UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UN DOMINIO EN EL CENTRO DE APOYO A LA DOCENCIA DEL CELE PARA LA OPTIMIZACIÓN DE SUS RECURSOS Y SERVICIOS

T E S I S

Para obtener el título de:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

YOSIMAR OLVERA OLIVA

JULIO CÉSAR RIZO GAONA

DIRECTOR: M.I. MAURICIO MORGADO CASTILLO

AGRADECIMIENTOS

Yosimar

En primer lugar quiero agradecer a Dios y a la Virgensita por cuidarme siempre y permitirme llegar a la finalización de este proyecto con salud y bienestar y por darme la entereza para alcanzar uno más de mis objetivos.

A la Universidad por todas las enseñanzas que me brindó a lo largo de este tiempo, por permitirme formar como profesionista y también como persona, por todos los amigos, compañeros y profesores a los que me dio la oportunidad de conocer y sobre todo por ser un espacio en el que pude desenvolverme en muchos aspectos importantes de mi vida.

A mis padres un agradecimiento especial por todo el apoyo me han brindado, por las palabras de ánimo que siempre tienen para mí y mis hermanos, por el interés que mostraron a lo largo de mis estudios, por brindarme las herramientas necesarias para alcanzar esta meta y sobre todo por haberme dado la oportunidad de tener una carrera universitaria que es la mejor herencia que cualquier hijo puede recibir. No escribo esta dedicatoria separada porque como otras veces se los he mencionado, juntos han logrado cosas importantes como ha sido educar a sus hijos y juntos pueden hacer mucho más.

A mi hermanita Areli por siempre estar ahí con una sonrisa, un abrazo o un juego que me permitía distraerme un momento o tomar un respiro para poder continuar con mis actividades. También ha sido una motivación importante el saber que ella sigue nuestros pasos y nos ve como ejemplo para continuar con sus estudios echándole ganas sabiendo que sí se puede.

A mi hermano y amigo Rubén a quien sin duda además de agradecerle le dedico este trabajo, porque es todo un ejemplo a seguir y porque me ha enseñado que cuando alguien tiene convicción, puede alcanzar sus metas no importando que tan difícil sea o los sacrificios que se tengan que hacer para lograrlas. Para ti mi mano va este trabajo, porque aunque no estemos cerca ahora siempre estás conmigo y pronto volveremos a estar juntos.

A César mi compañero y amigo desde el inicio de la Universidad, le agradezco infinitamente todo el apoyo que me brindó más allá de la realización de este proyecto, siempre fue una persona que estuvo ahí con quien sabía que podía contar y con quien aprendí muchas cosas tanto en la escuela como en la vida.

Y finalmente quiero agradecerle a una personita muy especial que estos últimos meses ha estado a mi lado apoyándome y motivando para seguir adelante con mis proyectos a pesar de los problemas o dificultades que he tenido, una persona que cada día se vuelve más importante en mi vida y a quien cada momento que pasa valoro más. Gracias por todo Jess, espero que ésta sea la primera de muchas metas que alcancemos estando juntos.

AGRADECIMIENTOS

Julio César

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi madre Dalinda y mi padre José Luis, por ser los dos pilares fundamentales en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo, corrigiendo mis faltas y celebrando mis triunfos, y aunque mi padre ya no este conmigo, en vida siempre supo cuidarme y guiarme por un buen camino, y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para el como lo es para mí.

A mi hermano Luis Miguel, por compartir momentos significativos conmigo y apoyarme siempre en todo momento.

A Daniel Colin, por siempre estar dispuesto a escucharme y ayudarme incondicionalmente.

Al M. I. Mauricio Morgado, por brindarme parte de su tiempo, apoyo, guía y asesoramiento en la realización de esta tesis.

A mi compañero Yosimar, por el gran apoyo que tuve de él tanto en la vida profesional como personal.

A Daniel Yoshiro, por ser un gran compañero de trabajo y a la vez un gran amigo en el cual puedo confiar.

A Erika y a Teresa, por darme siempre buenos consejos y apoyarme en todo momento.

Y gracias a todos los que nos brindaron su ayuda en este proyecto.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS.

INTRODUCCIÓN.

Hoy en día vivimos en un mundo cada vez más globalizado, en donde estar comunicados es parte esencial de nuestra vida; ya sea en el ámbito familiar, personal, educacional o laboral, la comunicación ha evolucionado enormemente, convirtiéndose en una de las grandes necesidades para la mayoría de los seres humanos y piedra angular para el desarrollo de la vida como hoy la conocemos. La necesidad de comunicarnos ha implicado un avance en la tecnología para dar solución a esta demanda; cada día existe una mayor diversidad de formas y medios para poder estar comunicados, una de ellas ha sido la aparición de las redes informáticas, permitiendo intercambiar información entre dispositivos de manera rápida, en mayor cantidad y a mayores distancias. Las redes informáticas han evolucionado de forma constante; en el presente, se han vuelto una herramienta valiosa en aspectos tales como educación, investigación, en la industria, en las empresas y en el desarrollo de éstas, debido a que una red no sólo sirve para comunicar, sino que además permite organizar de mejor manera la información y brindar un mayor grado de seguridad a la misma; no obstante, las exigencias de uso han llevado a requerir redes cada vez más veloces, con mayor capacidad de transmisión, confiables y seguras. Actualmente, muchas empresas importantes y poderosas deben parte de su éxito al uso de redes informáticas, por ello invierten una buena cantidad en mecanismos y soluciones que les permitan optimizar al máximo la calidad y el rendimiento de sus recursos.

Sin embargo, las redes informáticas no funcionan por sí solas, requieren de una buena administración para que logren funcionar de forma óptima y así poder garantizar la calidad de los servicios informáticos; por ello, no basta sólo con enfocarse en los servicios a brindar, también es importante conocer la infraestructura, tanto lógica como física de la red, necesaria para asegurar su correcto funcionamiento, siempre con el objetivo de salvaguardar correctamente el principal activo de los usuarios que es la información.

No obstante, las labores de administración no son cosa sencilla, se requiere de una idea clara de los objetivos para los cuales está funcionando la red, para poder llevar a cabo las actividades que permitan facilitar la gestión de los recursos y usuarios. Lamentablemente

existen casos en los que la falta de conocimiento, la falta de recursos económicos o simplemente el desinterés, generan que no se le dé la adecuada importancia a la administración de los activos, que sin duda son la parte fundamental para el crecimiento y desarrollo de toda organización.

Por otro lado, existen tecnologías informáticas que ofrecen herramientas para una adecuada administración de los recursos, servicios, usuarios y de la información, mismas que al ser conjuntadas con una buena estrategia y metodología de uso, solucionan los problemas anteriormente mencionados, facilitando las tareas de los administradores de las redes. Sin embargo, estas herramientas son cada vez más diversas y siempre están evolucionando para mejorar, haciendo en ocasiones complicada su elección, puesto que todas ellas tienen beneficios considerables. Luego entonces, es sumamente importante analizar las necesidades, objetivos y expectativas que cada organización tiene, para que en base a éstos, se haga la elección de las tecnologías que mejor se ajusten a cada organización.

Tomando en cuenta todos los factores mencionados, el presente trabajo se centra en optimizar la administración de los recursos y usuarios que se tienen actualmente en el CAD (Centro de Apoyo a la Docencia del CELE), de modo que se tenga un control más eficiente sobre éstos, a través de estrategias basadas en los requerimientos, necesidades y recursos del propio CAD y a la vez haciendo uso de las tecnologías más apropiadas para llevar a cabo esta tarea. Asimismo, este trabajo se enfoca en desarrollar estrategias dirigidas a salvaguardar aspectos fundamentales de la información tales como la integridad, confidencialidad y disponibilidad. Además, parte del trabajo consiste en el diseño, desarrollo e implementación de una aplicación que automatice la obtención de estadísticas de uso de los recursos de cómputo, de modo que esta información sirva para que los administradores, tengan parámetros de uso que les permitan hacer una mejor planeación de la adquisición, mantenimiento y distribución, tanto de recursos físicos como lógicos. Finalmente se espera que este trabajo establezca las bases para que, si eventualmente la red se extiende, el proceso sea lo más sencillo posible, mediante una infraestructura que permita agregar más equipos a la red sin incrementar la complejidad.

Para su realización, este trabajó se estructuró en cinco capítulos que explican la manera en la que llevó a cabo la solución general, de forma que a través de la lectura de cada uno de ellos, se entienda lo que se realizó en las diferentes etapas del proyecto. A continuación se describe brevemente el contenido de los capítulos:

El primer capítulo trata de los conceptos fundamentales utilizados a lo largo del trabajo, de manera que cualquier persona que lo lea, pueda entender las ideas principales que se exponen en él.

El segundo capítulo explica cuáles eran las condiciones inicales en el CAD al comenzar este proyecto y define las problemáticas identficadas acerca de la administración de los recursos y usuarios del CAD.

El tercer capítulo presenta la solución planteada para dar solución a las problemáticas identificadas, además de que explica las herramientas y sus funcionalidades, alineadas a los requerimientos del Centro, con las cuales se ejecutó la solución.

El cuarto capítulo es acerca de la implementación de la solución, explicando cómo se ajustaron las funcionalidades de las herramientas y configuraciones tecnológicas a las necesidades que se requerían cubrir.

Finalmente, el quinto capítulo expone los resultados obtenidos con la implementación de la solución, explicando si se cumplieron o no los objetivos propuestos y presentando datos que comparan aspectos de la administración y seguridad de los recursos y usuarios del CAD antes y después de la ejecución de la solución. Además, presenta también algunos puntos que se pueden realizar como trabajo a futuro, importantes para el desarrollo de las actividades del Centro.

OBJETIVOS.

El propósito principal de este trabajo es mejorar la administración de los usuarios y recursos de cómputo que se tienen en el CAD (Centro de Apoyo a la Docencia del CELE), mediante un esquema de administración centralizada. Este esquema, deberá facilitar la gestión del software que se usa en el centro, además de permitir desarrollar estrategias dirigidas a salvaguardar aspectos fundamentales de la información tales como integridad, confidencialidad y disponibilidad. Asimismo, deberá ofrecer una administración sencilla, eficaz y segura para los administradores.

Para lograr lo anterior, se plantean los siguientes objetivos particulares:

- Implementar un dominio en la red para mejorar aspectos de seguridad y administración en la misma.

- Instalar y actualizar software vía red a fin de disminuir lo más posible el tiempo invertido por los administradores y ofrecer servicios que sean compatibles en todos los equipos.

- Gestionar a los usuarios del CAD a través de un Directorio Activo, planteando un esquema de roles y políticas para dichos usuarios.

- Desarrollar una aplicación que automatice la obtención de información de uso de recursos de cómputo y generación de estadísticas, a fin de disminuir el tiempo invertido por los administradores en el procesamiento de dicha información.

CAPÍTULO 1

MARCO TEÓRICO

CAPÍTULO 1. MARCO TEÓRICO

INTRODUCCIÓN.

Este capítulo sienta las bases para explicar y entender las ideas de los capítulos posteriores, ya que aquí se explican, de manera general, los conceptos necesarios para entender ¿qué es una red?, ¿cómo se integra?, ¿cómo se lleva a cabo la comunicación en ella y los elementos necesarios que involucra este proceso?. Además, también se abordarán aspectos fundamentales de la seguridad en las redes como son los servicios y las políticas de seguridad. Finalmente, se trata el tema de la administración de redes enfatizando la importancia que tiene y comparando dos diferentes formas de administración, la administración centralizada y la descentralizada.

TEMA 1. REDES DE COMPUTADORAS.

La necesidad de intercambiar información y compartir recursos informáticos en las organizaciones, ha sido factor fundamental para su crecimiento y desarrollo. Para satisfacer estas necesidades se crearon las redes de computadoras, que son “dos o más computadoras conectadas entre sí que permiten compartir recursos e información” (1.1). Esta conexión se puede realizar mediante uno o más medios de transmisión. Los medios de transmisión pueden ser, desde un cable de datos hasta el uso del espacio aéreo como medio de interconexión. Los recursos que una computadora comparta en red, incluyen unidades de almacenamiento de datos, archivos, programas, dispositivos tales como impresoras, escáners, etc. Debido a esto, el uso de las redes de computadoras es actualmente tan importante, que pensar en una organización que no haga uso de ellas es complicado.

1.1 ELEMENTOS QUE INTEGRAN UNA RED.

Para que una red de computadoras funcione correctamente, es necesaria la interacción de varios elementos tales como las estaciones de trabajo, las cuales son computadoras capaces de aprovechar los recursos que otras computadoras comparten en la red (1.2). Cada computadora conectada a la red, conserva la capacidad de funcionar de manera independiente, es decir, realiza sus propios procesos de trabajo. Para que las estaciones de trabajo puedan comunicarse con otras, requieren contar con una tarjeta de interfaz de red (Network Interface Card, NIC), esta proporciona conectividad entre ellas permitiéndoles compartir recursos e información. Las NIC de cada computadora se conectan a través de un medio de transmisión, que es el canal que permite la transmisión de datos entre las computadoras en una red. Los medios de transmisión se clasifican en 2 tipos:

- Guiados o terrestres.
  Los medios de transmisión guiados, son aquellos que utilizan un medio sólido para guiar la señal, como un cable. Algunos ejemplos son:

- UTP (Unshielded twisted pair). Par trenzado sin blindaje. Consiste en 4 pares de alambres de cobre aislados, como en una molécula de ADN. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor (4.3).

- STP (Shielded twisted pair). Par trenzado blindado. Es similar al UTP con la diferencia de que este tipo de cable cuenta con un material envolvente contra las interferencias. El STP es más caro en comparación con el UTP.

- Coaxial. Consta de un alambre de cobre duro, en su parte central, que constituye el núcleo, el cual se encuentra rodeado por un material aislante (4.1).

- Fibra óptica. Transmite datos por medio de una serie de pulsos de luz a través de una hebra fina de fibra de vidrio (1.3).

En la tabla 1.1 se muestran algunas de las características principales de los medios de transmisión guiados.

Medio	Velocidad de transmisión (Mbps, mega bits por segundo)	Distancia máxima entre nodos.	Tipo de conector	Ventajas	Desventajas
UTP	10, 100 y 1000	100 metros	RJ45	Fácil manejo y bajo costo	Susceptibilidad a interferencias
STP	10, 100 y 1000	100 metros	RJ45	Menor susceptibilidad a interferencias	Mayor costo y dificultad de manejo
Coaxial	10	185 metros	BNC	Bajo costo y fácil de instalar	Poca inmunidad al ruido electromagnético
Fibra óptica	1000	Decenas de kilómetros	ST, SC y MT-RJ	Mayor velocidad de transmisión, atenuación muy baja	Alto costo

Tabla 1. 1 Características de los medios de transmisión guiados (14).

- Medios de transmisión No Guiados o aéreos.
  Los medios de transmisión no guiados, son aquellos donde la transmisión no se realiza mediante un medio físico sino que se utiliza el aire o el espacio exterior. Por ejemplo:

- Microondas. Son señales electromagnéticas comprendidas en un rango de frecuencia de entre 300MHz y 300GHz. Cuanto mayor sea la frecuencia utilizada, mayor es el ancho de banda y por lo tanto mayor es la velocidad de transmisión (2.3). Para transmitir estas señales, se utilizan antenas parabólicas que permiten aplicaciones para comunicaciones a decenas de kilómetros. Este sistema es ampliamente utilizado en transmisiones telefónicas y de video. La propagación de las microondas se ve afectada por las tormentas y otros fenómenos atmosféricos.

- Infrarrojo. Son señales producidas por un láser o un LED. Tiene un alcance de hasta varios kilómetros para su transmisión, aunque la velocidad a estas distancias es de tan sólo 100 Kbps. A distancias menores, por ejemplo de 2 km, la velocidad de transmisión puede alcanzar 1.5 Mbps. Las comunicaciones con infrarrojos se llevan a cabo mediante transmisores/receptores; éstos deben estar alineados directamente, o bien deben estar accesibles a través de la reflexión en una superficie (2.4). A diferencia de las microondas, los rayos infrarrojos no pueden atravesar objetos. Sin embargo tienen inmunidad contra la interferencia eléctrica.

- Satélites. Generalmente son estaciones que retransmiten microondas desde el espacio exterior. Se usa como enlace entre dos o más receptores/transmisores terrestres denominados estaciones base (2.2). La mayoría de los satélites que proporcionan servicio de enlace punto a punto operan en el intervalo de frecuencia de entre 5,9 y 6,4 GHz para la transmisión desde las estaciones terrestres hacia el satélite y entre 3,7 y 4,2 GHz para la transmisión desde el satélite hasta la Tierra.

- Ondas de radio. Son señales electromagnéticas cuya longitud de onda es mayor que las microondas alcanzando cientos de kilómetros. Las ondas de radio oscilan en frecuencias entre unos cuantos kilohertz (kHz) y unos cuantos terahertz (THz). Las ondas de radio son omnidireccionales, es decir, que pueden viajar en cualquier dirección, esto hace que no necesiten antenas parabólicas para su transmisión (2.4). Las ondas de radio son menos flexibles a la atenuación producida por la lluvia u otros fenómenos meteorológicos.

- Wi-Fi. Es una de las tecnologías de comunicación inálambrica más utilizada hoy en día. Wi-Fi, basado en el estándar IEEE 802.11 no es la abreviatura de Wireless Fidelity, simplemente es un nombre comercial. Las redes inalámbricas se componen normalmente de una o más computadoras portátiles o de escritorio que deben contar con tarjetas de red inalámbricas y de una estación base central, conocida como punto de acceso. Sin embargo, es posible tener una red inalámbrica en ausencia de algún punto de acceso. A este tipo de redes se les conoce como redes ad hoc o infraestructura en donde la comunicación se hace sin control central y sin conexiones a otras redes, únicamente entre los dispositivos que se han encontrado próximos entre sí (3.5) (7.4).

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado (13.1):

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de frecuencia de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps , 54 Mbps y 300 Mbps, respectivamente.
- En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de frecuencia de 5 GHz. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es menor que el de los estándares que trabajan a 2.4 GHz, debido a que la frecuencia es mayor y por lo tanto tiene un menor alcance.

- WiMAX. Son las siglas de Worldwide Interoperability for Microwave Access (Interoperabilidad mundial para acceso por microondas). Es un sistema de comunicación digital conforme con los estándares de acceso inalámbrico IEEE 802.16.
  WiMAX permite conexiones de hasta 50-60 Kilómetros de distancia. Si lo comparamos con el protocolo Wireless IEEE 802.11, el cual está limitado en la mayoría de las ocasiones a unos 100 metros, nos damos cuenta de la gran diferencia que separa estas dos tecnologías inalámbricas.

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos. Dependiendo del medio, la red inalámbrica tendrá diferentes características (13.2).

La importancia de conocer la infraestructura necesaria para una red de computadoras es que permite conocer qué elementos se requieren y cómo unirlos para poder hacer que la red sea funcional.

1.2 CLASIFICACIÓN DE REDES POR COBERTURA GEOGRÁFICA

Las redes pueden tener diversos usos, basados en los diferentes objetivos que cada organización tiene. Puede haber casos donde se requiera tener una red en un solo edificio; por ejemplo, un laboratorio escolar, o casos en los que se requiera que la red abarque una mayor área, como es una organización que tiene sucursales en distintas zonas del país o incluso del mundo. Para esto, las redes se pueden clasificar en base a la cobertura geográfica que abarcan. Las diferencias entre las categorías que se muestran a continuación son cada vez más difusas, tanto en términos tecnológicos como de posibles aplicaciones; no obstante, esta clasificación es una forma sencilla de organizar su estudio (2.1):

- PAN. (Personal Area Network) Redes de área personal.
  Las redes de área personal están integradas por los dispositivos situados en el entorno personal y local del usuario, ya sea en la casa, trabajo, escuela, etc. Esta configuración permite establecer una comunicación entre los dispositivos de manera rápida y eficaz.

- LAN (Local Area Network). Red de área local.
  Es una red de comunicaciones de cobertura pequeña, generalmente un edificio o a lo mucho un conjunto de ellos próximos (2.5). Por lo general, las LAN tienen tres características particulares:
  1. Un campo de acción cuyo tamaño no es mayor de unos cuantos kilómetros.
  2. Una velocidad de transmisión alta.
  3. Pertenencia a una sola organización.

  La red del CAD es de este tipo.

- MAN (Metropolitan Area Network). Redes de área metropolitana.
  Es una red que conecta varias LANs a través de medios de transmisión tales como UTP, fibra óptica, microondas, etc. Las MAN son redes que se extienden sobre áreas geográficas de tipo urbano, como una ciudad, aunque en la práctica dichas redes pueden abarcar varias ciudades (8).

- WAN (Wide Area Network). Redes de área amplia.
  Generalmente, se considera como redes de área amplia a aquellas que cubren una extensa área geográfica. Las redes WAN abarcan países enteros, y pertenecen a múltiples organizaciones.

En la Tabla 1.2, se muestra una comparación de la cobertura que tienen los diferentes tipos de redes así, como un ejemplo de donde podrían funcionar.

Distancia entre procesadores	Nodos ubicados en el mismo…	RED
1m	m^2	PAN
10m	Cuarto	LAN
100m	Edificio	LAN
1km	Campus	LAN
10km	Ciudad	MAN
100km	País	MAN
1000km	Continente	WAN

Tabla 1. 2 Clasificación de redes por cobertura geográfica (3.1).

Actualmente, esta clasificación no tiene un gran impacto en la funcionalidad de las redes, puesto que los avances tecnológicos han sido tales que las diferencias entre una red MAN y una LAN, no pasan por los aspectos funcionales de la red, sino únicamente son en términos de extensión geográfica.

1.3 TOPOLOGÍAS DE RED

Como se mencionó anteriormente, las redes pueden clasificarse con base a su tamaño, sin embargo también es importante considerar la forma que debe tener dicha red para cumplir con los requerimientos de las organizaciones. Este aspecto es relevante, ya que involucra características tales como la velocidad, seguridad, mantenimiento, etc.

Al hablar de forma, se hace referencia al concepto de topología de red, es decir, la forma geométrica en la que se conectan los diversos dispositivos que conforman una red, con el objetivo de proporcionar la máxima fiabilidad en la transmisión de datos (5.1).

En la actualidad existen diferentes topologías de red, a continuación se mencionan los principales:

- Bus: En esta topología todos los dispositivos se encuentran conectados a un mismo segmento de cable de red. Este segmento es conocido como medio de transmisión lineal o bus lineal, el cual permitirá la transmisión y recepción de datos. En esta topología, cuando se realiza una transmisión de datos desde cualquier dispositivo, ésta se propaga en ambos sentidos, y es recibida por el resto de los dispositivos, esto implica que cualquiera de ellos tiene acceso a la información transmitida.

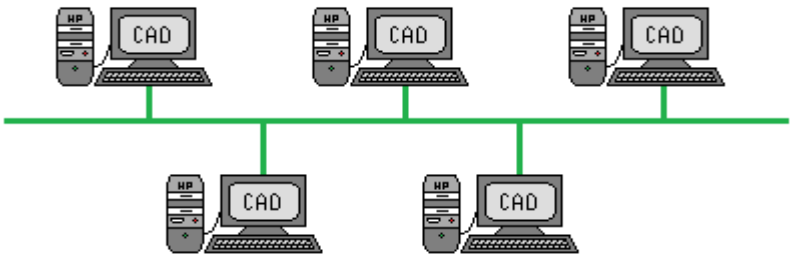


Figura 1. 1 Topología de Bus.

- Malla: En este tipo de topología, todos los dispositivos de la red se encuentran interconectados de forma que un nodo puede recibir o transmitir información de cualquier

otro nodo por diversos caminos. Esto permite que si algún enlace falla, sea posible mantener la comunicación utilizando otro enlace.

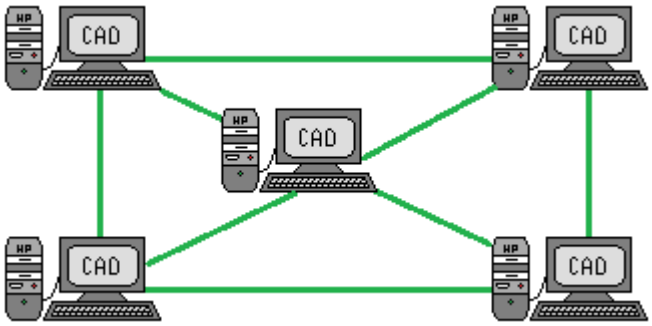


Figura 1. 2 Topología de Malla.

- Estrella: En esta topología todos los dispositivos de la red se encuentran conectados directamente a un dispositivo central, el cual controla el envío y recepción de datos permitiendo la comunicación entre ellos. Cuando un dispositivo de la red desea comunicarse con otro, manda los datos al dispositivo central, el cual se encarga de retransmitirlos al dispositivo requerido para entablar la comunicación.

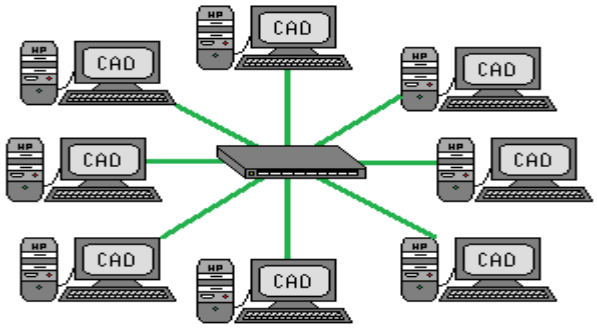


Figura 1. 3Topología de Estrella.

- Árbol: Este tipo de topología cuenta con uno o varios dispositivos centrales secundarios, que se enlazan con un dispositivo central primario. En cada uno de los dispositivos centrales secundarios se conectan los nodos que forman la red. Este tipo de topología

puede considerarse como una combinación de varias topologías en estrella, con la topología de bus.

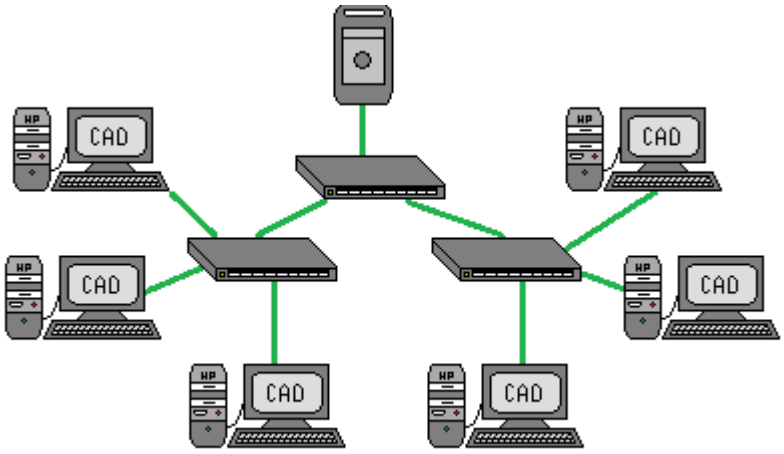


Figura 1. 4 Topología deÁrbol.

- Anillo: En esta topología cada dispositivo está conectado solamente con sus vecinos inmediatos formando un anillo. La información en este tipo de red pasa de dispositivo a dispositivo en una sola dirección hasta que alcanza su destino.

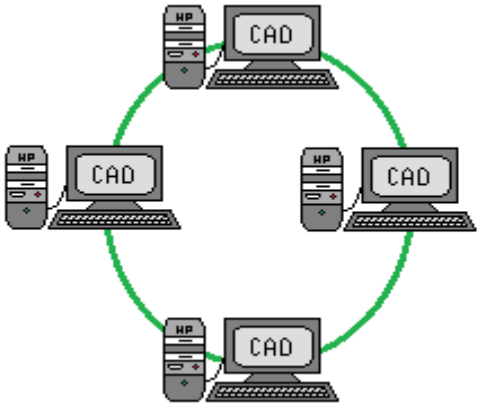


Figura 1. 5 Topología deAnillo.

- Híbrida: En una topología híbrida, se combinan dos o más topologías para formar un diseño de red completo. La topología híbrida es una de las más utilizadas ya que permite soluciones de red de alta complejidad o bien permite solucionar problemas debido al aumento en el número de dispositivos.

Como se puede observar, existen varias topologías que una red puede tener, pero la elección de alguna de éstas se basa en los requerimientos de las organizaciones y de las ventajas y desventajas de cada una de las topologías.

Para cumplir con los objetivos planteados en este trabajo referentes a cuestiones de seguridad, se requiere que la red cuente con al menos un dispositivo central que controle la transferencia de datos entre las máquinas. En la tabla 1.3 se mencionan algunas de estas ventajas y desventajas de las diferentes topologías.

Topologías	Ventajas	Desventajas
Bus	• Si un nodo falla la red sigue funcionando	• Si el bus no funciona la red tampoco • Susceptible a colisiones
Malla	• Si un nodo falla la red sigue funcionando	• Alto costo por la cantidad de cable necesario
Estrella	• No hay colisiones • Mejor control en la transferencia de datos	• Si el dispositivo central falla la red también
Árbol	• Permite un buen control de la transferencia de datos cuando la cantidad de nodos es alta	• Si el dispositivo central primario falla la red también; si lo hace uno de los dispositivos secundarios, los nodos conectados quedan fuera de la red
Anillo	• No hay colisiones	• Todos los nodos se enteran de la información que circula en la red
Híbrida	• Soluciona problemas que requieren de un diseño de red más complejo	• Difícil de configurar y alto costo para su implementación

Tabla 1. 3 Comparativa de Topologías.

TEMA 2. MODELO DE REFERENCIA OSI.

Una vez definido qué es una red y algunas de sus particularidades como son su integración y las formas que pueden tener, a continuación se explica cómo se lleva a cabo la comunicación entre los dispositivos que las conforman. Es importante mencionar que las comunicaciones requieren de un conjunto de reglas que precisen la forma en que debe efectuarse este proceso dentro de las redes. A este conjunto de reglas se les conoce como protocolo (1.4). Además de los protocolos, las redes requieren de guías y reglas que se refieran al tipo de componentes que deben usarse, a la manera de conectar los componentes, así como a los protocolos de comunicación que hay que emplear de manera que equipos de distintos fabricantes puedan trabajar entre sí sin problemas; a estas especificaciones se les conoce como estándar (1.4).

Sin embargo, debido a la complejidad que implican las comunicaciones en las redes, un solo estándar no fue suficiente, en su lugar se estructuró una arquitectura de comunicaciones que dividió las distintas funcionalidades en partes más manejables. Esta arquitectura fue establecida por la Organización Internacional de Estandarización ISO (International Organization for Standarization), cuyos objetivos principales son el desarrollo, actualización, unificación, aprobación, ampliación de las normas y estándares que se emplean, y el resultado fue el modelo de referencia OSI (Open System Interconection) Interconexión de Sistemas Abiertos (2.6).

2.1 CAPAS DEL MODELO OSI.

El modelo OSI está conformado por distintas capas, cada capa realiza un subconjunto de tareas relacionadas entre sí. Además, cada una de ellas depende de la capa inferior y proporciona servicios a la capa superior.

El modelo OSI se divide en 7 capas (Figura 1.1).

Figura 1. 6 MODELO OSI.

A continuación se explican las funciones de cada una de las capas (2.7) (3.2):

Capa Física

Se encarga de la transmisión de cadenas de bits sobre el medio de transmisión; está relacionada principalmente con 3 características importantes para acceder al medio:

- Mecánicas: relacionadas con las propiedades físicas de la interfaz de red y el medio de transmisión. Se incluye la especificación del conector que transmite las señales a través de conductores llamados circuitos.
- Eléctricas: especifica cómo se representan los bits en cuanto a voltaje, así como su velocidad de transmisión.
- Funcionales: especifica las funciones que realiza cada uno de los circuitos de la interfaz de red entre el dispositivo y el medio de transmisión.

Capa de Enlace de Datos

Provee un servicio de transferencia de datos fiable a través del enlace físico, además proporciona los medios para activar, mantener y desactivar el enlace. El principal servicio proporcionado por esta capa a las capas superiores es el de detección y control de errores en el conjunto de datos que son intercambiados (tramas) causados por daño, pérdida o duplicidad de ellos.

Capa de Red

La capa de red determina la ruta por la cual deben pasar los paquetes (conjunto de tramas) del origen al destino. Además, proporciona independencia a los niveles superiores respecto a las técnicas de transmisión utilizadas para conectar los dispositivos.

Capa de Transporte

Proporciona un mecanismo para intercambiar datos entre dispositivos. La función principal de esta capa consiste en asegurar que todos los datos de la capa superior lleguen correctamente al otro dispositivo eligiendo el tipo de conexión de transporte más conveniente. El tipo más común de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes en el mismo orden en que fueron enviados. Sin embargo, existe otro tipo de conexión de transporte, en el cual se pueden enviar datos a multiples dispositivos sin garantizar el orden de distribución de los datos. El tipo de servicio se determina cuando se establece la conexión.

Capa de Sesión

Permite que los usuarios de diferentes dispositivos puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo el transporte de datos ordinario, permitiendo al usuario acceder a un sistema a distancia o transferir un archivo entre dos dispositivos. Uno de los servicios de la capa de sesión consiste en gestionar el control de la comunicación. Las sesiones permiten que la transmisión de datos vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado.

La capa de sesión permite el servicio de recuperación, proporcionando un procedimiento de puntos de comprobación a lo largo del flujo de datos, de forma que si ocurre algún tipo de falla entre puntos de comprobación, la capa de sesión permite retransmitir todos los datos desde el último punto de comprobación correcto.

Capa de Presentación

La capa de presentación es la encargada del formato de los datos. Esta capa traduce los datos entre formatos específicos para asegurarse de que los datos sean recibidos en un formato legible para el dispositivo al que se presenta. Algunos ejemplos de servicios específicos que se pueden realizar en esta capa son los de compresión de datos, que se puede utilizar para reducir el número de bits que tienen que transmitirse, y el concepto de cifrado de datos que se necesita por políticas de seguridad.

Capa de Aplicación

La capa de aplicación proporciona a los programas de aplicación un medio para que accedan al entorno OSI. En esta capa residen las aplicaciones de uso general como la transferencia de archivos, el correo electrónico, gestores de bases de datos, entre otros.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación, sino que suele utilizar programas que a su vez interactúan con este nivel.

2.1.1 TRANSMISIÓN DE DATOS EN EL MODELO OSI.

Para entender cómo se transmiten los datos mediante el empleo del modelo OSI, se describe un ejemplo ilustrado en la figura 1.2.

El proceso emisor tiene algunos datos que desea enviar al proceso receptor. Este entrega los datos a la capa de aplicación, la cual añade entonces la cabecera de aplicación AH (Application Header), por sus siglas en inglés, que contiene información necesaria para el protocolo de esta capa, a la parte delantera de los datos y entrega el elemento resultante a la capa de presentación.

La capa de presentación trata el elemento resultante como si fueran solamente datos y le añade su propia cabecera PH (Presentation Header), por sus siglas en inglés. Es importante observar que la capa de presentación no sabe qué parte de los datos que le dio la capa de aplicación, corresponde a AH, y cuáles son los que corresponden a los verdaderos datos del usuario.

Este proceso se sigue repitiendo hasta que los datos alcanzan la capa de enlace, que normalmente añade una cabecera DH (Data Header) y una cola DT (Data Tail), por sus siglas en inglés. La unidad de la capa 2, llamada trama, se pasa al medio de transmisión mediante la capa física. En la otra máquina, se van quitando una a una las cabeceras, a medida que los datos se transmiten a las capas superiores, hasta que finalmente llegan al proceso receptor.

La idea fundamental, a lo largo de este proceso, es que si bien la transmisión de datos es vertical, cada una de las capas está programada como si fuera una transmisión horizontal. Cuando la capa de transporte emisora obtiene un mensaje de la capa de sesión le asigna una cabecera de transporte y virtualmente lo envía a la capa de transporte receptora. Sin embargo, lo que realmente sucede es que entrega el mensaje a la capa de red de su propia máquina, y así sucesivamente a las capas inferiores hasta llegar a la capa física que es la que realmente transmite los datos a la computadora receptora a través del medio físico.

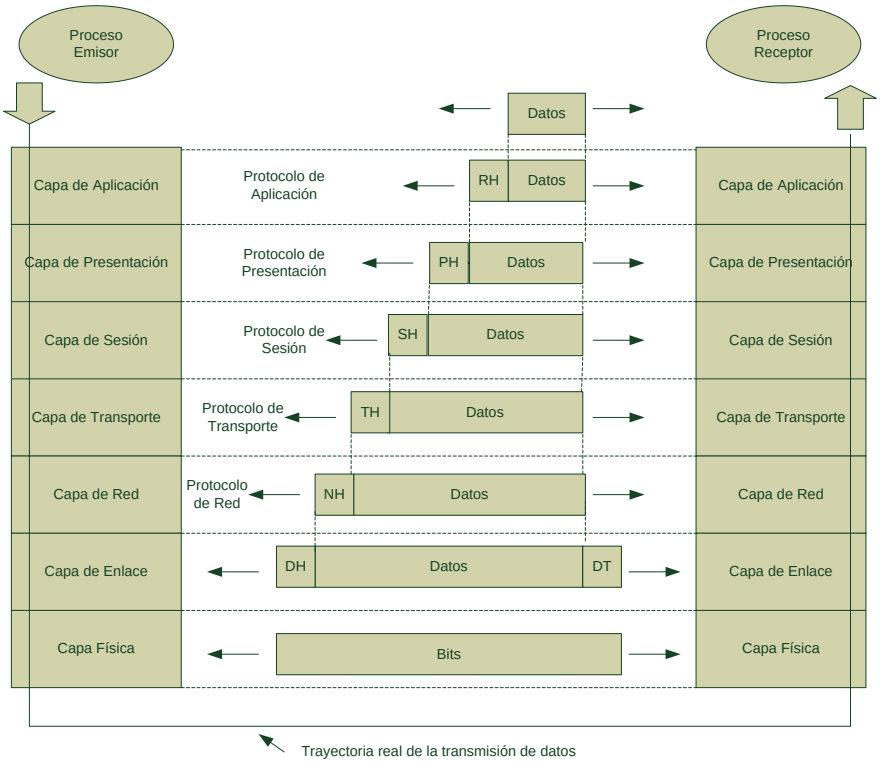


Figura 1. 7 Ejemplo de utilización del modelo OSI (4.4).

TEMA 3. PROTOCOLOS DE RED

A finales de los años 60, las redes no estaban diseñadas de forma que fuera posible compartir recursos entre redes diferentes ya que las redes eran incompatibles entre sí, o no se podían comunicar debido a problemas de administración, como la utilización excesiva de los recursos de las redes por parte de los usuarios.

Para solucionar estos problemas, surgió el modelo TCP/IP, cuyas siglas son: Protocolo de Control de Transmisión/Protocolo de Internet (en inglés Transmission Control Protocol/Internet Protocol), un sistema de protocolos que hace posible comunicar y compartir recursos entre redes diferentes(5.2).

El modelo TCP/IP es una arquitectura de red basada en el modelo OSI anteriormente mencionado, sólo que la capa de Aplicación, Presentación y Sesión, del modelo OSI, se unieron en una sola la cual es la de Aplicación en el modelo TCP/IP.

3.1 CAPAS DEL MODELO TCP/IP

El modelo TCP/IP estructura el proceso de la comunicación en 5 capas (Tabla 1.4), las cuales se explican a continuación (2.8):

Capa 5	Aplicación
Capa 4	Transporte
Capa 3	Internet
Capa 2	Acceso a la red
Capa 1	Física

Tabla 1. 4 Capas del modelo TCP/IP

Capa Física.

Define el enlace físico entre el dispositivo que transmite los datos y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la velocidad de datos, etc.

Capa de Acceso a la red.

Es responsable del intercambio de datos entre el sistema final (emisor y receptor) y la red a la cual está conectado. El dispositivo emisor debe proporcionar a la red la dirección del dispositivo destino, de tal manera que ésta pueda encaminar los datos hasta el destino apropiado.

El objetivo principal de esta capa es separar todas aquellas funciones que tengan que ver con el acceso a la red, de modo que las capas superiores no tengan que ocuparse de los detalles específicos de la red a utilizar y puedan funcionar correctamente con independencia de la red a la que el dispositivo final está conectado.

Capa de Internet.

En esta capa se utiliza el protocolo de Internet (IP Internet Protocol), el cual ofrece el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los dispositivos finales como en los dispositivos encaminadores (routers), los cuales conectan dos o más redes y tienen como función principal retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar al destino.

Capa de Transporte.

La capa de transporte se encarga de asegurar que el intercambio de datos se realice de forma fiable. Esta capa agrupa todos los mecanismos que permiten asegurar que los datos lleguen al dispositivo destino y en el mismo orden en el que fueron enviados. El protocolo para el control de la transmisión, TCP (Transmission Control Protocol), es el más utilizado para proporcionar esta funcionalidad.

Capa de Aplicación.

La capa de aplicación contiene toda la lógica necesaria para posibilitar que las distintas aplicaciones de usuario puedan acceder a las capas del modelo TCP/IP.

3.1.1 FUNCIONAMIENTO DEL MODELO TCP/IP.

Para poder entender cómo se lleva a cabo la comunicación dentro del modelo TCP/IP, es importante conocer el funcionamiento de los principales protocolos involucrados en este modelo, es decir, los protocolos TCP e IP.

Dentro de este modelo (TCP/IP), el **protocolo TCP** se implementa solamente en los dispositivos finales, donde supervisa los bloques de datos para asegurar que todos se entregan de forma fiable a la aplicación apropiada.

El **protocolo IP** se implementa en todos los dispositivos finales y dispositivos de encaminamiento. Este protocolo permite transportar bloques de datos desde una computadora hasta otra, a través de uno o varios dispositivos de encaminamiento.

Para tener éxito en la transmisión de datos, cada computadora y dispositivo de encaminamiento deben tener una única dirección de red que les permita enviar los datos al dispositivo adecuado. Además, cada proceso que se ejecute dentro de un dispositivo debe

tener una dirección que sea única. Esto permite al protocolo TCP entregar los datos al proceso adecuado. A estas últimas direcciones se les denomina puertos (2.9).

A continuación se describe un ejemplo de cómo se transmiten los datos empleando el modelo TCP/IP ilustrado en la figura 1.3:

Se tiene un proceso asociado al puerto 1 en la computadora A, el cual desea enviar un mensaje a otro proceso asociado al puerto 2 de la computadora B. Los pasos que se siguen para transmitir los datos son:

Paso 1. El proceso A en la capa de aplicación, pasa el mensaje a la capa de transporte donde se agrega la cabecera TCP con la instrucción de enviarlo al puerto 2 de la computadora B.

Paso 2. La capa de Transporte pasa el mensaje a la capa de internet con la instrucción, especificada en la cabecera TCP, de enviarlo a la computadora B.

Paso 3. La capa de internet agrega su cabecera IP, la cual contiene la dirección de la computadora destino. A esta capa no es necesario comunicarle la identidad del puerto destino, todo lo que necesita saber es que los datos van dirigidos a la computadora B.

Paso 4. La capa de internet pasa el mensaje que contiene la cabecera IP a la capa de acceso a la red la cual le agrega su cabecera de red con la orden de enviarlo al dispositivo de encaminamiento “J” a través de la red 1.

Paso 5. En el dispositivo de encaminamiento “J” la cabecera de red se elimina y se examina la cabecera IP. Este dispositivo direcciona el paquete a través de la red 2 hacia la computadora B basándose en la dirección destino que contenga la cabecera IP. Además, se le añade a los datos una cabecera de acceso a la red.

Paso 6. Cuando se reciben los datos en la computadora B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos originales alcancen al proceso destino.

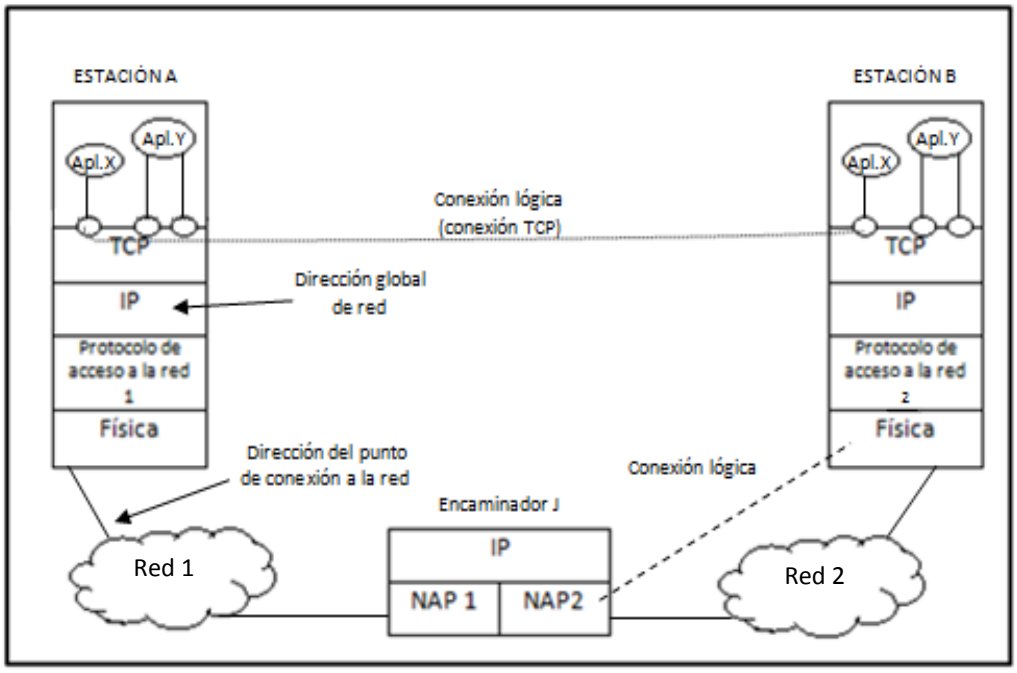


Figura 1. 8 Funcionamiento de TCP/IP (2.9).

3.2 SISTEMA DE NOMBRES DE DOMINIO DNS.

Anteriormente se explicó como se realiza el proceso de comunicación dentro del modelo OSI y también del modelo TCP/IP. Se dijo que cada computadora tiene una única dirección IP que le permite ser identificada y comunicarse con otras computadoras en la red. Sin embargo, si un usuario quisiera comunicarse con otra computadora, ya sea para el envío de un correo electrónico, la conexión a una base de datos, acceder a alguna página web, etc., el usuario tendría que conocer la dirección IP de la máquina con la cual se quiere comunicar. Por ejemplo, supóngase que se desea enviar un correo electrónico a cierta computadora destino, el usuario tendría que utilizar una dirección como esta: cad@128.111.124.41. Al usuario se le dificultaría recordar este tipo de direcciones. Para resolver esta situación se utiliza el DNS (Domain Name Service), el cual se usa para relacionar los nombres de host (computadora conectada a la red) y destinos de correo electrónico con las direcciones IP. Por lo tanto DNS permite al usuario enviar el correo utilizando direcciones más sencillas de recordar, por ejemplo, la dirección de correo cad@cele.unam.mx.

Para poder entender el funcionamiento del DNS es necesario antes hablar más detalladamente del protocolo IP. Como se mencionó en el tema de funcionamiento del modelo TCP/IP, el protocolo IP utiliza direcciones de red para identificar a cada una de las

computadoras que conforman una red, a estas direcciones se les denomina direcciones IP. Las direcciones IP están formadas de 32 bits divididos en 4 octetos, los cuales constan de un identificador de red y un identificador de host, estos identificadores permiten establecer el número de redes y el tamaño de una red en cuanto a número de hosts (2.10). Existen principalmente tres clases de redes las cuales se muestran en la tabla 1.5:

CLASE DE RED	Número de Octetos ID red	ID Host	Rango	Número de Redes	Número de Host
A	1	3	1.0.0.1 - 127.255.255.254	126	16,777,214
B	2	2	128.0.0.1 -191.255.255.254	16,382	65,534
C	3	1	192.0.0.1– 223.255.255.254	2,097,150	254

Tabla 1. 5 Clases de Redes.

Las clases mencionadas anteriormente, conocidas también como direccionamiento por clases, ya no son parte, al menos formalmente, de la arquitectura de direccionamiento de IP (7.1). El requisito de que el tamaño de la porción de red de cada dirección IP fuera exactamente 1 (Clase A), 2 (Clase B) ó 3 (Clase C) bytes daba problemas al intentar ajustar el creciente número de organizaciones con redes de mediano y pequeño tamaño (7.1). Por ejemplo, una red de clase C admite 254 host lo que es demasiado para una organización con solamente 15 host originando que 239 direcciones IP queden sin utilizarse.

Para solucionar lo anterior, en 1993 se estandarizó el rutado interdominio sin clase (CIDR; Classless Interdomain Routing) en el cual la parte del identificador de red de una dirección IP puede tener cualquier tamaño en lugar de estar limitada a 8 (clase A), 16 (clase B) ó 24 (clase C) bits. Una dirección de red utilizando CIDR se denota con la forma a.b.c.d/x donde x indica el número de bits iniciales (del total de los 32) que constituyen la porción de la dirección de red. Por ejemplo, si el número de host que se requiere son 15 se tendría una dirección de la forma a.b.c.d/27 en la cual se tendrían como máximo 32 direcciones de host disponibles (25). Sin embargo, el direccionamiento debe hacerse pensando en el posible crecimiento del número de host.

Como se mencionó anteriormente, el direccionamiento se realiza sobre las direcciones IP, las cuáles pueden ser públicas o privadas. Las direcciones IP públicas son visibles por cualquier dispositivo independientemente de la red en la que se encuentren. Por ejemplo, un dispositivo con una dirección IP pública es accesible desde cualquier otro dispositivo conectado a Internet. En cambio, las direcciones IP privadas, son visibles únicamente por otros dispositivos de su propia red o de otras redes privadas interconectadas por routers.

Los dispositivos con direcciones IP privadas pueden salir a Internet por medio de un router que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

Como se vió anteriormente, existen dos formas de identificación de un host: por un nombre de host y por una dirección IP. Para poder relacionar estas dos formas de identificación, se necesita del servicio de DNS.

DNS es una base de datos distribuida implementada en una jerarquía de servidores de nombres, estos servidores son máquinas específicas en la red que brindan el servicio de DNS. Además, DNS es una aplicación de la capa de aplicación que permite que se comuniquen los host y los servidores de nombres (7.2).

3.2.1 EL ESPACIO DE NOMBRES DEL DNS.

Internet se divide en 200 dominios de nivel superior, cada uno de los cuales abarca muchos hosts. Cada dominio se divide en subdominios, los cuales, a su vez, también se dividen en más subdominios. Todos estos dominios pueden representarse en un árbol como se muestra en la figura 1.4.

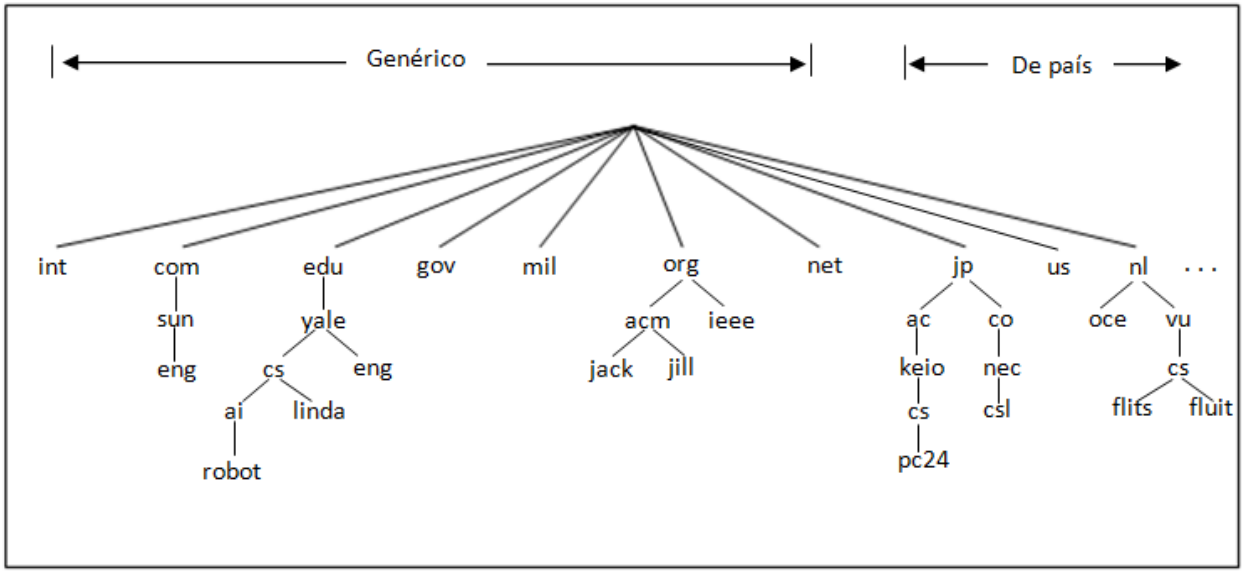


Figura 1. 9 Parte del espacio de nombres de dominio de Internet (3.3)

Las hojas del árbol representan los dominios que no tienen subdominios pero que por supuesto contienen máquinas.

Los dominios de nivel superior se dividen en dos categorías:

- Genéricos: com (Comercial), edu (Instituciones educativas), gov (Gobierno federal de Estados Unidos), int (Ciertas organizaciones Internacionales), mil (Las fuerzas armadas de EU), net (Proveedores de red) y org (Organizaciones no lucrativas).

- De país. Estos dominios incluyen una entrada para cada país. Por ejemplo mx es de México, us de Estados Unidos, jp de Japón.

Cada dominio se nombra por la ruta hacia arriba de él a la raíz. Los componentes se separan con puntos. Por lo tanto, el CAD (Centro de Apoyo a la Docencia) del Centro de Enseñanza de Lenguas Extranjeras de la UNAM, podría utilizar cad.cele.unam.mx.

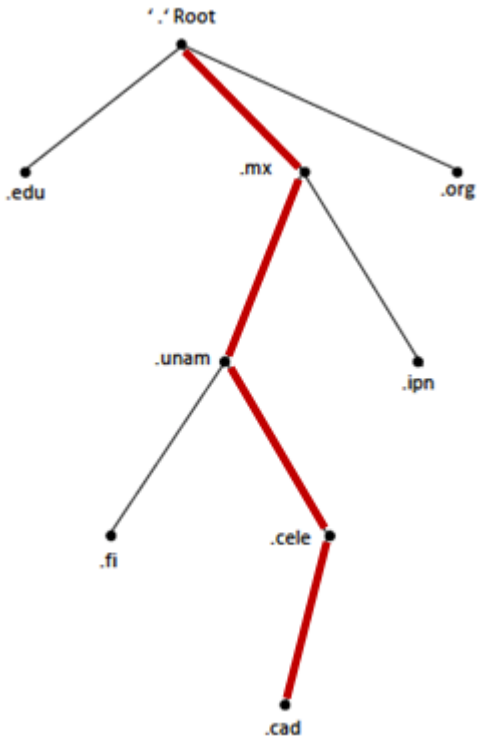


Figura 1. 10 Estructura del espacio de nombres del CAD.

Los nombres de dominio no hacen distinción entre mayúsculas y minúsculas por lo que mx y MX significan lo mismo. Los nombres de componentes pueden ser de hasta 63 caracteres de longitud, y los de ruta completa de hasta 255 caracteres (3.4).

3.2.2 FUNCIONAMIENTO DEL SERVICIO DNS.

La asociación que el protocolo DNS hace de los equipos en una red con una dirección IP para permitir la localización y comunicación entre ellos es información almacenada en la base de datos propia del servidor DNS, la cual contiene una parte de la estructura del espacio de nombres. Todo servidor DNS controla una parte del espacio de nombres en donde puede haber varios subdominios, cada uno con cierta cantidad de equipos, esta parte del espacio de nombres se denomina zona DNS y es el espacio en el que el servidor DNS es un servidor autoritativo. La zona DNS es un mecanismo que establece un límite sobre el cual un servidor DNS puede resolver consultas, es decir, la zona en la que puede localizar y comunicar equipos. Un servidor puede ser autoritativo para una o más zonas.

La zona DNS se divide en dos: zona de búsqueda directa y zona de búsqueda inversa. La zona de búsqueda directa permite identificar a un equipo a través del nombre del equipo, es decir, el servidor DNS recibe el nombre del equipo y revisa en su base datos si contiene la IP correspondiente. La zona de búsqueda inversa identifica a un equipo mediante la dirección IP que el servidor recibe, buscando después el nombre del equipo al cual corresponde esa dirección.

Esta información es almacenada en el Servidor DNS, sin embargo, el funcionamiento de este protocolo requiere que en los equipos cliente también se almacene cierta información importante.

Cuando un equipo en una red necesita comunicarse con otro para usar una aplicación o algún recurso utiliza el servicio DNS para consultar al servidor DNS acerca de la ubicación del otro equipo. Para realizar estas tareas, dentro del protocolo se utilizan dos conceptos importantes: resolvedor DNS y los registros de recursos.

Un resolvedor DNS es un servicio que usa este protocolo para solicitar información de los servidores DNS. La función del resolvedor es desempeñada por el cliente DNS para comunicarse con un servidor DNS y poder localizar a algún otro equipo. Esta información es almacenada localmente en los equipos cliente dentro de un espacio llamado caché del resolvedor DNS para que las búsquedas posteriores se realicen de manera más eficiente.

En lo que respecta a los registros de recursos, cada dominio puede tener un grupo de registros de recursos asociados a él. El registro de recursos más común es simplemente su dirección IP, pero existen muchos otros tipos de registros. Cuando un resolvedor da un nombre de dominio al servidor DNS, lo que recibe son los registros de recursos asociados a ese nombre. Por lo tanto, la función real del DNS es relacionar los dominios de nombres con los registros de recursos. Un registro de recursos tiene cinco tuplas.

Nombre_dominio	Tiempo_de_vida	Clase	Tipo	Valor

El Nombre_dominio indica el dominio al que pertenece este registro. Por lo tanto, este campo es la clave primaria de búsqueda usada para atender las consultas.

El campo de Tiempo_de_vida indica el tiempo en segundos durante el cual este registro será almacenado en la cache del resolvedor DNS y en otros servidores DNS cuando la consulta pasa a través de ellos.

El tercer campo de cada registro de recursos es la Clase. Para la información de Internet, siempre es IN. Para información que no es de Internet, se pueden utilizar otros códigos, sin embargo, éstos raramente son usados.

El campo Tipo indica el tipo de registro de que se trata. Algunos de estos tipos de registros son:

TIPO	SIGNIFICADO	VALOR
A	Dirección IP de host	Entero de 32 bits
CNAME	Registros que permiten la creación de un alias para que los usuarios y los programas den con la dirección correcta aún no conozcan exactamente el nombre del dominio.	Nombre de dominio
SOA	Marca del inicio de una zona de autoridad	Parámetros para esta zona
PTR	Registro regularmente usado para asociar un nombre a una dirección IP con el fin de permitir búsquedas de la dirección IP y devolver el nombre de la máquina correspondiente.	Alias de una dirección IP

Tabla 1. 6. Registros DNS.

Por último se tiene la tupla Valor. Este campo puede ser un número, un nombre de dominio o una cadena de caracteres. El valor depende del tipo de registro. En la tabla 1.6 se presenta la descripción del valor para cada uno de los tipos de registro indicados.

De este modo en una consulta el nombre de dominio DNS podría ser de la forma CAD-P-01.cad.cele.unam.mx y el tipo de consulta especificada para la búsqueda de un registro A. Así, el servidor revisaría en su base de datos si existe un registro A para un equipo llamado CAD-P-01.cad.cele.unam.mx. Si el registro existe, entonces regresa al cliente DNS la dirección IP del equipo cuyo nombre corresponde al envíado por el cliente y esta información es guardada en la caché del resolvedor DNS el tiempo indicado en la tupla Tiempo_de_vida.

En general el proceso de una consulta al DNS ocurre en dos pasos:

- Una computadora cliente realiza una consulta acerca del nombre de otro equipo pasándola al servicio DNS del propio cliente para la resolución.
- Cuando una consulta no puede ser resuelta localmente con el servicio DNS del cliente entonces pasa la consulta a un servidor DNS.

Analizando la siguiente imagen se entenderá más fácilmente el proceso que se sigue cuando se utiliza el protocolo DNS en una red.

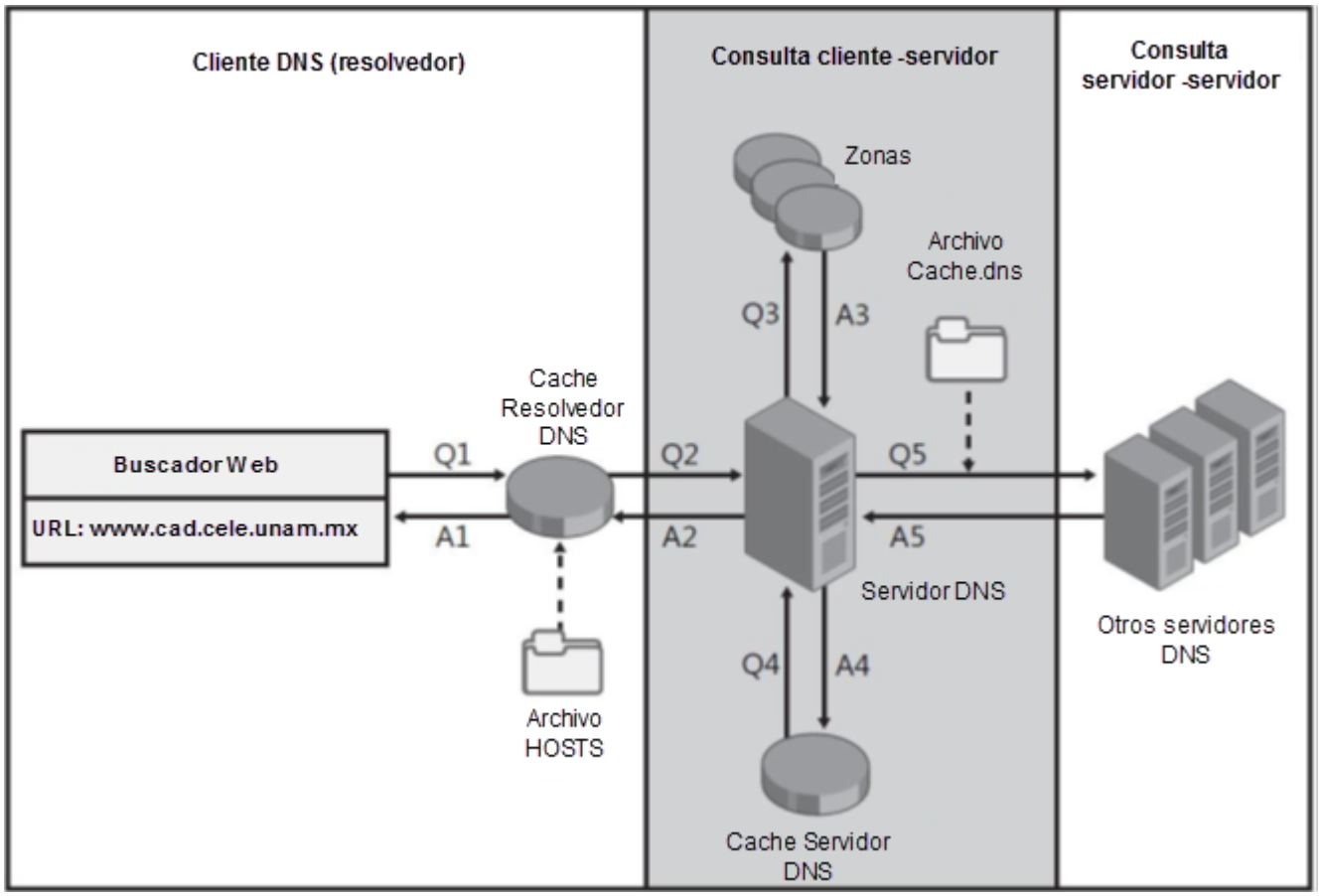


Figura 1. 11 Funcionamiento DNS.

Cuando un cliente necesita localizar a otro equipo puede hacerlo mediante el nombre o por la dirección IP del otro equipo. Por ejemplo, un equipo cliente a través de un navegador de internet solicita la ubicación del equipo en donde se encuentra alojada la página www.microsoft.com. En primer lugar, esta solicitud es gestionada como una consulta por el servicio DNS del propio equipo. Este servicio revisa en la caché del resolvedor DNS local, es decir, la contenida en el equipo cliente. Si el registro del equipo que se desea ubicar se encuentra, entonces la consulta es respondida y el proceso termina.

El registro puede encontrarse en la caché del resolvedor DNS local por dos razones. Una es que dentro del archivo Hosts, contenido en el servidor DNS, se encuentre el registro solicitado por el equipo cliente.

Este archivo Hosts, es cargado a la caché del resolvedor DNS cuando el servicio es iniciado.

Los registros contenidos en dicho archivo, son registros autorizados, es decir, son los registros que relacionan los nombres y direcciones IP de los equipos sobre los cuáles el servidor DNS es autoritativo.

La otra razón es que este registro haya sido almacenado de una consulta anterior al DNS las cuales son registradas en la cache del resolvedor DNS local por un período de tiempo.

Sin embargo, cuando el registro no está dentro de la caché del resolvedor DNS local, la consulta es pasada al servidor DNS configurado para el equipo cliente como servidor DNS preferido. Debido a que el registro del equipo que se desea ubicar no se encuentra dentro de la zona sobre la que el servidor DNS es autoritativo, entonces busca en la caché propia del servidor DNS la cual contiene registros de consultas previas al Servidor DNS de nivel superior. Si el registro es encontrado en esta caché entonces lo regresa al equipo cliente el cual almacena el registro en su caché de resolvedor DNS local temporalmente. De lo contrario, si el registro no es encontrado en la caché del servidor DNS entonces pasa la consulta al servidor DNS de nivel superior que contiene otra parte del espacio de nombres del DNS.

El servidor DNS de nivel superior verifica si puede resolver la consulta de forma autoritativa, es decir, con la información contenida en la zona de búsqueda sobre la cual es autoritativo. Si el registro consultado coincide con un registro de la zona de búsqueda, el servidor resuelve la consulta contestando al servidor DNS preferido del equipo cliente que hizo la consulta. El servidor DNS guarda el registro en su caché y pasa el registro al equipo cliente quien también almacena el registro en la memoria cache del resolvedor DNS local.

Nuevamente, si el registro no es encontrado, entonces se pasa la consulta a otro servidor que contenga otra porción del espacio de nombres y el proceso se repite.

Este proceso descrito se conoce como consulta recursiva, puesto que cada servidor que no tiene toda la información solicitada, la busca en algún otro lado y luego la proporciona. Es posible un procedimiento alternativo. En él, cuando una consulta no puede satisfacerse localmente, ésta falla, pero se devuelve el nombre del siguiente servidor a intentar. Algunos servidores no implementan consultas recursivas y siempre devuelven el nombre del siguiente servidor a intentar.

Para realizar la consulta recursiva apropiadamente, el servidor DNS necesita conocer en dónde comenzar a buscar los nombres en el espacio de nombres de dominio. Esta información es provista en la forma de los DNS raíz, una lista de registros DNS usados por el servicio de DNS de los servidores autoritativos.

3.3 PROTOCOLO DE CONFIGURACIÓN DE HOST DINÁMICO (DHCP).

Debido a la gran cantidad de computadoras que existen en la actualidad se requiere tener controles en la asignación de direcciones IP. Hay dos formas de realizar este procedimiento, la asignación estática y la dinámica. Para ello, existe un servicio que permite hacer la asignación de direcciones IP a los hosts de una red, el cual está almacenado en un dispositivo específico de la red llamado servidor DHCP.

DHCP permite que un host obtenga (le sea asignada) una dirección IP de modo automático, así como cierta información adicional como la dirección del router más cercano y la dirección de su servidor DNS.

El administrador de la red puede configurar DHCP de modo que cierto host reciba siempre una misma dirección IP, es decir, que cada vez que el host se conecte a la red reciba la misma dirección IP preasignada o también puede configurar de modo que el servidor DHCP asigne arbitrariamente una dirección de su depósito de direcciones disponibles previamente establecido; cada vez que se desconecta un host su dirección vuelve al depósito (7.3).

Es importante conocer este protocolo ya que está muy ligado a las labores de administración que se requieren dentro de la red, no es lo mismo realizar las asignaciones de direcciones IP de manera manual a hacerlo de manera automática en términos de inversión de tiempo.

TEMA 4. SEGURIDAD EN UNA RED.

Además de conocer los conceptos fundamentales de las redes y cómo se lleva a cabo la comunicación en ellas es importante hablar de algunos aspectos esenciales en cuanto a seguridad que las redes deben tener para funcionar de manera correcta.

4.1 SERVICIOS DE SEGURIDAD

Uno de estos aspectos esenciales se refiere a los servicios de seguridad cuyo objetivo es proteger las comunicaciones de los usuarios en las redes de una organización. Estos servicios se clasifican de la siguiente manera (6.1):

1. Confidencialidad
2. Autenticación
3. Integridad
4. No repudio
5. Control de acceso
6. Disponibilidad

Confidencialidad

Es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a la información. El objetivo principal de la confidencialidad es proteger los recursos y la información contra el descubrimiento intencional o accidental por personas no autorizadas.

Los servicios de confidencialidad proveen protección de los recursos y de la información almacenada o del flujo de la misma, para asegurar que:

- Nadie pueda leer, copiar, descubrir o modificar la información sin autorización.
- Nadie pueda interceptar los mensajes entre entidades.

Autenticación

Este servicio garantiza que las entidades que participan en una comunicación sean auténticas, es decir, asegura al receptor que el mensaje no provenga de una fuente falsa. Para lograr lo anterior, el sistema verifica la información que alguien provee contra la información que el sistema conoce sobre esa entidad.

La autenticación es realizada principalmente a través de:

- Algo que se sabe, (Información personal, firma, etc.).
- Algo que se tiene, (Tarjetas bancarias, credenciales, etc.).
- Algo que se es, (Huella digital, retina, etc.).

Integridad

Este servicio garantiza que el contenido de los datos no haya sido modificado por personas no autorizadas y que el flujo de los datos en una comunicación se mantenga intacto, es decir, se asegura que los datos enviados coinciden exactamente con los datos recibidos.

No repudio

Este servicio previene a los emisores o a los receptores de negar un mensaje transmitido. Cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. Esto es, el no repudio ofrece protección a un usuario frente a otro usuario que niegue, posteriormente, haber realizado cierta comunicación o recepción de un mensaje enviado.

Control de acceso

El control de acceso es la habilidad para limitar y controlar el acceso tanto a los sistemas informáticos como a los recursos e información que se tengan en ellos. Para lograr este control, cada entidad que trata de ganar acceso debe primero identificarse y luego autenticarse de manera exitosa para que entonces le sea permitido el acceso.

Disponibilidad

Se refiere a que las personas autorizadas puedan acceder a la información deseada cuando lo requieran y tantas veces como sea necesario. Es importante aclarar que la disponibilidad se refiere únicamente al tiempo para obtener la información y no importa si la información es correcta o no.

Disponer de la información después del momento necesario, puede equivaler a la no disponibilidad.

4.2 POLÍTICAS DE SEGURIDAD.

Otro factor importante de considerar son las políticas de seguridad, las cuáles son un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los ojetivos de seguridad informática dentro de la misma. La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política específica qué propiedades de seguridad el sistema debe proveer.

Los conceptos de seguridad explicados anteriormente forman un aspecto fundamental de lo que se quiere lograr en este trabajo, puesto que representan un parámetro de comparación entre el antes y el después de la implementación del dominio de red.

TEMA 5. SISTEMAS OPERATIVOS.

Los host son máquinas conectadas a una red que comparten información y recursos con otras máquinas. Para poder realizar esto, cada máquina debe contar con un programa que permita controlar las operaciones entre el host y la red, a este programa se le conoce como sistema operativo, el cual es el programa fundamental de toda máquina, y cuya función principal es administrar los recursos de la computadora y proporcionar la base sobre la cual pueden escribirse los programas de aplicación, es decir, los programas que utilizan los usuarios (9.1).

5.1 FUNCIONES DEL SISTEMA OPERATIVO

Las funciones clásicas del sistema operativo se pueden agrupar en las siguientes tres categorías (10.1):

- Gestión de los recursos de la computadora.
- Ejecución de servicios para los programas.
- Ejecución de los mandatos de los usuarios.

El sistema operativo se divide en tres capas principales. La capa denominada núcleo (kernel), es la capa que administra los recursos físicos (hardware) de la máquina, proporcionando la funcionalidad básica del sistema operativo. La capa de servicios o llamadas al sistema; es la interfaz entre el sistema operativo y los programas del usuario, las llamadas al sistema crean, eliminan y utilizan varios objetos de los programas, controlados por el sisema operativo. La capa de intérprete de comandos o shell; funciona como una interfaz a través de la cual el usuario puede interactuar con la computadora. El shell recibe los comandos del usuario, los interpréta, y si puede, los ejecuta (9.2) (10.2).

5.2 COMUNICACIÓN ENTRE PROCESOS.

Como se mencionó anteriormente, un usuario puede comunicarse con otro por medio de la red, esto se realiza a través de procesos, los cuales son programas que se ejecutan en las máquinas de los usuarios. La comunicación entre los usuarios consiste en la transferencia de mensajes entre los programas que los usuarios ejecutan, estos programas son ejecutados por el sistema operativo como procesos. El sistema operativo se encarga de la gestión de los procesos, ofreciendo en general los siguientes servicios (10.3):

- Crear un proceso: El proceso es creado por el sistema operativo cuando así lo solicita otro proceso, que se convierte en el padre del nuevo.

- Ejecutar un proceso: Los procesos se pueden ejecutar de dos formas: batch e interactiva. En la primera se utilizan archivos con comados u órdenes que realizan tareas específicas relacionadas con el proceso. En el modo interactivo, el proceso

está asociado a un shell, por el que recibe la información del usuario y por el que contesta con los resultados.

- Terminar la ejecución de un proceso: un proceso puede finalizar su ejecución por varias causas, entre las que se encuentran las siguientes:

    - Ha terminado de ejecutar el programa.
    - Se produce una condición de error en su ejecución.
    - Otro proceso o el usuario deciden que ha de terminar.

Cuando un proceso A de un usuario quiere comunicarse con un proceso B de otro usuario, el sistema operativo construye primero el mensaje que será transmitido, luego ejecuta una llamada al sistema, que es el método usado por un proceso para solicitar una acción por el sistema operativo (11.1), para que el sistema operativo busque el mensaje y lo envíe a través de la red hacia B(9.3). Posteriormente se lleva a cabo el procedimiento de comunicación dentro de la capa de aplicación del modelo OSI o TCP/IP y continúa el flujo de comunicación descrito anteriormente.

Tener claro el concepto y funcionamiento del sistema operativo es muy importante puesto que es la herramienta principal que se usó en este trabajo para poder cumplir con las metas planteadas. En capítulos posteriores se detallará más sobre el sistema operativo que se utilizó para alcanzar los objetivos de este trabajo.

TEMA 6. ARQUITECTURA CLIENTE-SERVIDOR.

Como se mencionó, el sistema operativo es el programa que permite administrar los recursos físicos y lógicos de las computadoras. En una red, el sistema operativo se encarga de gestionar este compartimiento de recursos con otras computadoras de la red. Sin embargo, es necesario que exista una forma de estructurar la manera en que se lleve a cabo este procedimiento. Esa forma, generalmente es el modelo cliente-servidor. La idea del modelo cliente-servidor es la estructuración del sistema operativo como un grupo de procesos en cooperación, llamados servidores, que ofrezcan servicios a los usuarios, llamados clientes (9.4). El proceso servidor puede residir en la misma máquina que el cliente o en una distinta, en cuyo caso la comunicación deberá realizarse a través de una red de interconexión(10.4).

La comunicación entre los procesos cliente y servidor, se basa en un protocolo solicitud/respuesta. El cliente envía un mensaje de solicitud al servidor para pedir cierto servicio. El servidor hace el trabajo y regresa los datos solicitados o un código de error que indique la razón por la cual no se pudo llevar a cabo el trabajo.

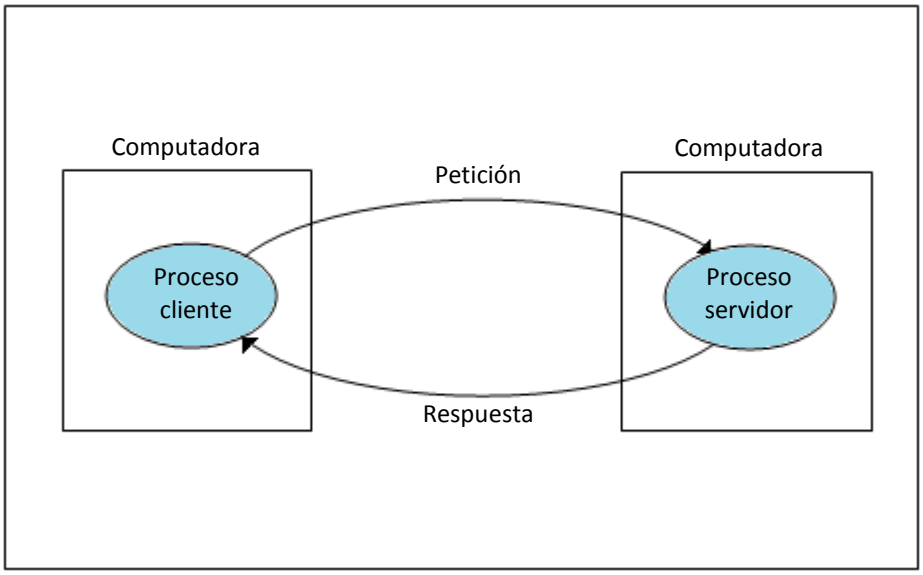


Figura 1. 12 Comunicación cliente-servidor. (10.4)

6.1 VENTAJAS DEL MODELO CLIENTE-SERVIDOR

En las organizaciones, comúnmente los procesos servidor y cliente se tienen en máquinas distintas con el objetivo de centralizar los recursos, albergándolos en la máquina servidor que contiene los procesos servidor y estando disponibles para todos los clientes que los

requieran, de igual forma este modelo permite centralizar funciones de gestión de red tales como la interoperabilidad, de manera que los distintos sistemas que se utilicen queden vinculados. Además, desde el punto de vista de la seguridad, en el modelo cliente-servidor se mejoran los servicios de seguridad como auntenticación, confidencialidad, integridad, disponibilidad, mencionados anteriormente. También, el modelo cliente-servidor permite disminuir las labores de administración de los recursos en los equipos cliente puesto que es el servidor quien realiza esta tarea. Finalmente, este modelo brinda la posibilidad de que la red crezca en cuanto a número de equipos de manera sencilla ya que es posible quitar o agregar clientes sin afectar el funcionamiento de la red y sin la necesidad de realizar mayores modificaciones. Debido a lo anterior, la forma de administración propuesta en este trabajo requiere del modelo cliente-servidor para poder funcionar como se espera.

6.2 FUNCIONALIDADES COMÚNES DE LOS CLIENTES Y SERVIDORES

Frecuentemente en las organizaciones, las máquinas cliente son computadoras de escritorio que ofrecen una interfaz sencilla para el usuario. Estas máquinas presentan, en general, un tipo de interfaz gráfica cómoda para los usuarios que les permite utilizar aplicaciones tales como procesadores de texto, hojas de cálculo y presentaciones.

A su vez, los servidores ofrecen una serie de servicios compartidos a los clientes, un ejemplo son los servidores de bases de datos que permiten a los clientes compartir el acceso a la misma base de datos, y permiten el uso de un sistema de computación de alto rendimiento para gestionar la base de datos (12.1). Otros servicios que pueden brindar los servidores son: servicios DNS, DHCP, almacenamiento de archivos, alojamiento de sitios WEB etc. Puede haber servidores dedicados a un solo servicio, o servidores que brinden distintos servicios, dependiendo de las necesidades y objetivos de las organizaciones.

TEMA 7. ADMINISTRACIÓN DE REDES.

Parte fundamental del correcto funcionamiento de las redes es la administración de los recursos y de la información que se maneja en ellas. La administración de redes es un proceso que busca mediante la planeación, organización y control de actividades mantener una red operativa, eficiente y segura, lo cual se verá reflejado en la calidad de los servicios ofrecidos; algunos objetivos de la administración de redes son:

- Mejorar la continuidad de la red con mecanismos de control interno y externo.
- La resolución de problemas en el menor tiempo posible.
- Hacer uso eficiente de todos los recursos de la red: programas, impresoras, etc.
- Controlar cambios y actualizaciones en la red y en el software para minimizar las interrupciones en el servicio a los usuarios.

Existen dos formas de administrar una red, la administración descentralizada y la administración centralizada.

7.1 ADMINISTRACIÓN DESCENTRALIZADA DE UNA RED.

En la administración descentralizada no se maneja el modelo cliente-servidor, sino que cada host actúa como cliente y servidor a la vez, administrando y compartiendo sus propios recursos dentro de la red. Comúnmente, en este tipo de administración se maneja el concepto de grupo de trabajo.

Un grupo de trabajo es un grupo de dispostivos en red que comparten recursos. Desde el punto de vista de la administración, el esquema de grupo de trabajo no requiere de la existencia de servidores, lo cual podría resultar en un ahorro para las organizaciones pero, por otro lado, en este esquema se requiere de una mayor inversión de tiempo para administrar los equipos, ya que esta tarea se debe realizar individualmente cada vez que sea necesaria alguna configuración.

Ahora bien, la seguridad en este esquema se maneja localmente en cada equipo, es decir, cada máquina tiene su lista de usuarios autorizados con las contraseñas correspondientes, así que tanto la autenticación como la autorización de acceso a los recursos se ejecutan localmente en cada máquina. Sin embargo, si los usuarios requieren acceder a otros recursos de la red tendrán que recordar muchas contraseñas, una para cada recurso de la red. En este caso, los procesos de autenticación y autorización se realizan tanto en la máquina desde donde se solicita el recurso como en la máquina donde se encuentra dicho recurso.

7.2 ADMINISTRACIÓN CENTRALIZADA DE UNA RED.

En la administración centralizada se maneja el modelo cliente-servidor por lo que la comunicación y el compartimiento de recursos se realiza necesariamente a través de un dispositivo central que funge como servidor de la red. En este modelo, es necesario llevar una buena administración en el servidor ya que si este llegara a funcionar incorrectamente toda la red se vería afectada. Debido a esto comúnmente se utilizan los dominios de red cuyo objetivo principal es facilitar la gestión tanto de recursos como usuarios a través de servicios y mecanismos que se brindan desde él o los servidores denominados controladores de dominio.

Un dominio, es una agrupación de dispositivos que comparten un directorio centralizado. Este directorio contiene todas las cuentas de usuario y la información de seguridad del dominio y se encuentra almacenado en los controladores de dominio desde donde se manejan los aspectos y cuestiones de seguridad de los recursos, usuarios e interacciones con el dominio, centralizando tanto la seguridad como la administración. Por lo tanto, las cuestiones de administración y seguridad se ven mejoradas en comparación con el modelo de grupo de trabajo, ya que la centralización permite realizar las configuraciones necesarias desde el servidor a uno, a varios o a todos los dispositivos que las requieran. Además, bajo este esquema, la confidencialidad, disponibilidad e integridad de la información de los usuarios se ve mejorada en gran medida. Obviamente, todo depende de la configuración de los servidores controladores de dominio, así como de la correcta administración que se tenga en éstos. Otra ventaja importante de los dominios, es la facilidad de integrar nuevos equipos a la red, lo que es bueno para las organizaciones que tengan la necesidad de aumentar su infraestructura.

La administración de redes es otro de los pilares de este trabajo; la explicación de las formas de administración anteriores se hizo con la idea de justificar el por qué se estableció la meta de contar con la forma de administración centralizada en el CAD.

CAPÍTULO 2

ANÁLISIS DEL PANORAMA ACTUAL DEL CENTRO DE APOYO A LA DOCENCIA (CAD)

CAPÍTULO 2. ANÁLISIS DEL PANORAMA INICIAL DEL CENTRO DE APOYO A LA DOCENCIA (CAD).

INTRODUCCIÓN

Este capítulo explica las condiciones iniciales del escenario donde se realizó este proyecto, explicando qué es el CAD, cuáles son sus objetivos principales, cuáles son sus funciones, la manera en que se encuentra organizado y los recursos con los que cuenta. La finalidad del capítulo es mostrar la situación del CAD antes de realizar la implementación del dominio de red, y a la vez, identificar los puntos susceptibles de mejoras. Así, los resultados de este capítulo sirvieron como base para llevar a cabo la comparación entre el estado inicial y final del proyecto; dicha comparación será abordada en el capítulo correspondiente al análisis de los resultados obtenidos.

TEMA 1. ANTECEDENTES DEL CAD.

1.1 HISTORIA DEL CAD.

La UNAM con el propósito de aumentar la cobertura y mejorar la calidad de la educación, ha impulsado el proceso de enseñanza-aprendizaje mediante el establecimiento de centros equipados con plataformas de cómputo y telecomunicaciones, para la creación de nuevos ambientes de aprendizaje a través del uso interactivo de estos medios. Para lograr este propósito, la UNAM a través del programa Servicios Educativos en Red (SER-UNAM) contempló la creación de Centros de Apoyo a la Docencia (CAD) enfocados a cumplir con el propósito mencionado.

Por otro lado, el Centro de Enseñanza de Lenguas Extranjeras (CELE) se interesó en la creación y desarrollo de uno de estos centros, a fin de lograr la incorporación de un enfoque didáctico que incluyera el uso interactivo de tecnologías y medios, apoyando a los docentes mediante el uso de equipos de cómputo y el manejo de Tecnologías de la Información y la Comunicación (TICs), que les permitiera optimizar los procesos de enseñanza-aprendizaje.

De esta forma, en el año 2000 se propuso la creación de un Centro de Apoyo a la Docencia por parte de la Lic. Marina Chávez, coordinadora de la Mediateca del CELE. El CAD del CELE comenzó su funcionamiento en febrero del 2002.

1.2 IMPORTANCIA DEL CAD DENTRO DEL CELE.

Para el CELE, la creación de un CAD representa la oportunidad de extender la cobertura de sus servicios educativos, innovando en el campo de la enseñanza de las lenguas extranjeras.

El CAD ayuda a impulsar y reforzar la formación de los profesores en el uso pedagógico de medios y TIC's. También fomenta la creación de materiales didácticos de

apoyo al aula y el desarrollo de actividades y materiales que favorezcan el aprendizaje autodirigido, mediante el uso de la tecnología. En conclusión, el centro representa para el CELE la parte de innovación y actualización tecnológica que todo centro educativo debe tener hoy en día.

1.3 OBJETIVOS DEL CENTRO.

Los objetivos que el CAD tiene y por los cuáles se rige son los siguientes:

- Apoyar a los docentes del CELE en la optimización de los procesos enseñanza-aprendizaje que utilizan mediante:
  - Asesoría y capacitación sobre el uso de recursos de cómputo.
  - Proporcionar el uso de infraestructura. (PC'S, Software, Impresoras, Escáner).

- Brindar servicios de calidad, adecuados y oportunos a los docentes.

- Desarrollar proyectos académicos que estén a la vanguardia respecto al avance tecnológico actual.

Para cumplir con los objetivos mencionados, el CAD desarrolla determinadas funciones y brinda servicios específicos, algunos de los cuales se detallan a continuación.

1.4 FUNCIONES Y SERVICIOS DEL CAD.

Desde sus inicios, la función principal del CAD dentro del CELE ha sido la de impulsar, bajo un enfoque pedagógico-mediático integral, el desarrollo de actividades y productos basados en nuevas tecnologías de apoyo, enfocadas en los procesos de enseñanza–aprendizaje de lenguas extranjeras (15). Actualmente, las funciones del CAD están basadas en dos ejes rectores: Docencia y Personal Académico.

Dentro del eje de la Docencia, se encuentra el programa de "Implementación de tecnologías de información y comunicación (TICs) en la docencia", que incluye dos proyectos:

- Desarrollo de recursos digitales: materiales multimedia, herramientas en línea.

- Prestación de servicios de Tecnologías de la Información y Comunicación: infraestructura, asesoramiento, exploración e implementación de nuevos recursos.

Por otro lado, en el eje del Personal Académico se incluye el “Programa de Capacitación y Actualización Docente”, del que forma parte el proyecto:

- Capacitación y formación de los docentes en el uso de Tecnologías de la Información y la Comunicación.

Para llevar a cabo las funciones mencionadas, en el CAD se brindan los siguientes servicios:

- Desarrollo de proyectos tales como sitios web de apoyo a clases presenciales, blogs y foros académicos, repositorios de recursos, materiales u objetos de aprendizaje, podcast, entre otros.
- Formación y capacitación a los docentes del CELE y personal que labora en el CAD. El objetivo para los docentes es que conozcan las TICs existentes y puedan aplicarlas como herramientas en su labor de enseñanza. La capacitación es brindada por el personal del CAD, que a su vez, debe de actualizarse constantemente sobre las TICs para poder transmitir estos conocimientos a los profesores.
- Uso de infraestructura como equipos de cómputo, impresoras y escáner.

1.5 ORGANIZACIÓN DEL CAD.

El CAD se encuentra organizado de la siguiente manera:

- Existe un Responsable quien es el encargado de planear, organizar y controlar los proyectos, actividades y/o estrategias necesarias para el correcto funcionamiento del centro, así como coordinar y gestionar los vínculos con los que tiene relación el centro bajo una orientación académica.
- Además, hay Técnicos Académicos cuyo objetivo es operar la infraestructura del centro y proporcionar apoyo a los usuarios del CAD, así como participar en el desarrollo de diversos proyectos académicos.
- También participan prestadores de Servicio Social, cuyo objetivo es apoyar en el desarrollo de las actividades y proyectos.
- Por otra parte, están los Tesistas, quienes desarrollan su trabajo de tesis en proyectos orientados a beneficiar al centro, además de apoyar a los usuarios del CAD en relación a dudas con el uso de los equipos.

Para poder visualizar más claramente la forma en que se encuentra organizado el CAD, se muestra el siguiente diagrama:

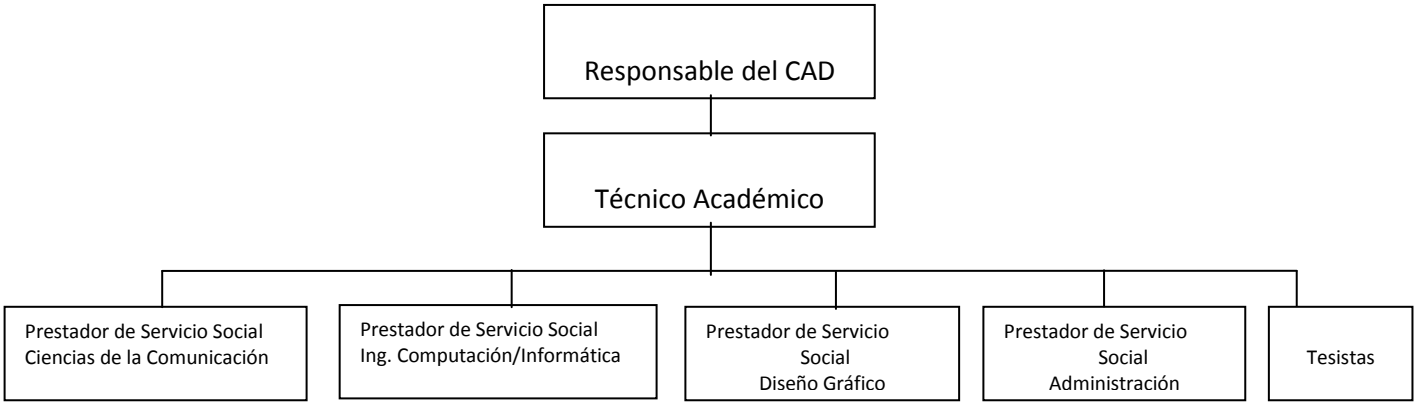


Figura 2. 1 Diagrama del personal del cad (15).

1.6 RECURSOS DE CÓMPUTO CON LOS QUE CUENTA EL CAD.

Como se mencionó, uno de los objetivos que el centro tiene es el de apoyar a los profesores mediante el uso de infraestructura. Sin embargo, la infraestructura también juega un papel muy importante en el desarrollo de los proyectos, a continuación, se describen los recursos que se tienen así como la forma en que son utilizados dentro de las operaciones del CAD.

1.6.1 HARDWARE Y SOFTWARE.

En cuanto a hardware, el CAD cuenta con 15 computadoras de escritorio, dos impresoras y un escáner. Respecto al software, las computadoras cuentan con sistemas operativos Windows 7, Mac y Linux predominando el primero. De esos 15 equipos, 3 son de uso interno para el personal, 2 funcionan como servidores y 1 más está destinado para efectos de esta tesis. Las 9 máquinas restantes son para el uso de profesores y personal del CAD (Servicios Sociales y Tesistas), todas ellas con Windows 7; en estas máquinas se almacena la información necesaria para que los usuarios desarrollen sus actividades.

1.6.2 MANTENIMIENTO DE LOS RECURSOS.

Como en todo centro de cómputo, es importante tener planes de mantenimiento de los recursos, éstos deben incluir la actualización del software y la instalación de nuevos programas. En el CAD estas tareas se llevan a cabo principalmente en periodos de intersemestre, y son realizadas de manera individual para cada uno de los equipos. Los mantenimientos incluyen tareas como respaldo de información, formateo de los equipos, depuración y actualización de software. Adicionalmente se lleva un registro de cuáles son los programas más utilizados aportando información de gran utilidad para los administradores del centro.

1.6.3 ESTADÍSTICAS DE USO DE LOS RECURSOS.

El registro que se lleva, permite conocer el nivel de asistencia de usuarios al CAD y los servicios que utilizan. Para el CAD es importante tener estas estadísticas ya que con base a esta información se determinan las necesidades de los docentes, se establecen criterios para proveer los recursos y también permite organizar las actividades del personal del centro para cumplir con los servicios requeridos. Como se puede notar, es importante que estos datos sean confiables puesto que de ello depende la planeación de actividades y adquisición de material.

TEMA 2. ADMINISTRACIÓN DE LOS USUARIOS Y DE SUS PRIVILEGIOS.

Las máquinas del centro están configuradas para atender a los diferentes tipos de usuarios, esta configuración considera los distintos usos que se dan a los equipos y las características de funcionamiento que deben tener para poder cumplir con las necesidades de los usuarios. La gestión en la configuración de las máquinas prevé también los permisos que cada usuario tiene sobre los equipos para poder realizar cambios, estos permisos se basan en las características que tienen las diferentes cuentas de usuario por omisión, las cuales se tratarán más adelante.

2.1 PERFIL DE LOS DIFERENTES TIPOS DE USUARIOS.

Para entender de mejor manera la administración y control que se tiene sobre los usuarios y sus permisos, es necesario detallar los distintos tipos de usuario que asisten al CAD, así como las tareas que realizan en los equipos.

En general, asisten al CAD tres tipos de usuario los cuales son:

- Administradores: Son las personas que se encargan de planear, organizar y controlar las actividades y/o estrategias necesarias para el correcto funcionamiento del centro. Como antes se dijo, los administradores tienen máquinas específicas para realizar sus tareas, cada uno de ellos se encarga de la administración de sus equipos y de su información. Nadie más tiene acceso a esos equipos

- Docentes: Son los usuarios que se apoyan en los servicios del CAD para sus labores académicas dentro del CELE. Utilizan equipos destinados para ellos y pueden utilizar cualquiera que esté disponible. Las tareas que realizan los docentes deben estar destinadas para ayudar a cumplir con su trabajo en el proceso de enseñanza-aprendizaje. El software que requieren es, básicamente, paquetería de oficina (Word, Excel, Power Point, etc.), reproductores de audio y/o video, correo electrónico, servicio de internet para realizar investigaciones, etc. También utilizan el servicio de impresión y escáner. Actualmente el servicio de almacenamiento de información es libre, cada usuario guarda su información en la computadora que este utilizando, por lo tanto, no se tienen cuentas personales ni carpetas de almacenamiento individual.

- Personal que labora en el CAD, servicios sociales y tesistas: Son las personas que ayudan en la elaboración de proyectos, soporte técnico a los docentes y en general dan apoyo a todas las actividades relacionadas con el CAD. Debido a las tareas que desempeñan estos usuarios, y a las diferentes áreas a las que pertenecen, el material que utilizan es específico para poder llevar a cabo su trabajo.

Como se puede observar, el uso de los equipos del CAD destinados para los docentes, prestadores de Servicio Social y Tesistas es muy variado, por lo que el software de los equipos también es distinto, sobre todo el software que requieren los prestadores de servicio social; este software no está disponible en todas las máquinas.

2.2 ASIGNACIÓN DE PRIVILEGIOS EN LOS EQUIPOS.

En los equipos del CAD destinados para los usuarios mencionados en el párrafo anterior, existen diferentes tipos de permisos para cada usuario. Para asignar estos permisos, los equipos tienen tres tipos diferentes de cuenta, las cuales se muestran en la tabla 2.1. Una cuenta de usuario indica al sistema operativo los archivos a los que un usuario puede tener acceso y los permisos que tiene sobre éstos. En el sistema operativo Windows, existen 3 tipos distintos de cuenta que proporcionan al usuario un nivel diferente de control sobre el equipo. Estos tipos de cuenta son:

- Estándar. Una cuenta de usuario estándar permite que una persona use la mayoría de las funciones del equipo pero con acciones limitadas, es decir, que no puede realizar cambios en la configuración del equipo que afecten a los demás usuarios. En este tipo de cuenta se pueden usar casi todos los programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware ni eliminar archivos que son necesarios para que el equipo funcione.
- Administrador. Este tipo de cuenta otorga al usuario el control total del equipo, permitiéndole realizar cambios en la configuración del mismo que puedan o no afectar a los demás usuarios. Las acciones que este tipo de cuenta permite son:
    - Cambiar la configuración de seguridad del equipo.
    - Instalar software y hardware.
    - Obtener acceso a todos los archivos existentes en el equipo.
- Invitado. Este tipo de cuenta está pensada para usuarios que no tienen una cuenta permanente en el equipo o dominio y usan el equipo temporalmente. Los usuarios que utilicen la cuenta de invitado no pueden instalar software o hardware, ni realizar cambios en la configuración del equipo.

Nombre de Cuenta	Tipo de Cuenta	A quién va dirigido	Privilegios
Profesor (Sin contraseña)	Estándar	Docentes	Limitados
Staff (Con contraseña)	Administrador	Administradores, Servicio social, tesistas, etc.	Todos
Supervisor (Con contraseña)	Administrador	Administradores	Todos

Tabla 2. 1 Descripción de las cuentas existentes.

2.3 MANEJO DE CUENTAS DE USUARIOS.

La administración de las cuentas de usuario la realiza el sistema operativo, este se encarga de asignar los permisos sobre el equipo dependiendo del tipo de cuenta con que se ingrese. El CAD no dispone de políticas de seguridad en cómputo, sino que utiliza los diferentes tipos de permisos que tienen las cuentas de usuario para dar seguridad a los equipos. Se cuenta con políticas de seguridad, pero éstas están encaminadas a la seguridad física de los equipos como es el uso de sensores para evitar el robo de equipos.

TEMA 3. MANEJO DE LA INFORMACIÓN.

En el CAD, la información que se maneja se puede dividir en dos grupos:

1. La información propia de los profesores como son archivos de texto, de audio, presentaciones, etc.

2. La información que el centro genera para el desarrollo de proyectos. Como en todo centro de cómputo, la información es el activo más importante y es uno de los aspectos que se deben proteger en mayor medida.

3.1 CONTROL Y RESGUARDO DE LA INFORMACIÓN DE LOS USUARIOS.

Actualmente, el CAD no se hace responsable de la información que los profesores guarden en los equipos, así se evita que existan problemas relacionados con la pérdida de información, que a su vez, genera molestia o inconformidad entre los profesores, ya que algunos de ellos no cuentan con dispositivos de almacenamiento. Por otra parte, la cuenta de usuario *Profesores* no tiene contraseña, lo que significa que todos los usuarios tienen acceso a la misma información.
La información propia del centro, es de vital importancia puesto que en ella radican los proyectos que ahí se realizan, y como medida de protección, la cuenta de usuario *Staff,* que utilizan las personas que generan esta información, si tiene contraseña, por lo que solo las personas que la conocen tienen acceso a esta información. Además, periódicamente se llevan a cabo respaldos de la información que contienen los equipos, como una medida preventiva que protege los datos de algunos riesgos como pérdida de la información y/o falta de disponibilidad de ella.

3.2 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN.

Confidencialidad.

Con las medidas explicadas sobre el resguardo y control de la información, puede observarse que la información de los profesores actualmente carece de confidencialidad, ya que al no tener contraseña la cuenta *Profesores*, todos los usuarios pueden acceder a la información.

En cuanto a la información del CAD, la confidencialidad tampoco existe; aunque la cuenta de usuario *Staff* tiene contraseña, el número de personas que están autorizadas para tener acceso a este tipo de cuenta, y por lo tanto también a la información, es alto. Además de esto, también sucede que el personal que apoya en el desarrollo de proyectos como prestadores de servicio social y tesistas, cuando terminan su período se van conociendo las contraseñas de los equipos, lo cual representa una amenaza para la información.

Integridad.

Con respecto a la información de los profesores, la integridad es mínima, ya que si todos tienen acceso a esa información, todos pueden modificarla o eliminarla y por eso es complicado que los profesores tengan la confianza de dejar su información en los equipos.

Disponibilidad.

La disponibilidad de los datos no se puede garantizar completamente en ninguno de los dos grupos de información; como se mencionó anteriormente, puede suceder que se viole la integridad de la información y que ésta sea eliminada, lo que ocasionaría que la información no esté disponible. Por otro lado, también sucede que el equipo donde está almacenada la información que algún usuario requiere puede estar ocupado por otro, haciendo que la información requerida no esté disponible en ese momento.

TEMA 4. IDENTIFICACIÓN DE ASPECTOS SUCEPTIBLES DE MEJORAS.

Los aspectos susceptibles de mejoras que se listan a continuación, se identificaron mediante la observación directa en el funcionamiento diario del CAD y de un análisis de cuestionarios realizados a los diferentes tipos de usuarios del centro (Anexo Cuestionarios Personal CAD).

Aspecto 1. Mejorar el tratamiento de la información.

El activo más importante del centro, que es la información de los usuarios, no está debidamente protegido contra las distintas amenazas existentes en cuanto a su confidencialidad, disponibilidad e integridad. Esto se debe a que tener cuentas de usuario compartidas en las máquinas no es una medida suficiente para su protección, debido a que todos los usuarios pertenecientes al mismo tipo de cuenta tienen acceso a los archivos almacenados en esa computadora, aunque sean propiedad de otros usuarios. Esto provoca que se recomiende a los usuarios no guardar información importante en los equipos.

Aspecto 2. Optimizar la forma en la que se realizan las configuraciones del sistema.

Las distintas configuraciones que se requieren en los equipos, como la instalación y desinstalación de software, la actualización del sistema operativo, las configuraciones del sistema y del escritorio, se realizan de manera independiente en cada uno de ellos; esto requiere de inversión de tiempo por parte del personal del centro y repercute en una menor disponibilidad de equipos durante el tiempo en el que son configurados.

Aspecto 3. Mejora en el proceso de instalación del software básico en los equipos del Centro.

No se tiene instalado el mismo software en todos los equipos, lo que dificulta la distribución de los mismos a los usuarios cuando el servicio de uso de infraestructura es muy demandado, puesto que podrían requerir de cierto software en específico que se encuentra disponible solamente en algunas computadoras.

Aspecto 4. Mejorar la administración de las impresoras.

Las impresoras se encuentran conectadas a máquinas específicas de la red, lo que implica que estas máquinas estén encendidas permanentemente si se requiere hacer uso de las impresoras. Además, esto también significa que cuando suceden problemas de conexión con esos equipos, el servicio de impresión se interrumpe. Otro problema es que las impresoras se desconfiguran de los equipos por distintas causas por lo que hay que reinstalarlas nuevamente.

Aspecto 5. Automatizar la obtención de estadísticas del Centro.

Las estadísticas de asistencia al centro y de uso de los recursos, se realizan manualmente. Esto implica que los docentes tengan que invertir tiempo en el llenado de formatos para el registro de estos datos, y para los administradores, repercute en el tiempo de captura y procesamiento de esta información, además de que es alta la incertidumbre en la información, ya que algunos usuarios no se registran o no ingresan los servicios que utilizaron.

Aspecto 6. Optimizar la forma en la que se realizan los respaldos de información.

Los respaldos de información de los equipos se realizan periódicamente pero se llevan a cabo de manera individual, es decir, de forma separada por cada uno de ellos. Esto requiere mayor inversión de tiempo del que pudiera ser necesario.

Aspecto 7. Difundir políticas para el uso de los equipos.

No existen políticas o controles que protejan la información, configuración e integridad en general de los equipos, o al menos no han sido difundidas de manera suficiente, para que los usuarios del centro estén enterados de lo que tienen permitido y lo que se recomienda evitar.

Aspecto 8. Optimizar la forma en la que se realizan las configuraciones de seguridad del sistema.

Los equipos no están protegidos contra configuraciones sensibles, que puedan alterar el correcto funcionamiento de los mismos, esto puede originar la falta de disponibilidad de las computadoras.

CONCLUSIÓN.

Los aspectos susceptibles de mejoras identificados están orientados a dos temas principalmente:

- La administración de usuarios y recursos.
- La seguridad de la información.

Estos temas, son fundamentales en el desarrollo de las operaciones de la mayoría de los centros de cómputo y en ámbitos educativos donde las operaciones tienen un enfoque de apoyo en los procesos de enseñanza-aprendizaje. Por ello es tratar de que estos temas sean ejecutados de la manera más óptima posible, así como también lo es entender la magnitud de la importancia que tienen y desarrollar estrategias enfocadas al mejoramiento continuo de los mismos.

CAPÍTULO 3

PROPUESTA PARA LA MEJORA EN LA ADMINISTRACIÓN DE LOS RECURSOS Y USUARIOS DEL CAD

CAPÍTULO 3.- PROPUESTA PARA LA MEJORA EN LA ADMINISTRACIÓN DE LOS RECURSOS Y USUARIOS DEL CAD.

INTRODUCCIÓN.

En este capítulo se presentan las soluciones a las distintas problemáticas identificadas en el capítulo anterior, centradas en la optimización de las labores de administración de los recursos, usuarios y la seguridad de la información. También se analiza la elección de las herramientas y configuraciones tecnológicas necesarias para lograr las mejoras esperadas con la propuesta, explicando los conceptos fundamentales así como su funcionamiento en los temas de administración y seguridad de la información, además de describir los beneficios puntuales que el CAD obtendrá de ellas. En los siguientes capítulos, se tratará la implementación de las soluciones propuestas al igual que los resultados obtenidos.

TEMA 1. PROPUESTAS DE MEJORAMIENTO.

Para comenzar, se enlistan las propuestas de solución a los aspectos susceptibles de mejora identificados en el capítulo anterior. Las propuestas están orientadas a hacer cumplir los objetivos del CAD, ayudando en el desarrollo de las funciones como también de los servicios que brinda.

Propuestas:

Propuesta 1. Implementación del dominio de red.

Cambiar la forma de administración de red, pasando de un esquema en grupo de trabajo a un dominio de red. Con esto se centralizará el control de los usuarios y recursos, optimizando las labores de administración. A través del dominio se podrán instalar actualizaciones del sistema operativo y software vía red, y las distintas configuraciones de funcionamiento y seguridad que se implementen podrán ser distribuidas a todas las máquinas, haciendo uniforme el comportamiento de los equipos y de los servicios ofrecidos. Desde el punto de vista de la seguridad, la implementación de un dominio permitirá tener un mayor control en el acceso a los equipos y la información, mejorando los servicios de seguridad como la autenticación y el control de acceso mediante el uso de contraseñas que todos los usuarios del dominio tendrán. Para que los usuarios puedan iniciar sesión en el dominio y tengan acceso a la red, se utilizarán credenciales de identificación de los usuarios, es decir, nombre de usuario y contraseña.

Propuesta 2. Almacenamiento centralizado de la información y software del centro.

Hacer que la información de los usuarios y el software que utilizan se encuentren almacenados en el servidor, de modo que éstos estén disponibles siempre, independientemente de la máquina en la que inicien sesión. Para realizar esto, se propone redirigir la carpeta donde se encuentra su información hacia el servidor, de tal manera que aunque la información sea manipulada en los equipos clientes, será

almacenada en el disco duro del servidor, beneficiando de este modo la disponibilidad de la misma.
En cuanto al software, ésto se refiere a los programas especializados que algunos usuarios requieren, principalmente personal que labora en el CAD. Se propone tener un servidor de aplicaciones, de modo que los usuarios que cuenten con los permisos suficientes, accedan a él para descargar el programa que requieran e instalarlo en la máquina en la que se encuentren.
Los aspectos de seguridad que se verán mejorados son los referentes a la integridad, disponibilidad y confidencialidad de la información, además del control de acceso sobre los equipos clientes y el servidor.

Propuesta 3. Instalación automática del software básico de los equipos.

Mediante una configuración especial, hacer que al momento de agregar los equipos al dominio se instale en ellos el software básico que requieren los usuarios para realizar sus actividades. Este software es el mínimo necesario que estará instalado en los equipos, independientemente del usuario que inicie sesión en ellos.
Esta propuesta ayudará a disminuir la cantidad de tareas y tiempo que los administradores invierten en la configuración de los equipos y beneficiará el funcionamiento uniforme que se desea en las computadoras.

Propuesta 4. Integración de las impresoras al dominio.

Integrar las impresoras al dominio con el objetivo de mejorar la disponibilidad de estos recursos para todos los equipos y usuarios. Las impresoras estarán gestionadas por un servidor de impresión, para mitigar los problemas de conexión y/o configuración de los dispositivos y por ende del funcionamiento de los mismos.

Propuesta 5. Desarrollar una aplicación que automatice la obtención de estadísticas.

Generar las estadísticas de uso de los equipos y recursos del CAD de forma automática mediante una aplicación, la cual estará ligada al dominio para llevar un registro de la asistencia de los usuarios al centro. Esta aplicación permitirá automatizar el procedimiento del registro de asistencia y por otro lado permitirá a los usuarios indicar los recursos utilizados de una manera sencilla, a través de una interfaz gráfica clara. Además de facilitar el registro de estos datos, se pretende también incrementar la certeza de los mismos, disminuyendo las posibilidades de errores tanto en el registro como en la captura de los datos. También, la aplicación tendrá la funcionalidad de graficar la información que se obtenga, de forma que los administradores de la red cuenten con más herramientas que les permitan optimizar la planeación de actividades y adquisición de insumos.

Propuesta 6. Optimización del respaldo de la información.

Dado que la información de los usuarios se almacenará en el servidor de la red, es importante contar con medidas de seguridad especiales para proteger este activo, por lo que se propone crear una estrategia que permita al administrador respaldar la información específica del servidor en otra máquina del dominio. De esta forma, la información de los usuarios estará replicada y los riesgos de pérdida serán disminuidos. Además, el proceso de respaldo se verá mejorado tanto en forma como en tiempo, dado que la información será almacenada centralizadamente y el respaldo se hará para el disco duro del servidor y no para todos los discos de los equipos cliente.

Propuesta 7. Difusión de políticas para el uso adecuado del dominio.

Difundir entre los usuarios las nuevas características de funcionamiento que se tendrán con el dominio, así como los permisos y restricciones que asumirán sobre los equipos. También, se hará de su conocimiento la forma en que deberán utilizar la aplicación de registro de asistencia al Centro y los momentos en los que se esta aplicación se ejecutará durante su visita al CAD.

En la tabla 3.1 se puede observar qué aspecto susceptible de mejora, identificado en el capítulo 2, resuelve cada propuesta planteada en este capítulo.

.

	Aspecto 1 Tratamiento de la información	Aspecto 2 Configuraciones del sistema	Aspecto 3 instalación del software básico	Aspecto 4 administración de las impresoras	Aspecto 5 obtención de estadísticas	Aspecto 6 respaldos de información	Aspecto 7 políticas para el uso de los equipos	Aspecto 8 configuraciones de seguridad
Propuesta 1 Implementación del dominio de red.	x	x						x
Propuesta 2 centralizado de la información y software	x							
Propuesta 3 Instalación automática del software básico			X					
Propuesta 4 Integración de las impresoras al dominio				x				
Propuesta 5 aplicación que automatice la obtención de estadísticas					x			
Propuesta 6 Optimización del respaldo de la información						x		
Propuesta 7 Difusión de políticas							x	

Tabla 3. 1 Matriz de Traza.

1.1 JUSTIFICACIÓN DE LAS MEJORAS.

Algunas de las propuestas planteadas surgen como respuesta a problemáticas que el centro tiene en ciertas actividades que desempeña y que dificultan el total cumplimiento de los objetivos del CAD, otras son medidas proactivas para las actividades que se realizan, pensadas como mejoras a los servicios actuales y también como soluciones anticipadas a dificultades futuras que pueden surgir, como consecuencia del proceso de maduración que toda red informática tiene, tales como el incremento en el número de usuarios y del volumen de la información, el crecimiento de la infraestructura y la necesidad de cubrir nuevos y mejores servicios alineados al avance de la tecnología. Así, la finalidad de las propuestas listadas, es la optimización de las tareas y funciones que se realizan en el centro así como el mejoramiento en los procesos de protección de la información.

Los resultados que se esperan de las propuestas son: la optimización de los procesos de administración y el mejoramiento en aspectos de seguridad. Esto permitirá ahorrar tiempo en las labores de administración así como mejorar los procesos, haciéndolos menos complejos y con mayores alcances. Respecto a la seguridad, los resultados deben generar mayor certidumbre en el manejo de la información, ya que las propuestas están orientadas a salvaguardar sus aspectos fundamentales de confidencialidad, integridad y disponibilidad. Este último punto debe recalcarse ya que para toda organización el activo más importante es la información; desde este enfoque, cualquier medida que se tome con el objetivo de mejorar el resguardo de este activo, debe considerarse como algo positivo.

TEMA 2. ANÁLISIS DE LAS TECNOLOGÍAS PROPUESTAS PARA LA SOLUCIÓN.

Para implementar las propuestas se requirió seleccionar las herramientas adecuadas, para ello, se tomó como base un análisis a dos instituciones (Anexo Análisis de las encuestas aplicadas), que cuentan con un esquema de administración de usuarios y recursos similar al propuesto, es decir, que se basan en el uso de un dominio de red para llevar a cabo sus labores de administración. Además, la elección también consideró el estudio de la situación actual del CAD presentado en el capítulo anterior.

Del análisis realizado se determinó, que para implementar la primera propuesta planteada, la cual considera funcionalidades que van desde la implementación del dominio hasta la distribución de configuraciones a partir de él, el sistema operativo del servidor que controla al dominio sería Windows Server 2008, ya que integra las características necesarias para efectuar las propuestas, tanto de mejora en la administración como en la seguridad de la información planteadas.

A continuación se detallan las características de este sistema operativo, así como las funcionalidades utilizadas en el proyecto y los beneficios que representa para el CAD.

2.1 WINDOWS SERVER 2008.

Windows Server 2008 es el nombre del sistema operativo que la empresa Microsoft diseñó especialmente para equipos servidores, el cual ofrece una plataforma segura de administración para ambientes de red. Es un sistema operativo que tiene una cantidad considerable de versiones anteriores cuyas mejoras paulatinas han resultado en la versión 2008 (El seguimiento de las distintas versiones de este sistema operativo se explica en el tema “Redes en Windows” en el Anexo de Tecnologías).

Windows Server 2008 permite un mayor control en el acceso a los recursos e información, verificando la identidad de quién accede, gestionando los permisos que requieren los usuarios e incrementando la eficiencia de la infraestructura de red que permiten realizar las mejoras en cuanto a seguridad planteadas en la primera propuesta. Además, Windows Server 2008 proporciona una serie de tecnologías de seguridad nuevas y mejoradas que aumentan la protección del sistema operativo. El sistema de protección de servicios de Windows ayuda a mantener más seguros los sistemas al evitar que los servicios críticos del servidor, estén en riesgo por actividades anormales en el sistema de archivos, registro o red. Otra característica importante de este sistema, es la flexibilidad para adaptar la infraestructura a los cambios producidos por las necesidades de las organizaciones, ya que permite una ágil implementación y mantenimiento de sistemas, además de ayudar en la consolidación de diferentes roles de servidor en un mismo equipo (16).

Windows Server 2008 tiene diferentes versiones con características y funcionalidades distintas. La elección de la versión del sistema operativo para este proyecto, se hizo en base a la magnitud de la infraestructura con la que cuenta el CAD, así como de las necesidades que se identificaron previamente. De esta manera, se decidió utilizar la versión Standard ya que es suficiente para satisfacer las necesidades encontradas y está alineada con la infraestructura del centro, puesto que esta versión soporta el uso de servidores como DNS y DHCP, servidor de archivos, servidor de impresión, controladores de dominio, etc. (Para ver una tabla comparativa de las versiones de Windows Server 2008 ir al Anexo de Tecnologías).

Ahora bien, debido a la infraestructura que se tiene en el centro, detallada en el capítulo 2, los servidores mencionados en el párrafo anterior estarán instalados en un mismo equipo. Esta es otra de las razones por la que se eligió una solución de servidor de la familia Windows ya que integra muchas funcionalidades en un mismo equipo.

A continuación se presentan las características principales de Windows Server 2008 Standard utilizadas en el proyecto y los beneficios de cada una para el CAD:

- Identificación y acceso a la infraestructura de red.

  Este servicio permite controlar quién, a qué hora y cómo se tiene acceso a los recursos e infraestructura de red a través de las credenciales de acceso que cada uno de los usuarios utilizará para iniciar sesión en el dominio. De esta manera el personal del CAD podrá administrar la información acerca de los usuarios, los equipos, los recursos y el uso de éstos, garantizando la disponibilidad y controlando el acceso a ellos. Para la aplicación de registro de asistencia y uso de los recursos, este servicio es fundamental porque permite obtener los datos que se requieren. Con esta funcionalidad, el CAD incrementa la seguridad en la red optimizando los procesos de identificación y autenticación de los usuarios, utilizando los protocolos que el sistema operativo maneja para estos servicios de seguridad, los cuales se explican más adelante. Además, la confidencialidad e integridad de la información de cada uno de los usuarios se ven beneficiadas en gran medida al utilizar las credenciales de acceso a los equipos, de este modo, cada usuario tiene un ambiente de trabajo independiente del equipo que utilice, teniendo mayor certeza de que sus archivos de trabajo y configuraciones no serán alteradas por terceras personas, ya que son gestionados centralizadamente. Con este punto se desarrollan funcionalidades propias de la primera propuesta referente a la seguridad de la información, así como de la propuesta de la aplicación para el registro de asistencia al CAD.

- Seguridad y políticas.

  Windows Server 2008 permite definir políticas que mejoran la seguridad para los usuarios y para la infraestructura de red, a través de estándares y mecanismos de seguridad como políticas de grupo (Group policy) y autenticación a través del Directorio Activo con Kerberos. Aunque estos temas se detallarán más adelante, es importante señalar en este punto, que mediante las políticas, se harán las configuraciones necesarias y se distribuirán a todos los equipos desde el servidor para que el funcionamiento en el centro sea uniforme. De este modo, los tiempos de configuración para los equipos disminuyen y se tiene un mejor control de las mismas ya que se hacen de manera centralizada. Las políticas de grupo representan un punto importante en este proyecto ya que a través de ellas se definirá el comportamiento que los equipos tendrán, además permitirán la implementación de varias de las funcionalidades propuestas como el almacenamiento de la información de los usuarios en el servidor, la instalación automática de los programas básicos en los equipos clientes y la instalación de las impresoras.

- Instalación de sistemas operativos vía red.

  A través del servicio WDS (Windows Deployment Service o Servicio de Implementación de Windows) se permite una rápida implementación de los sistemas operativos Windows en los equipos cliente. Con esto, se pueden instalar sistemas operativos a partir de una instalación basada en red, de forma que se facilita la labor de administración, debido a que no hay que estar presente físicamente en cada máquina y no hay que instalar el sistema operativo desde un CD, DVD o cualquier otro tipo de dispositivo de almacenamiento. De este modo, la instalación de los sistemas operativos en los equipos, que antes se hacía de manera individual, se podrá realizar de forma simultánea, inclusive para todos los equipos del CAD si es necesario. El tiempo que se ahorra para realizar esta tarea es significativo, además, si se considera la constante actualización o generación de versiones nuevas que se tiene en los sistemas operativos, esta funcionalidad facilita la actualización que el centro irá teniendo en cuanto a sistemas operativos eventualmente. Por otro lado, previendo el posible crecimiento que tendrá el centro en cuanto a infraestructura, los beneficios de este servicio, aunados a la distribución de configuraciones desde el servidor, se reflejarán en la sencilla y rápida adaptación de los equipos al entorno de trabajo que se tenga. Este punto tiene que ver con la primera propuesta que se refiere a la optimización de las labores de administración, ya que facilita y mejora el proceso de instalación de sistemas operativos.

- Servidores de administración sencilla.

  Entre las razones por las que se instaló el sistema operativo Windows Server 2008 en el servidor del dominio, es por ser un sistema de fácil adopción para los administradores de la red. La sencillez en las configuraciones a través del manejo de interfaces gráficas y asistentes, ha sido una de las principales características de los sistemas Windows, sin embargo, en los sistemas pensados para servidor, se cuenta además con consolas que facilitan la gestión del servidor como la consola de Administrador de Servidor (Server Manager) en Windows Server 2008. Esta consola permite ver y administrar la totalidad de la información y las herramientas involucradas en la funcionalidad de los servidores, permitiendo instalar o quitar roles y características de servidor y agregar o quitar componentes de Windows. El beneficio principal, es la facilidad que otorga a las personas encargadas de gestionar el funcionamiento del equipo servidor, permitiendo delegar funciones a otros sin requerir que cuenten necesariamente con el conocimiento profundo y especializado de alguna tarea o función en particular. Como en el punto anterior, esta característica representa funcionalidades que optimizan el proceso de administración planteado en la primera propuesta.

- Implementación de Servicios y Aplicaciones Web.

  Windows Server 2008 integra el servidor web IIS 7.0 que permite el control sobre los servicios y aplicaciones web y brinda una serie de mejoras en la seguridad de los mismos. Para esta implementación, este servidor web es un requerimiento necesario para la descarga y distribución de las actualizaciones que Microsoft periódicamente desarrolla para el funcionamiento de los equipos, proceso que se detalla más adelante.

Hasta aquí, se han descrito las funcionalidades que tiene el sistema operativo Windows Server 2008 y la forma en que benefician al CAD. Ahora, se describirán las funcionalidades que el servidor realiza como Controlador de Dominio, tema que aunque ya se mencionó en capítulos anteriores, es muy importante de retomar, dada la importancia de este concepto dentro del ambiente de dominio del CAD propuesto.

2.2 CONTROLADOR DE DOMINIO.

En el Capítulo 1 se mencionó que un dominio de red utiliza un directorio centralizado para almacenar las cuentas de usuario y la información de seguridad de la red, también se puntualizó que este directorio reside en equipos configurados como controladores de dominio. Además de esto, los controladores de dominio se encargan de realizar el proceso de autenticación para permitir o denegar a un usuario el acceso a recursos compartidos o a otros equipos de la red, normalmente mediante el uso de credenciales (nombre de usuario y

contraseña) para el inicio de sesión. Una vez que un usuario es identificado y autenticado por el controlador de dominio, una ficha especial (o token) de autenticación es retornada al cliente, de manera que el usuario no necesita volver a "loguearse" para acceder a otros recursos, ya que se considera "logueado" en el dominio.

Como se observa, las funcionalidades que lleva a cabo el Controlador de Dominio son fundamentales para los objetivos que se desean alcanzar con las propuestas, en especial para las mejoras de seguridad esperadas, orientadas a la optimización de lo servicios de seguridad de autenticación, confidencialidad, integridad y control de acceso. Para desarrollar estas funciones, el Controlador de Dominio utiliza distintas tecnologías interesantes e importantes, las cuáles se explican a continuación.

2.2.1 DIRECTORIO ACTIVO.

El Directorio Activo es la herramienta que el dominio utiliza para almacenar información de los usuarios, de los recursos de la red, así como información de seguridad importante. Las principales funciones de esta herramienta son agilizar las búsquedas de recursos, usuarios, además de asegurar el proceso de autenticación, optimizando la comunicación entre los equipos de la red (17).

Utiliza principalmente los protocolos DNS, LDAP y Kerberos para llevar a cabo el proceso de autenticación, así como la comunicación entre usuarios y equipos, además de ubicarlos dentro de la red. Estos protocolos se explican más adelante con mayor detalle.

El Directorio Activo utiliza el concepto de objetos para hacer referencia a los recursos como son impresoras, computadoras, scanner, usuarios, etc. Estos objetos a su vez contienen atributos que los identifican como únicos como se puede ver en la Tabla 3.2. De este modo los objetos son una manera coherente de nombrar, describir, administrar, asegurar y tener acceso a la información centralizada.

Usuario: Julio	
Atributos	***Valores***
Nombre	Julio Rizo Gaona
Departamento	Centro de Apoyo a la Docencia
Usuario	JRizoG

Tabla 3. 2 Atributos de un objeto en Active Directory.

Estos objetos se encuentran organizados de manera jerárquica en estructuras llamadas Unidades Organizativas que facilitan la búsqueda y recuperación de la información concerniente a cada uno. Las Unidades Organizativas representan las estructuras de administración que integran al centro, por lo que hay unidades que almacenan diferentes tipos de objetos como usuarios, departamentos o equipos. La forma en que se diseñaron las Unidades Organizativas, se explican en el siguiente capítulo. Estos componentes forman parte de la estructura lógica que compone el Directorio Activo, sin embargo, existe una estructura física que se compone del controlador de dominio y el sitio en el que se encuentra la red del CAD. (Para profundizar en los componentes de la estructura lógica y física del Directorio Activo, referirse al Anexo de Tecnologías).

El Directorio Activo brinda muchos beneficios en general, sin embargo, las necesidades de cada organización son diferentes. De este modo, las funcionalidades y por lo tanto los beneficios, están orientados a las necesidades que se desean cubrir. Las necesidades ya se han comentado en el tema del análisis de las problemáticas, a continuación se exponen los beneficios que el centro obtendrá al utilizar un servicio de Directorio Activo.

2.2.1.1 BENEFICIOS DEL DIRECTORIO ACTIVO PARA EL CAD.

Los beneficios de implementar un Servicio de Directorio en el CAD son los siguientes:

- En primer lugar, el Servicio de Directorio permite almacenar una gran cantidad de datos como usuarios y recursos que puede ir expandiéndose a medida que las necesidades del CAD lo hacen. Considerando que el CELE recibe cada semestre nuevos profesores, becarios y personal, se potencializa en gran medida la escalabilidad de la red.
- Se optimiza el proceso de administración al gestionar los objetos de la red (usuarios, grupos de usuarios, recursos, programas, etc.) de manera centralizada; permitiendo agregar nuevos objetos, eliminarlos o modificar características como permisos o pertenencia a un grupo. También, es posible delegar la gestión de objetos a distintas personas para efectos de distribución de trabajo o responsabilidades en la red del CAD.
- Desde el punto de vista técnico, el uso de un Servicio de Directorio Activo permite mantener la estructura establecida para la gestión de usuarios y recursos, incluso si es necesario realizar cambios físicos en la red, como por ejemplo, la incorporación de nuevos equipos, dispositivos de red o cambios en la topología. Dado el crecimiento que se espera tenga el CAD, este punto representa un beneficio al centro al facilitar el crecimiento de la infraestructura de red ya que las configuraciones, al distribuirse de manera centralizada a través de la estructura del Directorio activo, no requieren que se invierta demasiado tiempo en cada uno de los equipos que se integren. De este modo, el funcionamiento de la red se vuelve independiente del tamaño de esta, siempre y cuando sea correctamente administrada.

- Un Servicio de Directorio establece un límite de seguridad y administración de la red del CAD, ya que gestiona funciones básicas como la identificación y autenticación de los usuarios cuando ingresen a la red iniciando sesión en los equipos. Esto significa que aunque la red del CAD forma parte de una red más extensa, al utilizar el Servicio de Directorio, se genera un límite que permite tener un mayor control sobre el uso de los recursos, no de manera física sino de manera lógica a través de la red. De esta forma, los administradores de la red del CAD pueden establecer alcances de autoridad sobre los recursos del dominio, es decir, que los administradores definen permisos para controlar qué usuarios pueden utilizar ciertos equipos o recursos pertenecientes al dominio del CAD. Por lo tanto, cualquier persona ajena al centro o sin los permisos necesarios, no podrá hacer uso de los activos hasta que no le sea generada una cuenta por parte de algún administrador. Esto representa mejoras en la integridad de la información, así como en su confidencialidad, otorgando a cada usuario el pleno control de sus datos, dándole la confianza de que estarán resguardados y que nadie, sin los permisos necesarios, accederá a ellos. La disponibilidad de la información es otro de los puntos que se ve beneficiado, ya que el servicio de directorio, a través de los procesos de identificación y autenticación, permite a los usuarios tener su información disponible en cualquiera de los equipos en que inicien sesión y no estar sujetos a que un equipo en específico este desocupado como ocurría antes.
- Al tener todos los elementos de la red almacenados como objetos en el Directorio, se mejora la comunicación entre los equipos y recursos de la red, este proceso aunque es transparente para los usuarios, representa un gran beneficio, ya que se reducen los problemas de conexión entre los equipos y los dispositivos como las impresoras. Para los usuarios que requieren compartir información entre equipos para realizar sus actividades, este punto significa una ventaja considerable respecto a los problemas de conexión que llegaban a suceder con el esquema de red que se tenía anteriormente.

Los beneficios listados son mejoras en cuatro aspectos fundamentales para el CAD:

- ❖ Optimización de los procesos de administración
- ❖ Seguridad de la información
- ❖ Comunicación entre los equipos
- ❖ Control y crecimiento de la infraestructura de red.

Por otro lado, una funcionalidad importante del dominio, que en conjunto con el Servicio de Directorio Activo permite desarrollar muchas de las tareas de administración y seguridad en el dominio, planteadas en la primera propuesta, es la que se refiere a las Políticas o Directivas de grupo, punto fundamental en este proyecto.

2.3 OBJETOS DE DIRECTIVA DE GRUPO (GPO)

Las Directivas o Políticas de Grupo son un conjunto de reglas o configuraciones que dependen del Directorio Activo y que dan a los administradores un alto grado de control sobre los usuarios y equipos de la red, permitiendo definir las características del ambiente de trabajo de los usuarios, con configuraciones del escritorio, sistema operativo, seguridad, scripts de encendido y apagado, scripts de inicio y cierre de sesión, redirección de directorios, reconfiguración de permisos, valores del registro, directivas de cuenta y otras características de los equipos de la red como la instalación de software desde el servidor a los equipos cliente (18).

Las directivas de grupo constituyen también una herramienta importante de seguridad, tanto que son utilizadas como un mecanismo de seguridad debido a las configuraciones que se pueden implementar. Sin embargo, la función principal de las directivas de grupo es la de facilitar la administración con configuraciones centralizadas y no es la de ser una herramienta de seguridad, por lo que hay que estar conscientes de sus limitaciones en este tema.

Para ejecutar las políticas, éstas se definen y almacenan dentro del Directorio Activo en Objetos de Directiva de Grupo (Group Policy Object) y se distribuyen a los equipos y/o usuarios correspondientes. Un GPO almacena casi 300 configuraciones de forma predeterminada. (La explicación del funcionamiento y otros temas importantes de las GPO's se encuentra en el Anexo de Tecnologías).

Muchas de las configuraciones que se desean aplicar con la propuesta, utilizan GPO's para ser distribuidas a los equipos y usuarios del centro. La configuración y funcionalidad de cada una de las GPO's definidas para este proyecto, se explica en el capítulo de Implementación. Sin embargo, a continuación se mencionan las ventajas y beneficios que representa la utilización de las GPO's para el CAD.

Los beneficios que el CAD tiene de utilizar las Directivas de Grupo son:

- El control administrativo que permiten las configuraciones sobre los recursos de la red, teniendo pleno control de los equipos clientes. Las GPO's utilizan modificaciones sobre el registro de Windows de los equipos, de forma que es posible hacer cualquier configuración que se requiera. Además, también se utilizan las GPO's para que se ejecuten los procesos de distintos servidores como el servidor de impresión, de

actualizaciones, de aplicaciones y los servidores necesarios para la instalación de sistemas operativos vía red.

- Facilidad en la creación de GPO's a través de las interfaces del sistema operativo. Utilizando las consolas de administración que contiene el sistema operativo, la creación de las GPO's se lleva a cabo a través de asistentes con los que interactúa el administrador, de tal forma que este procedimiento no requiere de una gran inversión de tiempo o de un profundo conocimiento en temas especializados. Sin embargo, las GPO's que se utilicen deben estar pensadas correctamente en base a las necesidades que se tienen en el centro y a las implicaciones que tendrán las configuraciones sobre los equipos.
- Aplicación selectiva de configuraciones. Las GPO's hacen uso de la estructura del Directorio Activo para la distribución de las configuraciones sobre los equipos y usuarios a los cuáles se desean aplicar. De este modo, es posible tener un mayor control en las configuraciones permitiendo a los administradores decidir cómo aplicarán las configuraciones, sobre quiénes y en qué momento, dependiendo de los privilegios y funciones de los usuarios. Así, el administrador decide si la configuración se aplicará de forma global para todo el centro, o si se hará para un grupo de usuarios en específico o incluso para un solo usuario haciendo uso de la estructura jerárquica del Directorio Activo por medio de los vínculos (Ver anexo de Tecnologías).
- La uniformidad en el comportamiento de los equipos. Dadas las características y funcionalidades que el CAD tiene, se requiere que todos los equipos funcionen de manera similar. Con uniformidad, deben entendere configuraciones como por ejemplo, las características de los escritorios de los usuarios, las configuraciones de bloqueo de sesiones, restricciones para ciertos tipos de usuarios a modificaciones al registro, scripts de apagado y encendido de los equipos, etc.
- Ahorro en tiempo y forma de la aplicación de configuraciones de manera centralizada. Con el uso de las GPO's creadas desde el equipo servidor, las configuraciones se definen sólo una vez y se aplican a los equipos requeridos sin necesidad de ir configurándolos individualmente como antes se hacia. Esto facilita también la integración de nuevos equipos al dominio del CAD, permitiendo aplicar configuraciones de manera automática a través de los GPO's cuando son ingresados a dominio.

A continuación se detallan los temas de seguridad que el dominio de red emplea y que se mencionan en las propuestas de solución, referentes a la protección de la información y las mejoras de la seguridad del dominio de red.

2.4 AUTENTICACIÓN DE RED

La autenticación de red confirma la identificación del usuario en cualquier servicio al que éste intente tener acceso, como loguearse en un equipo o compartir archivos, aplicaciones y recursos de la red. Para proporcionar este tipo de autenticación, el sistema de seguridad admite numerosos mecanismos y protocolos de autenticación. Windows Server 2008 utiliza el protocolo LDAP para proporcionar este servicio de seguridad (19).

2.4.1 LDAP. PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS

Es un protocolo que permite el acceso a un servicio de directorio ordenado (Active Directory Domain Services), para buscar información en un entorno de red. LDAP permite realizar consultas y actualizaciones de los elementos del Directorio Activo. A través de este protocolo, el dominio verifica si el usuario que inicia sesión está contenido dentro del Directorio para darle acceso y para darle los permisos que tiene configurados. Este procedimiento se lleva a cabo internamente en el sistema, de modo que es transparente para el usuario final, sin embargo, son varios los beneficios que se tienen al utilizar este procedimiento de autenticación.

El principal beneficio en términos de seguridad es contar con el servicio de seguridad de autenticación, que otorga acceso solamente a personas autorizadas a los equipos y por ende a la información del centro. Este procedimiento funciona en conjunto con otros servicios de seguridad como el Control de Acceso para llevar a cabo esta tarea.

Sin embargo, la seguridad de la información requiere de otros mecanismos para llevar a cabo sus funciones. En Windows Server 2008 la autenticación trabaja conjuntamente con el protocolo Kerberos cuando se solicita algún servicio a través de la red, como se explica a continuación.

2.4.2 KERBEROS EN EL DIRECTORIO ACTIVO.

Kerberos es el principal protocolo de seguridad para la autenticación dentro de un dominio. Permite realizar el intercambio de información entre los equipos cliente con el servidor, así como atender las peticiones de servicios de los clientes de forma segura. Utiliza el concepto de Ticket para su funcionamiento el cual es un conjunto de datos que identifica a un cliente que ha solicitado un servicio o recurso en la red, este ticket es intercambiado entre el cliente y el servidor y tiene una vigencia para hacer uso del servicio o recurso solicitado (20).

En la red del CAD, este protocolo funciona cuando los usuarios se autentican en los equipos del dominio, verificando en la base de datos del Directorio Activo, que el usuario es quién dice ser, para que posteriormente, el controlador de dominio permita o niegue el acceso a los recursos, dependiendo de los permisos que se tengan. La identificación se hace a partir de las credenciales con las que el usuario inicia sesión en el dominio, datos que son almacenados en los tickets.

Este ticket es protegido de tal manera que no pueda ser conocido o alterado por terceras personas, ya que es un dato que viaja en forma de mensajes para transportar las credenciales del usuario a través de la red del CAD.

De tal forma que este protocolo especifíca mecanismos para:

- Autenticación de la identidad del usuario.
- Empaquetamiento seguro de las credenciales de usuario.
- Aseguramiento de entrega de las credenciales de usuario.

Estos mecanismos, además de mejorar la autenticación de los usuarios y la integridad de los recursos, optimizan los servicios de seguridad de control de acceso, confidencialidad, disponibilidad e incluso no repudio al identificar a los participantes en la comunicación, es decir, tanto al usuario o equipo que solicita el servicio como al servidor que lo otorga.

Al igual que el protocolo LDAP, el funcionamiento de éste, es transparente tanto para los usuarios como para los administradores del CAD, ya que está completamente integrado dentro del sistema operativo. Sin embargo, en el Anexo de Tecnologías, en la sección del Protocolo Kerberos, se explica con mayor detalle técnico el funcionamiento de este protocolo.

TEMA 3. SERVICIOS DE WINDOWS.

En cuanto a los beneficios que brinda para las labores de administración, Windows Server cuenta con varios servicios que facilitan los procesos administrativos. Uno de estos servicios es el que permite instalar sistemas operativos a través de la red, haciendo este procedimiento mucho más ágil y sencillo para los administradores y que forma parte de la propuesta de solución enfocada a la optimización de las labores de administración. Este servicio es el Servicio de Implementación de Windows.

3.1 SERVICIOS DE IMPLEMENTACIÓN DE WINDOWS WDS (WINDOWS DEPLOYMENT SERVICES).

Es un servicio incorporado en Windows Server 2008 para configurar sistemas operativos en equipos mediante una instalación basada en red, esto significa que no es necesario estar presente físicamente en cada equipo ni tampoco instalar cada sistema operativo directamente desde un CD o DVD (21).

Los Servicios de Implementación de Windows se dividen en tres componentes:

- *Componentes de servidor*. Estos componentes incluyen un servidor de Entorno de ejecución previo al arranque (PXE Preboot Execution Environment) y un servidor de Protocolo Trivial de Transferencia de Archivos (TFTP Trivial File Transfer Protocol) para el arranque de red de un cliente, a fin de cargar e instalar un sistema operativo. TFTP es un protocolo de transferencia que se utiliza para mandar pequeños archivos entre equipos en una red. PXE es utilizado para iniciar clientes de red desde un servidor central que brinda el software y configuración necesarios para ejecutar el sistema operativo. PXE obtiene información del DHCP, que informa acerca de servidores de inicio WDS, además de proporcionar una dirección IP que utilizará para comunicarse con este servidor. Mediante TFTP descargará un archivo inicial (network bootstrap program NBP) del servidor de inicio, lo copiará en la memoria RAM de la computadora, lo verificará, y finalmente lo ejecutará.
  En este componente se incluyen también una carpeta compartida y un repositorio que contiene las imágenes de arranque e instalación, así como los archivos necesarios para el arranque en red.

- *Componentes de cliente*. Estos componentes incluyen una interfaz gráfica de usuario (GUI) que se ejecuta dentro del Entorno de Preinstalación de Windows (Windows PE). Cuando un usuario selecciona una imagen del sistema operativo, los componentes del cliente se comunican con los componentes del servidor para instalarla.

- *Componentes de administración*. Estos componentes son un conjunto de herramientas que se usan para administrar el servidor, las imágenes del sistema operativo y las cuentas del equipo cliente.

3.1.1 VENTAJAS DE SERVICIOS DE IMPLEMENTACIÓN DE WINDOWS

La utilización de Servicios de Implementación de Windows en el CAD ofrece las siguientes ventajas:

- Permite la instalación basada en red de sistemas operativos Windows.
- Implementa imágenes de Windows en equipos que no tienen sistema operativo o que requieren ser instalados nuevamente. Dado el uso que los equipos tienen a lo largo del semestre y del volumen de datos que se generan, la reinstalación de sistemas operativos en el Centro ocurre cada 6 meses si es necesario.
- Reduce la complejidad de las Implementaciones y tiempos asociados a procesos de instalación manual.
- Se beneficia el crecimiento de la infraestructura al facilitar el proceso de instalación de sistemas operativos en los equipos.

La configuración e implementación de este servicio se explica en el siguiente capítulo.

Además de instalar sistemas operativos, es importante tenerlos siempre actualizados para efectos de seguridad y de un correcto funcionamiento. En una red, este procedimiento es muchas veces complicado ya que se requiere dedicar tiempo a cada máquina para verificar qué actualizaciones se requieren en cada equipo o si éstas se instalaron correctamente. Como parte de las propuestas, se planteó una mejora que ayudara en la optimización de este proceso; esta mejora centraliza la gestión de las actualizaciones, permitiendo verificar el estado de los equipos y aceptar o no la descarga e instalación de las actualizaciones. Este servicio se explica a continuación.

3.2 WSUS (WINDOWS SERVER UPDATE SERVICES).

Es un componente del sistema operativo Windows Server 2008, que permite administrar el proceso de obtención de actualizaciones que se envían a través del sitio de internet Microsoft Update y su distribución a los servidores y a las computadoras clientes de la red (22).

La infraestructura de WSUS permite que desde un servidor central se descarguen automáticamente los parches y actualizaciones para los clientes en la red, en lugar de hacerlo equipo por equipo desde el sitio web Microsoft Windows Update. Esto ahorra ancho de banda, tiempo y espacio de almacenamiento debido a que las computadoras no necesitan conectarse individualmente a servidores externos al CAD, sino que se conectan directamente al Servidor WSUS instalado en el Controlador de Dominio.

3.2.1 COMPONENTES DE WSUS.

- Microsoft Update.
  El sitio web de Microsoft que distribuye actualizaciones de los productos propios de esta empresa.

- Servidor WSUS (Windows Server Update Services).
  El componente servidor que es instalado en una computadora que ejecuta un sistema operativo Microsoft Windows Server. Para el CAD este servidor se encuentra instalado en el servidor Controlador de Dominio.

- Consola de Administración de WSUS.
  Es una consola de administración automáticamente instalada en el servidor WSUS que permite a los administradores gestionar y distribuir actualizaciones.

- Actualizaciones Automáticas.
  Es una herramienta que permite mantener actualizado el sistema operativo de las máquinas clientes. Habilita al servidor y a las computadoras cliente para conectarse a los servidores de Microsoft Update o de un servidor WSUS para buscar, recibir e instalar las actualizaciones.

Las actualizaciones pueden ser descargadas total o parcialmente dependiendo de la configuración que se requiera para las necesidades del CAD. Para poder hacer esto, las actualizaciones se dividen en dos componentes:

Archivos de Actualización: son los archivos que se requieren para instalar una actualización en un equipo.

Metadatos de Actualización: son datos que permiten identificar la actualización y los usos que tendrá.

De esta manera, si no se almacenan los archivos de actualización localmente, solo los metadatos de actualización son descargados en el Servidor WSUS y las computadoras cliente recibirán los archivos de actualización directamente de Microsoft Update. Si se almacenan las actualizaciones localmente en el servidor WSUS, se pueden descargar tanto los metadatos como los archivos de actualización, aunque esto implica un mayor uso de espacio en el disco duro del servidor.

El funcionamiento de este servicio y las características de las actualizaciones se explican en el Anexo de Tecnologías, sección Funcionamiento WSUS y Actualizaciones de Software.

Las ventajas de este servicio para el CAD son:

- La reducción de tiempo en el proceso de actualización de los sistemas operativos de los equipos de la red. El procedimiento se hará de manera centralizada desde el servidor y desde ahí se distribuirán las actualizaciones de los equipos cliente.
- Mayor control en la gestión de las actualizaciones. Desde el servidor a través de la consola de administración se decidirá qué actualizaciones requieren los equipos, permitirá aprobar o rechazar actualizaciones que no necesariamente son críticas o de seguridad, determinar el momento de instalarlas, a qué equipos aplicarlas y cómo realizar la sincronización de las actualizaciones en el servidor.
- Permite responder con rapidez a las vulnerabilidades de seguridad al identificar los equipos vulnerables bajo su control y distribuir las actualizaciones a esos equipos. Reduce el riesgo asociado con la distribución de actualizaciones al permitir la desinstalación de las mismas.
- Ofrece opciones para obtener informes del estado de los procesos de distribución de las actualizaciones a los equipos clientes.

CONCLUSIÓN.

Este capítulo presentó la solución general que se planteó ante las problemáticas identificadas en el capítulo anterior. Los objetivos principales fueron orientados a la optimización de las labores de administración y al mejoramiento de los servicios de seguridad. La importancia de este capítulo es que muestra el análisis de la solución, con base en los requerimientos previamente identificados. De este modo, se delimitaron las acciones a seguir para solucionar los problemas específicos del centro, considerando también los recursos y necesidades de éste. Así, se buscaron las herramientas y configuraciones tecnológicas más adecuadas para llevar a cabo las acciones de solución, adaptando las funcionalidades de las herramientas a las soluciones requeridas, ya que la mayoría de éstas tienen utilidades que van más allá de las necesarias para el centro. Sin embargo, en un futuro, podrían utilizarse funcionalidades adicionales que generen beneficos para el CAD y los usuarios. En el siguiente capítulo se explica la implementación de la solución general, detallando el proceso para cada una de las configuraciones y herramientas tecnológicas utilizadas.

CAPÍTULO 4

IMPLEMENTACIÓN DEL DOMINIO Y CONFIGURACIÓN DEL DIRECTORIO ACTIVO

CAPÍTULO 4.- IMPLEMENTACIÓN DEL DOMINIO Y CONFIGURACIÓN DEL DIRECTORIO ACTIVO.

INTRODUCCIÓN.

En capítulos anteriores se explicó el funcionamiento que el CAD tenía y se identificaron aspectos susceptibles de mejora cuya solución representa el objetivo principal de este proyecto. Sobre estos aspectos se analizaron y presentaron propuestas que ayudaran a resolver las problemáticas. En este capítulo se explica la implementación realizada de cada una de las propuestas, explicando cómo se ajustaron las características de las distintas herramientas y configuraciones tecnológicas, a las necesidades y requerimientos específicos que se requerían cubrir en el CAD.

TEMA 1. IMPLEMENTACIÓN DEL DOMINIO.

La solución general está basada en la implementación del dominio de red. Sobre el dominio se establecieron las configuraciones y herramientas descritas anteriormente enfocadas a la centralización de la administración de los recursos, los usuarios de la red y la seguridad de la información, optimizando aspectos importantes como la autenticación e identificación de los usuarios y equipos. A través del dominio se definen y distribuyen configuraciones que se aplican sobre los equipos cliente, de forma que se controla el funcionamiento de los mismos de manera centralizada, permitiendo a los administradores establecer distintos perfiles de funcionamiento en los equipos dependiendo de los usuarios que los utilizan y de los permisos que se configuren para ellos en el dominio de red.

Para desarrollar las funcionalidades mencionadas, todo dominio de red cuenta en su estructura con uno o varios equipos centrales, que gestionan diferentes configuraciones importantes de los equipos cliente. Para el CAD, la estructura utilizada se describe a continuación.

1.1 ARQUITECTURA DEL DOMINIO DE RED IMPLEMENTADO.

Considerando los recursos de cómputo con los que contaba el CAD descritos en el capítulo 2 Sección 1.6, el dominio implementado consiste de un equipo central que funge como el servidor de dominio y de diez equipos cliente utilizados por los usuarios del centro. Los equipos cliente son todos iguales por lo que sus características técnicas son las mismas. Las especificaciones técnicas de los equipos cliente y servidor se describen en la siguiente tabla.

	MARCA	MODELO	PROCESADOR	MEMORIA RAM	CAPACIDAD DISCO DURO	SISTEMA OPERATIVO
SERVIDOR	DELL	DIMENSION 5150	Intel Pentium 4 a 3.00 GHz, doble núcleo	3 GB	250 GB interno y uno de 2 TB extraíble.	Windows Server 2008 Standard
CLIENTES	DELL	OPTIPLEX 960	Intel Core 2 Duo a 3.33 GHz	4GB	500 GB	Windows 7 Professional

Tabla 4. 1 Especificaciones técnicas de los equipos del Dominio.

Otros equipos que forman parte del dominio son las impresoras, éstas permiten ser conectadas a la red de forma que pueden ser administradas por un servidor de impresión. Se decidió integrarlas al dominio ya que la impresión es un servicio básico del centro y estando conectadas de esta forma no es necesario instalar las impresoras en cada uno de los equipos, disminuyendo así los contratiempos que se presentaban anteriormente. Estas impresoras tienen las siguientes características.

	MARCA	MODELO	TIPO DE CONEXIÓN
IMPRESORA 1	HP	DeskJet 990	USB
IMPRESORA 2	HP	LaserJet P2055dn	USB y de red, con entrada para conector RJ45

Tabla 4. 2 Características de las impresoras.

Respecto al software, se mantuvo el sistema operativo Windows 7 instalado en los equipos cliente, mientras que en el equipo servidor se instaló el sistema operativo Windows Server 2008 versión Standard (Anexo Implementación del Dominio). Este sistema operativo, como se mencionó en capítulos anteriores, tiene varias funcionalidades importantes que se usaron en la implementación de la solución. Una de ellas es que permite instalar distintos servidores en un solo equipo físico, es decir, que un mismo equipo ejecuta diferentes roles de servidor importantes para desarrollar las funcionalidades requeridas en la solución. La implementación de estos roles se describe a continuación.

TEMA 2. ROLES DEL SERVIDOR..

Cuando se instala el sistema operativo Windows Server 2008 en un equipo, de manera predeterminada, no tiene habilitado ningún rol de servidor, estos roles son instalados posteriormente de acuerdo a las necesidades que se quieran cubrir dentro del dominio a través de una consola incorporada en el sistema operativo para la administración del servidor.

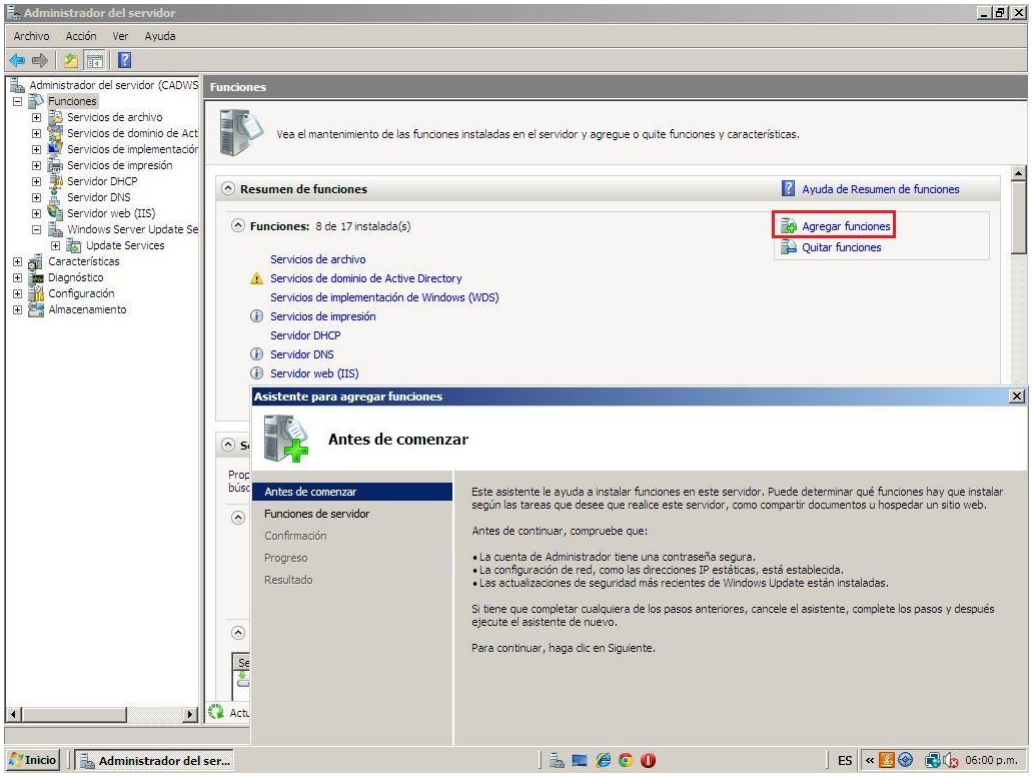


Figura 4. 1 Consola Administrador del Servidor.

Para que un dominio funcione como tal, debe contar con un equipo central que funja como Servidor Controlador de Dominio. Este rol es esencial ya que en este servidor se almacena el directorio centralizado que contiene las cuentas de usuario e información de seguridad de la red. Sin embargo, para la implementación del CAD, antes de instalar la funcionalidad de Servidor Controlador de Dominio fue necesario habilitar el rol de Servidor DNS con el objetivo de que los equipos cliente pudieran ser localizados y se comunicaran dentro de la red.

2.1 CONFIGURACIÓN DEL SERVIDOR DNS.

Para la implementación del servicio DNS en el dominio, se habilitó el rol de servidor DNS en el equipo servidor a través de la consola de administración del servidor, incluida en el sistema operativo Windows Server 2008 (Ver Anexo de Tecnologías).

Una vez instalado el servidor, se estableció el nombre del dominio, el cual está ligado al concepto de espacio de nombres definido en el capítulo 1 Sección 3.2.1. Así, el nombre del dominio configurado para el CAD, de acuerdo a la estructura del espacio de nombres es:

cad.cele.unam.mx.

Este nombre forma parte del FQDN (Fully Qualified Domain Name) de los equipos del dominio del CAD que sirve para indicar la localización de los equipos en el espacio de nombres de DNS. El FQDN está formado por el nombre del equipo y por el nombre del dominio. En la siguiente tabla se muestra el nombre de cada uno de los equipos, así como su respectivo FQDN.

NOMBRE DE EQUIPO	FQDN
CADWS	CADWS.cad.cele.unam.mx
CAD-P-01	CAD-P-01. cad.cele.unam.mx
CAD-P-02	CAD-P-02. cad.cele.unam.mx
CAD-P-03	CAD-P-03. cad.cele.unam.mx
CAD-P-04	CAD-P-04. cad.cele.unam.mx
CAD-P-05	CAD-P-05. cad.cele.unam.mx
CAD-P-06	CAD-P-06. cad.cele.unam.mx
CAD-P-07	CAD-P-07. cad.cele.unam.mx
CAD-P-08	CAD-P-08. cad.cele.unam.mx
CAD-P-09	CAD-P-09. cad.cele.unam.mx
CAD-P-10	CAD-P-10. cad.cele.unam.mx

Tabla 4. 3 Nombres establecidos para los equipos del dominio.

Este servidor, es el servidor DNS autoritativo del dominio en el cual se encuentran registrados todos los equipos del CAD, para resolver las consultas de los equipos cliente. Las consultas pueden hacerse ya sea por el nombre FQDN de los equipos o por la dirección IP; para desarrollar esta funcionalidad, se configuraron en el servidor DNS las zonas de búsqueda directa e inversa respectivamente.

Para establecer los tipos de zona en el servidor DNS, se utilizó un asistente automático en el Sistema Operativo el cual permite establecer los parámetros para la configuración, así como crear los archivos necesarios para el servicio DNS. Estos archivos contienen registros que se utilizan internamente por el servicio DNS haciendo un mapeo del nombre del equipo, dirección IP y tipo de registro de recursos.

Otros archivos importantes que se crean durante la configuración del servidor DNS son el archivo “Hosts” y el archivo de la caché DNS del servidor.

El archivo “Hosts” contiene los registros que relacionan los nombres de los equipos con su respectiva dirección IP. Cuando se agregan los equipos cliente al dominio, los registros de cada uno de los equipos se escriben automáticamente en el archivo Hosts del servidor, de este modo, cuando se inicia el servicio DNS, el archivo Hosts es cargado en la caché del resolvedor DNS de los equipos clientes, haciendo a cada uno de ellos capaz de identificar a los otros equipos del dominio, permitiendo la comunicación y localización de los equipos.

Además de los registros de los equipos del dominio, la caché del resolvedor DNS incluye entradas que el cliente ha recibido en respuestas a consultas del servidor DNS, sobre equipos que no están dentro del dominio. La caché del resolvedor DNS es limpiada cuando el servicio del cliente DNS es detenido.

El archivo de la caché DNS contiene los registros usados por el servicio DNS del servidor autoritativo, para saber dónde comenzar a buscar cuando las consultas de los clientes solicitan equipos fuera de la zona autoritativa del servidor. Estos registros contienen las direcciones de servidores raíz en el espacio de nombres de DNS, a los cuales el servidor DNS consulta para localizar al equipo solicitado por el cliente.

De forma predeterminada, los servidores DNS en Windows Server 2008 usan un archivo pre-configurado de servidores DNS raíz. El contenido de este archivo es precargado cuando el servicio es iniciado.

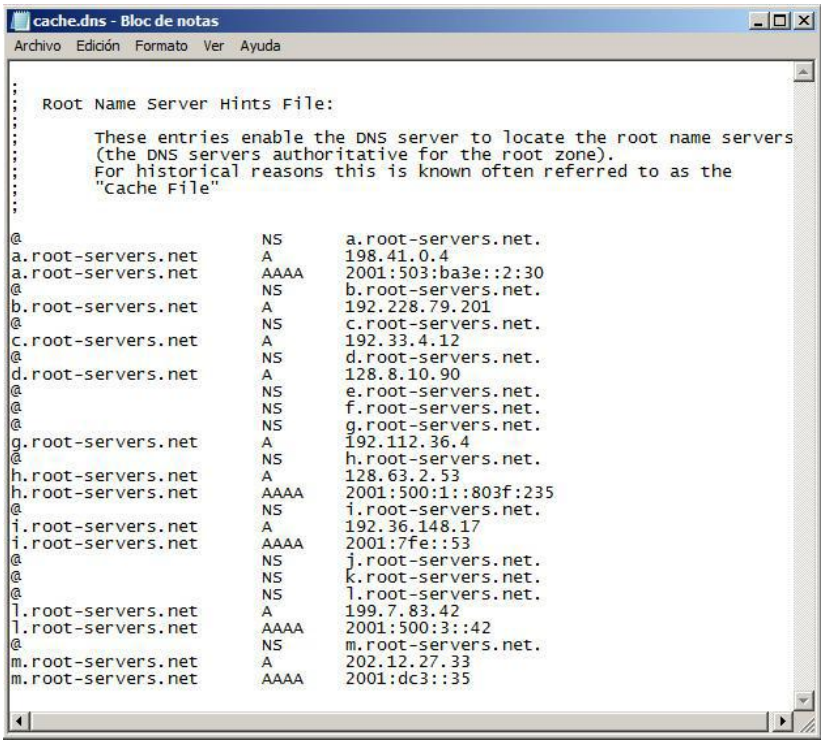


Figura 4. 2 Contenido del archivo cache.dns

Otro rol importante que debe desarrollar el servidor del dominio es el de contener el directorio y gestionar la información que contiene para efectuar distintas operaciones como la búsqueda de usuarios y permisos. A continuación se explican aspectos importantes de este rol.

2.2 ROL CONTROLADOR DE DOMINIO Y ESTRUCTURA DEL DIRECTORIO ACTIVO DEL CAD.

Es importante hacer énfasis en la importancia que tiene definir correctamente la estructura del Directorio Activo, ya que esto determina el modo en el que las configuraciones y las consultas son ejecutadas y por lo tanto, define el funcionamiento correcto del dominio.

Para poder configurar el Directorio Activo, el servidor que lo contiene debe ser promovido como controlador de dominio, esto se realiza mediante el comando DCPROMO ejecutado desde el servidor (Ver Anexo Implementación del Dominio). Al ejecutar este comando se realizan dos tareas. La primera es que el servidor se establece como el servidor controlador de dominio que los equipos identificarán cuando sean agregados al dominio. La segunda es la instalación de los Servicios de Dominio del Directorio Activo.

Esta instalación se realiza a través de un asistente del sistema operativo en el que se establecen distintos parámetros importantes del dominio como el nombre del dominio raíz, el nivel funcional del bosque y del dominio, se definen las rutas donde se almacenará la información del directorio, etc. (El detalle de la configuración se explica en el Anexo Implementación del Dominio). Con la instalación de estos Servicios de Dominio del Directorio Activo, se tiene la base sobre la cual después se agregarán los componentes del Directorio como los usuarios, grupos de usuarios, unidades organizativas y demás estructuras importantes como.

Después de que se instalan los Servicios de Dominio del Directorio Activo se establece la estructura del Directorio. Este punto es medular por la importancia que tiene el directorio en el funcionamiento correcto del CAD. La estructura implementada considera principalmente los diferentes tipos y grupos de usuarios que asisten al CAD, así como las tareas que desarrollan y los permisos que tienen asignados sobre los recursos de la red.

Como se mencionó en el capítulo 2, al CAD asisten tres tipos diferentes de usuarios como son administradores, docentes y personal del centro (Desarrolladores, tesistas, prestadores de servicio social). Cada uno de ellos realiza distintas actividades y tiene diferentes permisos sobre los equipos de la red. De este modo, este factor fue uno de los principales para la estructura implementada del Directorio, ya que era necesario organizar a los usuarios de tal modo que la distribución de las configuraciones y las búsquedas se realizaran de manera eficiente.

Es importante explicar las particularidades que tiene el grupo de usuarios “Docentes” para que se entienda la estructura utilizada en el Directorio detallada más adelante. Los docentes son profesores del CELE los cuales están divididos en Departamentos. Existe un departamento para cada idioma que se imparte en este centro. La lista de departamentos es la siguiente:

- Departamento de Francés, Catalán y Rumano.
- Departamento de Inglés y Sueco.
- Departamento de Ruso, Lenguas Asiáticas y Griego Moderno.
- Departamento de Italiano.
- Departamento de Portugués.
- Departamento de Alemán.
- Instituto Camoes
- Náhuatl

Además de los docentes hay otros trabajadores que pertenecen a la Mediateca del CELE y a la Coordinación de vinculación que también asisten al CAD para realizar sus actividades. Sin embargo, para efectos prácticos estos usuarios tienen los mismos permisos asignados para los docentes sobre los equipos.

Ahora que se ha explicado la forma en la que los docentes están organizados dentro del CELE, se presenta la estructura general del Directorio implementada en este trabajo.

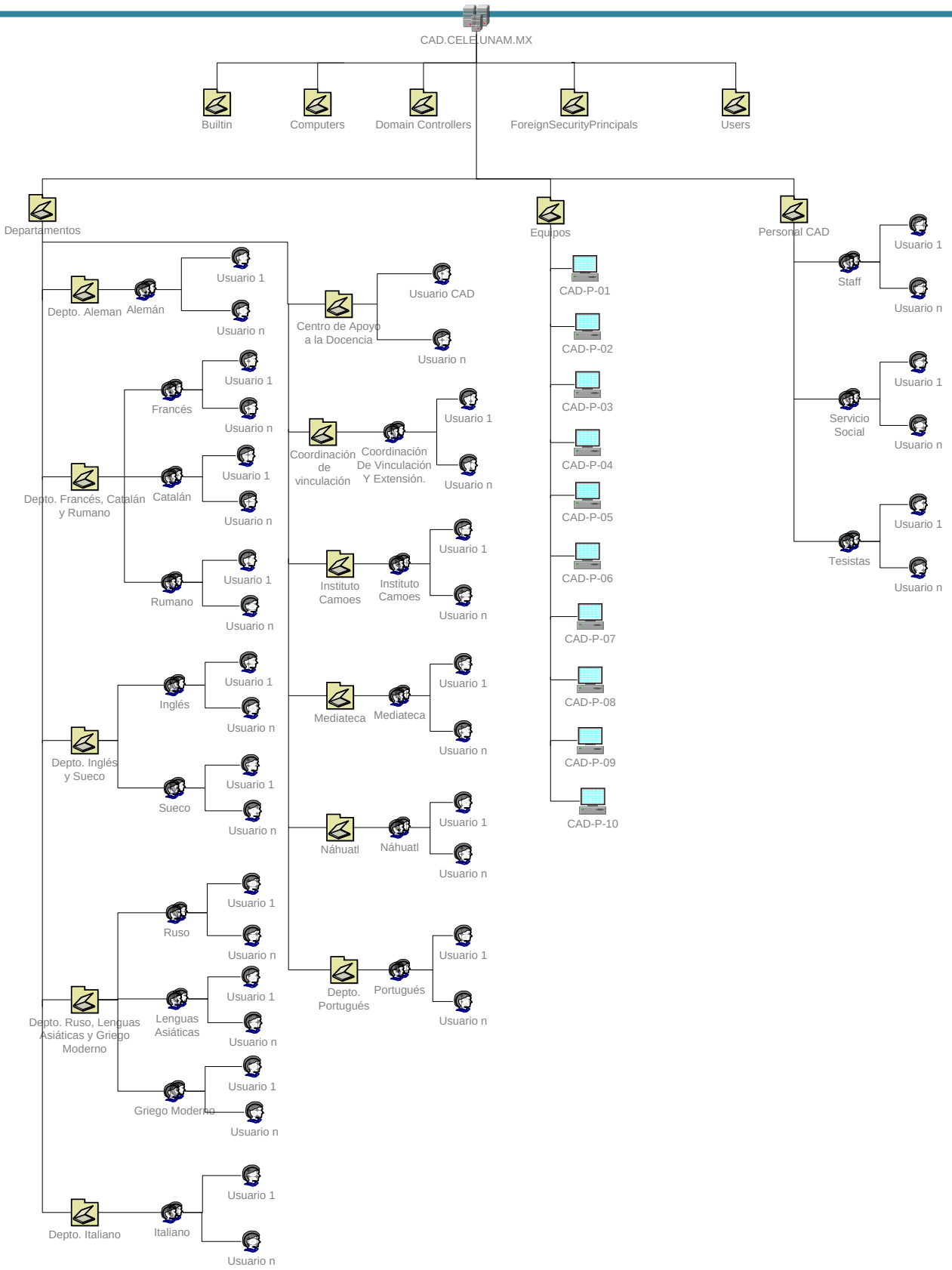


Figura 4. 3 Estructura del Directorio Activo implementado en el CAD.

Como se observa, para la implementación hecha en el CAD se tiene un solo dominio CAD.CELE.UNAM.MX. Después, la estructura jerárquica muestra las OU's (Unidades Organizativas) predefinidas por el sistema. La explicación de cada una de ellas se muestra en la siguiente tabla:

OU	DESCRIPCIÓN
Builtin	Contenedor para cuentas de usuario integradas.
Computers	Contenedor predeterminado para objetos de equipo.
Domain Controllers	Contenedor predeterminado para controladores de dominio.
ForeignSecurityPrincipals	Contenedor para entidades principales de seguridad de dominios externos de confianza. Los administradores no deben modificar manualmente el contenido de este contenedor.
Users	Contenedor predeterminado para objetos de usuario.

Tabla 4. 4 Unidades organizativas predefinidas.

Después se muestran las OU's implementadas para el CAD.

Como se puede observar existen 3 grandes grupos de Unidades Organizativas:

- Departamentos
- Equipos
- Personal CAD

En cuanto a los departamentos, la forma en la que se organizaron estas unidades organizativas ayuda, tanto para hacer la distribución de las configuraciones en un departamento en específico o varios, así como también mejora las búsquedas de usuarios. Desde el punto de vista administrativo, al contar con esta estructura las tareas de agregar, modificar o eliminar las cuentas de los usuarios por departamento se hará de mejor manera, más ordenada y sencilla para la persona encargada de realizar estas actividades. Para aplicar las políticas de grupo, esta estructura permite hacer selectivamente ciertas configuraciones a un grupo en específico, es por eso que en las unidades organizativas que incluyen más de un departamento, por ejemplo la OU Depto. Francés, Catalán y Rumano, internamente se dividen en un grupo para cada idioma, es decir, para la OU mencionada, existe un grupo para Francés, Catalán y otro para Rumano. Las cuentas de usuario que se agreguen en esta OU se asociarán al grupo correspondiente, de forma que sea posible aplicar una configuración sobre un grupo en particular, a varios o a todos los grupos sobre la OU general. Sin embargo si se quisiera aplicar una política sobre toda la OU basta con vincularla sobre la OU padre. Del mismo modo, si una política se desea aplicar sobre todos

los docentes, al aplicarla sobre la OU Departamentos se tendrá el resultado esperado. Por lo tanto, esta forma de estructurar las OU's permite que los políticas de grupo sean aplicadas de cualquier forma que se requiera, ya sea a un solo departamento, a varios o a todos. Al tener esta división de OU's por departamentos, también se tiene la opción de delegar el control de un departamento o un grupo de ellos a distintas personas con los permisos necesarios, de tal forma que las labores de administración pueden llevarse a cabo por más de una persona si así se requiriere.

Para el grupo Equipos, se generó esta OU con el objetivo de poder aplicar alguna configuración sobre ciertos equipos, por ejemplo, se realizó una configuración que permite utilizar la impresora de color sólo a dos equipos. De este modo, si una configuración se requiere aplicar sólo a un equipo o a un grupo de ellos la estructura lo permite, al igual que si se requiere aplicar a todos los equipos. También permite agregar fácilmente un nuevo equipo a la OU así como darlo de baja. Ahora bien, dado que los equipos pueden ser utilizados por cualquier tipo de usuario del dominio, el comportamiento que tenga en cuanto a las configuraciones, dependerá del perfil del usuario y no de la máquina en específico, es decir, la mayoría de las configuraciones se aplican a nivel de usuario y no de equipo.

Para la unidad organizativa Personal CAD se tienen definidos tres grupos: Staff, Servicio Social y Tesistas. De este modo las configuraciones se aplican a un solo grupo, a varios o a todos, dependiendo de la política de grupo que se requiere aplicar. La división de grupos tiene el objetivo de tener un mayor orden y control en la forma en que se apliquen las políticas, pero también permite optimizar las búsquedas de los usuarios y grupos en el flujo de datos interno del dominio. Esta OU, es sensible ya que los usuarios que pertenecen a ella, requieren de permisos especiales sobre los recursos en la red, los cuales podrían afectar al dominio si se aplicaran arbitrariamente a todos los usuarios. Por ende, se debe tener especial cuidado cuando se agregue o se dé de baja a un usuario que pertenezca a esta OU y también se debe cuidar que las configuraciones se vinculen correctamente a las personas que corresponda dentro de ella.

Los roles y la pertenencia a los grupos predeterminados en el sistema operativo del servidor para los tipos de usuarios del dominio se presentan en la siguiente tabla.

Rol	**Grupo predeterminado**
Administradores	Administradores
Personal CAD (Administradores)	Administradores
Servicios Social	Usuarios
Tesistas	Usuarios
Docentes	Usuarios

Tabla 4. 5 Roles y permisos de los usuarios del dominio.

La descripción de los permisos que tienen los grupos predeterminados se presentan a continuación.

Grupo	Descripción
Administradores	Los miembros de este grupo tienen pleno control del servidor de dominio y de los equipos cliente del CAD. También tiene los privilegios de hacer copias de seguridad de archivos y directorios con el propósito de realizar copias de seguridad del sistema. Tienen privilegios de gestión de impresoras y pueden analizar el rendimiento del sistema o de un solo proceso entre otros. Puesto que este grupo tiene un control total del dominio se debe tener precaución al agregar usuarios a este grupo.
Usuarios	Los miembros del grupo “Usuarios” pueden realizar las tareas más habituales, como ejecutar aplicaciones, usar las impresoras del centro, y bloquear el equipo. Los miembros de este grupo no pueden compartir directorios ni crear impresoras locales. Los grupos Usuarios de dominio y Usuarios autenticados que existen en el sistema de manera predeterminada son miembros de este. Por lo tanto, todas las cuentas de usuario que se crean en el dominio son miembros de este grupo.

Tabla 4. 6 Descripción de los grupos predeterminados (23).

Un rol importante que desempeña el servidor del dominio, en pro de la seguridad de la información, es el de brindar los servicios de autenticación. A continuación se explican los detalles de la implementación de este rol.

2.3 ROL DE AUTENTICACIÓN.

En capítulos anteriores se estableció la importancia que este servicio de seguridad tiene para la seguridad del dominio y la forma en que se propuso mejorarlo a través del uso de los protocolos LDAP y Kerberos incluidos en el Directorio Activo. Estos protocolos funcionan conjuntamente para brindar acceso a los usuarios y equipos, tanto al dominio como a los recursos contenidos en él, así como también, aseguran la identidad de los servidores haciendo un procedimiento de autenticación mutua. Con la información contenida en el directorio, la cual es consultada por el protocolo LDAP, se corroboran los datos con los cuales los usuarios y equipos intentan acceder al dominio o algún recurso y se otorgan los permisos que tendrán sobre ellos, el proceso de autenticación para obtener el acceso al dominio es gestionado por el protocolo de Kerberos.

Estos protocolos están incorporados de manera predeterminada en el sistema operativo Windows Server 2008 con el Directorio Activo, de modo que a diferencia de otros roles

específicos de servidor como DNS, no requieren ser habilitados desde la consola de administración del servidor.

Cuando el servidor es promovido como controlador de dominio y los servicios de directorio son configurados, se crea una cuenta especial llamada “KRBTGT” que utilizará el protocolo Kerberos para su funcionamiento.

La cuenta “KRBTGT” es usada por el “TGT” (Ticket Granting Ticket de Kerberos, ver Anexo de Tecnologías), y sirve para cifrar mensajes con la contraseña establecida para esta cuenta cuando la solicitud de sesión entre equipos clientes y servidor es hecha. Esta cuenta está deshabilitada de forma predeterminada y no puede cambiarse su estado debido a que es usada internamente por el sistema.

El funcionamiento conjunto de estos protocolos puede resumirse de la siguiente manera. El protocolo que se encarga de los procesos de autenticación es Kerberos, este gestiona los mensajes de solicitud de acceso al dominio entre los equipos cliente y el servidor. Para desarrollar sus funciones, Kerberos utiliza la información contenida en el directorio, la cual es accedida por LDAP, para corroborar los datos y verificar que los usuarios estén contenidos en el directorio para así otorgar el acceso de los usuarios al dominio. También utiliza información de seguridad importante, almacenada en el directorio, como lo es la información acerca de los permisos configurados para los distintos usuarios al igual que información específica que utiliza para el cifrado de los mensajes, como se explicó con la cuenta KRBTGT. Sin embargo, la implementación de estos protocolos se desarrolla de forma automática y es utilizada a partir de que el servidor se promueve como controlador de dominio.

2. 4 CONTENEDOR DE POLÍTICAS DE GRUPO.

El servidor del dominio también es un contenedor de las políticas de grupo que se ejecutan en los equipos cliente. A través de una consola de Administración de directivas de grupo se definen, gestionan y almacenan las políticas. Las políticas implementadas como parte de la propuesta de solución para este proyecto son las siguientes:

Política No. 1 Revisión de contraseñas, longitud y complejidad.

Esta política ayuda a resolver problemáticas identificadas referentes a la protección de la información.

Contar con contraseñas para acceder a los equipos del CAD no es suficiente para garantizar que sólo personas autorizadas tengan acceso a ellos. Estas contraseñas deben ser difíciles de obtener por terceras personas, haciéndolas robustas, es decir, forzando a que tengan características especiales tanto de longitud como de caracteres contenidos. Estos rasgos

especiales de las contraseñas serán validados automáticamente por el sistema mediante la configuración de esta directiva.

Los beneficios de esta política de grupo son:

- Control automático de validación de la complejidad de las contraseñas de los usuarios.
- Disminución de riesgos de obtención de contraseñas por terceras personas.
- Mejora en la confidencialidad, integridad y control de acceso para la información del Centro.

Política No. 2 Distribución e instalación de Software

Aplica sobre la problemática referente a no tener instalado el mismo software en todos los equipos. El objetivo es automatizar la instalación de software básico en los equipos al momento de su integración al dominio.

Los beneficios de esta política de grupo son:

- Reducción en la inversión de tiempo por parte de los administradores para la habilitación de los equipos cuando se integran al dominio.
- Uniformidad en el funcionamiento de los equipos.
- Facilitar la transición en el cambio de esquema de red de grupo de trabajo a dominio de forma que no impacte en el funcionamiento de los equipos.

Política No. 3 Almacenamiento de Software

Aplica sobre la problemática que se refiere a no tener instalado el mismo software en todos los equipos y la dependencia en la disponibilidad de algunos de ellos para el uso de software especializado.

Los objetivos de esta política son:

- Permitir a los usuarios autorizados disponer del software especializado necesario desde cualquier máquina del dominio.

- Centralizar el software necesario para la realización del trabajo de los usuarios del CAD como los prestadores de servicio social, tesistas, administradores, etc.

- Evitar que la falta de disponibilidad de equipos obstaculice la realización del trabajo de los usuarios en el CAD.

Beneficios:

- Mejora en la disponibilidad de los equipos.
- Los usuarios autorizados podrán instalar el software necesario en los equipos fácilmente sin necesidad de buscarlo o descargarlo de internet.

Política No. 4 Política de actualizaciones de los sistemas operativos Windows

Se refiere al aspecto susceptible de mejora relacionado con la configuración individual de las actualizaciones en los equipos cliente.

Los objetivos de esta política son:

- Centralizar la administración de las actualizaciones para tener un mayor control de las mismas.
- Optimizar la tarea de actualización en los equipos del centro.
- Mantener a los equipos actualizados y funcionando lo más uniforme posible.

Beneficios:

- Mejorar el proceso de actualización con un control centralizado de la descarga y distribución de las actualizaciones a los equipos del dominio, así como de la revisión del estado de las mismas en cada uno de los equipos.

- Disminución en la inversión de tiempo de los administradores para la ejecución de esta tarea.

Política No. 5 Política para asignar cuotas de espacio de disco duro a usuarios

Esta política se enfoca en apoyar en la resolución de las problemáticas referentes a la seguridad por las que se sugería a los usuarios evitar guardar información importante en los equipos del CAD.

El objetivo principal es dotar a los usuarios de espacio en disco duro del servidor para que guarden su información y que esta pueda ser utilizada en cualquier equipo donde inicien sesión.

Beneficios:

- Los usuarios tendrán la opción de almacenar su información en el disco duro del servidor.
- La información podrá ser manipulada por los usuarios autorizados en cualquier equipo en el que inicien sesión, mejorando la disponibilidad de la misma en el centro.

Política No. 6 Política para bloquear sesión después de cierto tiempo de inactividad

Se refiere a las problemáticas identificadas en cuanto a la protección de la información.

El objetivo es proteger los datos de los usuarios cuando dejen abierta su sesión por algún descuido u omisión.

Beneficios:

- Protección de la información.
- Disminución de riesgos en cuanto a la alteración o pérdida de información de manera accidental por otro usuario.

Política No. 7 Política para restringir opciones de administración del sistema.

Esta política se refiere a la problemática que trata acerca de las configuraciones de seguridad que pueden ser mejoradas.

El objetivo es proteger a los equipos de configuraciones que pueden ocasionar problemas en su funcionamiento limitando la disponibilidad de los mismos. Con esta política se disminuye la posibilidad de que personas sin los permisos necesarios, realicen configuraciones sensibles en los equipos que generen un funcionamiento erróneo.

Beneficios:

- Disminución de riesgos de configuraciones incorrectas en los equipos.
- Protección de la integridad de los equipos.

Política No. 8 Política para redireccionar carpeta “Documentos” a unidad en red.

Esta política se enfoca en apoyar en la resolución de las problemáticas referentes a la seguridad por las que se sugería a los usuarios evitar guardar información importante en los equipos del CAD.

El objetivo es permitir a los usuarios almacenar información en el disco duro del servidor de tal manera que esté disponible en cualquier máquina del dominio con las condiciones suficientes de integridad, confidencialidad, disponibilidad y autenticación.

Beneficios:

- Los usuarios podrán almacenar información el disco duro del servidor.
- La información estará disponible en cualquier máquina desde la cual los usuarios inicien sesión.

- La distribución de los equipos será independiente de la información almacenada en ellos.

Política No. 9 Política para la agregación de impresoras al dominio.

Esta política funciona en conjunto con el rol de servidor de impresión para solventar el aspecto susceptible de mejora referente a las impresoras.

El objetivo es publicar los dispositivos de impresión desde el servidor de impresión para que los equipos que se integran al dominio hagan uso de ellos de forma predeterminada.

Beneficios:

- Se automatiza la configuración de impresoras en cada equipo.
- Optimización de integración de los equipos al dominio para su utilización inmediata.

Además de estas políticas, se utilizaron otras que requirieron de la habilitación de ciertos roles de servidor para que se lograra cubrir la funcionalidad deseada en las propuestas. Estos roles se explican a continuación

2.5 ROL DE SERVIDOR DE IMPRESIÓN

A través de este servicio, se publican y asignan las dos impresoras del centro de forma predeterminada a cada una de las computadoras del dominio sin necesidad de configurarlas individualmente, esto implica una instalación de impresoras mediante el dominio del CAD de una forma más eficiente para los administradores.

También, con este servicio se tiene un mayor control de los trabajos de impresión, ya que muestra un panorama general de la cantidad de impresiones que se realizaron, así como los equipos que usaron este servicio, dotando a los administradores de información adicional.

Para realizar la implementación total de este servicio, se utilizó conjuntamente una política de grupo (Anexo Políticas de grupo “Política para la integración de impresoras al dominio”), la cual publica los dispositivos de impresión en el dominio y es vinculada a los equipos cliente, para que éstos tengan instaladas las impresoras automáticamente en el momento en que son integrados al dominio.

Los principales beneficios que se tienen con la implementación de este servicio y la política de grupo son:

- Disminución en problemas de conexión de las impresoras con los equipos del dominio al instalarlas mediante políticas de grupo y controlarlas desde el servidor de impresión.

- Instalación automática de las impresoras en los equipos al momento de ser agregados al dominio.
- No se requieren conectar las impresoras a equipos clientes del CAD para que puedan ser utilizadas como se hacía anteriormente.
- Se tiene un registro del número total de impresiones que se llevan al día, con fines de planeación de adquisición de insumos.

2.6 ROL DE SERVIDOR WSUS.

Otro de los roles que se habilitó en el servidor del dominio es el Servicio de Actualización WSUS. WSUS constituye un servicio integral para administrar las actualizaciones en la red del CAD. Es una solución que automatiza el proceso de gestión de actualizaciones todo lo posible mejorando y facilitando las tareas de los administradores en cuanto al control de las actualizaciones en los equipos del dominio.

Dado que los requisitos mínimos de hardware para el servidor WSUS (Descritos en el anexo de Tecnologías) son satisfechos por el servidor del CAD, fue necesario tener en cuenta los requisitos de software. De este modo, se instaló el servidor IIS7.0 que WSUS usa para actualizar a los equipos clientes. Durante la configuración de WSUS se crea un directorio virtual llamado Selfupdate en un sitio web que utiliza el puerto 80 del servidor WSUS. Este directorio virtual contiene el software de compatibilidad de Actualizaciones Automáticas de WSUS que utilizan los equipos cliente. También se requiere de una base de datos en donde el servidor WSUS almacena los datos de las actualizaciones. Esta base de datos es Microsoft Server SQL que tiene de manera predeterminada WSUS en la implementación del dominio del CAD. Además de esto, WSUS requiere del software Report Viewer 2008 para la presentación de los informes del estado de las actualizaciones. La instalación del servidor IIS, la base de datos y Report Viewer 2008 se explican en el Manual de implementación.

Además de la configuración del servicio de WSUS, se utilizó una política de grupo (Anexo Políticas de grupo, “Política de actualizaciones de los sistemas operativos Windows”) para habilitar en los equipos la opción de permitir las actualizaciones automáticas así como establecer la ruta con la cual los equipos clientes se comunican con el servidor WSUS.

Aunque la descripción de la instalación y configuración del software mencionado se explica en el Manual de implementación, es importante explicar opciones importantes utilizadas y las razones por las que se eligieron.

En primer lugar se eligió que toda la información de las actualizaciones se guarde localmente en el servidor WSUS de modo que la distribución de las mismas a los equipos clientes se haga directamente desde el servidor. Esto disminuirá el tráfico de datos para la descarga de actualizaciones desde servidores externos en la red ya que sólo el equipo servidor se conecta con Microsoft Update para hacer la descarga.

La instalación de las actualizaciones está programada para que se realice de forma automática, en períodos de tiempo que no afecten las labores diarias del centro, evitando la pérdida de disponibilidad de los equipos, sobre todo con actualizaciones que requieren del reinicio de los mismos.

Las actualizaciones que se descargan son únicamente las necesarias para mantener la seguridad y estabilidad de los equipos por lo que se estableció descargar las actualizaciones críticas, de seguridad y los parches de los Sistemas Operativos (Service Pack). De este modo se reduce el volumen de información de descarga dejando únicamente la necesaria para el correcto funcionamiento de los equipos.

Las configuraciones mencionadas pueden ser modificadas en cualquier momento que se requiera desde la consola de administración de WSUS.

2.7 ROL PARA EL SERVICIO WINDOWS DEPLOYMENT SERVICES (WDS).

Un rol más de servidor que se habilitó fue el de Servicios de implementación de Windows (WDS) el cual resuelve uno de los aspectos susceptibles de mejoras identificados en el capítulo 2 que se refiere al proceso de instalación de sistemas operativos de forma individual. Con la implementación de este servicio se optimiza el proceso de instalación de sistemas operativos, ya que permite a los administradores agregar uno o varios archivos imagen que contienen el sistema operativo que se podrán instalar en los equipos clientes desde la red, esto centraliza el proceso de instalación, ya que la imagen sólo se agrega una vez en el servidor y podrá ser accedida por los clientes en cualquier momento y la veces que sea requerido sin la necesidad de contar con el CD o algún otro dispositivo de almacenamiento que contenga el sistema operativo.

Para desarrollar esta funcionalidad el servicio WDS requiere trabajar en conjunto con el servicio DHCP el cual, se encargará de la repartición de direcciones ip temporales a los equipos cliente que soliciten este servicio para poder entablar una comunicación con el servidor, de esta forma tendrán acceso a los archivos que contienen el sistema operativo almacenados en el servidor, para ejecutarlos e instalarlos desde la red de la forma usual a través de un asistente que proporciona Windows.

Los beneficios que se tienen con este servicio son:

- Reducción de tiempo para la instalación de sistemas operativos.
- Mayor control en la versión de los sistemas operativos instalados en los equipos al estar centralizadas las imágenes en el servidor.
- Mejora en las labores de mantenimiento, al permitir el formateo de los equipos en un tiempo considerablemente menor al que se invertía anteriormente.

En el siguiente capítulo se explican con mayor detalle los resultados obtenidos.

TEMA 3. DESARROLLO E INTEGRACIÓN DE LA APLICACIÓN SISTEMA DE ADMINISTRACIÓN DE INFORMACIÓN DEL CAD (SAID).

Un aspecto susceptible de mejora que se identificó fue el que se refiere a la obtención de estadísticas de asistencia y uso de los recursos del CAD. Anteriormente esta tarea se realizaba de forma manual lo que generaba ciertos problemas explicados en el capítulo 2. Para mejorar este proceso se decidió desarrollar una aplicación que automatizara esta tarea. El nombre de la aplicación es Sistema de Administración de Información del CAD.

El objetivo principal de esta aplicación, en primera instancia fue automatizar el registro de la asistencia de los usuarios al CAD cuando éstos inician sesión en algún equipo del dominio. Sin embargo, se observó que también se podían desarrollar otras funcionalidades con esta aplicación como son las que se listan a continuación:

- Conocer la frecuencia con las que los usuarios asisten al Centro.
- Conocer cuál o cuáles son los recursos más utilizados por los usuarios.
- Obtención y graficación de datos que permiten saber la frecuencia de uso de los equipos en un cierto periodo de tiempo.

Para registrar la asistencia de usuarios al centro, se creó un programa que se ejecuta automáticamente cuando un usuario inicia sesión de trabajo en algún equipo del dominio, dicho programa envía la siguiente información a una base de datos:

- El nombre de inicio de sesión del usuario.
- El nombre de la computadora donde el usuario inició sesión.
- La dirección IP del equipo.
- La fecha y hora en que el usuario inició sesión.
- La fecha y hora en que el usuario finalizó su sesión.

Para registrar el uso de recursos se creó otro programa, el cual permite al usuario introducir información para posteriormente ser almacenada en una base de datos. Cuando un usuario del dominio cierra su sesión de trabajo automáticamente se ejecuta esta segunda aplicación y la información que se envía es la siguiente:

- El nombre de inicio de sesión del usuario.
- El nombre de la computadora donde el usuario inició sesión.
- La dirección IP del equipo.

- Nombre del recurso utilizado.
- Cantidad de uso del recurso.
- Fecha que cerró su sesión el usuario.

SAID consulta la base de datos y obtiene la información para procesarla y presentar los datos de forma gráfica, todo esto permite a los administradores tener un panorama actual del uso de los recursos y asistencia al CAD.

Una funcionalidad adicional que se agregó a esta aplicación es la de el registro a una asesoría, el cual es uno de los servicios brindados actualmente en el CAD.

SAID permite al usuario registrar la siguiente información.

- Su nombre de usuario.
- Hora y fecha de la asesoría.
- El nombre de usuario de inicio de sesión en el dominio del asesor.
- El nombre de su correo electrónico al que se enviará una notificación, en caso de que no esté registrado en el dominio.

Esta aplicación aprovecha el esquema del Directorio Activo y LDAP que se tiene en el dominio para validar su nombre de inicio de sesión y su contraseña para confirmar la asesoría.

Para el desarrollo de SAID se hizo uso de una tecnología llamada GRAILS, la cual es un marco de trabajo para el desarrollo WEB.

Dado el conocimiento y la experiencia en la utilización de esta tecnología, se llegó a la conclusión de que es una herramienta que permitía cubrir los requerimientos necesarios para que la aplicación funcionara debidamente (Anexo Requerimientos aplicación).

La tecnología utilizada para la gestión de la base de datos fue PostgreSQL, dado el conocimiento y experiencia previa que se tenía con ella. Es un gestor de base de datos que se adapto bien a las necesidades de la aplicación.

Para realizar las operaciones referentes a la información contenida en la base de datos del directorio que desarrolla la aplicación, se utilizó el lenguaje de desarrollo C# desarrollado por Microsoft, lo que representa una ventaja en cuanto a compatibilidad y facilidad de integración de ambas tecnologías.

Con esta tecnología y en conjunto con el lenguaje de consulta LDAP para el Directorio Activo se logró cumplir con uno de los requerimientos de la aplicación, el cual, consiste en validar la existencia de los usuarios en el directorio.

CONCLUSIONES.

En este capítulo se presentó la implementación de las herramientas y configuraciones empleadas en la solución general propuesta para este proyecto.

La tabla 4.7 muestra la relación entre los aspectos susceptibles de mejora, las propuestas de solución y su implementación en forma de políticas de grupo, funcionalidades del servidor y la aplicación SAID. Como puede observarse, todos los aspectos susceptibles de mejora se ven cubiertos con las propuestas y su implementación, utilizando en algunos casos más de una forma de ejecución, para que en forma conjunta cubrieran la funcionalidad total propuesta.

Esta implementación buscó solucionar las distintas problemáticas identificadas en el centro, sin embargo, una vez que la solución fue ejecutada, se requirió de tiempo para visualizar los resultados del trabajo realizado, así como detectar los problemas que surgieron con el nuevo esquema de red implementado y del funcionamiento de las herramientas y configuraciones utilizadas. En el siguiente capítulo se hace un análisis de los resultados obtenidos y se presentan las conclusiones finales de este proyecto.

	Rol /Política/ Aplicación	Aspecto 1 Tratamiento de la información	Aspecto 2 Configuraciones del sistema	Aspecto 3 instalación del software básico	Aspecto 4 administración de las impresoras	Aspecto 5 obtención de estadísticas	Aspecto 6 respaldos de información	Aspecto 7 políticas para el uso de los equipos	Aspecto 8 configuraciones de seguridad
Propuesta 1 Implementación del dominio de red.	Rol Controlador de Dominio	X	X						X
	Política 1								
	Política 4								
	Política 6								
	Política 7								
Propuesta 2 centralizado de la información y software	Política 3	X							
	Política 5								
	Política 8								
Propuesta 3 Instalación automática del software básico	Política 2			X					
Propuesta 4 Integración de las impresoras al dominio	Servidor de impresión				X				
	Política 9								
Propuesta 5 aplicación que automatice la obtención de estadísticas	Aplicación SAID					X			
Propuesta 6 Optimización del respaldo de la información	Política 5						X		
	Política 8								
Propuesta 7 Difusión de políticas								X	

Tabla 4. 7 Relación entre aspectos susceptibles de mejora, propuestas e implementación.

CAPÍTULO 5

RESULTADOS

CAPÍTULO 5. RESULTADOS.

INTRODUCCIÓN

Este capítulo muestra los resultados obtenidos con cada una de las propuestas implementadas en el centro para hacer frente a los aspectos susceptibles de mejora identificados. Para presentarlos, se realizó un análisis individual de los resultados de cada una de las propuestas, algunos de éstos son cuantitativos con datos que los fundamentan y otros son cualitativos, con una explicación que respalda los cambios obtenidos. Se explican estos resultados realizando una comparación, entre el estado inicial mostrado en el segundo capítulo de este proyecto, contra el estado final, una vez realizada la implementación de las propuestas. A partir de esta comparación, se exponen los aspectos que se mejoraron así como también se hace un símil entre el número de incidencias presentadas antes y después del dominio mediante una tabla comparativa. Finalmente, a partir de los resultados presentados en este capítulo, se identificaron algunos puntos sobre los que se pueden desarrollar funcionalidades extras más adelante y que forman parte del trabajo a futuro que se plantea al final de este capítulo.

TEMA 1. MEJORAS CON LA IMPLEMENTACIÓN DEL DOMINIO.

A continuación se listan los resultados obtenidos para cada aspecto susceptible de mejora identificado en el capítulo 2.

Aspecto 1. Mejorar el tratamiento de la información.

Resultados.

Se logró el objetivo principal de esta mejora de salvaguardar los aspectos fundamentales de confidencialidad, disponibilidad e integridad de la información. La confidencialidad se mejoró mediante el uso, para cada uno de los miembros del dominio, de un nombre de usuario y su respectiva contraseña para iniciar sesión en los equipos del centro. De esta forma, ningún usuario no autorizado puede tener acceso a información que no le corresponda. Cabe mencionar, que en un principio, esta medida generó cierta inconformidad por parte de algunos usuarios, que argumentaron que estos datos hacían más complejo el uso de los equipos, al tener que generar sus contraseñas, recordarlas y protegerlas además de ingresar estos datos en los equipos cada vez que los utilizaran. Sin embargo, una vez que se les explicaron las razones de esta medida en base a los beneficios que representan sobre la confidencialidad de la información, los usuarios accedieron a probar esta medida y finalmente la adoptaron de forma correcta. Respecto a la disponibilidad, los resultados representan una mejora considerable de este servicio, ya que a través del almacenamiento centralizado de la información en el servidor, se logró que independientemente del equipo en el que los usuarios trabajen, tengan siempre su información a la mano para realizar su

trabajo. Esto representa una mejora en el servicio que el CAD presta de uso de Infraestructura, facilitando la distribución de los equipos a los usuarios. En cuanto a las mejoras de la integridad, los resultados permiten dar certeza a los usuarios de que su información está protegida correctamente al contar con mecanismos de autenticación que aseguran el inicio de sesión, de tal manera que sólo los usuarios autorizados tienen acceso a la información para poder manipularla y/o alterarla. Además el mejoramiento del procedimiento de respaldo de información, también representa mejoras para su integridad, ya que de esta manera se reduce en gran medida las posibilidades de pérdida de información de los usuarios.

Estos resultados son de gran importancia para el proyecto en general, ya que están enfocados a la protección del activo más importante que se tiene, esto genera que los usuarios tengan la confianza suficiente para guardar su información en los equipos del centro, sabiendo que sólo ellos y los usuarios que autoricen pueden acceder a esta. También, los resultados mejoran el procedimiento de trabajo respecto a la distribución de los equipos, ya que la información “sigue” a los usuarios, es decir, está disponible desde cualquier equipo en el que inician sesión, agilizando la distribución y permitiendo también desarrollar actividades de los profesores como la aplicación de exámenes de manera simultánea en los equipos.

Aspecto 2. Optimizar la forma en la que se realizan las configuraciones del sistema.

Resultados.

Para esta mejora se observó un cambio notorio en los tiempos de instalación del Sistema Operativo (S.O.) en los equipos del CAD, ya que el servicio que se implementó permite instalar un S.O. en varios equipos simultáneamente, lo que representó un ahorro de tiempo por parte de los administradores y mayor disponibilidad de equipos para los usuarios como indica la Tabla 5.1. De igual forma, mediante el servicio de actualización implementado, se ahorró tiempo en la instalación de actualizaciones de los Sistemas Operativos, ya que esta tarea se realiza automáticamente y de una forma más eficiente por parte del servidor en todos los equipos del dominio, además, los administradores del centro tienen una mejor gestión de todas las actualizaciones que se requieren enviar a cada computadora, con ello se evitan de mandar actualizaciones innecesarias a los equipos.

	SIN DOMINIO	CON DOMINIO
TIEMPO DE INSTALACIÓN DE SISTEMAS OPERATIVOS EN UN EQUIPO	18.06 minutos	18 minutos
TIEMPO DE INSTALACIÓN DE SISTEMAS OPERATIVOS EN TODOS LOS EQUIPOS	180.6 minutos	18 minutos

Tabla 5. 1 Tiempos de instalación de Sistemas Operativos.

Aspecto 3. Instalar automáticamente el software mínimo necesario en todos los equipos del centro.

Resultados.

Los resultados que se tuvieron sobre este punto básicamente impactan en la disminución de tiempos que los administradores requieren invertir para la instalación del software básico en los equipos como se observa en la Tabla 5.2. Esta disminución en tiempo se debe a que a través del dominio y con políticas de grupo, la instalación del software básico se hace de manera automática cuando los equipos son agregados al dominio, de tal manera que no se requiere configurarlos individualmente como anteriormente se realizaba. Esta mejora, además de beneficiar en tiempo, ayudó a que el cambio que significó pasar de un esquema de red en grupo de trabajo a dominio, afectara lo mínimo posible a los usuarios de los equipos, de tal manera que éstos estuvieran disponibles inmediatamente con el software básico requerido. Otro beneficio que se tuvo con esta mejora, es la uniformidad en el software instalado en los equipos y por lo tanto en su funcionamiento, lo que significa que para los usuarios que utilizan el software básico, cualquier equipo del dominio cumple con los requerimientos necesarios para apoyar en la realización de sus actividades, por lo que los programas instalados en los equipos ya no es factor a considerar para su distribución a los usuarios.

Para los usuarios que requieren de ciertos programas en específico, y que por lo tanto cuentan con permisos especiales, los resultados de la mejora son la centralización de los programas en una carpeta dentro del equipo servidor desde donde se pueden instalar en el equipo en el que se encuentren trabajando. Esto significa tener mayor control de los programas y versiones que se instalan, así como facilidad para su búsqueda e instalación. El contar con esta medida, significa también, que este tipo de usuarios puede utilizar cualquier equipo disponible del dominio para realizar su trabajo e instalar los programas que necesitan

de manera sencilla y rápida, lo que resuelve el problema que se tenía anteriormente de la dependencia de ciertos equipos y su distribución a los usuarios, misma que puede observarse en la tabla 5.4 dentro de la Incidencia “Falta de disponibilidad de programas” . Para los administradores del Centro, esto significa además una disminución considerable de tiempo para buscar el software e instalarlo en los equipos, ya que a través de los permisos configurados para los usuarios, estas actividades se delegan a aquellos con los privilegios suficientes para llevar a cabo la instalación y desinstalación de programas..

Así, esta medida, además de facilitar y disminuir las tareas relacionadas con la gestión del software en el centro por parte de los administradores, mejora la disponibilidad de los programas para la realización de las actividades de los diferentes usuarios que asisten, así como también, mejora la disponibilidad de los equipos y facilita su distribución a los usuarios.

	SIN DOMINIO	**CON DOMINIO**
INSTALACIÓN DE SOFTWARE ESENCIAL EN UN EQUIPO	10 minutos	10 minutos
INSTALACIÓN DE SOFTWARE ESENCIAL EN TODOS LOS EQUIPOS	100 minutos	10 minutos

Tabla 5. 2 Tiempos instalación de software esencial.

Aspecto 4. Mejorar la administración de las impresoras.

Resultados.

Con la implementación del servicio de impresión del dominio, se tiene un mayor control de las impresoras dado que la configuración y gestión se realiza de manera centralizada en el servidor del dominio. Esto facilita el proceso de instalación ya que la configuración se realiza únicamente en el servidor, de tal forma que cuando un equipo es ingresado al dominio, automáticamente se instalan las impresoras en el equipo, esto reduce el tiempo que anteriormente se le dedicaba a esta tarea, la cual se realizaba de forma independiente en cada uno de los equipos.

En la siguiente tabla se hace una comparación de los tiempos invertidos en la instalación de las impresoras con y sin dominio.

	SIN DOMINIO	CON DOMINIO
TIEMPO DE INSTALACIÓN Y CONFIGURACIÓN INDIVIDUAL	6 minutos	10 minutos
TIEMPO DE INSTALACIÓN Y CONFIGURACIÓN EN TODOS LOS EQUIPOS	60 minutos	10 minutos

Tabla 5. 3 Tiempos de instalación de impresoras.

El tiempo de instalación y configuración individual que indica la tabla, se refiere al tiempo de instalación de las dos impresoras que se tienen en el centro en cada uno de los equipos, y dado que se tienen 10 equipos, se invertían 60 minutos para instalar los dispositivos de impresión en todos ellos. Con el servicio de dominio que se tiene actualmente, el tiempo en la tabla es el mismo para la configuración individual y global ya que el procedimiento de instalación y configuración se realiza únicamente en el servidor. Este tiempo involucra la instalación del servidor de impresión, la generación de las políticas de grupo necesarias y su vinculación a los equipos.

Sin dominio, el tiempo global de instalación de impresoras depende del número de equipos que se tengan, a diferencia de contar con el servicio de impresión en dominio, en donde el tiempo será el mismo sin importar el total de equipos en el centro.

También hay que considerar que frecuentemente las impresoras se desconfiguraban de los equipos cuando no había dominio, por lo que se tenían que instalar nuevamente las impresoras en los equipos. Actualmente con la instalación del servicio de impresión, este problema disminuyó, dado el mayor control que se tiene de estos dispositivos mediante el servicio de impresión gestionado únicamente por los usuarios con los permisos correspondientes.

Esta disminución de problemas puede observarse en la tabla 5.4 en la fila correspondiente a problemas al imprimir, que muestra el número de incidencias con las impresoras en un periodo determinado sin y con dominio.

LISTA DE INCIDENCIAS.			
NOMBRE DE INCIDENCIA	**DESCRIPCIÓN**	**TOTAL DE INCIDENCIAS SIN DOMINIO 1 de febrero al 28 de septiembre del 2012**	**TOTAL DE INCIDENCIAS CON DOMINIO 1 de octubre al 10 de febrero del 2013**
Pérdida de archivos	Se refiere a que uno o más archivos propios del usuario que se tenían guardados en el disco duro de las computadoras no se encuentra donde fueron dejados.	5	0
Falta de disponibilidad de programas	Cuando el equipo en donde se encuentran los archivos o programas que un usuario necesita está ocupado por alguien más. También cuando a alguien de servicio social o tesista se le pida desocupar el equipo en el que está debido a que ahí haya información de otro usuario aunque existan otros equipos disponibles.	28	5
Problemas al imprimir	Especifica problemas de los equipos para poder realizar impresiones o usar el escáner.	34	2
Problemas al compartir archivos	Se refiere a problemas para intercambiar archivos entre equipos del Centro.	22	0

Tabla 5. 4 Incidencias

Aspecto 5. Automatizar la obtención de estadísticas del Centro.

Resultados.

Los resultados de esta mejora son tres principalmente. El primero es la optimización en el proceso para recabar los datos de las estadísticas, al tomar la asistencia de los usuarios de manera automática, durante el proceso de autenticación en los equipos cuando inician sesión. Para los datos que se toman referentes al uso de los recursos, esta medida cambia la forma manual que se utilizaba anteriormente al uso de una interfaz gráfica que se ejecuta en el equipo en el que trabajaron y desde la cual los usuarios introducen los datos de los recursos usados. El segundo resultado implica el tener mayor confianza de los datos que se obtienen ya que con esta medida, además de que la asistencia se toma de manera automática, también se redujo el problema que había de usuarios que olvidaban registrar sus datos o que los que registraran incorrectamente. Con el incremento en la precisión de esta información, los administradores tienen mayores y más confiables parámetros para llevar a cabo la planeación de la compra de insumos y de distintas actividades y estrategias que mejoren el servicio que se presta en el centro. Finalmente, el tercer resultado logrado, se refiere al alcance que permiten las funcionalidades de la aplicación SAID para realizar la graficación de los datos, lo que es una herramienta importante para la organización y planeación de distintas actividades por parte de los administradores. Además, esta aplicación, dada su vinculación con el directorio activo del dominio, puede servir como base para desarrollar más funcionalidades importantes como la gestión de cursos o talleres que se den en el centro.

En la siguiente tabla se observa el tiempo que se ahorran los administradores para realizar la captura de información contenida en los formatos de asistencias, con la incorporación del dominio, esta tarea se realiza en automático mediante el sistema desarrollado (SAID).

	SIN DOMINIO	CON DOMINIO
TIEMPO PARA CAPTURAR LA INFORMACIÓN CONTENIDA EN LOS FORMATOS DE ASISTENCIAS	72 hrs.	Automático
TIEMPO PARA PROCESAR LA INFORMACIÓN	24 hrs.	Automático

Tabla 5. 5 Tiempos para la obtención de estadísticas.

Aspecto 6. Optimizar la forma en la que se realizan los respaldos de información.

Resultados.

Los resultados de esta mejor se reflejan en la optimización de la forma en la que se realiza esta tarea, ya que ahora para comodidad de los administradores, el respaldo se hace únicamente de la información que está almacenada en el servidor de dominio, disminuyendo la inversión de tiempo que se requería para hacer el respaldo individual de cada uno de los equipos. Además de esto, se mejora el control en el respaldo de la información ya que con el dominio, dicho respaldo se tiene por usuario y no por equipo como anteriormente se hacía, de esta forma, teniendo la información de los respaldos mejor organizada, las búsquedas se hacen de manera más eficiente.

Con esta forma de respaldo, se reducen las posibilidades de pérdida de la información de los usuarios, esta es una mejora sobresaliente dado la importancia que este activo representa y que se puede observar en la Tabla 5.4 dentro de la Incidencia llamada “Pérdida de archivos”.

En la siguiente tabla se observa el tiempo que se ahorran los administradores para realizar el respaldo de información, ya que actualmente éstos son automáticos.

	SIN DOMINIO	CON DOMINIO
TIEMPO PARA RESPALDAR LA INFORMACIÓN DE UN EQUIPO	2.5 hrs. (aproximadamente)	automático
TIEMPO PARA RESPALDAR LA INFORMACIÓN DE TODOS LOS EQUIPOS	23 hrs. (aproximadamente)	automático

Tabla 5. 6 Tiempos para los respaldos de información.

Aspecto 7. Difundir políticas para el uso de los equipos.

Esta propuesta se realizó con la intención de que cada usuario del centro conociera el funcionamiento del dominio mediante el seguimiento de reglas que se redactaron en el anexo de “Reglamento de seguridad del dominio”, que describen brevemente lo que se debe y no hacer en el dominio. Los resultados de esto son la seguridad que el usuario tiene al hacer uso de algún equipo con las nuevas funcionalidades, además de procurar un buen uso del dominio, todo esto conlleva a que el centro brinde un mejor servicio con mayor seguridad y de mejor calidad.

Aspecto 8. Optimizar la forma en la que se realizan las configuraciones de seguridad del sistema.

Resultados.

Esta propuesta fue una medida proactiva que se tomó para disminuir los riesgos de configuraciones críticas que afectaran el funcionamiento de los equipos. Así, el resultado de esta medida fue evitar que los usuarios pudieran ejecutar estas configuraciones críticas voluntaria o involuntariamente. De esta manera los equipos se mantienen menos susceptibles a amenazas como las configuraciones dañinas que pudieran presentarse.

Estos resultados ayudan a mantener la integridad y disponibilidad de los equipos para poder llevar a cabo las actividades que en el centro se realizan. Sin embargo, la seguridad nunca existirá al 100% por lo que es necesario concientizar a los usuarios en el uso correcto de los equipos y las consecuencias potenciales de configuraciones peligrosas para los equipos y en general para los recursos con los que se cuentan.

Durante la implementación de las soluciones se identificaron algunas funcionalidades adicionales que se pueden llevar a cabo teniendo como base la solución general desarrollada en este proyecto. En la siguiente sección se explican estas funcionalidades y la forma en que apoyarían al centro.

TEMA 2. TRABAJO A FUTURO.

A continuación se presentan algunos puntos que se proponen como trabajo a futuro que puede generar beneficios interesantes para las actividades del CAD:

- Dado el potencial crecimiento del centro en cuanto a número de equipos, se propone la adquisición de otro servidor para que funcione concurrentemente, de este modo habrá un balanceo de carga dada la virtualización de roles en el servidor y habrá más fiabilidad en las operaciones, ya que si alguno llega a fallar siempre se tendrá la opción de respaldo del otro equipo.

- Escalar las características de hardware y software del servidor controlador de dominio cuando se dé el crecimiento en el número de equipos clientes ya que esto incrementará el procesamiento requerido por el servidor. Al tener un servidor con mayores capacidades de procesamiento las tareas y peticiones que se realicen hacia el servidor se realizarán con mayor eficiencia. Para el software se recomienda el tener siempre actualizado el equipo y dado el desarrollo de las versiones del sistema operativo estar al pendiente de las mejoras que se generen y si son necesarias para las tareas que se requieren.

- Conectar el servidor a una fuente de poder ininterrumpida para que en caso de fallas en el suministro eléctrico sigan en funcionamiento las tareas críticas que desarrolla el servidor. Esto evitará pérdida de información y de configuraciones en el servidor que pudieran generar daños críticos paulatinamente en el funcionamiento en general de los equipos.

- Adquirir software de terceros para crear archivos de instalación de Microsoft cuya extensión es “.msi” a partir de archivos ejecutables “.exe”, de tal manera que se instalen más programas de manera automática, inclusive el software especializado y no solamente el básico. Esto hará mucho más sencillo el procedimiento de instalación dando a los administradores la oportunidad de decidir si estos programas se instalarán para todos los equipos o se publicarán para que los usuarios con los permisos necesarios los instalen directamente desde la función de “Agregar o quitar programas” del sistema operativo Windows y no desde una carpeta del servidor.

- Dada la integración que la aplicación tiene con el directorio activo del dominio, se puede desarrollar la funcionalidad de la gestión de cursos y talleres que en el centro se desarrollan para que la asistencia y notificación de nuevos cursos y talleres, se realice automáticamente. Incluso, se podrían generar estadísticas de asistencia a los cursos y notificaciones masivas para los interesados. De esta forma se tendrá otra forma para el control y planeación de estas actividades que involucra tanto a la aplicación SAID como al directorio activo.

- Al igual que con la consola que se tiene para la gestión centralizada de las actualizaciones, es posible administrar el software de antivirus, de tal forma que desde el servidor se pueda tener registro del estado de los equipos y poder ejecutar tareas como el escaneo a uno, a varios o a todos los equipos del dominio. Para esto es necesario adquirir la licencia del software antivirus e instalar la versión de consola de administración en el equipo servidor. Esto permitirá elevar los niveles de seguridad de los equipos, recursos y de la información en general.

- En el centro existen diversas aplicaciones propias y otras más que están en desarrollo las cuales requieren de la autenticación de los usuarios. Este procedimiento de autenticación puede ligarse al directorio activo del dominio de tal manera que al iniciar sesión, con las credenciales respectivas, se tenga acceso a estas aplicaciones. Sin embargo, esta medida requiere de un análisis detenido y de tomar las provisiones necesarias de seguridad para que sólo los usuarios autorizados tengan los permisos debidos.

- Instalación del servicio de correo de Outlook en los equipos cliente y servidor del dominio de manera que se ligue con el directorio activo y se puedan desarrollar todas las funcionalidades como la sincronización de calendarios y la generación de eventos. Esto facilitará la sincronización del calendario de actividades y permitiría tener paulatinamente el servicio de correo utilizando el dominio del centro.

- Generar “clones” periódicamente del disco duro del servidor para que funcionen como puntos de restauración y se eviten problemas posteriores de alguna índole. Esto permitirá regresar a estados del servidor en el que las configuraciones funcionaban adecuadamente y no requerir formatear el equipo hasta un nivel inicial de fábrica.

CONCLUSIÓN.

En este capítulo se presentaron los resultados de cada una de las implementaciones de las configuraciones realizadas en este proyecto, presentando las mejoras logradas en tiempo y forma. También se realizó una comparativa del número de incidentes presentados antes y después de la implementación del dominio de red. De esta comparativa se puede observar una reducción considerable en el número de incidentes presentados, lo que significa una mejora importante en el funcionamiento día a día de las actividades del centro; esto es debido a que los resultados obtenidos mejoran las labores de administración y brindan mayor seguridad en el manejo de la información, lo que significa también, que se logró el objetivo principal del proyecto. Por otro lado, en el apartado de “Trabajo a futuro”, se presentaron las funcionalidades potenciales que tienen algunas de las mejoras implementadas y que se pueden desarrollar más adelante tomando como base esta implementación, explicando la forma en que apoyarían en las actividades del CAD.
En la siguiente sección de “Conclusiones”, se presentan los resultados generales obtenidos con la realización de este proyecto, tanto para el Centro como personalmente.

CONCLUSIONES

CONCLUSIONES FINALES.

Al finalizar este trabajo y una vez realizado el análisis de los resultados, se obtuvieron las siguientes conclusiones, tanto del proyecto como personales. En primer lugar, se presentan las conclusiones del proyecto tomando como base los objetivos planteados al inicio.

Con la implementación del dominio, se logró centralizar la administración de los principales recursos del centro, es decir, los usuarios y la información. Además, se centralizó también la gestión del software utilizado en el centro y de las actividades de configuración de los equipos, desde la instalación de sistemas operativos y programas, hasta configuraciones importantes de seguridad. Con esto se mejoraron los procesos de administración tanto en tiempo como en forma, de tal manera que ahora los administradores realizan las configuraciones en el equipo servidor y las distribuyen a los equipos de la red del centro. Con estas mejoras se permite también, la delegación de responsabilidades y tareas para los administradores de forma que se apoya la organización y planeación de las actividades sobre los equipos. Por otro lado, con la agrupación de la información, se mejoró en gran medida el resguardo y control de esta, permitiendo alcanzar el objetivo planteado de salvaguardar los aspectos fundamentales de integridad, disponibilidad y confidencialidad de la información. Este objetivo representa para los usuarios contar con su información en cualquier equipo del centro, sabiendo que está debidamente protegida y a salvo de modificaciones por usuarios ajenos, dado el uso de credenciales de inicio de sesión que ahora se requiere en todos los equipos.

Además de los beneficios obtenidos sobre la administración de los recursos y de la información, el implementar el dominio, significó también mejoras importantes para la seguridad en el centro, ya que estos tópicos, administración y seguridad, están intrínsecamente relacionados, dado que una correcta administración conlleva a tener el escenario ideal para la implementación o preservación de los servicios de seguridad. Para el proyecto, las configuraciones de seguridad se realizaron mediante políticas de grupo, las cuales permite definir, distribuir y gestionar el servidor controlador de dominio. Dado que la implementación del dominio y la instalación de las herramientas utilizadas en este proyecto no significaron una gran complejidad, los esfuerzos principales se enfocaron en el diseño de la solución a las problemáticas identificadas con base a las necesidades puntuales y específicas del centro.

Por otro lado, la implementación del directorio activo permite la integración con otras aplicaciones como la aplicación SAID desarrollada en este proyecto. Esta aplicación registra la asistencia al centro por parte de los usuarios y permite obtener estadísticas de uso de los recursos, pero además tiene funcionalidades potenciales para ser desarrolladas más adelante ya que se conecta con el directorio activo del dominio donde se encuentra almacenada la información básica indispensable de cada uno de los usuarios.

Sin embargo, dentro de las conclusiones caben también algunos aspectos cuya implementación en un futuro requiere analizarse dada la potencial importancia que representan para las actividades en el Centro como por ejemplo, la centralización de la gestión de los antivirus; esto representaría una mejora importante para la seguridad de los equipos y la posibilidad de programar escanéos periódicos automáticos en los equipos, lo que disminuiría la vulnerabilidad hacia la amenaza de código malicioso que pudiera llegar a perjudicarlos y eventualmente generar problemas más serios en la red del centro.

Otro punto que no se logró completar del todo fue la estrategia que se planteó para mantener siempre en funcionamiento el controlador de dominio para brindar los principales servicios. En ambos casos se debe gestionar la adquisición de material adicional que permita cubrir es su totalidad estos puntos. Para el antivirus se debe tener un software que acepte la administración centralizada, en el mercado existe una gran variedad de estos programas cumpliendo la mayoría de ellos con las necesidades indispensables para el centro. Para el caso del controlador de dominio, lo ideal es contar con un servidor de respaldo que funcione inmediatamente cuando exista algún problema con el equipo principal. Estos temas quedan como propuesta ya que la adquisición de material es un tema que excede los alcances del proyecto.

Ahora bien, respecto a las conclusiones personales, el haber realizado esta implementación representó la oportunidad de poner en práctica los conocimientos adquiridos durante los estudios y desarrollar otros para cumplir con los objetivos planteados. A lo largo del proyecto, fue evidente la importancia que tuvieron los conocimientos teóricos para planear y diseñar las soluciones, pero sin duda, la perspectiva es muy diferente cuando se llega a la fase de construcción de las soluciones. Y es que es ésta fase la que muestra la diferencia entre los supuestos y la realidad, la que permite obtener resultados palpables y comprobar hipótesis o suposiciones. De este modo, al integrar la teoría con la práctica en el desarrollo de este proyecto, se lograron aterrizar conceptos importantes y muy interesantes para el cómputo en temas de seguridad informática, administración de redes, programación, arquitectura cliente-servidor y varios más. Por eso, este proyecto fue integral ya que se cubrieron varias ramas de la computación, pero siempre fue un trabajo orientado a resultados y objetivos específicos para los que se tuvo que planear, diseñar, ejecutar y controlar acciones que permitieran llegar a los objetivos planteados. Así, este fue un trabajo metódico, que bajo la guía de personas con mucha capacidad y experiencia, permitió por una parte desarrollar capacidades y habilidades personales poniendo en práctica los conocimientos adquiridos y por otro lado sirvió para dar solución a necesidades puntuales que generaran beneficios, en este caso, para los usuario del Centro. Es por ello, que éste proyecto fue importante, ya que cumple con el verdadero significado de la Ingeniería, que es idear y ejecutar soluciones con los recursos que se tienen a la mano para solucionar problemas en beneficio de la comunidad.

Además, este proyecto dejó aprendizajes personales que seguramente servirán en futuras etapas y proyectos que se desarrollen más adelante. El haber trabajado en equipo significó todo un reto para hacer la planeación de las actividades, la administración de los tiempos y para transmitir, escuchar y encausar las ideas para la obtención de los resultados deseados. También, sirvió para aprender a transformar las necesidades en requerimientos y las ideas en soluciones, aspectos muy importantes que sin lugar a dudas serán provechosas en el ámbito laboral.

Finalmente, con todo lo explicado anteriormente, se puede terminar diciendo que el haber realizado este proyecto valió la pena, porque más allá de ser el trabajo que dé la opción de obtener un título, es un trabajo que brinda una satisfacción personal difícil de describir porque significa la culminación de un esfuerzo importante que posiblemente se pudo haber hecho de otra forma, en menos tiempo quizás, pero que finalmente, es una meta más que se logró alcanzar.

REFERENCIAS

Referencias

(1) Stoltz, Kevin.: “Todo acerca de las Redes de Computadoras”, Prentice Hall, México 1995.
   (1.1) pp. 16
   (1.2) pp. 34
   (1.3) pp. 91
   (1.4) pp. 65
(2) Stallings, William.: “Comunicaciones y Redes de Computadoras”, Prentice Hall, 7ª ed., España 2004.
   (2.1) pp. 15
   (2.2) pp. 113
   (2.3) pp. 112
   (2.4) pp 117
   (2.5) pp. 17
   (2.6) pp. 29
   (2.7) pp. 36-39
   (2.8) pp. 40
   (2.9) pp. 42
   (2.10) pp. 611
(3) Tanenbaum, Andrew.: “Redes de Computadoras”, Pearson, 4ª ed., México 2003.
   (3.1) pp. 16
   (3.2) pp. 38-41
   (3.3) pp. 581
   (3.4) pp. 579-582
   (3.5) pp. 68
(4) Tanenbaum, Andrew S.: “Redes de ordenadores”, Prentice Hall, 2ª ed.
   (4.1) pp. 67
   (4.2) pp. 25
   (4.3) pp. 66
   (4.4) pp. 23
(5) Black, Uyless.: “Redes de Computadoras, Protocolos, Normas e Interfaces”, RA-MA Editorial, España 1995.
   (5.1) pp.8
   (5.2) pp. 349
(6) López Barrientos, Ma. Jaquelina; Quezada Reyes, Cintia.: “Fundamentos de seguridad informática”, UNAM, Facultad de Ingeniería, México 2006.
   (6.1) pp. 115-125
(7) Kurose, James; Ross, Keith.: “Redes de Computadores *Un enfoque Descendente Basado en Internet*”, Pearson, Madrid 2004, 2ª ed..
   (7.1) pp. 316
   (7.2) pp. 120
   (7.3) pp. 320
   (7.4) pp. 469-470
(8) MAN http://aprendaredmanunerg.blogspot.com/
(9) Tanenbaum, Andrew S.: “Sistemas operativos modernos”, Prentice Hall, 1ª ed., México 1993.
   (9.1) pp. 1

(9.2) pp. 13
(9.3) pp. 450
(9.4) pp. 457

(10) Pérez Carretero, Jesús : "Sistemas Operativos *Una visión aplicada*", Mc Graw Hill, 1ª ed.,España 2001.
(10.1) pp. 34
(10.2) pp. 35
(10.3) pp. 45
(10.4) pp. 231

(11) Silberschatz, Abraham: "Sistemas Operativos", Limusa, 6ª ed., México D.F., 2002.
(11.1) pp. 39

(12) Stallings, William: "Sistemas Operativos", Prentices-Hall, 4ª ed., España, 2001.
(12.1) pp. 557

(13) WIFI
(13.1) http://es.wikipedia.org/wiki/Wi-Fi
(13.2) http://wifiw.com/802/componentes-de-una-red-inalambrica-wireless.html#ixzz1NEB9tln2

(14) Curso de Redes de datos, Facultad de Ingeniería, M.C. Quezada Reyes Cintia. AÑO 2007.

(15) Propuesta de Organización del CAD.

Introducción técnica a Windows Server 2008

(16) http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx#top [Citado el 15 de Marzo de 2013] Pág. → 65

INTRODUCCION A ACTIVE DIRECTORY

(17) http://foro.elhacker.net/tutoriales_documentacion/introduccion_a_active_directory-t40090.0.html#ixzz1XlQZzaI0 [Citado el 16 de agosto de 2012] Pág → 69

Planeación e implementación de directivas de grupo

(18) http://technet.microsoft.com/es-es/library/cc754948%28v=ws.10%29.aspx [Citado el 1 de Junio de 2012] Pág. → 72

http://technet.microsoft.com/es-es/library/cc781988%28v=ws.10%29.aspx [Citado el 21 de julio de 2012]

Introducción a la autenticación

(19) http://technet.microsoft.com/es-es/library/cc782219%28v=ws.10%29 [Citado el 08 de junio de 2012] → Pag. 74

What Is Kerberos Authentication?

(20) http://technet.microsoft.com/en-us/library/cc780469%28v=ws.10%29.aspx [26 de febrero de 2012] Pág. → 74

Windows Deployment Services Getting Started Guide

(21) http://technet.microsoft.com/en-us/library/cc771670%28WS.10%29.aspx#BKMK_InstallingWDS [Citado el 13 de marzo de 2012] Pág. → 76

Implementación de Directivas de Grupo:

WSUS:

(22) http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx [Citado el 14 de junio de 2012] Pág. → 78

Grupos Predeterminados en Active Directory

(23) http://technet.microsoft.com/es-mx/library/cc756898(v=ws.10) [Citado el 28 de agosto de 2012] → Pág. 91

Windows Server 2008 R2:
administración avanzada: books.google.com.mx/books?isbn=2746071940 [Citado el 20 de mayo de 2012]

Historia de Sistemas Operativos por Red

http://www.osmosislatina.com/diversos/mas_facil.htm [Citado el 15 de marzo de 2011] → Pág. 133

Windows NT y NetBIOS

http://usuarios.multimania.es/administracionredes/hacknt1.htm [Citado el 16 de mayo de 2011 Pág. → 133

ANEXOS

Este cuestionario se realizó a los administradores de red de dos instituciones que cuentan con un esquema centralizado de red a través de un dominio. Las Instituciones encuestadas fueron el Instituto de Ingeniería en la UNAM y el Colegio de México COLMEX. El objetivo principal fue conocer las características, ventajas y experiencias que se tienen de la utilización de este esquema para después diseñar una solución propia en base a las necesidades del CAD. Además permitó conocer herramientas y funcionalidades importantes que posteriormente se investigaron para adecuarlas a las necesidades identificadas en el Centro.

1. ¿Cuál es el objetivo principal de administrar su red utilizando un dominio?
   Las respuestas hablan de los mismos objetivos que son administrar los recursos de cómputo y la optimización de los servicios que se brindan en su red como: internet, inicio de sesión, autenticación, políticas, software, administración de archivos y llevar un mejor control de los usuarios.

   Por lo tanto, este proyecto seguirá los objetivos mencionados pero además se enfocará en brindar la seguridad adecuada mediante políticas de seguridad y de uso, mejorar la eficiencia en la utilización de los recursos de cómputo mediante un servicio que permita la disponibilidad de la información en cualquier computadora del dominio y una mejora en la obtención de datos para la generación de estadísticas.

2. ¿Cuánto tiempo lleva administrando su dominio?
   Las personas encuestadas tienen un tiempo considerable implementando o administrando un dominio, en la siguiente tabla se muestra el tiempo de experiencia de los administradores encuestados.

Organización	Experiencia
Torre de Ingeniería	8 años (IINGEN) 6 meses (Torre)
COLMEX	12 años

3. ¿Conoce algún otro tipo de estrategia de administración que satisfaga las necesidades como lo hace la administración en base a un dominio, y en caso de conocer otra alternativa, que tan utilizado es en México o en el extranjero?
   Para esta pregunta se habló sobre dos estrategias conocidas de administración distintas a las de un dominio. Una fue la de arquitecturas de nube de la cual se explicó que es una arquitectura que implica complicaciones en la administración, dificultades para adaptarse a esos sistemas, complejidad en la implementación y sobre todo que las funcionalidades de una arquitectura nube eran distintas a las requeridas para las necesidades de la red. La otra estrategia que nos comentaron está basada en sistemas Novell y Linux

En el caso de Novell las razones por las que se dejó de usar fueron las siguientes:

En los inicios de la implementación del dominio el conocimiento sobre las tecnologías de Novell no estaba tan generalizado.
Para poder adquirir el conocimiento se requería de capacitación lo cual significa un gasto adicional para las organizaciones.
Las tecnologías de Microsoft adquirían importancia y la gente comenzaba a familiarizarse con el sistema operativo Windows.
Respecto a Linux la razón principal que se dio fue que con este sistema operativo se necesita ir integrando varias tecnologías para conformar el dominio, todo ello de forma manual a diferencia de Windows que tiene todo integrado en Windows Server.
Los administradores entrevistados optaron por tener una red en dominio basada en servidores Microsoft, ya que de esta forma se obtiene una eficiente y fácil administración además de contar con funcionalidades adecuadas para la administración de usuarios y recursos de cómputo.

4. ¿Cuál es el tipo de topología que utiliza la red, y qué tanto influye el tipo de topología en la implementación y administración del dominio?
   Las topologías que se mencionaron fueron Híbrida y de bosque para el Active Directory en los tres casos, pero la implementación de un Dominio no depende de qué topología se tenga, depende más de los servicios y recursos que se vayan a administrar en la red.

5. ¿En cuánto a hardware, cómo está conformado su dominio, es decir, servidores, estaciones de trabajo, etc.?
   - Existen servidores dedicados para la comunicación que son servidores (DHCP y DNS),
   - Servidores controladores de dominio con Windows server 2003 o 2008
   - Estaciones de trabajo (PCs de escritorio, laptops)
   - Servidores de almacenamiento
   - Servidores de correo electrónico
   - Servidores web
   - Bases de datos
   - Recursos adicionales como impresoras, escáneres, multifuncionales

6. Antes de implementar el dominio, ¿cuál era la cantidad de máquinas inicial que se pensó podría soportar el mismo y cuál es la cantidad actual?
   En los dos casos no se obtuvo un número exacto de computadoras que se tenían contempladas para la implementación de un dominio, se explicó que esto depende más de la organización donde estará el dominio, su forma de administrar los recursos y el crecimiento que tendrá en un futuro.

Organización	Núm. Inicial de máquinas	Núm. Actual de máquinas	Tiempo de crecimiento
Torre de Ingeniería	20	1200	8 años
COLMEX	100	800	12 años

7. A partir de cuántos equipos considera conveniente implementar un dominio y ¿por qué?
   En los lugares donde se realizó la entrevista existe un número aproximado de entre 400 a 1000 computadoras por lo que si se compara el número de los equipos que hay en el CAD (Centro de Apoyo a la Docencia) es una diferencia amplia. Sin embargo, los entrevistados coincidieron en que más allá de la cantidad de equipos en una red, los factores a tomar en cuenta para la implementación del dominio dependen de las necesidades de cada organización y de las posibilidades de crecimiento de la misma.

8. ¿Cree usted que el número de equipos dentro del dominio influya para brindar más y mejores servicios?, ¿por qué?
   Definitivamente el número de equipos influye ya que la calidad está directamente relacionada con el modo de administrar los recursos.
   Sin embargo, en este caso los entrevistados explicaron que más que la cantidad de equipos lo que verdaderamente influye es el tipo y número de servicios que se vayan a brindar, los cuales dependen de la organización y sus objetivos. Por lo tanto, puede haber una organización que tenga pocas computadoras y que ofrezca los mismos servicios que otra organización con el doble o más de computadoras; todo va a depender de las necesidades que se tengan.

9. ¿Cuánto tiempo se invirtió en la implementación del dominio?
   Las respuestas coincidieron en que la parte técnica para la implementación es sencilla y por lo tanto no requiere de mucho tiempo, sin embargo, esto depende de la experiencia y de los conocimientos que se tengan sobre el funcionamiento tanto del sistema operativo, requisitos para instalarlo, servicios que se instalarán para el funcionamiento entre las tecnologías Microsoft. Por lo tanto, una actividad previa a la implementación es la definición de los servicios que se desean ofrecer, así como de los recursos de la red que serán administrados. Tener la información de los usuarios

   que van a ingresar al dominio, así como la estructura de árbol que quedará en el Directorio Activo. También se requiere diseñar las políticas que serán aplicadas para los usuarios o grupos. En la siguiente tabla se muestra el tiempo en el que los entrevistados recuerdan haber implementado sus ambientes de dominio.

Organización	Parte Técnica	Maduración
Torre de Ingeniería	1 semana y media	6 meses
COLMEX	2 semanas a 1 mes	3 meses

   Nota: El tiempo de maduración se refiere al tiempo requerido para considerar que todos los equipos están totalmente integrados al dominio además de los servicios y las políticas necesarias para considerar que el dominio es funcional y operativo.

10. ¿Qué problemas encontró en el proceso de implementación del dominio?, y ¿Cómo se solucionaron?
    Los encuestados respondieron que debido a la facilidad técnica de implementación, no existieron problemas que representaran una gran complejidad, pero uno de ellos mencionó que la parte del licenciamiento es algo que se debe considerar, pues para algunas organizaciones el gasto que se debe hacer puede estar fuera de sus prioridades.
    Por lo tanto, es importante tener claro el tipo de licenciamiento del sistema operativo, así como conocer las herramientas integradas como el Directorio Activo, el servicio de DNS y si se requiere de programas adicionales que impliquen otro tipo de licenciamiento. También hay que conocer las características del hardware en donde se instalará el sistema operativo para asegurar que funcionará para brindar los servicios a los usuarios que se estén contemplando.

11. ¿Qué sistemas operativos se utilizan para la administración del dominio?
    En los tres casos utilizan tecnologías de Microsoft las cuales han ido evolucionando desde Windows NT4 hasta Windows Server 2008 y ha resultado favorable para la administración de los recursos en los lugares donde se aplicó la encuesta.

12. ¿Qué factores influyeron para la elección de Windows (Active Directory) y descartar otros sistemas operativos como Linux?
    Las respuestas muestran que el principal factor que influyó fue que al inicio de la implementación del dominio los usuarios estaban más familiarizados con las tecnologías de Microsoft; asimismo, la naturaleza de los equipos y el escaso conocimiento de otras tecnologías en aquel tiempo hacían difícil la utilización de otros sistemas operativos como Linux o Novell.

    Hoy en día hay mucha información sobre los diferentes tipos de tecnologías disponibles, sin embargo, la decisión del sistema operativo debe basarse en las necesidades del lugar donde se implementará el dominio.

13. ¿Cuáles son las ventajas y desventajas de la administración con Windows Server?
    Las respuestas hablan de que existen más ventajas que desventajas ya que al administrar con Windows Server se tiene el respaldo de soporte, documentación, la facilidad de configuración de servicios y de su implantación, además de la facilidad de escalabilidad que permite.
    Las desventajas mencionadas tienen que ver con la vulnerabilidad ante virus informáticos, sin embargo se explicó que esto no sucede sólo con este sistema operativo sino que todos son vulnerables en mayor o menor medida.

14. ¿Cómo es la relación costo-beneficio con el uso de Windows Server, es decir, los resultados obtenidos justifican el costo que implica el uso de este sistema operativo, en cuestiones de eficiencia, eficacia, dinero, etc.?
    El costo-beneficio en los dos casos se justifica, pues se tiene soporte, garantía, actualizaciones, aseguramiento de software sin ningún costo extra.

15. ¿Cómo es el modo de licenciamiento que manejan para la distribución del software?
    Las respuestas indican que cuando la red es grande en cuestión de número de equipos o cuando hay expectativas altas en cuanto a la extensión de la red, el licenciamiento por volumen es el más conveniente económicamente hablando. Además de que con Microsoft se tienen ventajas como el soporte y el aseguramiento del software comprado que significa poder adquirir actualizaciones o nuevas versiones sin costo en un determinado tiempo.

    NOTA: Hábitat Puma Es un sitio creado especialmente para alumnos y profesores de la UNAM, con la finalidad de que incrementen sus conocimientos y habilidades en el uso de TIC (Tecnologías de la Información y la Comunicación), y aprovecharlos en su desarrollo académico y profesional. Como parte de Hábitat Puma la UNAM y Microsoft tienen un convenio en donde la UNAM se afilia al programa MSDN AA (Microsoft Developer Network Academic Alliance). Este programa les da a los académicos, investigadores y alumnos de la UNAM, la posibilidad de descargar de manera GRATUITA, algunos productos de Microsoft, esto para fines de aprendizaje, investigación y desarrollo en la Universidad.

16. ¿Cuáles son los servicios más utilizados en su dominio y a qué tipo de usuarios van dirigidos?
    En las respuestas a esta pregunta se nota que los servicios más utilizados son prácticamente los mismos en las dos organizaciones (internet, inicio de sesión, autenticación, políticas, software, administración de archivos) y además que son independientes del tipo de usuarios. Por ello, se debe poner especial atención a estos servicios puesto que son objetivos importantes que coinciden con los planteados para el CAD.

Organización	Tipos de Usuarios
Torre de Ingeniería	Académicos, Estudiantes y Administrativos.
COLMEX	Académicos, Estudiantes y Administrativos.

17. De los servicios que brindan, cuáles son los que hacen mayor uso de los recursos de la red. (ancho de banda, procesamiento, tiempo y espacio de almacenamiento etc.)
    Para esta pregunta las respuestas coincidieron en que el servicio de internet es el que más recursos de la red utiliza. Para el caso del Centro, considerando que al ser pocos los equipos de cómputo y que no siempre son utilizados al mismo tiempo el servicio de internet no impactará tanto en la utilización de los recursos; sin embargo, el hecho de que las personas encuestadas hayan coincidido, hace que sea un factor que se deba considerar en el análisis y diseño del dominio. Además, las respuestas dejan ver nuevamente que los servicios que se brinden, siempre dependerán de los requerimientos de los usuarios; por ello, hay que estar conscientes de qué servicios se requieren para esta red y su impacto en los recursos.

18. ¿Cuáles son los problemas más frecuentes que se han presentado al administrar su dominio y cómo los solucionó?
    Los problemas siempre van a existir, no obstante la manera de solucionarlos es lo importante. Las respuestas a esta pregunta fueron muy variadas; en el caso del COLMEX no han tenido problemas o al menos no han sido de consideración, en la Torre de Ingeniería los problemas han sido intrascendentes solucionándose mediante configuraciones del dominio.

En las siguientes tablas se muestran los problemas recurrentes que han tenido las instituciones encuestadas así como el impacto y la solución utilizada.

TORRE DE INGENIERÍA		
Problema	Impacto	Solución
Documentación de las soluciones	Retraso en tiempo y algunas veces costo adicional.	Búsqueda de información con el fabricante, soporte técnico por parte del fabricante.
Integrar soluciones de terceros	Retraso en tiempo	Sacar la solución del dominio y administrarla independientemente.

COLMEX
Problema
En el colmex no han tenido problemas de consideración que impacten en las operaciones del Colegio.

19. ¿Qué tipo de políticas de seguridad implementó en su dominio y en base a qué están diseñadas (tipos de usuarios, tipos de servicios, uso de recursos, etc.)?
    En el Instituto de Ingeniería las políticas están dirigidas a máquinas, usuarios y servicios. Hay políticas de acceso, servicios (qué se permite hacer y qué no) y uso (de los equipos de cómputo, administración de servicios). En COLMEX, también cuentan con políticas como los antivirus, parches de Microsoft, políticas para las aplicaciones y servicios, por ejemplo, cuáles usuarios pueden hacer uso de las impresoras, quién se va a conectar a alguna página, quién la va a administrar, etc. Estas políticas se explican en la siguiente tabla.

Organización	Política	Objetivo
Torre de Ingeniería	Usuarios	Control de Acceso, Manejo de Información, Administración.
	Equipos de Cómputo	Control de Acceso, Mantenimiento, Administración.
	Servicios	Control de acceso de los usuarios, administración.
	Software	Licenciamiento, control de versiones.
COLMEX	Antivirus Parches Últimas versiones	Resguardar la seguridad y mantener a la vanguardia la tecnología.
	Control	Control de acceso de los usuarios a las sesiones y a su información.

20. ¿Utilizan algún servicio, aplicación o programa que les permita la administración de software por red? ¿Cómo cuáles?
    Este servicio sólo es utilizado en el Torre de Ingeniería, pero para la solución pensada en el Centro, forma parte de los objetivos planteados. Es un servicio que depende mucho del rol de las organizaciones y por ende del tipo de usuarios. En el CAD se piensa que facilitará en gran medida las tareas del administrador de la red y disminuirá los problemas de compatibilidad del software mediante actualizaciones automáticas del mismo. En la siguientes tablas se muestran las principales herramientas utilizadas en las Instituciones encuestadas.

TORRE DE INGENIERÍA	
Herramienta	Objetivo
WSUS	Automatizar y distribuir actualizaciones de software vía red.
Windows Deployment Services	Distribuir Sistemas Operativos vía red.
System Center Configuration	Administración de servicios internos y web.

COLMEX	
Herramienta	Objetivo
WSUS	Automatizar y distribuir actualizaciones de software vía red.
Windows Deployment Services	Distribuir Sistemas Operativos vía red.
System Center Configuration	Administración de servicios internos y web.
Windows PowerShell	Administrar los equipos de la empresa desde la línea de comandos

21. En base en su experiencia, ¿qué cambios o mejoras visualiza en la administración en base a un dominio y por qué?
    Los cambios o mejoras se enfocan en los usuarios y recursos pero como una optimización de lo que ya existe, es decir, al parecer los entrevistados están a gusto con las herramientas y soluciones existentes en este momento y no consideran grandes innovaciones para el futuro. Los cambios que visualizan son evoluciones de lo que ya hay o mejoras para administrar los recursos. Esto brinda certeza de que la solución considerada para el Centro, cumplirá con las expectativas de mejoramiento de la administración de los recursos y usuarios.

En este anexo se profundizan varios conceptos vistos en este proyecto desde un punto mayormente técnico y se añade información que no necesariamente se necesitó para la implementación, pero que resulta importante de conocer, sobre todo si se piensan extender las funcionalidades del dominio en el Centro en un futuro.

1.1 REDES EN WINDOWS.

El primer tipo de implementación utilizada en un sistema de Red sencillo fue denominado "workgroup" o grupo de trabajo. Un grupo de trabajo es un grupo de computadoras que comparten información y recursos como impresoras, escaners y otros dispositivos pero que no requieren de un servidor central. La falta de un servidor central en este tipo de implementación hace que la arquitectura de la red sea sencilla. Sin embargo, el uso de una red con la implementación de grupo de trabajo genera un descontrol en la administración y además produce un uso excesivo de ella.

“En los años 80’s la empresa IBM desarrolló el Protocolo de Red denominado NetBIOS (Network Basic Input/Output System) el cual proporciona a los programas un conjunto de comandos necesarios para administrar nombres, entablar sesiones y enviar información entre los equipos de la red. En otras palabras, NetBIOS se creó con el fin de suministrar a los programas de una interfaz que pudiera acceder a los recursos de otras máquinas en redes locales. Esto permitía distribuir la carga del uso excesivo de la red generada por la implementación en grupo de trabajo.

Posteriormente surgió la alianza entre Microsoft e IBM y se creó el sucesor de NetBIOS, NetBEUI (NetBIOS Extended User Interface). NetBEUI comenzó a ser integrado en plataformas con equipos Windows 3.1 bajo el nombre de "Windows for Workgroups" y posteriormente en Windows 95 y 98. NetBEUI permitía dividir el sistema en varios grupos de trabajo y tener un servidor central, sin embargo, debido a la sencillez en el diseño de NetBEUI este protocolo no podía ser ruteado, es decir, no establecía rutas de comunicación entre los equipos, ya que para ubicar a los equipos en la red, NetBEUI utiliza nombres de equipo en vez de utilizar direcciones lógicas como las direcciones IP en TCP/IP.”

1.2 SURGIMIENTO DE WINDOWS NT

Con la alianza de Microsoft e IBM para desarrollar NetBEUI surgió la propuesta de crear un sistema operativo de servidor, este fue OS/2 desarrollado por IBM, sin embargo, Microsoft abandonó el proyecto en sus inicios y empezó el trabajo sobre su propio sistema operativo para servidores: Windows NT (Windows "Nueva Tecnología"). Windows NT realiza el seguimiento de archivos con el sistema de archivos NTFS (NT File System), sistema que es el núcleo de los niveles de control de acceso a la información del servidor y responsable de la estructura de seguridad en NT. Pero Windows NT presentaba algunas desventajas en su administración, por ejemplo, no se podía limitar la capacidad del disco duro por usuario, además de tener limitaciones de memoria que provocaban una reducción en el número de archivos abiertos y en el almacenamiento en el disco duro.

1.3 WINDOWS 2000 SERVER

En la sucesión de Sistemas Operativos para Red desarrollados por Microsoft siguió Windows 2000 Server; entre las principales diferencias que posee este sistema operativo comparado con Windows NT son: el uso de un sistema de encriptación de archivos; una mejor administración en cuanto al

almacenamiento en disco; y, como punto importante, estos sistemas operativos incluyeron los servicios de Directorio Activo (Active Directory) los cuáles se detallarán más adelante.

Con Windows 2000 se introdujo también la Consola de Administración de Microsoft (MMC Microsoft Management Console) que permite crear, guardar y abrir herramientas administrativas además de permitir la administración central de estas herramientas en otras máquinas. Con Windows 2000 Server se integró la autenticación de red utilizando Kerberos (ver tema 2.4.2.2), de manera que se mejoraron las relaciones de confianza entre los equipos y por lo tanto aspectos de seguridad. Una relación de confianza es un vínculo que se establece entre dos dominios o en un solo dominio entre los equipos cliente y el o los servidores para poder compartir información y recursos.

1.4 WINDOWS SERVER 2003

Posteriormente, en 2003 surgió el sistema operativo Windows Server 2003 basado en la familia de Windows 2000 Server, integrando un entorno de aplicación para desarrollo de servicios Web. Este sistema operativo mejoró la eficiencia de varias de las aplicaciones de Windows 2000 Server como el Directorio Activo, en donde ahora había varias mejoras orientadas a facilitar su uso y la presencia de otras funcionalidades, como las relaciones de confianza entre servidores y la capacidad de renombrar dominios. Una funcionalidad de este sistema operativo fue la inclusión de la consola de administración de Políticas de Grupo, que permite a los administradores poder usar precisamente las Políticas de Grupo para definir las configuraciones y acciones permitidas para los usuarios y equipos.

La administración basada en Políticas, simplifica tareas tales como la actualización del sistema, perfiles de usuario y protección del sistema de equipos de escritorio. En Windows Server 2003 se integró el servidor web IIS (Servicios de Información de Internet o Internet Information Services) 6.0 con la finalidad de facilitar el uso de aplicaciones y servicios Web. Se integró también el modelo de programación de tecnologías y software Microsoft .NET Framework para desarrollar, implementar y ejecutar aplicaciones Web.

En la siguiente tabla se muestran las características de las distintas versiones de Windows Server 2008.

EDICIÓN	DESCRIPCIÓN
Windows Server 2008 Standard	Incorpora capacidades mejoradas de Web y virtualización en ediciones de 64 bits. Está diseñado para aumentar la fiabilidad y flexibilidad de la infraestructura de red, reduciendo costos y tiempo de mantenimiento. Además con esta versión se mejoran las características de seguridad que trabajan para fortalecer el sistema operativo ayudando a proteger los datos y la red.

EDICIÓN	DESCRIPCIÓN
Windows Server 2008 Enterprise	Esta versión está diseñada para ambientes empresariales con aplicaciones críticas de negocio. Tiene las mismas funcionalidades que la versión Standard pero con esta versión se mejora el rendimiento del sistema mediante funcionalidades como el clúster.
Windows Server 2008 Datacenter	Esta versión está diseñada para ambientes empresariales con aplicaciones críticas de negocio y virtualización a gran escala para reducir costos de infraestructura mediante la consolidación de aplicaciones con derechos de licenciamiento de virtualización.
Windows Web Server 2008	Esta edición está diseñada para ser usada exclusivamente como servidor Web. Esta versión es una plataforma sólida de funcionalidades web como IIS 7.0, ASP.NET y .NET Framework.

Versiones Windows Server 2008

2.1 ESTRUCTURA LÓGICA DEL DIRECTORIO ACTIVO

La estructura lógica está centrada en la administración de usuarios y recursos de la organización incluyendo los siguientes componentes:

Objetos: son representaciones de los usuarios y recursos de red, tales como impresoras, computadoras, teléfonos de red, etc.

Clases de objetos: son plantillas o modelos para los tipos de objetos que se pueden crear, cada clase de objeto es definida por un conjunto de atributos, los cuales definen los valores posibles que se pueden asociar a un objeto.

Unidades Organizativas (OU): son contenedores de objetos o de otras unidades organizativas, con el propósito de facilitar su localización y administración en el Directorio Activo. Se utilizan para:

- Organizar objetos en un dominio. Las unidades organizacionales agrupan objetos como grupos, cuentas de usuario y de equipo, además de archivos e impresoras compartidas.

- Delegar el control administrativo. Se pueden asignar permisos específicos a uno o más usuarios y grupos en una unidad organizacional y a los objetos que esta unidad contenga.

Dominio: es la parte fundamental del Directorio que permite agrupar de forma estructurada y jerárquica los objetos administrativos OU, las políticas de seguridad y otros objetos

2.2 ESTRUCTURA FÍSICA DEL DIRECTORIO ACTIVO.

Su objetivo principal es optimizar el tráfico de la red, determinando cómo y cuándo ocurre la replicación y el tráfico de inicio de sesión entre dominios. La replicación se refiere a la aplicación de los cambios sobre los controladores de dominio. Incluye los siguientes componentes:

- Controladores de dominio: realizan las funciones de almacenamiento y replicación, cada controlador de dominio soporta sólo un dominio.
- Sitios: es la representación lógica de como se encuentran distribuidos los equipos físicamente. Cuando se establece un sitio, los Controladores de Dominio dentro de él pueden comunicarse con frecuencia. Se crean sitios para optimizar el uso de ancho de banda y el tráfico de red entre los distintos controladores de dominio.

El directorio activo utiliza una estructura de árbol y bosques que permiten la escalabilidad de la red fácilmente. Los árboles son estructuras jerárquicas de dominios y subdominios con relaciones de confianza entre sí que comparten recursos, clientes y un sistema de resolución de nombres (DNS). Un bosque es un conjunto de árboles de dominio con relaciones de confianza entre sí. Para este proyecto, el concepto de bosque no se usará, pero si la red crece en un futuro, este concepto tomará una importancia considerable.

3.1 FUNCIONAMIENTO.

Las configuraciones se definen dentro de un GPO en el Directorio Activo y son replicadas en los equipos clientes o a los usuarios en distintos momentos dependiendo del tipo de directiva de grupo

que se trate y cómo se hayan configurado. La replicación puede ser cuando la computadora encienda o cuando el usuario inicia sesión, además es posible configurar que las directivas se apliquen en intervalos programados o inmediatamente.

Existen dos contenedores principales para un GPO:

- Configuración de Equipo (Computer Configuration)
- Configuración de Usuario (User Configuration)

Las configuraciones dentro del contenedor Configuración de Equipo se aplican cuando el equipo es encendido. Cuando una computadora inicia, descarga los GPOs que corresponden a la Unidad Organizativa. Después, la computadora procesará únicamente las opciones configuradas en Configuración de Equipo e ignorará las configuraciones establecidas en el otro contenedor.

A su vez, las opciones dentro de Configuración de Usuario sólo se aplican cuando el usuario inicia sesión, la computadora consulta al directorio activo para saber en qué Unidad Organizativa reside la

cuenta de usuario y descarga los GPOs que le aplican para después procesarlos. La computadora sólo procesará las opciones establecidas en Configuración de Usuario e ignorará las del otro contenedor. Normalmente, este tipo de configuraciones son removidas cuando el usuario cierra sesión, así que no permanecen en el equipo. Esto significa que el siguiente usuario que inicie sesión en la computadora tendrá distintas configuraciones y/o sobrescribirá las que sean similares.

Las configuraciones utilizadas en este proyecto, que se hicieron a través de GPO's, son algunas establecidas en el contenedor de Configuración de equipo y otras en el de usuario. Esto depende de la configuración que se trate y de la manera en que se requiere aplicar. Las GPO'S utilizadas así como su configuración se describen en el capítulo de Implementación.

3.2 VÍNCULOS.

Un GPO es creado en el Servicio de Directorio Activo, pero es necesario que sea enlazado a alguna Unidad Organizativa (OU) o a todo un sitio o dominio, de lo contrario no tendrá ningún efecto en los equipos de la red. Este enlace es conocido como el vínculo del GPO.

Las directivas o políticas de grupo pueden ser vinculadas a:

- Sitios.
- Dominios.
- Unidades organizativas (OUs) y
- De forma local para un equipo.

Un solo GPO puede ser creado y vinculado a varias OUs. Al editar este GPO, todas las OUs a las cuáles está vinculado, recibirán las configuraciones en la siguiente actualización.

3.3 ORDEN DE PRECEDENCIA DE LAS POLÍTICAS DE GRUPO.

Varios GPOs pueden ser aplicados a distintos niveles del árbol del Directorio Activo (Sitio, Dominio, Unidad Organizativa o Localmente) a un equipo o usuario. Podría darse el caso de que las configuraciones entren en conflicto, por lo tanto, el orden de cómo son aplicados los GPOs es importante.

Los GPOs son aplicados de manera predeterminada en el orden siguiente:

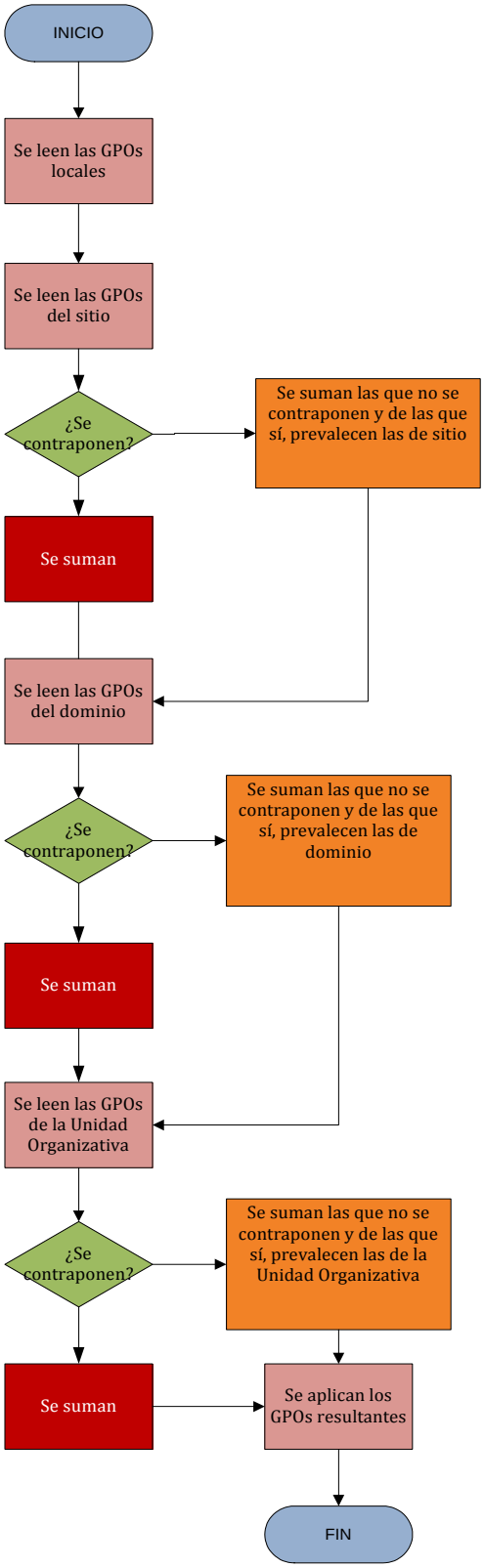
1.- GPO Local (configuración en el equipo, no en Active Directory).

2.- GPO del sitio.

3.- GPO del dominio.

4.- GPO de Unidades Organizativas.

Las configuraciones aplicadas al último, sobrescriben a las configuraciones aplicadas inicialmente cuando existen conflictos. Esto significa que cuando una configuración en un GPO a nivel del sitio, por ejemplo, entra en conflicto con una configuración en un GPO a nivel de dominio o Unidad Organizativa, la configuración que prevalece es la que se aplica al último. Cuando las configuraciones no se contraponen entonces simplemente se van sumando (figura 3.1).


INICIO
Se leen las GPOs locales
Se leen las GPOs del sitio
¿Se contraponen?
Se suman las que no se contraponen y de las que sí, prevalecen las de sitio
Se suman
Se leen las GPOs del dominio
¿Se contraponen?
Se suman las que no se contraponen y de las que sí, prevalecen las de dominio
Se suman
Se leen las GPOs de la Unidad Organizativa
¿Se contraponen?
Se suman las que no se contraponen y de las que sí, prevalecen las de la Unidad Organizativa
Se suman
Se aplican los GPOs resultantes
FIN

3.4 PLANEACIÓN DE LA SEGURIDAD Y ADMINISTRACIÓN MEDIANTE DIRECTIVAS DE GRUPO.

Después de que se han detallado las características y el funcionamiento de las Directivas de Grupo en general, es importante resaltar la trascendencia de lograr representar conceptualmente al CAD en Unidades Organizativas, ya que esto ayudará para las labores de administración y hará más sencilla la implementación de las Directivas de Grupo. Las GPOs, dependiendo de la configuración que involucren, se vinculan a una o varias OUs que después aplicarán la configuración del GPO a los usuarios y equipos dentro de esa OU. Por ende, el correcto diseño de las OUs es importante porque permitirá la implementación de las directivas de grupo a los equipos cliente y usuarios del CAD de acuerdo a lo planeado. El diseño de OUs debe tener una estructura adecuada para aplicar también las configuraciones de seguridad a tipos específicos de usuarios en el CAD. Hay que considerar que existen tipos de usuarios como desarrolladores o diseñadores que necesitan privilegios distintos o ciertas aplicaciones específicas en los equipos. Como se mencionó antes, en el siguiente capítulo se detalla la estructura del directorio activo y por lo tanto las Unidades Organizativas empleadas, así como las políticas de grupo utilizadas y su distribución dentro de la estructura jerárquica del Directorio Activo.

Otra característica importante del sistema operativo Windows Server 2008, es el modo en que realiza el procedimiento de autenticación a través de mecanismos orientados a proveer este servicio de seguridad de manera correcta. Para entender cómo se lleva a cabo este procedimiento en los ambientes Windows, a continuación se explican distintos conceptos importantes.

3.5 PROCESAMIENTO DE DISTINTOS GPOS EN UN MISMO CONTENEDOR.

Múltiples GPOs pueden ser aplicados a un mismo contenedor (Unidad Organizativa), en este caso los GPOs son aplicados en orden creciente de acuerdo a la prioridad, es decir que primero se aplican los GPOs de prioridad más baja. Esto resuelve los conflictos entre configuraciones que se contrapongan puesto que prevalecerán las configuraciones de los GPOs con mayor prioridad. La prioridad es dada automáticamente dependiendo del tipo de configuración que sea.

Lo anterior no significa que los GPOs con prioridad mayor anulen a los de menor prioridad sino que, como sucede con las GPOs que se aplican en el árbol del Directorio Activo, las configuraciones que no se contraponen se van sumando.

Existe un tipo de procesamiento distinto llamado Loopback que puede ser utilizado en situaciones especiales dependiendo de las necesidades que se quieran cubrir con las configuraciones (para ver cómo funciona este procesamiento ver Anexo de Tecnologías).

Existe también el concepto de herencia en las políticas de grupo para poder replicar configuraciones o reutilizarlas. Sin embargo, en este proyecto no se utilizó dicho concepto, aunque este se describe en el Anexo de Tecnologías por si fuera necesario utilizarlo en algún futuro dentro de las configuraciones.

3.6 INTERVALO DE ACTUALIZACIÓN DE LAS DIRECTIVAS DE GRUPO.

Como se mencionó, la actualización de las políticas generalmente se aplica durante el inicio de la computadora o el inicio de sesión (Ver Aplicación Síncrona y asíncrona de las directivas de grupo en Anexo de Tecnologías). Sin embargo, las políticas también se actualizan durante intervalos regulares. Por omisión, los GPOs son actualizados de manera automática cada 90 minutos con un desplazamiento aleatorio de hasta 30 minutos, a excepción de los controladores de dominio cuyo intervalo es de 5 minutos[4]. Estos intervalos pueden ser configurados pero no se recomienda disminuir el tiempo ya que se podría incrementar el tráfico de datos en la red provocando un aumento en la carga de los controladores de dominio.

Si se requiere, puede aplicarse la actualización en un equipo cliente sin tener que esperar el intervalo de tiempo para que se haga la actualización automática. Para hacerlo, desde el equipo cliente se ejecuta el comando “gpupdate /force” que forzará la actualización de las directivas de grupo en el momento. Algunas configuraciones como la redirección de directorios y la asignación de aplicaciones de software requieren que se reinicie el equipo o la sesión del usuario.

3.7 FILTRADO DE SEGURIDAD EN LOS GPOS.

Como se ha visto, los GPOs se pueden vincular a sitios, dominios o a unidades organizativas, pero no se pueden vincular directamente a un equipo, a un usuario o a un grupo de usuarios; para poder hacerlo, existe el filtrado de seguridad. Este filtrado permite aplicar las configuraciones de directiva de grupo a un cierto equipo, usuario o grupo de usuarios dentro del lugar (sitio, dominio u OU) donde el GPO esté vinculado.

De manera predeterminada, los GPOs se vinculan a un grupo definido por el directorio activo llamado Usuarios Autenticados, en el cual están registrados todos los usuarios que han iniciado sesión en el dominio alguna vez, de tal forma que todos los usuarios autenticados en el dominio reciben la configuración de un nuevo GPO al aplicarse a una unidad organizativa, un dominio o un sitio. Sin embargo, los vínculos pueden cambiarse para controlar a quiénes se desea que se apliquen las configuraciones dentro de la unidad organizativa, el dominio o el sitio.

3.8 OPCIONES DE SEGURIDAD EN LAS DIRECTIVAS DE GRUPO.

Las directivas de grupo aportan importantes soluciones en aspectos de seguridad, tanto, que son consideradas un buen mecanismo de seguridad. Esto se debe, principalmente, a que a través de directivas de grupo es posible establecer configuraciones referentes a las contraseñas y directivas de cuentas.

Las directivas de cuentas son importantes ya que mejoran o agregan características que permiten controlar de la seguridad de las cuentas, como por ejemplo, establecer un número de intentos máximo para acceder a la cuenta y bloquearla después de ciertos intentos fallidos de inicio de sesión.

Las directivas de contraseña permiten configurar aspectos tan importantes como establecer períodos de caducidad de las contraseñas, establecer características propias de las mismas, como la longitud,

los tipos de caracteres permitidos, y también es posible establecer un historial de contraseñas que evite que los usuarios vuelvan a utilizar la misma en un corto período de tiempo, etc.

Además, el directorio activo permite definir distintos derechos a los usuarios dependiendo de los permisos de configuración que se desea que tengan. Para ello, el directorio activo tiene definidos distintos tipos de grupos de seguridad predeterminados, se detallan algunos de los grupos más importantes a continuación.

Grupo	Descripción	Derechos de usuario predeterminados
Operadores de cuentas	Los miembros de este grupo pueden crear, modificar y eliminar cuentas de usuarios, grupos y equipos que se encuentran en los contenedores Usuarios o Equipos y en las unidades organizativas del dominio, excepto la unidad organizativa Controladores de dominio. Los miembros de este grupo no tienen permiso para modificar los grupos Administradores o Administradores del dominio ni las cuentas de los miembros de dichos grupos. Los miembros de este grupo pueden iniciar la sesión de forma local en los controladores del dominio y apagarlos.	Permitir el inicio de sesión local; Apagar el sistema.
Administradores	Los miembros de este grupo gestionan por completo todos los controladores del dominio. De forma predeterminada, los grupos Administradores del dominio y Administradores de organización son miembros del grupo Administradores. La cuenta Administrador es miembro de este grupo de forma predeterminada.	Ajustar las cuotas de memoria de un proceso; hacer copia de seguridad de archivos y directorios; habilitar la confianza para la delegación de las cuentas de usuario y de equipo; forzar el apagado desde un sistema remoto; cargar y descargar controladores de dispositivo; permitir el inicio de sesión local; restaurar archivos y directorios; apagar el sistema.

Grupo	Descripción	Derechos de usuario predeterminados
Invitados	De forma predeterminada, el grupo Invitados del dominio es un miembro de este grupo. La cuenta Invitado (que está deshabilitada de forma predeterminada) también es un miembro predeterminado de este grupo.	No hay derechos de usuario predeterminados.
Operadores de configuración de red	Los miembros de este grupo pueden modificar la configuración TCP/IP, así como renovar y liberar las direcciones TCP/IP en los controladores del dominio. Este grupo no tiene ningún miembro predeterminado.	No hay derechos de usuario predeterminados.
Operadores de impresión	Los miembros de este grupo pueden administrar, crear, compartir y eliminar impresoras que están conectadas a los controladores del dominio.	Permitir el inicio de sesión local; Apagar el sistema.
Usuarios de escritorio remoto	Los miembros de este grupo pueden iniciar la sesión en los controladores del dominio de forma remota. Este grupo no tiene ningún miembro predeterminado.	No hay derechos de usuario predeterminados.
Operadores de servidores	En los controladores de dominio, los miembros de este grupo pueden iniciar sesiones interactivas, crear y eliminar recursos compartidos, iniciar y detener varios servicios, hacer copias de seguridad y restaurar archivos.	Hacer copia de seguridad de archivos y directorios; Cambiar la hora del sistema; Forzar el apagado desde un sistema remoto; Restaurar archivos y directorios; Apagar el sistema.

Grupos de Seguridad Predeterminados

3.9 PROCESAMIENTO LOOPBACK DE LAS GPO.

Algunas veces se desea aplicar ciertas configuraciones a los equipos independientemente del usuario que inicie sesión en ellas. Es probable que estas configuraciones estén disponibles en el contenedor de Configuración de Usuario, sin embargo, como se vio anteriormente, cuando una computadora procesa sus propios GPOs normalmente ignora las opciones de este contenedor. Para solucionar esto, se utiliza el procesamiento loopback que altera la forma de procesamiento en las configuraciones del contenedor Configuración de Usuario. Con el procesamiento loopback se logra que un equipo aplique las configuraciones establecidas en el contenedor Configuración de usuario de su GPO a cualquier usuario que inicie sesión en él, es decir, que ya no ignoraría las configuraciones en este contenedor como sucede normalmente. El procesamiento Loopback tiene dos opciones:

Modo	Funcionamiento
Sustituir	Reemplaza las configuraciones normales del usuario con las especificadas en las configuraciones de usuario de los GPOs del equipo.
Combinar	Combina las configuraciones de usuario de los GPOs del equipo con las configuraciones normales del equipo. Si las configuraciones entran en conflicto, prevalecerán las configuraciones de los GPOs del equipo.

Tipos de procesamiento Loopback

3.10 HERENCIA DE GPOS.

Los GPOs se heredan a las ramas inferiores del árbol de Active Directory de forma predeterminada, estas políticas se van acumulando y se heredan las GPOs de la rama superior, así, en una Unidad Organizativa de nivel 2, es decir una Unidad Organizativa dentro de otra Unidad Organizativa, se tendría la acumulación de todas las políticas superiores, en otras palabras, las GPOs locales, del

sitio, del dominio y de la Unidad Organizativa superior. Sin embargo, esta herencia se puede bloquear.

3.10.1 BLOQUEAR LA HERENCIA DE GPOS.

Se puede prevenir que los usuarios y equipos hereden GPOs de niveles más altos bloqueando la herencia, esto puede hacerse por razones de políticas o para disminuir la complejidad de la infraestructura de GPOs. De esta forma, si se bloquea la herencia en el nivel de dominio, entonces las políticas de este nivel no se aplicarán en ninguna de las Unidades Organizativas, ni en las superiores ni en las inferiores, lo que significa que el bloqueo de herencia no es selectivo, es decir, que si se aplica el bloqueo se hará para todas las GPOs de ese nivel. También es importante mencionar que existen configuraciones importantes de seguridad que se aplicarán aún si la herencia es bloqueada, estas configuraciones son las directivas de Kerberos, las directivas de contraseñas y directivas de bloqueo de cuenta. Además, las políticas aplicadas a nivel local, de manera predeterminada, no pueden bloquearse.

3.11 APLICACIÓN SÍNCRONA Y ASÍNCRONA DE LAS DIRECTIVAS DE GRUPO.

El procesamiento sincrónico de GPOs consiste en procesar todos los GPOs del equipo durante el inicio del mismo, por lo que no se podrá iniciar sesión hasta que el procesamiento haya sido completado. Este tipo de procesamiento es el que está configurado de manera predeterminada. Sin embargo, este procesamiento puede ser cambiado a un procesamiento de tipo asincrónico, de tal forma que al encender el equipo se pueda iniciar sesión aunque no todos los GPOs hayan sido procesados, siguiendo con el procesamiento de los faltantes en segundo plano. Aunque, desde el punto de vista de seguridad, es mejor dejar el procesamiento predeterminado para evitar que posibles configuraciones críticas se aplacen afectando el objetivo de las mismas.

AUTENTICACIÓN

Los elementos en un directorio de LDAP deben estar identificados de forma única por un **distinguished name (DN) (Nombre distintivo)**. El DN es el nombre que identifica de forma única un objeto en el directorio. Un DN se compone de pares atributo=valor, separados por comas, por ejemplo:

CN: Fabiola Herrera Zepeda, **OU**: Italiano, **DC**: cad, **DC**: cele, **DC**: unam, **DC**: mx

El DN contiene un componente para cada nivel de la jerarquía de objetos del directorio activo, desde la raíz hasta el nivel donde se encuentra el objeto; considerando el ejemplo anterior, este constaría de los siguientes componentes:

En primer lugar, el componente DC (Controlador de Dominio) que define el nombre del DNS en la red, es decir, **DC**: cad, **DC**: cele, **DC**: unam, **DC**: mx

En segundo lugar, el componente OU que identifica a la Unidad Organizativa que almacena el objeto, OU: Italiano.

Finalmente el componente CN (Nombre Común) que identifica al objeto dentro del directorio activo, CN: Fabiola Herrera Zepeda.

Estos componentes son registrados en el Directorio cuando se agrega un objeto, por ejemplo un usuario, a través de la consola del Directorio Activo.

Existe también un relative distinguished name (nombre distintivo relativo) de un objeto, el cual es, básicamente un nombre distintivo (DN) truncado, que define el lugar del objeto con un grupo contenedor. Por ejemplo:

OU: Italiano, **DC**: cad, **DC**: cele, **DC**: unam, **DC**: mx

Durante el proceso de autenticación el DN permite validar la existencia de un objeto dentro del Directorio del dominio. Este procedimiento es realizado conjuntamente con el protocolo de Kerberos

KERBEROS.

En este protocolo hay tres partes involucradas. (Figura 1):

- Cliente
- KDC (Centro de Distribución de Tickets)
- Servidor que provee el servicio, Servidor de archivos, por ejemplo.

El KDC es instalado como parte del controlador de dominio y se divide a su vez en dos partes:

- Servidor de Autenticación (AS)
- Servidor de Tickets de Concesión (TGS). Brinda tickets para todos los servicios.

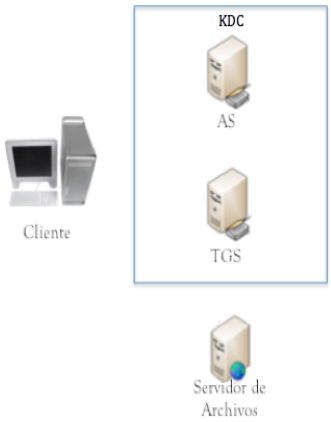


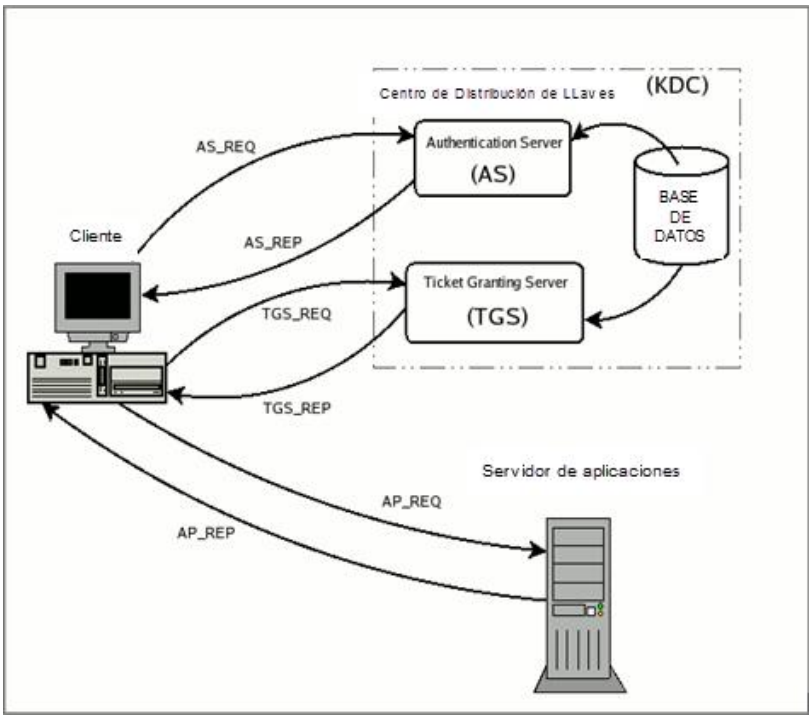
FIGURA 1. Componentes de Kerberos.

5.1 FUNCIONAMIENTO.

Para entender de mejor manera el funcionamiento de las partes involucradas en este protocolo se describe el procedimiento interno que se lleva a cabo en el proceso de autenticación. Cabe señalar que para este proceso se realiza un intercambio de mensajes entre los componentes de Kerberos, los cuales son protegidos mediante procedimientos de cifrado y descifrado que ocultan la información intercambiada para que no sea conocida por entidades no autorizadas. Para realizar el cifrado y descifrado, las partes involucradas en el flujo de mensajes utilizan Llaves, tanto para cifrar como para descifrar, que sólo ellas conocen o saben cómo generarlas. Estas Llaves son datos que se utilizan en los mecanismos de cifrado, y son una analogía de las llaves que permiten cerrar y abrir algún objeto en la vida cotidiana.

Aunque el funcionamiento de Kerberos es complejo de entender por el número de procedimientos que realiza, es posible sintetizarlo de la siguiente manera.

Cuando un equipo cliente desea obtener un servicio de algún servidor de aplicaciones, no hace la petición directamente con este servidor, sino que antes tiene que acreditar su identidad en el dominio, específicamente con el Servidor de Autenticación AS. Este servidor verifica que el cliente exista en el Directorio del dominio, utilizando el protocolo LDAP. Cuando éste último comprueba que el cliente existe en la base de datos, le otorga un mensaje cifrado que utilizará para comunicarse con el TGS. El TGS se encarga de validar los datos, revisar la identidad del cliente, el servicio solicitado y el tiempo de validez de la solicitud. Si todo es correcto, entonces le envía al cliente un Ticket que le permitirá finalmente ponerse en contacto con el Servidor de aplicaciones, quien nuevamente revisará los datos enviados y otorgará el servicio al cliente si los datos son válidos.



Funcionamiento de Kerberos

5.2 FLUJO DE MENSAJES DE AUTENTICACIÓN KERBEROS.

Cuando un equipo cliente se autentica en el dominio genera una Llave secreta de cliente mediante una combinación del nombre de usuario y contraseña.

Si el cliente desea obtener un servicio del servidor de aplicaciones, primero manda un mensaje al servidor de autenticación (AS). Este mensaje contiene el nombre del usuario y el timestamp (dato que registra la hora y fecha en que sucedió un evento) cifrado con la Llave secreta del cliente.

AS, como parte de KDC, quien tiene acceso a la información de cuenta del usuario en el Directorio Activo, verifica que el usuario esté en la base de datos. Si es así, AS genera la Llave secreta de cliente basada en la combinación del nombre de usuario y contraseña y descifra el timestamp enviado. Verifica que el timestamp esté dentro del período correspondiente y, si es válido, AS envía dos mensajes de respuesta al cliente. Figura 2:

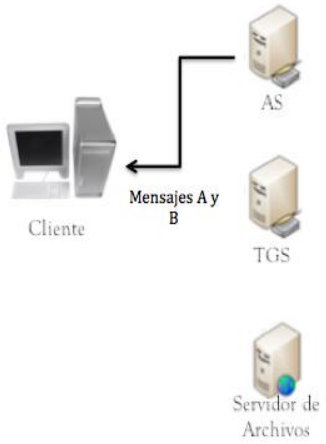


Figura 2. Mensajes de respuesta al Cliente

- Mensaje A. Contiene la Llave de sesión Cliente/TGS que será usada entre el cliente y el TGS y que es cifrada con la Llave secreta del cliente.

- Mensaje B. Es el Ticket de Concesión de Ticket (TCT, expira después de 10 hrs. y se almacena localmente en un espacio de memoria volátil), contiene el ID del cliente, la dirección de red del cliente, el período de validez del ticket y la Llave de sesión Cliente/TGS, cifrada con la Llave TGS secreta. Esta llave secreta, conocida también como KDC secreto, es la contraseña de la cuenta de usuario krbgt que todo dominio de Directorio Activo tiene. Esta cuenta se crea cuando el Controlador de Dominio es promovido como tal.

Cuando el cliente recibe los dos mensajes, descifra el mensaje A y obtiene la Llave de sesión Cliente/TGS. Sin embargo, no puede descifrar el mensaje B porque no tiene la Llave TGS secreta.

El cliente envía dos mensajes al TGS, Figura 3:

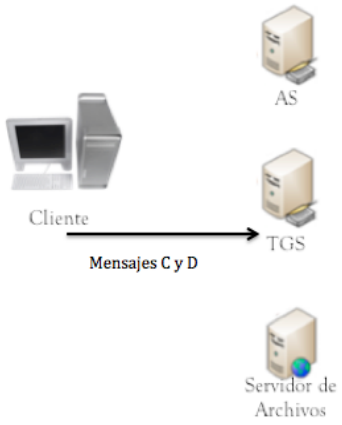


Figura 3.

- Mensaje C. Es el Ticket Granting Ticket que recibió anteriormente y también contiene la información del servicio que quiere acceder. Esta información es el Identificador (ID) del servicio.
- Mensaje D. Autenticador compuesto del ID del cliente y del timestamp cifrado con la Llave de sesión Cliente/TGS.

TGS descifra el mensaje C y obtiene el Ticket Granting Ticket que incluye datos del cliente, el período de validez del ticket y la Llave de sesión Cliente/TGS. Con esto, tanto el cliente como el TGS pueden comunicarse el uno con el otro porque ahora los dos tienen la Llave de sesión Cliente/TGS.

TGS descifra el mensaje D obteniendo el ID del cliente y el timestamp, con lo que sabe cuándo envío el mensaje el cliente.

El TGS verifica que el ID del cliente obtenido en el mensaje D corresponda al ID del cliente obtenido en el mensaje C además de verificar que el timestamp no exceda el período de validez del ticket. Si estos datos son válidos entonces TGS envía al cliente los siguientes mensajes, Figura 4:

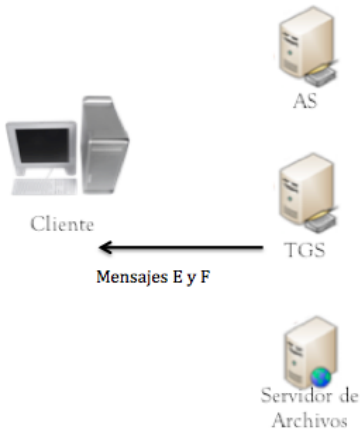


Figura 4.

- Mensaje E. Ticket Cliente a Servicio o ticket de servicio el cual contiene el ID del cliente, la dirección de red, el timestamp y la llave de sesión Cliente/Servidor cifrada con la llave secreta del servidor de archivos.
- Mensaje F. El timestamp y la llave de sesión Cliente/Servidor cifrada con la llave de sesión Cliente/TGS.

El cliente descifra el mensaje F y obtiene la llave de sesión Cliente/Servidor.
El cliente envía dos mensajes al Servidor del servicio solicitado (Servidor de Archivos en este caso), Figura 5:

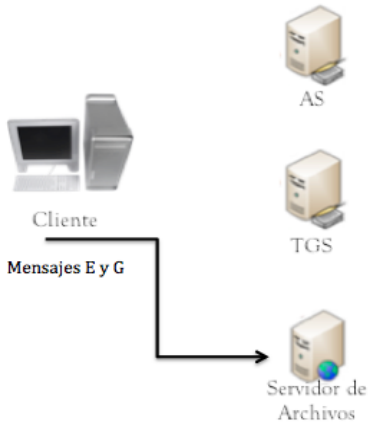


Figura 5.

- Mensaje E recibido del TGS.
- Mensaje G. Autenticador compuesto del ID del cliente y del timestamp cifrado con la llave de sesión Cliente/Servidor.

El Servidor de Archivos descifra el mensaje E y obtiene la llave de sesión Cliente/Servidor además del ID del cliente, la dirección de red y el período de validez.

También descifra el mensaje G y obtiene el ID del cliente y el timestamp.

Verifica que el ID del cliente obtenido en el mensaje E corresponda al obtenido en el mensaje G además de revisar que el timestamp no exceda el período de validez. Si los datos son válidos el Servidor envía el mensaje H (Figura 6), confirmando la identidad del cliente y avisando que está listo para proveer el servicio.

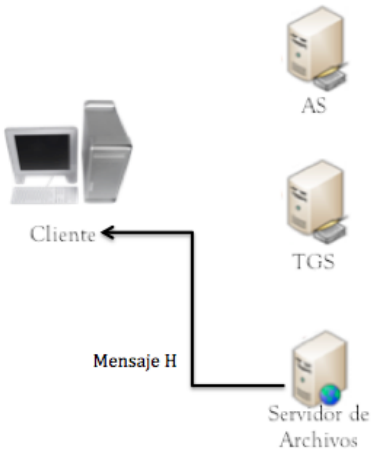
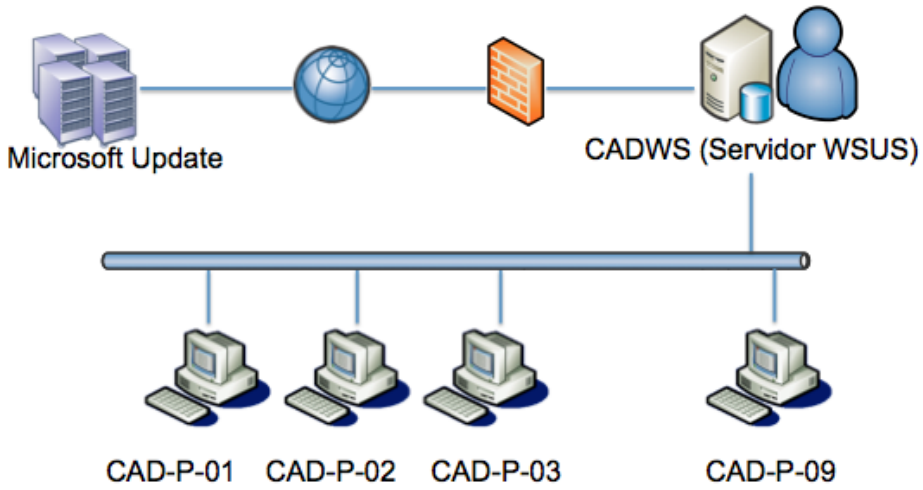


Figura 6.

Por último, el cliente emite una solicitud de servicio al FS y el servidor atiende la solicitud.

FUNCIONAMIENTO WSUS.



Funcionamiento WSUS.

1.- El administrador del servidor selecciona las actualizaciones que requiere del catálogo de productos de actualización de WSUS.

2.- El servidor descarga las actualizaciones disponibles desde Microsoft Update.

3.- Los clientes se registran con el servidor WSUS.

4.- El administrador organiza a los equipos cliente en grupos de equipos.

5.- El administrador aprueba las actualizaciones.

6.- Se instalan las actualizaciones aprobadas por el administrador.

6.1 ACTUALIZACIONES DE SOFTWARE.

Las actualizaciones se usan para reparar o reemplazar software instalado en un equipo. Cada actualización disponible en Microsoft Update está formada por dos componentes:

- Archivos de actualización.
  Son los verdaderos archivos que se requieren para instalar una actualización en un equipo.

- Información de actualización, también llamada Metadatos de actualización.
  Es información que permite determinar rápidamente los usos de la actualización. El paquete de metadatos descargado para una actualización es generalmente mucho más pequeño que el paquete de archivos de actualización real. Los metadatos incluyen los siguientes datos:

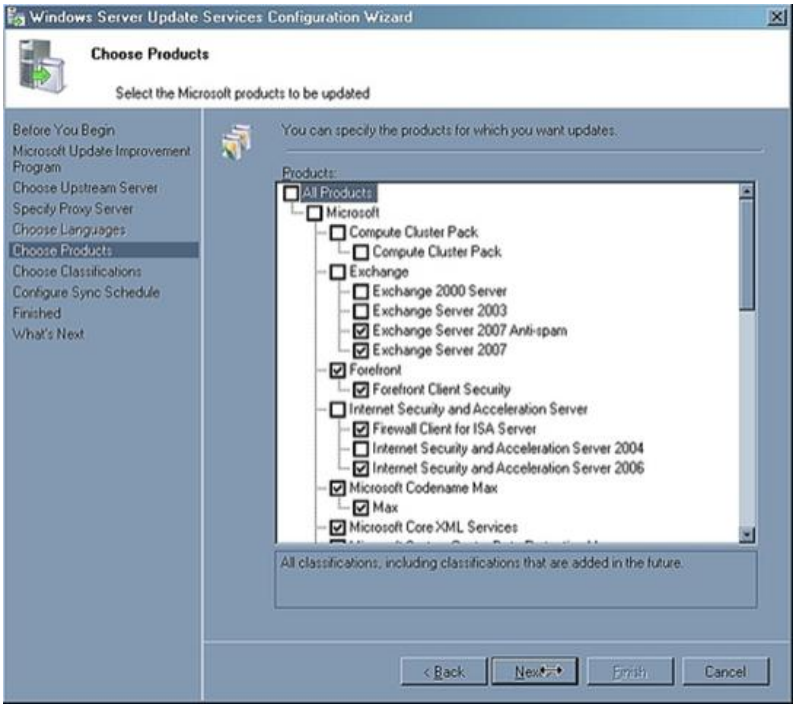
  - Propiedades de actualización
    Título, descripción, comportamientos (por ejemplo, si se puede quitar la actualización, si requiere reinicio del sistema, si requiere la intervención del usuario, etc.), productos a los que se aplica la actualización, idiomas admitidos por la actualización, actualizaciones a las que reemplaza, y el número MSRC (Centro de Respuesta de Seguridad de Microsoft) que sirve para dar seguimiento a eventos de seguridad relacionados con la actualización.

  - Reglas de aplicabilidad.
    Reglas que son usadas por las actualizaciones automáticas para determinar si la actualización es requerida sobre alguna máquina en particular.

  - Información de Instalación.
    Opciones de línea de comandos para aplicar cuando las actualizaciones son instaladas.

6.2 ACTUALIZAR SINCRONIZACIONES.

Las sincronizaciones se refieren al procedimiento en el cual el servidor agrega las nuevas actualizaciones disponibles en el sitio de Microsoft Update. Cuando el servidor WSUS realiza la primera sincronización, descarga todas las actualizaciones especificadas al configurar las opciones de sincronización.



Configuración de actualizaciones en WSUS.

Después de la primera sincronización, el servidor WSUS descarga sólo las nuevas actualizaciones disponibles desde la última vez que se puso en contacto con el origen de actualización.

A medida que los equipos cliente de WSUS se ponen en contacto con el servidor WSUS, exploran automáticamente las actualizaciones para determinar si son necesarias.

Con WSUS es posible sincronizar determinados conjuntos de actualizaciones y configurar una programación de sincronización para que este procedimiento se realice de manera automática.

6.3 ADMINISTRACIÓN DE EQUIPOS EN WSUS.

WSUS permite tener un mayor control en el proceso de actualización en los equipos cliente, permitiendo a los administradores determinar cuáles son las actualizaciones que requieren, especificar cuándo se van a instalar y supervisar el estado de implementación de las mismas.

Además, con WSUS es posible administrar las actualizaciones para grupos de equipos cliente, lo que garantiza que los equipos obtienen las actualizaciones correctas en el momento más conveniente. Por ejemplo, es posible determinar cuándo se deben actualizar los equipos de una configuración específica y qué actualizaciones deben obtener. Posteriormente, se puede evaluar el éxito de la implementación de las actualizaciones para dicho grupo de equipos utilizando las características de informes de WSUS. La creación de grupos de equipos así como la administración de las actualizaciones y la capacidad de informar acerca del estado de las actualizaciones son algunas de las tareas que permite realizar la consola de administración de WSUS.

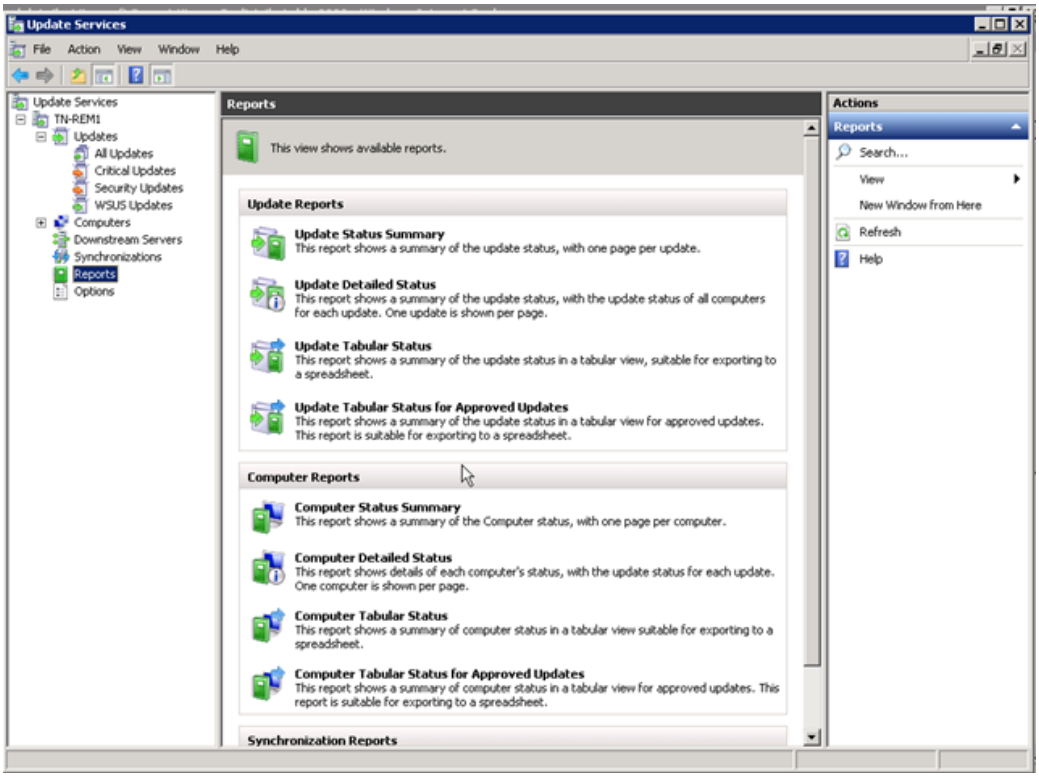
6.4 INFORMACIÓN GENERAL DE INFORMES.

Los informes disponibles en WSUS permiten supervisar las actualizaciones, los equipos y los resultados de la sincronización para los equipos y servidores WSUS administrados a través del servidor. Los informes disponibles desde la opción Informes en la consola de administración (Figura 5) se agrupan en las categorías siguientes:

- **Actualizaciones:** resumen del estado de la actualización, estado detallado de la actualización, estado tabular de la actualización y estado tabular de la actualización para actualizaciones aprobadas. Los estados tabulares son vistas con información agrupada en filas y columnas, la cual puede ser exportada a procesadores de texto especiales como las hojas de cálculo de Microsoft Office Excel para su manejo.

- **Equipos:** resumen del estado del equipo, estado detallado del equipo, estado tabular del equipo y estado tabular del equipo para actualizaciones aprobadas.

- **Sincronización:** resultados de la sincronización.



Informes en WSUS

Generalmente, WSUS muestra el estado de actualización para un determinado equipo o grupo de equipos. En la siguiente tabla se explican estos estados.

Estado de la actualización	Descripción
Instalada	La actualización se instaló en el equipo.
No aplicable	La actualización no se aplica al equipo.
Necesaria	Cuando se refiere al estado de un equipo, significa que la actualización debe instalarse en el equipo. Cuando se refiere al estado de un grupo de equipos, la columna Necesaria muestra el número de equipos del grupo en los que se debe instalar la actualización.
Error	Error de instalación en el equipo.
Sin estado	WSUS no pudo obtener el estado de la actualización. Generalmente, esto significa que el equipo no se ha puesto en contacto con el servidor WSUS una vez sincronizada la actualización con el servidor WSUS.

Estados de actualización.

Cuestionarios Personal CAD.

Estos cuestionarios se realizaron al personal del CAD antes de realizar el proyecto para conocer las opiniones sobre el funcionamiento en general del Centro. El objetivo fue identificar problemáticas con los recursos de la red, el manejo de la información y la administración de los recursos. También, fueron una importante herramienta que permitió tomar las opiniones del personal para idear soluciones enfocadas a la resolución de las problemáticas identificadas. Los cuestionarios se dividieron en dos, uno para el personal con mayor experiencia y responsabilidad en el Centro, es decir para los técnicos académicos y otro cuestionario para los prestadores de servicio social quienes tienen otra perspectiva del Centro, los recursos y las actividades que ahí se realizan.

TIPO DE USUARIO: ADMINISTRADORES, TÉCNICOS ACADÉMICOS

Erika Grisel Rodríguez

1.- ¿Cuánto tiempo llevas trabajando en el CAD?

6 años

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

Si, la mayor parte del tiempo.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

No

4.- El tiempo de configuración de las máquinas normalmente es:

- Excesivo
- Justo
- Mínimo

¿A qué crees que se deba?

Muy manual, equipo por equipo. No hay documentos o manuales que se vayan realizando.

5.- ¿Cuándo se quiere ingresar un nuevo equipo a la red cómo es este proceso?

Teniendo una IP fija asignada es rápido (Si esta no da problemas).

6.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

Si, varias, la más grave fue que al encontrarse los archivos compartidos, una persona (posiblemente el mismo dueño del archivo) borró imágenes de un proyecto y al no tener logs de ese proceso exactamente o forma de controlarlo, se culpó injustamente a una persona. Se han encontrado claves de acceso compartidas en claro y sin restricciones tanto del CAD como de otros departamentos, incluso de servidores y bases de datos.

7.- ¿Cuáles son los problemas más comunes que se presentan en el CAD?

Las fallas en la luz afectan a los servidores, la falla constante en la red que en ocasiones se deja de acceder a otros equipos y otras no, el tener que buscar en todas las máquinas posibles para buscar algún archivo compartido, respaldar, instalar, etc., se vuelve laborioso. Problemas con las impresoras.

8.- ¿Algún usuario se ha quejado alguna vez de perder su información, o que esta haya sido alterada o usada incorrectamente? ¿Se solucionó el o los incidentes? ¿Cómo?

Si, no. (Software especial para recuperar pero nunca es al 100%)

9.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

Más bien no es eficiente, cada vez que llega un servicio social hay que compartir passwords, los profesores por la necesidad de no cargarles la mano a utilizar contraseña en el CAD, pueden causar intencionalmente o no errores, pérdidas de información de sus colegas y del CAD.

Control de acceso no lo es ya que los servicios sociales se van conociendo los passwords y no es eficiente estarlos cambiando cada vez que uno de ellos termina.

10.- ¿Ha existido algún problema en cuanto a la recabación de estadísticas de asistencia y uso de recursos del CAD y/o en el manejo de estos datos? ¿Cuáles fueron las consecuencias?

Muy manual, implica tiempo y en ocasiones la Directora solicita los datos de imprevisto, es más fácil cometer errores de dedo o que la información no sea correcta.

11.- En general, ¿Cuál crees que es la opinión de los usuarios respecto a la red del CAD y los servicios que se brindan? ¿Y la tuya?

Usuarios en general buena, muchos prefieren usar equipos del CAD por la velocidad y asesoría, que los equipos de sus departamentos.

La mía, se podrían implementar muchas mejoras a la administración de los equipos, incluso indirectamente se mejoraría la seguridad de los servidores e incluso la información valiosa del propio CELE.

12.- ¿Qué mejora(s) consideras que deberían hacerse en cuanto a la red, su administración, la seguridad y/o los servicios que se brindan y por qué?

Mejoras en cuanto a las cuentas de usuario, en cuanto a la documentación de procesos como son la administración de usuarios, instalaciones, control de discos de instalación y también revisar la seguridad de la red inalámbrica ya que al estar sin contraseña pudiera haber problemas de seguridad dentro del CAD.

Laura San Juan Ceja

1.- ¿Cuánto tiempo llevas trabajando en el CAD?

9 años

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

Es funcional pero no eficiente. Cuando hay una alta carga de trabajo en la red, el comportamiento de esta puede ser un poco errático y por lo tanto no funciona como debe.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

Actualmente el servicio de almacenamiento de información por parte de los usuarios en los equipos del CAD ya no está disponible debido a algunos detalles como el almacenamiento excesivo de información. Debido a esto, la parte de compartir archivos la uso menos puesto que ya no es algo tan requerido, a diferencia de antes que cuando algún usuario deseaba ver su información esta debía estar disponible desde cualquier máquina de la red.

4.- El tiempo de configuración de las máquinas normalmente es:

- Excesivo
- Justo
- Mínimo

¿A qué crees que se deba?

Considero que este aspecto podría mejorarse, de tal forma que la configuración que se requiere que tengan los equipos en cuanto a los idiomas, el teclado, los plug-ins, etc., se haga sólo en un equipo y está configuración se copie a las demás por medio de una imagen por ejemplo, en vez de configurar cada máquina independientemente.

5.- ¿Cuándo se quiere ingresar un nuevo equipo a la red cómo es este proceso?

En realidad el proceso es sencillo, sin embargo el problema que se tiene es la disponibilidad en cuanto a direcciones IP, ya que actualmente hay un sobrepaso de equipos respecto al número de direcciones IP disponibles. Este es un problema importante porque el crecimiento de la red en cuánto a número de equipos es algo latente y cada vez se requieren más direcciones IP.

6.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

Hace mucho tiempo DGSCA detectó un problema de seguridad en la red del CELE, no del CAD, al parecer algunos de los servidores en cómputo fueron hackeados provocando que la información se viera comprometida y que se limitara la red mientras se llevaban a cabo las investigaciones. Además

ha habido momentos en que la red está muy lenta, no funciona, se cayó algún servicio, etc. Esto se ha visto mejorado mediante un mejor control de los equipos de conexión (routers, switches, hubs) por parte de la gente de cómputo. Aunque los problemas debidos a las interrupciones eléctricas aún no se han solucionado.

7.- ¿Cuáles son los problemas más comunes que se presentan en el CAD?

La cuestión de las impresoras que algunos equipos no pueden imprimir, también la comunicación entre las computadoras, algunos equipos se ven otros no, no puedes compartir información con todas, etc.

8.- ¿Algún usuario se ha quejado alguna vez de perder su información, o que esta haya sido alterada o usada incorrectamente? ¿Se solucionó el o los incidentes? ¿Cómo?

Cuando se va la luz y la información no había sido guardada. A través del uso del SVN se ha tratado de evitar la perdida de información de la gente que forma parte del desarrollo de proyectos, pero inclusive antes del uso del SVN no recuerdo que se tuvieran muchos problemas de este tipo.

9.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

A nivel de seguridad los mecanismos de control de acceso no creo que sean tan buenos porque se puede tener acceso a todo, lo único que se restringe en la cuenta de profesor es poder instalar programas, de ahí en fuera creo que tienen acceso a todo. Me parece que sería bueno tener un mejor control en la cuenta de supervisor.

Respecto al uso de contraseñas creo que hay que ser sensibles con los profesores y entender que ya tienen un gran número de contraseñas que recordar para los distintos servicios que ocupen.

10.- ¿Ha existido algún problema en cuanto a la recabación de estadísticas de asistencia y uso de recursos del CAD y/o en el manejo de estos datos? ¿Cuáles fueron las consecuencias?

No, es una lista donde se recaban los servicios que se utilizan, no la cantidad, no ha habido problema.

11.- En general, ¿Cuál crees que es la opinión de los usuarios respecto a la red del CAD y los servicios que se brindan? ¿Y la tuya?

En general creo que la red ahora esta mejor a comparación de antes que se pasmaba y teníamos varios problemas y eso funciona para los profesores aunque los servicios creo que aún podría mejorarse sobre todo en busca de que los profesores se sientan más atraídos al CAD, servicios como ver canales de televisión extranjera manteniendo la velocidad, la accesibilidad y otros aspectos de la red que permitan brindar estos servicios que despierten el interés en los profesores.

Mi opinión es que dado que uno de los objetivos del CAD es el desarrollo de ideas y proyectos es esencial contar con una infraestructura que funcione, que no sea voluble, inestable. Creo que es importante que la parte del direccionamiento IP se resuelva para evitar los problemas de que los equipos a veces se conectan y otras no, y también lograr que los servicios sean confiables, esos aspectos creo que son esenciales para un centro de cómputo.

Teresa Cesáreo Castillo

1.- ¿Cuánto tiempo llevas trabajando en el CAD?

6 años

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

En cuanto a los recursos que yo puedo utilizar en mi trabajo creo que si funciona de manera correcta, si han existido algunos problemas pero son más cuestiones de configuración en mi equipo y no tanto de la red.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

Debido a que ahora estoy en el proceso de cambio de equipo si he tenido varios problemas para poder compartir información y recursos con las otras máquinas. Ahorita ya he estado investigando sobre distintos tipos de conexión para poder solucionar estas problemáticas pero aun no se han logrado resolverse del todo, sobre todo porque no hemos podido integrar la máquina al grupo de trabajo.

4.- El tiempo de configuración de las máquinas normalmente es:

- Excesivo
- Justo
- Mínimo

¿A qué crees que se deba?

Se debe a que no hay una persona que se dedique exclusivamente a la configuración, en el caso de mi máquina soy yo quien se tiene que encargar de estos procedimientos apoyándome de los chicos de servicio social y en ocasiones del personal de cómputo. Sin embargo, cuando la carga de trabajo es mucha esto se complica ya que me tengo que dividir entre las labores de configuración y mis actividades del trabajo que tengo que realizar. Por eso a veces este tiempo si es excesivo.

5.- ¿Cuándo se quiere ingresar un nuevo equipo a la red cómo es este proceso?

Es complicado por el número de direcciones IP disponibles, cuando un equipo se reemplaza se ocupa la misma dirección IP, pero cuando el equipo es nuevo primero se tuvo que haber justificado el por qué de su adquisición y que le sea otorgada la dirección IP que le permita integrarse a la red.

6.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

Hubo un caso en el que se encontró un archivo que estaba compartido, en el cual se especificaba la información de las máquinas de la red, como números de serie, contraseñas, etc. Lo cual pudo tener consecuencias serias de seguridad; este caso no fue tanto un problema técnico sino un problema interno de organización.

Otro caso que recuerdo fue que anteriormente había un equipo en el cual se almacenaba la información de los usuarios así como de proyectos que se estaban realizando para facilitar la disponibilidad de esta información, y lo que sucedió fue que una profesora perdió información valiosa culpando al personal de aquí de lo que había sucedido, aunque también estaba la posibilidad de que ella no hubiera guardado la información correctamente o algo similar, y aunque se hizo una búsqueda en todas las máquinas de la red, la información no se pudo recuperar causando mucha molestia en la profesora quien inclusive se quejó con la Directora.

7.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

Es una situación que involucra varios riesgos y en la que se debería tener un mejor control ya que debido a que se presentan casos en los que se requiere alguna configuración que requiere de la contraseña de administrador pues muchas veces ha ocurrido que se cambia a la cuenta de administrador y se queda abierta, de forma que un usuario puede llegar y entrar en esta cuenta teniendo todos los permisos y accediendo a información importante.

8.- ¿Ha existido algún problema en cuanto a la recabación de estadísticas de asistencia y uso de recursos del CAD y/o en el manejo de estos datos? ¿Cuáles fueron las consecuencias?

Las estadísticas son datos de los que no tengo mucho conocimiento puesto que la persona encargada de esto es el responsable del CAD y quien él solicite que lleve a cabo esta tarea de recabar los datos.

9.- En general, ¿Cuál crees que es la opinión de los usuarios respecto a la red del CAD y los servicios que se brindan? ¿Y la tuya?

En general creo que los usuarios tienen una buena referencia del CAD tanto así que mucha de la gente nueva que viene lo hace por recomendación de alguien más. Y creo que esto sucede por los servicios que se dan, por ejemplo el de asesoría; inclusive personas de otros departamentos acuden al CAD para pedir asesoría de problemas que ellos tienen, y aunque a nosotros nos corresponde asesorar únicamente a los usuarios del CAD cuando podemos ayudar a otras personas lo hacemos.

Mi opinión es que en general si cubrimos las expectativas o las necesidades de un usuario promedio en el CAD. Pero a veces creo que les quedamos a deber en cuestión de disponibilidad de equipos ya

que hay ocasiones en las que todos los equipos están ocupados y esto crea cierta incomodidad en los usuarios.

10.- ¿Qué mejora(s) consideras que deberían hacerse en cuanto a la red, su administración, la seguridad y/o los servicios que se brindan y por qué?

Tal vez buscar más estrategias de integración de los equipos MAC a la red para que no sea tan complicado trabajar con las otras máquinas. Terminar de integrar mi equipo completamente a la red porque aún tengo varios problemas.

TIPO DE USUARIO: SERVICIOS SOCIALES.

Areli Espinoza de los Monteros

1.- ¿Cuánto tiempo llevas asistiendo al CAD?

1 mes

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

Se podrían mejorar varias cosas, actualmente la velocidad de la red en ciertas horas del día no es la que se desea. A veces se pierde la conexión con la red y también hay problemas con la comunicación entre los equipos y ciertos servicios como el escáner creo que se pueden hacer más eficientes.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

No, porque no todos los equipos están en red.

4.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

Una vez hubo una pequeña interrupción en la energía eléctrica y perdí el trabajo que estaba realizando en ese momento, así que tuve que volver a hacerlo. También sucedió que se encontró un archivo con información sensible de los equipos como contraseñas y este archivo estaba compartido así que todos podían verlo.

5.- ¿Cuáles son los problemas más comunes que se presentan en el CAD?

Lentitud de la red, problemas con la conexión entre los equipos. En lo particular ha sucedido que el equipo donde tengo información está ocupado y tengo que esperar a que se desocupe.

6.- ¿Algún usuario se ha quejado alguna vez de perder su información, o que esta haya sido alterada o usada incorrectamente? ¿Se solucionó el o los incidentes? ¿Cómo?

No he sabido de un evento de este tipo.

7.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

Creo que sólo debería haber dos cuentas, la de Staff y la de profesor. La de Staff con los privilegios para poder instalar, actualizar software aunque sería bueno que para configuraciones más sensibles como cambiar el Sistema Operativo existiera otra cuenta con privilegios para poder hacerlo.

8.- En general, ¿Cuál es tu opinión respecto a la red del CAD y los servicios que se brindan?

Creo que está bien pero se podrían mejorar varias cosas como controlar de mejor manera la parte de la comunicación entre los equipos y también los escritorios de las máquinas, están muy saturados.

9.- ¿Qué mejora(s) consideras que deberían hacerse en cuanto a la red, su administración, la seguridad y/o los servicios se que brindan y por qué?

Creo que sería bueno que los usuarios pudieran guardar información en los equipos y por lo tanto habría que mantener esta información bien protegida. También sería bueno hacer que la información este disponible en todas las máquinas para no detener el trabajo o las actividades que tenemos que realizar. Otra mejora podría hacerse en la configuración de los equipos, que se haga de manera general y no de manera independiente.

TIPO DE USUARIO: SERVICIOS SOCIALES.

Abelardo Adalberto Jiménez

1.- ¿Cuánto tiempo llevas asistiendo al CAD?

5 meses

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

Hay algunas ocasiones en que la red se traba, o es lenta.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

En ocasiones es tardado el proceso de conectarte con la máquina que deseas, yo comparto información con Laura y a veces no encuentro su máquina o tarda la interfaz en ubicar a las máquinas conectadas.

4.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

No.

5.- ¿Cuáles son los problemas más comunes que se presentan en el CAD?

Problemas con la impresora y que a veces no abren las páginas de internet.

6.- ¿Algún usuario se ha quejado alguna vez de perder su información, o que esta haya sido alterada o usada incorrectamente? ¿Se solucionó el o los incidentes? ¿Cómo?

No he sabido de un evento de este tipo.

7.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

Yo creo que está bien pero debería haber un mejor control en ellas, sobre todo de los privilegios que cada una de ellas tiene y debería tener.

8.- En general, ¿Cuál es tu opinión respecto a la red del CAD y los servicios que se brindan?

En general yo creo que están satisfechos porque normalmente los servicios y recursos que utilizan son los básicos y esos funcionan de forma aceptable para ellos.

En mi opinión siento que debería tratarse de mejorar la rapidez de la red y la confiabilidad en los servicios como la comunicación, la conexión con internet y la impresora.

9.- ¿Qué mejora(s) consideras que deberían hacerse en cuanto a la red, su administración, la seguridad y/o los servicios se que brindan y por qué?

Mejorar la rapidez y la confiabilidad de los servicios que se brindan.

TIPO DE USUARIO: SERVICIOS SOCIALES.

Admer Luis Gallegos

1.- ¿Cuánto tiempo llevas asistiendo al CAD?

5 meses

2.- ¿Consideras que la red del CAD funciona de manera correcta considerando factores como la velocidad, la conexión, los servicios?

En cuanto a la velocidad a veces es lenta, la conexión creo que si siempre es estable, siempre hay acceso a internet y respecto a los servicios a veces fallan como la impresora y el escáner que tiene una falla en el software que utiliza.

3.- ¿La forma de compartir información con las demás máquinas es sencilla?

A veces es complicado porque se presentan problemas para conectar con ciertas máquinas, en unas se requiere de permisos y en otras no, además de que considero que debería hacerse algo para proteger que las máquinas están conectadas con toda la Red del CELE, es un riesgo alto. También

me he dado cuenta de que existen dos grupos de trabajo en la red del CAD uno es CADCELE y el otro el CELECAD, no se que tan problemático pudiera ser esto.

4.- ¿Ha habido alguna eventualidad en el funcionamiento de la red? ¿De qué tipo (seguridad, administración, externa, etc.)? ¿Cuál ha sido la más grave que recuerdes? ¿Cuál fue la solución?

Sólo los problemas de comunicación con ciertas máquinas, y la configuración de la máquina de Tere que es MAC que no hemos podido integrarla al grupo de trabajo.

5.- ¿Cuáles son los problemas más comunes que se presentan en el CAD?

Problemas con la impresora y el escáner.

6.- ¿Algún usuario se ha quejado alguna vez de perder su información, o que esta haya sido alterada o usada incorrectamente? ¿Se solucionó el o los incidentes? ¿Cómo?

No he sabido de un evento de este tipo.

7.- ¿Qué piensas respecto a las diferentes cuentas de usuario que tienen las máquinas, crees que son suficientes, excesivas, agregarías otra(s)? ¿Y respecto al control de acceso de cada una de ellas?

Pienso que la cantidad está bien al igual que los mecanismos de control de acceso ya que para los profesores es cómodo que no tengan que ingresar alguna contraseña y para las otras cuentas también creo que está bien contar sólo con una contraseña puesto que si hubiera una para cada usuario sería difícil de controlar esto, por ejemplo se tendría que checar la vigencia de las cuentas porque por ejemplo los servicios sociales sólo estamos cierto tiempo. Para proteger la información que tenemos pienso que está bien el uso del SVN y si los profesores quieren proteger su información pueden utilizar carpetas con contraseña o algo similar.

8.- En general, ¿Cuál es tu opinión respecto a la red del CAD y los servicios que se brindan?

En general yo creo que la opinión es buena, el CAD cumple con los servicios que requieren los usuarios pero siento que deberían procurarse resolver los problemas con la impresora y el escáner que son muy recurrentes.

9.- ¿Qué mejora(s) consideras que deberían hacerse en cuanto a la red, su administración, la seguridad y/o los servicios se que brindan y por qué?

Mejorar la velocidad de la red, resolver las fallas que se tienen en la comunicación entre las máquinas, revisar las problemáticas con la impresora y el escáner.

Este anexo es un manual que explica la forma de configurar las políticas de grupo utilizadas en la implementación, de forma que los administradores puedan referirse a él como una guía para volverlas a configurar, si fuera necesario, o también para crear nuevas. De igual manera, se detalla el objetivo, los beneficios y el modo de funcionamiento de cada una de ellas.

Políticas del Dominio

1.- Revisión de contraseñas, longitud y complejidad.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de Directivas de grupo/Editar Default Domain Policy (Dominio)/Configuración del equipo/Directivas/Configuración de Windows/Configuración de seguridad/Directivas de cuenta/Directiva de contraseñas

Objetivo: Esta política ayuda a resolver problemáticas identificadas referentes a la protección de la información.

Beneficios:

- Control automático de validación de la complejidad de las contraseñas de los usuarios.
- Disminución de riesgos de obtención de contraseñas por terceras personas.
- Mejora en la confidencialidad, integridad y control de acceso para la información del Centro.

Funcionamiento: Sobre todo el dominio.

2.- Distribución e instalación de Software.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de Directivas de grupo/En objetos de directiva de grupo crear una nueva GPO con el nombre del programa (Firefox por ejemplo)/Editar la nueva GPO/Configuración del equipo/Directivas/Configuración de software/Instalación de software:

- Nuevo -> Paquete
- Colocar la ruta del programa \\CADWS\Programas\Firefox.msi
- Abrir -> Avanzada -> Implementación -> Asignada
- Marcamos la opción de Desinstalar esta aplicación cuando este fuera del ámbito de administración.
-

Objetivo: Automatizar la instalación de software básico en los equipos al momento de su integración al dominio.

Beneficios:

- Reducción en la inversión de tiempo por parte de los administradores para la habilitación de los equipos cuando se integran al dominio.
- Uniformidad en el funcionamiento de los equipos.

- Facilitar la transición en el cambio de esquema de red de grupo de trabajo a dominio de forma que no impacte sobremanera en el funcionamiento de los equipos.

Funcionamiento: Sobre todos los equipos del dominio.

3.- Almacenamiento de Software (Servidor de aplicaciones).

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de Directivas de grupo/En objetos de directiva de grupo crear una nueva GPO con el nombre del programa/Editar la nueva GPO/Configuración de usuario/Directivas/Configuración de software/Instalación de software

- Nuevo -> Paquete
- Colocar la ruta del programa \\CADWS\Programas\Firefox.msi
- Abrir -> Avanzada -> Implementación -> Publicada
- Marcar la opción de Desinstalar esta aplicación cuando este fuera del ámbito de administración.

Objetivo:Permitir a los usuarios autorizados disponer del software especializado necesario desde cualquier máquina del dominio.

Centralizar el software necesario para la realización del trabajo de los usuarios del CAD como los prestadores de servicio social, tesistas, administradores, etc.

Evitar que la falta de disponibilidad de equipos obstaculice la realización del trabajo de los usuarios en el CAD.

Beneficios:

- Mejora en la disponibilidad de los equipos.
- Los usuarios autorizados podrán instalar el software necesario en los equipos fácilmente sin necesidad de buscarlo o descargarlo de internet.

Funcionamiento: Sobre todos los usuarios que pertenecen a la Unidad Organizativa Personal CAD del dominio.

4.- Política de actualizaciones de los sistemas operativos Windows.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de directivas de grupo/Crear GPO en Objetos de directivas de grupo -> editar/Configuración del equipo/Directivas/Plantillas administrativas/Componentes de Windows/Windows Update/Configurar actualizaciones automáticas -> Habilitada /Configurar la opción de “Especificar la ubicación del servicio Windows Update” -> Habilitada -> Establecer el servicio de actualización de la intranet para detectar actualizaciones automáticas -> http://CADWS/Establecer el servidor de estadísticas de la intranet -> http://CADWS

Una vez creada la GPO, se instalan los siguientes programas:

Instalación de servidor IIS con (ASP.NET, Autenticación de Windows, Compresión de contenido dinámico y Compatibilidad con la administración de IIS 6)

- Herramientas administrativas
- Administrador del servidor
- Funciones -> agregar funciones
- Seleccionar Servidor web (IIS)
- Agregar características necesarias
- Agregar selección de ASP.NET (funciones requeridas automáticamente), Autenticación de Windows, Compresión de datos de contenido y Compatibilidad con la administración de IIS 6
  -> instalar

- Instalar Microsoft Report Viewer Redestributable 2008
  - http://www.microsoft.com/download/en/details.aspx?id=6576

- Instalación de WSUS 3.0 SP2(Service Pack 2)
  - Descargar software de www.microsoft.com/download/en/details.aspx?id=5216
  - Ejecutar software.

Finalmente se configura WSUS desde la opción “Configurar WSUS” en el menú de WSUS

- Sincronizar desde Microsoft Update
- No Usar un servidor proxy al sincronizarse
- Iniciar conexión
- Elegir idioma
- Elegir productos (Report Viewer 2010, Microsoft Security Essentials, Dictionary Updates for Microsoft IMEs, New Dictionaries for Microsoft IMEs, Office 2007, Office 2010, Administrador de Windows Server: WSUS, Paquetes de idiomas de Windows 7, Windows Server 2008
- Clasificación de actualizaciones a sincronizar agregar Service Pack
- Sincronizar manualmente -
- Iniciar la consola de administración de Windows Server Update Services ->finalizar

Del lado del cliente revisar que se está ejecutando el servicio “wuauserv”. Para que los equipos cliente se reporten con el servidor WSUS una vez que se verificó que el servicio mencionado se está ejecutando ejecutar el comando: wsusclt /detectnow o wsusclt /testWSUSServer para revisar detalles de la conexión.

Cuando un cliente reporta su estado esto se anota en el log. La ruta del log es C:\Windows\WindowsUpdate.log

Objetivo:

- Centralizar la administración de las actualizaciones para tener un mayor control de las mismas.
- Optimizar la tarea de actualización en los equipos del Centro.
- Mantener a los equipos actualizados y funcionando lo más uniforme posible.

Beneficios:

- Mejorar el proceso de actualización con un control centralizado de la descarga y distribución de las actualizaciones a los equipos del dominio, así como de la revisión del estado de las mismas en cada uno de los equipos.
- Disminución en la inversión de tiempo de los administradores para la ejecución de esta tarea.

Funcionamiento: Sobre todos los equipos del dominio.

5.- Política para monitorear impresiones en la red.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administrador del servidor/Funciones -> Agregar Funciones/Seleccionar función -> Servicios de impression/Seleccionar las opciones:

- Servidor de impresión
- Servicio LPD

Generar política en Objetos de directiva de grupo (Print para esta política)

- Editar la política “Print” -> Configuración del equipo -> Directivas -> Configuración de Windows
- Click derecho -> impresoras implementadas -> implementar impresora
- Dar la ruta de acceso a la impresora \\CADWS\hp deskjet 990c -> agregar
- Crear OU Equipos en Usuarios y equipos de Active Directory
- Actualizar dominio en administración de directiva de grupo -> La política “print” se vincula a la OU equipos

Una vez hecho ir a Herramientas administrativas

- Administración de impression/Impresoras implementadas
- Click derecho sobre la impresora a configurar -> implementar con directiva de grupo
- Nombre del GPO -> Examinar -> Equipos cad.cele.unam.mx
- Seleccionar la GPO generada anteriormente “Print”
- Seleccionar la opción:
  - Los equipos a los que se aplica este GPO

Para monitorear los sucesos de la impresora implementada:

- Herramientas administrativas/Monitor de confiabilidad y rendimiento/Monitor de rendimiento/Agregar contadores -> Cola de impresión

Objetivo:

Contar con un servidor de impresión que gestione las operaciones de estos dispositivos. Desde este servidor se agregan las impresoras y se lleva un registro del número de impresiones y equipos que realizan esta actividad.

Beneficios:

- Disminución en problemas de conexión de las impresoras con los equipos del dominio.
- Instalación automática de las impresoras en los equipos al momento de ser agregados al dominio.
- No se requieren conectar las impresoras a equipos clientes del CAD para que puedan ser utilizadas como se hacía anteriormente.
- Se tiene un registro del número total de impresiones que se llevan al día, con fines de planeación de adquisición de insumos.

Funcionamiento: Sobre todos los equipos del dominio.

6.- Política para asignar cuotas de espacio de disco duro a usuarios.

- Dar clic derecho al disco duro del cual se asignarán cuotas
- Propiedades -> cuota
- Habilitar la administración de cuota
    - Denegar espacio de disco a usuarios que superen el límite de cuota
    - Registrar un evento cuando algún usuario supere su límite de cuota
- Seleccionar:
    - Limitar espacio en disco: Seleccionar la cantidad a limitar, la cual significa el espacio del disco duro que se desea limitar a todos los usuarios.
- Valores de cuota -> cuota -> Nueva entrada de cuota
- Seleccionar el usuario o grupo de usuarios al cual aplicar esa cuota
- Limitar su espacio en disco dando clic al usuario creado
- Aplicar -> Aceptar
- No limitar espacio de disco duro a las entidades autoritativas.
    - Propiedades -> No limitar espacio en disco -> Aceptar

Objetivo:

Dotar a los usuarios de espacio en disco duro del servidor para que guarden su información y que esta pueda ser utilizada en cualquier equipo donde inicien sesión.

Beneficios:

- Los usuarios tendrán la opción de almacenar su información en el disco duro del servidor.
- La información podrá ser manipulada por los usuarios autorizados en cualquier equipo en el que inicien sesión, mejorando la disponibilidad de la misma en el Centro.

Funcionamiento: Sobre todos los usuarios del dominio.

7.- Política para bloquear sesión después de cierto tiempo de inactividad.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de directivas de grupo/Objetos de directiva de grupo -> crear GPO (Bloqueo sesión) -> editar/Configuración del usuario/Directivas/Plantillas administrativas/Panel de control -> Pantalla -> Habilitar las siguientes opciones:

  - Proteger el protector de pantalla mediante contraseña
  - Tiempo de espera del protector de pantalla en el cual se especifica el tiempo en segundos
- Vincular a todo el dominio
- En el lado del cliente, en la opción de Personalización -> Cambiar protector de pantalla -> ninguno -> reiniciar

Objetivo: Proteger los datos de los usuarios cuando dejen abierta su sesión por algún descuido u omisión.

Beneficios:

- Protección de la información.
- Disminución de riesgos en cuanto a la alteración o pérdida de información de manera accidental por otro usuario.

Funcionamiento: Sobre todos los usuarios del dominio.

8.- Política para instalación de sistemas operativos por red WDS

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administrador del servidor/Funciones /Agregar funciones/ Servicios de implementación de Windows (WDS)

- Seleccionar:
  - Servidor de implementación
  - Servidor de transporte
- Instalar
- Herramientas administrativas/Administrador del servidor/Funciones -> Agregar funciones -> Servidor DHCP
- Seleccionar:
  - 132.248.74.212 IPv4
- Dominio primario: cad.cele.unam.mx
- Dirección IPv4 del servidor DNS preferido: 132.248.74.212
- No se requiere WINS
- Agregar -> Nombre de ámbito: CAD
  - Dirección IP inicial: 132.248.74.201
  - Dirección IP final: 132.248.74.201
  - Máscara de subred: 255.255.255.0
  - Puerta de enlace: 132.248.74.254
- Deshabilitar el modo sin estado DHCPv6 para este servidor

- Usar credenciales actuales -> instalar
- Dentro de servicios de implementación de Windows , click derecho en el nombre del servidor CADWS.cad.cele.unam.mx -> configurar servidor
- Asignar ruta de imágenes: D:\RemoteInstall
- Seleccionar las dos opciones:
    - No escuchar en el puerto 67
    - Configurar la opción 60 DCHP como “PXEClient”
- Seleccionar:
    - Responder sólo a los equipos cliente conocidos
- Expandir árbol del servidor en WDS,
    - Botón derecho en imágenes de instalación -> agregar imagen de instalación
- Crear un nuevo grupo de imágenes -> SO CAD
- Examinar -> Dvd:\sources\install.wim -> Seleccionar Windows 7 Professional 32 bit -> finalizar
- Botón derecho en imágenes de arranque -> Agregar imagen de arranque
- Examinar -> Dvd:\sources\boot.wim ->siguiente
- Nombre de la imagen: Microsoft Windows Setup (x86)
- Descripción de la imagen: Microsoft Windows Setup (x86) ->Finalizar

NOTA: Si aparece en pantalla “PXE-E32: TFTP open timeout”:

Abrir servicios de implementación de Windows.

Expandir los servidores.

Clic derecho sobre el CADWS-> Configuración de red

En Intervalo de puertos UDP:

DE: 50000 Hasta: 65000

Aceptar

Reiniciar el servicio de WDS en Administración del Servidor.

Agregar equipo al Servicio de dominio de Active Directory.

- Herramientas Administrativas
- Usuarios y equipos de Active Directory
- Expandir árbol de cad.cele.unam.mx
- Clic derecho en OU Computers -> Nuevo -> Equipo
- Nombre de equipo: cad-p-01 -> siguiente
- Palomear: Éste es un equipo administrador y escribir la GUID del equipo -> siguiente
- Seleccionar:
    - Cualquier servidor de instalación remota disponible

Crear reservación en DHCP.

- Herramientas administrativas
- DHCP
- Expandir servidor DHCP
- Expandir IPv4
- Expandir Ámbito
- Clic derecho en Reservas->Reserva nueva…
- Nombre de reserva: Temporal
- Dirección IP 132.248.74.201
- Dirección MAC XX:XX:XX:XX:XX:XX
- Descripción: xxxxxxx
- Tipos compatibles: ambos
- Agregar

Objetivo:

Optimizar el proceso de instalación de los sistemas operativos en los equipos cliente, disminuyendo tiempo y facilitando el procedimiento para los administradores del Centro.

Beneficios:

- Reducción de tiempo para la instalación de sistemas operativos.
- Mayor control en la versión de los sistemas operativos instalados en los equipos al estar centralizadas las imágenes en el servidor.
- Mejora en las labores de mantenimiento de los equipos al permitir el formateo de los equipos en un tiempo considerablemente menor al que se invertía anteriormente.

Funcionamiento: Sobre todos los equipos del dominio.

9.- Política para Restringir el símbolo del sistema, modificación al registro de Windows y quitar la opción de "ejecutar" del menú inicio.

Para establecerla se sigue la siguiente ruta:

Herramientas administrativas/Administración de directivas de grupo/Crear GPO en Objetos de directiva de grupo (Restringe cmd) -> editar/Configuración del usuario/Directivas/Plantillas administrativas/Menú inicio y barra de tareas/Habilitar opción -> quitar el menú ejecutar del menú inicio/elegir sistema -> habilitar opciones:

- impedir el acceso a herramientas de edición del registro
- impedir el acceso al símbolo del sistema

Objetivo: Proteger a los equipos de configuraciones que pueden ocasionar problemas en su funcionamiento limitando la disponibilidad de los mismos. Con esta política se disminuye la posibilidad de que personas sin los permisos necesarios realicen configuraciones sensibles en los equipos como modificaciones en el registro del sistema que generen un funcionamiento erróneo.

Beneficios:

- Disminución de riesgos de configuraciones incorrectas en los equipos.
- Protección de la integridad de los equipos.

Funcionamiento: Sobre todos los equipos del dominio.

10.- Política para redireccionar carpeta Documentos a unidad en red.

Herramientas administrativas/Administración de directivas de grupo/Crear GPO en Objetos de directiva de grupo (Redirect) -> editar/Configuración del usuario/Directivas/Configuración de Windows/Redirección de carpetas/Botón derecho sobre carpeta “Documentos” -> Propiedades:

  - Configuración -> Avanzado: especificar ubicaciones para diversos grupos de usuarios->Agregar
  - Elegir grupo de seguridad. “Profesores”
  - En Ubicación de la carpeta de destino elegir: Crear una carpeta para cada usuario en la ruta raíz.
  - Dar ruta de acceso raíz \\CADWS\Info_Profesores_CAD
- Vincular GPO a Unidad Organizativa Profesores.
  - Compartir carpeta Info_Profesores_CAD con permisos de copropietario
- Del lado del cliente Ejecutar GPUPDATE/FORCE, cerrar sesión, reiniciar máquina.

Objetivo: Permitir a los usuarios almacenar información en el disco duro del servidor de tal manera que esté disponible en cualquier máquina del dominio con las condiciones suficientes de integridad, confidencialidad, disponibilidad y autenticación.

Beneficios:

- Los usuarios podrán almacenar información el disco duro del servidor.
- La información estará disponible en cualquier máquina desde la cual los usuarios inicien sesión.
- La distribución de los equipos será independiente de la información almacenada en ellos.

Funcionamiento: Sobre todos los usuarios del dominio.

En este anexo se presentan los requerimientos sobre los que se basó el desarrollo de la aplicación para la toma de asistencia en el Centro. Para la obtención de los requerimientos se siguió la norma ISO 29110 en la cual se hace un análisis por caso de uso.

SISTEMA DE GESTIÓN DE ASISTENCIAS Y USO DE RECURSOS DEL CAD.

Requerimientos Asistencia:

Identificador	Caso de Uso	Prioridad
1	***ABML Usuarios***	*Normal*
2	***Identificar en Aplicación***	*Normal*
3	***Cerrar sesión en Aplicación***	*Normal*
4	***Mostrar estadísticas***	*Alta*
4.1	***Mostrar por mes***	*Alta*
4.2	***Mostrar por período***	*Alta*
5	***Exportar estadísticas a Excel***	*Normal*
5.1	***Exportar estadísticas a Excel de mes***	*Normal*
5.2	***Exportar estadísticas a Excel del período***	*Normal*
6	***ABML asistencia***	*Alta*
7	***ABML recurso***	*Alta*
8	***AML recurso utilizado***	*Alta*

Identificación de datos.

Caso de uso 1 (***ABML Usuarios***)

Dato	Descripción (Tipo, extensión, formato, datos validos)	Requerido
D1	*Usuario (Carácter, 5-30,--,[a-z][A-Z])*	*Si*
D2	*Contraseña (Carácter, 7-15,--, [a-z][A-Z] [0-9])*	*Si*

Caso de uso 2 (***Identificar en Aplicación***)

Dato	Descripción (Tipo, extensión, formato, datos validos)	Requerido
D1	*Usuario (Carácter, 5-30,--,[a-z][A-Z])*	*Si*
D2	*Contraseña (Carácter, 7-15,--, [a-z][A-Z] [0-9])*	*Si*

Caso de uso 6 ***(ABML asistencia)***

Dato	Descripción (Tipo, extensión, formato, datos validos)	Requerido
D1	*Usuario del dominio (Carácter, 5-30,--,[a-z][A-Z])*	*Si*
D2	*Contraseña del dominio (Carácter, 5-15,--, [a-z][A-Z] [0-9])*	*Si*
	Nombre de usuario *JRizoG*	*Si*
	Equipo en el que se logeó *cad-p-04*	*Si*
	Fecha y hora *10-04-2012 13:30:04*	*Si*

*Los campos en rojo significa que son los que se registran automáticamente cuando el usuario inicia sesión.

Caso de uso 8 ***(ABML recurso utilizado)***

Dato	Descripción (Tipo, extensión, formato, datos validos)	Requerido
D1	*Asesoría (Campo de selección)*	*No*
D2	*Uso básico (Campo de selección)*	*No*
D3	*Impresión (Campo de selección)*	*No*
D4	*Scanner (Campo de selección)*	*No*
D5	*Quemador de CD (Campo de selección)*	*No*
D6	*Servicios extraordinarios (Campo de selección)*	*No*
D7	*Comentarios (Texto, --,--,[a-z][A-Z] [0-9]y[Caracteres especiales])*	*No*

Flujos de casos de uso

****

Caso de uso 1 (***ABML Usuarios***)

Descripción breve del caso de uso Agregar usuarios

- Todo usuario registrado con permisos de Administrador tiene la capacidad para agregar usuarios en **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se identifica en el Sistema de gestión de asistencias.*	*2*	*Presenta la página principal del sistema.*	
3	*Se ubica en el apartado para agregar un nuevo usuario en el sistema.*	*4*	*Presenta la página de registro de usuarios.*	
5	*Llena el formulario con el nombre de usuario y contraseña para el ingreso al sistema del nuevo usuario.*	*6*	*Verifica que el nombre de usuario no existan en el sistema, se validan los datos del formulario y se completa el registro del usuario, posteriormente se muestra un mensaje: "Registro finalizado".*	*E1-E2-E3*

Descripción breve del caso de uso Borrar usuarios

- Todo usuario registrado con permisos de Administrador tiene la capacidad para Borrar usuarios en **Sistema de gestión de asistencias**.

Administrador		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el usuario que desea eliminar, indicando al sistema que desea borrarlo.*	*2*	*Presenta un mensaje preguntando al usuario: ¿está seguro de que desea eliminar al usuario?*	
3	*Elige la opción de aceptar la eliminación*	*4*	*Manda un mensaje indicando que el usuario ha sido eliminado con éxito.*	

Descripción breve del caso de uso Modificar usuarios

- Todo usuario registrado con permisos de Administrador tiene la capacidad para Modificar usuarios en **Sistema de gestión de asistencias**.

Administrador		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el usuario que desea editar, indicando al sistema que desea modificarlo.*	*2*	*Muestra los campos llenos con la información del usuario a ser editado.*	
3	*Modifica los campos correspondientes, indicando al sistema la edición de los mismos.*	*4*	*Manda un mensaje indicando que la información del usuario fue modificada con éxito, mostrando los datos nuevos del usuario.*	*E1,E2,E3*

Descripción breve del caso de uso Listar usuarios

- Todo usuario registrado tiene la capacidad para Listar usuarios en **Sistema de gestión de asistencias**.

Administrador, Usuario para Consulta		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el usuario que desea mostrar, indicando al sistema que desea listarlo.*	*2*	*Muestra la información del usuario seleccionado.*	

Listado de Excepciones

ID	Tipo	Acción
E1	*Se ingresó uno o más datos incorrectos en el registro del usuario.*	*Mostrar el mensaje "Existe uno o más datos incorrectos". Resaltar los datos incorrectos del formulario.*
E2	*El nombre de usuario para ingresar en el sistema ya existe.*	*Mostrar el mensaje "El nombre de usuario ya está en uso". Muestra nuevamente el formulario para escoger nuevamente el nombre de usuario.*
E3	*La contraseña de usuario es menor de siete caracteres.*	*Mostrar el mensaje "La contraseña tiene menos de siete caracteres". Muestra nuevamente el formulario para escoger nuevamente una contraseña.*

Flujo alternativo

Administrador		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
FA1	*Corrige los datos del formulario que hayan sido marcados como incorrectos, posteriormente le indica al sistema el registro del curso.*	*FA2*	*Se validan los datos del formulario y se completa el registro del curso, posteriormente se muestra un mensaje: "Registro de usuario finalizado".*	*E1,E2,E3*

****

Caso de uso 2 (***Identificar en Aplicación***).

Descripción breve del caso de uso Identificar en Aplicación

- El usuario que desee identificarse en el sistema deberá estar previamente registrado en el sistema y posteriormente indicar la url de acceso al mismo.

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*El usuario indica al sistema que quiere autenticarse en el Sistema de gestión de asistencias.*	2	*Presenta la página de ingreso al sistema.*	
3	*Digita su nombre de usuario y contraseña e indica que quiere autenticarse en el Sistema de gestión de asistencias.*	4	*Valida el nombre de usuario y contraseña e ingresa en el Sistema de gestión de asistencias.*	*E1*

Listado de Excepciones

ID	**Tipo**	**Acción**
E1	*El nombre de usuario o contraseña son incorrectos / no existe el usuario*	*Mostrar el mensaje "El usuario o contraseña son incorrectos". Se limpian las casillas de usuario y contraseña.*

Flujo alternativo

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
FA1	*Corrige los datos del formulario (nombre de usuario y/o contraseña) que hayan sido marcados como incorrectos, posteriormente le indica al sistema el ingreso al mismo.*	*FA2*	*Se validan los datos del formulario dando acceso al sistema al usuario.*	*E1*

****

Caso de uso 3 (***Cerrar sesión en Aplicación***).

Descripción breve del caso de uso Agregar usuarios

- Todo usuario registrado tiene la capacidad para poder cerrar una sesión en el **Sistema de gestión de asistencias**.

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*El usuario le indica al sistema que quiere cerrar sesión.*	2	*Cierra la sesión del usuario y muestra la página principal del sistema con un mensaje de: "Sesión finalizada con éxito".*	

****

Caso de uso 4 (***Mostrar estadísticas***).

Descripción breve del caso de uso Mostrar estadísticas.

- Todo usuario registrado tiene la capacidad para ver las estadísticas de asistencia y uso en el **Sistema de gestión de asistencias**. Las estadísticas pueden darse por mes o por un período en específico dependiendo de las necesidades del usuario.

Caso de uso 4.1 (***Mostrar estadísticas por mes***).

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el apartado de mostrar estadísticas por mes indicando el mes y año del cual está interesado.*	2	*Muestra el número total de asistentes en ese mes y el calendario del mes seleccionado.*	
3	*Indica el día del cual desea revisar la asistencia y uso de recursos.*	4	*Muestra una tabla con la información de los asistentes al centro en el día seleccionado. La información será el nombre del usuario, el departamento al que pertenece y el recurso utilizado.*	

Caso de uso 4.2 (***Mostrar estadísticas por período***).

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el apartado de mostrar estadísticas por período, indicando el mes y año de inicio y el mes y año de fin del período del cual está interesado.*	2	*Muestra una gráfica que indica el número de asistentes durante los meses del período seleccionado y una tabla con los datos graficados.*	*E1*
3	*Puede seleccionar un mes en específico de la gráfica mostrada para ver los detalles de asistencia y uso de recursos durante ese mes.*	4	*Muestra el número total de asistentes en ese mes y el calendario del mes seleccionado.*	
5	*Indica el día del cual desea revisar la asistencia y uso de recursos.*	6	*Muestra una tabla con la información de los asistentes al centro en el día seleccionado. La información será el nombre del usuario, el departamento al que pertenece y el recurso utilizado.*	

Listado de Excepciones

ID	**Tipo**	**Acción**
E1	*Los datos fueron introducidos incorrectamente. Esto sucede si en el período seleccionado, la fecha de inicio es mayor que la fecha fin.*	*Se muestra un mensaje indicando que el período seleccionado es incorrecto.*

Flujo alternativo

Administrador, Usuario para Consulta		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
FA1	*Corrige los datos del periodo.*	*FA2*	*Muestra las gráficas de uso en el período seleccionado además de mostrar una tabla con los datos graficados.*	*E1*

****

Caso de uso 5 (***Exportar estadísticas a Excel***).

Descripción breve del caso de uso Exportar estadísticas a Excel.

- Todo usuario registrado tiene la capacidad para Exportar las estadísticas de asistencia y uso de recursos a Excel en el **Sistema de gestión de asistencias**. Los datos para exportar pueden ser los datos de asistencia y uso de un mes en específico o los datos de asistencia durante un período seleccionado.

Caso de uso 5.1 (***Exportar estadísticas a Excel de mes***).

Administrador, Usuario para Consulta		Sistema de gestión de asistencias		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el apartado de exportar estadísticas que se encuentra en la tabla mostrada en el caso de uso* ***Mostrar estadísticas por mes.***	2	*El sistema abre un archivo en formato de Excel con la información de la tabla que contiene los datos de asistencia y uso de recursos.*	

Caso de uso 5.2 (***Exportar estadísticas a Excel del período***).

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el apartado de exportar estadísticas que se encuentra en la tabla de los datos graficados mostrada en el caso de uso* ***Mostrar estadísticas por período.***	2	*El sistema abre un archivo en formato de Excel con la información de la tabla que contiene los datos de la grafica del período.*	

****

Caso de uso 6 (***ABML asistencia***)

Descripción breve del caso de uso Agregar asistencia.

- La asistencia se registrará de manera automática cuando los usuarios del dominio inicien sesión.

Descripción breve del caso de uso Borrar asistencias

- Todo usuario registrado con permisos de Administrador tienen la capacidad para Borrar asistencias en **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en la asistencia que desea eliminar dentro de la tabla que se genera en el caso de uso (5.1), indicando al sistema que desea borrarla.*	*2*	*Presenta un mensaje preguntando al usuario: ¿está seguro de que desea eliminar el registro?*	
3	*Elige la opción de aceptar la eliminación*	*4*	*Manda un mensaje indicando que la asistencia ha sido eliminada con éxito.*	

Descripción breve del caso de uso Modificar asistencias

- Todo usuario registrado con permisos de Administrador tiene la capacidad para Modificar asistencia en **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en la asistencia que desea modificar dentro de la tabla que se genera en el caso de uso (5.1), indicando al sistema que desea editarla.*	*2*	*Muestra los campos de selección de recursos llenos con la información anteriormente llenada.*	
3	*Modifica los campos correspondientes, indicando al sistema la edición de los mismos.*	*4*	*Se validan los datos del formulario y se completa la modificación de la asistencia, posteriormente se muestra un mensaje: "Asistencia modificada".*	*E1*

Descripción breve del caso de uso Listar usuarios

- Todo usuario registrado tiene la capacidad para Listar usuarios en **Sistema de gestión de asistencias**.

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el día del mes del año del cual se desea listar la asistencia indicando al sistema que desea listarla.*	*2*	*Muestra la tabla de asistencia para el día seleccionado.*	

Listado de Excepciones

ID	Tipo	Acción
E1	*No ingresó el recurso utilizado*	*Mostrar el mensaje "Favor de ingresar el o los recursos utilizados". Resaltar los datos incorrectos del formulario.*

Flujo alternativo

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
FA1	*Ingresar el recurso utilizado e indicar al sistema la edición.*	*FA2*	*Se validan los datos del formulario y se completa la modificación de la asistencia, posteriormente se muestra un mensaje: "Asistencia modificada".*	*E1*

****

Caso de uso 7 (***ABML recurso***)

Descripción breve del caso de uso Agregar recurso

- Todo usuario registrado tienen la capacidad para agregar recursos en **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el apartado para agregar un nuevo recurso en el sistema.*	*2*	*Presenta la página de registro de recursos.*	
3	*Llena el formulario con el nombre del recurso a ser agregado, posteriormente le indica al sistema que desea agregarlo.*	*4*	*Se validan los datos del formulario y se completa el registro del nuevo recurso, posteriormente se muestra un mensaje: "Recurso agregado con éxito".*	*E1-E2*

Descripción breve del caso de uso Borrar recurso

- Todo usuario registrado tienen la capacidad para Borrar recursos en **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el recurso que desea eliminar,* *indicando al sistema que desea borrarlo.*	*2*	*Presenta un mensaje preguntando al usuario: ¿está seguro de que desea eliminar el recurso?*	
3	*Elige la opción de aceptar la eliminación*	*4*	*Manda un mensaje indicando que el recurso ha sido eliminado con éxito.*	

Descripción breve del caso de uso Modificar recursos

- Todo usuario registrado tienen la capacidad para Modificar recursos en el **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el recurso que desea editar, indicando al sistema que desea modificarlo.*	*2*	*Muestra los campos llenos con la información del recurso a ser editado.*	
3	*Modifica los campos correspondientes, indicando al sistema la edición de los mismos.*	*4*	*Manda un mensaje indicando que la información del recurso fue modificada con éxito, mostrando los datos nuevos del recurso.*	*E1,E2*

Descripción breve del caso de uso Listar recursos

- Todo usuario registrado tienen la capacidad para Listar recursos en **Sistema de gestión de asistencias**.

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en el recurso que desea mostrar,* *indicando al sistema que desea listarlo.*	*2*	*Muestra la información del recurso seleccionado.*	

Listado de Excepciones

ID	Tipo	Acción
E1	*Se ingresó uno o más datos incorrectos en el registro del usuario.*	*Mostrar el mensaje "Existe uno o más datos incorrectos". Resaltar los datos incorrectos del formulario.*
E2	*El nombre del recurso para ingresar en el sistema ya existe.*	*Mostrar el mensaje "El nombre de recurso ya está en uso". Muestra nuevamente el formulario para escoger nuevamente el nombre de recurso.*

Flujo alternativo

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
FA1	*Corrige los datos del formulario que hayan sido marcados como incorrectos, posteriormente le indica al sistema el registro del recurso.*	*FA2*	*Se validan los datos del formulario y se completa el registro del recurso, posteriormente se muestra un mensaje: "Registro de recurso finalizado".*	*E1,E2*

****

Caso de uso 8 (***AML recurso utilizado***)

Descripción breve del caso de uso Agregar recurso utilizado

- Todo usuario que inicia sesión en el dominio tiene la capacidad para agregar recursos utilizados en **Sistema de gestión de asistencias**.

Usuario del Dominio		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Cierra su sesión en el dominio.*	*2*	*Muestra la interfaz para indicar que recursos fueron utilizados por el usuario.*	
3	*Selecciona la(s) opción(es) del(os) recurso(s) utilizado(s).*	*4*	*Se validan los datos del formulario y se completa el registro del recurso utilizado, posteriormente se muestra un mensaje: "Gracias por su visita al CAD, vuelva pronto".*	

Descripción breve del caso de uso Modificar recursos utilizados.

- Todo usuario registrado tienen la capacidad para Modificar recursos en el **Sistema de gestión de asistencias**.

Administrador		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en la opción de Servicio Utilizado por Usuario indicando al sistema que desea ver algún dato.*	*2*	*Muestra un apartado donde se puede seleccionar el usuario y la fecha de interés.*	
3	*Selecciona el usuario y el día de interés y le indica al sistema que desea ver los recursos utilizados en dicho día.*	*4*	*Muestra los recursos que el usuario utilizó el día seleccionado con opción para poder modificar.*	*E1,E2*
5	*Se ubica en la opción de modificar. Le indica al sistema que desea modificar.*	*5*	*Muestra el formulario con los campos llenos con la información correspondiente.*	
6	*Modifica la información y le indica al sistema que desea guardar los cambion*	*7*	*Se validan los datos del formulario y se completa la edición del o los recursos utilizados, posteriormente se muestra un mensaje: "Información editada con éxito".*	

Descripción breve del caso de uso Listar recursos utilizados.

- Todo usuario registrado tienen la capacidad para Listar recursos utilizados en **Sistema de gestión de asistencias**.

Administrador, Usuario para Consulta		**Sistema de gestión de asistencias**		
Paso	**Acción**	**Paso**	**Acción**	**Excepción**
1	*Se ubica en la opción de Servicio Utilizado por Usuario indicando al sistema que desea ver algún dato.*	*2*	*Muestra un apartado donde se puede seleccionar el usuario y la fecha de interés.*	
3	*Selecciona el usuario y el día de interés y le indica al sistema que desea ver los recursos utilizados en dicho día.*	*4*	*Muestra los recursos que el usuario utilizó el día seleccionado.*	

REGLAMENTO DE SEGURIDAD DEL DOMINIO.

1.- La primera vez que un usuario se autentique en el dominio, el sistema pedirá cambiar su contraseña de inicio de sesión por una nueva, la cual deberá ser de mínimo 8 caracteres sin importar mayúsculas, minúsculas y números. Esta contraseña debe ser correctamente resguardada por el usuario ya que es su clave para acceder a los equipos y a su información.

2.- Los usuarios deben cerrar su sesión de dominio cuando hayan terminado de utilizar algún equipo, esto evitará la posibilidad de que otros usuarios accedan a información de terceros.

3.- Al finalizar una sesión el sistema mostrará una interfaz en donde el usuario deberá registrar los recursos que utilizó durante su estancia en el centro, las posibles opciones a elegir serán: impresión a color, impresión en blanco y negro, scanner y grabado de discos, junto con sus respectivos campos para indicar la cantidad de uso de cada uno de ellos.

4.- Queda prohibido a los usuarios intentar modificar los archivos contenidos en la carpeta Windows del sistema.

5.- Los usuarios autenticados en el dominio pueden guardar archivos en la carpeta Mis documentos contenida en el sistema, los cuales podrán ser vistos en cualquier equipo del dominio por el propietario de los mismos. Sólo se permiten 10GB de espacio en disco por usuario para la carpeta documentos. Esta información será depurada cada semestre por lo que los usuarios deberán hacer un respaldo de los datos que consideren importantes.

6.- Se pide a los usuarios evitar dejar los equipos en donde están trabajando con la sesión abierta. Sin embargo, para reducir riesgos con la información, después de 5 minutos de inactividad en algún equipo del dominio, se bloqueará automáticamente la sesión que haya sido iniciada por algún usuario y se solicitará nuevamente la contraseña para poder acceder a la información.

7.- Los usuarios solamente pueden imprimir un máximo de 40 hojas a blanco y negro y 5 hojas a color por día.

8.- La instalación de software sólo será realizada por personas autorizadas en el dominio, la mayoría del software estará disponible en la red. Si algún usuario necesitara de algún programa en específico deberá notificarlo a los administradores de la red quienes se encargarán de la instalación.

9.- La asistencia al centro será registrada automáticamente cuando un usuario inicie sesión en cualquier equipo del dominio. De esta manera ya no será necesario que registren la asistencia manualmente como se hacía anteriormente.

10.- Los usuarios deben escanear las memorias USB u otros dispositivos de almacenamiento que utilicen, antes de utilizarlos en los equipos para evitar la contaminación de los mismos, que puedan generar algún daño en el funcionamiento o pérdidas de información.

11.- Queda prohibido compartir entre usuarios las contraseñas de acceso a los equipos con la finalidad de evitar problemas con la información. Todos los usuarios autorizados tendrán sus propios datos de acceso, por lo que cada quien será responsable de ellos y del uso que se les dé.

IMPLEMENTACIÓN DEL DOMINIO

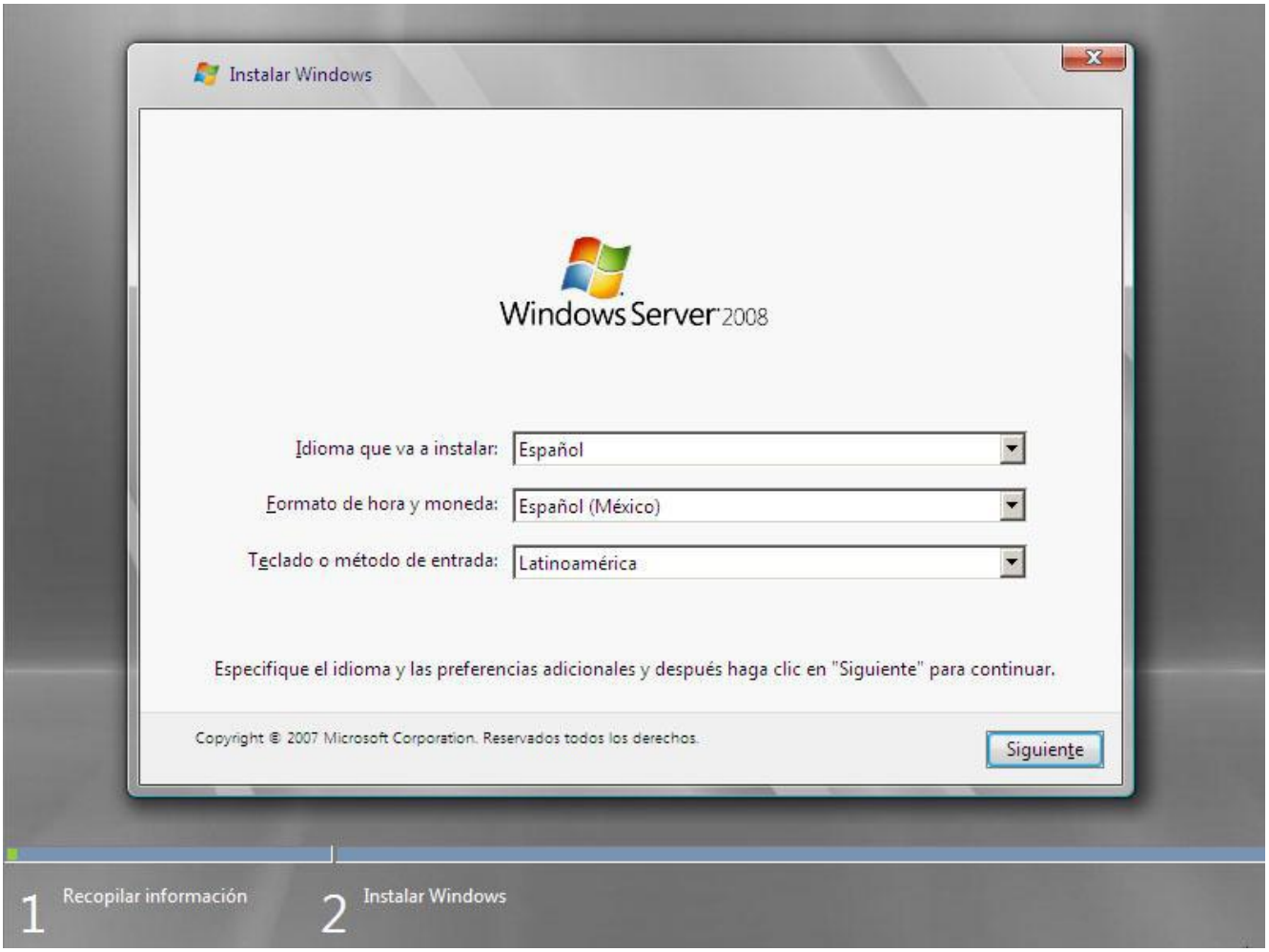
En este anexo se explica cómo se realizó la implementación completa del dominio de red del CAD. Se explica desde la instalación del sistema operativo Windows Server, la configuración de los servicios necesarios del DNS, Directorio Activo, la creación y manejo de usuarios y la creación de las políticas de grupo.

En primer lugar se muestra cómo se realizó la instalación del sistema operativo, este programa se obtuvo desde Hábitat Puma gracias a la colaboración del prestador de servicio social Abelardo Adalberto Jimenez a quien se le agradece por su apoyo.

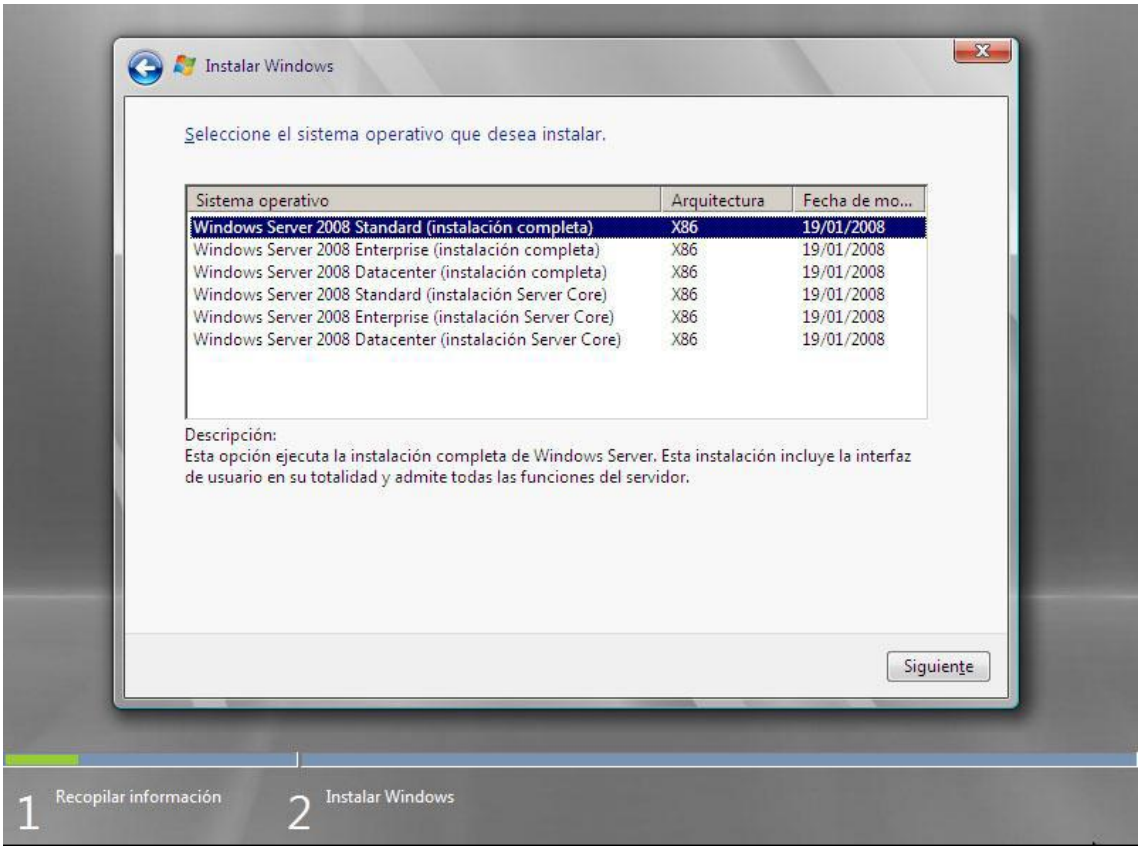
INSTALACIÓN WINDOWS SERVER.

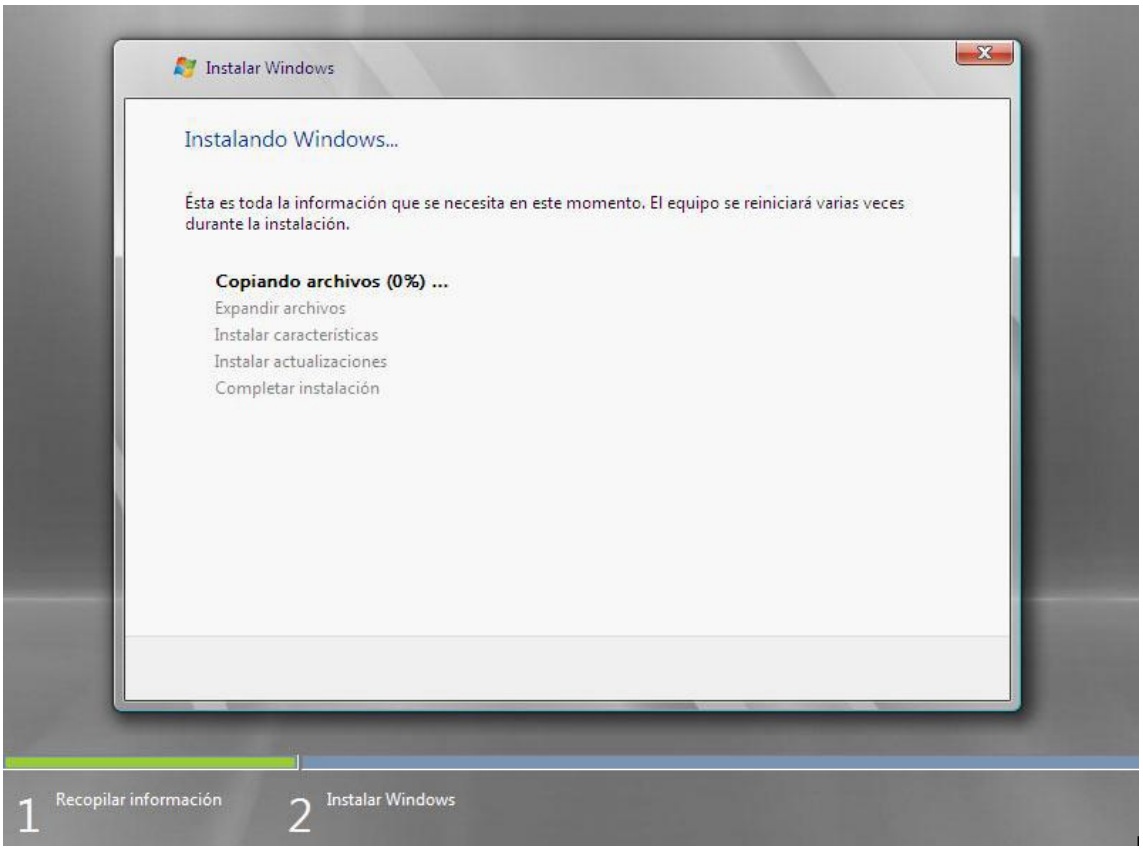
Después de iniciar el equipo servidor con el disco de instalación del sistema operativo, aparece la primera ventana del asistente de instalación en la que se pide:

Elegir el idioma, el formato de hora y el tipo de teclado que tendrá el sistema operativo.



Posteriormente se elige la versión del sistema, para este caso se instaló la versión Estándar.

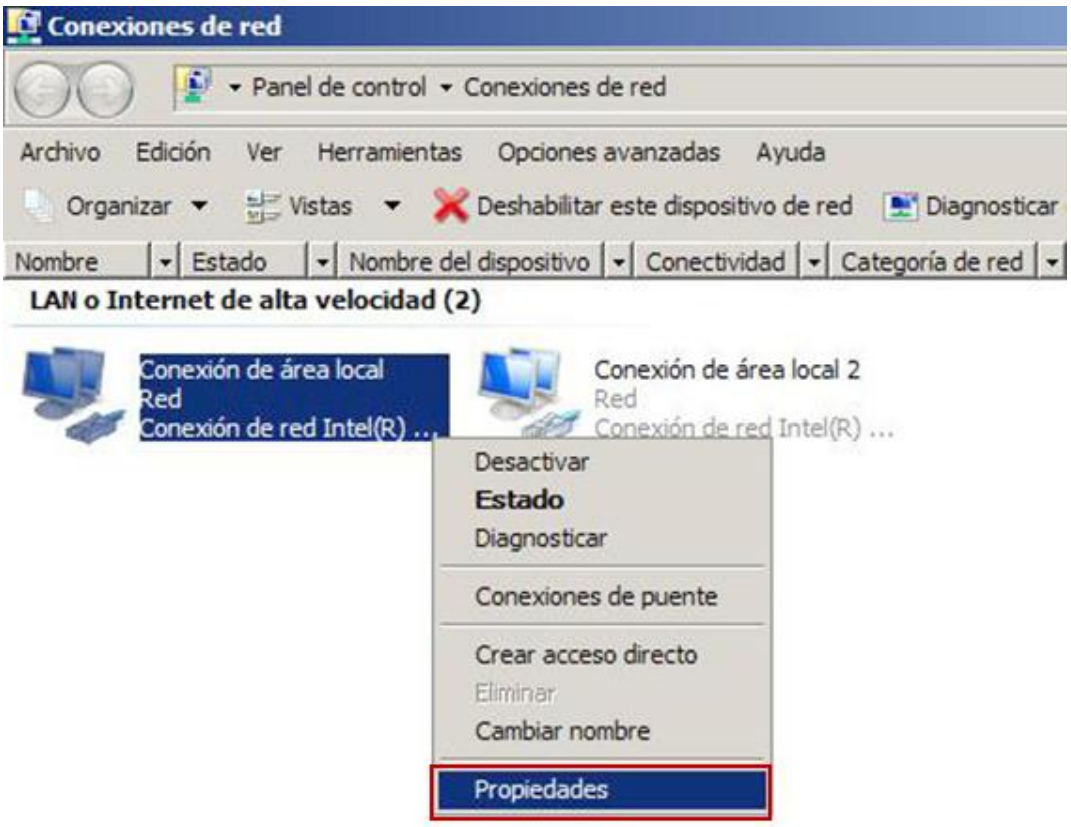




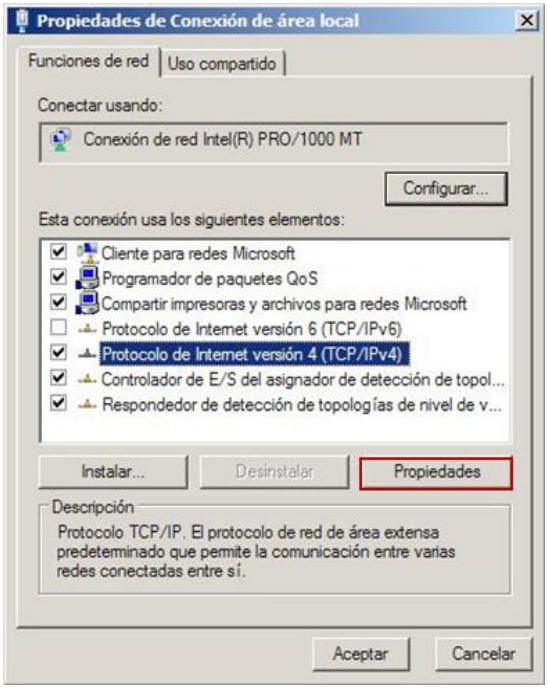
Una vez instalado el sistema operativo, se procede hacer la configuración de los parámetros de red para que el equipo servidor quede listo para instalar los servicios necesarios.

Para acceder a las propiedades de la tarjeta de red y configurar los parámetros, en **Inicio** dar clic en **Panel de Control**. En **Centro de redes y recursos compartidos** dar doble clic, hacer clic en **Conexiones de red**. En esta ventana se muestran las tarjetas de red de la computadora; elegir la tarjeta a configurar.

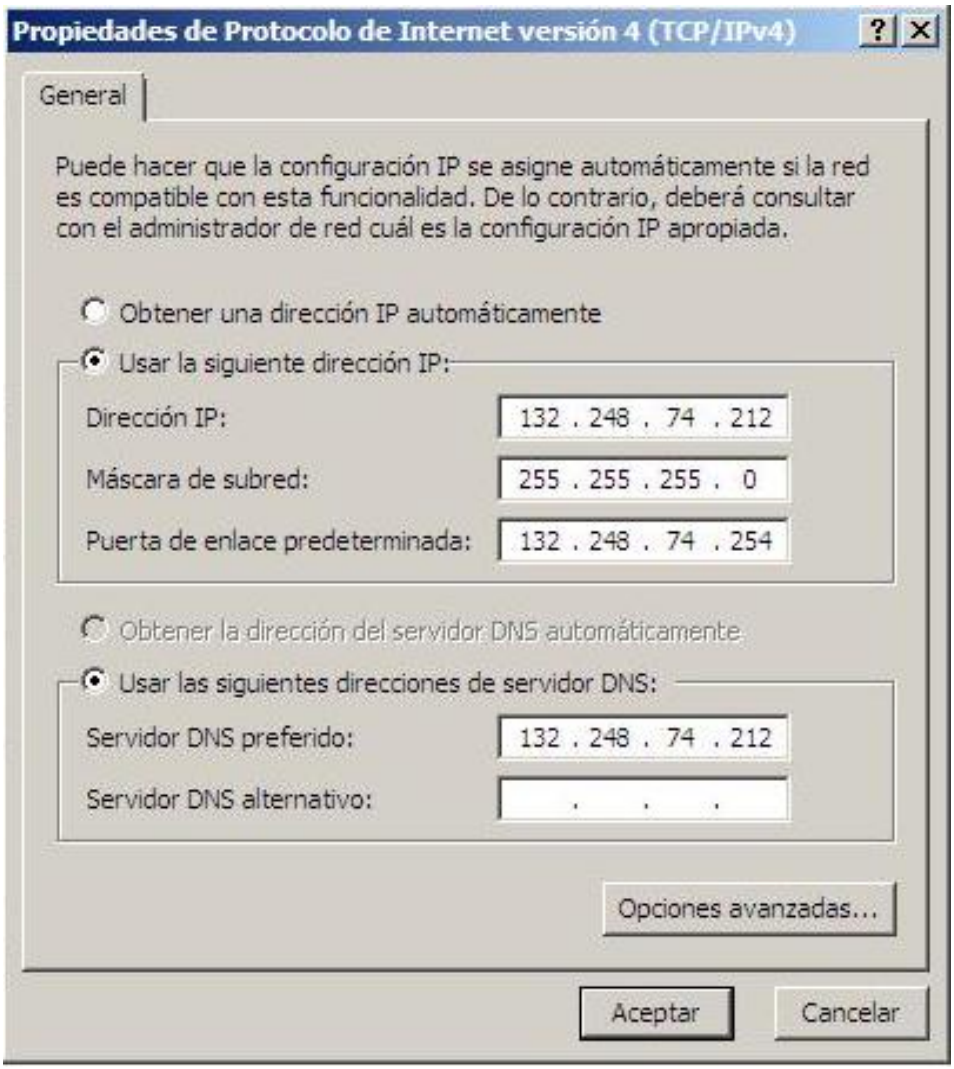
Seleccionar la tarjeta de red, dar clic con el botón derecho del mouse y dar clic en la opción de Propiedades.



En la ventana de propiedades de conexión de área local se deshabilita el protocolo IPv6 ya que no se va a hacer uso de él.
Seleccionar el elemento Protocolo de Internet versión 4 (TCP/IPv4), dar clic en el botón Propiedades.

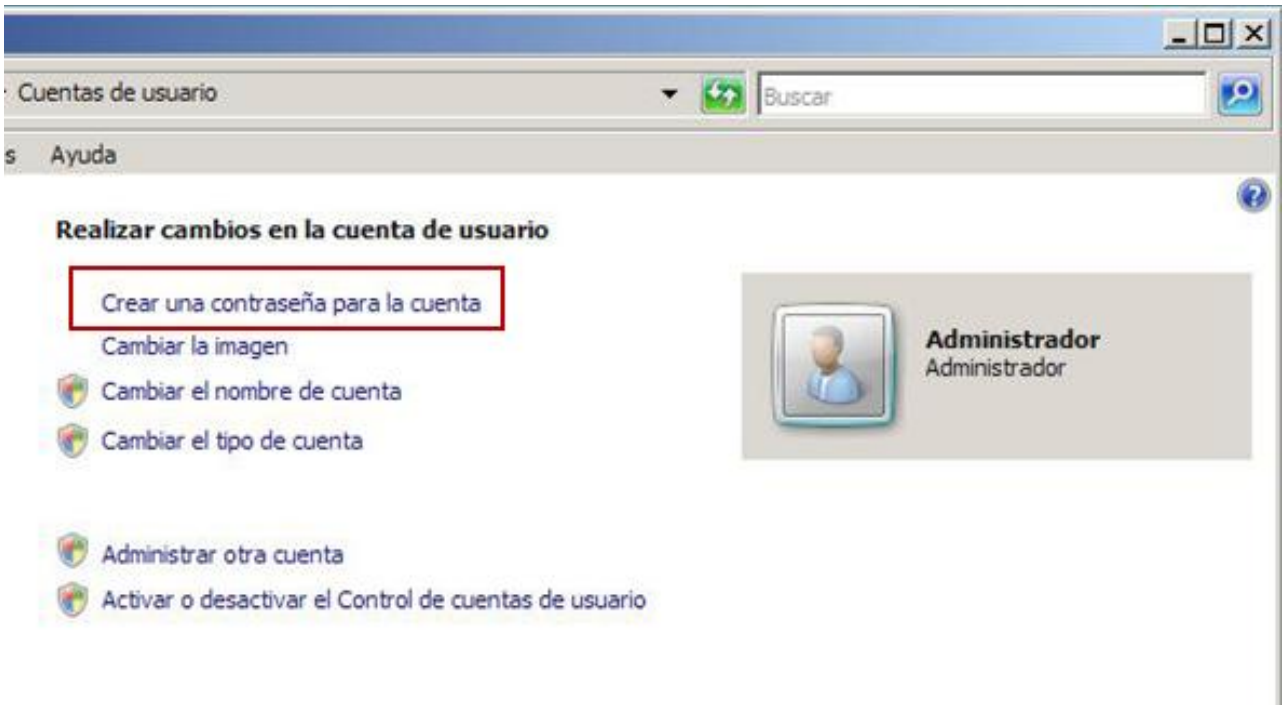


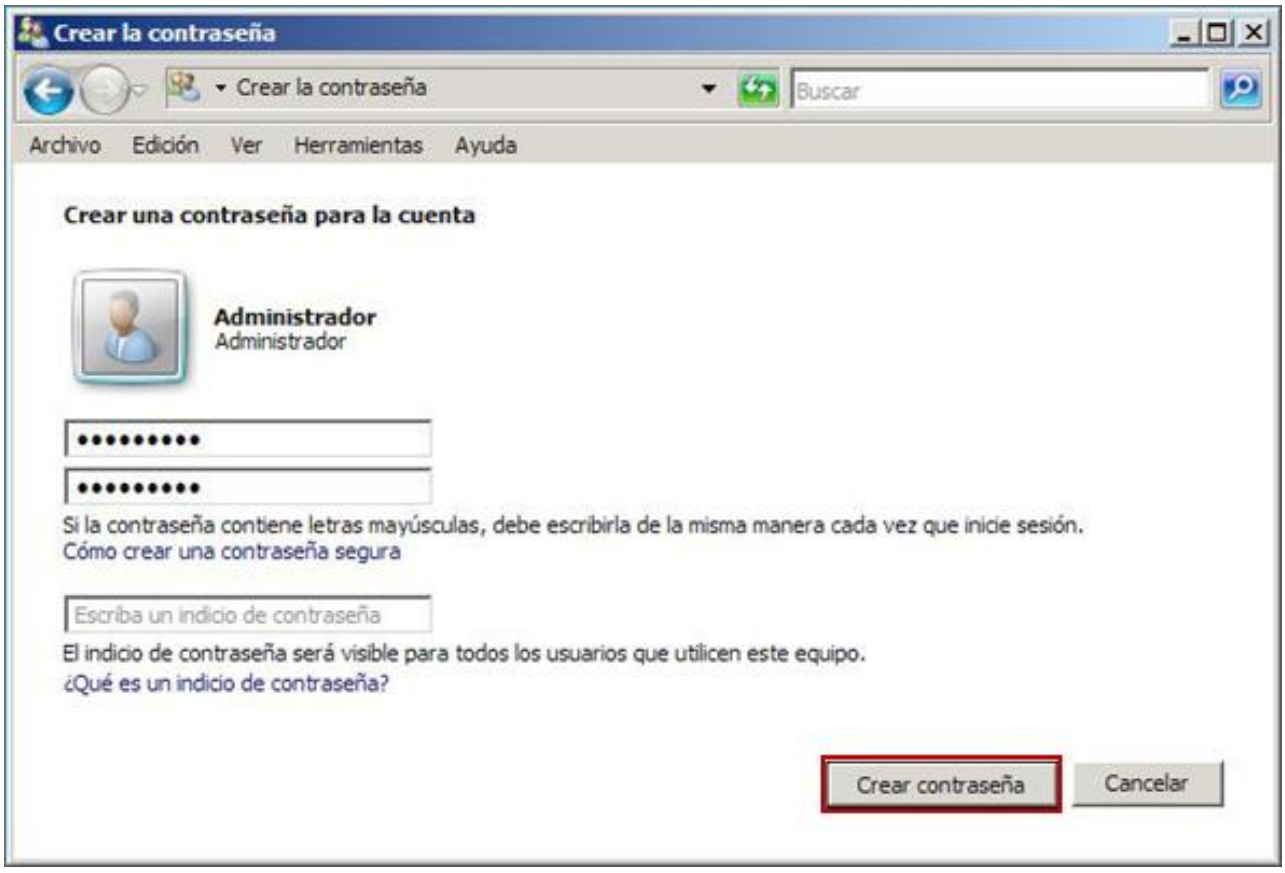
En esta ventana, se configura la tarjeta de red, se asigna una dirección IP, una máscara de subred, el Gateway, y como DNS se coloca la dirección de Loop Back, debido a que el mismo servidor resolverá las consultas al DNS.



Una vez realizada esta configuración se establece la contraseña que tendrá el servidor de la siguiente manera:

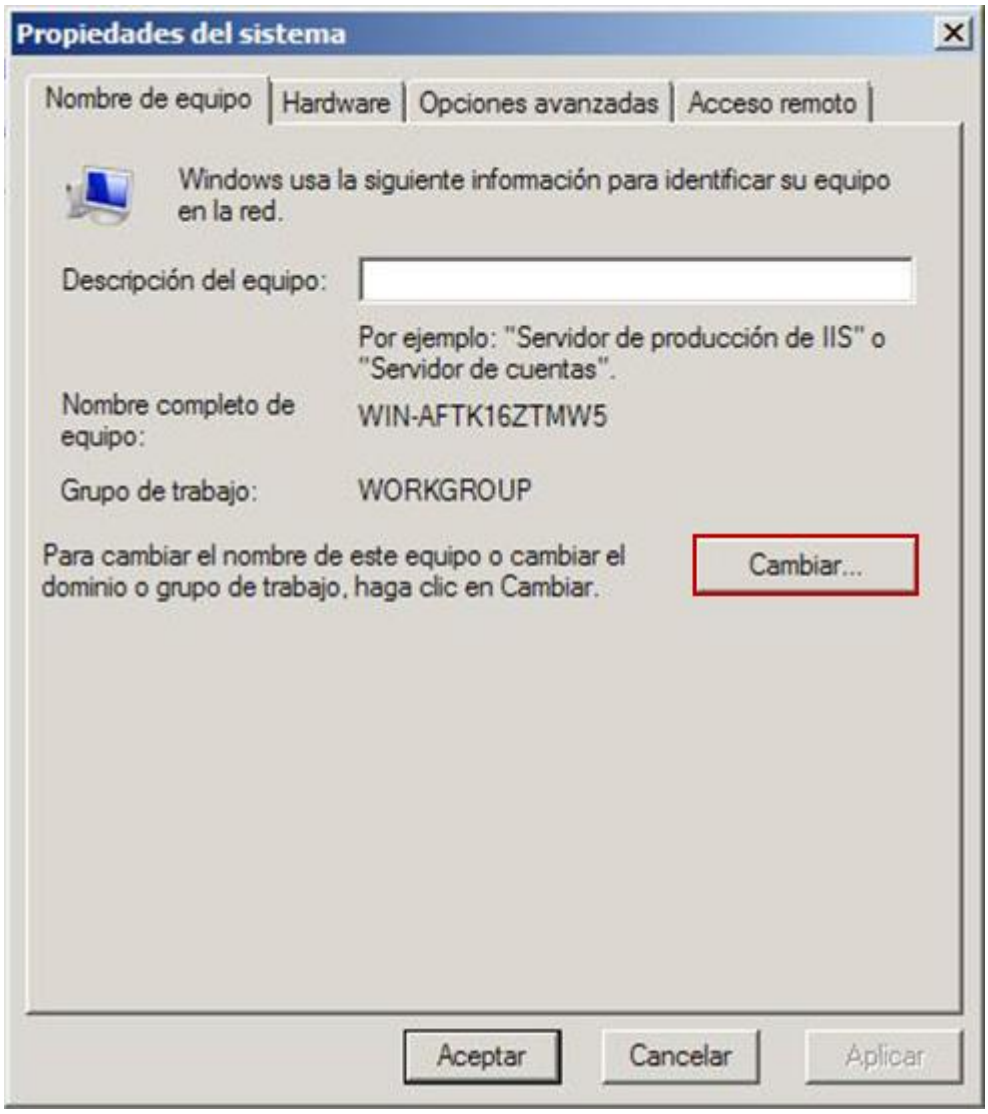
Para configurar la contraseña, en Inicio dar clic en Panel de Control. En Cuentas de usuario dar doble clic, hacer clic en Crear una contraseña para la cuenta.



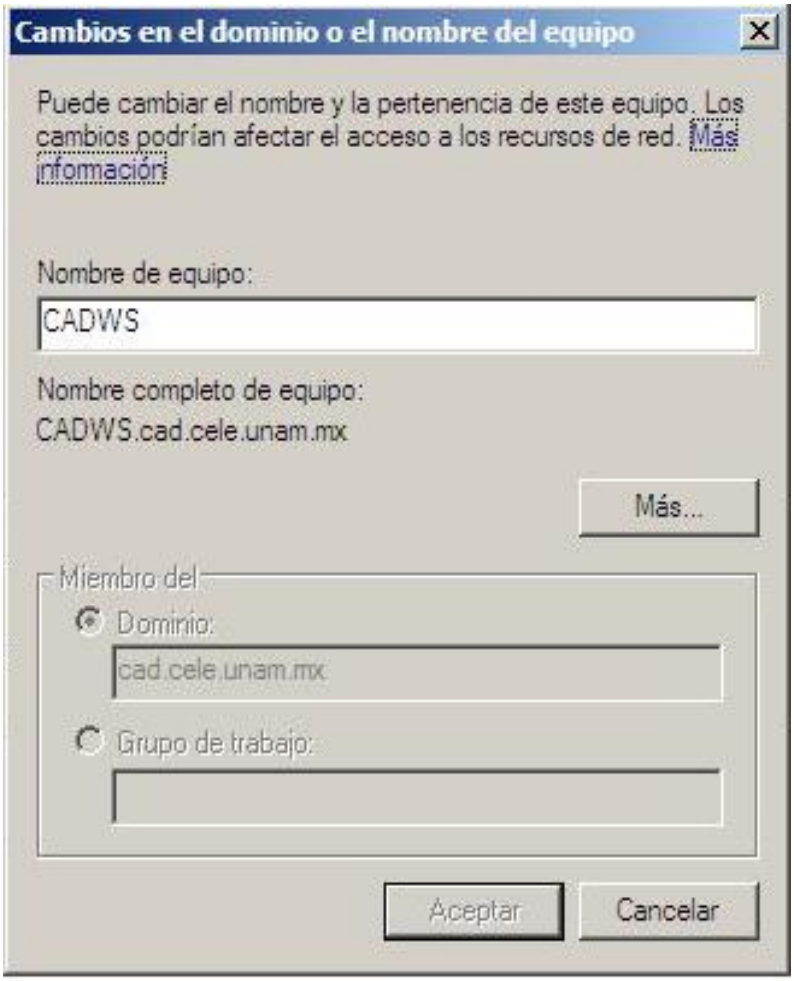


Antes de instalar los servicios necesarios en Windows Server 2008, se requiere configurar tanto el nombre del equipo como el nombre de dominio.

Para configurar el nombre del equipo, en Inicio dar clic en Panel de Control. En Sistema dar doble clic, hacer clic en Cambiar configuración; en la ventana Propiedades del Sistema dar clic en el botón Cambiar.


Propiedades del sistema
Nombre de equipo
Hardware
Opciones avanzadas
Acceso remoto
Windows usa la siguiente información para identificar su equipo en la red.
Descripción del equipo:
Por ejemplo: "Servidor de producción de IIS" o "Servidor de cuentas".
Nombre completo de equipo:
WIN-AFTK16ZTMW5
Grupo de trabajo:
WORKGROUP
Para cambiar el nombre de este equipo o cambiar el dominio o grupo de trabajo, haga clic en Cambiar.
Cambiar...
Aceptar
Cancelar
Aplicar

En la ventana Cambios en el dominio o el nombre del equipo, colocar el nombre del equipo deseado. Seleccionar la opción de Dominio e ingresar el nombre correspondiente, es decir, “cad.cele.unam.mx”.

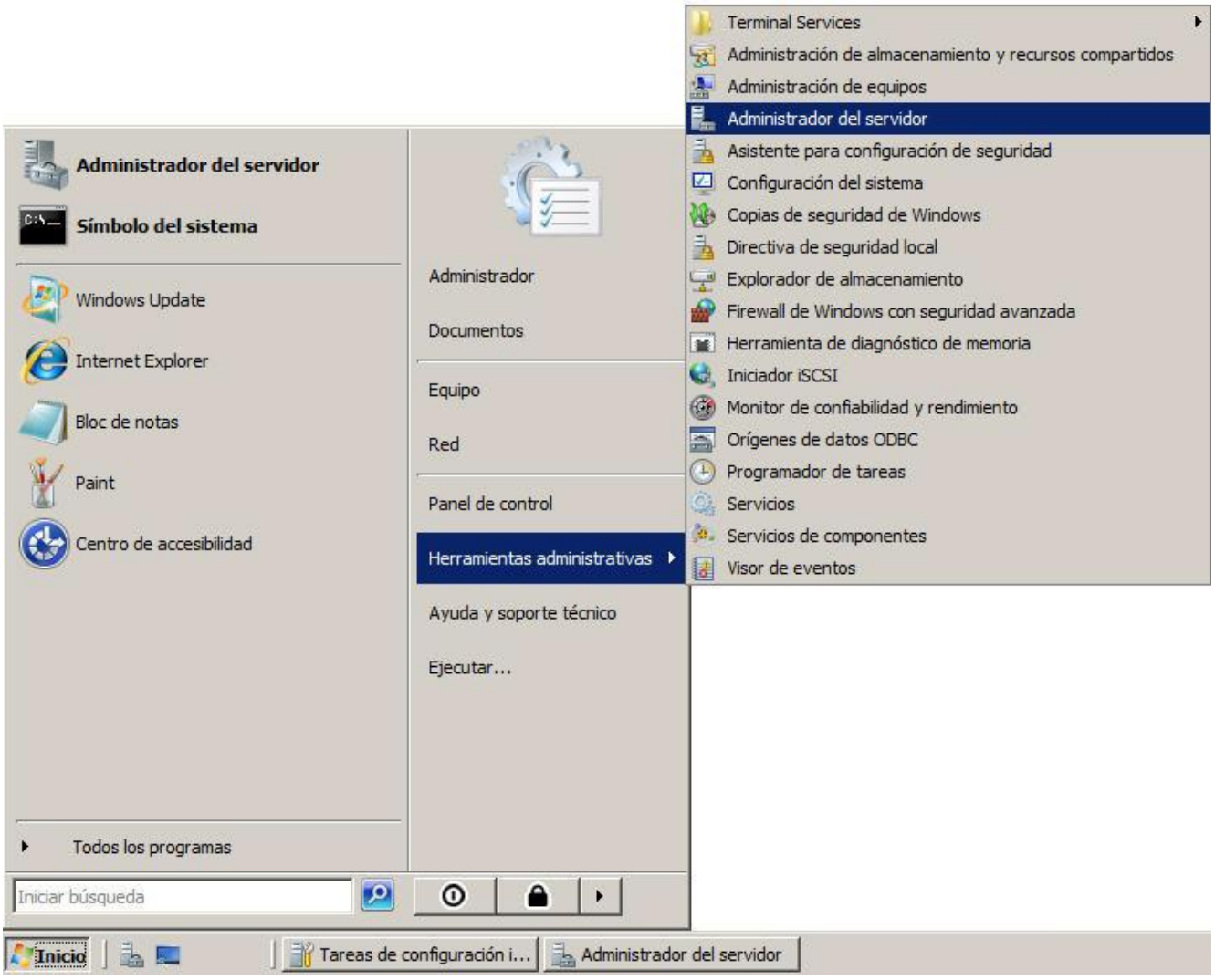


Después de hacer las configuraciones, el sistema se reiniciará.

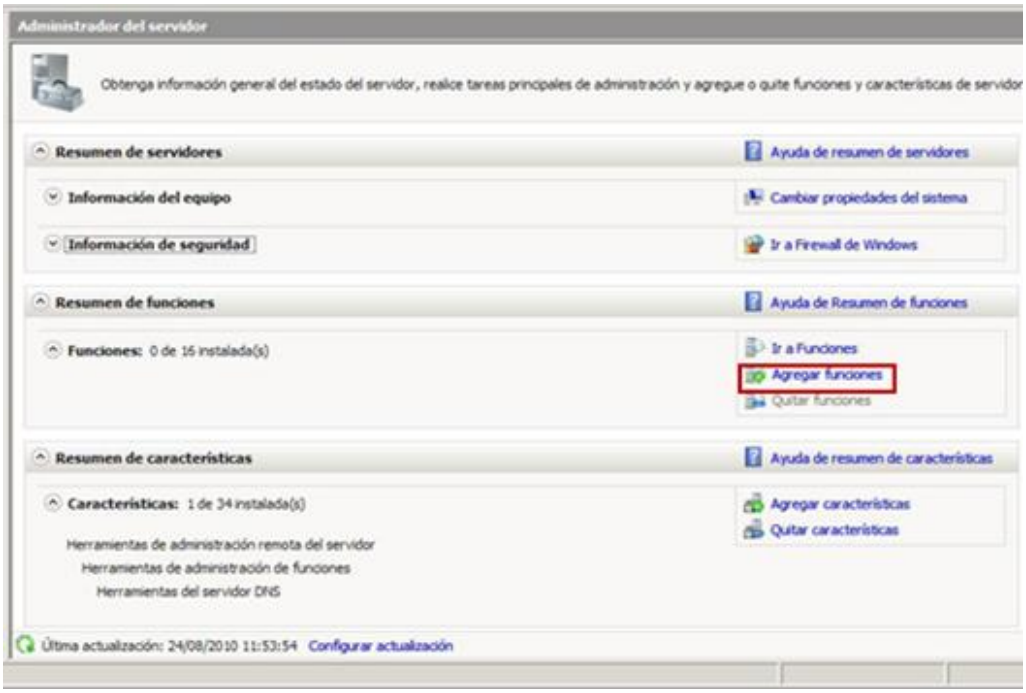
Después de que el sistema se ha reiniciado, para iniciar sesión en el equipo, se pedirá la contraseña establecida en pasos anteriores. Una vez que se ingresan las credenciales de acceso, se procede a hacer la instalación y configuración del Servicio DNS.

INSTALACIÓN DEL SERVIDOR DNS.

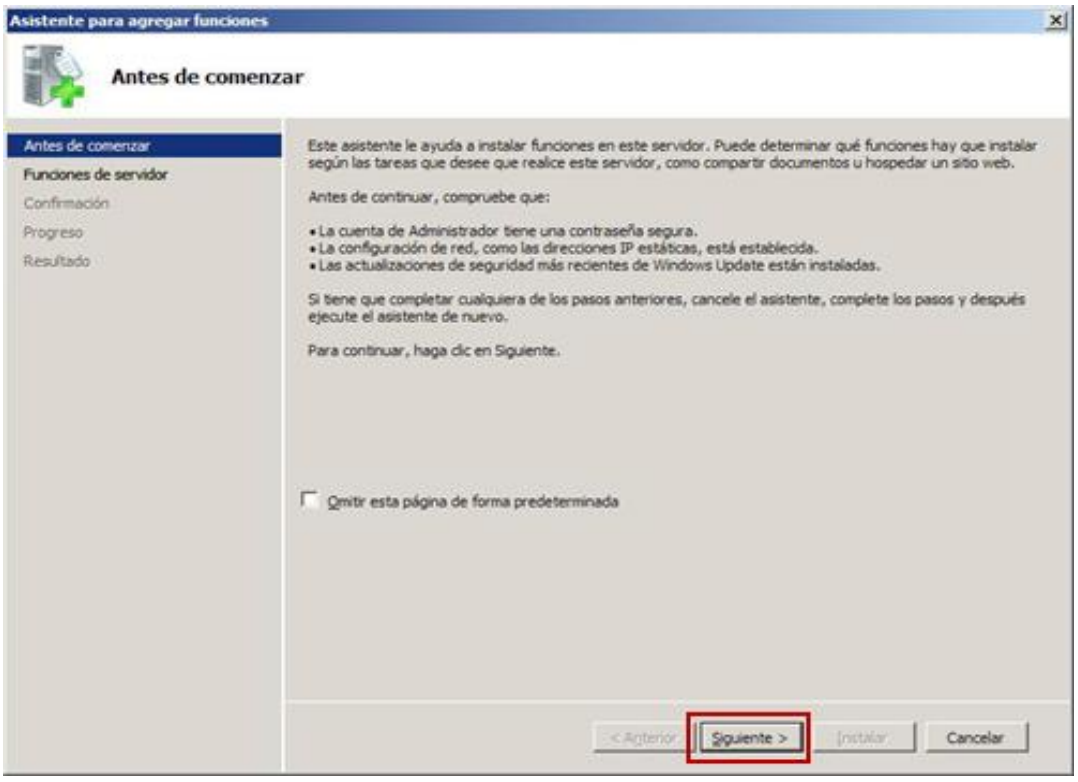
En Inicio, dar clic en Herramientas Administrativas, se mostrará un panel en donde se encuentran el acceso a las Características y Funciones (Roles) disponibles en Windows Server 2008, dar clic en Administrador del Servidor.



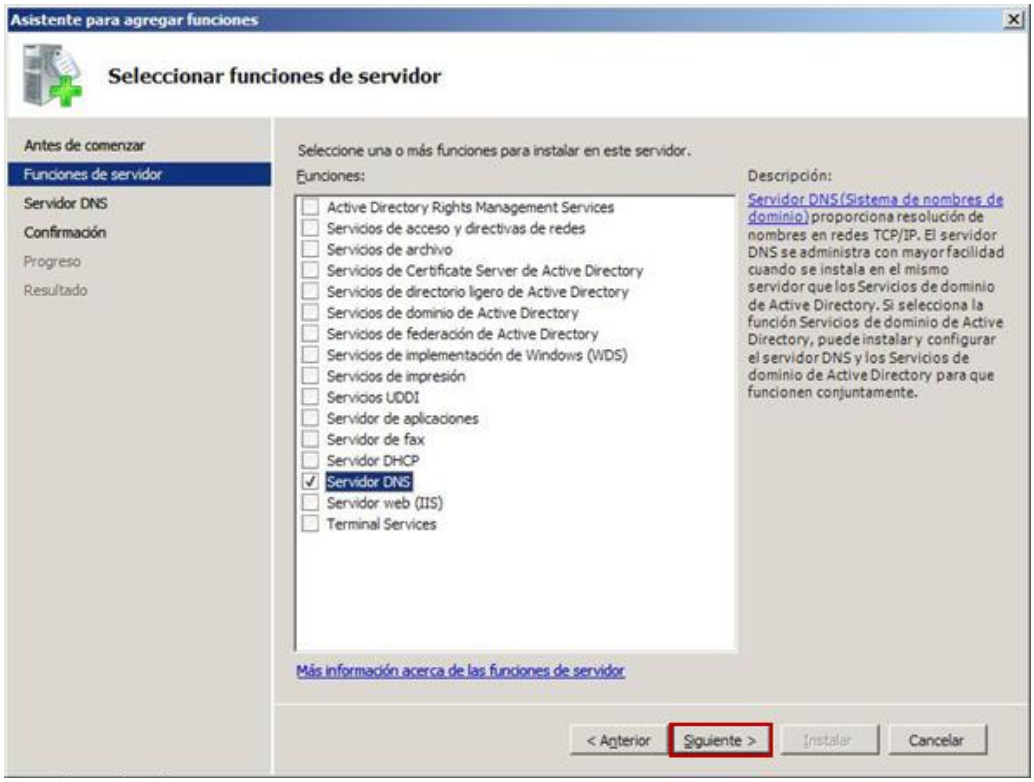
En esta ventana se encuentra el resumen con las Características y Funciones disponibles para Windows Server 2008. Dar clic en Agregar Funciones.

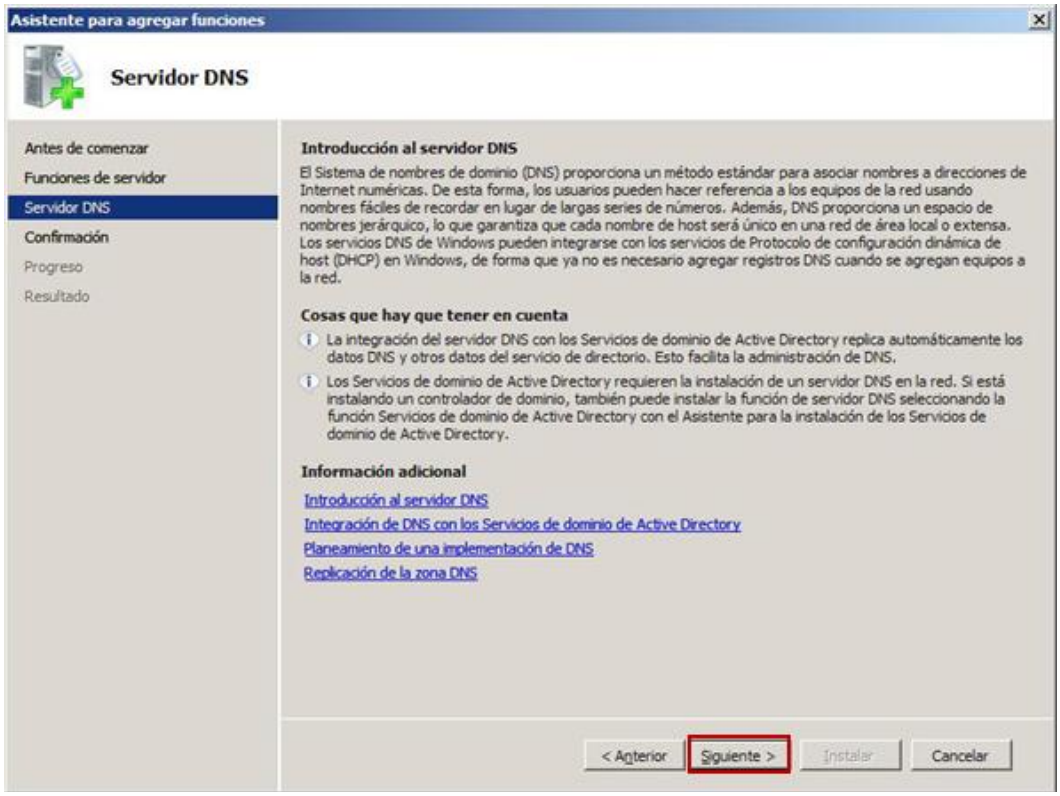


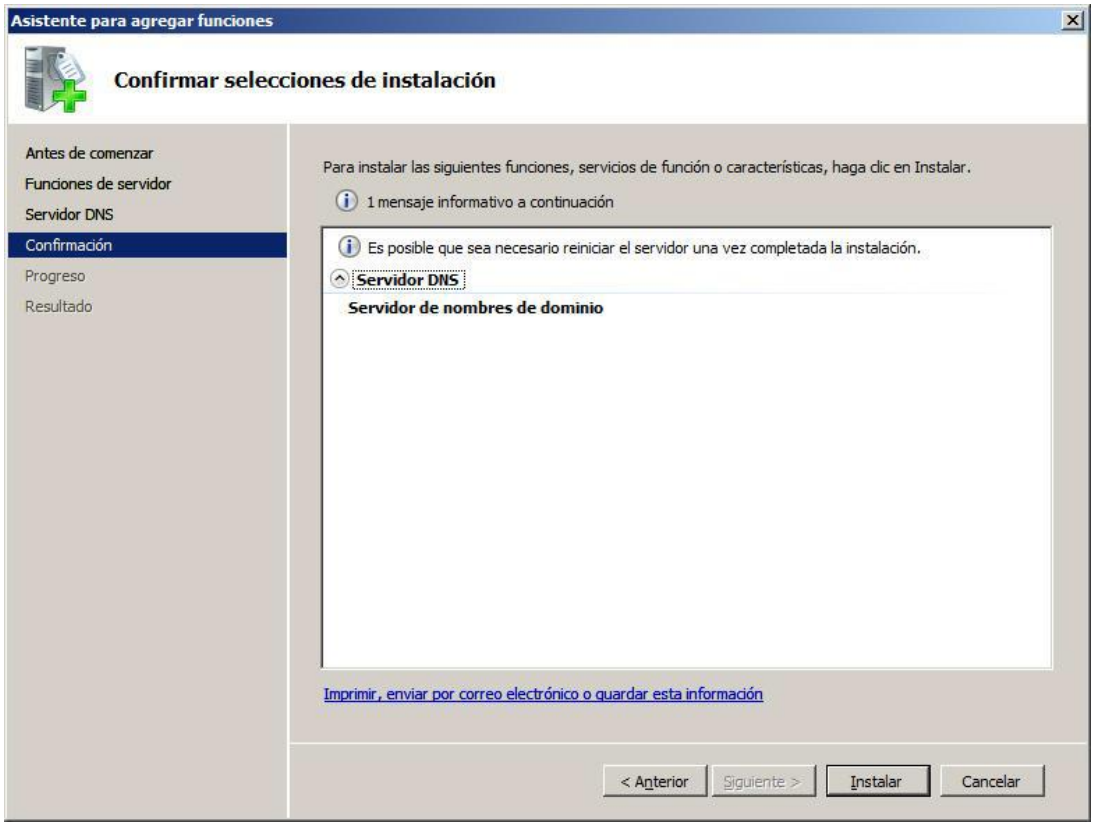
Aparece el Asistente para agregar funciones, dar clic en Siguiente

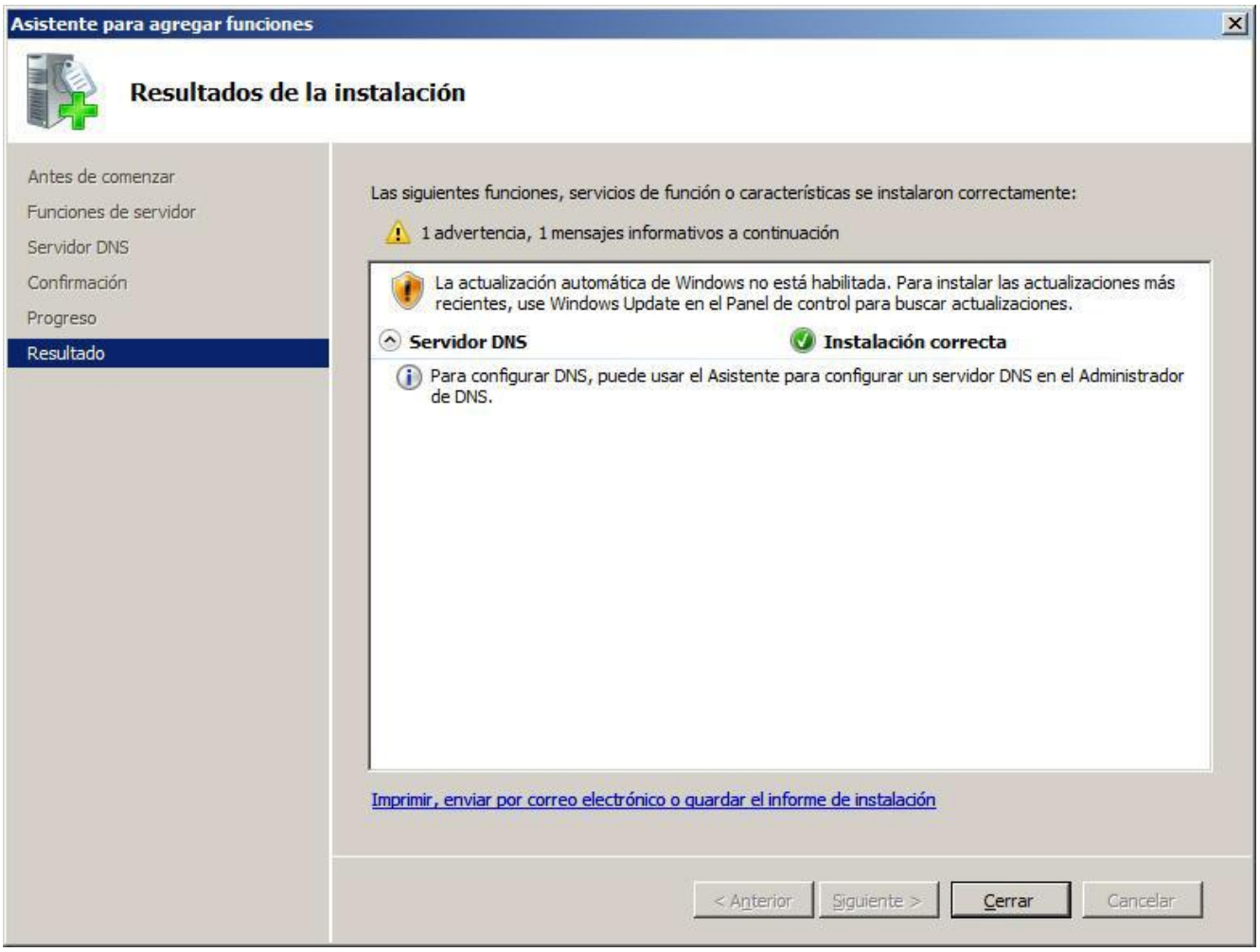


Se elige la función de Servidor DNS, dar clic en Siguiente y seguir las instrucciones del asistente.

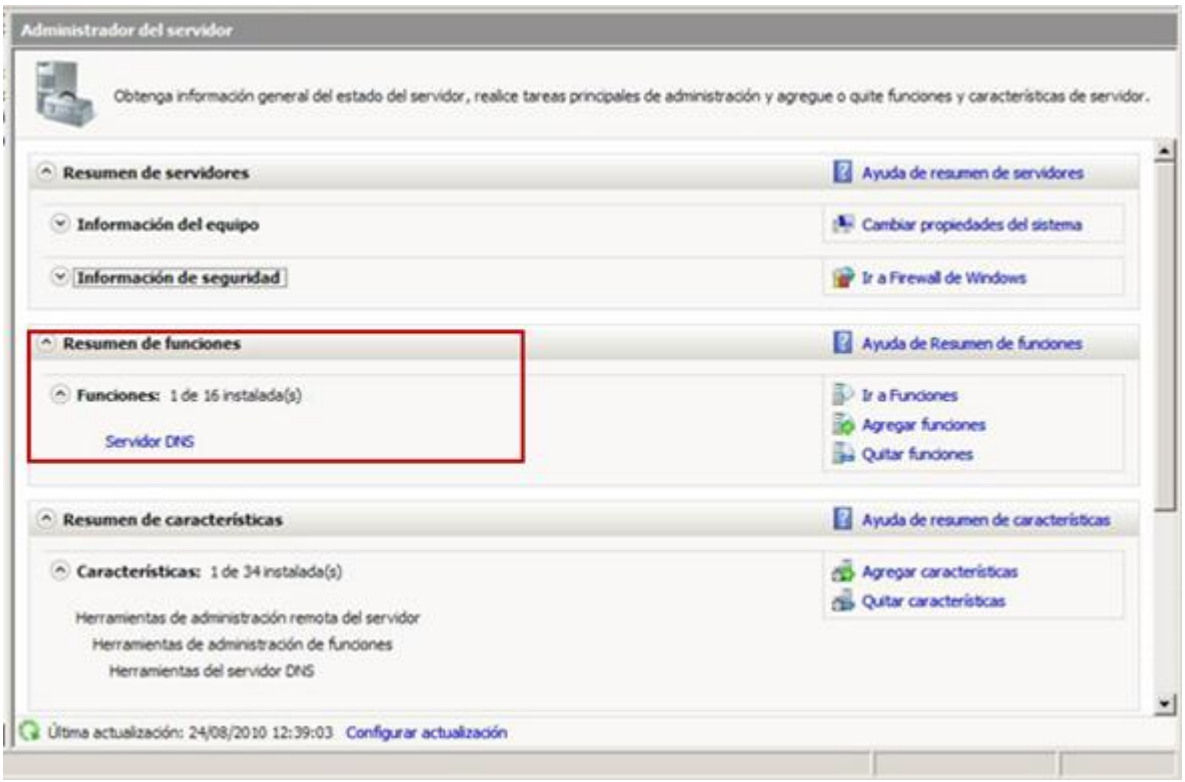



Asistente para agregar funciones
Servidor DNS
Antes de comenzar
Funciones de servidor
Servidor DNS
Confirmación
Progreso
Resultado
Introducción al servidor DNS
El Sistema de nombres de dominio (DNS) proporciona un método estándar para asociar nombres a direcciones de Internet numéricas. De esta forma, los usuarios pueden hacer referencia a los equipos de la red usando nombres fáciles de recordar en lugar de largas series de números. Además, DNS proporciona un espacio de nombres jerárquico, lo que garantiza que cada nombre de host será único en una red de área local o extensa. Los servicios DNS de Windows pueden integrarse con los servicios de Protocolo de configuración dinámica de host (DHCP) en Windows, de forma que ya no es necesario agregar registros DNS cuando se agregan equipos a la red.
Cosas que hay que tener en cuenta
La integración del servidor DNS con los Servicios de dominio de Active Directory replica automáticamente los datos DNS y otros datos del servicio de directorio. Esto facilita la administración de DNS.
Los Servicios de dominio de Active Directory requieren la instalación de un servidor DNS en la red. Si está instalando un controlador de dominio, también puede instalar la función de servidor DNS seleccionando la función Servicios de dominio de Active Directory con el Asistente para la instalación de los Servicios de dominio de Active Directory.
Información adicional
Introducción al servidor DNS
Integración de DNS con los Servicios de dominio de Active Directory
Planeamiento de una implementación de DNS
Replicación de la zona DNS
< Anterior
Siguiente >
Instalar
Cancelar


Asistente para agregar funciones
Confirmar selecciones de instalación
Antes de comenzar
Funciones de servidor
Servidor DNS
Confirmación
Progreso
Resultado
Para instalar las siguientes funciones, servicios de función o características, haga clic en Instalar.
1 mensaje informativo a continuación
Es posible que sea necesario reiniciar el servidor una vez completada la instalación.
Servidor DNS
Servidor de nombres de dominio
Imprimir, enviar por correo electrónico o guardar esta información
< Anterior
Siguiente >
Instalar
Cancelar

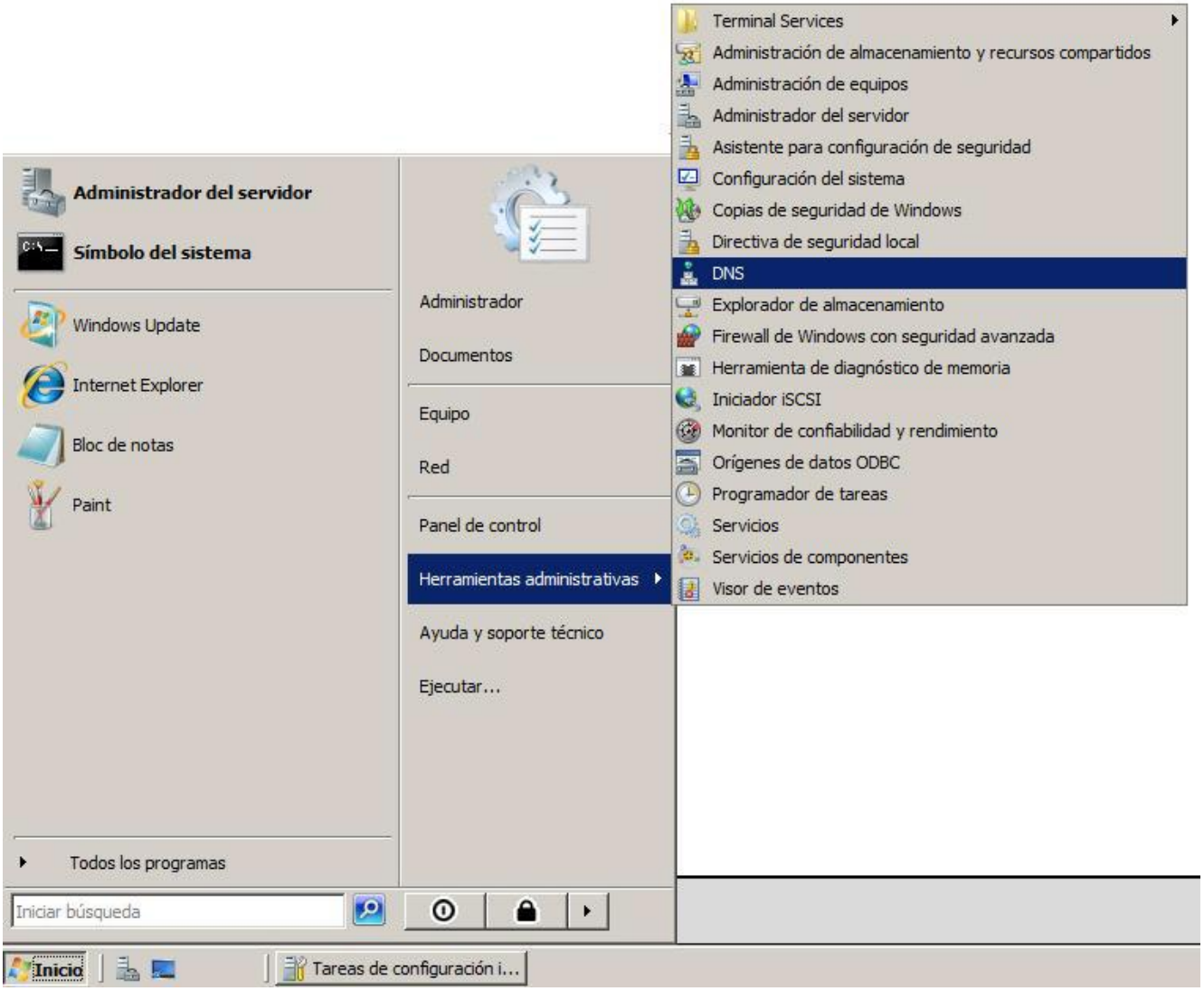


Una vez instalado el servicio, en la ventana de Administrador del servidor, aparecerá agregada la nueva función de Servidor DNS.

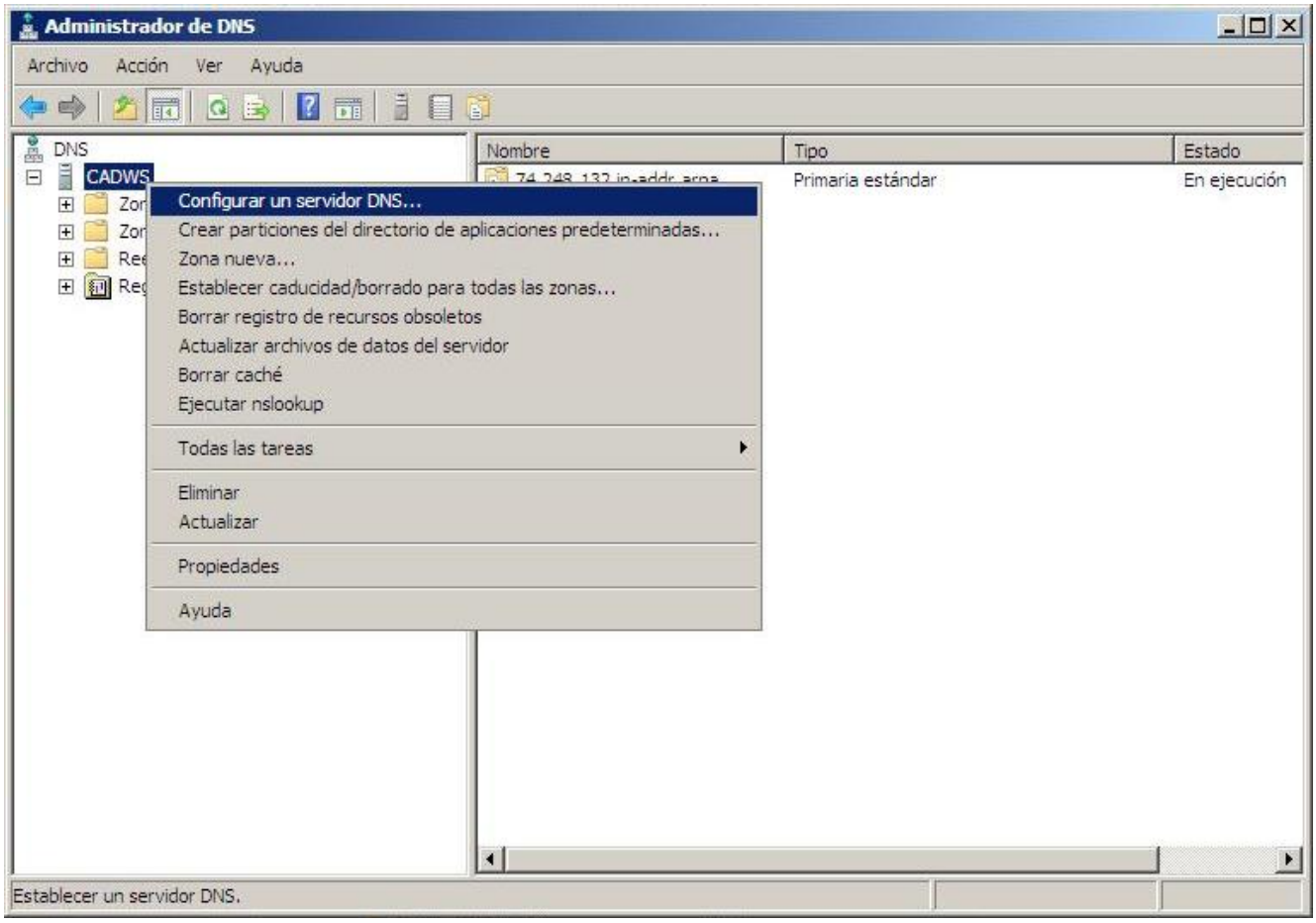

Administrador del servidor
Obtenga información general del estado del servidor, realice tareas principales de administración y agregue o quite funciones y características de servidor.
Resumen de servidores
Ayuda de resumen de servidores
Información del equipo
Cambiar propiedades del sistema
Información de seguridad
Ir a Firewall de Windows
Resumen de funciones
Ayuda de Resumen de funciones
Funciones: 1 de 16 instalada(s)
Servidor DNS
Ir a Funciones
Agregar funciones
Quitar funciones
Resumen de características
Ayuda de resumen de características
Características: 1 de 34 instalada(s)
Herramientas de administración remota del servidor
Herramientas de administración de funciones
Herramientas del servidor DNS
Agregar características
Quitar características
Última actualización: 24/08/2010 12:39:03
Configurar actualización

CONFIGURACIÓN DEL SERVIDOR DNS.

Después de que ha sido instalada la función de servidor DNS, es necesario configurarlo. En Inicio dar clic en Herramientas administrativas, dar clic en DNS.

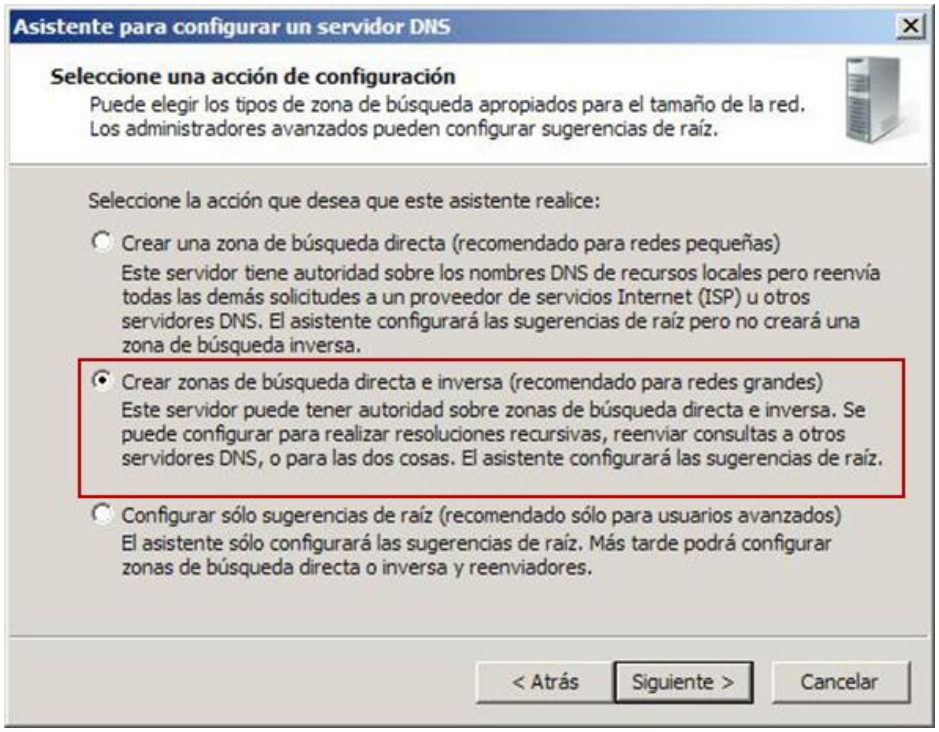


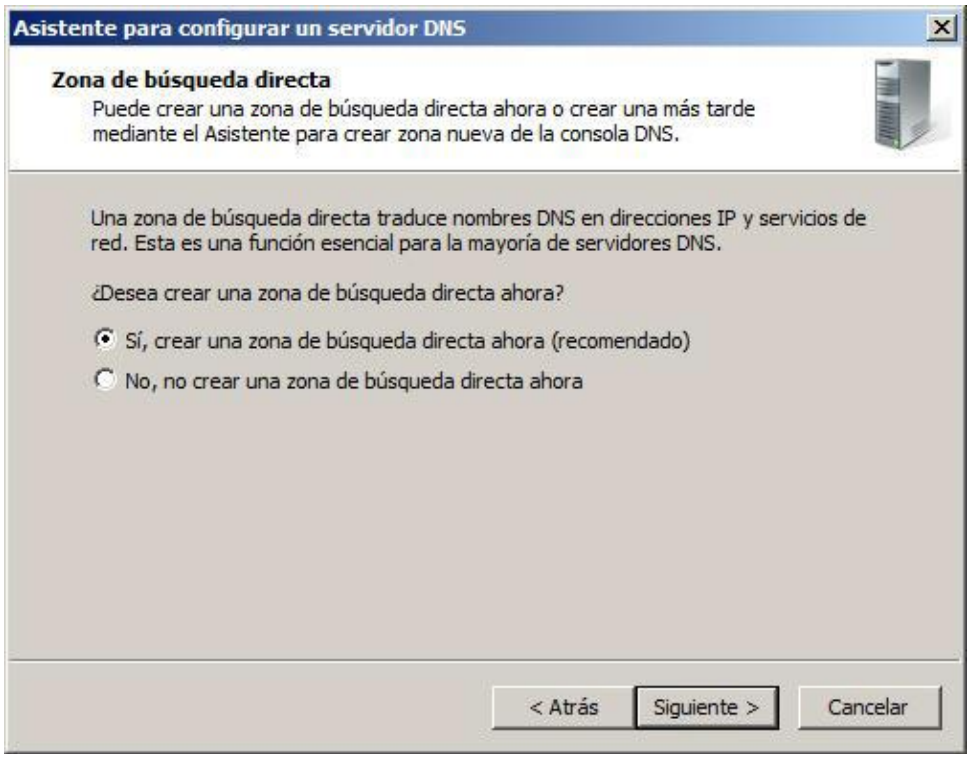
Dar clic con el botón derecho en el nombre del equipo, una vez desplegada la lista dar clic en Configurar un servidor DNS.



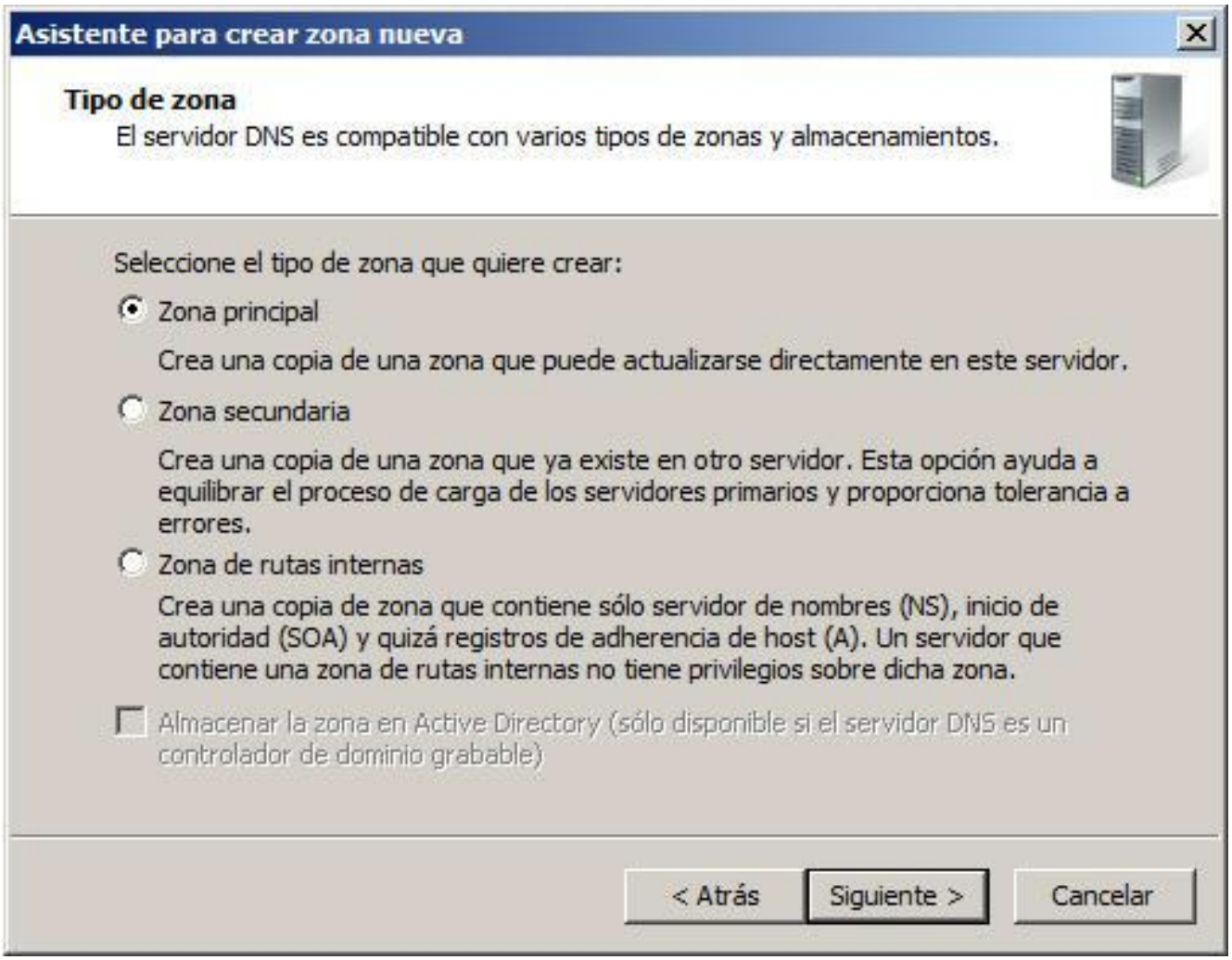
Aparece el asistente para la configuración del servidor DNS.

Dar clic en Crear zonas de búsqueda directa e inversa, para crear los tipos de zonas para las cuales el servidor DNs será autoritativo. Se configurarán la zona de búsqueda directa como la de búsqueda inversa.

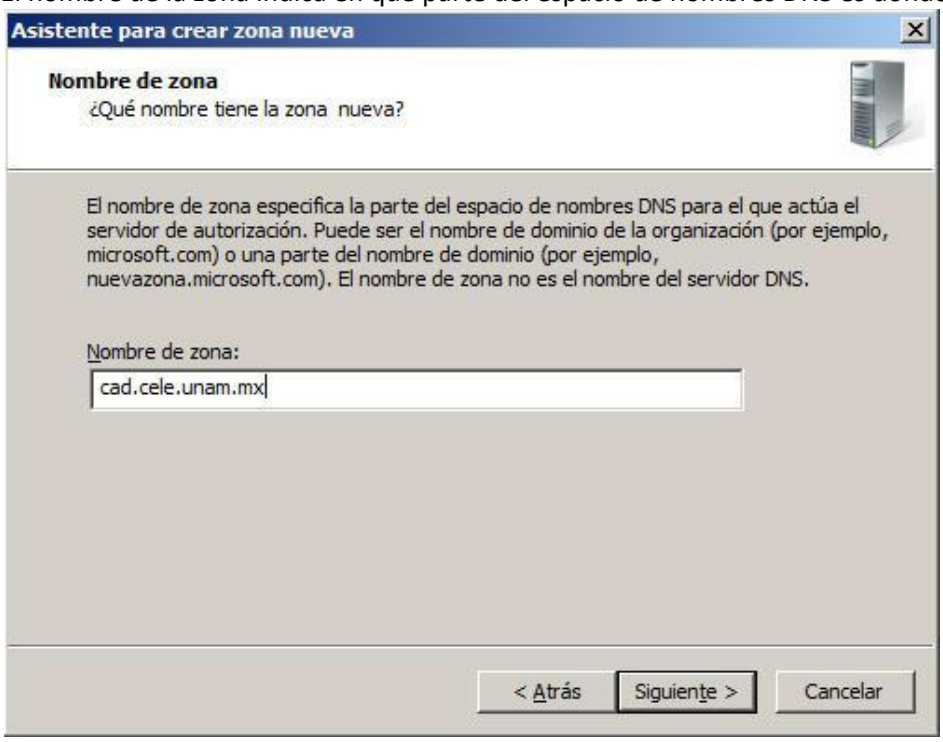




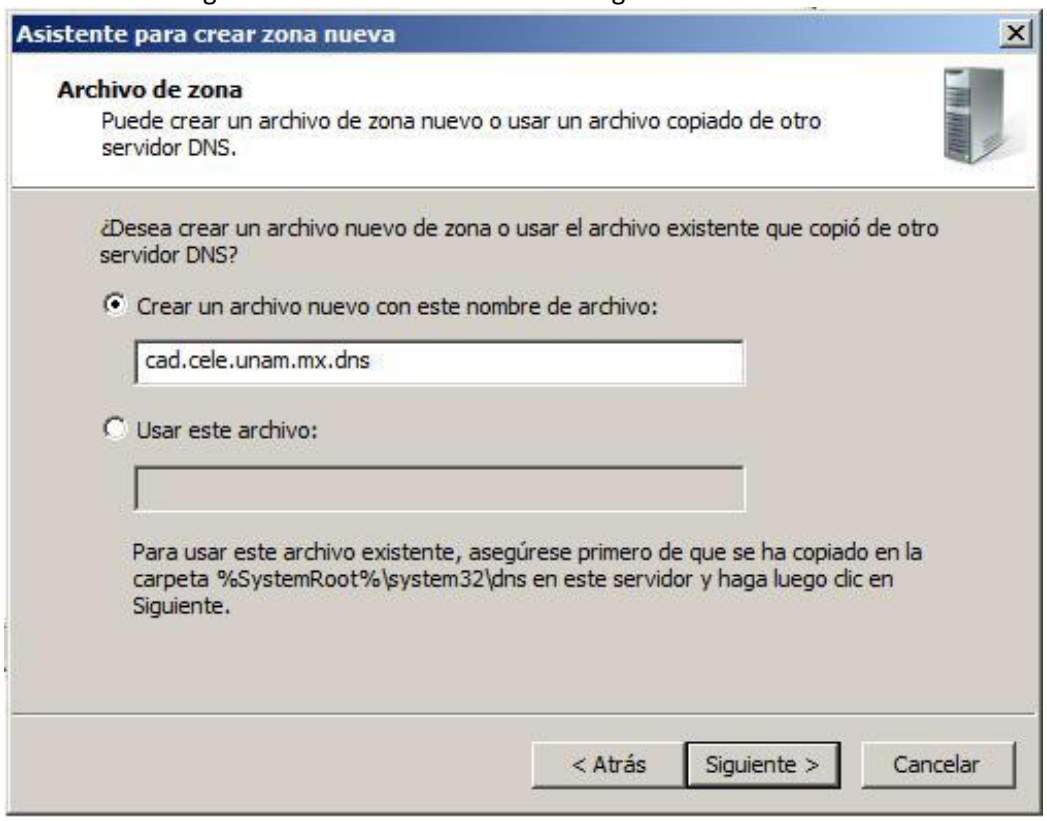
La zona que se configura debe ser Zona Principal, ya que es la primera que se configura en el dominio. En las Zonas Primarias o Principales, se permite leer y escribir en su base de datos, mientras que en las Zonas Secundarias sólo permite leer de la base de datos DNS.


Asistente para crear zona nueva
Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.
Seleccione el tipo de zona que quiere crear:
Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.
Zona secundaria
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores primarios y proporciona tolerancia a errores.
Zona de rutas internas
Crea una copia de zona que contiene sólo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.
Almacenar la zona en Active Directory (sólo disponible si el servidor DNS es un controlador de dominio grabable)
< Atrás
Siguiente >
Cancelar

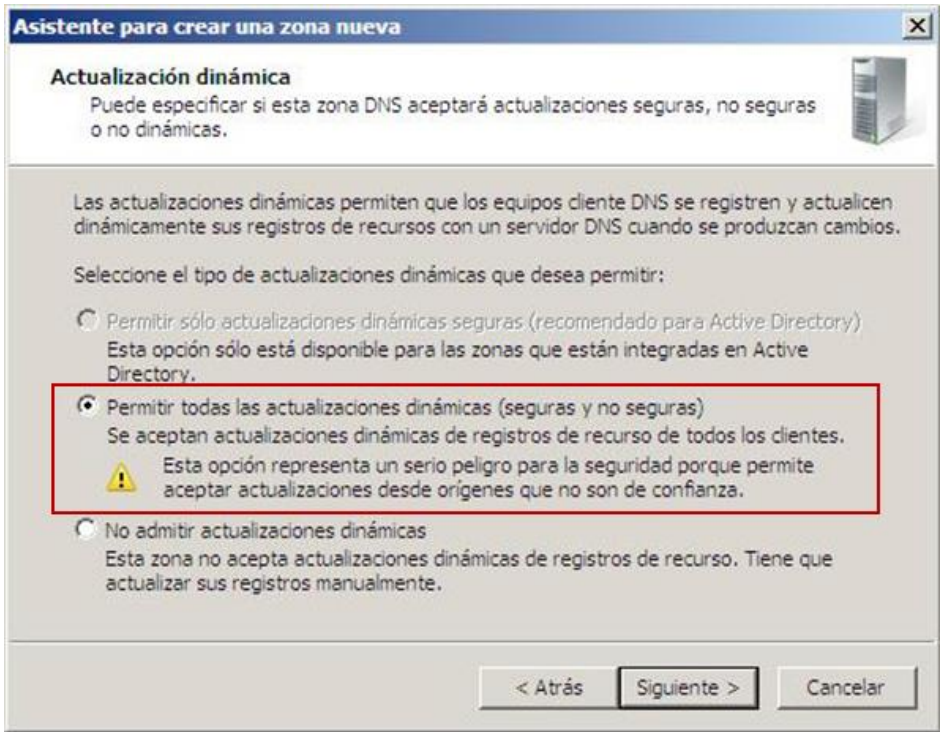
El nombre de la zona indica en que parte del espacio de nombres DNS es donde el servidor será autoritativo.



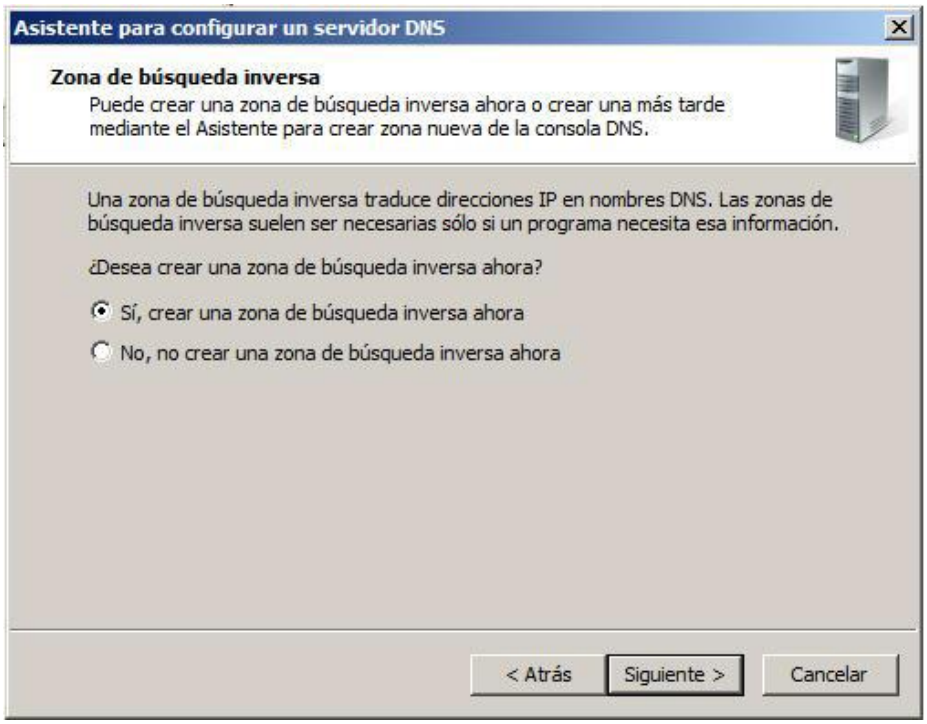
Al archivo de zona se puede acceder a través de la ruta WINDOWS/System32/dns, en este archivo se encuentran configuraciones relacionadas con los registros DNS.

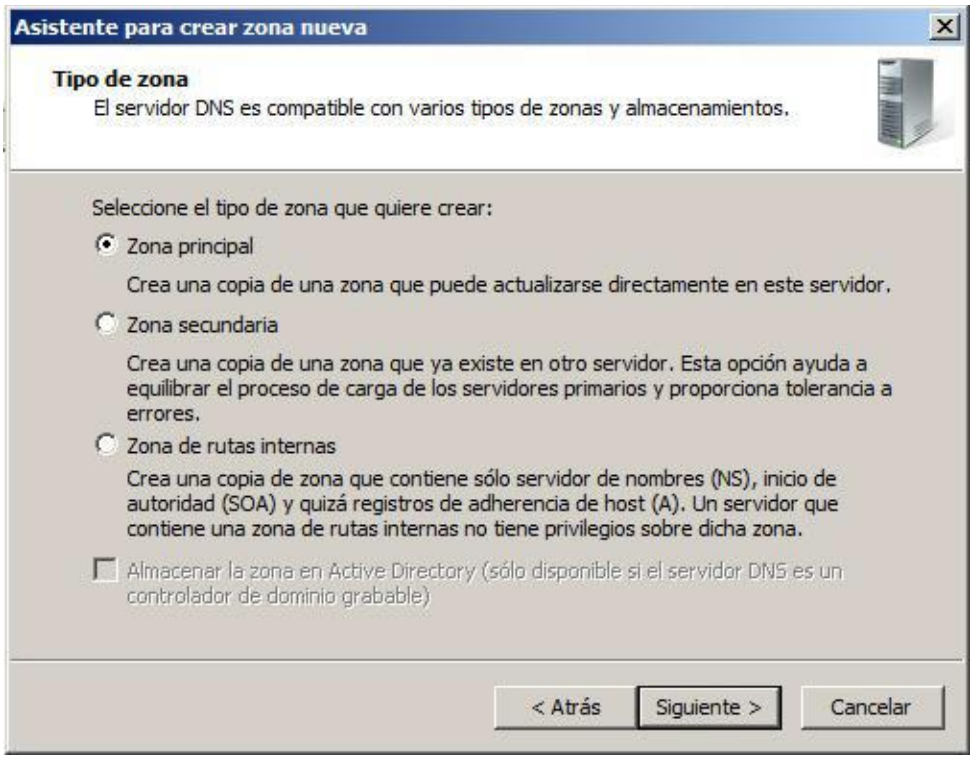


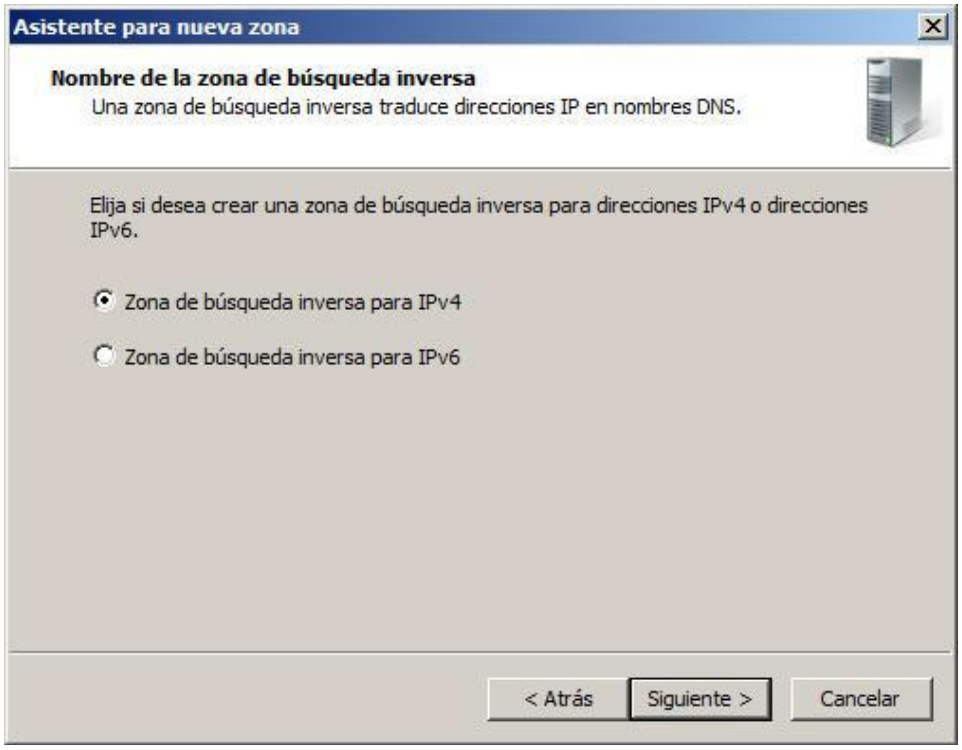
Para poder realizar las actualizaciones de la zona, es necesario elegir la opción Permitir todas las actualizaciones dinámicas (seguras y no seguras), esto será una opción temporal, al instalar el Directorio Activo las zonas pasaran a ser seguras.



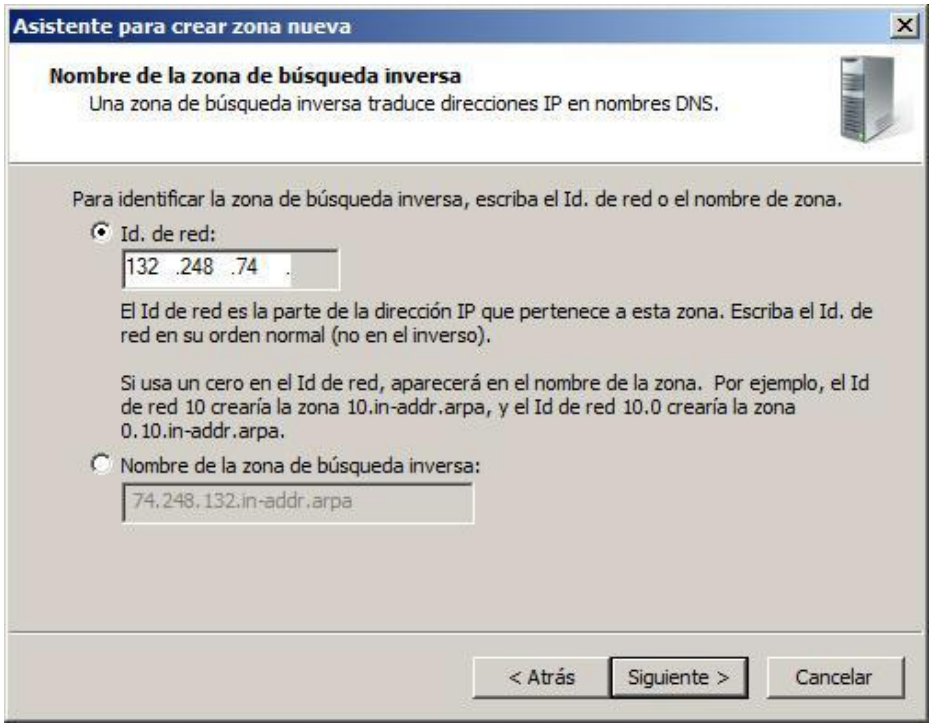
Posteriormente se configura la zona de búsqueda inversa.



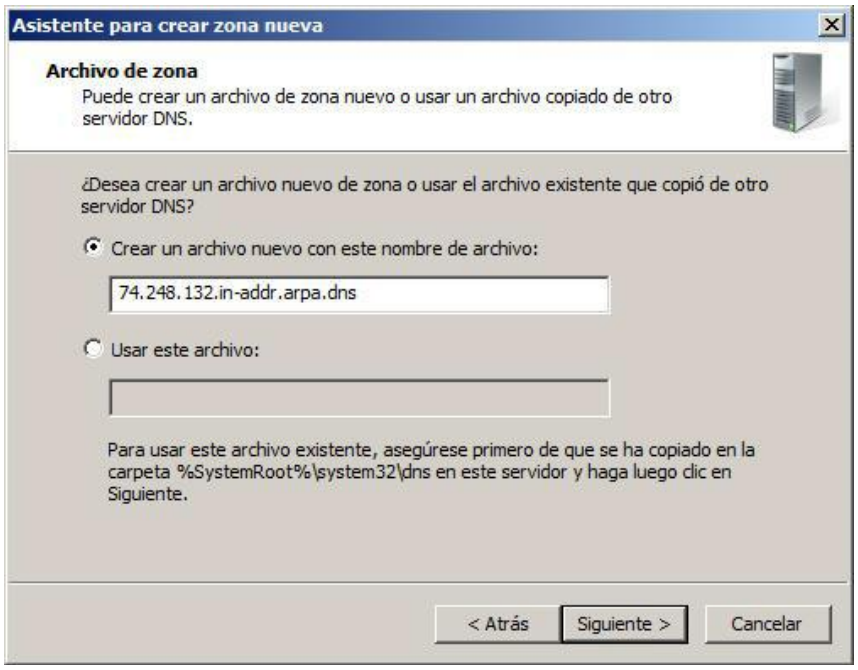

Asistente para crear zona nueva
Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.
Seleccione el tipo de zona que quiere crear:
Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.
Zona secundaria
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores primarios y proporciona tolerancia a errores.
Zona de rutas internas
Crea una copia de zona que contiene sólo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.
Almacenar la zona en Active Directory (sólo disponible si el servidor DNS es un controlador de dominio grabable)
< Atrás
Siguiente >
Cancelar

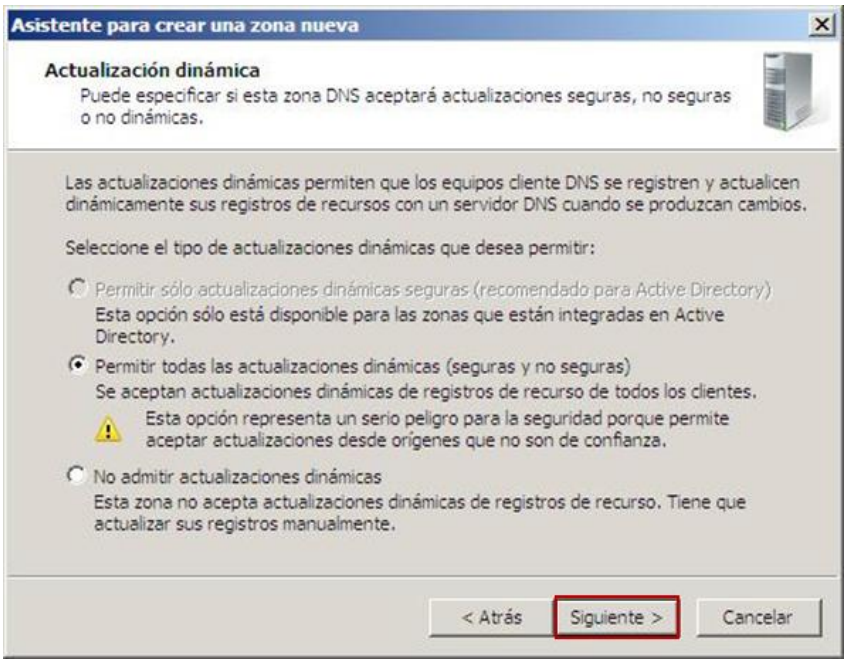

Asistente para nueva zona
Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.
Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.
Zona de búsqueda inversa para IPv4
Zona de búsqueda inversa para IPv6
< Atrás
Siguiente >
Cancelar

En esta parte del asistente se configura el identificador de red, para este caso que se usa una máscara de subred 255.255.255.0 se usa el identificador 132.248.74.x, por ejemplo, si la máscara de subred fuera 255.255.0.0 el identificador sería 132.248.x.x.



También es necesario crear una archivo para la zona de búsqueda inversa, este archivo puede ser accedido a través de la ruta WINDOWS/System32/dns.



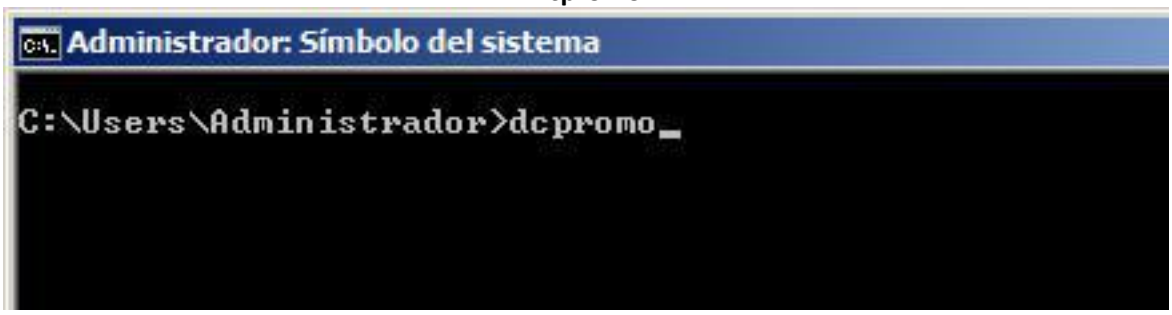

Asistente para crear una zona nueva
Actualización dinámica
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.
Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.
Seleccione el tipo de actualizaciones dinámicas que desea permitir:
Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción sólo está disponible para las zonas que están integradas en Active Directory.
Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.
< Atrás
Siguiente >
Cancelar


Asistente para configurar un servidor DNS
Finalización del Asistente para configurar un servidor DNS
El Asistente para configurar un servidor DNS se completó con éxito. Se guardará la configuración siguiente cuando haga clic en Finalizar.
Configuración:
Servidor DNS que desea configurar: CADWS
Zona de búsqueda directa que desea crear:
cad.cele.unam.mx
Configure los host que utilizarán ese servidor DNS para que apunten a él para la resolución de nombres y, a continuación, utilice nslookup para comprobar la resolución de nombres. Si agregó una nueva zona principal, agréguele registros de recurso para los host cuyos nombres debe resolver este servidor DNS.
Para cerrar el asistente, haga clic en Finalizar.
< Atrás
Finalizar
Cancelar

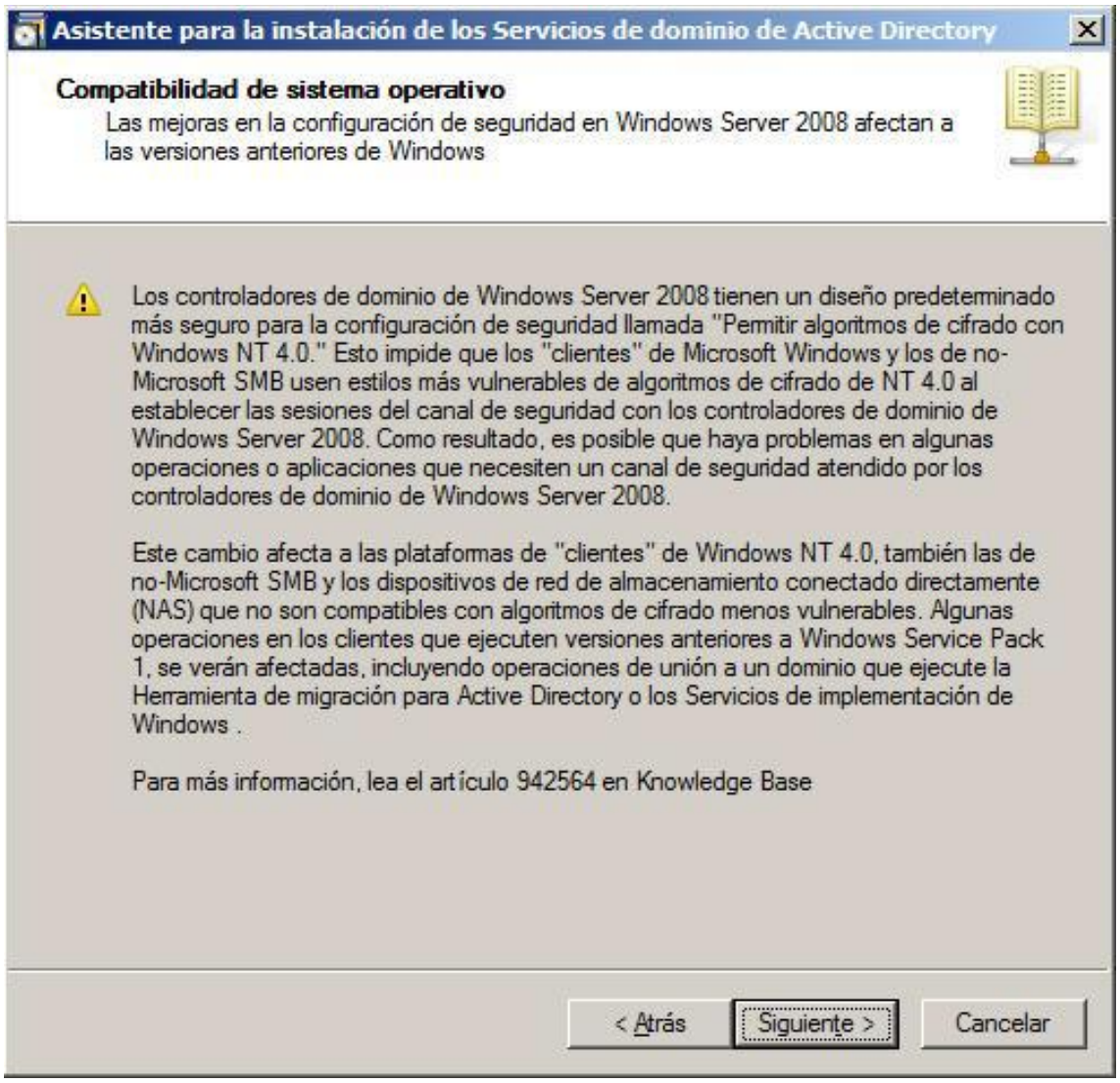
Una vez que se tiene instalado y configurado el servidor DNS, se configura el Directorio Activo.

Configuración del Directorio Activo.
El primer paso para la configuración del Directorio Activo es promover el servidor a Controlador de Dominio, esto se realiza con el comando:

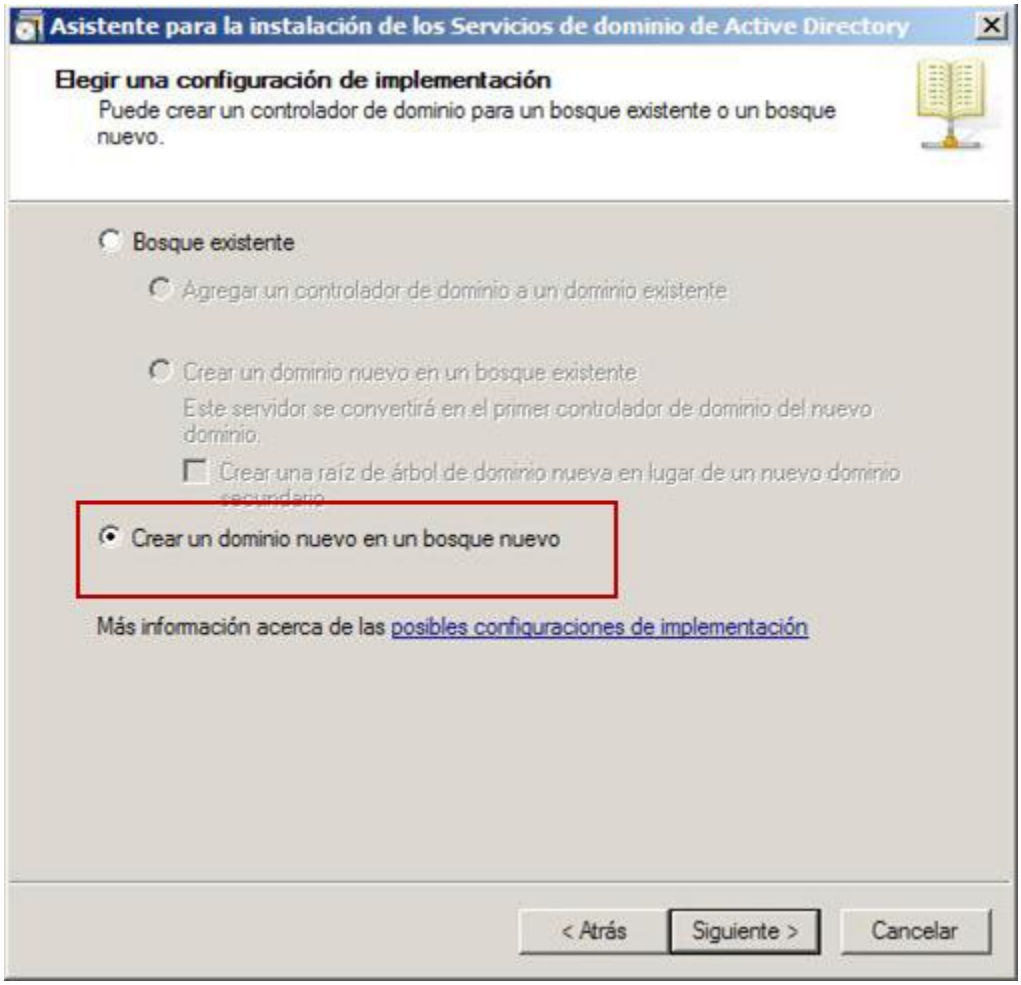
Dcpromo



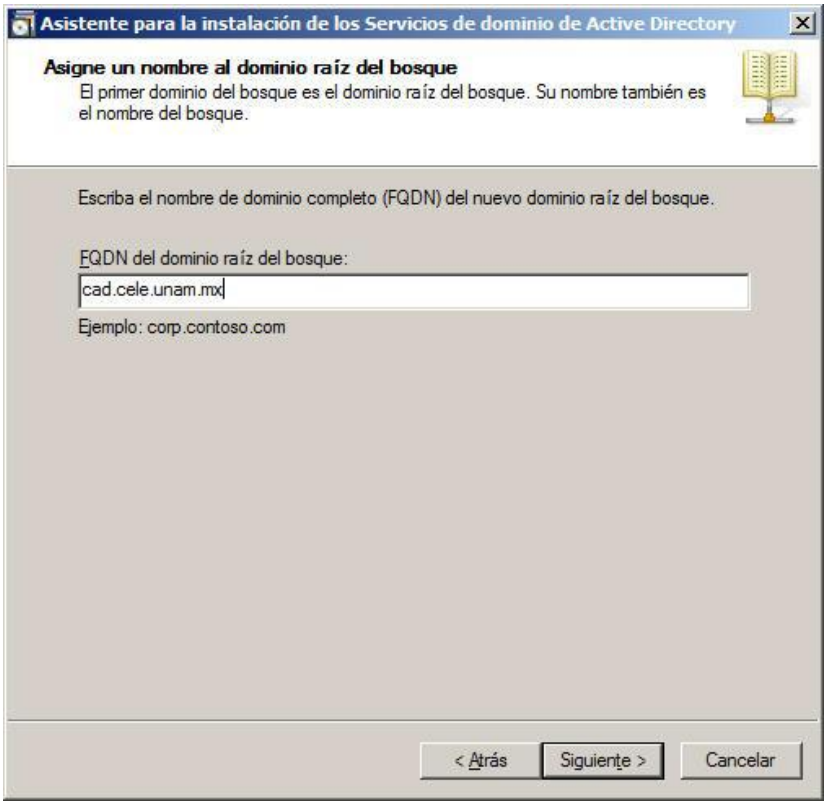
Con esto se abrirá el Asistente para la instalación de los Servicios de dominio del Directorio Activo, elegir la opción de Instalación en modo avanzado.

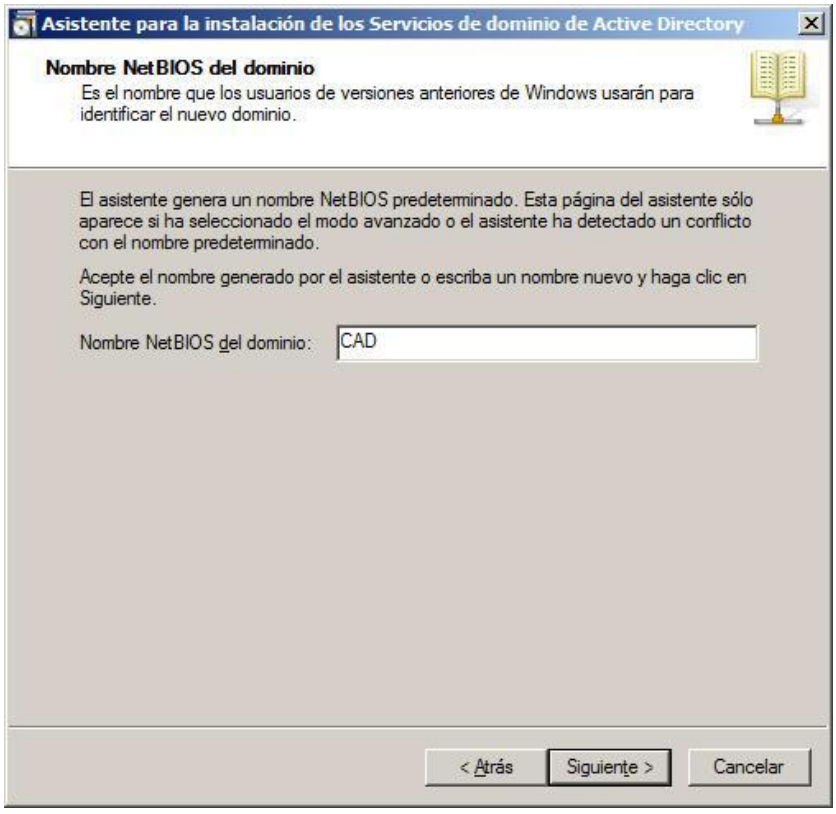

Asistente para la instalación de los Servicios de dominio de Active Directory
Compatibilidad de sistema operativo
Las mejoras en la configuración de seguridad en Windows Server 2008 afectan a las versiones anteriores de Windows
Los controladores de dominio de Windows Server 2008 tienen un diseño predeterminado más seguro para la configuración de seguridad llamada "Permitir algoritmos de cifrado con Windows NT 4.0." Esto impide que los "clientes" de Microsoft Windows y los de no-Microsoft SMB usen estilos más vulnerables de algoritmos de cifrado de NT 4.0 al establecer las sesiones del canal de seguridad con los controladores de dominio de Windows Server 2008. Como resultado, es posible que haya problemas en algunas operaciones o aplicaciones que necesiten un canal de seguridad atendido por los controladores de dominio de Windows Server 2008.
Este cambio afecta a las plataformas de "clientes" de Windows NT 4.0, también las de no-Microsoft SMB y los dispositivos de red de almacenamiento conectado directamente (NAS) que no son compatibles con algoritmos de cifrado menos vulnerables. Algunas operaciones en los clientes que ejecuten versiones anteriores a Windows Service Pack 1, se verán afectadas, incluyendo operaciones de unión a un dominio que ejecute la Herramienta de migración para Active Directory o los Servicios de implementación de Windows .
Para más información, lea el artículo 942564 en Knowledge Base
< Atrás
Siguiente >
Cancelar

Dado que no existe otro dominio en la red, se elige la opción de Crear un dominio nuevo en un bosque nuevo.



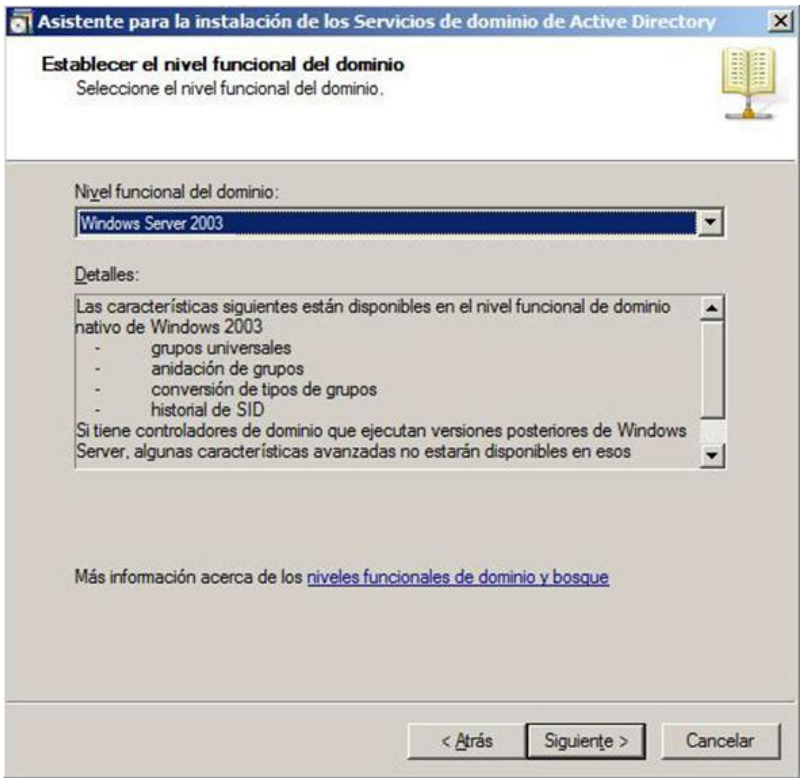
Se establece el nombre del dominio raíz del bosque.

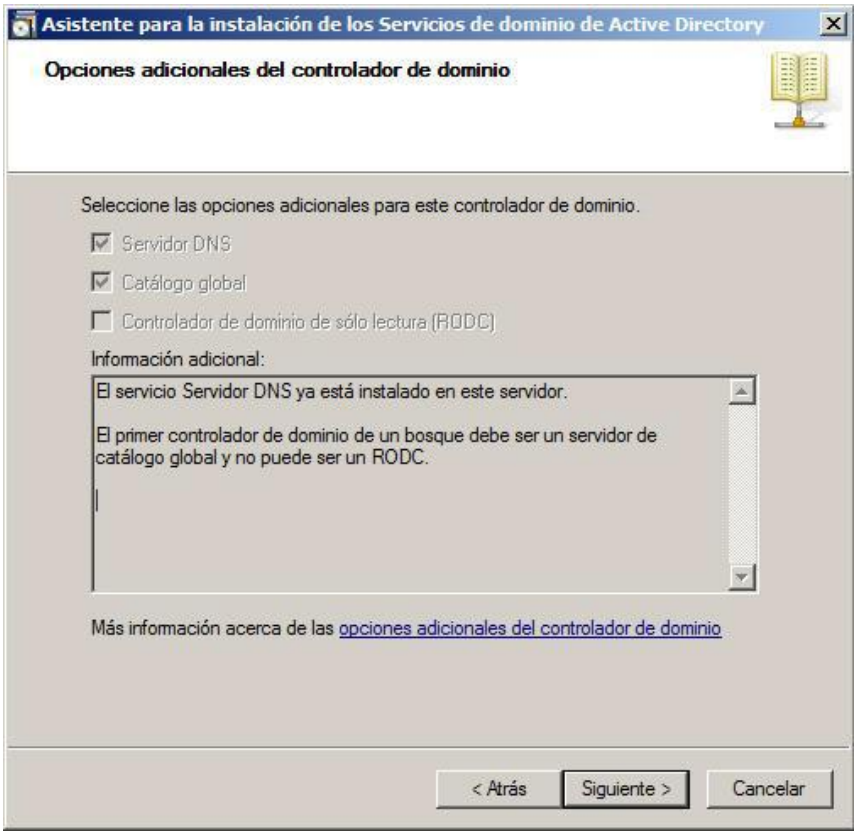




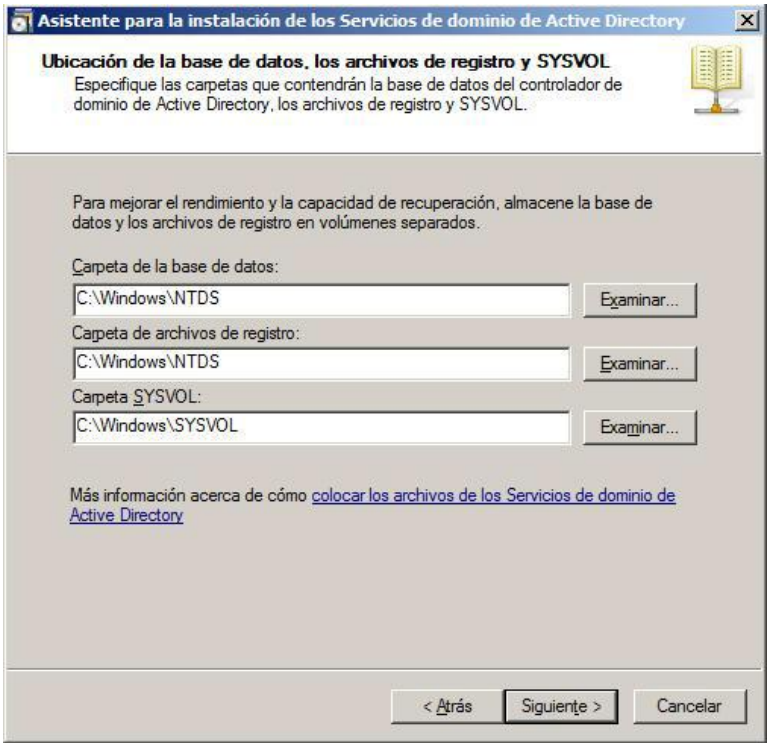
Para evitar problemas de compatibilidad se elige un nivel funcional del bosque con Windows 2003, dado que no existen equipos con una versión anterior a la de este sistema operativo.

Al igual que para el nivel funcional del bosque, se elige un nivel funcional para el dominio con Windows 2003.

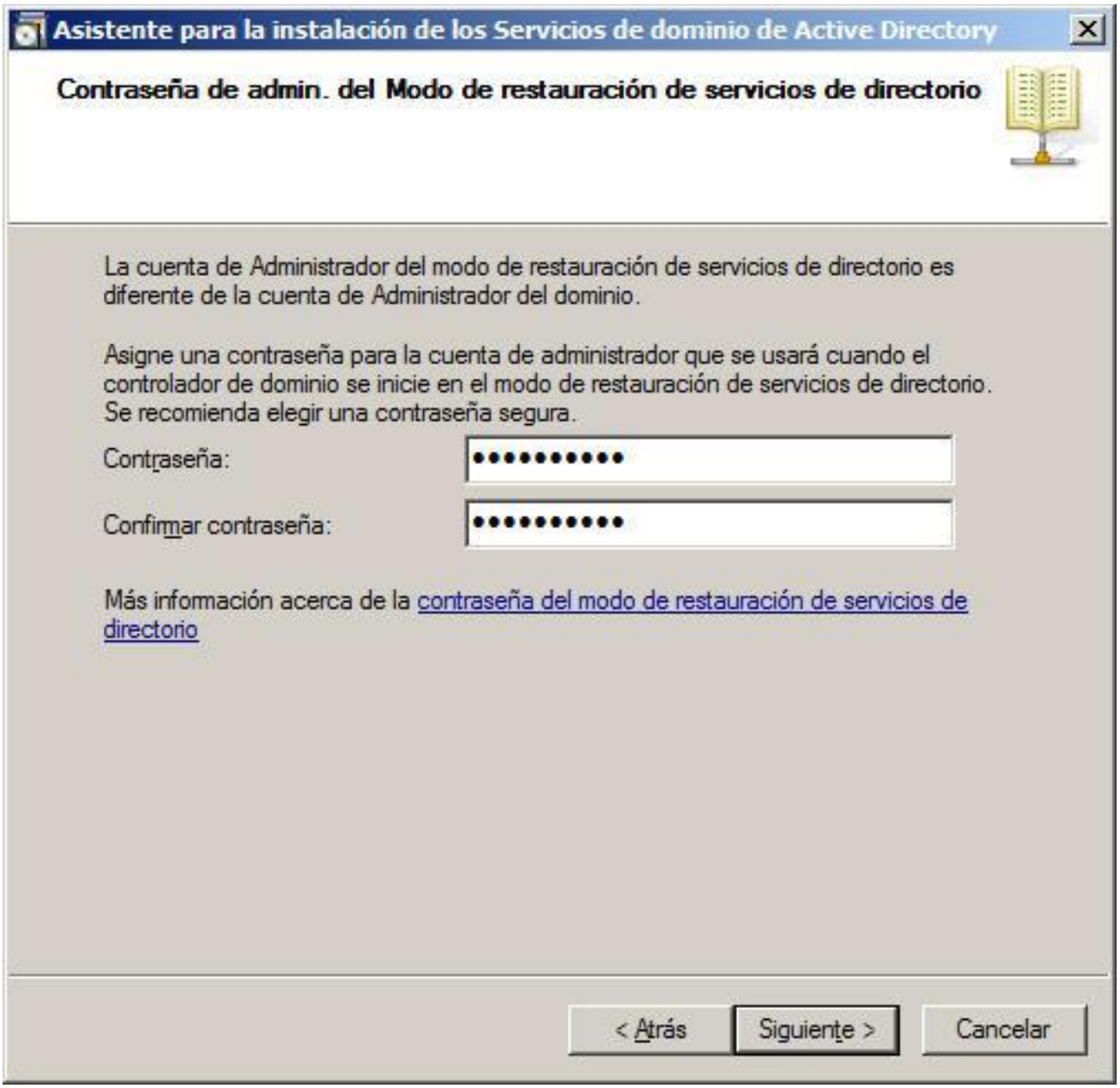

Asistente para la instalación de los Servicios de dominio de Active Directory
Establecer el nivel funcional del dominio
Seleccione el nivel funcional del dominio.
Nivel funcional del dominio:
Windows Server 2003
Detalles:
Las características siguientes están disponibles en el nivel funcional de dominio nativo de Windows 2003
- grupos universales
- anidación de grupos
- conversión de tipos de grupos
- historial de SID
Si tiene controladores de dominio que ejecutan versiones posteriores de Windows Server, algunas características avanzadas no estarán disponibles en esos
Más información acerca de los niveles funcionales de dominio y bosque
< Atrás
Siguiente >
Cancelar


Asistente para la instalación de los Servicios de dominio de Active Directory
Opciones adicionales del controlador de dominio
Seleccione las opciones adicionales para este controlador de dominio.
Servidor DNS
Catálogo global
Controlador de dominio de sólo lectura (RODC)
Información adicional:
El servicio Servidor DNS ya está instalado en este servidor.
El primer controlador de dominio de un bosque debe ser un servidor de catálogo global y no puede ser un RODC.
Más información acerca de las opciones adicionales del controlador de dominio
< Atrás
Siguiente >
Cancelar

Se deja la ruta predeterminada de las carpetas en donde se almacenarán la base de datos del controlador de dominio, los archivos de registro y SYSVOL que utiliza el Directorio Activo.



Se establece la contraseña que se utilizará para el modo de restauración de los servicios del directorio en caso de que fuera necesario.


Asistente para la instalación de los Servicios de dominio de Active Directory
Contraseña de admin. del Modo de restauración de servicios de directorio
La cuenta de Administrador del modo de restauración de servicios de directorio es diferente de la cuenta de Administrador del dominio.
Asigne una contraseña para la cuenta de administrador que se usará cuando el controlador de dominio se inicie en el modo de restauración de servicios de directorio. Se recomienda elegir una contraseña segura.
Contraseña:
Confirmar contraseña:
Más información acerca de la contraseña del modo de restauración de servicios de directorio
< Atrás
Siguiente >
Cancelar

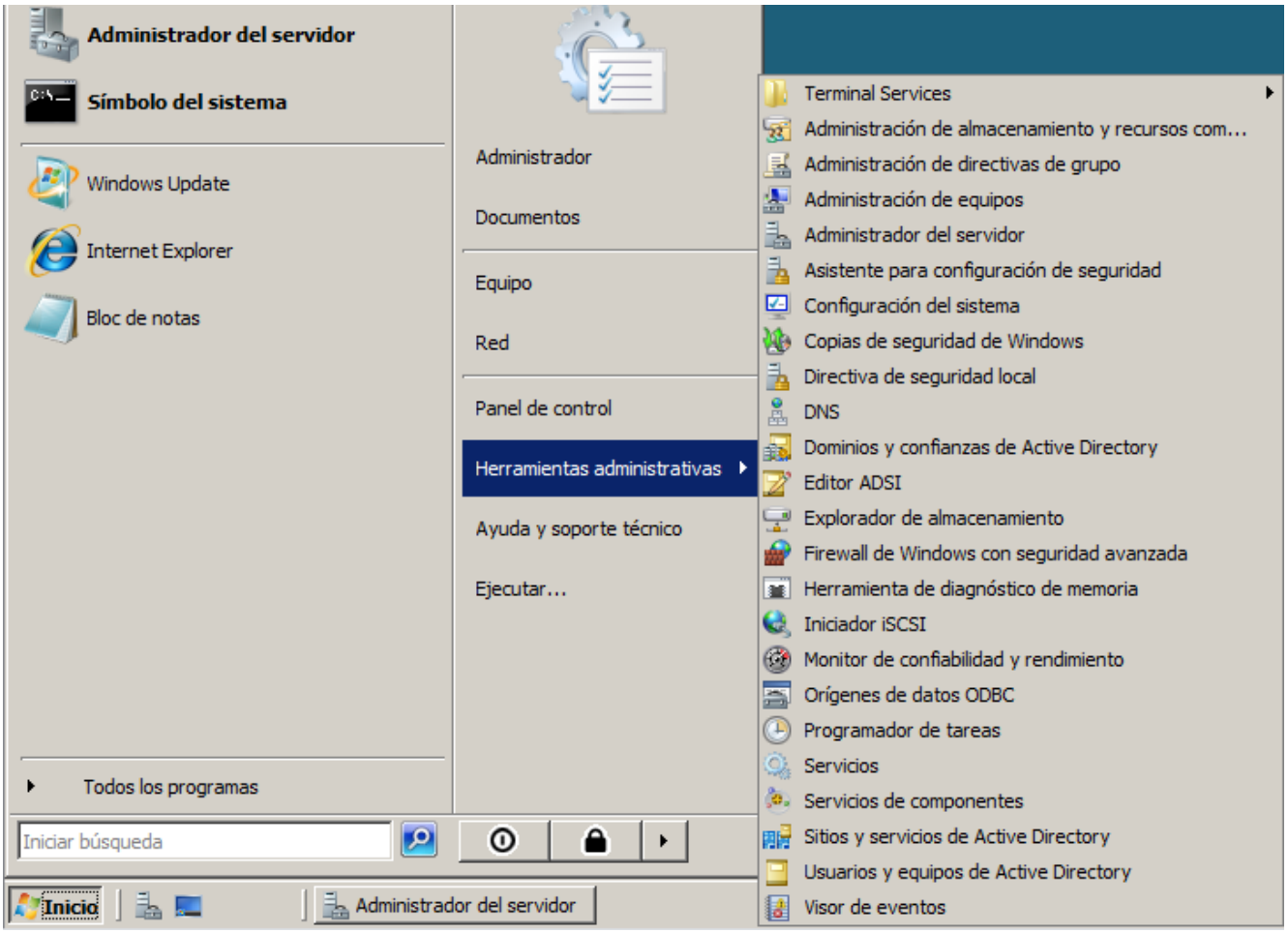
Finalmente se muestra el resumen con las configuraciones seleccionadas para la instalación de los servicios de dominio del Directorio Activo.

Una vez que se ha reiniciado el sistema, los servicios del Directorio Activo están listos para utilizarse. A continuación se explica cómo crear y administrar cuentas de usuario.

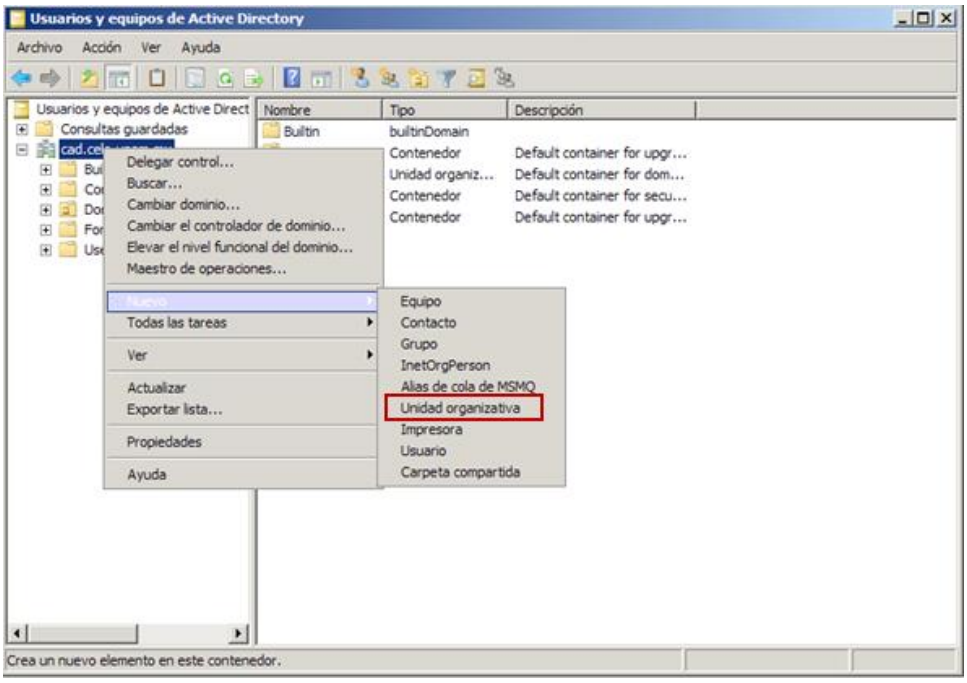
Crear y manejar cuentas de usuario.

Para poder crear nuevos usuarios, es necesario, como mínimo, pertenecer al grupo Opers. de cuentas, Admins. del dominio, Administradores de organización o equivalente.

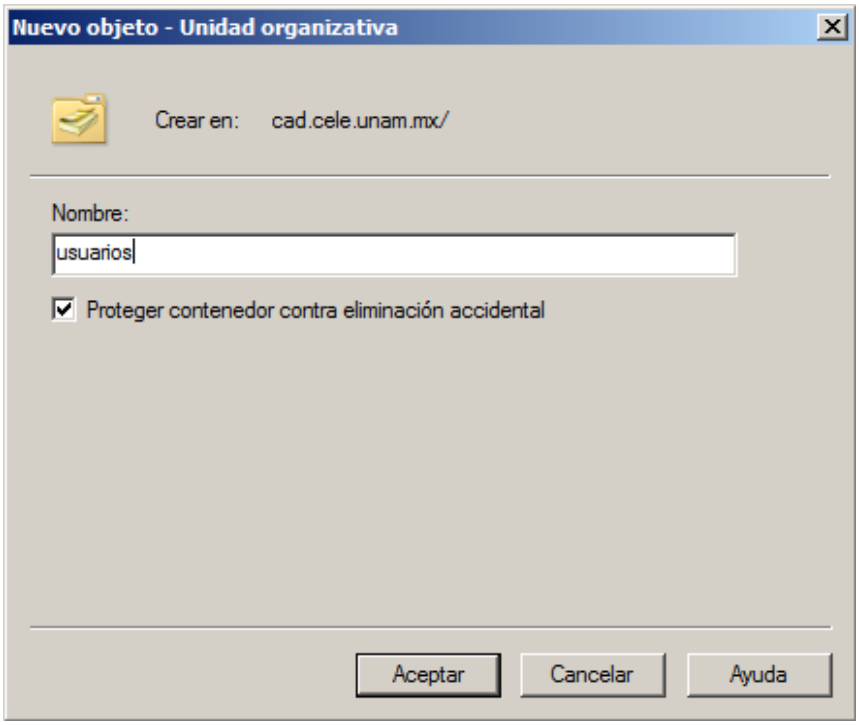
Dar clic en Inicio, Herramientas Administrativas, Usuarios y equipos de Active Directory.



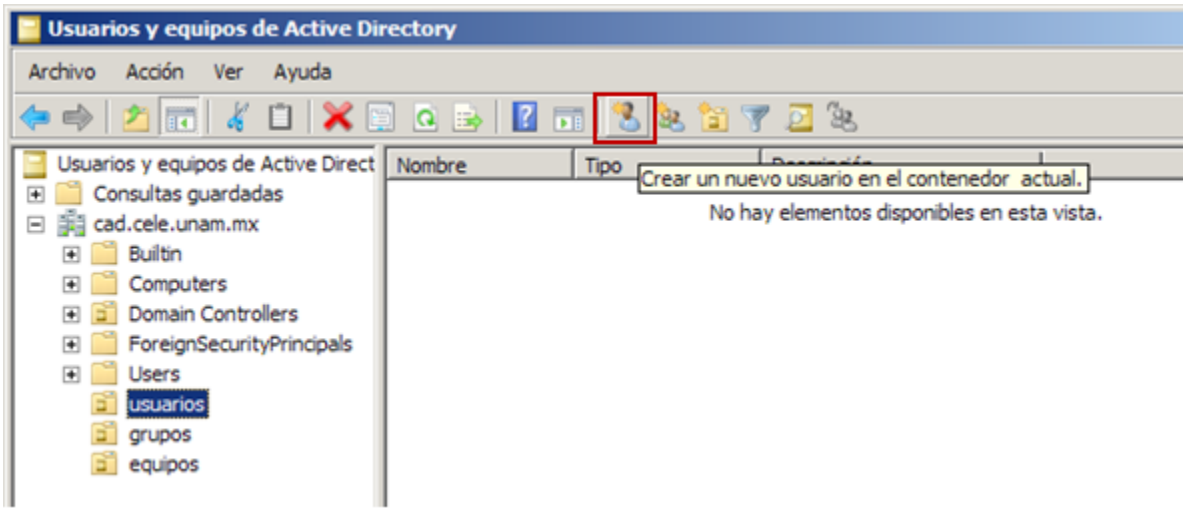
En la consola de administración Usuarios y equipos de Active Directory, dar clic con el botón derecho una vez expandido el árbol, en la lista desplegada, dar clic en Nuevo y en Unidad Organizativa.



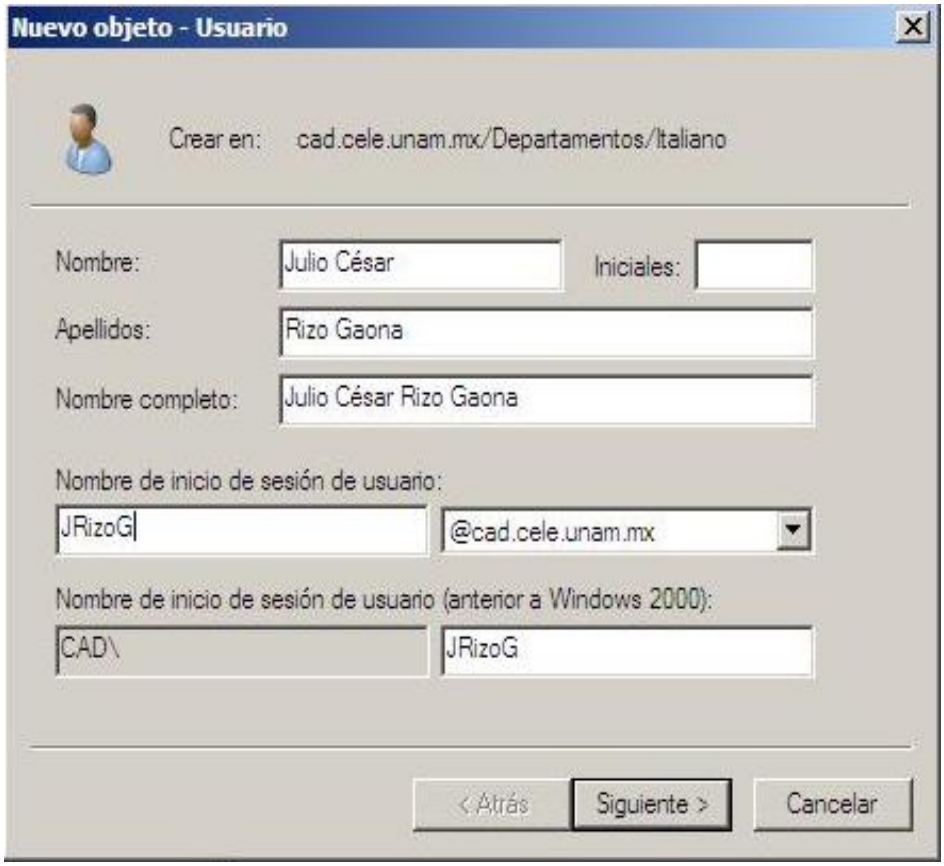
Dar el nombre de la unidad organizativa “Usuarios”. Verificar que este marcada la casilla de Proteger contenedor contra eliminación accidental.



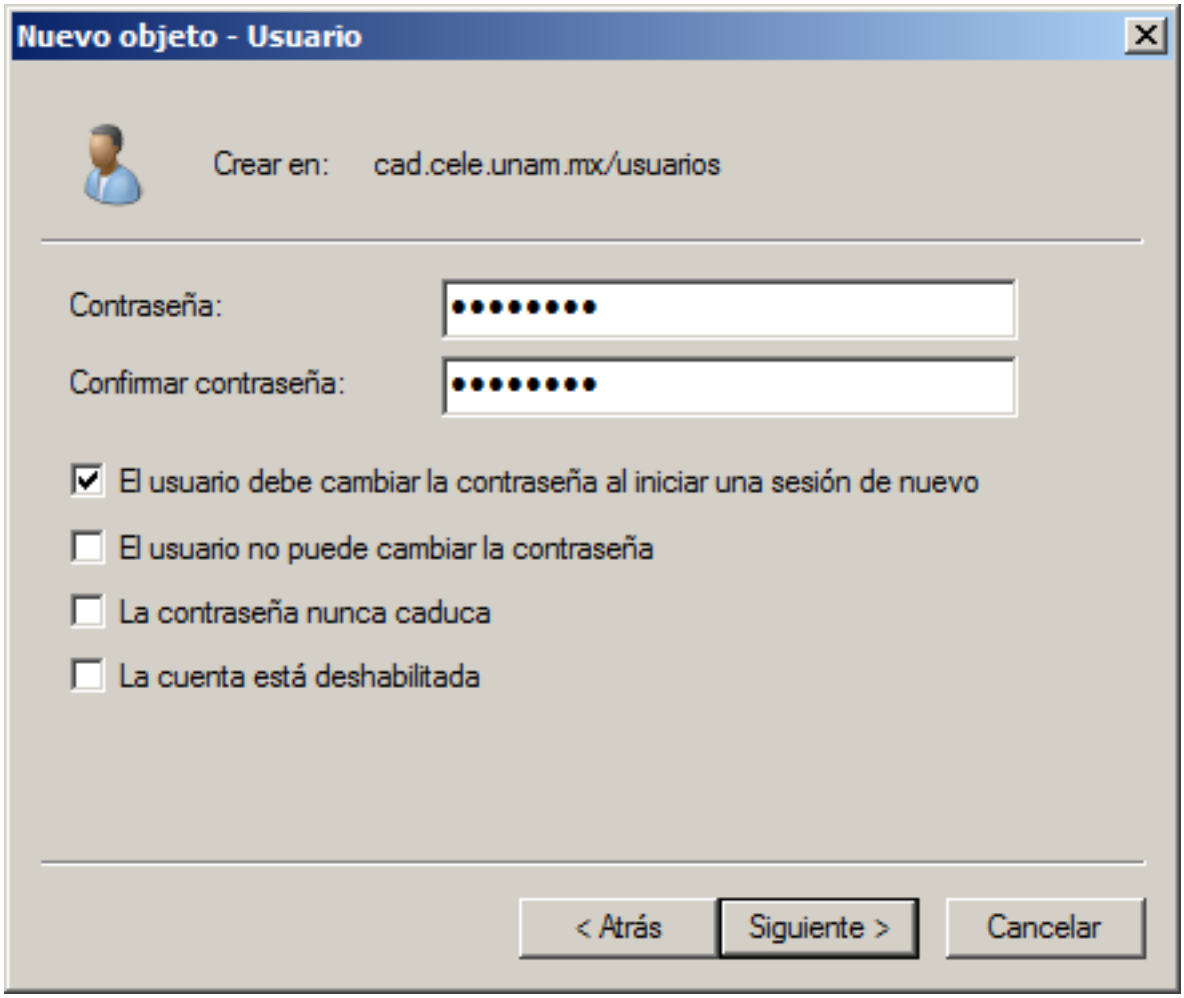
Dentro la OU “usuarios”, crear los usuarios correspondientes.



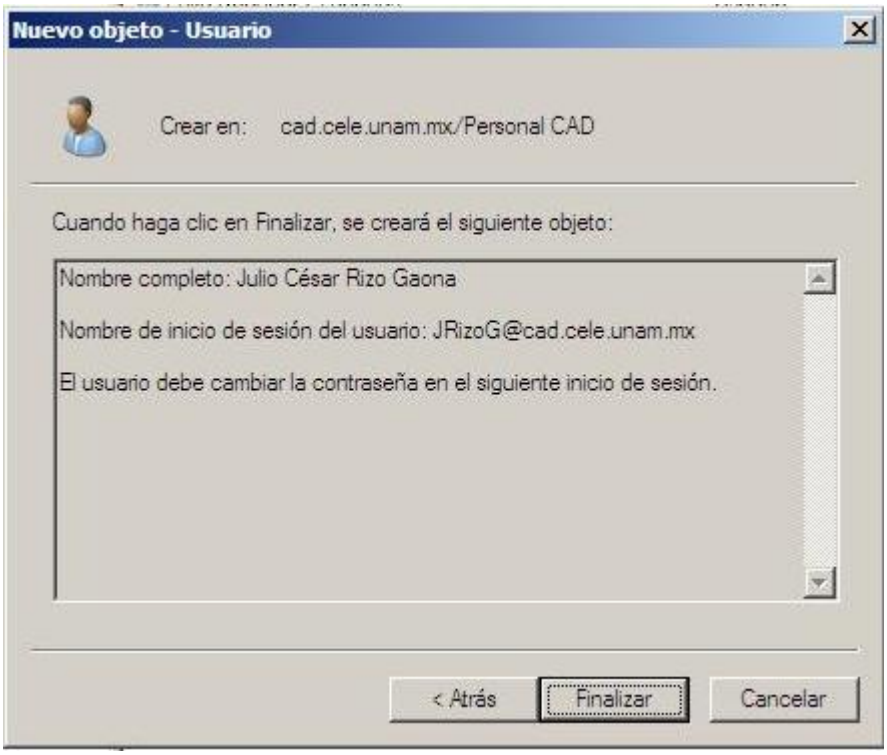
Se establecen los datos del usuario, entre ellos el nombre de inicio de sesión de usuario que tendrá. Para este campo se usa la inicial del nombre, seguido del primer apellido y de la inicial del segundo como se muestra en la imagen.



Se establece una contraseña temporal la cual será cambiada por el propio usuario cuando inicie sesión en algún equipo del dominio.

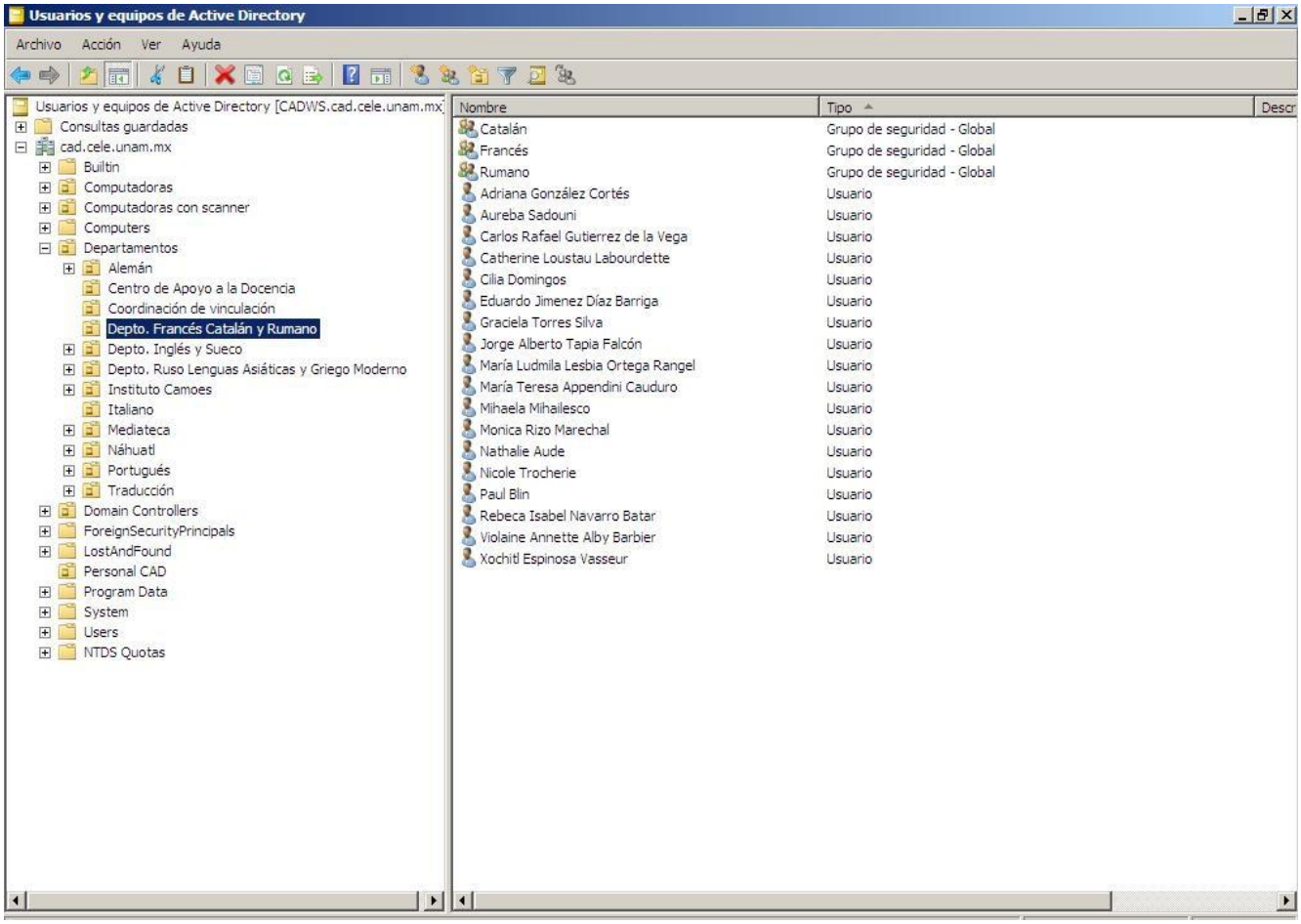


Se muestra el resumen de creación de la cuenta de usuario creada.

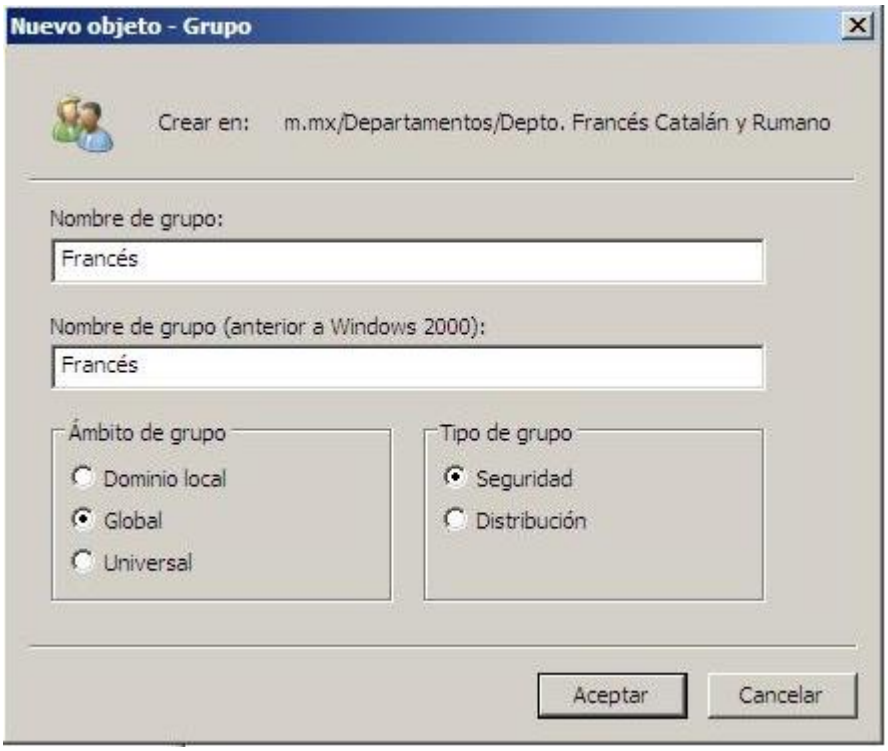


Para las otras unidades organizativas creadas, se sigue el mismo procedimiento para agregar nuevos usuarios.

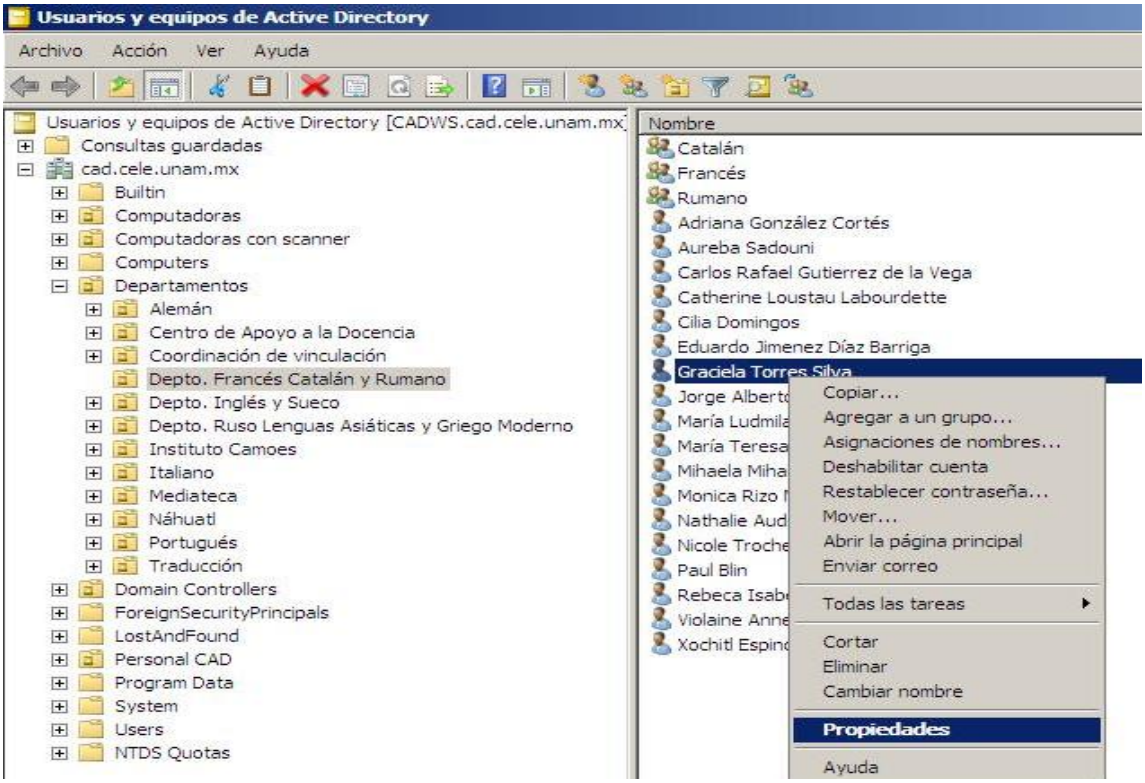
Algunas unidades organizativas tienen grupos de usuarios, como lo es la OU profesores. Para la creación de grupos de usuarios se realiza lo siguiente:
Dentro del la OU “Departamentos”, crear las sub-unidades organizativas y los grupos correspondientes a los departamentos del CELE



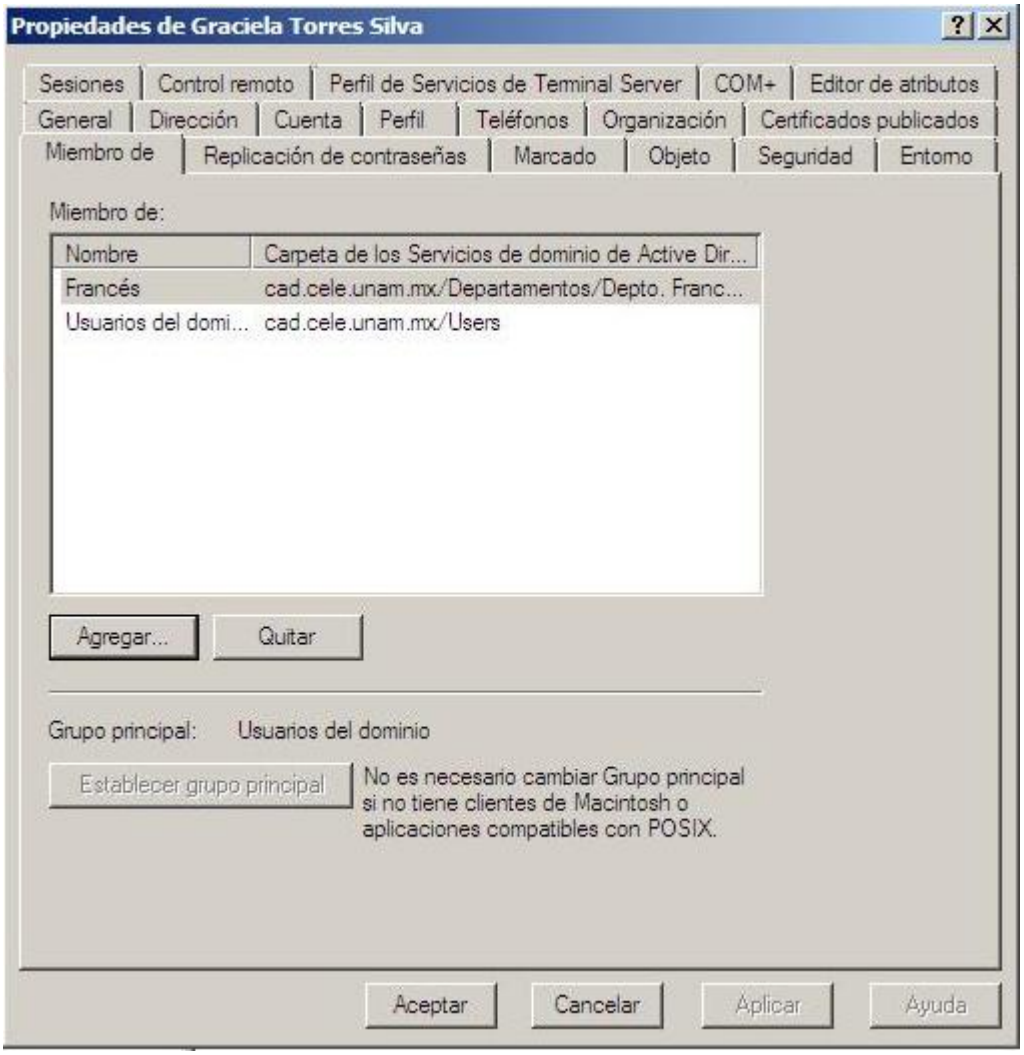
Al momento de crear un grupo es importante considerar si será un grupo de tipo Seguridad o Distribución. Los grupos de tipo Seguridad cuentan con permisos administrativos sobre el Ámbito de grupo definido, en cambio, el tipo de Grupo de Distribución sólo cuenta con permisos de usuarios normales.



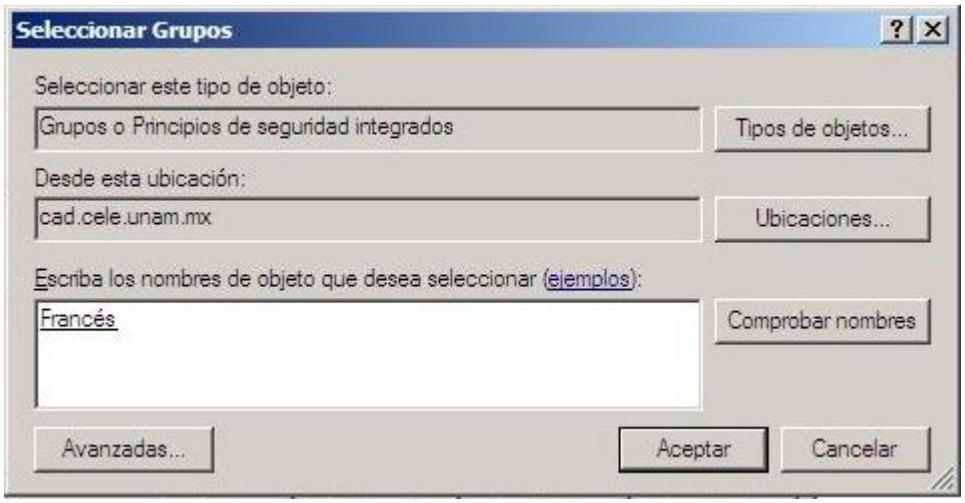
Para agregar un usuario a un grupo, dar clic con el botón derecho en el nombre del usuario, dar clic en **Propiedades**.



Una vez abierta la ventana, dar clic en la pestaña Miembro de, dar clic en el botón Agregar.

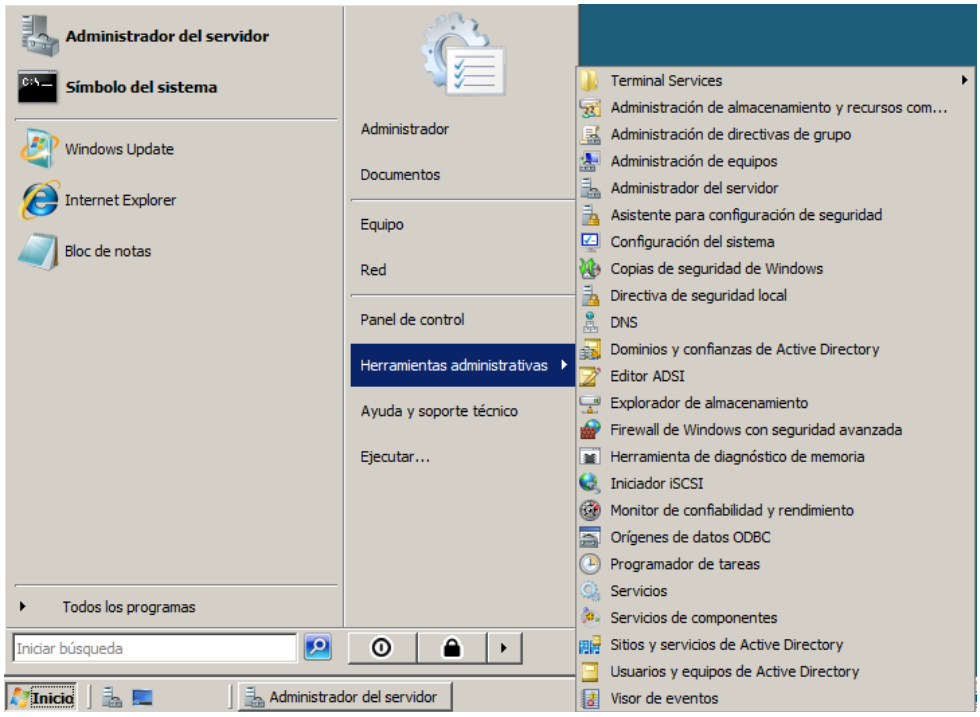


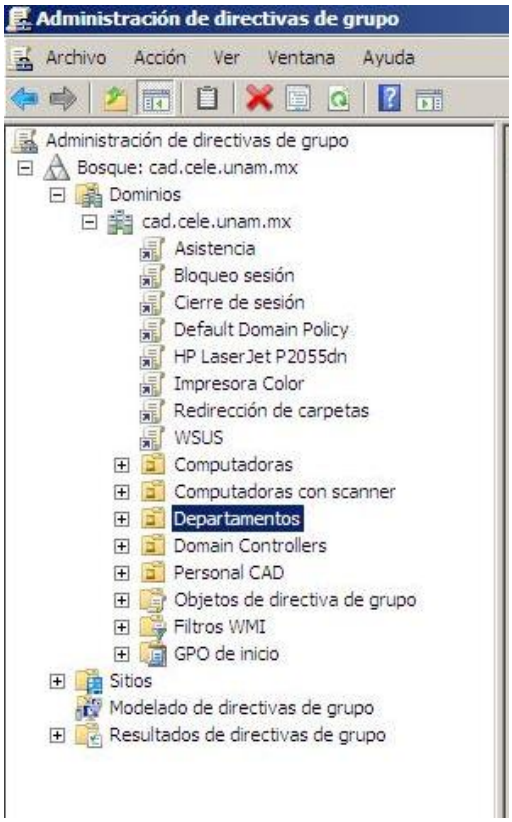
Seleccionar el grupo al cual va a pertenecer el usuario y dar clic en Aceptar.



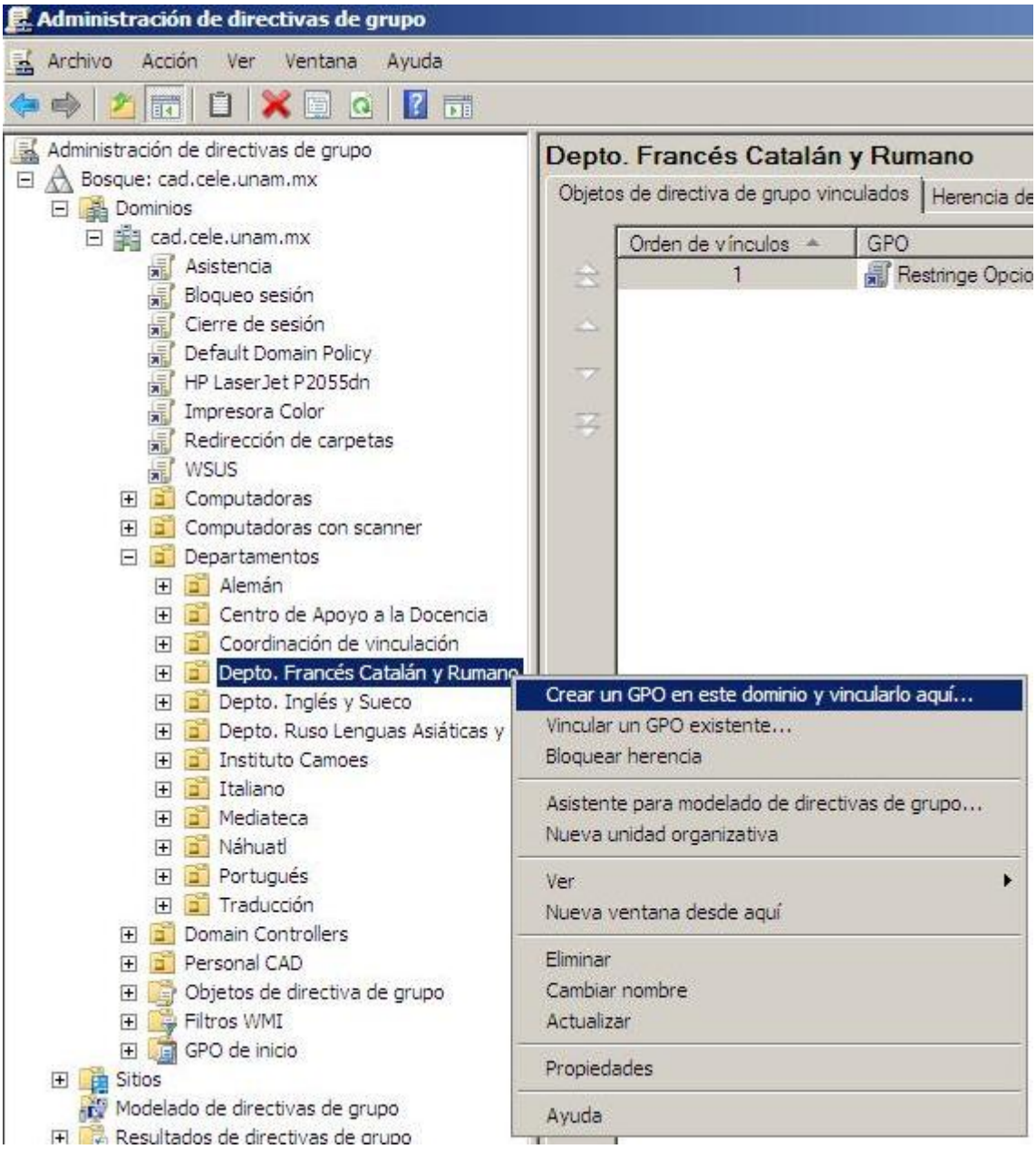
Finalmente se explica la creación de las políticas de grupo GPOs.

Dar clic en Inicio, Herramientas Administrativas, Administración de directivas de grupo.

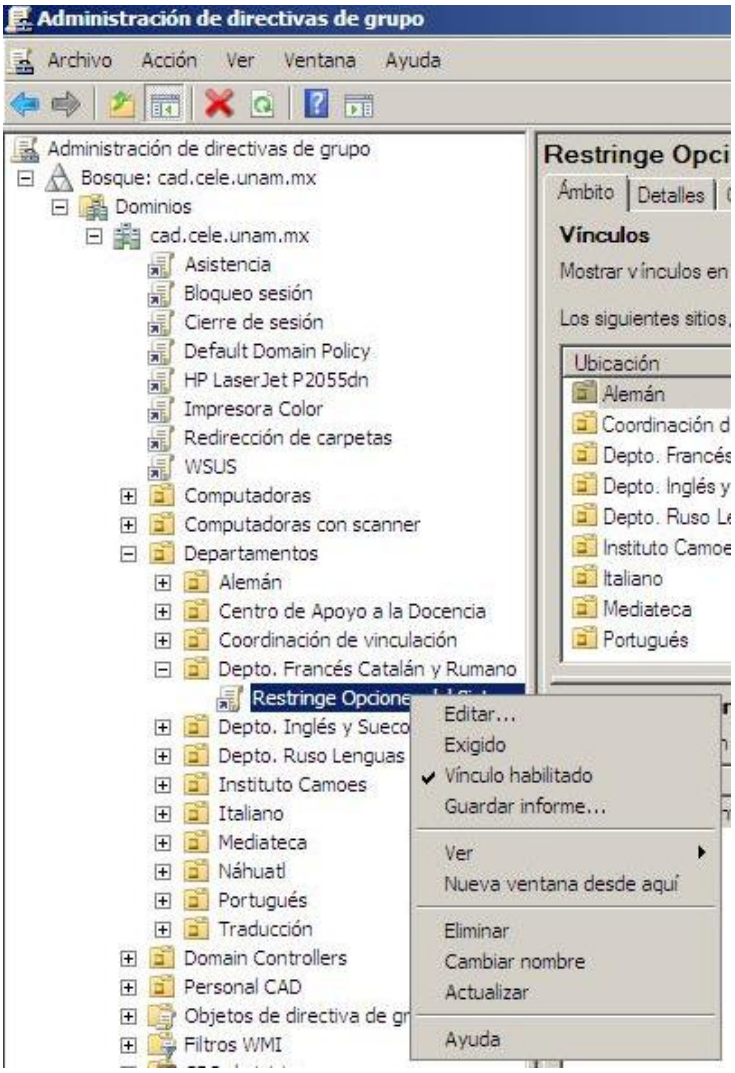




Dar clic con el botón derecho en la OU, dar clic en Crear un GPO en este dominio y vincularlo aquí.


Administración de directivas de grupo
Archivo
Acción
Ver
Ventana
Ayuda
Administración de directivas de grupo
Bosque: cad.cele.unam.mx
Dominios
cad.cele.unam.mx
Asistencia
Bloqueo sesión
Cierre de sesión
Default Domain Policy
HP LaserJet P2055dn
Impresora Color
Redirección de carpetas
WSUS
Computadoras
Computadoras con scanner
Departamentos
Alemán
Centro de Apoyo a la Docencia
Coordinación de vinculación
Depto. Francés Catalán y Rumano
Depto. Inglés y Sueco
Depto. Ruso Lenguas Asiáticas y
Instituto Camoes
Italiano
Mediateca
Náhuatl
Portugués
Traducción
Domain Controllers
Personal CAD
Objetos de directiva de grupo
Filtros WMI
GPO de inicio
Sitios
Modelado de directivas de grupo
Resultados de directivas de grupo
Depto. Francés Catalán y Rumano
Objetos de directiva de grupo vinculados
Herencia de
Orden de vínculos
GPO
1
Restringe Opcio
Crear un GPO en este dominio y vincularlo aquí...
Vincular un GPO existente...
Bloquear herencia
Asistente para modelado de directivas de grupo...
Nueva unidad organizativa
Ver
Nueva ventana desde aquí
Eliminar
Cambiar nombre
Actualizar
Propiedades
Ayuda

Una vez creada la Política de grupo, dar clic con el botón derecho en **Editar**.



Configurar las políticas en la ventana Editor de administración de directivas de grupo.