UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"INTEGRACIÓN DE DIRECTORIOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE
I N G E N I E R O EN COMPUTACIÓN
P R E S E N T A
GARCÍA LEÓN TRINIDAD EUGENIA

DIRECTOR DE TESIS: M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

México, D.F. MARZO DEL 2005

Esta tesis es dedicada a dos personas que fueron importantes durante su elaboración: En primer lugar, a mí Madre+, que siempre me espero y me hizo compañía durante la carrera. Ella hasta su último suspiro de su vida me demostró su amor, su confianza, su fortaleza y enseñanza; y desafortunadamente no pudo compartir conmigo esta etapa, pero sus recuerdos me impulsaron día a día para seguir adelante. La segunda persona al Ing. Cesar Balderas, quien me brindó su amistad, enseñándome que la vida no es fácil, pero siempre hay que ver lo positivo y bello de ella. Además me compartió sus conocimientos, ideas, tiempo y su trabajo, que para mí fueron una pieza importante para este logro. Este triunfo es para los tres.

DIOS
Quién con su luz me guió, para llegar hasta aquí...

A ROMAN
Por tus consejos que me han ayudado a crecer profesionalmente, para convertirme en lo que soy ahora. Piensa que mis errores se corrigieron y que intentaré no defraudarte!!!

A JUANITA
Una gran mujer en todos los aspectos. Gracias por ayudarme a entender mejor el mundo para poder ser feliz y por tenerme una vela encendida en la oscuridad.

A MIS PADRES+
Por todo lo bueno que me enseñaron ser, espero que desde el cielo, se sientan orgullosos de mí y piensen que nunca los he dejado de extrañar.

A GINA
La vida tiene que seguir, la libertad está en nuestras manos y nuestra felicidad en nuestro corazón. Pero mientras encuentras esa luz, yo te apoyaré.

A FERNANDO
Un hermano que me apoyado en toda la extensión de la palabra. Tú confianza será recompensada.

A GRISELDA
Por el apoyo incondicional sin merecerlo, que tu esfuerzo lo tengo valorado y no se me olvida.

A MIS SOBRINOS
Por enseñarme la parte bella de la vida con su inocencia, su dulzura y su amor desinteresado.

A JAQUI
Por su confianza y apoyo para lograr este proyecto,

A VICKY
Gracias por tolerar mi mal carácter y creer en mí. Espero que nuestra relación se haga cada día más fuerte.

A YOLANDA, LIZ, GABRIEL, MARCO Y ALFREDO
Por darnos su cariño y amistad a todo mi familia.

A LA FACULTAD DE INGENIERÍA,
Que represento mi segunda casa durante la carrera, donde adquirí conocimientos de sus profesores, que fueron guiando mi camino para que mis tropiezos fueran aprendizajes y los triunfos fueron disfrutados.

A MIS COMPAÑEROS Y AMIGOS

Cuando uno inicia su camino es grato conocer a esas personas que el destino nos da y más aún que pudieran ser algo especial. Les doy las gracias a todos mis amigos Andrés, Claudia, Cesar, Gil, Mayra, Mario, Vane, Vianey, Xochilth, los de la baticueva y compañeros quienes compartieron y disfrutaron los momentos más alegres y tristes de mi vida, demostrándome a cada instante su lealtad.

A ERANDI, ADAL Y CESAR

Por brindarme su amistad, motivarme y alentarme a no desistir hasta terminar el presente trabajo. Además de hacerme sonreír con sus ocurrencias y llenándome de alegría cada instante.

AL ING. ANTONIO CARVALLO MARTINEZ

Por haberme brindado su confianza, amistad y haberme dado una oportunidad de participar con su equipo de trabajo en este proyecto, proporcionándome todas las facilidades para emprenderlo.

Y a las tantas otras personas que por algún medio hicieron constar su amor, su apoyo y lealtad para este proyecto.

ÍNDICE

PÁG.

INTRODUCCIÓN

La empresa PEMEX Exploración y Producción desea que todas las Gerencias que incorporan este organismo, su administración de recursos informáticos deben ser integrados bajo las mismas condiciones para proporcionar un mejor servicio interno.

Los miembros de esta paraestatal han estado conscientes de que la Gerencia de Recursos Financieros es independiente a todo el organismo, porque tienen la administración informática a través de su propio Directorio Activo; por lo cual están interesados que esta dependencia migre sus recursos al Administrador Central denominado Directorio Activo de México.

Esta tesis se dedica a explicar un proceso de integración, a través de la migración de recursos informáticos, cumpliendo la principal expectativa de mantener los servicios y recursos informáticos disponibles de la gerencia antes y después de la extinción de su propio Directorio Activo.

De manera que en la institución un grupo de especialistas, llevó a cabo el análisis que determinó la solución y para ello se consideró que lo más viable para el proyecto era utilizar los recursos de la empresa para no generar un gasto adicional.

En el primer capítulo, se darán a conocer los conceptos sobre la estructura física y lógica del Directorio Activo en Windows 2000, la cuál es una aplicación que administra los recursos de la red. Los beneficios que se esperan obtener son una Administración Delegada, reforzamiento de la seguridad y extensión de la interoperatibilidad.

En el segundo capítulo, se analizarán los elementos de los dominios de origen y destino; y con base en esa información se determinarán los beneficios reales y los riesgos que se pueden presentar en la integración.

En el tercer capítulo, se conocerá el entorno de un piloto, con el fin de realizar las pruebas necesarias, que se analizarán y se identificarán los problemas del proyecto, corrigiendo errores para que la implementación sea un éxito.

En el antepenúltimo capítulo, contiene un diseño funcional del proyecto, con un planeación de las tareas y actividades que se tienen que realizar en la integración del dominio.

En el último capítulo, se explica como fue llevada a cabo la implementación de acuerdo al diseño, con el seguimiento adecuado al plan de trabajo para garantizar una mejor eficiencia en la operación, evaluación y el mantenimiento de los elementos de la Gerencia.

Finalmente, con está integración de la Gerencia al Directorio Activo de México, se mejoro la administración de los recursos informáticos dentro del organismo.

CAPÍTULO 1
DIRECTORIO ACTIVO

El Directorio Activo en Windows 2000 es una red de servicios de directorio, donde se almacena la información de los recursos de la red para organizarlos, administrarlos y controlarlos. Los servicios de directorio proporcionan una consistencia para el nombre, descripción, localización, acceso, administración y seguridad en la información acerca de estos recursos. Para poder implementar y administrar los servicios de directorio debemos tener conocimiento de su estructura por lo cual el Directorio Activo se divide en una estructura lógica y una física. Además nos proporciona una administración centralizada y poder administrarla en un solo lugar o en su defecto delegarla con otros administradores de la organización.

1.1 Definición

El Directorio Activo es una red de servicios de directorio en Windows 2000. Almacena la información para organizar, administrar y controlar los recursos de red y hace que estos sean accesibles para los usuarios y aplicaciones.

1.2 Funcionalidad

El Directorio Activo proporciona la funcionalidad del Servicio de Directorio, además incluyen los conceptos de organización, administración centralizada y control de acceso a los recursos de la red.

- **Organización**

  El Directorio Activo está organizado en secciones que permiten almacenar un gran número de objetos. Los servicios de directorio se pueden expandir de tal manera que inicialmente se tenga un servidor con pocos objetos y finalmente se pueden tener muchos servidores con millones de objetos.

- **Administración centralizada**

  El administrador principal puede dar privilegios a otros administradores para delegar la administración de los objetos del Directorio Activo, es decir puede otorgar derechos y restricciones a los objetos.

- **Control de acceso**

  El Directorio Activo facilita el acceso al usuario a los recursos sin que sea necesario conocer como están las topologías, las conexiones y los protocolos de la red. Por ejemplo: Un usuario está en la Cd. de México y pueda mandar imprimir a una impresora en Monterrey, en caso de que le soliciten alguna información.

1.3 Sistema de nombres de dominio (DNS)

El DNS (*Domain Name System*) es un mecanismo estándar de resolución de nombres en Intranet e Internet.

Proporciona las siguientes funciones en una red del Directorio Activo.

- **Resolución de nombres**

Se utiliza para la traducción de nombres de computadoras a direcciones IP y viceversa.

- **Convención de nombres para dominios**

El Directorio Activo usa una convención de nombres DNS para nombrar dominios. Los nombres de dominio DNS y dominios de Directorio Activo comparten una estructura común jerárquica. Pero ellos representan dos diferentes espacios de nombres[1] (ver figura 1.1) porque almacenan diferente información acerca de los mismos objetos físicos. Por ejemplo: unam.mx es un DNS válido y podría ser un dominio de Windows 2000.

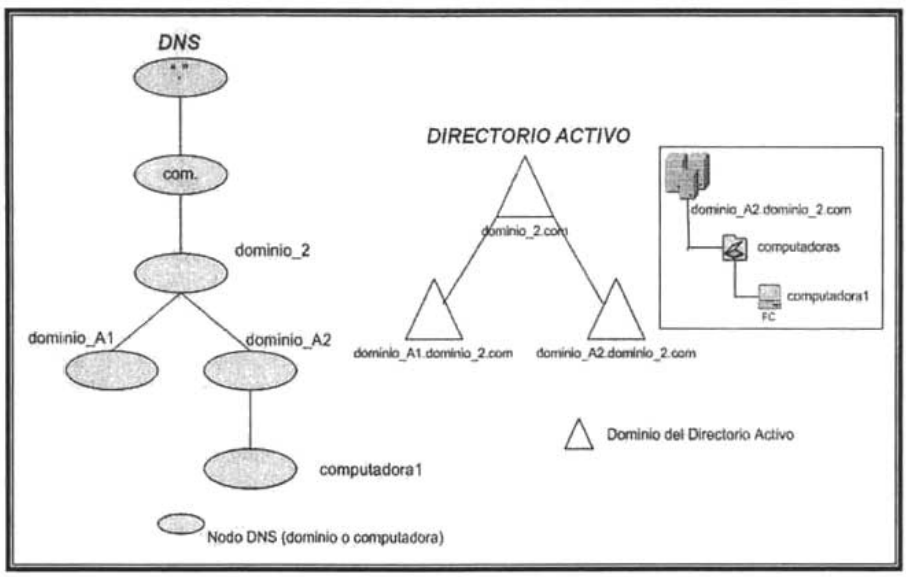

FIGURA 1.1 Espacio de nombres

[1] Espacio de nombres (*namespace*): Es una estructura de nombres jerárquicos en el cual los nombres en el espacio de nombres pueden resolver a los objetos que ellos representan.

- **DNS *Host names***

  Una computadora es representada en el espacio de nombres DNS y el espacio de nombres del Directorio Activo por el mismo nombre. Por ejemplo: Computadora1 está unida al dominio del Directorio Activo dominio_A2.dominio_2.com tiene su siguiente FQDN (*fully qualified domain name*): computadora1.dominio_A2.dominio_2.com. (ver figura 1.1)

- **Localización de los componentes del directorio activo**

  DNS identifica a los controladores de dominio por su servicio que ellos proporcionan. Por ejemplo: Cuando hacer una búsqueda en el Directorio, se localiza al catálogo global Server para el proceso.

Windows 2000 incorpora DNS Dinámico que permite propagar automáticamente a todos los servidores DNS, cualquier cambio que se produzca en los nombres de equipos o direcciones IP guardadas en su base de datos. Los controladores de dominio también registran de forma dinámica los SRV (Registros de recursos de servicios) en los servidores DNS Dinámico. De esta forma, los clientes de las redes pueden buscar los SRV en el servidor DDNS para localizar el Directorio Activo de la red y sus servicios. Por ejemplo: el servicio de inicio de sesión.

1.4 Esquema

El esquema del Directorio Activo contiene las definiciones de todos los objetos[2]. En Windows 2000, hay solamente un esquema por un bosque, así que todos los objetos creados en el Directorio conforman las mismas reglas.

El esquema contiene dos tipos de componentes (ver figura 1.2):

- **Objetos clase**

  Describe los posibles objetos que pueden ser creados en el Directorio. Cada objeto clase es una colección de atributos.

[2] Objeto: Se le denomina, a la representación de los recursos de red, como: usuarios, grupos, computadoras, unidad organizacional e impresoras. Sin embargo todos los servidores, dominios y sitios en la red son también representados como objetos.

- **Atributos**

Se definen independientemente de las clases. Cada atributo sólo se define una vez y se puede utilizar en múltiples clases.

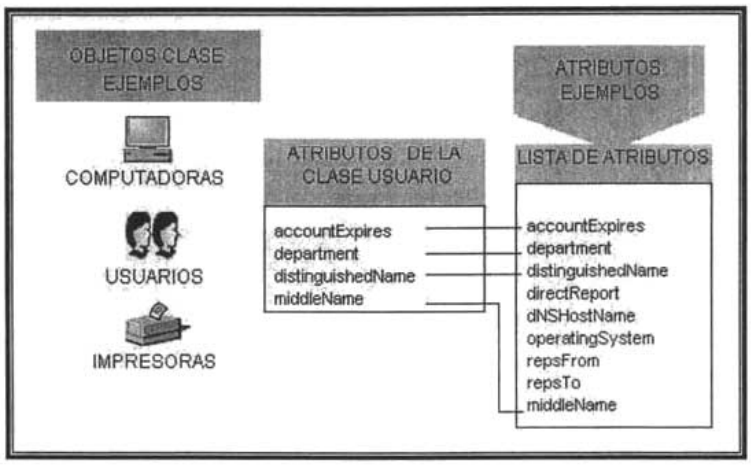

FIGURA 1.2 Esquema del directorio activo

1.5 *Lightweight directory access protocol* (LDAP)

Es un protocolo de comunicaciones para uso de redes TCP/IP. En él se define cómo un cliente LDAP, donde puede acceder a un servidor LDAP para realizar operaciones en el directorio y en sus datos compartidos.

En Windows 2000 se utiliza para la comunicación de clientes del Directorio Activo donde es usado para preguntar y actualizar el Directorio. LDAP, específica que un objeto debe ser representado por una serie de componentes de dominio, unidades organizacionales y nombres comunes los cuales son creados en la ruta LDAP. Esta ruta es usada para acceder objetos al Directorio Activo e incluyen los siguientes:

- **Nombre distinguido *LDAP (DN)***

En este tipo de denominación se incluye el nombre concreto del objeto y el camino completo dentro del árbol hasta llegar a él (ver tabla 1.1). Por ejemplo:

CN= Carla Martínez, OU= Ventas, DC= prueba, DC=com

Llave	Atributo	Descripción
CN	Nombre Común	Algún otro objeto que en los componentes del dominio y unidades organizacionales, tales como o usuarios y objetos de computadora.
OU	Unidad Organizacional	Una Unidad Organizacional que puede ser usada para contener otros objetos.
DC	Componente de Dominio	Un componente del nombre del DNS del dominio.

TABLA 1.1 Componentes de nombre distinguido

- **Nombre distinguido relativo *LDAP (RDN)***

Es el nombre concreto del objeto sin tener en cuenta su ubicación en el árbol. Por ejemplo:

CN= Carla Martínez

1.6 Estructura lógica

La estructura lógica es flexible y proporciona un método para un diseño jerárquico dentro del Directorio Activo. Esta estructura nos permite encontrar un recurso por su nombre o sus atributos. Los componentes lógicos son: Dominios, Unidades Organizacionales, Catálogo Global, Árboles y Bosques.

1.6.1 Dominios

La unidad básica de la estructura lógica para el Directorio Activo es el dominio.

Un dominio es un contenedor de computadoras, definidos por un administrador, que comparte una base de datos común. Los dominios tienen un nombre único y se usan para definir como la información y los recursos son organizados, almacenados y mantenidos por el administrador del dominio.

Los servidores dentro del dominio pueden tener los siguientes papeles:

- **Frontera de seguridad**

Su propósito es asegurar que el administrador de un dominio tenga los permisos necesarios y correctos para el funcionamiento dentro de él. Cada dominio tiene políticas de seguridad y relaciones de confianza con otros.

- **Unidad de replicación**

Cada dominio tiene controlador de dominio que contiene una replica del Directorio Activo. En un dominio particular se puede recibir cambios de información del Directorio Activo y replicarse éstos para todos los controladores de dominio.

- **Servidor miembro**

Pertenecen al dominio y se utilizan para almacenar los archivos y otros recursos de red.

1.6.2 Unidades organizacionales (OU)

Es un contenedor de objetos que se utiliza para organizarlos dentro de un dominio. Un OU puede contener objetos como: cuentas de usuarios, grupos, computadoras, impresoras, aplicaciones, ficheros compartidos y otras OUs.

Jerarquía de la unidad organizacional

Es agrupar objetos dentro de una jerarquía lógica mejorando las necesidades de tu administración. Puedes crear una OU jerárquica de las siguientes formas (ver figura 1.3):

- **Modelo administrativo de red**

Se basa en responsabilidades administrativas. Por ejemplo: Una organización tiene un administrador que es responsable para todos los usuarios y otro para todas las computadoras. Por lo tanto se debe crear una OU para usuarios y otra para computadoras.

- **Estructura organizacional**

Se basa en departamentos o fronteras geográficas

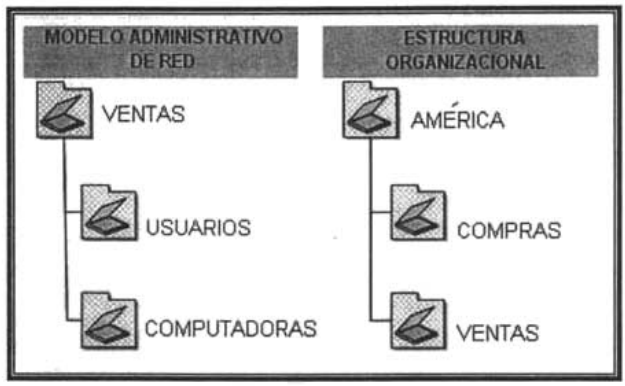

FIGURA 1.3 Jerarquía de la unidad organizacional

Control administrativo de OUs
Es delegar el control administrativo de los objetos de una OU dentro de un dominio. Para delegar el control debes especificar los permisos para la OU y los objetos que contengan la unidad para uno o más usuarios o grupos.

1.6.3 Árboles y bosques

1.6.3.1 Árbol

Es una agrupación jerárquica de uno o más dominios que comparten un espacio de nombres contiguos.

Cuando agregamos un nuevo dominio a un árbol, el nuevo dominio es llamado un dominio hijo. El nombre del dominio sobre el dominio hijo es llamado padre. El nombre del dominio hijo es una combinación del dominio hijo y el dominio padre separado por un punto para integrar su nombre DNS. Este DNS forma un espacio de nombres contiguos jerárquica. Al primer dominio en un árbol se le denomina dominio raíz *(the tree root domain)* (ver figura 1.4).

Ejemplo: Un dominio hijo llamado dominio_A que tiene un dominio padre llamado dominio_1.com entonces su DNS del dominio hijo sería dominio_A.dominio_1.com (ver figura 1.4)

1.6.3.2 Bosque

Es una colección de uno o más árboles. Los árboles en un bosque no comparten un espacio de nombre contiguo. El primer dominio en un bosque es llamado dominio raíz *(forest root domain)* (ver figura 1.4).

Los dominios en un bosque comparten información de configuración común, esquema común y catálogo global. Por Ejemplo: Dos organizaciones dominio_1.com y dominio_2.com no comparten un espacio para nombres, pero los dominios están en un bosque donde comparten recursos y funciones administrativas (ver figura 1.4).

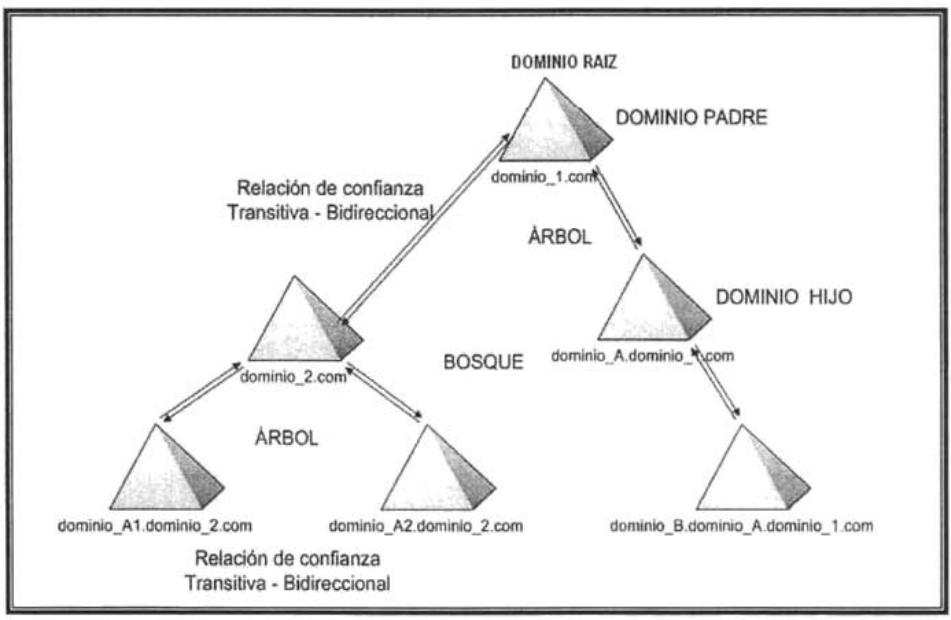

FIGURA 1.4 Árbol y bosque

1.6.3.3 Relaciones de confianza

La autentificación de las cuentas entre dominios es fácil hacerlo mediante las relaciones de confianza bidireccional y transitiva basados en el protocolo de seguridad Kerberos V5.

1.6.3.3.1 Confianza entre dominios

Es una relación establecida entre los dominios que habilita un controlador de dominio en un dominio para autentificar al usuario en otro dominio.

Las relaciones de confianza entre dominios pueden ser:

- **Unidireccional**
  Relación única de confianza. Por ejemplo el Dominio A tiene una confianza unidireccional con el Dominio B, y éste a su vez con el dominio C. Pero Dominio A no tiene ninguna relación de confianza con el Dominio C. Todas las relaciones unidireccionales son intransitivas y todas intransitivas son unidireccionales.

- **Bidireccional**
  Significa que hay dos caminos en direcciones opuestas entre dos dominios. Por ejemplo, el dominio dominio_A2.dominio_2.com confía en dominio_2.com en una dirección y dominio_2.com confía en dominio_A2.dominio_2.com en la otra dirección opuesta (ver figura 1.4).

- **Transitiva**
  La relación de confianza extendida a un dominio es automáticamente extendida para todos los demás dominios que confían en ese dominio. Por ejemplo: el dominio de dominio_A1.dominio_2.com confía directamente en dominio_2.com y también dominio_A2.dominio_2.com confía directamente en dominio_2.com porque tiene una relación de confianza transitiva, pero dominio_A1.dominio_2.com confía indirectamente en dominio_A2.dominio_2.com (ver figura 1.4).

Todas las confianzas entre dominios de un bosque Windows 2000 son transitivas. Las relaciones de confianza transitivas son siempre bidireccionales. Además solo pueden existir entre dominios de Windows 2000 del mismo bosque.

La relación de confianza transitiva-bidireccional se crea automáticamente entre dominios adyacentes cuando se crea un dominio en un árbol de dominios. En un bosque, se crea

automáticamente esta relación de confianza entre el dominio raíz del bosque y el dominio raíz de cada árbol de dominio que se agrega al bosque.

- **Intransitiva.**

Está limitada por dos dominios de la relación y no fluye a cualquier otro dominio del bosque. En la mayoría de los casos, se debe crear las confianzas intransitivas manualmente.

Una relación de confianza intransitiva se puede establecer de las siguientes formas:

- Un dominio de Windows 2000 y un dominio de Windows NT,
- Un dominio de Windows 2000 en un bosque y un dominio de Windows 2000 en otro bosque, y
- Un dominio de Windows 2000 y un protocolo de seguridad Kerberos V5.

1.6.3.3.2 Confianzas explícitas entre dominios

Las confianzas explícitas son relaciones de confianza que son creadas por los usuarios. Para crearlas se necesita conocer los nombres de dominio y una cuenta de usuario con privilegios para poder hacerlo en cada dominio. A cada confianza se le asigna una contraseña que solamente deben conocer los administradores de los dominios relacionados. Existen dos clases de confianzas explícitas:

- **Confianzas explícitas externas**

Crean relaciones de confianza con dominios que se encuentran fuera del bosque. La ventaja es permitir la autentiticación de usuarios en un dominio que no se encuentra en las rutas de confianza de un bosque. Todas las confianzas externas son intransitivas y de un solo sentido.

- **Confianzas explícitas de acceso directo "*Shortcut Trusts*"**

Son confianzas transitivas de uno o dos sentidos, que permiten acortar la ruta en árbol complejo. Se crean de forma explícita entre dominios del mismo bosque. Además es una optimización del rendimiento que acorta la ruta de confianza. Para que un controlador de dominio de otro dominio pueda conceder el acceso a

determinados recursos, se debe determinar si el dominio destino tiene una relación de confianza con el dominio en el que se encuentra la cuenta (dominio origen). En Windows 2000 se calcula una ruta de confianza entre los controladores de los dominios de origen y de destino; calcular y atravesar la ruta puede llevar tiempo.

1.6.3.3.3 Protocolo kerberos

Kerberos V5 es un protocolo de seguridad para la identificación de los usuarios. Consiste en un servidor central donde se verifica la identidad de los usuarios y autoriza el acceso a los recursos enviando claves específicas. Cada petición de un recurso va acompañada de un ticket. Si el ticket es válido se autoriza el acceso al recurso y en caso contrario, se deniega.

El centro de distribución de claves (KDC) que se ejecuta en cada controlador de dominio como parte del Directorio Activo, se utiliza para almacenar todas las contraseñas del cliente y otros datos de su cuenta.

El proceso de identificación Kerberos V5 funciona de la manera siguiente[3]:

1. Un usuario de un sistema cliente se identifica en el KDC mediante una contraseña o tarjeta inteligente.
2. El KDC emite al cliente un vale especial que concede vales (TGT[4]). El sistema de cliente utiliza este (TGT) para tener acceso al servicio de concesión de vales (TGS[5]) que forma parte del mecanismo de autentificación Kerberos V5 en el controlador de Dominio.
3. El TGS emitirá al cliente un vale de servicio.
4. El cliente presenta este vale de servicio al servicio de red solicitado. El vale de servicio prueba la identidad del usuario al servicio y la identidad al usuario.

[3] Pág 902 Windows 2000 Server: Instalación, Configuración y Administración.
[4] TGT: *Ticket Granting Ticket*
[5] TGS: *Ticket Granting Services*

Los servicios Kerberos se instalan en cada controlador de dominio y un cliente en cada estación de trabajo. Cada controlador de dominio trabaja como un KDC.

1.6.4 Catálogo global

El catálogo global permite el almacenamiento de las propiedades de un subconjunto de los atributos de todos los objetos del Directorio Activo. De esta manera se pueden realizar búsquedas de objetos en el directorio.

Realiza dos funciones de directorio principales:

- Permite el inicio de sesión en la red al proporcionar información de pertenencia a grupos universales a un controlador de dominio cuando comienza un proceso de inicio de sesión.

- Encuentra información del Directorio Activo en el bosque con independencia de cual sea el dominio que contiene realmente los datos. Asegurando que los usuarios puedan encontrar los objetos a los cuales tienen acceso.

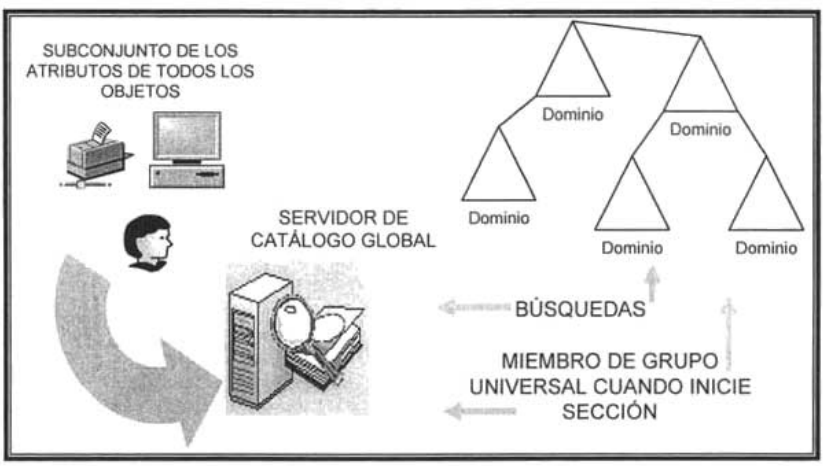

FIGURA 1.5 Catálogo global

1.7 Estructura física

La estructura física es usada para configurar y administrar el tráfico de red. La estructura define dónde y cuándo ocurre la replicación y el inicio de sesión. Los componentes físicos son el controlador de dominio y los sitios.

1.7.1 Controlador de dominio

Un *Domain Controller* es una computadora que tiene como plataforma Windows 2000 *server* donde almacena una réplica del directorio. También administra los cambios de información para el Directorio y replica estos cambios a los otros controladores de dominio en el mismo dominio. Estos controladores almacenan datos en el directorio y administran los procesos de inicio de sesión, identifican y búsquedas del directorio.

1.7.1.1 Replicación del directorio activo

La replicación es el proceso de actualización de información en el Directorio Activo desde un controlador a otro en una red. Sincroniza la copia de los datos, asegurando que toda la información está disponible para todos los usuarios y servicios al mismo tiempo.

La replicación de información en todos los dominios ocurre con las actualizaciones, estás son iniciadas cuando uno o más objetos en un controlador de dominio son agregados, modificados, borrados o movidos.

Los controladores de dominio en un dominio y en un bosque automáticamente replican algún cambio para la base de datos del Directorio Activo a través del proceso llamado replicación *Multimaster* (ver figura 1.6). En un modelo de replicación *Multimaster*, cada dominio tiene uno o dos controladores. Cada controlador almacena una copia de la base de datos para su dominio y administra los cambios y actualizaciones para su copia.

Los controladores de dominio tal vez dejan diferente información por periodos cortos hasta que todos los controladores tengan una sincronización de sus cambios para el Directorio.

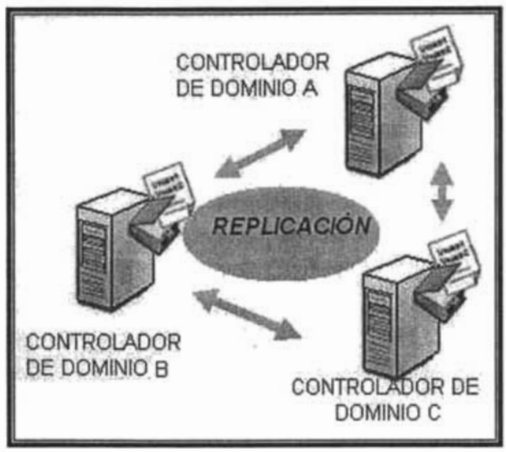

FIGURA 1.6 Replicación multimaster

1.7.1.2 Protocolos de replicación

Para asegurar que las computadoras en una red estén disponibles para comunicarse para enviar y recibir actualizaciones durante la replicación, ellos deben compartir un lenguaje común conocido como protocolos de replicación.

1.7.1.2.1 *Remote procedure call* (RPC)

RPC es un protocolo estándar para cliente/servidor, es decir el proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Éste, al recibir la llamada, estudia los procedimientos del proceso llamado, obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta.

RPC sincroniza la transferencia, requiere disponibilidad de conexión, genera menos tráfico y se usa para replicar dentro y entre sitios en el Directorio Activo. Puede utilizarse con controladores de dominio en el mismo dominio.

1.7.1.2.2 *Simple mail transfer protocol* (SMTP)

Es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente debe enviar desde un computador al

servidor de otro, pero no específica cómo debe de almacenarse el correo ni con qué frecuencia se debe intentar el envío de los mensajes.

SMTP soporta la replicación del esquema de configuración, el catálogo global y además sirve para la replicación entre sitios. Pero no puede ser usado con controladores de dominio en el mismo dominio.

1.7.1.3 Maestro de operaciones

Algunos cambios para el Directorio Activo son imprácticos para el funcionamiento usando el modelo de replicación *Multimaster* en conflictos de operaciones esenciales.

Los maestros de operaciones (*single master operations*), son asignados específicamente para los controladores de dominio. Los maestros de operaciones son un poco diferentes en cuanto a que sólo puede tener uno por bosque o uno por dominio, dependiendo de la función que el Maestro de operaciones intente satisfacer.

Un maestro de operaciones es un controlador de dominio que funciona como un role específico del Directorio Activo y controla un conjunto de cambios para el directorio. Para cada role, solamente el controlador deja que cada role pueda hacer los cambios asociados al directorio. Hay caminos para mover estos cambios desde un controlador a otro, en caso de que un master falle.

Los cinco tipos de Maestro de operaciones son el Maestro de esquema, Maestro de nombre de dominio, el Maestro de RID (Identificador relativo), el Emulador PDC y el Maestro de infraestructura. El primer cuadro que construya en ese primer dominio de raíz tendrá los cinco tipos de Maestros de operaciones. Su segundo dominio tendrá tres de las funciones: Maestro de RID, Emulador PDC y el Maestro de infraestructura (ver figura 1.7).

Puede realizar la ejecución sin ninguno de éstos por un periodo limitado de tiempo. Incluso puede no saber que le falta uno hasta que realiza algo que requiere una de estas funciones.

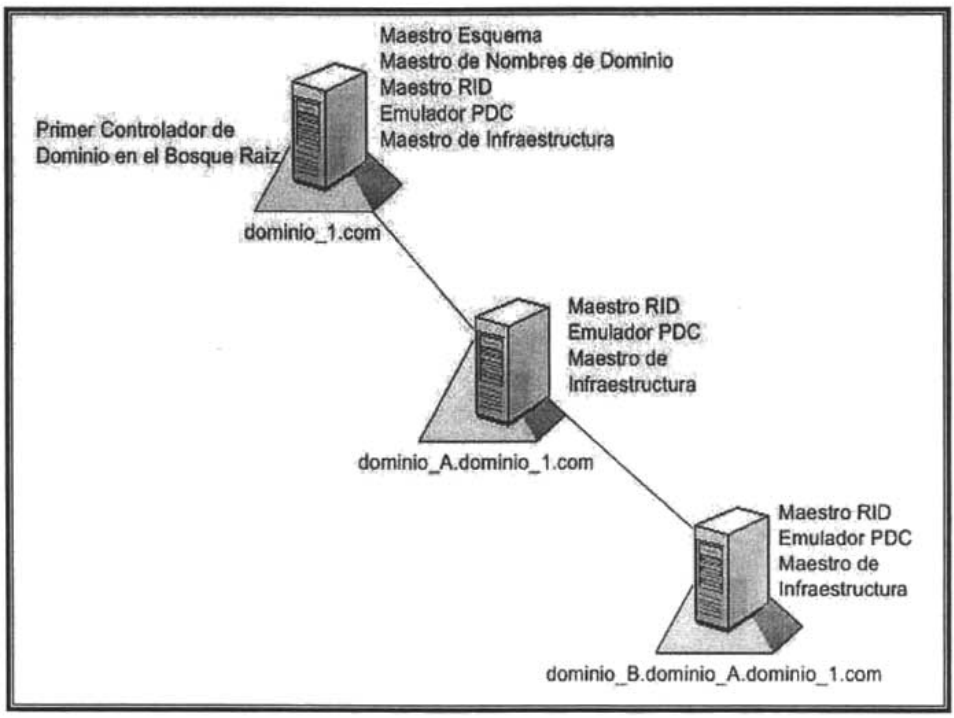

FIGURA 1.7 Maestro de operaciones

1.7.1.3.1 Maestro esquema

Maestro Esquema (*Schema Master*). Permite hacer todas las actualizaciones y modificaciones al esquema del Directorio Activo por usuarios que estén en el grupo de Administradores; y replica todas las actualizaciones para todos los controladores de dominio en el bosque (ver figura 1.8).

Solamente un controlador de dominio por bosque puede tener este rol. Además debe estar en un controlador de dominio que sea Catálogo Global y debe ser transferido únicamente dentro del dominio raíz.

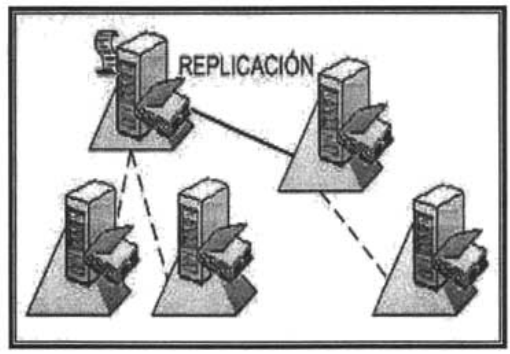

FIGURA 1.8 Maestro esquema

1.7.1.3.2 Maestro de nombres de dominio

Sólo puede existir un Maestro de nombre de dominio (*Domain Naming Master)* por bosque y debe estar en un controlador de dominio que sea Catálogo Global. El Maestro de nombre de dominio es el equipo que asegura que no tenga dos dominios en el mismo árbol con el mismo nombre (ver figura 1.9).

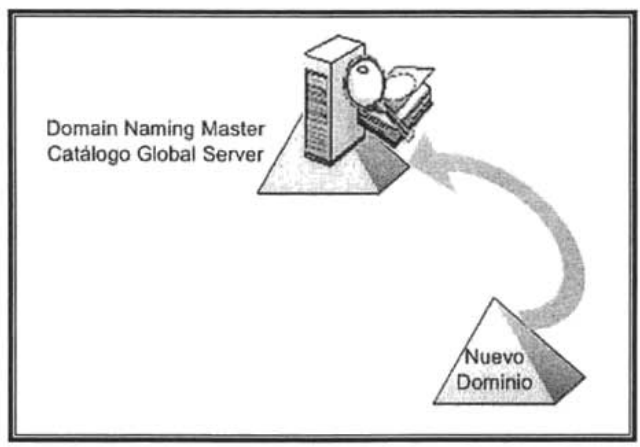

FIGURA 1.9 Maestro de nombres de dominio

Por ejemplo, si establece dominio_1.com como su dominio de raíz y crea dominio_A.dominio_1.com, el Maestro de nombre de dominio evitará que coloque otro dominio con el mismo nombre evitando así un conflicto. Además permite agregar o remover dominios dentro del bosque; y debe ser transferido únicamente dentro del dominio raíz.

1.7.1.3.3 Maestro emulador del controlador principal del dominio

Primary Domain Controller Emulator Master (PDC Emulator) utilizado por compatibilidad con ambientes Windows NT 3.51 y 4.0. Este emulador es el primer controlador de dominio que es creado en un nuevo dominio, por lo tanto es uno sólo por dominio (ver figura 1.10).

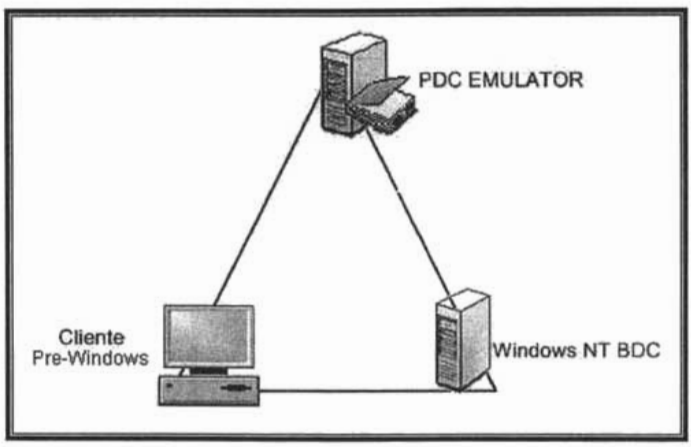

FIGURA 1.10 Maestro emulador PDC

El PDC emulator tiene las siguientes funciones:

- Actúa como un PDC para una respaldo de un controlador de dominio (*backup domain controllers [BDCs]*). Si un dominio contiene una BDCs o un cliente que corre en Windows 2000 ó Windows, el PDC emulador funciona como un de Windows NT PDC. Este PDC sirve como cliente y replica los cambios para algunas BDCs que corren en Windows NT.
- Administra los cambios de contraseña de computadoras que trabajan en Windows NT, Windows 95, ó Windows 98, las cuales son escritas para el directorio.

- Minimiza las replicaciones para cambios de contraseña.
- Sincroniza el tiempo de todos controladores de dominio a través del dominio principal
- Previene las posibilidades de sobrescribir el Grupo de Políticas de objetos (GPOs).

1.7.1.3.4 Maestro de identificadores relativos

Asocia secuencias de identificadores relativos (RID) a cada uno de los distintos controladores de su dominio. Únicamente puede haber un maestro de identificadores relativos en cada dominio del bosque. Cada vez que un controlador de dominio crea un objeto de usuario, grupo o equipo, asigna al objeto un identificador de seguridad único. Este identificador de seguridad consta de un identificador de seguridad de dominio (SID) que es el mismo para todos los identificadores de seguridad creados en un dominio específico y de un identificador relativo (RID) que es único para identificador de seguridad creado en el dominio. Además previene la duplicación de los objetos cuando son movidos de un controlador a otro.

1.7.1.3.5 Maestro de infraestructura

El Maestro de infraestructura es uno por dominio. Debe estar en un controlador de dominio que no sea catálogo global porque no contiene referencias a los objetos.

Realiza un seguimiento de actualización y sincronización del movimiento de los objetos de referencia. Si mueve un usuario de un dominio o Unidad organizativa a otra parte, el nombre del usuario cambiará. Y desea que el grupo en donde el usuario se encuentra refleje ese cambio de nombre lo más pronto posible. El Maestro de infraestructura lo hará en su lugar.

Los objetos de referencia contienen los objetos de identificador único global (GUID[6]), nombres distinguidos y posiblemente un identificador único de seguridad (SID[7]). Los dos últimos son periódicamente actualizados para reflejar los cambios en el objeto actual. Estos

[6] GUID: *Globaly Unique Identifier*
[7] SID: *Security Identifier*

cambios incluyen movimientos dentro y entre dominio, así como borrado de objetos.
El maestro de infraestructura actualiza objetos referenciados, por las siguientes reglas:

- Si el objeto se mueve completamente, su nombre distinguido cambiará porque el representa su localización exacta en el directorio.
- Si el objeto es movido dentro del dominio, su SID será el mismo.
- Si el objeto es movido a otro dominio, el SID cambiará para incorporarse al del nuevo dominio.
- El GUID no cambiará, no importando la localización.

1.7.2 Sitios

Es una o más subred TCP/IP enlazadas mediante conexiones de red por un enlace de alta velocidad.
Puedes crear sitios para controlar:

- **El tráfico de replicación**
  Cuando un cambio ocurre en el Directorio Activo, el sitio puede ser usado para controlar cómo y cuándo los cambios son replicados para controladores de dominio en otro sitio.

- **Trafico de inicio de sesión**
  Cuando un usuario desea iniciar sesión, intenta encontrar un controlador de dominio en el mismo sitio como la estación de trabajo.

- **Petición al catálogo global**
  Cuando una petición para el catálogo es solicitada por un usuario o un controlador de dominio encuentra un catálogo global en un sitio local.

Si se establecen varios sitios, debe tenerse en cuenta cómo va intercambiarse la información entre los sitios para poder revisar, ajustar o complementar la configuración actual de vínculos de los sitios. Para complementar la topología de la replicación entre los sitios de la red, se pueden crear vínculos de sitios para que la configuración de replicación sea más fiable y tolerante a errores.

1.8 Administración en una red de Windows 2000

1.8.1 Métodos de administración

El Directorio Activo proporciona a los administradores una manera fácil y útil de centralizar la administración de todos de los escritorios de las computadoras o las tareas administrativas de manera descentralizada en una organización.

Los métodos de administración que utiliza el Directorio Activo son:

- Administración Centralizada
- Administración del ambiente de Usuario.
- Delegación del Control Administrativo.

1.8.1.1 Administración centralizada

El Directorio Activo permite la administración centralizada de un gran número de recursos desde una localización central (ver figura 1.11).

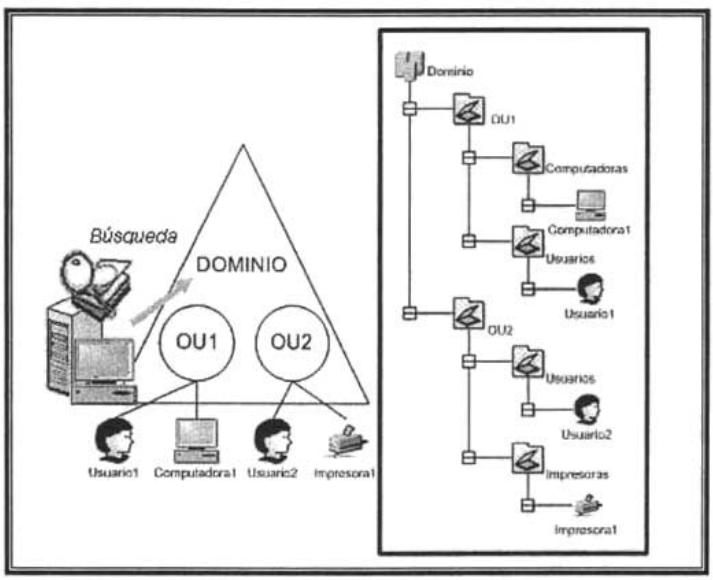

FIGURA 1.11 Administración centralizada

Ventajas

- El Directorio Activo asigna un solo administrador para manejar los recursos.
- Permite la facilidad de localizar la información acerca de los objetos por medio de búsquedas.
- Deja que varios grupos de objetos estén en contenedores con similitud en necesidades para proporcionarles una autoridad administrativa para aplicar una configuración de políticas de grupo y delegar el control administrativo.
- Utiliza una Políticas de Grupo para especificar la configuración para un Sitio, Dominio o una Unidad Organizacional.

1.8.1.2 Administración de un ambiente de usuario

Significa controlar a los usuarios que pueden hacer en el momento que se autentican en la red además asegura que los usuarios tengan las configuraciones necesarias en el escritorio, conexiones y en la interfaz evitando que ellos corrompan o configuren incorrectamente su ambiente.

El Directorio Activo proporciona una herramienta para administrar el ambiente de usuario llamada "*Group Policy*", Políticas de Grupo que es habilitada por los administradores para especificar la configuración de usuarios y computadores a nivel Dominio, Sitio y Unidad Organizacional. Una Política de Grupo afecta a todo el contenedor que es aplicado y Windows 2000 aplica la configuración de está cuando la computadora inicia o el usuario inicia sesión (ver figura 1.12).

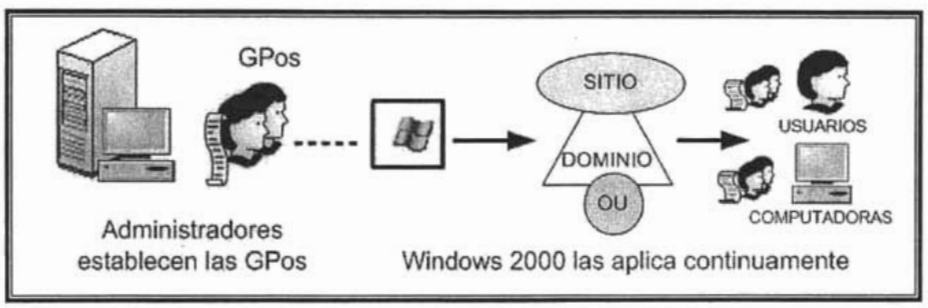

FIGURA 1.12 Políticas de grupo

El tipo de configuración de políticas de grupo nos facilita la configuración de un ambiente de usuario o computadora y se utilizan las siguientes:

- **Plantillas administrativas**
  Son una colección de políticas de grupo que modifican la configuración del registro, organizadas en siete tipos (ver tabla 1.2), las cuáles, las configuraciones de equipos se basan en la administración de Windows 2000 mientras las configuraciones de usuario se basan en el control de un ambiente de escritorio.

Tipo de Configuración	Descripción	Disponible
Componentes de Windows	Las partes de Windows 2000 y sus herramientas y componentes que pueden acceder.	Computadoras y Usuarios
Sistema	Iniciar y terminar procedimientos. Administrar las GPOs, las cuotas de disco e implementar los procesos *loopback*[8].	Computadoras y Usuarios
Red	Las propiedades de conexiones de red y conexiones dial-in	Computadoras y Usuarios
Impresoras	Configuraciones de Impresoras	Computadoras
Menú Inicio y Task bar	Agrega o elimina botones. Por ejemplo el comando ejecutar.	Usuarios
Escritorio	Puede configurar agregando o quitando iconos que no accesos los usuarios.	Usuarios
Panel de Control	Varias aplicaciones como restricción a agregar/quitar programas.	Usuarios

TABLA 1.2 Plantillas administrativas

- **Seguridad**
  Estas configuraciones son en computadora local, dominio y red. Incluyen los accesos de control de los usuarios a la red, la cuenta de inicio y auditar políticas. Por ejemplo: puedes controlar los intentos de inicio de sesión en caso de varios errores se bloqueará la cuenta.

[8] El proceso Loopback es una configuración de GPOs que fuerza la configuración de usuario para que se aplique en la computadora y más tarde al objeto usuario para evitar conflictos.

- **Instalación de software**

Se puede configurar una administración centralizada de software para instalarlo, actualizarlo o removerlo.

- ***Scripts***

Las configuraciones de scripts pueden habilitarse cuando inicia o se apaga un equipo o cuando se inicia o cierra sesión un usuario. Se utilizan procesos por lotes y se determina el orden en los cuales se ejecutarán.

- **Servicios de instalación remota**

Configura las opciones disponibles que controlan a los usuarios cuando corren un cliente de Instalación *Wizard* usado por RIS.

- **Carpetas redireccionadas**

Configura una carpeta de almacenamiento al perfil del usuario en un servidor de red. Esta configuración crea una liga al servidor y la carpeta compartida aparece localmente, donde el usuario cuando inicie sesión en cualquier equipo encontrara su carpeta redireccionada.

1.8.1.3 Delegación del control administrativo

La delegación es la habilidad para asignar la responsabilidad de la administración de los objetos del Directorio Activo a usuarios, grupos u organización (ver figura 1.13).

Puedes delegar el control administrativo de la siguiente forma:

- Asignación de permisos, tales como: Control total para una unidad organizacional específica para diferentes grupos de dominio local.
- Asignando permisos para modificar los atributos específicos de un objeto en una unidad organizacional. Por ejemplo: Asignando los permisos para cambiar nombre, dirección, teléfono, etc., de una cuenta de usuario.
- Asignando permisos para el funcionamiento de las mismas tareas, tales como cambiar contraseña en todas las OU de todo el dominio.

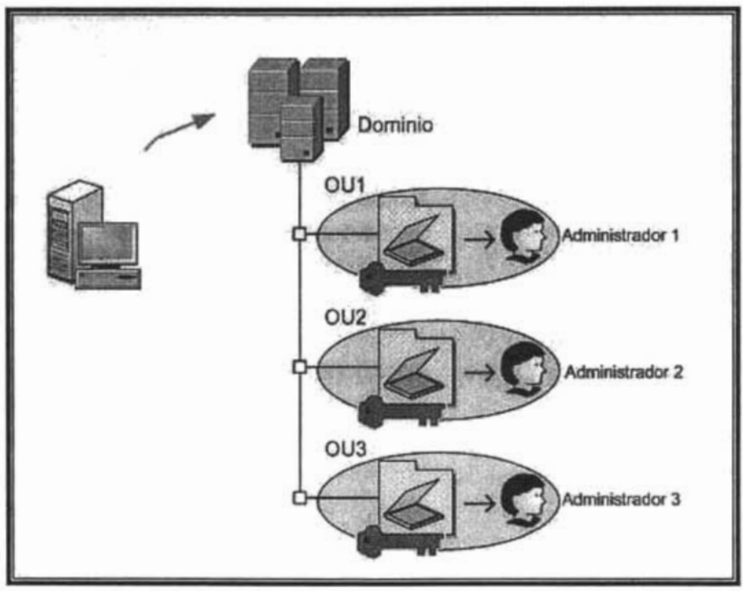

FIGURA 1.13 Delegación del control administrativo

Windows 2000 proporciona una herramienta administrativa para:

- Otorgar los permisos que han sido asignados a los usuarios para una tarea administrativa.
- Diseñar una interfaz para usuario con privilegios limitados de administración.

1.8.2 Configuración de usuarios y grupos

Después de explicar como se comporta el Directorio Activo, es importante definir la configuración de los objetos de usuarios y grupos dentro del Directorio.

1.8.2.1 Usuarios

Una cuenta de usuario es un objeto almacenado en el Directorio que habilita *single sing-on*[9].

[9] *Single sing-on*, significa que el usuario necesitan autenticarse, es decir introducir su nombre y contraseña solamente una vez en una estación de trabajo para poder acceder a todos los recursos de la red donde este autorizado.

Existen diferentes tipos de cuentas de usuarios:

- **Cuenta de usuario local**
  Es aquella cuenta donde habilita a un usuario a iniciar sesión en una computadora específica para conseguir acceso a los recursos de esa computadora.

- **Cuenta de usuario de dominio**
  Es aquella cuenta donde habilita a un usuario a iniciar sesión al dominio para conseguir accesos a los recursos de la red.

- **Cuenta de usuario built-in**
  Es aquella cuenta donde habilita a un usuario para el funcionamiento de tareas administrativas o para conseguir accesos temporales a los recursos de la red.

El usuario puede iniciar sesión con:

- **Nombre principal de usuario** (User Principal Name)
  Este es usado para iniciar sesión en cliente Windows 2000 y se compone de dos partes: Prefijo y Sufijo (ver figura 1.14). Además no se puede cambiar cuando se mueve una cuenta en diferente dominio, porque este nombre es único dentro del bosque y puede ser el mismo que el correo electrónico.

- **User logon name** (Pre-Windows 2000)
  Si un usuario inicia sesión en estaciones de trabajo que tenga cliente una versión de Windows anterior debe autenticarse de la siguiente forma: dominio\nombre. Por ejemplo de la Figura 1.14 dominio_1\lquirozc.

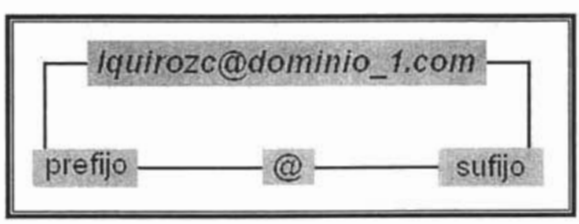

FIGURA 1.14 Nombre principal de usuario

1.8.2.2 Grupos

Un grupo se considera como una colección de cuentas de usuario y se utiliza para administrar eficientemente los accesos a los recursos del dominio.

Existen dos tipos de grupos en el Directorio Activo:

- **Grupos de seguridad**
  Estos grupos se muestran en las listas DACL[10]. Además se pueden utilizar también como entidades de correo electrónico es decir, al enviar un mensaje de correo electrónico al grupo, el mensaje se envía a todos los miembros del grupo.

- **Grupos de distribución**
  Este tipo de grupos no es posible habilitar la seguridad ya que no aparecen en las listas DACL. Sólo se pueden utilizar con aplicaciones de correo electrónico, para enviar correo a los grupos de usuarios.

Cada grupo de seguridad o de distribución tiene un ámbito que identifica el alcance de aplicación del grupo. Existen cuatro tipos de grupos en función a su aplicación como se muestra en la siguiente tabla 1.3.

[10] DACL: Listas de control de acceso discrecional que es el lugar donde están definidos los permisos sobre los recursos y los objetos.

Grupos	Globales	Universales	Dominio Local
		Miembros "Membership"	
Modo Mixto [11]	Cuentas de usuarios del mismo dominio.	No aplica.	Cuentas de usuarios y grupos globales de algún dominio.
Modo Nativo	Cuentas de usuarios y grupos globales del mismo dominio.	Cuentas de usuarios, grupos globales y grupos universales de algún dominio en el bosque.	Cuentas de usuarios, grupos globales y grupos universales de algún dominio en el bosque, y grupos de dominio local del mismo dominio.
		Puede ser miembro de	
Modo Mixto	Grupos de dominio local.	No aplica	No ser un miembro de algún grupo.
Modo Nativo [12]	Grupos de dominios locales y universales en algún dominio y grupos globales en el mismo dominio.	Grupos de dominios locales y universales en algún dominio.	Grupos de dominio local en el mismo dominio.
		Alcance	
	Visible en su propio dominio y en todos dominio relacionados.	Visibles en todos los dominio en un bosque	Visibles en su propio dominio.
		Permisos	
	Todos los dominios en el bosque	Todos los dominios en el bosque.	Dominio en el cual el grupo de dominio local exista.

TABLA 1.3 Tipos de grupo

11 Modo Mixto: Es la configuración predeterminada del modo de dominio en los controladores de dominio de Windows 2000, permite que los controladores en Windows NT y Windows 2000 coexistan en un dominio.

12 Modo Nativo: Se habilita cuando todos los controladores de dominio se han actualizado en Windows 2000.

CAPÍTULO 2
ANÁLISIS

La finalidad de la organización es integrar una Gerencia al Dominio Sede para tener un control centralizado, por ello en este análisis se identificarán los elementos del Directorio Activo de la Región Sede y de la Gerencia de Recursos Financieros y en base a esa información se determinarán los beneficios reales y los riesgos que se pueden presentar en la nueva reestructuración.

2.1 Planteamiento general

La Organización de PEP (PEMEX Exploración y Producción) tiene su propio Directorio Activo, la región sede es un dominio de ese directorio. La Gerencia de Recursos Financieros "GRF" es independiente por lo tanto tienen su propio Directorio Activo.

PEP desea integrar todos los elementos de la Gerencia de Recursos Financieros en una Unidad Organizacional, dentro del Directorio del Dominio Sede, para no administrar complejas relaciones de confianza, proporcionar nuevas innovaciones tecnológicas y mejores servicios.

En la figura (2.1) se visualiza este planteamiento.

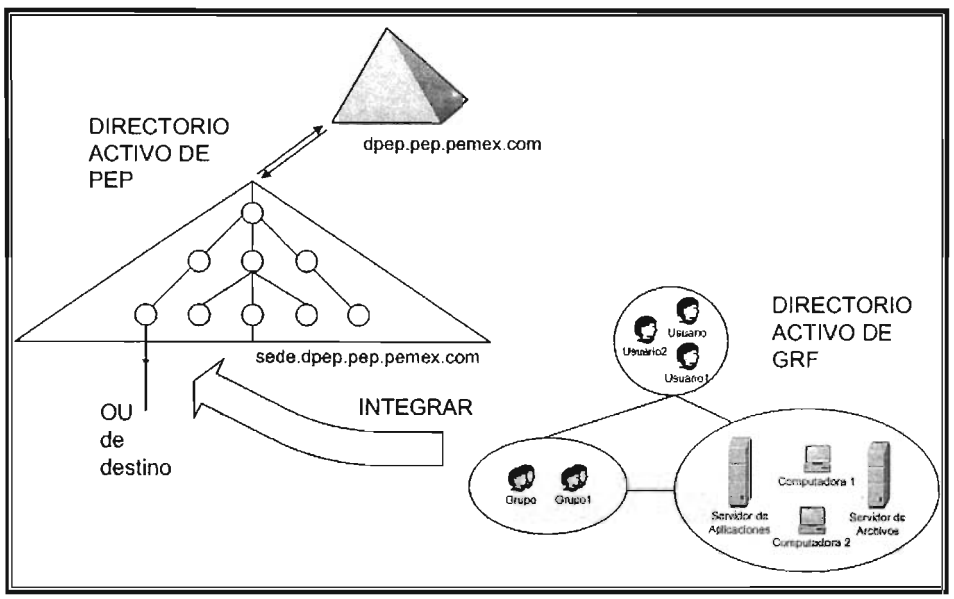

FIGURA 2.1 Problema original

2.2 Entorno de la región sede

El organismo Pemex Exploración y Producción "PEP" tiene muchas regiones en el país. En la Ciudad de México se conoce como la Región Sede, en ésta se conocerán las partes del Directorio Activo como se mencionaron en el capítulo anterior, las cuales se documentarán sin afectar la integridad y confidencialidad de su información.

2.2.1 Esquema de DNS

Actualmente el Organismo tiene definido un esquema híbrido de DNS:

- Para la red externa, esta implementado un DNS sobre plataforma Unix.
- Para la red interna, esta implementado un DNS en Microsoft Windows 2000 y Unix.

El diagrama que se muestra en la figura (2.2) contiene el esquema oficial de DNS de PEMEX Exploración y Producción.

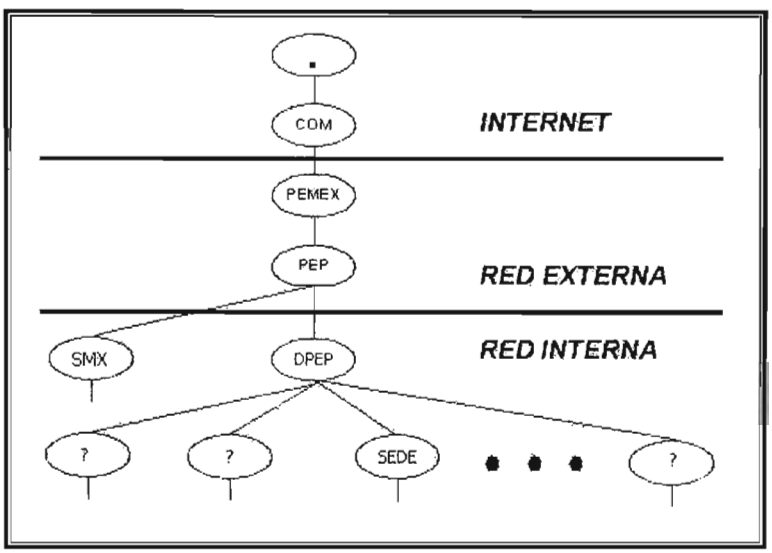

FIGURA 2.2 Esquema de DNS

2.2.2 Estructura del directorio activo

El Directorio Activo tiene una estructura lógica y física; en donde podemos identificar los componentes del Dominio Sede.

2.2.2.1 Estructura lógica

La figura (2.3) muestra la Región a nivel lógico.

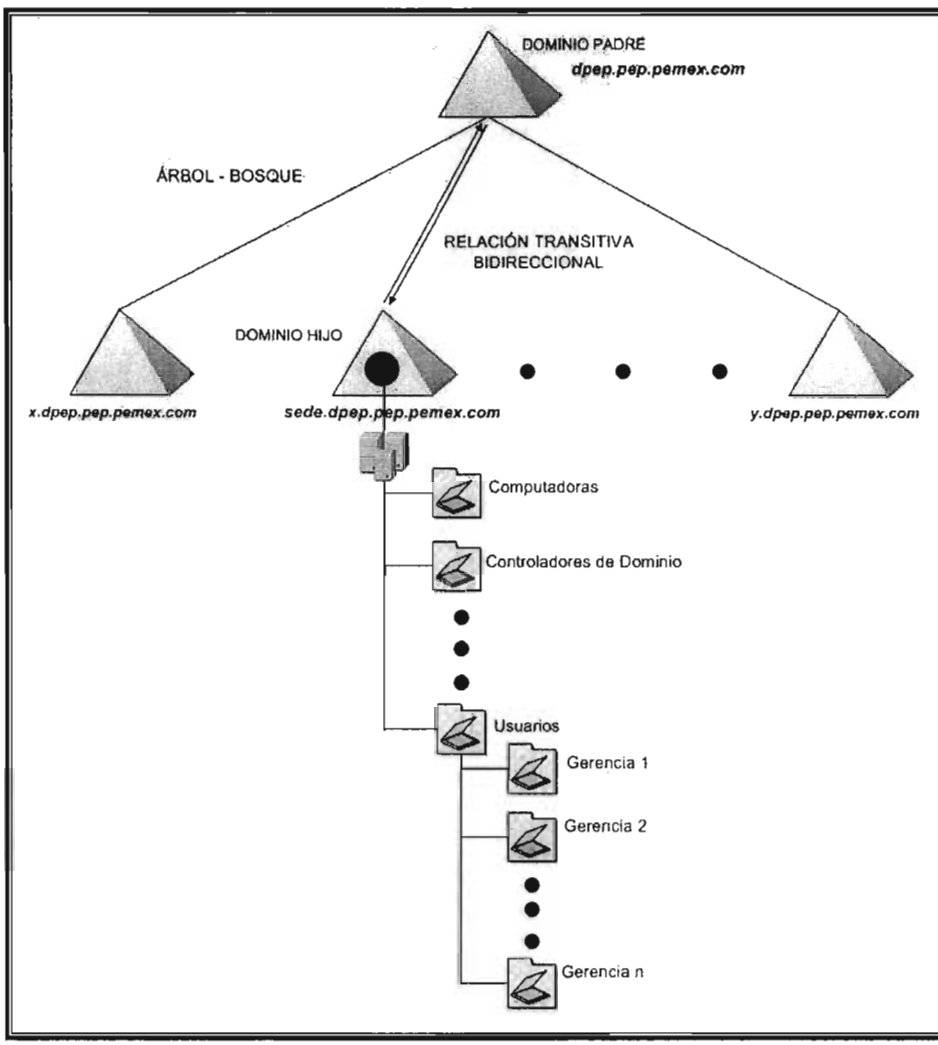

FIGURA 2.3 Estructura lógica de la región sede

La Región Sede tiene las siguientes características:

- La Región Sede es un dominio.
- El Dominio Sede es un dominio hijo del dominio padre DPEP.
- El Dominio Sede es una rama del árbol de DPEP, que forman un bosque.
- Tiene una relación de confianza Transitiva – Bidireccional con el Dominio Dpep, de Acceso Directo con otros dominios del mismo bosque y una externa con un dominio de diferente bosque.
- Las Unidades Organizacionales están compuestas de las carpetas: Computadoras, Controladores de Dominio, Usuarios, entre otros. En la carpeta de usuarios tiene un subnivel, en donde existen carpetas que representan cada Gerencia de la Región.
- Existe un catálogo global en dos controladores de dominio en pepsededc01 y pepsededc04.
- Utiliza el Protocolo de kerberos para la autenticación de los usuarios.

2.2.2.2 Estructura física

La figura (2.4) muestra la Región a nivel físico.

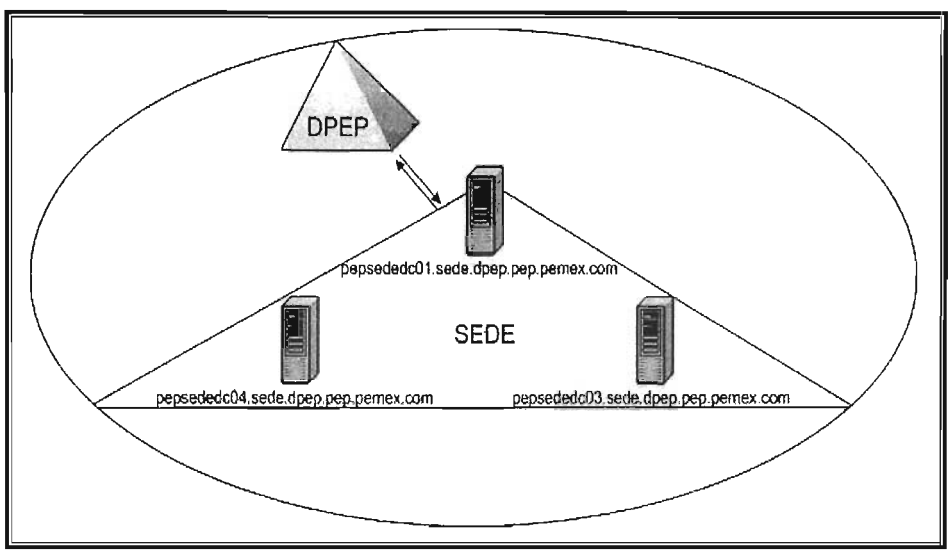

FIGURA 2.4 Sitio México

La Región Sede tiene las siguientes características:

- Tiene tres controladores de dominio: Pepsededc01, Pepsededc03 y Pepsededc04. (ver tabla 2.1)
- Existe un solo sitio en México
- Tiene dos dominios, en el Sitio México: El Dominio Sede y el Dominio Dpep (tiene dos controladores de dominio).
- Utiliza RPC como protocolo de Replicación
- Los roles de cada controlador de dominio son los siguientes:
  - Pepsededc01: Catálogo global, Maestro de emulador de PDC y Maestro RID.
  - Pepsededc03: Catálogo global y
  - Pepsededc04: Maestro de infraestructura.

2.2.3 Identificación de los activos

Como activos se identifican a los elementos de la organización, los cuales son: hardware, software o los menos tangibles como datos. En este punto se enuncian las características de los controladores de dominio del Dominio Sede (ver tabla 2.1).

Cabe señalar que los archivos de la base de datos del Directorio Activo se guardan en las carpetas *NTDS* y *SYSVOL* de la Unidad D. con un espacio de 2.70GB.

2.2.4. Administración del directorio activo

La Región Sede tiene una administración híbrida ya que aun cuando la base de operación es centralizada, diferentes Gerencias tienen bajo su control ciertas actividades de administración.

En la **administración centralizada,** el administrador del dominio controla todos los recursos de un solo punto y tiene las siguientes tareas en específico:

- Administra los controladores de dominio: Proporciona soporte y mantenimiento al equipo. Aplica las actualizaciones necesarias al directorio, al sistema operativo y al antivirus. Controla el acceso a este recurso.
- Verifica el estado del Directorio Activo: Replicación entre los controladores de dominio y entre ellos mismos, y la

disponibilidad de los recursos físicos, memoria y capacidades de almacenamiento.

- Verifica que todos los sitios y las subredes, sean creadas, actualizadas y que los costos e intervalos de sincronización sean fiables.
- Administra y verifica la base de datos de los servicios de DNS y WINS[13].
- Crea, borra o modifica las cuentas de Usuarios y Grupos en todo el Dominio Sede.
- Administra los servidores archivos, de aplicación y de impresión de la Gerencia de Infraestructura y Control Automatizado.

NOMBRE DEL CONTROLADOR	PEPSEDEDC01	PEPSEDEDC03	PEPSEDEDC04
HARDWARE			
MARCA	Hewlett-Packard	Dell	Hewlett-Packard
MODELO	Proliant ML570 G2	PowerEdge 6600	Proliant ML570 G2
IP	X.X.X.X	X.X.X.X	X.X.X.X
PROCESADORES	4 Intel a 2GHz.	4 Intel a 2.4Ghz	4 Intel a 2GHz.
MEMORIA	2 MB en RAM	1 MB en RAM	2 MB en RAM
ESPACIO USADO EN DISCO	C: 3.65 Gb D: 1.04 Gb E: 0.066 Gb	C: 3.32 Gb D: 0.96 Gb E: 2.46 Gb	C: 3.88 Gb D: 2.66 Gb
ESPACIO LIBRE EN DISCO	C: 10.6 Gb D: 18.5 Gb E: 67.7 Gb	C: 5.08 Gb D: 7.46 Gb E: 133 Gb	C: 11.1 Gb D: 16.2 Gb
SOFTWARE			
SISTEMA OPERATIVO	Windows 2000 Advanced Server	Windows 2000 Advanced Server	Windows 2000 Advanced Server
ANTIVIRUS	Symantec Norton Antivirus	Symantec Norton Antivirus	Symantec Norton Antivirus
ACTUALIZACIONES	Service Pack 4 Hotfix recomendados	Service Pack 4 Hotfix recomendados	Service Pack 4 Hotfix recomendados
OTROS	Quest Sw "Foglight" HP Managament Agents	Omniback Dell OpenManagament Applications	Quest Sw "Foglight"
TIPO DE MODO			
NATIVO O MIXTO	Nativo	Nativo	Nativo

TABLA 2.1 Características de los controladores de dominio

[13] WINS. *Windows Internet Name Service*

- Aplica políticas de grupo en los siguientes niveles:
  - **Dominio.** (ver tabla 2.2)

RUTA	DESCRIPCIÓN
Política 1. **Configuración de Computadora < Configuración de Windows < Seguridad < Política de Cuentas**	
Política de Contraseña <Política	Deshabilita que: La contraseña debe cumplir los requerimientos de complejidad y almacenar contraseñas usando encriptación irreversible.
Bloqueo de Cuentas < Política	Habilita el bloqueo de cuentas con cero intentos.
Políticas de Kerberos < Política	Forza al usuario al iniciar sesión con restricciones. Máximo tiempo de vida para el servicio de ticket de 600 minutos. Máximo tiempo de vida para otorgar ticket al usuario de 10 horas. Máximo tiempo de vida para renovar el ticket del usuario de 7 días. Máxima tolerancia para la sincronización del reloj de computadora de 5 minutos.
Configuración de Computadora < Configuración de Windows < Seguridad < Políticas Locales <	
Opciones de Seguridad <Política	Deshabilita el forzamiento de cierre de sesión cuando inicia sesión en horas expiradas.
Configuración de Computadora < Configuración de Windows < Seguridad < Políticas de llaves Públicas <	
Autoenrollment Settings	Proporciona certificados automáticamente. Deshabilite que renueva los certificados expirados, actualicé los que están pendientes y remueve los revocados. Deshabilite la actualización de los certificados que usan la platilla de certificados.
Encriptación de Archivos de Sistema < Propiedades	Habilita que permita a los usuarios encriptar sus archivos usando EFS" *Encrypting File System*".
Encriptación de Archivos de Sistema < Certificados	Habilita la recuperación de certificados solo para el administrador y expira 30/09/05.
Ruta de Confianza de Autoridades de Certificado.	Hablita la opción de permitir a los usuarios seleccionar una nueva ruta de CAs. "Autoridad de Certificados"para confiar.
Configuración de Usuario < Instalación de Servicios Remotos	
Cliente de Instalación de Opciones *Wizard*	Deshabilita herramientas, la configuración personalizada, y la configuración de reiniciar.
Política 2. **Configuración de Computadoras < Configuración de Windows< *Scripts* <**	
Startup	Los archivos Wins.vbs y Dns.vbs son para asignar WINS y DNS en forma automática a los equipos.

TABLA 2.2 Políticas a nivel dominio

- ***Unidad organizacional***. Son aplicadas dependiendo del nivel de requerimientos que necesiten los administradores de cada Gerencia para controlar el ambiente de usuarios. En la tabla (2.3) se mencionan políticas para configuración de Usuario.

RUTA	DESCRIPCIÓN
Configuración de Windows < Mantenimiento del Explorador de Internet <	
Conexiones < Configuración del Proxy	Configura el Proxy y los Protocolos HTTP, Seguro, FTP, Gopher y Socks con el respectivo puerto.
URLs < Importar URLs	Configura la dirección de Intranet al explorador de Windows como predeterminada.
Plantillas Administrativas <	
Escritorio < Política	Habilita la política de ocultar el icono de Mis sitios de red del escritorio.
Menú de Inicio y barra de Tareas < Política	Quita conexiones de red del menú de inicio y quita el ejecutar del menú inicio.
Conexiones de Red <Política	Prohíbe el acceso a las propiedades de una conexión LAN
Componentes de Windows < Explorador de Internet < Panel de Control < Política	Deshabilita la página de conexiones
Menú de Inicio y barra de Tareas < Política	Quita conexiones de red del menú de inicio y quita el menú ejecutar del menú de inicio.
Configuración de Windows <	
Script < Log on	Archivo llamado x.bat para cuando inicie sesión el usuario se mapeo sus conexiones al servidor respectivo y sus accesos a las impresoras correspondientes.
Carpeta de Redirección < Mis documentos	Especifica la carpeta de mis documentos en una partición del servidor que utilicen.

TABLA 2.3 Políticas a nivel unidad organizacional

- **Nivel Local** "equipo" es aplicada la Política 1 del dominio.

La **delegación de control administrativo**, se otorga a todos los Administradores de informática de cada Gerencia de la Región Sede; ellos tienen asignadas las siguientes tareas:

- Administrar servidores de impresión, de archivos y de aplicaciones que utilicen para su desempeño.
- Dar mantenimiento a sus equipos a nivel hardware y software.
- Ingresar equipos que tengan a su cargo al Dominio Sede.
- Desbloquear y cambiar contraseña en las cuentas de usuarios.
- Crear, modificar y borrar los grupos.

2.2.5 Estándar de nombres

El estándar de nombres se realizó, cuando se diseñó el Directorio Activo de PEP. Es un formato para asignar nombre a un objeto dentro del Directorio Activo, para llevar un control adecuado de los objetos los cuales algunos representan recursos en la red.

La organización tiene nombres asignados para: Dominios, Sitios, Sitios Link, Unidades Organizacionales, Usuarios y Grupos, Cuentas de Correo, Servidores, Estaciones de Trabajo, Impresoras y Políticas de Grupo. Todos los demás objetos no mencionados quedan a consideración del Administrador.

Por ejemplo: El objeto de cuenta de correo se compone de la siguiente manera (ver tabla 2.4):

Objeto:	**Cuenta de correo (SMTP)**
Formato:	<Iniciales><Paterno><Iniciales Materno>@pep.pemex.com <Iniciales>: Iniciales de los nombres <Paterno>: Apellido paterno <Iniciales Materno>: Primeras letras del apellido materno
Requerimientos:	El presente formato es solo una sugerencia para formar el alias de correo. Si hubiera duplicados estos deberán resolverse a criterio del administrador.
Ejemplos válidos:	Juan Manuel Pérez Jiménez: jmperezji@pep.pemex.com José Miguel Pérez Juárez: jmperezju@pep.pemex.com

TABLA 2.4 Estándar de cuenta de correo

2.3 Definición del proyecto

2.3.1 Enunciado del proyecto

PEP desea integrar todos los elementos de la Gerencia de Recursos Financieros en una Unidad Organizacional dentro del Directorio del Dominio Sede.

2.3.2 Objetivos del proyecto

- Definir una estrategia de migración para GRF.
- Mantener la disponibilidad de los recursos y servicios de los usuarios de la Gerencia en el proceso de integración.
- Desaparecer el Dominio grf.pep.pemex.com.
- Integrar la Gerencia de Recursos Financieros al Dominio Sede.

2.3.3 Resultados deseados

- Los recursos y servicios de GRF estén completamente disponibles.

2.4 Entorno de la gerencia de recursos financieros

En la Región Sede contiene muchas Gerencias como: Planeación, Recursos Humanos, de Administración de Bienes y Servicios, Recursos Financieros, entre otras; para su desempeño en actividades de la empresa.

Ahora debemos conocer todo el ambiente en que se desenvuelve actualmente la Gerencia de Recursos Financieros "GRF" sin estar integrada al Directorio Activo, ¿Cómo entran a Internet?, ¿Cómo funciona su Directorio Activo local?, ¿Cuáles son las actividades de su Administrador?, ¿Cómo están sus equipos?, etc.

2.4.1 Esquema DNS

Esta Gerencia tiene un Directorio Activo propio con un DNS configurado con las siguientes características:

- Tiene una dirección IP fija.

- En la configuración de la tarjeta de ted tiene: El DNS primario relacionado a su dirección IP de su Directorio Activo, como DNS secundario tiene la dirección IP del servidor Pepsededc01.
- Las direcciones de los servidores DNS están relacionados al dominio SMX, y todos los controladores de dominio de Sede. Sus sufijos correspondientes son: smx.pep.pemex.com, grf.pep.pemex.com y sede.dpep.pep.pemex.com[14]
- En la configuración de *forward lookup zones*, la zona de grf no es dinámica (Zona Integrada del Directorio Activo), y además tiene otras zonas creadas a varios dominios por ejemplo: al Dominio Sede.dpep.pep.pemex.com

2.4.2 Estructura del directorio activo

La estructura de su directorio Activo se visualiza en la figura (2.5).

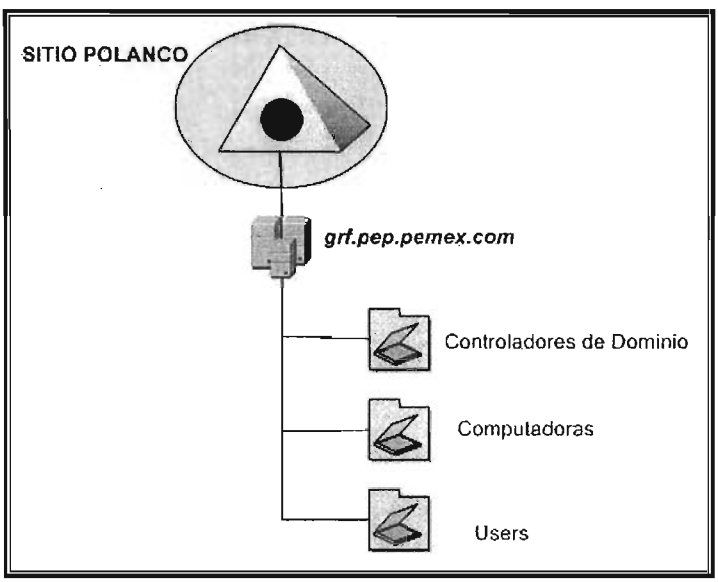

FIGURA 2.5 Dominio grf

[14] Esto se visualiza en *Advanced* TCP/IP *Settings* "DNS" de propiedades de la tarjeta de Red.

El Dominio GRF tiene las siguientes características:

- El dominio es único y se llama grf.pep.pemex.com, se hace notar que el sufijo de pep.pemex.com sólo lo colocaron por el nombre, pero este dominio es aislado y no tiene ninguna relación con PEP, no es delegado.
- No tiene unidades Organizacionales creadas, solamente las que la configuración inicial otorga. En este punto sus usuarios están creados en la carpeta llamada *users* y no en una llamada usuarios.[15]
- No tienen ninguna relación de confianza con algún otro dominio.
- Tiene un controlador de dominio "pepmxgrfw2k301" que posee los siguientes roles: Maestro Esquema, Maestro de Nombres de Dominio, Maestro Emulador PDC, Maestro de Identificadores Relativo y Maestro de Infraestructura; y tiene la característica de ser Catálogo Global.
- Tiene configurado un Sitio llamado Polanco.
- Maneja protocolo de replicación IP.

2.4.3 Identificación de los activos

Los activos de esta Gerencia se deben de tomar todos en cuenta, para cuando se integren al Dominio Sede, desde una impresora hasta los servidores que contienen su información.

2.4.3.1 Controladores de dominio

Cuenta con un controlador de dominio, con las siguientes características ver tabla (2.5).

2.4.3.2 Estaciones de trabajo

En forma general, las estaciones de trabajo cuentan con las siguientes características:

- Sistema Operativo Microsoft Windows XP o Microsoft Windows 2000.
- Las últimas actualizaciones recomendadas por Microsoft.

[15] Para una mejor administración es importante crear la carpeta de usuarios para manipularlos en el entorno.

- Antivirus administrado y actualizado por el servidor de antivirus.
- Sistema de Archivos *NTFS*.

NOMBRE DEL CONTROLADOR	Pepmxgrfw2k301
HADWARE	
MARCA	Hewlett-Packard
MODELO	PROLIANT DL740 G1
IP	X.X.X.X
PROCESADORES	8 Intel a 2 GHZ
MEMORIA	6 GB en RAM
ESPACIO USADO ES DISCO	C: 33.9GB E: 406 GB
ESPACIO LIBRE EN DISCO	C:20 GB E: 225 GB
SOFTWARE	
SISTEMA OPERATIVO	Windows 2003 Enterprise Edition
ANTIVIRUS	Symantec Norton Antivirus
ACTUALIZACIONES	Hot-fix recomendadas
TIPO DE MODO	
NATIVO O MIXTO	Nativo

TABLA 2.5 Controlador de dominio de grf

2.4.3.3 Impresoras

Es importante destacar que el servidor de impresión es el mismo controlador de dominio. Todas las impresoras están conectadas en red y este servicio debe estar disponible en el momento de la integración.

2.4.3.4 Datos

Los datos son primordiales para la Gerencia y conviene destacar que están ubicados en la unidad E del controlador de dominio llamado Pepmxgrfw2k301.

2.4.3.5 Servicios

El controlador de dominio presenta los siguientes servicios:

- ***Servicio DNS***, fue descrito en la configuración de DNS. (ver 2.4.1 Esquema DNS)

- ***Servicio WINS***

  Utilizado para la ubicación y localización de recursos del dominio grf.pep.pemex.com sin tener un alcance mayor a éste; ya que no tiene un *partner replication*[16].

- ***Servicio DHCP***

  Utilizado para la configuración de los parámetros de la tarjeta de red del protocolo IP, otorgando una dirección IP válida, máscara de subred, puerta de enlace, los DNS, WINS, entre otros.

2.4.4 Administración del directorio activo

La administración que se maneja en el Directorio Activo no es muy explotada, porque no tienen el personal capacitado para llevarla a cabo.

2.4.4.1 Tareas asignadas por el administrador

La administración es centralizada y realiza las siguientes tareas en específico:

- Administrar el controlador de dominio: Proporcionar soporte y mantenimiento al equipo. Aplicar las actualizaciones necesarias al directorio, al sistema operativo y al antivirus. Controlar el acceso a este recurso.
- Administrar y verificar la base de datos de los servicios de WINS, DHCP y DNS.
- Crear, borrar o modificar las cuentas de usuarios y grupos.
- Administrar servidores de impresión, de archivos y de aplicaciones que utilicen para su desempeño.
- Dar mantenimiento a sus equipos a nivel hardware y software.

[16] *Partner Replication*: Es otro servidor con el cual se replica la base de datos de WINS.

2.4.4.2 Políticas de grupo

El dominio de GRF no tiene implementadas políticas de grupo, solamente utilizan *scripts* por usuario para asignar todas las unidades de red e impresoras.

2.4.4.3 Usuarios

La Gerencia cuenta con 180 usuarios aproximadamente que no tienen una estructura de nombres uniforme, porque su *user logon name* son diferentes. Cabe destacar que estos objetos son creados en el contenedor de *Users*, lo cual no es recomendable porque no pueden aplicar políticas de grupo.

2.4.4.4 Grupos

Solamente tiene grupos globales, que son creados en la carpeta de *Users* con la siguiente estructura: GRUPO_Departamento. A estos grupos les asignan permisos a recursos o a información, lo cual no es recomendable porque a los que se asignan permisos son a los Grupos Locales.

2.5 Beneficios y riesgos

Después de presentar los elementos básicos de ambos Directorios se presentan las ventajas y desventajas encontradas:

Ventajas de ingresar al dominio

- La administración es delegada.
- Proporciona niveles de seguridad altos.
- Da el acceso a todos los servicios y recursos del dominio.
- Disminuye la carga de trabajo administrativo, por ejemplo: los administradores sólo necesitarán visitar el equipo un mínimo número de veces, y proporcionando una configuración de nuevos permisos para los recursos.
- Se implementa tecnología de innovación que llegue a la región.
- La resolución de nombres es adecuada.
- En cuanto a su diseño es escalable, es decir puede soportar la cantidad de objetos de GRF.

Desventajas de no estar en el dominio

- No pueden tener nuevos servicios de innovación tecnológica por ejemplo: Red inalámbrica.
- Se eleva el costo para el organismo.
- Para el nivel de Información que se maneja, no se tiene la seguridad adecuada.
- Crear una relación de confianza entre ambos dominios, sería demasiada complejo administrarla y mantenerla.
- La resolución de nombres que se mantiene actualmente es deficiente.
- La administración de su directorio activo no es al máximo.

Con base en las ventajas y desventajas se presentan los beneficios y los riesgos de la nueva reestructuración (ver tabla 2.6).

Cabe destacar que con la realización del presente proyecto, la GRF obtendrá entre otros de manera sobresaliente el acceso a los servicios y recursos de toda la red y verá notablemente disminuidas las interrupciones en el entorno de producción.

USUARIOS	
El usuario no notará el cambio en el entorno al momento de la integración.	Falta de entrenamiento oportuno personal de la Región Sede y no contar con la información completa y confiable.
El usuario tendrá buena disponibilidad de su equipo, accesos a la red y podrá seguir trabajando sin ningún problema.	Que algún acceso sea modificado con la nueva reestructuración sin haber notificado al usuario.
Los usuarios serán migrados con sus accesos y permisos correspondientes a los recursos.	Existan problemas al migrar el usuario que no se pueda autenticar al nuevo dominio.
EQUIPOS	
Los equipos se autenticarán a los controladores de dominio de la Región sede.	La autenticación se detenga cuando el servicio DNS tenga problemas.
Se entregarán en buen estado los equipos.	Falta de tiempo por el personal para cumplir las tareas determinadas. Exista problemas en el momento de la migración
El entorno del equipo para el usuario se mantendrá durante y después de la integración	Existan problemas en la migración del equipo.
El servidor de archivos se migrará con toda su información completa.	Que los usuarios se están conectando al servidor y se pierda la información de ellos en ese momento o que puedan perderse algunos permisos de usuarios o grupos cuando se migraron incorrectamente.
Se dejará su equipo como servidor de DHCP, de archivos y de impresión.	Que exista problemas con el DHCP en el momento de la migración de equipos que se tenga que consolidar el servicio al Dominio Sede.
ADMINISTRADORES	
La Gerencia de Recursos Financieros se consolidará como Unidad Organizacional al Dominio Sede	Poca participación de GRF.
Se le proporcionará una consola de administración para que pueda controlar a sus usuarios y grupos.	Solamente puede hacer cierto tipo de tareas y necesita autorización del administrador de sede para otros.
Serán administrados por políticas de grupo a su nivel OU para crear un ambiente a nivel usuario.	Mala planeación políticas puedan crear un descontrol que el administrador de GRF tenga depender del administrador de SEDE.
SERVICIOS	
Accederán a los Servicios y Recursos de toda la red.	Los servicios estén parados pero por problemas del proveedor de comunicaciones. La disponibilidad del servicio del Directorio Activo no sea del 100%.
Disminuirá la interrupción de actividad en el entorno de producción.	Que la mala planeación pueda detener el servicio.

TABLA 2.6 Beneficios y Riesgos

2.6 Requerimientos del proyecto

La Gerencia de Recursos Financieros de acuerdo a sus necesidades definió los siguientes requerimientos que son los siguientes:

- ***Administración:***
  Solicitan un control operativo sobre la OU de GRF en Sede.

- ***Controlador de dominio:***
  El DC del dominio grf.pep.pemex.com debe desaparecer después de la integración de sus recursos.

- ***Usuarios:***
  Los usuarios de GRF deben estar creados y actualizados en el Dominio Sede con la disponibilidad de sus servicios sin problemas.

- ***Grupos:***
  Los grupos deben conservar la estructura de sus miembros y los permisos correspondientes a sus datos.

- ***Estaciones de trabajo:***
  Los equipos deben tener las actualizaciones necesarias a los parámetros de sede y los usuarios deben poder iniciar sesión sin problemas en el Dominio Sede.

- ***Servicios de impresión:***
  Los servicios de impresión deben mantenerse durante y después de la integración. Las impresoras instaladas deben permanecer en el servidor Pepmxgrfw2k301.

- ***Servidor de archivos:***
  Mantener el hardware y la información sin pérdida de datos del servidor Pepmxgrfw2k301.

- ***Servicios DNS, WINS Y DHCP:***
  Los servicios de DNS y WINS, verificar que trabajen correctamente y en su defecto realizar las modificaciones necesarias a ellos; después de la integración éstos desaparecerán. El servicio DHCP debe de funcionar correctamente después de la integración con sus modificaciones correspondientes al nuevo dominio.

Nota: El controlador de Dominio de GRF cuenta con servicios de Impresión, Archivos, DNS, WINS y DHCP.

CAPÍTULO 3
PILOTO

El piloto fue creado como laboratorio de pruebas, para identificar las partes del diseño en la integración y donde se realizaron las pruebas necesarias con un modelo de producción; el cual nos ayudó a determinar los problemas a los que se puede enfrentar la implementación.

3.1 Laboratorio

Este laboratorio fue creado con base en los requerimientos del análisis para encontrar la óptima solución en el momento de la integración.

3.1.1 Objetivo

Identificar, analizar y resolver los contratiempos que se pueden presentar en la integración.

3.1.2 Entorno de laboratorio

Debido a los requerimientos del análisis, fue necesario mover el controlador de dominio a otro servidor para que no fuese afectada la disponibilidad de los recursos y servicios al realizar la migración del Servidor de Archivos; para lo cual se creó un ambiente con las siguientes características (ver figura 3.1):

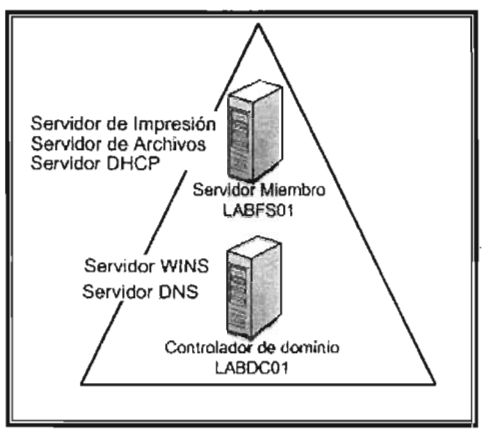

FIGURA 3.1 Laboratorio de gica

- Se creó un dominio llamado gica.pep.pemex.com.
- Se configuró un controlador de dominio llamado labdc01.gica.pep.pemex.com además es servidor DNS y WINS, con el siguiente equipo:

  Procesador Intel Pentium III a 860 MHz
  256 MB en RAM
  Disco Duro: 19 GB
  Sistema Operativo Microsoft Windows Server 2003

Enterprise Edition

- Se configuró un servidor de archivos llamado labfs01.gica.pep.pemex.com, que además es servidor de impresión y DHCP.
- Se configuró la tarjeta de red de ambos servidores de la siguiente:
  - DNS primario: Dirección IP del servidor labdc01
  - DNS secundario: Dirección IP del servidor pepsededc01
- Se crearon zonas de la siguiente forma:
  - En el labdc01 se creó una zona primaria tipo: Zona Integrada de Directorio Activo del dominio gica y una zona secundaria del dominio sede.
  - En el pepsededc01 se creó una zona secundaria del dominio gica.

3.1.3 Pruebas

Estas pruebas fueron determinantes para realizar los procedimientos de migración, adecuándolos a las necesidades en específico y resolviendo los problemas presentados.

3.1.3.1 Resolución de nombres entre dominios

La parte primordial para realizar la migración utilizando la herramienta es que exista una resolución de nombres entre los dominios del Directorio Activo.

- **Configurar *forwarders***

  En el controlador de dominio primario de GRF, en la parte de *forwarders*[17] agregamos el DC primario del dominio DPEP y en el DC primario de sede se agrego el DC de GRF (ver figura 3.2). Esto si permitió la resolución de nombres, pero el problema en caso del dominio GRF es que existían muchos registros no actualizados; por consecuencia no había una resolución de nombres correcta.

[17] *Forwarders:* Servidor que es contactado para responder a solicitudes de resolución de nombres de dominio, cuando el servidor autoritativo de la zona no puede resolver las peticiones recibidas por los clientes.

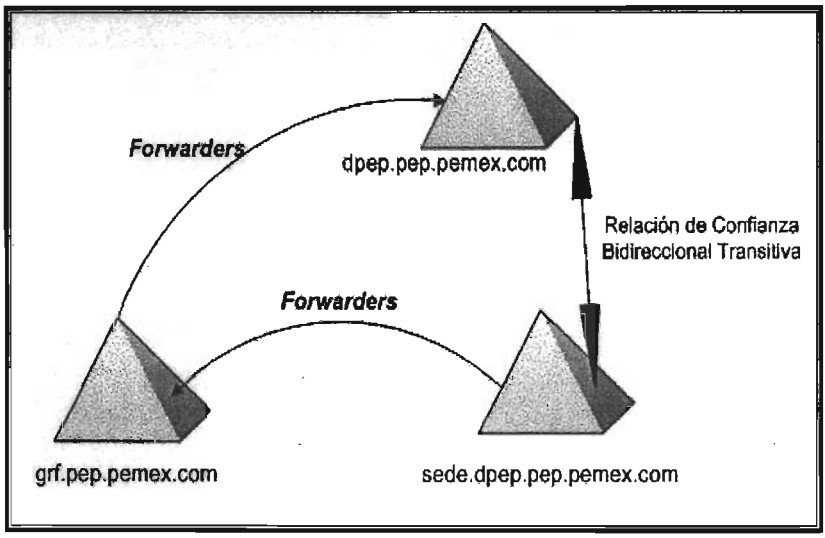

FIGURA 3.2 Forwarders

- **Configurar zonas en *forward lookup zone***
  Se creó una zona secundaria del dominio origen en el DC primario del dominio destino y viceversa. Esto permitió la comunicación correcta y evitó los problemas de resolución de nombres de ambos dominios.

Al resolver el problema de comunicación, se creó una relación de confianza externa bidireccional en ambos dominios. Esta relación permitió el acceso de recursos entre los dos dominios.

3.1.3.2 Migración de usuarios

En la migración de usuarios se prepararon las unidades organizacionales de ambos dominios, donde se crearon usuarios que se identificaron de la siguiente forma (ver tabla 3.1):

- Usuarios con igual *user logon name*
- Usuarios con diferente *user logon name*
- Usuarios creados en gica pero no existentes en sede:

Nombre del Usuario	*User Logon Name* GICA *OU* PRUEBA-GICA	*User Logon Name* SEDE *OU* PRUEBA-GICA
Cesar Balderas León	cbalderasl	cbalderasl
Leticia Lopez Hernandez	llopezh	llopezh
Luis Colorado Quiroz	lcolorado	lcoloradoq
Claudia Cortés Aguilar	ccortes	ccortesa
Mayra Morales García	mmoralesg	mmorales
Adalberto Chacon Longoria	achaconl	
Erandi Contreras Jurado	econtrerasj	
Administrator	administrator	admingrf

TABLA 3.1 Relación de usuarios

Con base en las pruebas realizadas es necesario lo siguiente:

- Crear un usuario en el Dominio Sede que sustituya al administrador del dominio gica.
- Crear los usuarios del dominio origen que no existen en el dominio destino en la OU PRUEBA-GICA del dominio destino.
- Mover aquellos usuarios que existen en el dominio destino pero que no se encuentran en la OU correspondiente.

3.1.3.3 Migración de grupos globales

En la migración de grupos globales, cabe mencionar que en el dominio GRF tiene un grupo Domain Users (contiene todos los usuarios del dominio) y el grupo administradores; los cuales tienen asignados permisos en el servidor de Archivos. De este punto se tienen dos soluciones para el dominio GICA:

1. Crear en el dominio origen dos nuevos grupos locales: Todos los usuarios y administradores, el cual debe de sustituir los mencionados anteriormente. Estos grupos deben de ser ingresados en el servidor de archivos con los permisos correspondientes y ser migrados posteriormente.
2. Crear en el dominio destino dos nuevos grupos locales: GICA_Todos los usuarios y GICA_administradores a los cuales debemos ingresar en el servidor de archivos con los permisos correspondientes.

Se eligió la segunda opción de estos dos grupos; los demás fueron migrados satisfactoriamente con sus miembros en la OU PRUEBA-GICA (ver tabla 3.2) del dominio sede agregando un prefijo.

Nombre del Grupo GICA *OU* PRUEBA-GICA	**Nombre del Grupo SEDE *OU* PRUEBA-GICA**	**Miembros del Grupo SEDE *OU* PRUEBA-GICA**
ADMINISTRATIVO	GICA_ADMINISTRATIVO	cbalderasl llopezh
CONTABILIDAD	GICA_CONTABILIDAD	llopezh econtrerasj
PERSONAL	GICA_PERSONAL	cbalderasl mmorales admingrf ccortesa achaconl
PRUEBA	GICA_PRUEBA	admingrf cccortesa
No existía el grupo	GICA_Todos los usuarios	Todos los usuarios del dominio gica
No existía el grupo	GICA_administradores	cbalderasl achaconl admingrf

TABLA 3.2 Relación de grupos

3.1.3.4 Migración del servidor de archivos

En la migración del servidor de archivos, el servidor se ingresó satisfactoriamente en el Dominio Sede, los permisos a los usuarios y grupos fueron respetados, las impresoras siguieron funcionando correctamente excepto el DHCP.

El servicio de DHCP dejó de funcionar, no asignando direcciones IP a los usuarios, por lo que se determinó que se deben de realizar actividades adicionales:

- Respaldar la base de datos del servidor DHCP
- Configurar un nuevo DHCP en el nuevo dominio de sede
- Restaurar la base de datos del servidor DHCP

3.1.3.5 Migración de computadoras

En la migración de las computadoras se escogieron 3 equipos de Windows XP con las siguientes características:

1. Equipo con un solo perfil de usuario que tenga acceso a Internet, accesos remotos, bases de datos, servicios de impresión y sus datos correspondientes.
2. Equipo con más de dos perfiles de usuario en el dominio gica.
3. Equipo con el Service Pack 2

Con base en las pruebas se determinó lo siguiente:

- En el equipo #1 no hubo ningún problema, pero se tiene que considerar, que en algunos casos si tienen configuración de agenda electrónica se debe seleccionar la opción "user rights" y "outlook profile" de la herramienta.
- En el equipo #2, sólo actualiza el último perfil, por lo que se tiene que hacer las demás copias de los perfiles de usuario en forma manual.
- En el equipo #3 se debe configurar los parámetros del Firewall personal que incluye el Service Pack 2, para poder contactar el equipo sin ningún problema y posteriormente migrarlo.

CAPÍTULO 4
DISEÑO

El diseño tiene como objetivo, la eficiencia total del proyecto con base en la planeación con un programa de trabajo identificando las tareas y actividades en forma secuencial, paralela o independiente de los elementos a integrar de GRF al dominio Sede.

4.1 Definición de diseño

Se realizaron las lecturas correspondientes sobre la integración de dominios y se efectuaron las pruebas necesarias, para lo cual es necesario primero identificar a qué se denomina diseño. El diseño es un conjunto de pasos que permiten describir e interpretar con suficientes detalles todos los aspectos de un proceso.

A partir de la definición de diseño para este proyecto, es posible pasar al siguiente aspecto que es el definir las etapas del diseño (figura 4.1):

FIGURA 4.1 Etapas del diseño

Etapa1: PRE-MIGRACIÓN

En la primera etapa se realizó la instalación de un nuevo controlador de dominio adicional al dominio grf.pep.pemex.com que sustituye el servidor Pepmxgrfw2k301 para establecerlo solamente como Servidor miembro de ese dominio. Además se crea una relación de confianza o de ambos dominios para que compartan sus recursos. Todas estás tareas no afectan en nada la disponibilidad en el accesos a sus recursos.

Etapa2: MIGRACIÓN

En la segunda etapa se modificaron los recursos porque se integraron al dominio sede, lo cual ya no es reversible. Toda modificación puede causar riesgos, pero cabe destacar que durante este proceso los usuarios accedieron factiblemente a sus recursos y se trató de realizar de una manera transparente.

Etapa3: POST-MIGRACIÓN

En la última etapa solamente se eliminó la relación de confianza, se verificó los servicios y accesos de los usuarios; y se entregó formalmente la documentación a la gerencia lo cual concluyó el proyecto.

4.2 Plan de trabajo[18]

En la tabla (4.1) se enuncian las tareas generales en cada etapa para llevar a cabo la implementación.

ENUNCIADO DEL PROYECTO: PEP desea integrar todos los elementos de la Gerencia de Recursos Financieros en una Unidad Organizacional dentro del Directorio del dominio Sede		
Tareas del Proyecto	**Duración**	**Relaciones de Dependencia**
PRE - MIGRACIÓN		
1. Integración de un nuevo DC.	1 día	-
2. Configuración y Verificación de los Servicios de DNS.	1 día	Después de Integrar el nuevo Controlador de Dominio.
3. Configuración y verificación de los Servicios WINS.	1 día	Después de verificar los servicios DNS.
4. Transferencia de los Roles al nuevo DC.	1 día	Después de verificar los servicios WINS.
5. Habilitación del Catálogo Global.	1 día	Después de la transferencia de Roles.
6. Despromoción del DC Original.	1 día	Después de Habilitar el Catálogo Global.
7. Creación de la Relación de Confianza.	1 día	Después de la Despromoción del DC.
MIGRACIÓN		
8. Migración de Usuarios con la Herramienta *FastLane Migrator.*	1 días	Después de Crear la relación de confianza.
9. Migración de Grupos Globales con la Herramienta *FastLane Migrator.*	1 día	Después de Migrar Usuarios.
10. Migración del Servidor de Archivos.	1 día	Después de la migración de grupos globales.
11. Migración de Estaciones de Trabajo con la Herramienta *FastLane Migrator.*	10 días	Después de la migración del servidor de Archivos.
POST-MIGRACIÓN		
12. Eliminación de la relación de confianza.	1 día	Después de la Migración de las Estaciones de Trabajo.
13. Despromoción del DC grf.pep.pemex.com	1 día	Después de la eliminación de la relación de confianza.
14. Entrega de la Administración.	1 día	Después de la Despromoción del DC

TABLA 4.1 Plan de trabajo

[18] NOTA: Todas estas tareas requieren de las cuentas de los Administradores de ambos dominios.

4.3 Definición de actividades

En esta sección se describen las actividades, asignando las personas encargadas de realizarlas, cubriendo los requerimientos dados.

4.3.1 Integración de un nuevo dc

Se debe instalar un controlador de dominio adicional al dominio grf.pep.pemex.com. (ver tabla 4.2)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Tener un equipo disponible.	Informático GRF	*[19]	2
2. Realizar la Configuración del Sistema Operativo.	Informático de GRF	1	2
3. Asignar nombre al equipo.	Informático de GRF	2	3 y 4
4. Fijar una Dirección IP.	Informático de GRF	3	5
5. Ejecutar el comando dcpromo.	Informático de Sede	3	*

TABLA 4.2 Integración de un nuevo dc

4.3.2 Configuración y verificación de los servicios de DNS

Se deben instalar los servicios DNS para la resolución de nombres de entre ambos dominios. (ver tabla 4.3)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Habilitar los servicios DNS en el nuevo DC.	Informático de Sede	*	2
2. Realizar la Configuración de los Servicios DNS.	Informático de Sede	1	3
3. Crear la zona de grf y sede en el nuevo DC.	Informático de Sede	2	4
4. Crear la zona de grf en el DNS de sede.	Informático de Sede	3	5
5. Verificar los servicios DNS.	Informático de Sede	4	*

TABLA 4.3 Configuración y verificación de los servicios DNS

[19] * Significa que estas actividades pueden tener una relación con alguna tarea, pero se visualizará mejor en el diagrama de tiempos.

4.3.3 Configuración y verificación de los servicios WINS

Se deben instalar los servicios WINS para resolución de nombres cortos entre ambos dominios. (ver tabla 4.4)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Habilitar los servicios WINS en el nuevo DC.	Informático de Sede	*	2
2. Realizar la configuración de los servicios WINS.	Informático de Sede	1	3
3. Agregar a los servicios WINS los servicios WINS del dominio dpep.	Informático de Sede	2	3
4. Verificar los servicios WINS.	Informático de Sede	3	4

TABLA 4.4 Configuración y verificación de los servicios WINS

4.3.4 Transferencia de los roles al nuevo dc

Se deben transferir los roles para poder despromover el DC original. (ver tabla 4.5)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Transferir los Roles: Maestro Emulador PDC, Maestro RID y Maestro Infraestructura.	Informático de Sede	*	2
2. Transferir los Roles: Maestro de Nombre de Dominio y Maestro Esquema.	Informático de Sede	1	*

TABLA 4.5 Transferencia de los roles al nuevo dc

4.3.5 Habilitación del catálogo global

Se debe habilitar en el nuevo DC para que puedan encontrar todos los objetos publicados en el directorio. (ver tabla 4.6)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Habilitar el nuevo DC como Catálogo Global.	Informático de Sede	*	*

TABLA 4.6 Habilitación del catálogo global

4.3.6 Despromoción del dc original

Se debe despromover el DC para que el servidor Pepmxgrfw2k301 quede como un Servidor Miembro. (ver tabla 4.7)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Ejecutar el comando dcpromo	Informático de Sede	*	2
2. Deshabilitar los servicios DNS y WINS	Informático de Sede	1	3
3. Modificar la configuración del DHCP para que el DNS primario sea el nuevo DC.	Informático de GRF	2	4
4. Verificar y actualizar los servicios DNS del nuevo DC.	Informático de Sede	3	*

TABLA 4.7 Despromoción del dc original

4.3.7 Creación de la relación de confianza

Se debe crear esta relación para que ambos dominios puedan acceder a los recursos mutuos. (ver tabla 4.8)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Verificar los servicios WINS y DNS en ambos dominios.	Informático de Sede y GRF	*	2
2. Ejecutar el comando netdom.	Informático de Sede y GRF	1	3
3. Verificar la validez de la relación de confianza.	Informático de Sede y GRF	2	*

TABLA 4.8 Creación de la relación de confianza

4.3.8 Migración de usuarios con la herramienta *fast lane migrator*

Algunos usuarios en el dominio de grf.pep.pemex.com están creados en el dominio de sede porque tienen su cuenta de correo en este dominio. Se deben de migrar los usuarios con todos sus privilegios de

ese dominio a sede para que puedan acceder a sus recursos posteriormente. (ver tabla 4.9)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Hacer una lista de usuarios actualizados en el dominio grf.	Informático de GRF	*	2
2. Relacionar la lista con los usuarios existentes en el Dominio Sede.	Informático de Sede	1	3
4. Crear nuevos usuarios de grf que no existan en el Dominio Sede.	Informático de Sede	2	4
3. Realizar el proceso de pre-requisitos que marca la herramienta.	Informático de Sede	3	5
5. Ejecutar la herramienta en un servidor del dominio sede.	Informático de Sede	4	6
6. Verificar el acceso a los recursos de los usuarios migrados.	Informático de GRF	5	*

TABLA 4.9 Migración de usuarios

4.3.9 Migración de grupos globales con la herramienta *fast lane migrator*

Se deben migrar los grupos con sus privilegios correspondientes del dominio original para que se mantengan intactos en el dominio sede. (ver tabla 4.10)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Hacer una lista actualizada de los Grupos de GRF con las siguientes características: • Nombre del grupo o departamento al que pertenecen. • Usuarios o grupos que integran cada grupo	Informático de GRF	*	2
2. Ejecutar la herramienta en un servidor del dominio sede.	Informático de Sede	1	3
3. Verificar que los grupos fueron migrados satisfactoriamente.	Informático de Sede	2	*

TABLA 4.10 Migración de grupos globales

4.3.10 Migración del servidor de archivos al dominio sede

Se debe migrar el servidor Pepmxgrfw2k301 para que pertenezca como servidor miembro del dominio sede. (ver tabla 4.11)

Actividades	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Configurar la tarjeta de red con los parámetros apropiados de Sede.	Informático de Sede	*	2
2. Sacar al equipo del Dominio Sede.	Informático de Sede	1	3
3. Ingresar el equipo a un grupo de trabajo.	Informático de Sede	2	3
4. Ingresarla al Dominio Sede.	Informático de Sede	3	4
5. Verificar y/o configurar los servicios DHCP	Informático de Sede	4	*

TABLA 4.11 Migración del servidor de archivos

4.3.11 Migración de estaciones de trabajo con la herramienta *fast lane migrator*

Se debe realizar la migración de los equipos para que dejen de pertenecer al dominio grf.pep.pemex.com. (ver tabla 4.12)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1.Hacer una lista actualizada de los equipos de GRF con las siguientes características: ▪ Nombre del equipo ▪ Dirección IP ▪ Dirección física (*MAC address*) ▪ Usuario al que pertenece el equipo.	Informático de GRF	*	3
2. Ingresar al administrador de sede en el grupo de administradores locales del equipo.	Informático de Sede	*	3
3. Revisar el equipo que cumpla con pre-requisitos de migración.	Informático de GRF	1	4
4. Realizar el proceso de migración del equipo con la herramienta *Fast-Lane Migrator.*	Informático de Sede	3	5
5. Verificar el acceso a los recursos de los usuarios de los equipos migrados.	Informático de GRF y Sede	4	*

TABLA 4.12 Migración de estaciones de trabajo

4.3.12 Eliminación de la relación de confianza

Se debe romper la relación de ambos dominios (sede y GRF) porque todos los recursos de la Gerencia están integrados en el dominio sede, con esto se termina la etapa de migración. (ver tabla 4.13)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Ejecutar el comando *netdom* para eliminar la relación.	Informático de GRF y Sede	*	2
2. Restablecer los parámetros modificados en el proceso de migración en el dominio sede.	Informático de Sede	1	*

TABLA 4.13 Eliminación de la relación de confianza

4.3.13 Despromoción del dominio grf.pep.pemex.com

Se debe desaparecer el dominio para finalizar la integración. (ver tabla 4.14)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Ejecutar el comando *dcpromo*.	Informático de GRF	*	2
2. Deshabilitar los servicios DNS y WINS.	Informático de GRF	1	*

TABLA 4.14 Despromoción del dominio grf

4.3.14 Entrega de administración

Se debe entregar formalmente la administración delegada de la OU de GRF a los responsables de la Gerencia de Recursos Financieros. (ver tabla 4.15)

Actividad	Personal Encargado	Actividad Anterior	Actividad Posterior
1. Configurar la consola de administración	Informático de SEDE	*	2
2. Notificar de normas seguidas en el dominio sede.	Informático de SEDE	1	*

TABLA 4.15 Entrega de administración

4.4 Diagrama de tiempos

En este apartado visualizaremos los diagramas de cada etapa del diseño mediante la técnica de diagramas de Gantt.

Esta técnica es usada en la planeación para mostrar gráficamente (mediante una seria de barras) el tiempo transcurrido y secuencia de cada elemento de la estructura de división del trabajo.

En los diagramas de tiempos que se presentan a continuación son:

El plan de trabajo (ver figura 4.2) y en las figuras (4.3, 4.4 y 4.5) las etapas de pre-migración, migración y post-migración del diseño.

PLAN DE TRABAJO
No.
Nombre de tarea
Tiempo de Ejecución
Duración
semana 1
semana 2
semana 3
semana 4
L M X J V S D L M X J V S D L M X J V S D L M X
INTEGRACIÓN DE UN DIRECTORIO ACTIVO 16.755 días 18 días
ETAPA 1: PRE-MIGRACIÓN 3 días 3 días
1 Integración de un nuevo DC 0.4 días
2 Configuración y verificación de los servicios DNS 0.33 días
3 Configuración y verificación de los servicios WINS 0.27 días
4 Transferencia de los Roles al nuevo DC 0.33 días
5 Habilitación del Catálogo Global 0.21 días
6 Despromoción del DC Original 0.46 días
7 Creación de la Relación de Confianza 1 día
ETAPA 2: MIGRACIÓN 12.375 días 13 días
8 Migración de Usuarios con la Herramienta FastLane Migrator 1 día
9 Migración de Grupos Globales con la Herramienta FastLane Migrator 0.625 día
10 Migración del Servidor de Archivos 0.75 día
11 Migración de Estaciones de Trabajo con la Herramienta FastLane Migrator 10 días
ETAPA 3: POST-MIGRACIÓN 1.38 días 2 días
12 Eliminación de la Relación de Confianza 0.25 días
13 Despromoción del dominio grf.pep.pemex.com 0.17 días
14 Entrega de Administración 0.38 días
ETAPA
TAREA

FIGURA 4.2

No.	Nombre de tarea	Tiempo de Ejecución	Duración
	ETAPA1:PREMIGRACIÓN	**3 días**	**3 días**
1	**Integración de un nuevo DC**	**0.4 días**	**1 día**
1.1	Tener un equipo disponible	30 mins	
1.2	Realizar la configuración del Sistema Operativo	90 mins	
1.3	Asigner nombre al equipo	10 mins	
1.4	Fijar una dirección IP	10 mins	
1.5	Ejecuter el comando dcpromo	50 mins	
2	**Configuración y verificación de los servicios de DNS**	**0.33 días**	**1 día**
2.1	Habilitar los servicios DNS en el nuevo DC	30 mins	
2.2	Realizar la configuración de los servicios	30 mins	
2.3	Crear la zona de grl y sede en el nuevo DC	40 mins	
2.4	Crear la zona de grl en el DNS de sede	30 mins	
2.5	Verificar los servicios DNS	30 mins	
3	**Configuración y verificación de los servicios WINS**	**0.27 días**	**1 día**
3.1	Habilitar los servicios WINS en el nuevo DC	30 mins	
3.2	Realizar la configuración de los servicios WINS	30 mins	
3.3	Agregar a los servicios WINS los servicios WINS del dominio dpep	40 mins	
3.4	Verificar los servicios WINS	30 mins	
4	**Transferencia de los Roles al nuevo DC**	**0.33 días**	**1 día**
4.1	Transferir los Roles: Maestro Emulador PDC, Maestro RID y Maestro Infraestructura	60 mins	
4.2	Transferir los Roles: Maestro de Nombre de Dominio y Maestro	100 mins	
5	**Habilitación del Catálogo Global**	**0.21 días**	**1 día**
5.1	Habilitar el nuevo DC como Catálogo Global	100 mins	
6	**Despromoción del DC Original**	**0.46 días**	**1 día**
6.1	Ejecuter el comando dcpromo	60 mins	
6.2	Modificar la configuración del DHCP para que el DNS primario sea el nuevo DC	70 mins	
6.3	Verificar y actualizar los servicios DNS del nuevo DC	90 mins	
7	**Creación de la Relación de Confianza**	**1 día**	**1 día**
7.1	Verificar los servicios WINS y DNS en ambos dominios	240 mins	
7.2	Ejecuter el comando netdom	120 mins	
7.3	Verificar la validez de la relación de Confianza	120 mins	

FIGURA 4.3

No.	Nombre de tarea	Tiempo de Ejecución	Duración
8	ETAPA2: MIGRACION	12.375días	13 días
8.1	**Migración de usuarios con la herramienta FastLane Migrator**	**1 día**	**1 día**
8.2	Hacer una lista de usuarios actualizados	60 mins	
8.3	Relacionar la lista con los usuarios existentes en el dominio Sede	60 mins	
8.4	Crear nuevos usuarios de grf que no existan en el dominio sede	60 mins	
8.5	Realizar el proceso de pre-requisitos que marca la herramienta	60 mins	
8.6	Ejecutar la herramienta en un servidor del dominio Sede	180 mins	
8.7	Verificar el acceso a los recursos de los usuarios migrados	60 mins	
9	**Migración de Grupos Gloables con FastLane Migrator**	**0.625 día**	**1 día**
9.1	Hacer una lista actualizada de Grupos	60 mins	
9.2	Ejecutar la herramienta en un servidor del dominio sede	180 mins	
9.3	Verificar que los grupos fueron migrados satisfactoriamente	60 mins	
10	**Migración del Servidor de Archivos al dominio Sede**	**0.75 día**	**1 día**
10.1	Configurar la tarjeta de red con los parámetros apropiados de Sede	30 mins	
10.2	Sacar al equipo del dominio Sede	30 mins	
10.3	Ingresar el equipo a un grupo de trabajo	30 mins	
10.4	Ingresarlo al dominio sede	30 mins	
10.5	Verificar y/o configurar los servicios DHCP	120 mins	
11	**Migración de Estaciones de Trabajo con la Herramienta FastLane Migrator**	**10 días**	**10 días**
11.1	Hacer una lista actualizada de los equipos	1 día	
11.2	Ingresar al administrador de sede en el grupo de administradores locales del equipo	1 día	
11.3	Revisar el equipo que cumpla con los pre-requisitos de migración	1 día	
11.4	Realizar el proceso de migración del equipo con la herramienta	6 días	
11.5	Verificar el acceso a los recursos de los usuarios de los equipos migrados	1 día	

FIGURA 4.4

No.	Nombre de tarea	Tiempo de Ejecución	Duración
	ETAPA 3: POST-MIGRACIÓN	**1.38 días**	**2 días**
12	**Eliminación de la relación de confianza**	**0.25 días**	**1 día**
12.1	Ejecutar el comando netdom	60 mins	
12.2	Restablecer los parámetros modificados en el proceso de migración	60 mins	
13	**Despromoción del Dominio grf.pep.pemex.com**	**0.17 días**	**1 día**
13.1	Ejecutar el comando dcpromo	50 mins	
13.2	Deshabilitar los servicios DNS y WINS	30 mins	
14	**Entrega de administración**	**0.38 días**	**1 día**
14.1	Configurar la consola de administración	120 mins	
14.2	Notificar las normas seguidas	60 mins	

FIGURA 4.5

CAPÍTULO 5
IMPLEMENTACIÓN

Convertir los conceptos del diseño en un proyecto funcional recibe el nombre de Implementación. Se incluye la operación y verificación para el acceso a la información y recursos; así como el mantenimiento posterior a la integración.

5.1 Etapa de pre-migración

En esta fase es representada la pre-migración de acuerdo con las primeras 7 tareas (ver tabla 4.1) las cuales definen las condiciones de un ambiente idealizado (ver figura 5.1) para la preparación del proceso de migración.

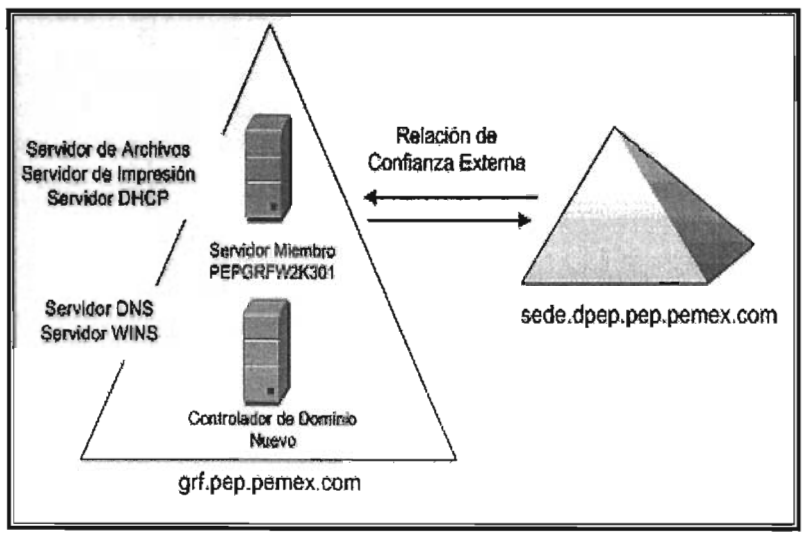

FIGURA 5.1 Fase de pre-migración

5.1.1 Configuración del nuevo dc

La configuración del nuevo controlador de dominio abarcó su integración como DC y la configuración y verificación de los servicios DNS y WINS.

Estas actividades se efectuaron en el nuevo servidor conforme a las tablas (4.2, 4.3 y 4.4) en la siguiente forma:

- El nuevo servidor tiene las siguientes características:
  a. Marca Dell
  b. Modelo *Power Edge* 8450
  c. 4 Procesadores *Intel Pentium Xeon* a 700 MHz
  d. I GB en RAM
  e. Dos discos Internos 8 GB
  f. Arreglo de discos de 169.5 GB

- Se instaló el sistema operativo en plataforma *Microsoft Windows Server 2003 Enterprise Edition.*
- Se asignó el nombre de pepgrfdc02.
- Se fijo una dirección IP: X.X.X.X
- Se instalaron las actualizaciones correspondientes[20] y el Norton Antivirus administrado por el servidor pepsededenav01.
- Se configuraron las direcciones DNS en los parámetros de la tarjeta de Red.
    a. DNS primario: IP del servidor pepmxgrfw2k301
    b. DNS secundario: IP del servidor pepgrfdc02
- Se ingresó al dominio grf.pep.pemex.com
- Se configuró al servidor pepgrfdc02 como controlador de dominio adicional al dominio grf.pep.pemex.com mediante el comando dcpromo (ver apéndice A.1 Procedimiento para el comando dcpromo parte 1).
- Se habilitaron los servicios DNS (ver apéndice A.2 Procedimiento de Instalación de los servicios DNS).
- Se realizó la configuración de los servicios DNS (ver apéndice A.3 Procedimiento de la Configuración de los servicios DNS).
- Se modificaron nuevamente las direcciones DNS en los parámetros de la tarjeta de Red.
    a. DNS primario: IP pepgrfdc02
    b. DNS secundario: IP pepsededc01
    c. Se agrego todos los controladores de dominio de sede[21]
- Se crearon las zonas de la siguiente forma:
    a. En el controlador de dominio adicional "pepgrfdc02" se creó una zona primaria de tipo "*Active Directory-Integrated*" del dominio grf.pep.pemex.com (ver apéndice A.4 Procedimiento de Configuración de Zonas parte 1) y una zona secundaria del dominio sede.dpep.pemex.com (ver apéndice A.4 Procedimiento de Configuración de zonas parte 2)
    b. En el controlador de dominio primario "pepsededc01" se creó una zona secundaria del dominio grf.pep.pemex.com
- Se dio la autorización de la transferencia de zonas en ambos controladores de dominio (ver apéndice A.4 Procedimiento de Configuración de zonas parte 3).

[20] Consultar la dirección www.windows update.com
[21] En la pestaña de DNS en la ventana de Configuración avanzada de TCP/IP

- Se actualizaron las zonas creadas (ver apéndice A.4 Procedimiento de Configuración de zonas parte 4).
- Se verificaron los servicios DNS ejecutando el comando ping[22] en la siguiente forma:
  a. En el servidor "pepgrfdc02"
     c:\ping pepsededc01.pep.pemex.com
  b. En el servidor pepsededc01
     c:\ping pepgrfdc02.grf.pep.pemex.com
- Se habilitaron los servicios WINS (ver apéndice A.5 Procedimiento de Instalación de los servicios WINS).
- Se realizó la configuración de los servicios WINS (ver apéndice A.6 Procedimiento de Configuración de los servicios WINS) y se configuró como *partner replicator* por lo menos un WINS del dominio Sede.
- Se agregaron los WINS de los servidores pepdpepdc04 y pepdepdc03 en los parámetros de la tarjeta de Red.
- Se verificaron los servicios WINS ejecutando el comando ping en la siguiente forma:
  a. En el servidor "pepgrfdc02"
     c:\ping pepsededc01
  b. En el servidor pepsededc01
     c:\ping pepgrfdc02

5.1.2 Eliminación del dc original

En este apartado se efectuaron las tareas 4,5 y 6 (ver tabla 3.1) del plan de trabajo que nos ayudó a la eliminación del controlador de dominio primario "pepmxgrfw2k301"del dominio grf.pep.pemex.com, conforme a las actividades de las tablas (4.5, 4.6 y 4.7):

- Como primer paso se realizó la transferencia de roles[23] del controlador de dominio pepmxgrf2kw301 al controlador de dominio pepgrfdc02 (ver apéndice A.7 Procedimiento para la Transferencia de Roles), los roles se transfirieron de la forma siguiente:
  a. Transfirió el Rol Maestro PDC Emulador,
  b. Transfirió el Rol Maestro RID

[22] Comando ping: Este programa nos indica el tiempo exacto que tardan los paquetes de datos en ir y volver a través de la red desde nuestro PC a un determinado servidor remoto.
[23] Para ejecutar la tarea de transferencia debe tener una cuenta de usuario con privilegios de Administrador y pertenecer al grupo de Schema admin.

c. Transfirió el Rol Maestro Infraestructura
d. Transfirió el Rol Maestro Nombre de Dominio y
e. Transfirió el Rol Maestro Esquema

- Se habilitó el controlador de dominio pepgrfdc02 como Catálogo Global (ver apéndice 4.4.8 Procedimiento para la habilitación del Catálogo Global).
- Se realizó la despromoción del controlador de dominio pepmxgrfw2k301 mediante el comando *dcpromo* (ver apéndice A.4 Procedimiento para el comando *DCPROMO* parte 2); por lo que el dominio de grf.pep.pemex.com tiene un solo controlador de dominio "pepgrfdc02"
- Se deshabilitaron los servicios DNS y WINS del servidor pepmxgrfw2k301 (ver apéndice A.9 Procedimiento para la deshabilitación de los Servicios DNS y WINS).
- Se modificaron los parámetros del servidor DHCP: Dirección IP de los DNS y direcciones IP de los servidores WINS.
- Se verificaron los servicios DNS mediante el comando ping (visto anteriormente pág 74).
- Se realizó nuevamente la actualización de las zonas en los servidores pepsededc01 y pepgrfdc02 (ver apéndice A.4 Procedimiento de Configuración de Zonas parte 4).

5.1.3 Relación entre dominios

La relación entre dominios grf y sede se hizo mediante una relación de confianza externa (ver apéndice A.10 Procedimiento para hacer la Relación de Confianza parte 1) que permitió la autenticación de los usuarios en un dominio fuera de un bosque.
Con esta tarea terminamos la etapa de pre-migración.

5.2 Etapa de migración

En la fase de migración (ver figura 5.2) se contempló la integración de los usuarios, grupos globales, servidor miembro y las estaciones de trabajo al dominio sede, lo que específica el plan de trabajo en las tareas 8 a la 11 (ver tabla 4.1).

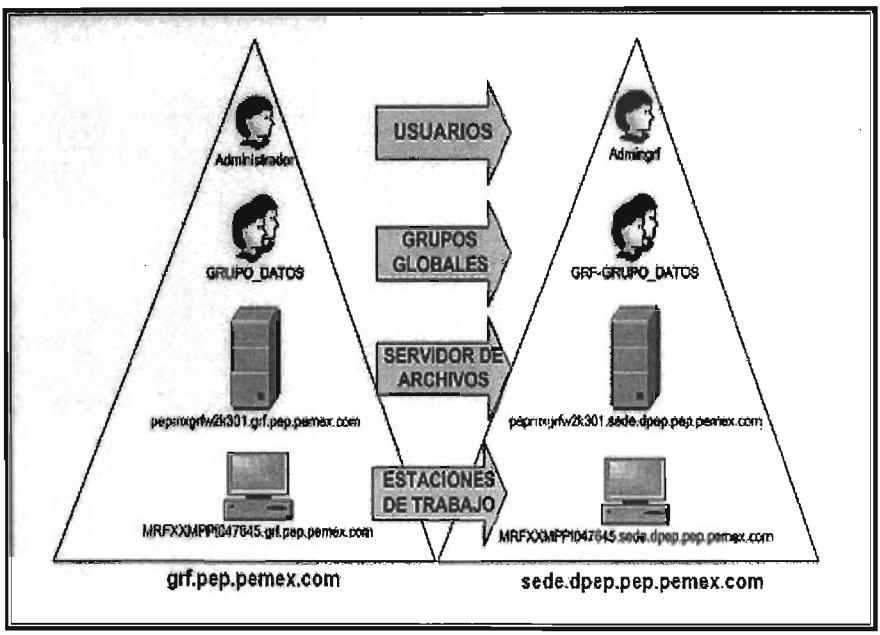

FIGURA 5.2 Fase de migración

5.2.1 Migración de usuarios

En la fase de migración de usuarios, el proceso funciona haciendo uso del atributo *SIDHistory*[24] (para trabajar con este atributo, se tuvo que deshabilitar el filtro de *SIDhistory*[25] cuando se creo la relación de confianza), el cual ayuda a migrar los *SID's*[26] de las cuentas de usuarios del dominio origen al dominio destino.

Las actividades se realizaron de la siguiente forma:

- Se solicitó una lista actualizada de usuarios al administrador del dominio grf.pep.pemex.com, para realizar una comparación con la lista de usuarios del dominio destino. De esta comparación se tuvo la necesidad de crear algunos usuarios que no existían en el dominio sede. Por último se hizo una relación de 180 usuarios

[24] SidHistory: Son los todos los Identificadores de seguridad que puede tener un objeto.
[25] Deshabilitando el filtro del atributo de SIDHistory, un usuario con privilegios de administrador del dominio confiado podría acceder a los recursos del otro dominio para otorgarse privilegios
[26] SIDs: Identificadores de Seguridad

de ambos dominios en un archivo llamado mapusuers.txt con el formato siguiente:

User logon name GRF,User logon name SEDE

Por ejemplo:

administrator,admingrf
ACorderoL,acorderol
asoberam,asoberam
AUribeV,auribev
averal,averal

- Se aplicaron los pre-requisitos (ver apéndice A.11 Procedimientos para los Pre-Requisitos de Migración de Usuarios).
- Se ejecutó la herramienta *FastLane Migrator* en el servidor pepsedeapp01.sede.dpep.pep.pemex.com (ver apéndice A.12 ver Procedimiento para la Migración de Usuarios).
- Se verificó el inicio de sesión de un usuario llamado ACordeloL a su equipo llenando los campos (tabla 5.1) y acceso a sus unidades de red, impresoras e información correctamente.

Nombre de Usuario	AcorderoL
Contraseña	********
Conectarse a	GRF

TABLA 5.1 Autenticación 1

5.2.2 Migración de grupos globales

Esta migración hizo que los grupos globales del dominio grf fueran creados en la OU de GRF del dominio sede y además fue copiado su SIDHistory al dominio sede.

Las actividades se realizaron de la siguiente forma:

Se solicitó una lista de grupos del dominio grf, en la cual se generó un archivo de 50 grupos llamado grupos.mtp a partir del archivo grupos.txt con el siguiente formato:

GRUPO_DEPARTAMENTO

Por ejemplo:

GRUPO_BANCA
GRUPO_CITRIX_CONTABILIDAD
GRUPO_CONSOLIDACION
GRUPO_CONTABILIDAD

- Se ejecutó la herramienta FastLane Migrator en el servidor pepsedeapp01 para la migración de grupos globales (ver apéndice A.13 Procedimiento de Migraciones de Grupos Globales).
- Adicionalmente se crearon dos grupos en forma manual directamente en la OU de GRF del dominio Sede: GRF-GRUPO_ Administradores que sustituyó al grupo de Administrators del dominio grf y GRF-GRUPO_Todos los usuarios, el grupo *Domain Users* de grf agregando los mismos permisos de los grupos de grf originales.
- Se verificó en el controlador de dominio pepsededc01 en la aplicación "Directorio Activo de Usuarios y Computadoras" en la OU de GRF que los grupos fueran creados satisfactoriamente en el dominio sede.

5.2.3 Migración del servidor de archivos

De acuerdo al laboratorio se previó el funcionamiento del Servidor DHCP, se movió la base de datos DHCP del servidor pepmxgrfw2k301 a un nuevo servidor llamado grf_DHCP.sede.dpep.pep.pemex.com para evitar el conflicto de IP's (ver apéndice A.15 Procedimiento para el servidor DHCP).

Posteriormente, el proceso de migración del servidor de archivos consiste en sacar el servidor del dominio origen e ingresarlo al dominio destino (ver apéndice A.14 Procedimiento para la Migración del Servidor de Archivos).

- Los grupos y usuarios del dominio grf que tenían acceso a las carpetas del servidor aparecen ahora en éstas como grupos y usuarios del dominio sede solamente.
- Se verificó el inicio de sesión de un usuario llamado ACorderoL a su equipo (ver tabla 5.1) y acceso a sus unidades de red, impresoras e información correctamente.

5.2.4 Migración de estaciones de trabajo

Antes de iniciar el proceso de migración de estaciones de trabajo se copió el archivo ***mapeos.bat*** en la OU de GRF del dominio sede para cuando los equipos estén migrados, el usuario puede ejecutar el archivo en el momento de su autenticación.

El proceso de migración de estaciones de trabajo en forma manual consiste en:

- Cambiar las direcciones DNS de la tarjeta de red,
- Sacar el equipo del dominio grf.pep.pemex.com,
- Ingresar el equipo al dominio sede.dpep.pep.pemex.com,
- Crear un perfil nuevo del usuario del dominio sede, que ocupa el equipo,
- Copiar el perfil anterior al nuevo perfil y
- Verificar el acceso a los recursos.

La herramienta, lo que hace, es ejecutar un script llamado "SetWKSDefaultDomain" para verificar el acceso al recurso por el administrador del dominio sede, actualiza los privilegios del perfil del usuario y migra el equipo al nuevo dominio.
Las actividades se realizaron de la siguiente forma:

- Se solicitó una lista de equipos actualizada con: nombre del equipo, dirección IP, dirección física y usuario al que pertenece el equipo.
- Se agregó una línea la siguiente línea: *"net localgroup administrators sede\administrator"* al archivo mapeos.bat que utilizan para cada usuario de grf, con la finalidad de incorporar el usuario administrador del dominio origen en todas las computadoras del dominio destino.
- Se revisaron los equipos cumpliendo los siguientes pre-requisitos para iniciar el proceso de actualización:
    a. No debe tener contraseña de arranque en BIOS o ninguna contraseña al momento de arranque,
    b. El usuario del equipo debe autenticarse como última vez,
    c. El usuario no debe utilizar el equipo en un lapso de 15 minutos aproximadamente,
    d. El equipo no debe tener *diskettes* al momento de migrar, y
    e. Debe estar prendido el equipo en el proceso.

- Se ejecutó el *script "SetWKSdefault Domain"* en el servidor pepsedeapp01 (apéndice A.16 ver procedimiento para la Migración de Estaciones de Trabajo parte 1).
- Se realizó la actualización de los equipos con la herramienta *FastLane Migrator* (apéndice A.16 ver procedimiento para la Migración de Estaciones de Trabajo parte 2).
- Se migraron los equipos al dominio sede (ver apéndice A.16 procedimiento para la Migración de Estaciones de Trabajo parte 3).
- Se verificó el inicio de sesión de un usuario llamado acorderol a su equipo llenando los campos (tabla 5.2) y acceso a sus unidades de red, impresoras e información correctamente.

Nombre de Usuario	acorderol
Contraseña	********
Conectarse a	SEDE

TABLA 5.2 Autenticación 2

5.3 Etapa de post-migración

En esta última fase se cumple con las tareas 12, 13 y 14 (ver tabla 4.1) que se dedica a eliminación de la relación del dominio sede y grf, a cancelar el controlador de dominio y entregar formalmente la administración delegada a los informáticos de grf, con esto, se culmina el proyecto de integración de dominios (ver figura 5.3).

5.3.1 Verificación de servicios

Una verificación de servicios de suma importancia es la correspondiente a la resolución de nombres, donde se verificó que los servicios de DHCP estén funcionando correctamente, asimismo se llevó a cabo la verificación de asignación de unidades de red para todos y cada uno de los usuarios.

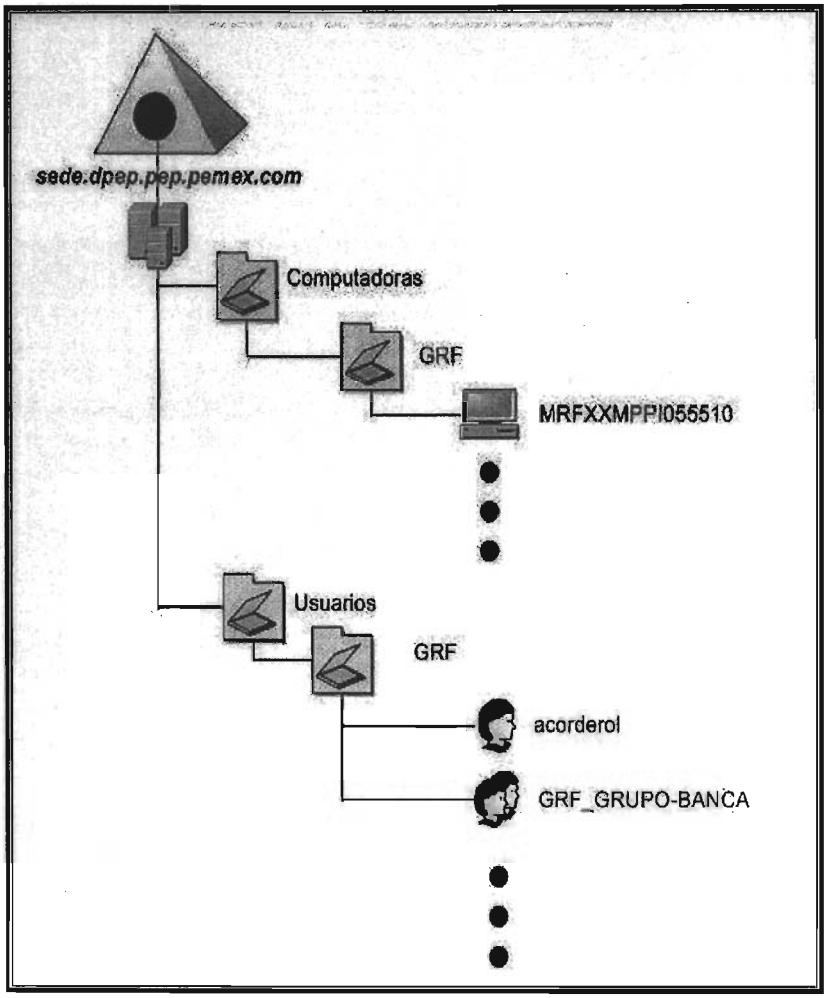

FIGURA 5.3 Fase de post-migración

5.3.2 Eliminación de la relación entre dominios

La eliminación de la relación entre dominios grf y sede se hizo mediante el comando *netdom* (ver apéndice A.9 Procedimiento para la Relación de Confianza parte 2) para que los usuarios se autentiquen solamente en el dominio sede.

Después de la eliminación de la relación de confianza, se restauraron los parámetros modificados en el dominio sede que fueron los siguientes:

- Se eliminó la cuenta de usuario del dominio grf.pep.pemex.com en el **grupo *Administrators*** del **contenedor *Builtin*** del dominio sede.dpep.pep.pemex.com en el programa del **Directorio Activo de Usuarios y Computadoras.**
- Se deshabilitó en el controlador de dominio pepsededc01 la **Auditoría** con la opción de ***Success*** y ***Failure*** en "***Audit account Management***" en el programa ***Domain Security Policy*** del dominio local de ***AD.***
- Se eliminó la zona secundaria grf.pep.pemex.com de los servicios DNS en el servidor pepsededc01.
- Se quitó la autorización de la zona grf.pep.pemex.com en los servicios DNS del servidor pepsededc01.

5.3.3 Despromoción del dc nuevo

La despromoción del controlador de dominio pepgrfdc02 se realizó mediante el comando *dcpromo* (ver apéndice A.1 Procedimiento para el comando *DCPROMO* parte 2); por lo que el dominio de grf.pep.pemex.com ya no existe y el servidor pergrfdc02 es un servidor miembro; así mismo se deshabilitó los servicios DNS y WINS (ver apéndice A.9 Procedimiento para la deshabilitación de los Servicios DNS y WINS).

5.3.4 Entrega de la administración

Con este punto se terminó el proyecto, se realizaron las siguientes actividades:

- Se delegó la administración al informático de GRF (ver apéndice A.17 Procedimiento para el Derecho de Delegar el Control).
- Se creó la consola de administración[27] de la OU de GRF (ver apéndice A.18 Procedimiento para la Consola Administrativa) y se entregó al informático de grf.
- Se le entregó un documento con la notificación de normas seguidas en el Dominio Sede que contiene:

[27] Está consola se instala con la herramienta Adminpack.msi

a. Las responsabilidades de su OU,
b. Lo que puede hacer en su OU (modificar y deshabilitar cuentas de usuarios; crear, borrar y modificar grupos), y
c. Derechos y Obligaciones que tienen con su servidor pepmxgrfw2k301 y grf_DHPC.

5.4 Mantenimiento

5.4.1 Definición

El mantenimiento es una actividad constante que conserva al sistema en buen funcionamiento, reduciendo sus errores y disminuyendo la interrupción de su servicio sin aumentar los costos.

5.4.2 Tipos de mantenimiento

- **Mantenimiento correctivo**

Es el conjunto de actividades dedicadas a corregir defectos en el hardware o en el software detectados por los usuarios durante la utilización del sistema.

- **Mantenimiento adaptativo**

Es el conjunto de actividades para adaptar el sistema a los cambios (hardware o software) en su entorno tecnológico.

- **Mantenimiento perfectivo**

Es el conjunto de actividades para mejorar o añadir nuevas funcionalidades requeridas por el usuario.

- **Mantenimiento preventivo**

Es el conjunto de actividades para hacer ajustes, modificaciones, cambios, limpieza y reparaciones necesarias para conservar las condiciones óptimas del sistema con el fin de evitar posibles daños.

5.4.3 Propuesta de mantenimiento

La siguiente propuesta es para conservar el acceso del usuario a la información y recursos después de la integración:

Se deberán realizar los siguientes tipos de mantenimiento en el dominio de sede:

Mantenimiento correctivo

- Cambiar hardware (servidor, disco, memorias, etc.) en mal funcionamiento.
- Cambiar el servicio de directorio a otro de diferente plataforma por un cambio de organización, una adquisición empresarial o la estructura actual deje de ser adecuada.

Mantenimiento adaptativo

- Modificar la estructura de las OU respecto a las necesidades de la empresa.
- Verificar mensualmente las tareas de la administración delegada.
- Cambiar servidores de acuerdo con las compras de la empresa.

Mantenimiento perfectivo

- Actualizar Parches en forma periódica.
- Actualizar el Sistema Operativo: Windows 2000 Advanced server a Windows 2003 Enterprise Edition.

Mantenimiento preventivo

- Actualizar diariamente el Antivirus.
- Actualizar periódicamente la administración de usuarios y grupos conforme se solicite por el personal.
    a. Borrar usuarios de las OU que no pertenezcan a las Gerencias
    b. Crear nuevos usuarios en las OU de cada gerencia conforme se soliciten (un nuevo miembro, o para proyectos).
    c. Deshabilitar cuentas de usuarios que estén de vacaciones o de comisión o no estén laborando actualmente.
    d. Crear, borrar o modificar Grupos dependiendo de la nueva reestructuración administrativa de cada Gerencia.
    e. Añadir, eliminar o agregar usuarios a los Grupos creados para conceder accesos a la información y recursos.

- Limpiar, conservar y reparar dos veces al año el equipo de cómputo.
- Rediseñar mensualmente las políticas de grupo para cambios de seguridad.
- Respaldar semanalmente la base de datos del Directorio Activo.
- Verificar semanalmente la replicación de controladores de dominio.
- Verificar semanalmente las bases datos de los servicios DNS y WINS.
- Verificar semanalmente los recursos físicos, de memoria y capacidades de almacenamiento.
- Verificar cada fin de mes los sitios y las subredes, son creadas, actualizadas y que los costos e intervalos de sincronización sean fiables.

CONCLUSIONES

La integración de dominios e infraestructura fue una de las actividades primordiales para la empresa, en este documento se plasmó la consolidación de un Directorio Activo Origen como una Unidad Organizacional en un Directorio Destino.

Este proyecto cumplió con las expectativas de los objetivos, los cuales definieron una estrategia de migración para integrar a la Gerencia de Recursos Financieros en el dominio de Sede; durante este proceso, antes y después de eliminar el dominio origen, en forma óptima se mantuvieron sus recursos y servicios disponibles; ejecutándose las tareas del proyecto en forma paralela a las actividades de la Gerencia.

La aportación del proyecto fue tomar todos los recursos y medios disponibles del dominio destino para llevar a cabo todas las etapas del proyecto en forma eficiente.

El beneficio para ambos dominios fue hacer la integración de manera transparente sin afectar su información primordial y hacerlo sin costos adicionales que pudieran afectar los recursos y costos del organismo de PEP.

Actualmente el proyecto está en operación desde diciembre del año pasado, durante este tiempo no ha existido alguna falla respecto a sus elementos que la integran.

Este proyecto, si lo llevarán a cabo en otras regiones del organismo de PEP que tienen características similares, las mejoras que obtendrían serían: menor tiempo de implementación, disponibilidad de recursos y servicios, costos nulos ya que tienen todos los recursos y medios propios en las regiones. Los beneficios se reflejan en una administración centralizada de los recursos, obteniéndose así mayores ingresos financieros.

Este proyecto también puede ser de gran utilidad a empresas privadas, externas; obteniendo de éste, como beneficio, una guía de proyecto de migración que puede ser implementada con algunas adecuaciones en cualquier otro entorno.

Finalmente, la Gerencia tiene la disponibilidad de sus recursos y servicios en buen funcionamiento, además de que el Dominio Sede, le está proporcionando mantenimiento e innovación tecnológica que tiene a su alcance.

APÉNDICE A
PROCEDIMIENTOS

Los procedimientos presentados a continuación, están basados en Windows 2003 server porque el origen de la migración estuvo en esta plataforma. Estos procedimientos son claros y precisos descritos en pasos de forma secuencial para ejecutar una tarea o actividad determinada.

A.1 Procedimiento para la ejecución del comando dcpromo

Parte 1. Configuración para un controlador de dominio Adicional

1. Abrir una ventana de Ms-Dos y ejecutar el comando ***dcpromo***
2. Dar clic en **Siguiente**
3. Dar clic en **siguiente** en la ventana de **Bienvenida a la Instalación del Directorio Activo**
4. Seleccionar **Un controlador de dominio adicional para un dominio existente** en la ventana de **Tipo de Controlador de Dominio**
5. Dar clic en **Siguiente**
6. Escribir el nombre de usuario y contraseña que tenga privilegios de administrador del dominio en la ventana de **Autenticación de la Red**
7. Escribir el nombre de dominio en la ventana de **Controlador de dominio Adicional**
8. Dar clic en **Siguiente**
9. Dar clic en **Siguiente** en la ventana de ***Database and Log Folders***
10. Dar clic en **Siguiente** en la ventana de ***Shared System Volume***
11. Escribir la contraseña y confirmarla en la ventana de **Modo de Restauración**
12. Dar clic en **Siguiente**
13. Dar clic en **Siguiente** en la ventana de **Resumen**
14. Dar clic en **Finalizar** en la ventana de **Completa la Instalación *Wizard* del Directorio Activo**
15. Dar clic en **Reiniciar ahora**

Parte 2. Despromoción de un controlador de dominio

1. Abrir una ventana de Ms-Dos y ejecutar el comando dcpromo
2. Dar clic en **Siguiente**
3. Dar clic en **Siguiente** en la ventana de **Bienvenida a la Instalación del Directorio Activo**
4. Dar clic en **siguiente** en la ventana de **Remover el Directorio Activo**
5. Escribir la nueva contraseña del administrador del servidor en la ventana de **Contraseña de Administrador**

6. Dar clic en **Siguiente** en la ventana de **Resumen**
7. Dar clic en **Finalizar** en la ventana de **Completa la Instalación *Wizard* del Directorio Activo**
8. Dar clic en **Reiniciar Ahora**

A.2 Procedimiento para la instalación de los servicios DNS

1. Dar clic en **Panel de Control**
2. Dar clic en **Agregar o remover programas**
3. Dar clic en **Agregar o remover componentes de Windows**
4. Seleccionar **Servicios de Red** en la ventana de **Componentes de Windows**
5. Dar clic en **Detalles**
6. Seleccionar **Sistema de Nombres de Dominio (DNS)** en la ventana de **Servicios de Red**
7. Dar clic en **Aceptar**
8. Dar clic en **Siguiente**
9. Dar clic en **Aceptar** en la ventana de **Insertar Disco**
10. Dar clic en **Buscar** en la ventana **Archivos necesarios**
11. Buscamos el directorio **i386**
12. Dar clic en **Abrir**
13. Dar clic en **Aceptar**
14. Dar clic en **Siguiente** en la ventana de **Componentes de Configuración**
15. Dar clic en **Finalizar** en la ventana de **Completo los Componentes de Windows**

A.3 Procedimiento para la configuración de los servicios DNS

1. Dar clic en **Herramientas Administrativas**
2. Dar clic en **DNS**
3. Seleccionar el servidor a configurar el servicio
4. Dar clic derecho
5. Dar clic en **Configurar los servicios DNS**
6. Dar clic en **Siguiente** en la ventana de **Bienvenido a la Guía de Configuración de un Servidor DNS**

7. Seleccionar ***Create forward and reverse lookup zones*** en la ventana de **Selección de acción de configuración**
8. Dar clic en **Siguiente**
9. Seleccionar **No crear ahora una zona *forward and reverse lookup*** en la ventana de ***Forward Lookup Zone***
10. Dar clic en **Siguiente**
11. Seleccionar **No debe reenviar peticiones** en la ventana de ***Forwarders***
12. Dar clic en **Siguiente**
13. Dar clic en **Finalizar** en la ventana de **Completo la configuración de un servidor DNS**

A.4 Procedimiento para configuración de zonas

PARTE 1. Configurar una zona primaria tipo "***Active Directory-Integrated***":

1. Seleccionar el servidor donde se creará la zona
2. Seleccionar **Zona primaria y almacenarla en el Directorio Activo** en la ventana de **Tipo de Zona**
3. Dar clic en **Siguiente**
4. Seleccionar **todos los controladores de dominio en el dominio** [nombre de dominio]
5. Escribir el nombre del dominio en la ventana de **Nombre de la zona**
6. Dar clic en **Siguiente** en **Archivos de zona**
7. Seleccionar **Permite la seguridad en las actualizaciones dinámicas** en la ventana **Actualizaciones Dinámicas**
8. Dar clic en **Siguiente**
9. Dar clic en **Terminar** en la ventana de **Completa la instalación de la zona**

PARTE 2. Configurar una zona secundaria

1. Seleccionar el servidor donde se creará la zona
2. Dar clic en **Siguiente** en la ventana de **Bienvenido a la Instalación de una nueva Zona**
3. Seleccionar **Zona secundaria** en la ventana de **Tipo de Zona**
4. Dar clic en **Siguiente**

5. Escribir el nombre del dominio en la ventana de **Nombre de la zona**
6. Dar clic en **Siguiente**
7. Escribir la dirección IP del servidor que se hará la copia en la ventana de ***Master DNS Servers***
8. Dar clic en **Siguiente**
9. Dar clic en **Terminar** en la ventana de **Completa la instalación de la zona**

PARTE 3. Autorizar la creación de la zona

1. Seleccionar el dominio que se va a copiar la zona
2. Abrir la consola de administración ***DNS***
3. Seleccionar el **controlador de dominio** de donde se va a hacer una copia de la zona
4. Dar clic derecho **en la zona**, ubicado en ***Forward Lookup Zones***
5. Seleccionar propiedades
6. Dar clic en la pestaña de **Transferencia de Zona**
7. Seleccionar **Permitir la zona de transferencia**
8. Seleccionar **Solo los siguientes servidores**
9. Escribir la IP del servidor al cual se va a transferir la copia de la zona
10. Dar clic en **Agregar**
11. Dar clic en **Aplicar**
12. Dar clic en **Aceptar**

PARTE 4. Actualizar la zona

1. Seleccionar el Controlador de dominio donde se creo la zona
2. Si la zona es primaria, tipo "***Active Directory-Integrated***":
   - 2.1 Dar clic Derecho en la zona ubicada en ***Forward Lookup Zones***
   - 2.2 Seleccionar Recargar
   - 2.3 Dar clic en Si en el mensaje: "¿Quieras recargar la zona [nombre del dominio] ?"
3. Si la zona es secundaria:
   - 3.1 Dar clic derecho en la zona ubicada en ***Forward Lookup Zones***
   - 3.2 Seleccionar Transferencia desde el Maestro

A.5 Procedimiento para la instalación de los servicios WINS

1. Dar clic en **Panel de Control**
2. Dar clic en **Agregar o remover programas**
3. Dar clic en **Agregar o remover componentes de Windows**
4. Seleccionar **Servicios de Red** en la ventana de **Componentes de Windows**
5. Dar clic en **Detalles**
6. Seleccionar ***Windows Internet Name Service*** **(WINS)** en la ventana de **Servicios de Red**
7. Dar clic en **Aceptar**
8. Dar clic en **Siguiente**
9. Dar clic en **Aceptar** en la ventana de **Insertar Disco**
10. Dar clic en **Buscar** en la ventana **Archivos necesarios**
11. Buscamos el directorio **i386**
12. Dar clic en **Abrir**
13. Dar clic en **Aceptar**
14. Dar clic en **Siguiente** en la ventana de **Componentes de Configuración**
15. Dar clic en **Finalizar** en la ventana de **Completo los Componentes de Windows**

A.6 Procedimiento para la configuración de los servicios WINS

1. Abrir la herramienta de administración de WINS **Inicio\Programas\Herramientas Administrativas\WINS**
2. Seleccionar y expandandir las **opciones del servidor**
3. Dar clic derecho en **Socio de Replicación** y seleccionar **New Replication Partner**
4. Ingresar la **dirección IP del servidor**, en la ventana siguiente con el cual se realizara la replicación de Base de datos de WINS
5. Dar clic en **Aceptar**
6. Cerrar la herramienta de administración

A.7 Procedimiento para la transferencia de roles

PARTE 1. Transferir el Role Maestro Emulador PDC, Maestro RID y Maestro de Infraestructura

1. Seleccionar el controlador de dominio donde se va a transferir el rol
2. Dar clic en **Herramientas Administrativas**
3. Dar clic en **Directorio Activo de Usuarios y Computadoras**
4. Dar clic derecho en el dominio
5. Seleccionar el **Maestro de Operaciones**
6. Seleccionar la pestaña del rol que se va a transferir: **RID, PDC o Infraestructura**
7. Dar clic en **Cambiar**
8. Dar clic en **Si** en el mensaje: **"¿Estás seguro que quieres transferir el rol de operación?"**
9. Dar clic en **Aceptar** en el mensaje: **"El rol fue transferida satisfactoriamente"**

PARTE 2. Transferir el rol del Maestro de Dominio

1. Ingresar al controlador de dominio que tiene el rol
2. Dar clic derecho en **Dominios y Confianzas del Directorio Activo**
3. Elegir **Conectar a un controlador de dominio**
4. Seleccionar el servidor al cual se desea transferir el rol
5. Dar clic derecho en **Dominios y Confianzas del Directorio Activo** y
6. Seleccionar el **Maestro de Operaciones**
7. Dar clic en **Cambiar**
8. Dar clic en **Si** en el mensaje: **"¿Estás seguro que quieres transferir el rol de operación?"**
9. Dar clic en **Aceptar** en el mensaje: **"El rol fue transferida satisfactoriamente"**

PARTE 3. Transferir el Rol Maestro Esquema

1. Ejecutar el comando cmd
2. Escribir ***c:\regsvr32 schmmgmt.dll***[27] [ENTER]

[27] Este registro es para visualizar el maestro esquema en la consola de administración.

3. Dar clic en Aceptar en el mensaje: DllRegisterServer in schmmgmt.dll suceded
4. Ejecutar ***mmc*** (Aparece una pantalla llamada Consela1)
5. Dar clic en **Agregar o Remover Componente** en la ventana de **Archivo**
6. Dar clic en **Agregar** en la ventana **Agregar o Remover Componente**
7. Seleccionar **Esquema del Directorio Activo** en la ventana **Agregar Componentes Individuales**
8. Dar clic en **Agregar** (dos veces)
9. Dar clic en **Cerrar**
10. Dar clic en **Aceptar**
11. Dar clic derecho sobre un componente de **Esquema del Directorio Activo** agregado anteriormente
12. Dar clic en **Cambiar el controlador de dominio**
13. Seleccionar **Nombre específico**, escribimos el nombre del controlador de dominio del rol del esquema maestro
14. Dar clic en **Aceptar**
15. Repetir los pasos 11, 12, 13 y 14 pero ahora dando el nombre del controlador de dominio destino
16. Dar clic en botón derecho sobre **Esquema del Directorio Activo destino**
17. Dar clic en **Maestro de Operaciones**
18. Dar clic en **Cambiar** de la ventana **Cambiar el Maestro Esquema**
19. Dar clic en **Si** en el mensaje: **"¿Estás seguro que quieres transferir el rol de operación?"**
20. Dar clic en **Aceptar** en el mensaje: **"El rol fue transferida satisfactoriamente"**

A.8 Procedimiento para la habilitación del catálogo global

1. Seleccionar el controlador de dominio donde se habilitará el Catálogo Global
2. Dar clic en **Herramientas Administrativas**
3. Dar clic en **Sitios y Servicios del Directorio Activo**
4. Dar clic en ***Sites\Default-First-Site-Name*** [Sitio donde pertenezca el *DC*] ***Servers*\Controlador Dominio*NTDS Settings***

5. Dar clic derecho en **Propiedades**
6. Dar clic en **Catálogo Global** en la pestaña de General
7. Dar clic en **Aplicar**
8. Dar clic en **Aceptar**

A.9 Procedimiento para deshabilitar los servicios DNS y WINS

PARTE 1: Para los servicios DNS

1. Dar clic en **Herramientas Administrativas**
2. Detener el servicio DNS
   - 2.1 Abrir el programa **DNS**
   - 2.2 Hacer clic en el **servidor DNS aplicable**, en el árbol de la consola
   - 2.3 Dar clic en **menú Acción**
   - 2.4 Seleccionar **Todas las tareas**
   - 2.5 Dar clic en **Detener el servicio**
3. Quitar el programa de **DNS**
   - 3.1 Dar clic en **Panel de Control**
   - 3.2 Dar clic en **Agregar o remover programas**
   - 3.3 Dar clic en **Agregar o remover componentes de Windows**
   - 3.4 Seleccionar **Servicios de Red** en la ventana de **Componentes de Windows**
   - 3.5 Dar clic en **Detalles**
   - 3.6 Desactivar **Sistema de Nombres de Dominio (DNS)** en la ventana de **Servicios de Red**
   - 3.7 Dar clic en **Aceptar**
   - 3.8 Dar clic en **Siguiente**
   - 3.9 Dar clic en **Finalizar**

PARTE 2: Para los servicios WINS

1. Dar clic en **Herramientas Administrativas**
2. Abrir el programa **WINS**
3. Repetir los pasos 2 y 3 de la parte 1 pero ahora ***Windows Internet Name Service (WINS)***

A.10 Procedimiento para la relación de confianza

PARTE 1: Para hacer la relación entre dominios

1. Abrir una ventana Ms-dos o ejecutar el comando ***cmd***
2. Buscar el directorio predeterminado donde estas instaladas las Herramientas de Suporte[28]: ***c:\Program Files\Support Tools>***
3. Utilizar el **comando *netdom*** tara hacer la relación de confianza entre ambos dominios.
4. Escribir la siguiente sintaxis:

C:\Program Files\Support Tools> netdom trust [nombre del dominio origen] ***/Domain :***[dominio destino] ***/UserD:*** [usuario con privilegios de administrador del dominio destino] ***/PasswordD:* /UserO:*** [usuario con privilegios de administrador del dominio origen] ***/PasswordO:* /PasswordT:***[Contraseña que se pondrá a la relación] ***/add /twoway /EnableSIDHistory:yes***[29] [***ENTER***]

4.1 ***Type the password associated with the domain user.***
Escribimos la contraseña del Origen [***ENTER***]

4.2 ***Type the password associated with the domain user.***
Escribimos la contraseña del Destino [***ENTER***]

4.3 Aparece el siguiente mensaje: "***SID history is disabled for this trust. The command completed successfully***"

PARTE 2: Para eliminar la relación entre dominios.

1. Abrir una ventana Ms-dos o ejecutar el comando cmd
2. Buscar el directorio predeterminado donde estas instaladas las Herramientas de Suporte: ***c:\Program Files\Support Tools>***
3. Utilizar el **comando *netdom*** para hacer la relación de confianza entre ambos dominios.
4. Escribir la siguiente sintaxis:

C:\Program Files\Support Tools> netdom trust [nombre del dominio origen] ***/Domain :***[dominio destino] ***/UserD:*** [usuario

[28] Si no están instaladas, obtenerlas del disco de Instalación de Windows 2003 Enterprise
[29] /EnableSIDHistory: Se utiliza para modificar las SID History de los objetos del Directorio Activo, este parámetro es de Windows 2003 que sustituyo /FilterSids en Windows 2000

con privilegios de administrador del dominio destino] ***/PasswordD:* /UserO:*** [usuario con privilegios de administrador del dominio origen] ***/PasswordO:* /PasswordT:***[Contraseña que se dio a la relación] ***/remove /twoway*** [***ENTER***]

A.11 Procedimiento para los pre-requisitos de migración de usuarios

1. Agregar la cuenta de usuario (tenga privilegios de administrador) del dominio sede.dpep.pep.pemex.com en el **grupo *Administrators*** del **contenedor *Builtin*** del dominio grf.pep.pemex.com en el programa del **Directorio Activo de Usuarios y Computadoras** [viceversa]
2. Habilitar en los Controladores de Dominio del dominio origen y destino la **Auditoría** con la opción de ***Success*** y ***Failure*** en "***Audit account Management***" en el programa ***Domain Security Policy*** del dominio local de ***AD***
3. Crear en el dominio origen un grupo local sin miembros con el siguiente nombre:<**Dominio Fuente**>**$$$** en el contenedor de ***Users*** del programa del **Directorio Activo de Usuarios y Computadoras**
4. Modificar o crear la siguiente llave del Registro en el dominio origen:
   HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA Value: TCPIPCLIENTSUPPORT type DWORD valor 1
5. Reiniciar el servidor del dominio origen después de haber modificado la llave del registro.
6. Instalar la herramienta ***FastLane Migrator*** en un servidor disponible que pertenezca al dominio Sede.

A.12 Procedimiento para la migración de usuarios

1. Seleccionar el ***Wizard*** **de Migración de Usuarios** dentro de la **Guía del Proyecto**
2. Dar clic en **Siguiente** en la ventana de **Bienvenida**
3. Seleccionar el dominio Origen y el controlador de dominio en la ventana de **Localización de Origen**

4. Dar clic en **Siguiente**
5. Seleccionar el dominio Destino y el controlador de dominio primario en la ventana de **Localización de Destino**
6. Dar clic en **Siguiente**
7. Seleccionar en el dominio Destino la OU donde se van migrar los usuarios
8. Dar clic en **Aceptar**
9. Dar clic en **Siguiente** en la ventana de **OU Destino**
10. Dar clic en **Actualizar**
11. Seleccionar los usuarios a migrar en la ventana de **Selección de Cuenta**
12. Dar clic en **Siguiente**
13. Dar clic en **Siguiente** en la ventana de **Selección de Atributos**
14. Dar clic en **Siguiente** en la ventana de **Configuración de Cuenta de Destino**
15. Seleccionar **No modificar la contraseña de la cuenta destino** en la ventana de **Fijar Contraseña**
16. Dar clic en **Siguiente**
17. Dar clic en **Siguiente** en la ventana de **Configuración de Cuenta Origen**
18. Dar clic en **Siguiente** en la ventana de **Opciones de Grupo**
19. Dar clic en **Siguiente** en la ventana de **Opciones de Conectar el Directorio Activo**
20. Seleccionar **Implementar SIDHistory para migraciones Windows 2000, Prompt para credenciales** y **Checar la dependencia del SIDHistory**
21. Dar clic en **Siguiente** en la ventana de **Opciones de SIDHistory**
22. Seleccionar MERGE **Fusionar la seguridad de las dos cuentas** y **Fusionar las propiedades de la cuenta**
23. Dar clic en **Siguiente** en la ventana de **Duplicación de Nombre**
24. Seleccionar ***Prompt for action during migration***
25. Dar clic en **Siguiente** en la ventana de ***Duplicate Mapping Migration Conflict***
26. Dar clic en ***Edit MMT Mapping File***
27. Dar clic en **Guardar** en la ventana de ***Edit Mapping***
28. Dar clic en **Cancelar**
29. Ejecutar el script **convertmmt.exe**

30. Dar clic en **Select Mapping File** y buscar la ruta del archivo ***wizard.mmt***
31. Dar clic en ***Select Matching File*** y buscar el archive ***mapusers.txt***
32. Dar clic en ***Build New MMT*** en la ventana de ***MMT File converter***
33. Dar clic en **Aceptar** en la ventan de **convertmmt**
34. Ejecutar el ***Wizard de Direct MMT Migrations***
35. Seleccionar el archivo ***Wizard.HDR***
36. Dar clic en **Abrir**
37. Dar clic en **Siguiente** en la ventana de ***Migration Mapping Technology***
38. Seleccionar el archivo ***NewMMT.mmt***
39. Dar clic en **Siguiente**
40. Dar clic en **Aceptar**
41. Escribir una cuenta de usuario con privilegios de administrador del dominio destino
42. Dar clic en **Aceptar**
43. Dar clic en **Siguiente**
44. Dar clic en **Migrar Ahora**

A.13 Procedimiento para la migración de grupos globales

1. Seleccionar el ***Wizard*** **de Migración de Grupos Globales** dentro de la **Guía del Proyecto**
2. Dar clic en **Siguiente** en la ventana de **Bienvenida**
3. Seleccionar el dominio Origen y el controlador de dominio en la ventana de **Localización de Origen**
4. Dar clic en **Siguiente**
5. Seleccionar el dominio Destino y el controlador de dominio primario en la ventana de **Localización de Destino**
6. Dar clic en **Siguiente**
7. Seleccionar en el dominio Destino la OU donde se van migrar los grupos
8. Dar clic en **Aceptar**
9. Dar clic en **Siguiente** en la ventana de **OU Destino**
10. Dar clic en **Actualizar**
11. Seleccionar los grupos a migrar en la ventana de **Selección de Cuenta**

12. Dar clic en **Siguiente**
13. Seleccionar **Adicionar un Prefijo a los Grupos Globales Destino**
14. Dar clic en **Siguiente** en la ventana de **Selección de Atributos**
15. Dar clic en **Siguiente** en la ventana de **Grupos Globales**
16. Seleccionar **Implementar SIDHistory para migaciones Windows 2000, Prompt para credenciales** y **Checar la dependencia del SIDHistory**
17. Dar clic en **Siguiente** en la ventana de **Opciones de SIDHistory**
18. Seleccionar MERGE **Fusionar la seguridad de las dos cuentas** y **Fusionar las propiedades de la cuenta**
19. Seleccionar ***Prompt for action during migration***
20. Dar clic en **Siguiente** en la ventana de ***Duplicate Mapping Migration Conflict***
21. Dar clic en ***Edit MMT Mapping File***
22. Dar clic en **Guardar** en la ventana de ***Edit Mapping***
23. Dar clic en **Siguiente**
24. Dar clic en **Finalizar**
25. Dar clic en **Si** en la ventana de **Configuración del Proyecto**
26. Escribir una cuenta de usuario con privilegios de administrador en el dominio origen en la ventana de ***Enter Network Password***
27. Dar clic en **Migrar ahora**

A.14 Procedimiento para la migración del servidor de archivos

1. Iniciar sesión como **administrador del equipo** ó con cuenta con privilegios de administrador al **servidor de archivos "pepgrfmxw2k301"**
2. Abrir las propiedades de **Mis sitios de red**
3. Dar clic derecho **Conexión de Área Local** y seleccionar **propiedades**
4. Seleccionar las **propiedades de TCP/IP** e ir a **opciones avanzadas**
5. Remover la dirección o direcciones IP de DNS que tenga dadas de alta en la pestaña de **DNS**
6. Agregar las dirección de servidor DNS: **pepsededc01** y **pepsededc03**

7. Verificar que este en blanco la casilla **Anexar estos sufijos DNS**
8. Marcar las casillas: **Anexar sufijos DNS principales y de conexiones especificas, Anexar sufijos primarios del sufijo DNS principal** y **Registrar estas direcciones de conexiones en *DNS***
9. Dar clic en agregar en la ventana de **WINS**
10. Agregar la **dirección IP pepdpepdc02** para el dominio sede en la ventana de Servidor ***WINS TCP/IP***
11. Seleccionar **Habilitar *NetBIOS sobre TCP/IP*** en la ventana de WINS en el recuadro de **Configuración de *NetBIOS***
12. Dar clic en Aceptar hasta salir de las propiedades de **Mis sitios de red**
13. Abrir a las **propiedades de Mi PC**
14. Dar clic en **Cambiar,** en la ventana de **Nombre de Equipo**
15. Habilitar la opción de **Grupo de Trabajo** y escribir Grupo de Trabajo
16. Ingresar los datos de la cuenta de usuarios con los permisos requeridos.
17. Sacar el equipo del dominio aparecerá el siguiente mensaje: **Bienvenido al Grupo de Trabajo**
18. Dar clic en **NO**, en la ventana de **reiniciar el equipo** y cerrar las **propiedades de MI PC**
19. Abrir a las **propiedades de Mi PC**
20. Dar clic en **Cambiar,** en la ventana de **Nombre de Equipo**
21. Dar clic en **Mas** en la ventana de **Cambios de Nombre de Equipo**
22. Escribir el sufijo de DNS: **sede.dpep.pep.pemex.com,** en la ventana de ***DNS Suffix and NetBIOS Computer Name***
23. Habilitar la opción de **Dominio** y escribir el nombre del dominio: **sede.dpep.pep.pemex.com** en la ventana de **Cambios en el nombre de equipo**
24. Dar clic en **Aceptar**
25. Ingresar los datos de la cuenta de usuarios con los permisos requeridos
26. Ingresar al dominio aparecerá el siguiente mensaje: **Bienvenido al dominio sede.dpep.pep.pemex.com**
27. Dar clic en **Aceptar**
28. Reiniciar el equipo

A.15 Procedimiento para el servidor DHCP

PARTE 1: Mover una base de datos DHCP a otro Servidor:

1. Agregar la cuenta del equipo Servidor DHCP a el grupo DHCP Administrador en el nivel Enterprise, esto para evitar el siguiente error: **Error initializing and reading the service configuration - Access Denied**[30]
2. Abrir una ventana Ms-dos o ejecutar el comando ***cmd***
3. Escribir la siguiente sintaxis: ***netsh dhcp server export C:\dhcp.txt all*** [***ENTER***]
4. Esperar hasta que aparezca el siguiente mensaje: **"Command completed successfully"**
5. Copiar el archivo al nuevo servidor
6. Escribir la siguiente sintaxis: ***netsh dhcp server import C:\dhcp.txt all***, [***ENTER***]

PARTE 2: Instalación de un servidor DHCP

1. Dar clic en **Inicio**
2. Dar clic en **Panel de Control**
3. Dar clic en **Agregar o remover programas**
4. Dar clic en **Agregar o remover componentes de Windows**
5. Seleccionar **Servicios de Red** en la ventana de **Componentes de Windows**
6. Dar clic en **Detalles**
7. Seleccionar ***Dynamic Host Configuration Protocol (DHCP)*** en la ventana de **Servicios de Red**
8. Dar clic en **Aceptar**
9. Dar clic en **Siguiente**
10. Dar clic en **Aceptar** en la ventana de **Insertar Disco**
11. Dar clic en **Buscar** en la ventana **Archivos necesarios**
12. Buscamos el directorio **i386**
13. Dar clic en **Abrir**
14. Dar clic en **Aceptar**
15. Dar clic en **Siguiente** en la ventana de **Componentes de Configuración**
16. Dar clic en **Finalizar** en la ventana de **Completo los Componentes de Windows**

[30] Este error puede sucede, cuando tu intentas exportar la Base de datos de DHCP desde un DC a un Servidor miembro del dominio

PARTE 3: Importar la base de datos de DHCP[31]

1. Copiar el archivo exportado de base de datos del DHCP al disco local del equipo con Windows 2003 Server
2. Verificar que el servicio de DHCP Server esta iniciado en el equipo
3. Abrir una ventana Ms-dos o ejecutar el comando ***cmd***
4. Escribir la siguiente sintaxis: **netsh dhcp server import *c:\dhcpdatabase.txt* all**, [***ENTER***], donde ***c:\dhcpdatabase.txt*** es el nombre de archivo y path completo del archivo de base de datos que fue copiado al Servidor
5. Esperar hasta que aparezca el siguiente mensaje: **"Command completed successfully"**
6. Cerrar la ventana Ms-dos

PARTE 4: Autorización del Servidor DHCP[32]

1. Dar clic en **Herramientas Administrativas**
2. Dar clic en ***DHCP***
3. Expandir el **nuevo servidor DHCP**, en la consola del servicio de DHCP (Si existe una flecha roja en la esquina derecha del objeto servidor, el servidor aun no ha sido autorizado)
4. Dar clic derecho sobre el objeto servidor
5. Dar clic en **Autorizar**
6. Dar clic derecho al servidor
7. Dar clic en **Refresh,**, (Una flecha verde indica que el Servidor DHCP esta autorizado)

A.16 Procedimiento para la migración de estaciones de trabajo

PARTE 1: Definir el dominio en los equipos y nos garantiza que el administrador del dominio destino tenga acceso al equipo.

1. Ejecutar el archivo ***SetWksDefaultDomain.exe***

[31] Debe de tener permisos de administrador local para importar los Datos
[32] Debe estar autenticado en el servidor con una cuenta que es miembro del grupo *"Enterprise Administrators"*.

2. Seleccionar ***Network browse list*** y presionar OK. y seleccionar los equipos a migrar
3. Escribir el nombre del dominio origen en la ventana de ***Enter the Old Default Logon Domain Value to be replaced***
4. Escribir el nombre del nuevo dominio destino en la ventana ***Enter the New Default Logon Domain Value***

PARTE 2: Realizar la actualización de equipos a migrar.

5. Dentro del Proyecto de Migración creado en el ***FastLane Migrator***, ejecutar el **Wizard de Actualización de Computadoras**
6. Dar clic en Siguiente en la ventana de **Bienvenida**
7. Seleccionar la opción **Seleccionar Computadoras** en la ventana de **Seleccionar Computadoras**
8. Buscar el dominio origen y seleccionar los equipos para la actualización
9. Dar clic en **Siguiente**
10. Seleccionar **Perfiles** en la ventana de Seleccionar **Opciones**
11. Dar clic en **Siguiente**
12. Seleccionar **Frecuencia Inmediata** en la ventana de **Escoge un tiempo para este trabajo**
13. Dar clic en **Siguiente**
14. Dar clic en **Finalizar**

PARTE 3: Realiza la migración de las computadoras utilizando el **Wizard de Migrator**.

15. Dar clic en **Siguiente** en la ventana de **Bienvenida**
16. Escribir el dominio origen y seleccionar el controlador de dominio en la ventana de **Localización de Origen**
17. Dar clic en **Siguiente**
18. Escribir el dominio destino y seleccionar el controlador de dominio primario en la ventana de **Localización de destino**
19. Dar clic en **Siguiente**
20. Seleccionar en el dominio Destino la OU donde se van migrar los equipos
21. Dar clic en **Aceptar**
22. Dar clic en **Siguiente** en la ventana de **OU Destino**

23. Dar clic en **Actualizar**
24. Seleccionar los equipos que deseas migrar en ese momento en la ventana de **Seleccionar Cuentas**
25. Dar clic en **Siguiente**
26. Seleccionar Borrar en el origen la cuenta de la computadora después de migrar, en la ventana de **Opciones Generales de Computo**
27. Dar clic en **Siguiente**
28. Dar clic en **Reiniciar** la computadora migrada y en Desplegar un mensaje antes del reinicio, definiendo el tiempo del proceso de reinicio de la computadora migrada en la ventana de **Opciones de Reinicio**
29. Dar clic en **Siguiente**
30. Dar clic en ***Edit MMT Mapping File***
31. Dar clic en **Guardar**
32. Dar clic en **Siguiente** en la ventana de ***Migration Mapping Technology***
33. Dar clic en **Finalizar**
34. Dar clic en **Si** en la ventana de **Configuración del Proyecto**
35. Escribir una cuenta de usuario con privilegios de administrador en el dominio origen en la ventana de ***Enter Network Password***
36. Dar clic en **Migrar ahora**

A.17 Procedimiento para el derecho de delegar el control

1. Dar clic en **Herramientas Administrativas**
2. Dar clic en **Directorio Activo de Usuarios y Computadoras**
3. Seleccionar la **OU de GRF** en el árbol del dominio
4. Dar clic derecho en la **OU de GRF**
5. Seleccionar **Delegar el Control**
6. Dar clic en **Siguiente**
7. Dar clic en **Agregar** en la ventana de **Usuarios y Grupos**
8. Seleccionar **el Usuario** al que se le debe otorgar los permisos
9. Dar clic en **Siguiente**
10. Seleccionar **Cambiar Contraseña, Leer toda la información de los usuarios, Crear y borrar grupos,**

modificar miembros de grupos y administrar ligas para GPO's en la ventana de **Tareas para Delegar**

11. Dar clic en **Siguiente**
12. Dar clic en **Finalizar**

A.18 Procedimiento para la consola administrativa

1. Escribir ***mmc.exe*** en la ventana de ejecutar
2. Dar clic en **Agregar/Remover Componente** en la Consola de Menú
3. Dar clic en **Agregar** en la ventana de **Agregar/Remover Componente**
4. Dar clic en **Directorio Activo de Usuarios y Computadoras** en la ventana de **Agregar Componentes Individuales**
5. Dar clic en **Agregar**
6. Dar clic en **Cerrar**
7. Dar clic en **Aceptar**
8. Expandir el árbol de **Directorio Activo de Usuarios y Computadoras**
9. Dar clic derecho en la **OU de GRF**
10. Dar clic en **Nueva Ventana desde Aquí**
11. Seleccionar **1 Consola de Raíz** en **Ventana de Menú**
12. Cerrar la Ventana de la **Consola de Raíz**
13. Dar clic derecho **Ver Nuevas Tareas (*Taskpad)***
14. Dar clic en Siguiente en la ventana de **Bienvenida**
15. Seleccionar **Pequeño** en el **Tamaño de Pantalla**
16. Dar clic en **Siguiente** en la ventana de **Exhibición de Tarea**
17. Seleccionar el **árbol** en la ventana de **Origen de *Taskpad***
18. Dar clic en **Siguiente**
19. Escribir **Administración de Usuario de la OU de GRF** en el **Nombre**
20. Dar clic en **Siguiente** en la ventana de **Nombre y Descripción**
21. Seleccionar **Herramienta para la Administración de Usuarios** en la caja de **Descripción**
22. Dar clic en Siguiente
23. Asegurar el **Iniciar la nueva tarea** en la ventana de **Completar el *Wizard***

24. Dar clic en **Finalizar**
25. Dar clic en **Bienvenida**
26. Seleccionar **Comando de Menú** en la ventana de **Tipo de Comando**
27. Dar clic en **Siguiente**
28. Seleccionar **Lista de Detalles** en **Comando de Destino**
29. Dar clic en **Deshabilitar la Cuenta** en **Comandos Disponibles**
30. Dar clic en **Siguiente** en **Comando de Menú de Acceso Directo**
31. Seleccionar **un icono** en la ventana de **Icono de *Taskpad***
32. Dar clic en **Siguiente**
33. Seleccionar **Ejecutar otra vez este *Wizard*** en la ventana de **Completar el *Wizard***
34. Dar clic en **Finalizar**
35. Repetir los pasos 28, 29, 30, 31, 32, 33 y 34; para **Agregar** las tareas de: **Borrar, Propiedades, Cambiar contraseña para usuario; Crear, borrar y Modificar grupos**
36. No seleccionar **Ejecutar otra vez este *Wizard*** en la ventana de **Completar el *Wizard***, después de completar las tareas del paso 35
37. Dar clic en **Finalizar**

APÉNDICE B
FIGURAS Y TABLAS

Figuras

CAPÍTULO 5

Tablas

No. Nombre pág

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

APÉNDICE C
FAST LANE MIGRATOR

Fast Lane Migrator es una solución adaptable para migraciones Microsoft Windows 2000 y Microsoft Exchange 2000. Con un manejador de proyecto e impresionantes características arregladas.

Esta aplicación, proporciona a los administradores herramientas sistemáticamente planeadas y migraciones ejecutables sincronizadas, disponibles en una vía o dos cuando son requeridas.

Certificada por Microsoft para Microsoft Windows 2000, *Fast Lane Migrator* es la opción para las empresas para facilitar sus migraciones.

- Proporciona una automatización completa de migración, sincronización y actualización de recursos y actividades claras.
- Proporciona las características de integración de Microsoft Active Directory y Microsoft Exchange 2000.
- Proporciona capacidad de administración para proyecto avanzado.
- Diseños de trabajo grandes, con redes distribuidas geográficamente, permitiendo migraciones múltiples.
- Proporciona migraciones robustas, actualizaciones de recursos y limpieza de características.
- Habilita una administración centralizada y una auditoria para migraciones Microsoft Windows NT, Microsoft Windows 2000 y Exchange 2000 y una administración en curso.
- Facilita la adquisición/fusiones y reorganizar negaciones por medio de Microsoft Exchange.

Fast Lane Migrator hace las migraciones más fáciles proporcionando una Guía interactiva de Migración. Permite a los administradores entender paso a paso e implementar los procesos de migración con un poco de tiempo de preparación. Cada paso es definido y todas las herramientas son explicadas y disponibles desde la Guía de Migración. Los Wizard facilitan a los administradores varias opciones de migración, reglas para aplicar y confirmaciones. Después sirve como información del proyecto con una disponibilidad de las situaciones migradas.

GLOSARIO

A

ACL Lista de Control de Acceso, son las listas que contienen a los objetos con sus descriptores de seguridad aplicados.

Administración Centralizada Es donde se pueden administrar los recursos desde una localización central.

Administración del Ambiente de Usuario Significa controlar a los usuarios que pueden hacer en el momento que se autentican en la red.

Árbol Es una agrupación jerárquica de uno o más dominios que comparten un espacio de nombres contiguo.

Atributo Son la descripción de los objetos. Cada atributo tiene su propia definición que sirve para describir el tipo de información que se puede especificar para el mismo.

Autenticación Es un proceso para acceder a la red donde el sistema válida la información del usuario cuando inicia sesión.

B

BIND *Berkeley Internet Name Domain*, es un DNS estándar.

Bosque Es una colección de uno o más árboles.

C

CA Entidad emisora de certificados, encargada de establecer y avalar la autenticidad de las claves públicas pertenecientes a los usuarios (entidades finales) u otras entidades emisoras de certificados.

Carpeta de Redirección	Es una opción de Políticas de Grupo que permite que direcciones las carpetas de los usuarios a un servidor.
Catálogo Global	Contiene una replica de cada objeto del Directorio Activo, pero con un número limitado de atributos, utilizados con mayor frecuencia en las operaciones de búsqueda.
Clase	Son definiciones para objetos fijos que comparten las mismas características o atributos.
Cliente	Es un programa que utiliza los servicios de otro programa, para contactar y obtener datos o servicios a partir del servidor.
Confianza Bidireccional	Tipo de relación de confianza en la que existe confianza mutua entre ambos dominios.
Confianza de Acceso Directo	Tipo de relación de confianza que es creada con un dominio en específico para agilizar las operaciones.
Confianza Explícita externas	Tipo de relación de confianza que es creada con dominios fuera del bosque.
Confianza Intransitiva	Está limitada por los dos dominios de la relación y no fluye a cualquier otro dominio del bosque.
Confianza Transitiva	Significa que la relación extendida a un dominio es automáticamente extendida para todos los demás dominios que confían en ese dominio.
Confianza Unidireccional	Tipo de relación de confianza en la que sólo uno de los dos dominios confía en el otro.
Contraseña	Es un código o una palabra que se utiliza para acceder a datos restringidos de un ordenador.

Correo Electrónico Se refiere a la dirección de correo de un ordenador a la cual se pueden enviar mensajes electrónicos.

Cuota de disco La máxima cantidad de espacio de disco disponible para un usuario.

D

DACL Listas de control de acceso discrecional que es el lugar donde están definidos los permisos sobre los recursos y los objetos.

DC Controlador de Dominio, es una computadora que tiene como plataforma Windows 2000 server donde almacena una replica del directorio.

DDNS DNS Dinámico que permite propagar automáticamente a todos los servidores DNS, cualquier cambio que se produzca en los nombres de equipos o direcciones IP guardadas en su base de datos.

Delegación del Control Administrativo La delegación es la habilidad para asignar la responsabilidad de la administración de los objetos del Directorio Activo a usuarios, grupos u organización.

DHCP *Dynamic Host Configuration Protocol*, es un sistema desarrollado para asignar direcciones IP a los clientes que lo soliciten.

Direccion IP Es un código numérico que identifica a un ordenador específico en Internet.

Directorio Activo Es una red de servicios de directorio en Windows 2000.

DN — *Distinguished Name* (nombre distinguido) que identifica en forma única al objeto. El DN incluye el nombre del dominio que contiene al objeto así como la ruta completa, a través de la jerarquía de contenedores, para llegar al objeto.

DNS — *Domain Name System*: "Sistema de Nombres de Dominio", Es usado para localizar nombres de dominio en Internet y en Redes Privadas TCP/IP. Proporciona un servicio de traducción de Nombres de dominio DNS a Direcciones IP y viceversa.

Dominio — Es un contenedor de objetos, definidos por un administrador, el cual comparte una base de datos común.

E

EFS — *Encrypting File System*, es un método para encriptar archivos y carpetas almacenados en computadores con plataforma Windows 2000.

Espacio de Nombres — *Namespace,* es una estructura de nombres jerárquicos en el cual los nombres en el espacio nombres pueden resolver a los objetos que ellos representan.

Esquema del Directorio Activo — Contiene las definiciones de todos los objetos del Directorio Activo.

Estación de Trabajo — Es una computadora conectada a la red, la cuál los usuarios interactúan con software almacenado en la red.

Extranet — Es una red que permite a una empresa compartir informaciones con otras empresas y clientes.

F

Forward lookup zones Se compone de zonas que tienen registros de nombres de computadoras y direcciones IP de dominios de otros Directorios Activos.

Forwarders Servidor que es contactado para responder a solicitudes de resolución de nombres de dominio, cuando el servidor autoritativo de la zona no puede resolver las peticiones recibidas por los clientes.

FQDN *Fully Qualified domain name*, un nombre de dominio DNS que indica la localización precisa en un espacio de nombres en un árbol.

FTP *File Transfer Protocol*, se utiliza para copiar y transferir archivos entre dos equipos en Internet.

G

Gateway Sistema de hardware o software que hace de puente entre dos aplicaciones o redes incompatibles para que los datos puedan ser transferidos entre distintos equipos.

Gopher Es una aplicación que permite organizar los ficheros en el Internet.

GPO's Políticas de grupo, es una tecnología que permite definir una configuración a usuarios y computadoras a nivel Sitio, Dominio o Unidad Organizacional.

Grupo Global Es el grupo donde se organiza objetos de usuarios de dominio a través de dominios.

Grupo Local Es el grupo donde se le concede permisos a los usuarios o grupos para acceder a los recursos de la red en un solo dominio.

Grupo Memberships Los grupos a los cuáles una cuenta de usuario pertenece.

Grupo Universal Es el grupo usado para agrupar grupos o usuarios para conceder permisos a través de un bosque.

Grupo Es una colección de usuarios y de otros grupos.

GUID Identificador Único Global.

H

Host Names Es el nombre del equipo conectado directamente a Internet.

Host Equipo conectado directamente a la red, donde se ejecuta un servicio o programa de servidor que utilizan clientes de red o remotos.

Hot Fix Es un paquete sencillo acumulativo compuesto por uno o más archivos utilizados para corregir un defecto en el producto.

HTTP Protocolo de transferencia de hipertexto, utilizado para trasferir información en el www.

I

Impresora Es un dispositivo que pone texto e imágenes en papel. La Impresora compartida, recibe datos de más de un equipo y la local es la conectada directamente a uno de los puertos de un equipo.

Intranet Es una red dentro de una organización que usa tecnología de Internet y protocolos, pero solamente está disponible para empleado de la compañía.

K

KDC — *Key Distribution Center*, servicio de red que suministra vales de sesión y claves temporales de sesión que se utilizan en el protocolo de autenticación *Kerberos V5.*

L

LDAP — *Lightweight Directory Access Protocol*, es un protocolo de servicio de directorio que es usado para buscar y actualizar los Servicios de Directorio.

Log off — Cierre de sesión, es cuando un usuario se desconecta de red.

Log on — Inicio de sesión, es cuando un usuario se conecta a la red proporcionar su nombre y contraseña que lo identifican.

M

Maestro de Emulador PDC — Es un controlador de dorninio que actúa como PDC de Windows NT para proporcionar servicio a clientes que no tienen instalado el software de cliente del Directorio Activo y replicar los cambios de directorio en los controladores (BDCs) de Windows NT dentro de un dominio de modo mixto.

Maestro de Identificadores Relativos — Controlador de dominio que se ocupa de la asignación de secuencias de identificadores relativos a cada controlador de dominio en su dominio.

Maestro de Infraestructura — Controlador de dominio al que se asigna la actualización de referencias de usuarios a grupos cada vez que cambian los miembros del grupo y la replicación de estos cambios en cualquier otro controlador del dominio.

Maestro de Nombre de Dominio Controlador de dominio al que se asigna el control de agregar o eliminar dominios en el bosque.

Maestro de Operaciones Controlador de dominio que tiene asignada una o varias funciones especiales en un dominio.

Maestro Esquema Controlador de dominio asignado para controlar todas las actualizaciones efectuadas al esquema en un bosque.

MMC *Microsoft Managamente Console.*

Modo Mixto Es la configuración predeterminada del modo de dominio en los controladores de dominio de Windows 2000, permite que los controladores en Windows NT y Windows 2000 coexistan en un dominio.

Modo Nativo Se habilita cuando todos los controladores de dominio se han actualizado en Windows 2000.

N

NTDS La capeta *NTDS* contiene el archivo ntds.dit donde se almacena todos los objetos del directorio activo.

O

Objeto Se le denomina, a la representación de los recursos de red, como: usuarios, grupos, computadoras, unidad organizacional e impresoras. Sin embargo todos los servidores, dominios y sitios en la red son también representados como objetos.

Opción Loopback Es una opción que permite a un administrador aplicar una configuración de Política de Grupo basada en la computadora que el usuario inicie sesión, después de la configuración de usuario ha sido procesada.

OU Unidad Organizacional, son un contenedor de objetos que se utiliza para organizarlos dentro de un dominio.

P

Partner Replication Es otro servidor con el cual se replica la base de datos de WINS.

PING Este comando nos indica el tiempo exacto que tardan los paquetes de datos en ir y volver a través de la red desde nuestro PC a un determinado servidor remoto.

Platillas Administrativas Son una colección de Políticas de Grupo que modifican la configuración del registro.

Proceso Loopback Es una configuración de GPO's que fuerza la configuración de usuario que aplica en la computadora y más tarde al objeto usuario para evitar conflictos.

Protocolo de Confianza Kerberos Es un mecanismo de autenticación utilizado para comprobar la identidad de usuarios o hosts.

Protocolo TCP/IP Proviene de dos de los protocolos: el Transmisión Control Protocol (TCP) y el *Internet Protocol* (IP). Diseñado para la comunicación de redes interconectadas formadas por equipos con distintas arquitecturas de hardware y sistema operativo.

Proxy Programa intermediario que actúa a la vez como servidor y cliente para realizar demandas de otros clientes.

R

RDN *Relative Distinguished Name* "Nombre Distinguido Relativo", es el nombre concreto del objeto sin tener en cuenta su ubicación en el árbol.

Replicación Multimaster Modelo de replicación en el que cualquier controlador de dominio acepta y replica los cambios de los directorios en cualquier otro controlador de dominio.

Replicación Es el proceso de actualización de información en el Directorio Activo desde un controlador a otro en una red.

RID *Relative Identifier*, parte de un identificador de seguridad (SID) que identifica de forma única una cuenta o grupo en un dominio.

RIS *Remote Installation Services*, es una componente opcional de Windows 2000 que remotamente instala Windows 2000 Profesional.

RPC *Remote Procedure Call*, es un protocolo estándar para cliente/servidor, es decir el proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Éste, al recibir la llamada, estudia los procedimientos del proceso llamado, obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta.

S

Servidor Es un equipo que proporciona equipo recursos compartidos a los usuarios de una red.

Servidor de Impresión Una computadora de aplicación específica que gestiona las impresoras y solicitudes de servicios de impresión; permite que múltiples usuarios compartan una impresora en red.

Servidor Miembro Pertenecen al dominio, tiene plataforma Windows 2000 server y se utilizan para almacenar los archivos y otros recursos de red.

SID Es un Identificador de Seguridad que es un nombre único donde identifica a un usuario cuando inicia sesión en una estación de Trabajo en Windows 2000 o NT. Puede representar a un usuario, grupo de usuarios o una computadora.

SIDHistory Son todos los identificadores que puede tener un objeto.

Single sing on Significa que el usuario necesitan autenticarse, es decir introducir su nombre y contraseña solamente una vez en una estación de trabajo para poder acceder a todos los recursos de la red donde este autorizado

Sistema de Archivos NTFS Sistema de archivos avanzado que proporciona características de rendimiento, seguridad, confiabilidad y avanzadas.

Sitio Una o varias subredes TCP/IP (de alta confiabilidad y rapidez) correctamente conectadas.

SMTP *Simple Mail Transfer Protocol,* es un protocolo de correo electrónico que especifica el formato exacto de los mensajes que un cliente debe enviar desde un computador al servidor de otro, pero no especifica cómo debe de almacenarse el correo ni con qué frecuencia se debe intentar el envío de los mensajes.

SRV Registros de Recursos de Servicios.

Subred Es una subdivisión de una Red IP. Cada subred tiene su propio identificador de red.

SYSVOL Directorio compartido que guarda la copia de servidor de los archivos públicos del dominio, que se replican en todos los controladores de dominio del dominio.

T

Taskpad Es una herramienta administrativa que tu puedes instalar para un subadministrador y usuarios quienes tienen responsabilidades asignadas que no se incluyen la administración de red.

Telnet Protocolo de emulación de Terminal muy utilizado en Internet para iniciar sesión en equipos de red. Una vez que se ha accedido a un sistema distante, se pueden realizar diferentes operaciones como si se estuviese directamente conectado al equipo.

Terminal Server Los servicios de Terminales es un entorno multisesión que proporciona acceso remoto a equipos que ejecutan programas basados en Windows (16 ó 32 bits) en un servidor.

TGS *Ticket Granting Services*, "Servicio de concesión de vales", es el servicio de *Kerberos V5* proporcionado por el Centro de distribución de claves (*KDC*) de *Kerberos V5* que emite vales de servicio que permiten a los usuarios autenticar los servicios de un dominio.

TGT *Ticket Granting Ticket* "Vale que concede vales", es una credencial emitida a un usuario por el Centro de distribución de claves (KDC) de Kerberos cuando el usuario inicia la sesión.

U

URL *Uniform Resource Locator*, es la dirección de un sitio o de una fuente, normalmente un directorio o un fichero, en el *World Wide Web* y la convención que utilizan los navegadores para encontrar ficheros y otros servicios distantes.

Usuario Persona que utiliza un equipo.

W

WINS *Windows Internet Name Service*, es un sistema desarrollado por Microsoft para convertir los nombres de los equipos *NetBios* en direcciones IP usadas en la red.

WWW *World Wide Web*.

Z

Zona Es un subárbol de la base de datos DNS que se administra como entidad separada, puede estar formada de un solo dominio o de un dominio con subdominios.

Zona Integrada del Directorio Activo Es la zona donde se actualizan los registros de DNS automáticamente en los DC de todo el Directorio Activo.

Zona Primaria Es una copia de la zona que es administrada localmente.

Zona Secundaria Es una copia de una zona DNS solamente de lectura que es transferida desde un DNS autoritativo a otro servidor DNS para proporcionar redundancia.

BIBLIOGRAFÍA

- Implementing and Administering Microsoft Windows 2000 Directory Services
- Designing a Microsoft Windows 2000 Directory Services Infrastructure.
- Windows 2000 server. Instalación, configuración y administración.
  José Luis Raya y Elena Raya
  Editorial Alfaomega Ra-Ma
  2001
- http://www.microsoft.com/windows2000/es/server/help
- http://www.microsoft.com/latam/technet/articulos/windows2k/mig ntw2k/du.aytolacoruna.es/noticias/diccionario/d.htm
- www.quest.com
- http://questsupportlink.quest.com/eSupport/SolutionFind.asp
- http://www.sc.ehu.es/jiwdocoj/mmis/externas.htm