extensión del conjunto de instrucciones x86 utilizado en la micro arquitectura de CPU.

Árbol:

Conjunto de dominios y la relación de confianza que existe entre ellos con la finalidad de compartir recursos entre ellos

Bosque:

Conjunto de árboles de dominio donde existe una relación entre sí

Cliente:

Es un programa o computadora que accede a recursos y servicios brindados por otro llamado Servidor

CMIP:

Protocolo de Información Común, protocolo de administración de red de OSI, creado y estandarizado por ISO para el control de redes heterogéneas.

CMIS:

Servicio de información de administración común. Interfaz de servicio de administración de red de OSI creada y estandarizada por ISO para la supervisión y control de redes heterogéneas.

CORBA:

Acrónimo de **C**ommon **O**bject **R**equest **B**roker **A**rchitecture. Arquitectura de Intermediario Común de Petición de Objetos. La arquitectura **CORBA** pretende definir una norma genérica para la comunicación y la interacción de sistemas creados por distintos fabricantes.

DAP:

Directory Access protocol, estándar para los servicios de directorio basado en X500

DC:

Domain Controller o Controlador de Dominio, servidor en donde se almacena la copia maestra de la base de datos del directorio

DHCP:

Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

DNS:

Sistema de Nombres de Dominio (Domain Name System) es un sistema que permite la resolución de los nombre de dominio a direcciones IP y viceversa

DoD:

Por sus siglas en inglés referido al Departamento de Defensa de los Estados Unidos (Department o Defense).

Dominio:

Agrupación de equipos de cómputo en torno a un servidor centralizado (o varios) que guarda una lista de objetos (usuarios, computadoras, impresoras, etc.) y de nivel de acceso de cada uno.

Equipo:

Representa un equipo de la red y proporciona la cuenta de máquina necesaria para que el sistema inicie sesión en el dominio.

eTOM:

Versión mejorada del modelo TOM, es el estándar de administración más ampliamente usado en procesos de negocios de la industria de telecomunicaciones.

FCAPS:

Acrónimo de *Fault, Configuration, Accounting, Performance, Security (*Falla, Configuracion, Contabilidad, Desempeño, Seguridad), que son las categorías en las cuales el modelo ISO define las tareas de gestión de Redes

Firewall:

Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

GAN:

Red de Área Global (Global Area Network) conjunto interconectado de redes WAN que cubren todo el planeta.

GPO:

Conjunto de políticas o reglas que son posibles aplicar a una serie de objetos del dominio como usuarios y/o equipos con el fin de prohibir, ayudar o permitir a estos realizar cambios, ejecutar programas, acceder a ciertos recursos

Grupo:

Objeto contenedor que representa una agrupación lógica de usuarios, equipos u otros grupos (o los tres) que es independiente de la estructura del árbol de Active Directory. Los grupos pueden contener objetos de diferentes unidades organizativas y dominios.

Grupo de Trabajo:

Grupo de computadoras interconectadas que comparten datos y recursos donde la administración es local

GUID:

Identificador Único Global (Globally Unique Identifier) Un número entero de 128 bits (16 bytes) que se puede usar través de todos los equipos y las redes donde quiera que un identificador único sea necesario. Dicho identificador tiene una probabilidad muy baja de poder ser duplicado.

Hardware:

Es la parte física de equipos, telecomunicaciones y otros dispositivos.

HTTP:

Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

i386:

Conjunto de instrucciones utilizada en la micro arquitectura de CPU, siendo también una denominación genérica dada a ciertos microprocesadores.

ia64:

Arquitectura de 64 bits desarrollada por Intel en cooperación con Hewlett-Packard para su línea de procesadores Itanium e Itanium 2.

IETF:

Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force). Organización abierta de normalización, tiene como objetivo contribuir a la ingeniería de Internet. Actua en áreas como transporte, encaminamiento y seguridad. Regula las propuestas y estándares de Internet, conocidos como RFC.

IIS:

Internet Information Server, Plataforma de Microsoft que brinda servicios de creación, configuración y administración de sitios Web.

IP:

Internet Protocol, Dirección que se utiliza para identificar un equipo o dispositivo en una red

IP dinámica Dirección:

IP temporal que asigna un servidor DHCP

IP estática:

Dirección fija asignada a un equipo o dispositivo conectado a una red.

ISO:

Es la Organización Internacional de Normalización, organismo encargado de promover el desarrollo de normas internacionales de fabricación, pueden ser tanto productos como servicios. La función principal es buscar la estandarización de normas de productos y seguridad para las organizaciones a nivel internacional.

Kerberos:

Protocolo de autenticación de red que permite que dos o más computadoras dentro de una red puedan comunicarse de una manera segura

LAN:

Local Area Network, son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud

LDAP:

Protocolo Ligero de Acceso al Directorio (Lightweight Directory Access Protocol) creado para establecer la comunicación entre un cliente y un servidor utilizando el servicio de directorio

LINUX:

Sistema operativo de libre distribución y modificación, cuenta con varias distribuciones en el mercado.

MAC Address:

Media Access Control, es una dirección compuesta por 12 caracteres hexadecimales única para identificar las tarjetas de Red.

MAN:

Red de Área Metropolitana (Metropolitan Area Network) generalmente se trata de un conjunto de redes LAN dispersas por la ciudad.

NetBIOS:

Sistema básico de Entrada y salida de Red (Network Basic Input/Output System) permite que aplicaciones en equipos distintos se comuniquen por una red de parea local

NTFS:

(Siglas en inglés de New Technology File System) es un sistema de archivos diseñado específicamente para Windows NT, con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base. También soporta compresión nativa de archivos y encriptación (esto último sólo a partir de Windows 2000).

OAM&P:

Operación, administración, mantenimiento y aprovisionamiento (OAM & P) se refiere a un grupo de funciones de gestión que proporciona el sistema o la red en una indicación de fallo, la supervisión del rendimiento, gestión de seguridad, funciones de diagnóstico, configuración y aprovisionamiento de usuarios. Las operaciones incluyen: coordinar las acciones entre la administración, mantenimiento y aprovisionamiento. La administración incluye el diseño de la red, el procesamiento de pedidos, asignación de direcciones, seguimiento del uso y la contabilidad. El mantenimiento incluye el diagnóstico y reparación de problemas cuando no funciona según lo previsto. Aprovisionamiento incluye la instalación de equipos, establecimiento de parámetros, verificar que el servicio está en funcionamiento, actualización y desinstalación.

OMG:

Grupo de Gestión de Objetos (Object Management Group), es una organización sin ánimo de lucro que promueve el uso de tecnología orienta a objetos mediante especificaciones para las mismas.

OS:

Sistema Operativo (Operating System) Conjunto de programas que gestionan los recursos de hardware y provee servicios a los programas de aplicación

OSI:

Modelo conceptual compuesto de siete capas; en cada una de ellas se especifican funciones de red particulares

OU:

Unidad Organizativa (Organizational Units) Objeto contenedor utilizado para crear agrupaciones lógicas de objetos equipo, usuario y grupo.

PAN:

Redes de Área Personal (Personal Area Network) están destinadas para una sola persona

Protocolo:

Lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí

Puerta de enlace:

Sistema de la red que nos permite, a través de sí mismo, acceder a otra red, o dicho de otra manera, sirve de enlace entre dos redes

PowerShell:

Es un shell de línea de comandos y un lenguaje de scripting basado en tareas especialmente diseñado para la administración del sistema. Basado en .NET Framework.

PXE:

(Preboot eXecution Environment) es un entorno para arrancar e instalar el sistema operativo en computadoras a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos instalados.

Red:

Una red de computadoras es un conjunto de dos o más computadoras o dispositivos conectados entre sí y que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, Chat, juegos), etc.

RFC:

Petición de comentarios (Request for Comments), serie de notas sobre internet donde en cada documento contiene una propuesta oficial para un nuevo protocolo.

SAI:

Sistema de Alimentación Ininterrumpida, dispositivo que permite mantener la alimentación eléctrica mediante baterías cuando falla el suministro o se produce una anomalía

Servicio de Directorio:

Conjunto de aplicaciones que almacena y organiza la información de usuarios y dispositivos y recursos de red el cual facilita la gestión de manera centralizada de dicha red.

Servidor:

Dispositivo que presta ciertos servicios y recursos a otros equipos cliente, los cuales están conectados en red

SNMP:

De sus siglas en ingles Simple Network Management Protocol (protocolo simple de administración de Red), protocolo de la capa de aplicación que facilita el intercambio de información para la administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y solucionar problemas

Software:

Conjunto de programas, aplicaciones e instrucciones que se ejecutan para realizar tareas determinadas en una computadora

Sysprep:

Herramienta de preparación del sistema, prepara una instalación de Windows para su duplicación, creación e implementación en equipos cliente.

SYSVOL:

Carpeta compartida en red que contiene las políticas de seguridad y se usa también para replicar en todos los controladores de dominio.

TCP/IP:

Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TMN:

Modelos de administración de Redes de comunicaciones definido por la ITU

TOM:

Telecom Operations Map, El Mapa de Operaciones para Telecomunicaciones es un modelo estándar basado en la división lógica por capas introducida por el TMN

Topología:

Distribución física de una red.

Unix:

Sistema operativo multitarea y multiusuario desarrollado inicialmente por empleados de Bell de AT&T

Usuario:

Representa un usuario de la red y funciona como un almacén de información de identificación y autenticación.

WAN:

Red de Área Amplia (Wide Area Netwok) proporcionan un medio de transmisión a lo largo de grandes extensiones geográficas (por lo general más de 100 km).

WDS:

Servicio de implementación de Windows (Windows Deployment Service), Es una tecnología de Microsoft basada en la instalación de sistemas operativos Windows a través de la Red.

WINS:

Servicio de resolución y registro de nombres de equipos que asigna nombres NetBIOS de equipo a direcciones IP de computadoras con sistema operativo Windows