UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA
INGENIERÍA EN COMPUTACIÓN

Migración de Directorio Activo Windows Server 2003 a Directorio Activo Servicios de Dominio Windows Server 2008 R2

INFORME DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

P R E S E N T A:

Diana Gabriela Paredes Cornejo

AVAL DE TESIS:
M.C. Alejandro Velázquez Mena

2014

Índice

Índice de Tablas vi

Introducción 1

1 Organigrama 2

2 Descripción de proyectos 4

3 Migración de Directorio Activo 5

3.1 ¿Por qué realizar una migración de Directorio Activo? 5

3.1.1 Escenario inicial de la Infraestructura del Cliente (planteamiento del Problema) 6

3.2 Análisis del escenario inicial de la infraestructura del cliente 7

3.2.1 Análisis inicial de la infraestructura 7

3.2.2 Análisis de las aplicaciones propias del negocio 8

3.2.3 Riesgos detectados en el escenario inicial 11

3.2.4 Alcance de la migración 12

3.2.5 Acciones esperadas a realizar durante el proyecto de migración 14

3.2.6 Análisis de beneficios 15

3.3 Desarrollo 17

3.3.1 Solución propuesta 17

3.3.2 Supuestos 19

3.3.3 Dependencias 19

3.3.4 Migración de Cuentas 20

4 Resultados 22

4.1 Diseño Lógico del Directorio Activo 22

4.2 Identificación de los participantes en el proyecto de implementación 23

4.2.1 Propietarios de datos y servicios 23

4.2.2 Administradores de Datos y Servicios 24

4.2.3 Propietario del Bosque 25

4.2.4 Propietario de DNS para AD DS 26

4.2.5 Propietario de las Unidad Organizacionales (OU) 27

4.3 Diseño del Bosque 27

4.3.6 Modelo de Bosque de Recursos 28

4.3.7 Definición del nombre del Bosque y del Dominio de Directorio Activo para el cliente 29

4.4 Creación del diseño de un Dominio 29

4.4.1 Modelo de Dominio Único 30

4.4.2 Definición del nombre de Dominio 30

4.4.3 Diseño de una Infraestructura DNS 31

4.5 Diseño de las Unidades Organizacionales (OUs) 31

4.5.1 Delegación de la Administración de OUs y contenedores predeterminados 33

4.5.2 Modelo de Estructura de OUs 35

4.5.3 Definición de Diseño 36

4.5.4 Perfiles de Computadoras 37

4.5.5 Perfiles de Usuarios 37

4.6 Topología de Sitios 38
4.6.1 Nomenclatura de Sitios 39
4.6.2 Definición de Diseño de Sitios y Subredes 40
4.6.3 Definición de Site Links 43
4.6.4 Definición de diseño de Site Links. 44
4.7 Definición de Diseño de la Distribución de Roles FSMO 46
4.8 Distribución de Controladores de Dominio y Localidades asignadas 46
4.9 Nomenclatura 48
4.9.1 Convención de nomenclatura para Usuarios de Dominio 48
4.9.2 Convención de nomenclatura de Usuarios con otras Funciones 51
4.9.3 Grupos de Distribución y Seguridad 52
4.10 Nivel Funcional 53
4.11 Diseño Físico del AD DS 58
4.11.1 Convención de Nomenclatura para Servidores 58
4.12 Hardware, Software y Configuración 61
4.13 Consideraciones de Virtualización para Directorio Activo 62
5 CONCLUSIONES 64
6 Glosario 65
7 REFERENCIAS 66

Índice de Tablas

Tabla 1 Descripción de mi participación profesional 4
Tabla 2 Aplicaciones de negocio del bosque1.mx 9
Tabla 3 DNSs de bosque1.mx 10
Tabla 4 Configuración de DNS presente en las aplicaciones de negocio. 10
Tabla 5 Tabla de Riesgos 11
Tabla 6 Modelos para el Diseño de OUs 33
Tabla 7 Clasificación de las OUs por nivel para el cliente. 36
Tabla 8 Sitios del cliente 39
Tabla 9 Servidores para cada site 40
Tabla 10 Servidores para cada site 43
Tabla 11 Configuración de los Site Links 44
Tabla 12 Distribución de los sites por Site link. 45
Tabla 13 Ubicación de los roles FSMO 46
Tabla 14 Ejemplo de nomenclatura para usuario 50
Tabla 15 Iniciales distintivas 51
Tabla 16 Convención de nomenclatura 51
Tabla 17 Nomenclatura para grupos de distribución 52
Tabla 18 Nomenclatura para grupos de administración 53
Tabla 19 Características de cada nivel funcional de dominio. 54
Tabla 20 Características de cada nivel funcional de bosque. 56
Tabla 21 Prefijo servidor 58
Tabla 22 Prefijo rol 59
Tabla 23 Identificador oficinas 59
Tabla 24 Número consecutivo 60
Tabla 25 Servidores en Oficinas Centrales 60

Tabla 26 Servidores Foráneos.....60

Tabla 27 Características de Hardware de los servidores para oficinas centrales 61

Tabla 28 Características de Hardware de los servidores para oficinas foráneas.....62

Tabla 29 Características de las máquinas virtuales para los controladores de dominio. 62

Introducción

El siguiente informe presenta conceptos técnicos y no está dirigido a un público en general, por lo que se espera que el lector esté familiarizado con conceptos de infraestructura, redes, servidores en general y sistemas operativos Windows Server 2003 y Windows Server 2008 R2.

Este informe contiene las actividades realizadas por un profesionista recién egresado de la carrera de Ingeniería de Computación en el ámbito profesional, laborando en la empresa Microsoft y ejecutando proyectos en instituciones cuya identidad no será revelada por motivos de confidencialidad de las mismas. En lo subsecuente se referirá indistintamente a esta institución como *Cliente*.

Las imágenes presentadas con las configuraciones recomendadas harán referencia siempre a los sistemas operativos Windows Server 2003 y/o a Windows Server 2008 R2.

Como fines prácticos de este informe sólo serán incluidas las imágenes de las configuraciones más relevantes.

El objetivo de lo aquí presentado es mostrar la actualización de la tecnología de *Microsoft, Directorio Activo* del *Cliente* para optimizar su infraestructura y que puedan hacer uso de nuevas características propias del sistema operativo e implementar nuevas tecnologías relacionadas con los servicios que ofrece el *Directorio Activo Servicios de Dominio*.

1 Organigrama

La estructura organizacional de la empresa está distribuida por diferentes departamentos, áreas, regiones y países.

Imagen 1 Estructura organizacional del área de servicios de Microsoft.

Como se puede observar en la imagen 1, mi puesto es de Consultor Asociado (Associate Consultant) del área de servicios de la subsidiaria de México.

Pertenezco al equipo de CORE I/O, (Core Infrastructure Optimization), donde nuestro objetivo es ayudar a las organizaciones a optimizar y mejorar sus infraestructuras en temas de seguridad, administración y operación; basándonos en los modelos de optimización que incluyen capacidades técnicas específicas que proporcionan un amplio conjunto de soluciones.

El modelo de optimización de infraestructura define cuatro capacidades que son necesarias para construir una infraestructura de TI más ágil:

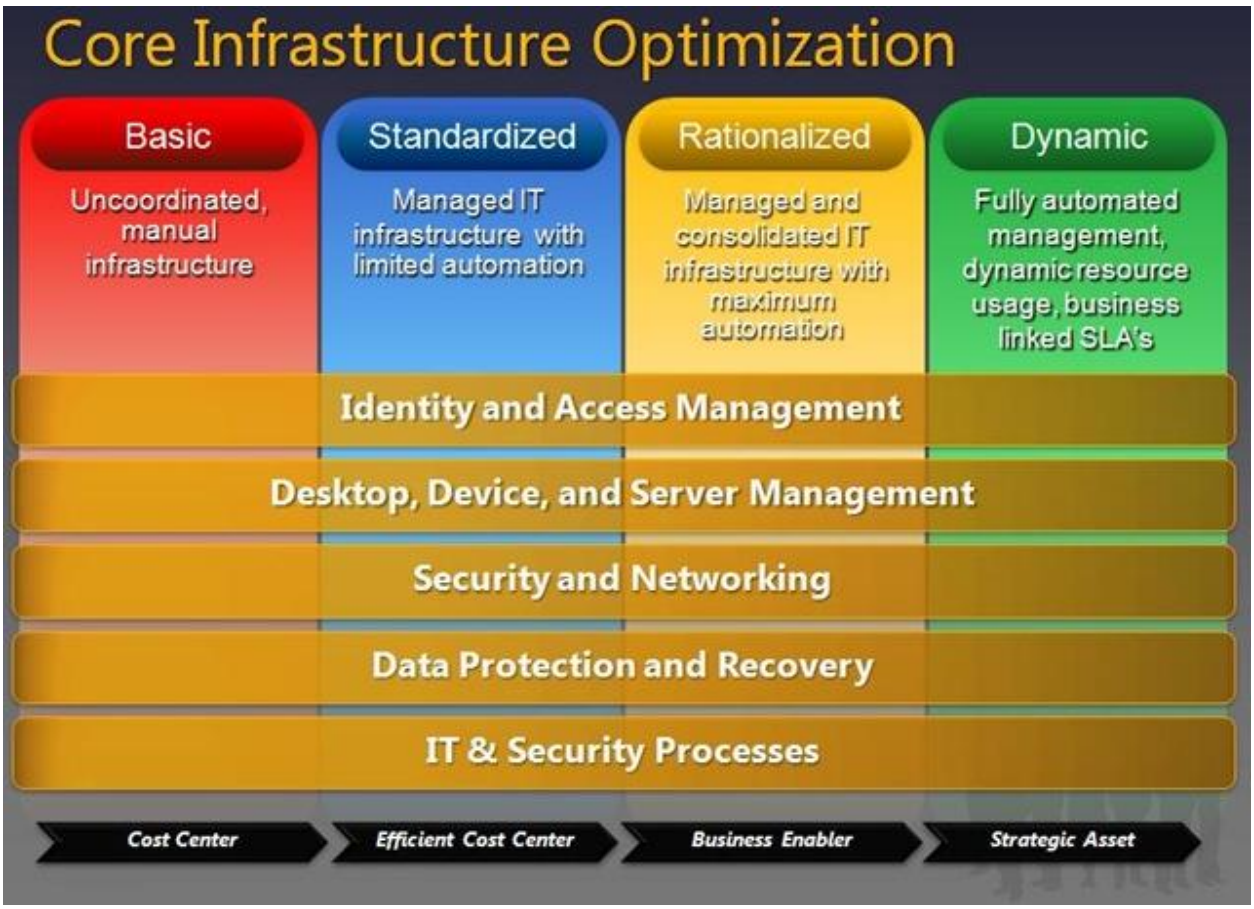


Imagen 2. Modelo de optimización para Infraestructuras de TI

2 Descripción de proyectos

El presente trabajo lo redacté en base a mis actividades desempeñadas como consultora de Microsoft.

Microsoft no es mi primer empleo, anteriormente estuve laborando en otras compañías de consultoría donde mi participación fue en los siguientes proyectos:

Tabla 1 Descripción de mi participación profesional

Actividades	Empresa	Rol
Desarrollo de servicios interbancarios en ANSI C	BCM Bufete Consultor Mexicano S.A. de C.V.	Consultor junior
Desarrollo de aplicaciones en C# para varios clientes.	Saitosoft	Programador junior
Implementación de la herramienta Project server para Saitosoft	Saitosoft	Programador junior
Creación de Base de datos para digitalizar expedientes del colegio	Colegio Mexicano de Terapeutas Profesionales en Masaje y Enfermería Holística A.C.	Coordinador técnico de logística del colegio

No puedo realizar una descripción más detallada de los proyectos en los que participé en BCM y Saitosoft por seguridad de la información de los clientes y por las cláusulas de confidencialidad que firmé al momento de integrarme a los mismos.

Mi participación profesional siempre ha sido enfocada a la consultoría, primero en desarrollo y actualmente en infraestructura. Siempre con la finalidad de planear, diseñar e implementar la mejor solución a las necesidades del cliente.

3 Migración de Directorio Activo

3.1 ¿Por qué realizar una migración de Directorio Activo?

Una migración de Directorio Activo (En adelante AD), de Windows Server 2003 a Directorio Activo Servicios de Dominio (En adelante AD DS) Windows Server 2008 R2, permite utilizar las nuevas características y servicios que ofrece una de las últimas versiones del sistema operativo de Windows para servidores.

Una migración de AD es necesaria para poder implementar nuevas tecnologías dentro de una empresa, que con versiones anteriores como 2003 no podría ser posible.

Una migración permite mantener a la vanguardia a la empresa, ya que utiliza los servicios de última tecnología necesarios para optimizar el rendimiento de su empresa y les permite utilizar aplicaciones y tecnologías de última generación que sólo son compatibles con las últimas versiones de sistema operativo Windows Server.

Una migración optimiza el número de servidores utilizados para el AD, el rendimiento y eficacia del directorio activo.

Actualmente hay instituciones, organizaciones y empresas que presentan los siguientes escenarios, no deseables, dentro de la infraestructura de su Directorio Activo:

- El Sistema Operativo es una versión muy antigua y/o no está actualizado
- No cuentan con un diseño para su Directorio Activo.
- Los objetos que componen su Directorio Activo carecen de una administración adecuada a sus necesidades.

- Desconocen las características que los servicios del Directorio Activo puede ofrecerles.
- Tienen una configuración que no está basada en las mejores prácticas de Microsoft.

En estos escenarios mencionados, la migración suele tener un nivel de dificultad mayor que en clientes que cuentan con una infraestructura sana y bien administrada por lo que su migración es sencilla y con bajo nivel de riesgo.

3.1.1 *Escenario inicial de la Infraestructura del Cliente (planteamiento del Problema)*

Con base en la información que me proporcionó el cliente, fue de mi entendimiento que necesitaba migrar e implementar **Directorio Activo Servicios de Dominio (AD DS) en Windows Server 2008 R2**, para efectos de mantener actualizada su infraestructura y aprovechar los beneficios que se incluyen en esta versión del sistema operativo para servidores. Manteniendo una base renovada, estable y actualizada para soportar futuras soluciones dependientes de esta herramienta de Microsoft.

Otra necesidad expresada por el cliente fue llevar a cabo un Re-diseño de la Estructura inicial de su Directorio Activo para implementar en la nueva versión del sistema operativo.

También fue de mi conocimiento el escenario inicial que presentaba la infraestructura de sus bosques **bosque1.mx y bosque2.local** y de que existían bosques y dominios en otras oficinas del Cliente totalmente independientes de los bosques principales, los cuales quedaron fuera de toda actividad a realizar en la migración

3.2 Análisis del escenario inicial de la infraestructura del cliente.

3.2.1 *Análisis inicial de la infraestructura*

Las oficinas del cliente están distribuidas de la siguiente manera: 1 por cada estado y 2 en el distrito federal, dando un total de 34 sedes. A las oficinas de cada estado las llaman ***foráneas*** y a las del Distrito Federal ***Oficinas Centrales***.

Algunas de sus oficinas foráneas, cuentan con una infraestructura de Directorio Activo propias e independientes, es decir con bosques y dominios propios, sin relación de confianza con los bosques que se encuentran en las oficinas centrales.

También había oficinas foráneas que no estaban unidas a ningún bosque ni dominio.

En este proyecto busqué la consolidación de los bosques de las oficinas centrales bosque1.mx y de bosque2.local en uno solo, basado en tecnología Windows Server 2008 R2.

A continuación muestro el detalle de esta infraestructura:

- **Bosque1.mx** tenía una infraestructura basada en Microsoft Windows Server 2003, con un solo dominio bosque1.mx. ; presentaba las siguientes características:
    - Infraestructura de Directorio Activo basada en servidores virtuales Microsoft Windows Server 2003 SP2.
    - Infraestructura física distribuida en un sitio central y 16 sitios remotos.
    - Administración centralizada.
    - Contaba con 16 Controladores de Dominio, 14 con Windows Server 2003 SP2 y 2 con Windows Server 2003 sin SP2.
    - 4 de los Controladores de Dominio eran Catálogo Global.

- Los 16 Controladores de Dominio eran DNS.
- El controlador de Dominio SRVA0B tiene todos los roles FSMO tanto de dominio como de bosque.

- La infraestructura de Directorio Activo del bosque **bosque2.local** estaba montada en Windows Server 2008 R2, tenía un solo dominio bosque2.local y presentaba las siguientes características:
  - Infraestructura de Directorio Activo basada en servidores virtuales Microsoft Windows Server 2008 R2
  - 1 Controlador de Dominio
  - 1 sitio
  - El Controlador de dominio es DNS

Los controladores de dominio en Windows Server 2003 fueron virtualizados, acción que no se recomienda, porque se pierde la integridad de la información de las bases de datos, así como la sincronización de los controladores de dominio. Para implementar el directorio Activo en máquinas virtuales se recomienda trabajar con una máquina virtual limpia con el sistema operativo a utilizar y después instalar el directorio activo unirlo al dominio para que sea un controlador de dominio réplica y después dar de baja los controladores de dominio físicos. Desafortunadamente esto no fue realizado por el cliente por ello presentan problemas al logearse, que desaparezcan cuentas de usuarios y cuentas de mail.

3.2.2 *Análisis de las aplicaciones propias del negocio*

Para conocer qué aplicaciones de negocio consumían servicios del Directorio Activo se aplicó un cuestionario al personal del cliente encargado de administrarlas.

A continuación muestro los resultados obtenidos:

- **bosque1.mx**

El cliente cuenta con 10 aplicaciones de negocio en este dominio, todas con dependencia directa al Directorio Activo ya que consumen los servicios de autenticación y LDAP.

La siguiente tabla resume la información de las aplicaciones:

Tabla 2 Aplicaciones de negocio del bosque1.mx

Nombre de la Aplicación	Sistema Operativo	Nombre del Servidor	IP del servidor donde se encuentra la aplicación	DNS
Exchange	Windows Server 2003 SP2	SRVCORREO01	10.36.10.110	10.36.0.199 10.36.0.122
FTP: ESTADOS	Windows Server 2003 Enterprise Edition SP2	Srvestados	10.36.0.104	10.36.0.199 10.36.0.122
Sistema KARDEX (Historial del Trabajador)	Windows Server 2003 Enterprise Edition SP2	srvproduccion	10.36.0.12	10.36.0.199 10.36.0.122
Citrix para publicar Archivo Digital	Windows Server 2003 Enterprise Edition SP1 Windows Server 2003 Enterprise Edition SP2 Windows Server 2003 Enterprise Edition SP2	AGASRVOC-HV01 agaw2k3-citrix1 w2k3-citrix2	192.168.2.33 192.168.2.35 192.168.2.32	no lo indica
Citrix para Map 3D	Windows Server 2003 Enterprise Edition SP1 Windows Server 2003 Enterprise Edition SP2	srv-citrix-map ctx1-map3d	10.36.0.118 10.36.0.146	no lo indica
Citrix servidor de licencias, citrix para map 3d	Windows Server 2003 Enterprise Edition SP2	srvcitrix01	10.36.10.10	10.36.0.199 10.36.0.122
Servidor de BES de Blackberry	Windows Server 2003 Enterprise Edition SP2	srvbesbb	10.36.0.119	10.36.0.199 10.36.0.122
ContPAQ 2005	Windows Server 2003 Enterprise Edition SP2	srvproduccion	10.36.0.12	10.36.0.199 10.36.0.122

ContPAQ i	Windows Server 2003 Enterprise Edition SP2	srvproduccion	10.36.0.12	10.36.0.199 10.36.0.122
ftp de srvproduccion	Windows Server 2003 Enterprise Edition SP2	srvproduccion	10.36.0.12	10.36.0.199 10.36.0.122

Todas las aplicaciones en este dominio utilizaban la misma configuración en sus DNSs:

Tabla 3 DNSs de bosque1.mx

DNS	
Primario	10.36.0.199
Secundario	10.36.0.122

Estos DNS correspondían a los siguientes controladores de dominio:

Tabla 4 Configuración de DNS presente en las aplicaciones de negocio.

NOMBRE	IP	S.O.	UBICACIÓN (SITE)
SRVAD0A	10.36.0.122	Windows Server 2003	OficinasDF
SRVAD0B	10.36.0.199	Windows Server 2003	OficinasDF

- **bosque2.local**

En este dominio no se encontraron aplicaciones con relación directa a su Directorio Activo.

3.2.3 *Riesgos detectados en el escenario inicial*

El análisis realizado a la infraestructura inicial del cliente y a sus aplicaciones de negocio arrojó los siguientes riesgos:

Tabla 5 Tabla de Riesgos

Id	Condition	Consequence	Responsible	Impact Low: 1-3 Medium: 4-6 High: 7-10
1	Problemas de replicación entre los Controladores de Dominio	Se está trabajando con información no homologada. Los cambios efectuados en los Controladores de Dominio como altas, bajas o cambios de cuentas de usuario no se ven reflejados en todos los Controladores de Dominio.	Cliente	7
2	Los roles FSMO están instalados en un solo controlador de dominio.	Se presentan comportamientos desconocidos con afectaciones directas al dominio y al bosque.	Cliente	7
3	Re-diseño de la infraestructura para bosque2.local no adaptado a las necesidades administrativas del cliente	Una migración y administración compleja en la infraestructura del Directorio Activo	Microsoft y cliente	2
4	No contemplar todas las incidencias y riesgos que se presenten en los Health Check de los bosques bosque1.mx y bosque2.local	Tener incidencias de alto riesgo no contempladas	Microsoft	1
5	Remediación tardía en los hallazgos encontrados en los Health check de los bosques bosque1.mx y bosque2.local	Detener el proyecto por no contar con una infraestructura con los requerimientos técnicos necesarios.	cliente	5
6	No contar con el sistema operativo Windows Server 2008 R2 instalado en los servidores que serán utilizados como los nuevos	No poder continuar con la etapa de construcción de este proyecto	cliente	3

	controladores de dominio en cada sitio.			
7	Que los recursos de Microsoft responsables de las actividades a ejecutar las realicen fuera de las instalaciones del cliente.	El personal del cliente no se involucre y no adquiera el expertise de las actividades a realizar en el proyecto.	Microsoft	5
8	Cambios en la arquitectura después de su aceptación.	Re-trabajo de definición de arquitectura, retrasos en la fecha de finalización de proyecto.	Microsoft y cliente	8
9	Enlace de red no suficiente para la replicación suscitada después de instalar los 33 Controladores de Dominio	La replicación no tendría efecto en todos los Controladores de Dominio, por lo que la información no estaría homologada.	cliente	6
10	Poca Colaboración e Involucramiento de la áreas de cliente para el Proyecto de Directorio Activo	Retrasos en las definiciones de diseño e implementación por tanto se generarían retrasos en la fecha de finalización del proyecto	Cliente	6
11	Cambios no dados a conocer en la infraestructura del Directorio Activo durante el proyecto.	La planeación y el re-diseño para la infraestructura del Directorio Activo no tendrá contemplados estos cambios y los tiempos en las últimas etapas del proyecto se pueden ver afectadas.	Cliente	7

3.2.4 *Alcance de la migración*

El proyecto de Directorio Activo, tenía como finalidad brindar las bondades operativas de los servicios del Directorio Activo, para optimizar la productividad del personal que lo conforma a través del uso de tecnologías de información y de servicios que fueron consolidadas bajo un ambiente confiable, controlado y seguro.

El propósito principal de este proyecto fue brindar al cliente un ambiente de coexistencia entre sus bosques bosque1.mx y bosque2.local, mediante una relación de confianza entre bosques, así como un re-diseño de los objetos pertenecientes al Directorio Activo del bosque bosque2.local de acuerdo a sus necesidades administrativas y operacionales del cliente.

El diseño que se aplicó al bosque bosque1.local estuvo basado en la versión de Microsoft del sistema operativo Windows Server y Servicios de Dominio de Directorio Activo (Windows Server 2008 R2). La combinación de requisitos actualizados, las nuevas características de las versiones más recientes y la experiencia en la industria de Microsoft serán claves para desarrollar una arquitectura empresarial que reducirá significativamente la complejidad actual de la infraestructura de servicios del Directorio Activo y su carga administrativa. Esto también permitió la introducción de otros servicios nuevos que en un futuro el cliente podrá hacer uso, como Acceso Directo (Direct Access), Políticas de Contraseñas Granulares (Fine-Grained Password Policies), monitoreo de Directorio Activo, entre otras.

El alcance de Microsoft fue crear una sola imagen con el sistema operativo Windows Server 2008 R2 para los nuevos Controladores de Dominio, crear un nuevo bosque **bosque3.lan** aplicando las mejores prácticas de Microsoft, crear una relación de confianza entre los bosques bosque1.mx y bosque3.lan, migrar 1200 cuentas del bosque bosque1.mx al bosque3.lan, crear 5 políticas de Grupo y crear un re-diseño en la estructura del directorio activo del cliente. Así como transferir los conocimientos al personal indicado del cliente.

3.2.5 *Acciones esperadas a realizar durante el proyecto de migración*

A continuación puntualizo las actividades que se propusieron al cliente para realizar en el proyecto:

- Análisis básico de de Health Check AD para el Bosque “bosque1.mx” y el bosque “bosque2.local”.
- Análisis inicial y supuestos para Consolidación Inter-Forest.
- Planeación de la Estructura del Bosque Windows Server 2008 R2.
- Diseño de Solución para virtualizar los controladores de dominio de bosque3.lan con System Center Virtual Machine Manager.
- Diseño de estructuras básicas de OUs (Unidades Organizacionales) para el Nuevo Bosque.
- Diseño de 5 Políticas de Grupo de Dominio con finalidad específica para el Bosque (bosque3.lan)
- Planeación de Consolidación de bosques
- Planeación de estrategia de migración de objetos del Directorio Activo Inter-Forest.
- Preparación y adecuaciones del primer controlador de dominio para migrar el servidor existente.
- Instalación de la consola de administración de Virtual Machine Manager, 2 Perfiles de HW y 2 perfiles de Software (SW).
- Instalación y configuración del primer Controlador de Dominio.
- Instalación y configuración del 2º Controlador de Dominio, configuración de Forest y Dominio Win2k8R2 y migración de roles de Directorio Activo FSMO (Flexible Single Master Operation).
- Instalación remota de 33 Servidores físicos con Windows 2008 R2 y rol de Hyper V (virtualización) así como la instalación y configuración remota de 1 servidor virtual por oficinas del cliente, para hacer un controlador de dominio en cada una de dichas sedes.
- Transferencia de conocimientos para la instalación de servidores virtuales.

- Creación de estructura Lógica del Nuevo Bosque (Sites, OUs, replicación)
- Revisión de Replicación Intra- Forest en Dominio Nuevo.
- Instalación de ADMT (Active Directory Migration Tool) para la migración objetos de Directorio Activo entre bosques, y creación de relaciones de confianza inter-forest.
- Definición de Ambiente de Pruebas para Piloto controlado de Migración Inter-Forest
- Elaboración de Matriz de Pruebas de Piloto de Migración
- Elaboración de Guía de Instalación y Configuración.
- Piloto de Migración Controlado para Bosques de bosque1.mx y bosque2.local (5 Cuentas de usuario y computadora)
- Identificación y resolución de incidentes de Migración
- Estabilización y ajustes al proceso de migración de acuerdo a resultados de piloto de migración controlado
- Workshop de transferencia de conocimiento (Creación de GPOs, replicación, operación básica).
- Entrega de infraestructura del Directorio Activo del bosque "bosque3.local" a la operación de cliente.

3.2.6 *Análisis de beneficios*

Los beneficios que se le presentaron al cliente al inicio de este proyecto y que ayudaron a sustentar la visión del mismo, se establecieron de la siguiente manera:

- **Reducir la complejidad de operación** - Al actualizar el Directorio Activo a través de una migración a la versión de Windows Server 2008 R2, se tendrán las nuevas características en la parte de operación que este sistema operativo ofrece. Y al realizar un re-diseño de los componentes del Directorio Activo (Unidades Organizacionales, usuarios, grupos y Políticas de Grupo) de acuerdo a las mejores prácticas de Microsoft, ayudará a los administradores del Directorio Activo a realizar las tareas administrativas con más facilidad.

- **Seguridad** - Implementando las políticas de grupo necesarias de una forma eficaz en el nuevo re-diseño de la estructura de su Directorio Activo aumentará la seguridad general en el dominio.
- **Capacidad de soporte** - El soporte para Windows Server 2003 terminó en julio de 2010 y su soporte extendido acabará en julio de 2015. Actualizando el entorno del Directorio Activo del cliente a Windows Server 2008 R2, se ampliará el apoyo de esta plataforma para los próximos años.
- **Habilitación de nuevos servicios** - Directorio Activo es la base de la mayoría de las tecnologías de Microsoft y depende de un entorno de infraestructura saludable. La Actualización de la infraestructura base permite la introducción de nuevas funciones del Directorio Activo.
- **Virtualización**. La implementación de Virtual Machine Manager 2012 permitirá la administración centralizada de la infraestructura virtual, una mayor utilización de los servidores y la optimización dinámica de recursos.

3.3 Desarrollo

3.3.1 *Solución propuesta*

El escenario inicial de la infraestructura del cliente presentaba dos bosques bosque1.mx y bosque2.local en tecnologías Windows Server 2003 y Windows server 2008 R2, respectivamente.

La propuesta que presenté al cliente la dividí en dos procesos:

1. Crear un tercer bosque implementando las mejores prácticas de Microsoft, **bosque3.lan**

2. Establecer una relación de confianza con el bosque1.mx que es el que tenía la base de objetos del Directorio activo más confiable y migrar dichos objetos al nuevo bosque. con sus respectivos supuestos y dependencias en base al análisis que se realizó y a las implicaciones de cada proceso.

   Nota: La relación de confianza con el bosque2.lan quedó fuera de este proyecto, ya que a pesar de que era de reciente implementación, encontré configuraciones no confiables que hubieran afectado el funcionamiento del nuevo bosque.

Las siguientes imágenes muestran con qué bosques se realizó la relación de confianza:

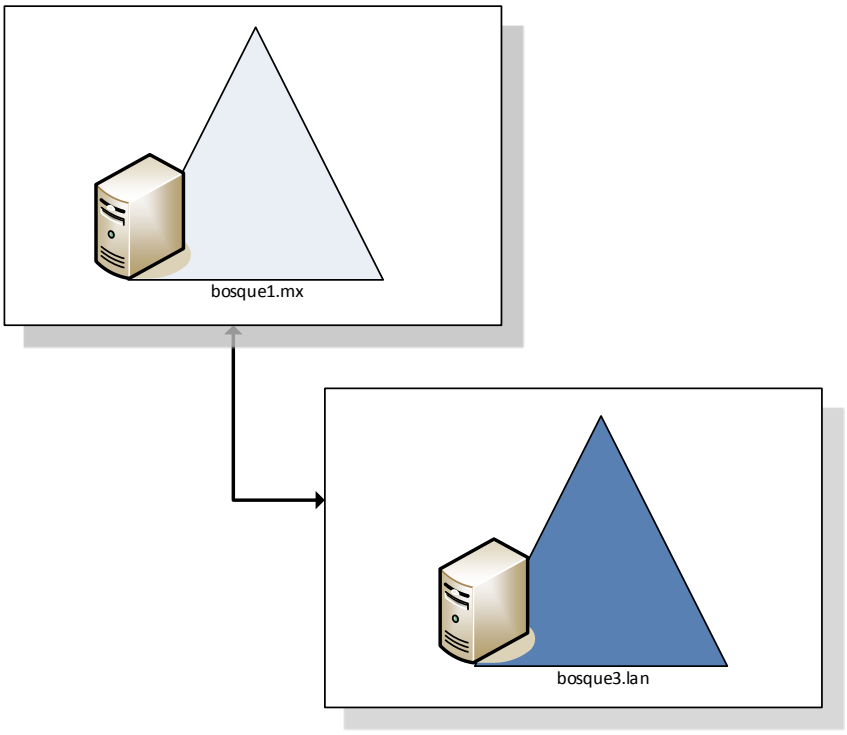


Imagen 3. Relación de confianza realizada en el proyecto.

3.3.2 *Supuestos*

Se establecieron algunos supuestos para garantizar una relación de confianza exitosa, se los presenté al cliente para concientizarlo al respecto y hacerle saber que sin estos no hubiera sido posible la relación:

- Funcionamiento óptimo del bosque1.mx .
- Replicación sin problemas entre los controladores de dominio del bosque bosque1.mx
- Contar con un medio físico que conecte a las dos infraestructuras: bosque3.lan y bosque1.mx
- La hora en los dominios bosque1.mx y bosque3.lan estarán sincronizados para que no falle la autenticación Kerberos

3.3.3 *Dependencias*

El proceso para realizar la relación de confianza entre los bosques presentaba las siguientes dependencias:

- Tener asignado un usuario Domain Admin de cada bosque, (bosque1.mx y bosque3.lan)
- El Nivel de funcionalidad en ambos bosques será: Windows Server 2003.
- Funcionamiento y configuración correctos en la resolución de nombres.
- El Domain Admin de bosque3.lan formará parte del grupo de *Administradores de dominio* de bosque1.mx
- El Domain Admin de bosque1.mx formará parte del grupo de *Administradores de dominio* de bosque3.lan

3.3.4 *Migración de Cuentas*

Para realizar la migración de cuentas entre los bosques bosque1.mx y bosque3.lan, se utilizó la Herramienta de Migración de Directorio Activo 3.1 **(ADMT).** Esta herramienta permite que los usuarios migrados puedan mantener el acceso a los recursos de red durante el proceso de migración y su ID original de cuando se creó el objeto.

A continuación se presentan los supuestos y dependencias de esta herramienta.

3.3.4.1 Supuestos de ADMT

Para realizar exitosamente la migración de cuentas con la herramienta ADMT, fue necesario tener en cuenta los siguientes supuestos:

- Que la relación de confianza entre los bosques bosque3.lan y bosque1.mx estuviera establecida.
- Que estuviera deshabilitado el filtrado de SIDs en el dominio bosque1.mx
- Que estuviera creado un archivo con una clave de encriptación en el controlador de dominio donde esté instalado AMDT.
- Que estuviera copiada la carpeta que contiene el archivo para ejecutar PES en un controlador de dominio donde esté instalado ADMT.
- La migración se llevó a cabo en conjuntos de 100 cuentas, esto permitió que el proceso de migración se pudiera gestionar.
- Los usuarios estuvieron enterados de la fecha en la que sus equipos serían migrados para tener conectado su equipo a la red.
- Los usuarios estuvieron al pendiente del momento en el que su equipo fue unido al Nuevo dominio, para verificar que el reinicio automático se llevará a cabo.
- Se contaba con un plan para “revertir la migración de cuentas”

- Se revisaron las instrucciones de preinstalación de la herramienta de Migración de Directorio Activo (ADMT).

3.3.4.2 Siguientes Dependencias

El proceso de migración de cuentas con la herramienta ADMT presenta las siguientes dependencias, si no se contaba con todas no hubiera sido posible la migración:

- Configurar la siguiente clave del registro en los controladores de dominio de bosque3.lan:

  Ruta de Registro: **HKLM\System\CurrentControlSet\Services\Netlogon\Parameters**

  Valor del Registro: **AllowNT4Crypto**

  Tipo: **REG_DWORD**

  Datos: **1**

- Tener instalada la herramienta de ADMT en un controlador de dominio de bosque3.lan.
- Instalar el servicio de exportación de contraseñas (PES) en un controlador de dominio de bosque1.mx
- La persona que ejecute el servicio de contraseñas (PES) debe de ser administrador del Dominio.
- Iniciar sesión en el dominio bosque3.lan con la cuenta de administrador de bosque1.mx cuando se vaya a realizar la migración de cuentas.
- Convertir la seguridad en modo “agregar”, en servidores para agregar los SID de las cuentas de usuario y grupo en el dominio de bosque3.lan.
- Realizar la conversión de seguridad en los servidores miembro después de que se finalice la migración.

4 Resultados

Como resultado del análisis y de la solución propuesta al cliente surgieron los siguientes diseños que se implementaron exitosamente en la nueva infraestructura del cliente.

4.1 Diseño Lógico del Directorio Activo

Servicios de Dominio de Directorio Activo (AD DS), es una base de datos distribuida que almacena y administra información acerca de los recursos de red así como datos específicos de las aplicaciones con directorio habilitado. AD DS permite a los administradores organizar los elementos de una red en una estructura de contención jerárquica. El contenedor de nivel superior es el bosque. Dentro de los bosques están los dominios y dentro de los dominios, las unidades organizacionales (OU). Se trata de un modelo lógico porque es independiente de los aspectos físicos de la implementación, como el número de controladores de dominio necesarios en cada dominio y topología de red.

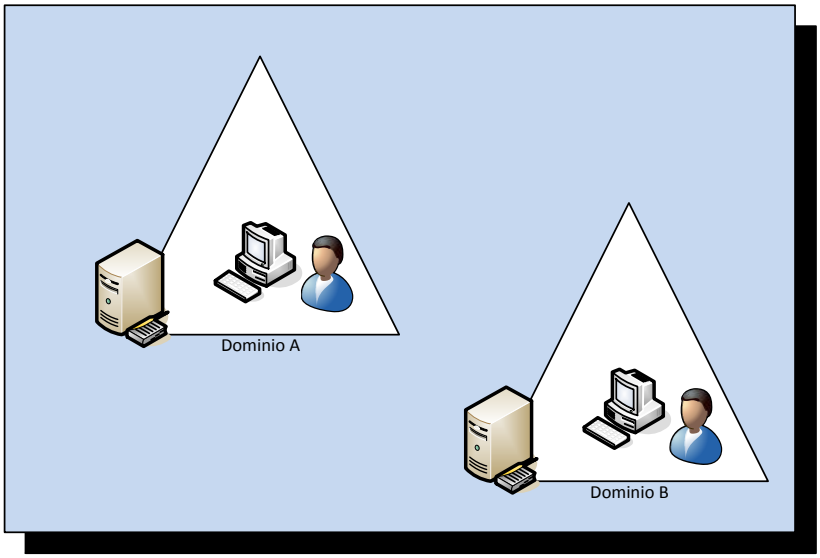


Imagen 5. Bosque contenedor de Dominios, que a su vez contienen objetos

Para el diseño lógico del Directorio Activo es necesario definir los siguientes puntos:

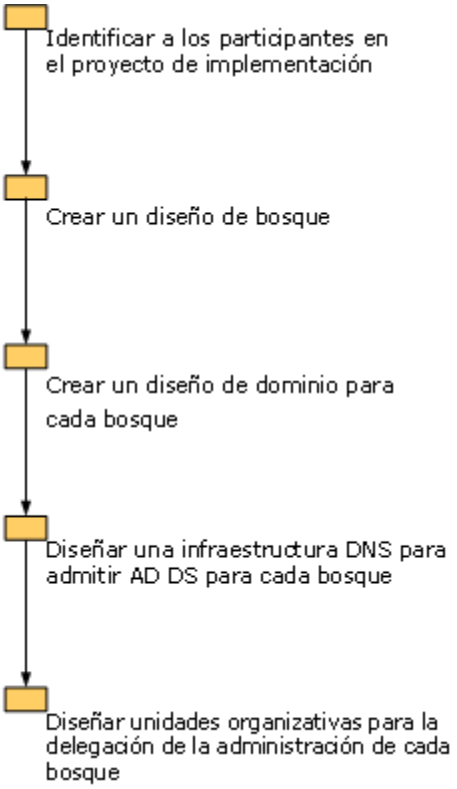


Imagen 6. Pasos para realizar el diseño lógico del AD DS.

4.2 Identificación de los participantes en el proyecto de implementación

Antes de realizar el diseño y la implementación del mismo, fue importante definir a los administradores, que son las personas responsables de realizar las tareas de implementación. Los administradores tienen los permisos y el acceso de red, necesarios para manipular el Directorio Activo y su infraestructura.

4.2.1 *Propietarios de datos y servicios*

En la administración diaria de AD DS intervienen dos tipos de propietarios:

- **Propietarios de servicios**, que son responsables de la planificación y el mantenimiento a largo plazo de la infraestructura de Directorio Activo y de garantizar que el directorio continúa funcionando y de que se mantienen los objetivos establecidos en los acuerdos de nivel de servicios.

- **Los propietarios de datos**, que son responsables del mantenimiento de la información almacenada en el directorio. Ello incluye la administración de cuentas de equipo y usuario y la administración de recursos locales, como estaciones de trabajo y servidores miembro.

Los propietarios de datos y servicios son responsables del mantenimiento a largo plazo del directorio una vez que ha finalizado el proyecto de implementación, es importante que estas personas proporcionen información relativa a las necesidades organizativas y estén familiarizados con los motivos y la forma en que se toman determinadas decisiones de diseño.

Entre los propietarios de servicios se incluyen **el propietario del bosque, el propietario del Sistema de nombres de dominio (DNS) de Directorio Activo y el propietario de la topología del sitio**.

Entre los propietarios de datos se incluye **a los propietarios de las unidades organizacionales (OU).**

4.2.2 *Administradores de Datos y Servicios*

Dos tipos de administradores intervienen en el funcionamiento de AD DS: **administradores de servicios y administradores de datos.** Los administradores de servicios implementan las decisiones de la directiva tomadas por los **propietarios de servicios** y se hacen cargo de las tareas diarias asociadas al mantenimiento de la infraestructura y el servicio del directorio, esto incluye administrar los controladores de dominio que hospedan el servicio de directorio, administrar otros servicios de red como DNS necesarios para AD DS, controlar la configuración de las opciones de todo el bosque y garantizar que el directorio esté siempre disponible.

- Los **administradores de servicios** son responsables también de completar las tareas continuas de implementación de Directorio Activo que son necesarias una vez que se ha completado el proceso inicial de implementación de Directorio Activo de Windows Server 2008. Por ejemplo, a medida que aumentan las demandas sobre el directorio, los administradores de servicios crean controladores de dominio adicionales y establecen o eliminan las relaciones de confianza entre los dominios, según sea necesario. Por este motivo, el equipo de implementación de Directorio Activo necesita incluir a administradores de servicios.

- Los **administradores de datos** son usuarios de un dominio responsables tanto de mantener los datos que se almacenan en AD DS, como cuentas de grupo y usuario, como de mantener los equipos miembros del dominio. Los administradores de datos controlan subconjuntos de objetos dentro del directorio y no tienen ningún control sobre la instalación o configuración del servicio de directorio.

Es mejor limitar el número de administradores de servicios de la organización al número mínimo necesario para garantizar que la infraestructura siga funcionando. La mayor parte del trabajo administrativo pueden llevarla a cabo los administradores de datos. Los administradores de servicios requieren un conjunto de destrezas mucho más amplio, ya que son responsables de mantener el directorio y la infraestructura que lo sustenta. Los administradores de datos sólo requieren las habilidades necesarias para administrar su parte del directorio. Dividir las asignaciones de trabajo de esta manera tiene como resultado un ahorro de costos para la organización, ya que sólo es preciso impartir formación a un número reducido de administradores para que haga funcionar y mantenga todo el directorio y su infraestructura.

4.2.3 *Propietario del Bosque*

El **propietario del bosque** suele ser un administrador jefe de tecnologías de la información (TI) de la organización que es responsable del proceso de implementación del Directorio Activo y de administrar, en última instancia, la prestación de los servicios dentro del bosque una vez finalizada la implementación. El propietario del bosque designa a las personas que desempeñarán las demás funciones de propietarios identificando al personal clave de la organización capaz de aportar la información necesaria sobre la infraestructura de la red y las necesidades administrativas.

El propietario del bosque es responsable de lo siguiente:

- Pertenencias de los grupos de administradores de servicios de todos los dominios del bosque.
- Creación del diseño de la estructura de la unidad organizativa para cada dominio del bosque.
- Delegación de la autoridad administrativa a los propietarios de la OU.

- Cambios en el esquema
- Cambios en las opciones de configuración de todo el bosque.
- Implementación de determinadas opciones de directiva de la directiva de grupo, incluidas las directivas de cuenta de usuario de dominio como las directivas de bloqueo de cuenta y de contraseñas específicas.
- Opciones de directiva de negocio que se aplican a los controladores de dominio.
- Cualquier otra configuración de directiva de grupo que se aplica en el nivel de dominio.

El propietario del bosque tiene autoridad sobre todo el bosque. Es responsabilidad del propietario del bosque establecer las directivas de negocio y la directiva de grupo para seleccionar a las personas que serán administradores de servicios. El propietario del bosque es un propietario de servicios.

4.2.4 *Propietario de DNS para AD DS*

El **propietario de DNS** para AD DS es una persona que tiene un conocimiento profundo de la infraestructura de DNS y del espacio de nombres existentes de la organización.

El propietario de DNS para AD DS es responsable de lo siguiente:

- Servir como enlace entre el equipo de diseño y el grupo de TI que posee actualmente la infraestructura de DNS.
- Proporcionar información sobre el espacio de nombres de DNS existente en la organización para ayudar a crear el nuevo espacio de nombres de Active Directory.
- Trabajar con el equipo de implementación para garantizar que la nueva infraestructura de DNS se implemente conforme a las especificaciones del equipo de diseño y de que ésta está funcionando adecuadamente.
- Administrar la infraestructura de DNS para AD DS, incluido el servicio Servidor DNS y los datos DNS.

El propietario de DNS para AD DS es un propietario de servicios.

4.2.5 *Propietario de las Unidad Organizacionales (OU)*

El propietario de la unidad organizacional (OU) es responsable de administrar los datos almacenados en el directorio. Esta persona necesita estar familiarizado con las directivas operativas y de seguridad vigentes en la red. Los propietarios de la unidad organizativa (OU) sólo pueden realizar las tareas que han delegado en ellos los administradores de servicios, y sólo pueden realizar dichas tareas en las unidades organizativas a las que están asignados. Entre las tareas que podrían asignarse al propietario de la OU se incluyen las siguientes:

- Realizar todas las tareas de administración de cuentas dentro de sus unidades organizativas (OU) asignadas.
- Administrar estaciones de trabajo y servicios miembro que son miembros de sus unidades organizacionales asignadas.
- Delegar la autoridad en los administradores locales dentro de sus unidades organizacionales (OU) asignadas.

El propietario de la unidad organizacional (OU) es un propietario de datos.

4.3 Diseño del Bosque

La creación del diseño de un bosque conlleva identificar primero los grupos de la organización que disponen de recursos para alojar un bosque de Directorio Activo y a continuación, definir los requisitos de diseño del bosque. Por último, es preciso determinar el número de bosques que se requieren para satisfacer las necesidades de la organización.

Para el diseño del bosque es necesario seleccionar uno de los tres modelos que se utilizan para Windows Server 2008 R2, los cuales son:

- Modelo de Bosque Organizativo
- Modelo de Bosque de Recursos
- Modelo de Bosque de Acceso restringido

De acuerdo a las necesidades del cliente y a los requerimientos presentados definí que se implementaría un solo bosque y fue de **Recursos**.

Sus características son:

- Un esquema único.
- Contenedor de configuración único.
- Relaciones de confianzas automáticas, bidireccionales y transitivas de los dominios que se tienen hoy en día en el cliente.
- Un catálogo global único.

4.3.6 *Modelo de Bosque de Recursos*

Elegí un modelo de **recursos** para el cliente porque necesitaban un bosque independiente para administrar sus recursos. Los bosques de recursos no contienen cuentas de usuario distintas de las requeridas para la administración del servicio y de las necesarias para proporcionar acceso alternativo a los recursos de dicho bosque en caso de que las cuentas de usuario del bosque organizativo dejen de estar disponibles. Se establecen confianzas de bosque para que los usuarios de otros bosques puedan obtener acceso a los recursos incluidos en el bosque de recursos.

Los bosques de recursos proporcionan un aislamiento de servicios que se usa para proteger las áreas de la red que necesitan mantener un estado de alta disponibilidad y para compartir recursos de forma unidireccional o bidireccional entre bosques.

En el esquema de un solo bosque, los usuarios ven un solo directorio a través del Catálogo Global y no tienen que ser conscientes de ninguna estructura de directorio.

Este diseño es flexible y permite que a futuro se puedan generar otros bosques y unirse a otros, debido al costo administrativo que esto implica, siempre que sea posible, se debe mantener la organización con un solo Bosque bajo la premisa de mantener un esquema centralizado.

Los puntos a considerar para tomar la decisión de crear o mantener otro bosque son:

- Dos organizaciones son totalmente independientes operativamente y no se confía en los administradores de la otra empresa y/o por la confidencialidad de la información.
- No se consigue un acuerdo para la política de cambios y administración de un Bosque común.
- Por asuntos de política institucional.

4.3.7 *Definición del nombre del Bosque y del Dominio de Directorio Activo para el cliente*

De acuerdo a las necesidades del cliente y a sus protocolos de nomenclatura, ellos seleccionaron el nombre para la nueva infraestructura de su Directorio Activo, no lo escribiré en este documento por cuestiones de seguridad a la información del cliente, lo único que conservo como dato fidedigno es la extensión .lan:

Bosque3.lan

4.4 Creación del diseño de un Dominio

Crear el diseño de un dominio implica examinar los requisitos de replicación y la capacidad de la infraestructura de red para crear una estructura de dominio que permita a los Servicios de dominio de Directorio Activo (AD DS) funcionar de la forma más eficiente.

Los dominios se usan para crear una partición del directorio de manera que la información del mismo se pueda distribuir y administrar de forma eficiente en toda la empresa. El objetivo de diseñar un dominio es maximizar la eficacia de la topología de replicación del Directorio Activo y garantizar, al mismo tiempo, que la replicación no consuma demasiado ancho de banda y no interfiera en el funcionamiento diario de la red.

Existen dos tipos de modelos para el diseño de un dominio los cuales son:

- Modelo de Dominio Único
- Modelo de Dominio Regional

El mejor diseño que se adaptaba a las necesidades del cliente es el de **Modelo de Dominio Único.** En la siguiente sección argumento porqué.

4.4.1 *Modelo de Dominio Único*

El modelo de dominio único es el más fácil de administrar y el menos costoso de mantener. Se compone de un bosque que contiene un solo dominio. Este dominio es el dominio raíz del bosque, y contiene todas las cuentas de grupo y usuario del bosque.

El modelo de bosque de dominio único reduce la complejidad administrativa y ofrece las siguientes ventajas:

- Cualquier controlador del dominio puede autenticar a cualquier usuario del bosque.
- Todos los controladores de dominio pueden ser catálogos globales, por lo que no es necesario planear la ubicación de un servidor de catálogo global.

En un bosque de dominio único, todos los datos del directorio se replican en todas las ubicaciones geográficas que hospedan controladores de dominio, es decir, en todas las oficinas foráneas y centrales del cliente. Si bien este modelo es el más fácil de administrar, también crea el mayor volumen de tráfico de replicación de los dos modelos de dominio. La partición del directorio en varios dominios limita la replicación de objetos.

4.4.2 *Definición del nombre de Dominio*

Con la finalidad de mantener la premisa de centralización del servicio, costos de administración de sistemas reducidos y el menor impacto a los usuarios del cliente durante la transición del servicio actual decidieron nombrar al dominio:

Bosque3.lan

En este dominio se ubican todos los recursos dentro de la infraestructura del cliente tales como usuarios, computadoras, servidores, impresoras, sitios de replicación, etc.

Como se puede observar es igual al nombre del bosque, esto se debe a las recomendaciones y mejores prácticas de Microsoft cuando se crea el primer bosque y dominio en una infraestructura nueva.

4.4.3 *Diseño de una Infraestructura DNS*

Los Servicios de Dominio de Directorio Activo usan los servicios de resolución de nombres del Sistema de Nombres de Dominio (DNS) para permitir que los clientes localicen controladores de dominio y que los controladores de dominio que hospedan el servicio de directorio se comuniquen entre sí.

El Directorio Activo permite una fácil integración del espacio de nombres en un espacio de nombres DNS existente. Características como las zonas DNS integradas en Directorio Activo facilitan la implementación de DNS eliminando la necesidad de configurar zonas secundarias y, después, transferencias de zona.

El cliente disponía de un servicio de Sistema de nombres de Dominio (DNS) en su bosque bosque1.mx por lo que realicé una Integración de AD en la infraestructura DNS del Nuevo dominio bosque3.lan. Con esto se evitó crear un fuerte impacto en los usuarios finales al momento de utilizar este servicio.

4.5 Diseño de las Unidades Organizacionales (OUs)

La estructura de una unidad organizacional (OU) para un dominio incluye lo siguiente:

- Un diagrama de la jerarquía de la unidad organizacional.
- Una lista de unidades organizacionales.
- Para cada unidad organizacional:
    - La finalidad de la unidad organizacional.

- Una lista de usuarios o grupos que tienen control sobre la unidad organizacional o los objetos de la misma.
- El tipo de control que los usuarios y grupos tienen sobre los objetos de la unidad organizacional.

La jerarquía de la unidad organizacional no tiene por qué reflejar la jerarquía de los departamentos de la organización o grupo. Las unidades organizacionales se crean para una finalidad específica, como la delegación de tareas de administración o la aplicación de una directiva de grupo, o bien para limitar la visibilidad de los objetos.

Es posible diseñar una estructura de unidad organizacional propia con el fin de delegar la administración en individuos o grupos de la organización que requieran autonomía para administrar sus propios datos y recursos. Las unidades organizacionales representan límites administrativos y permiten controlar el ámbito de autoridad de los administradores de datos.

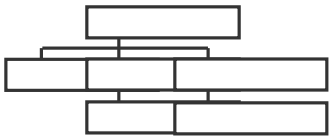
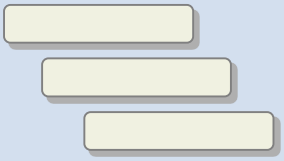
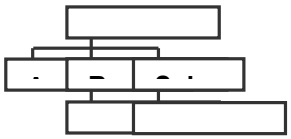
Si bien, desde el punto de vista técnico, no existe límite en el número de niveles que puede tener la estructura de una unidad organizacional, por razones de capacidad de administración se recomienda que no supere los 10 niveles de profundidad, técnicamente el número de unidades organizacionales de cada nivel no tiene límite. Se debe tener en cuenta que las aplicaciones habilitadas para Servicios de dominio de Directorio Activo (AD DS) pueden imponer restricciones al número de caracteres usados en el nombre distintivo, es decir, la ruta LDAP (Protocolo ligero de acceso a directorios) completa al objeto del directorio o al número de niveles de la unidad organizacional dentro de la jerarquía.

Las unidades organizacionales pueden usarse para delegar la administración de los objetos (como usuarios o equipos) de la unidad organizacional en el individuo o grupo que se haya designado.

Los Servicios de dominio de Directorio Activo (AD DS) permiten controlar las tareas administrativas que pueden delegarse en un nivel muy detallado.

Se recomienda mantener una estructura estandarizada para el diseño de las OUs, que está basada en los siguientes modelos:

Tabla 6 Modelos para el Diseño de OUs

MODELO DE ADMINISTRACIÓN	DISEÑO DE OU BASADO EN
Geográfico 	Localización
Organización 	Estructura de la organización
Negocio 	Funciones en la Organización
Híbrido  	Localización para las OU más altas. Estructura para las OU más bajas. O viceversa.

El contar con un modelo para la estructura de las OUs de un Directorio Activo, facilita la delegación de administración de objetos.

4.5.1 *Delegación de la Administración de OUs y contenedores predeterminados*

Todos los dominios de Directorio Activo contienen un conjunto estándar de contenedores y unidades organizativas (OU) que se crean durante la instalación de los Servicios de dominio de Directorio Activo (AD DS). A continuación se enumeran algunas:

- Contenedor de dominio que sirve como contenedor raíz para la jerarquía.
- Contenedor integrado que tiene las cuentas de administrador de servicios predeterminadas.
- Contenedor de usuarios, que sirve como ubicación predeterminada para las nuevas cuentas de usuario y grupos creados en el dominio.
- Contenedor de equipos que es la ubicación predeterminada para las nuevas cuentas de equipo creados en el dominio.
- Unidad organizacional (OU) Controladores de dominio, que es la ubicación predeterminada para las cuentas de equipo de las cuentas de equipo de controladores de dominio

El propietario del bosque controla estas unidades organizacionales y contenedores predeterminados.

Dos puntos importantes y que se tienen que tomar en cuenta para la definición de la estructura lógica de las unidades organizacionales son:

- **Delegar autoridad administrativa:** Se pueden crear unidades organizacionales dentro de un dominio para delegar el control administrativo de unidades organizacionales a usuarios o grupos determinados.
- **Asignación de Políticas de Grupo (GPO´s):** Durante la aplicación de GPO´s se debe pensar sobre todo en los objetos que se desea administrar, cuando se está definiendo el diseño de la estructura de unidades organizacionales, se debe pensar en las estaciones de trabajo, servidores y usuarios, de manera que se puedan aplicar estas políticas a perfiles o niveles de objetos estándar, es decir, definir la cantidad de acciones o restricciones a aplicar a un grupo s de usuarios, estaciones de trabajo o servidores.

4.5.2 *Modelo de Estructura de OUs*

De acuerdo a las necesidades administrativas y operacionales de cliente, el modelo para sus unidades organizacionales que mejor se adaptó fue un híbrido de 2 niveles: **Negocio / Organización**. El siguiente esquema muestra una sección de la estructura de OUs del modelo propuesto:

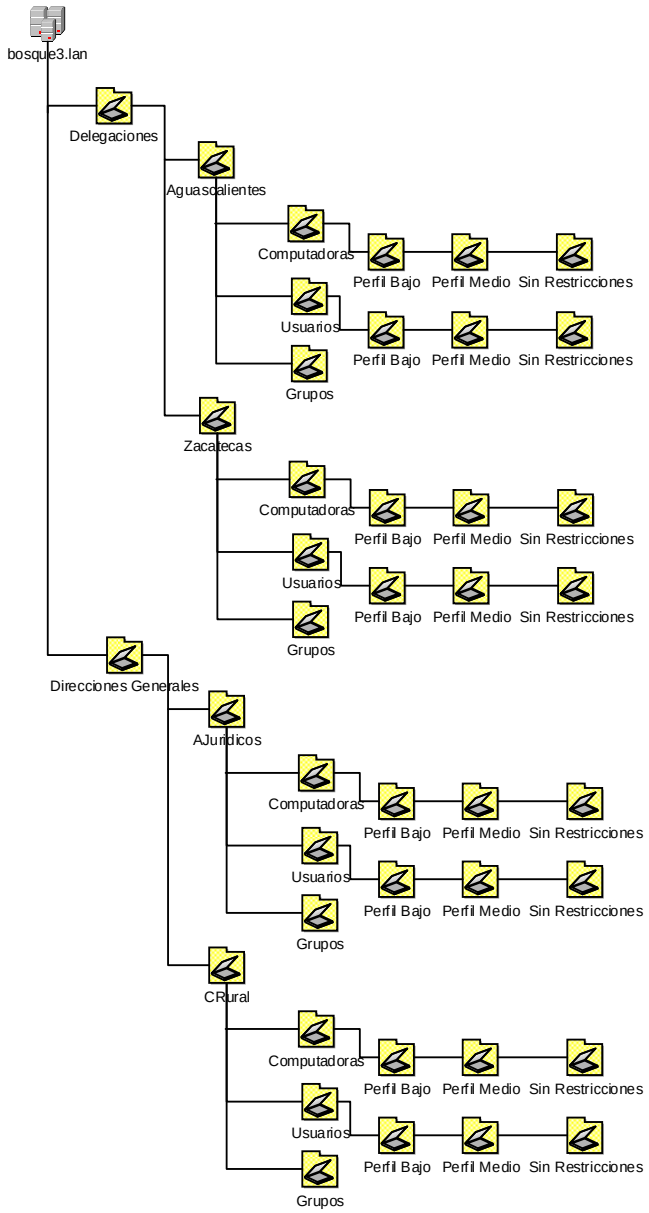


Imagen 7. Modelo de OUs para el cliente

4.5.3 *Definición de Diseño*

De acuerdo al modelo hibrido para la estructura de OUs, estas quedaron distribuidas de la siguiente forma:

Tabla 7 Clasificación de las OUs por nivel para el cliente.

Nivel	Unidades Organizacionales
Primer nivel: comprende las Unidades Organizacionales de Negocio	• Oficinas • Direcciones Generales • Servicios
Segundo Nivel: comprende las OUs de organización	• Oficinas: ○ Aguascalientes ○ AGA ○ Baja California ○ Baja California Sur ○ Campeche ○ Chiapas ○ Chihuahua ○ Coahuila –Saltillo ○ Colima ○ Distrito Federal ○ Durango ○ Estado de México ○ Guanajuato ○ Guerrero ○ Hidalgo ○ Jalisco ○ Laguna ○ Michoacán ○ Morelos ○ Nayarit ○ Nuevo León ○ Oaxaca ○ Puebla ○ Querétaro ○ Quintana Roo ○ San Luis Potosí ○ Sinaloa ○ Sonora ○ Tabasco ○ Tamaulipas ○ Tlaxcala ○ Veracruz ○ Yucatán ○ Zacatecas
	• Direcciones Generales: ○ DirccionJefe ○ DGRegistro ○ DGTitulacionCD ○ DGCatastroRural ○ DGDelegaciones ○ DGFinanzasAdmon ○ DGAJuridicos ○ OinternoControl
	• Computadoras

Tercer nivel: comprende los principales objetos a administrar en un Directorio Activo	• Usuarios • Grupos
Cuarto nivel: comprende los tipos de cuentas que se manejarán para "Usuarios" y "computadoras"	• Perfil Básico • Perfil Medio • Sin Restricciones

4.5.4 *Perfiles de Computadoras*

Las Unidades Organizacionales "computadoras" almacenarán los equipos de cómputo de tipo Desktop y Laptop, los cuales se clasificarán en los siguientes perfiles:

- Sin Restricciones: Es el perfil menos restringido y permite al usuario mantener el control considerable sobre su equipo.
- Perfil Medio: Este perfil permite realizar la mayoría de cambios de Hardware y Software pero no permite hacer personalizaciones.
- Perfil Básico: Este perfil tendrá los permisos mínimos necesarios para que puedan realizar las actividades laborales para las que están asignados los equipos.

4.5.5 *Perfiles de Usuarios*

- **Sin Restricciones**: Este perfil está enfocado a los usuarios móviles, puede iniciar sesión en distintos equipos asignados para consultar información importante relacionada a su perfil, le permite la instalación de aplicaciones de manera ilimitada, permite al usuario acceso sin restricciones a parámetros de configuración de red, permite al usuario desconectarse de la red sin apagar el equipo o cerrar sesión.
- **Perfil Medio:** Este perfil Permite al usuario iniciar sesión en distintos equipos, tiene acceso ilimitado a la instalación y desinstalación de aplicaciones, solo tiene acceso a los datos almacenados en su perfil de usuario
- **Perfil Básico:** Este perfil es el más restrictivo y el usuario solo tiene acceso a las aplicaciones publicadas para su perfil, no tiene acceso al menú de inicio ni al panel de control.

4.6 Topología de Sitios

La topología de sitios de Directorio Activo es la representación lógica de una red física. Los clientes (equipos de cómputo con sistemas operativos como Windows XP, Windows 7, etc.) y servidores del directorio utilizan la topología de sitios de un Bosque para el ruteo de manera eficiente el tráfico de consultas y de replicación, también indican en qué lugar de la red colocar los controladores de dominio.

Para la definición de la topología de sitios se consideran los siguientes conceptos clave:

- Un sitio es un conjunto de localidades con conectividad de red.
- Un Site Link es un enlace poco confiable o con un ancho de banda reducido que conecta dos o más sitios.
- Las computadoras cliente intentan comunicarse primero con los servidores que se encuentran en el mismo sitio que ellas.
- La replicación del Directorio Activo utiliza la topología de sitios para generar conexiones de replicación.

De acuerdo a las características de red que tiene el cliente en sus oficinas foráneas y centrales se definió un diseño en su topología de sitios como se muestra en los siguientes apartados:

4.6.1 *Nomenclatura de Sitios*

Los sitios son las entidades físicas distribuidas geográficamente e implicadas en la replicación del directorio activo (Controladores de Dominio).

La siguiente tabla muestra la lista de sitios que se tomarán en cuenta para el esquema de replicación del cliente, se consideró mantener un sitio de directorio Activo por cada oficina del cliente.

Tabla 8 Sitios del cliente

Sites			
Hidalgo	(DF)Oficinas Centrales	Zacatecas	Laguna
Puebla	Morelos	Coahuila	Guerrero
Tlaxcala	Baja California Norte	Nuevo Leon	Oaxaca
Aguascalientes	Baja California Sur	Tamaulipas	Chiapas
Guanajuato	Sonora	Jalisco	Campeche
San Luis Potosí	Sinaloa	Nayarit	Quintana Roo
Querétaro	Chihuahua	Colima	Yucatán
Estado de México	Durango	Michoacán	Tabasco
AGA	Laguna	Distrito Federal	Veracruz

4.6.2 *Definición de Diseño de Sitios y Subredes*

A continuación se presentan los nombres de sitios los cuales corresponden a cada una de las oficinas definidas por regiones, así como las subredes correspondientes a cada sitio.

Tabla 9 Servidores para cada site

Sitio	Servidores	Ip del servidor	Segmento / Mascara asociado a DC
Oficinas Centrales (DF)	XFDCOFC01	200.36.0.155	200.36.0.0 / 24
	XHVDCOFC01	200.36.0.181	
	XHVDCOFC02	200.36.0.182	
AGA	XHFHVAGA	200.168.2.155	192.168.2.0 / 24
	XHVDCAGA	200.168.2.252	
Aguascalientes	XHFHVAGS	200.39.1.155	200.39.1.0/24
	XHVDCAGS	200.39.1.252	
Baja California	XHFHVBCA	200.39.2.155	200.39.2.0/24
	XHVDCBCA	200.39.2.252	
Baja California Sur	XHFHVBCS	200.39.3.155	200.39.3.0/24
	XHVDCBCS	200.39.3.252	
Campeche	XHFHVCAM	200.39.4.155	200.39.4.0/24
	XHVDCCAM	200.39.4.252	
Chiapas	XHFHVCHI	200.39.7.155	200.39.7.0/24
	XHVDCCHI	200.39.7.252	
Chihuahua	XHFHVCHH	200.39.8.155	200.39.8.0/24
	XHVDCCHH	200.39.8.252	
Coahuila –Saltillo	XHFHVCOA	200.39.5.155	200.39.5.0/24
	XHVDCCOA	200.39.5.252	
Colima	XHFHVCOL	200.39.6.155	200.39.6.0/24

	XHVDCCOL	200.39.6.252	
Durango	XHFHVDGO	200.39.200.155	200.39.200.0/24
	XHVDCDGO	200.39.200.252	
Estado de México	XHFHVMEX	200.39.15.155	200.39.15.0/24
	XHVDCMEX	200.39.15.252	
Guanajuato	XHFHVGTO	200.39.11.155	200.39.11.0/24
	XHVDCGTO	200.39.11.252	
Guerrero	XHFHVGRO	200.39.12.155	200.39.12.0/24
	XHVDCGRO	200.39.12.252	
Hidalgo	XHFHVHGO	200.39.13.155	200.39.13.0/24
	XHVDCHGO	200.39.13.252	
Jalisco	XHFHVJAL	200.39.14.155	200.39.14.0/24
	XHVDCJAL	200.39.14.252	
Laguna	XHFHVCLG	200.39.33.155	200.39.33.0/24
	XHVDCCLG	200.39.33.252	
Michoacán	XHFHVMIC	200.39.16.155	200.39.16.0/24
	XHVDCMIC	200.39.16.252	
Morelos	XHFHVMOR	200.39.17.155	200.39.17.0/24
	XHVDCMOR	200.39.17.252	
Nayarit	XHFHVNAY	200.39.18.155	200.39.18.0/24
	XHVDCNAY	200.39.18.252	
Nuevo León	XHFHVNLN	200.39.19.155	200.39.19.0/24
	XHVDCNLN	200.39.19.252	
Oaxaca	XHFHVOAX	200.39.20.155	200.39.20.0/24
	XHVDCOAX	200.39.20.252	
Puebla	XHFHVPUE	200.39.21.155	200.39.21.0/24
	XHVDCPUE	200.39.21.252	

Querétaro	XHFHVQRO	200.39.22.155	200.39.22.0/24
	XHVDCQRO	200.39.22.252	
Quintana Roo	XHFHVQOO	200.39.23.155	200.39.23.0/24
	XHVDCQOO	200.39.23.252	
San Luis Potosí	XHFHVSLP	200.39.24.155	200.39.24.0/24
	XHVDCSLP	200.39.24.252	
Sinaloa	XHFHVSIN	200.39.25.155	200.39.25.0/24
	XHVDCSIN	200.39.25.252	
Sonora	XHFHVSON	200.39.26.155	200.39.26.0/24
	XHVDCSON	200.39.26.252	
Tabasco	XHFHVTAB	200.39.27.155	200.39.27.0/24
	XHVDCTAB	200.39.27.252	
Tamaulipas	XHFHVTAM	200.39.28.155	200.39.28.0/24
	XHVDCTAM	200.39.28.252	
Tlaxcala	XHFHVTLX	200.39.29.155	200.39.29.0/24
	XHVDCTLX	200.39.29.252	
Veracruz	XHFHVVER	200.39.30.155	200.39.30.0/24
	XHVDCVER	200.39.30.252	
Yucatán	XHFHVYUC	200.39.31.155	200.39.31.0/24
	XHVDCYUC	200.39.31.252	
Zacatecas	XHFHVZAC	200.39.32.155	200.39.32.0/24
	XHVDCZAC	200.39.32.252	

4.6.3 *Definición de Site Links*

Los sitios conectados entre sí a través del directorio activo son llamados Site Links, los Site Links unen uno o más sitios especificando el costo del Site-Link, cuando uno o más sitios están incluidos en un sitio, este asume que cualquiera de los dos sitios puede comunicarse con el costo especificado.

La siguiente tabla muestra los costos de replicación según el ancho de banda.

Tabla 10 Servidores para cada site

Ancho de Banda	Costo de replicación
28 Kbps	702
56 Kbps	586
64 Kbps	567
96 Kbps	517
128 Kbps	486
256 Kbps	425
512 Kbps	300
1024 Kbps	200
2048 Kbps	100
= > 4096 Kbps	50

4.6.4 *Definición de diseño de Site Links.*

El costo de replicación asociado se realizó en base a los enlaces de sitio de las oficnas del cliente, que son de 2048 Kbps, por lo que tienen costos de valor 100 en todos los enlaces de Sitio.

De acuerdo a la demanda de los servicios utilizados de Directorio Activo recomendé los siguientes horarios para la replicación entre los controladores de dominio.

Tabla 11 Configuración de los Site Links

Nombre del Site Link	Costo	Horario de Replicación	Intervalo de Replicación
Mex-Centro	100	De L a V 7 pm a 10 pm Sab. Y Dom. Todo el día.	15 min.
Mex-Norte	100	De L a V 7 pm a 10 pm Sab. Y Dom. Todo el día	15 min.
Mex-Sur	100	De L a V 7 pm a 10 pm Sab. Y Dom. Todo el día	15 min.

Las ocasiones en las que replican los controladores de dominio a simple vista parecen pocas, pero recordemos que se configuraron los controladores de dominio como Global Catalog, es decir, todos tendrán la misma Base de Datos y sólo necesitarán la actualización del día.

Los sitios que apuntan a cada link quedaron distribuidos de acuerdo a la zona que les corresponde en el país y se creó uno exclusivo para las oficinas centrales donde se encuentran también los servidores de Exchange:

Tabla 12 Distribución de los sites por Site link.

Nombre del Site Link	Sites
Mex-Centro	•Hidalgo •AGA •Puebla •Tlaxcala •Aguascalientes •Guanajuato •San Luis Potosí •Querétaro •Estado de México •Oficinas Centrales •Morelos
Mex-Norte	•Baja California Norte •Baja California Sur •Sonora •Sinaloa •Chihuahua •Durango •Zacatecas •Coahuila •Nuevo León •Tamaulipas •Jalisco •Nayarit •Colima •Michoacán •Laguna
Mex-Sur	•Guerrero •Oaxaca •Chiapas •Campeche •Quintana Roo •Yucatán •Veracruz •Tabasco

4.7 Definición de Diseño de la Distribución de Roles FSMO

Para un óptimo desempeño y una administración sencilla, propuse que los roles FSMO quedaran instalados en los controladores de dominio de oficinas centrales que, como me indicó el cliente, será donde se encuentren los administradores y dueños del directorio Activo.

Los controladores de dominio con los sitios y roles definidos quedaron instalados de la siguiente forma:

Tabla 13 Ubicación de los roles FSMO

Sitio	Domain Controller	Rol FSMO
Oficinas Centrales (DF)	XHFDCOFC01	PDC Emulator Domain Naming Master Schema Master RID Operations Master
Oficinas Centrales (DF)	XHVDCOFC01	Infrastructure Master
Oficinas Centrales (DF)	XHVDCOFC01	Certificadora para Exchange

4.8 Distribución de Controladores de Dominio y Localidades asignadas

Como definición de diseño y en base a la distribución de roles y servicios de DNS, a continuación se muestra la imagen de la distribución de los controladores de dominio, las oficinas en donde se ubican son:

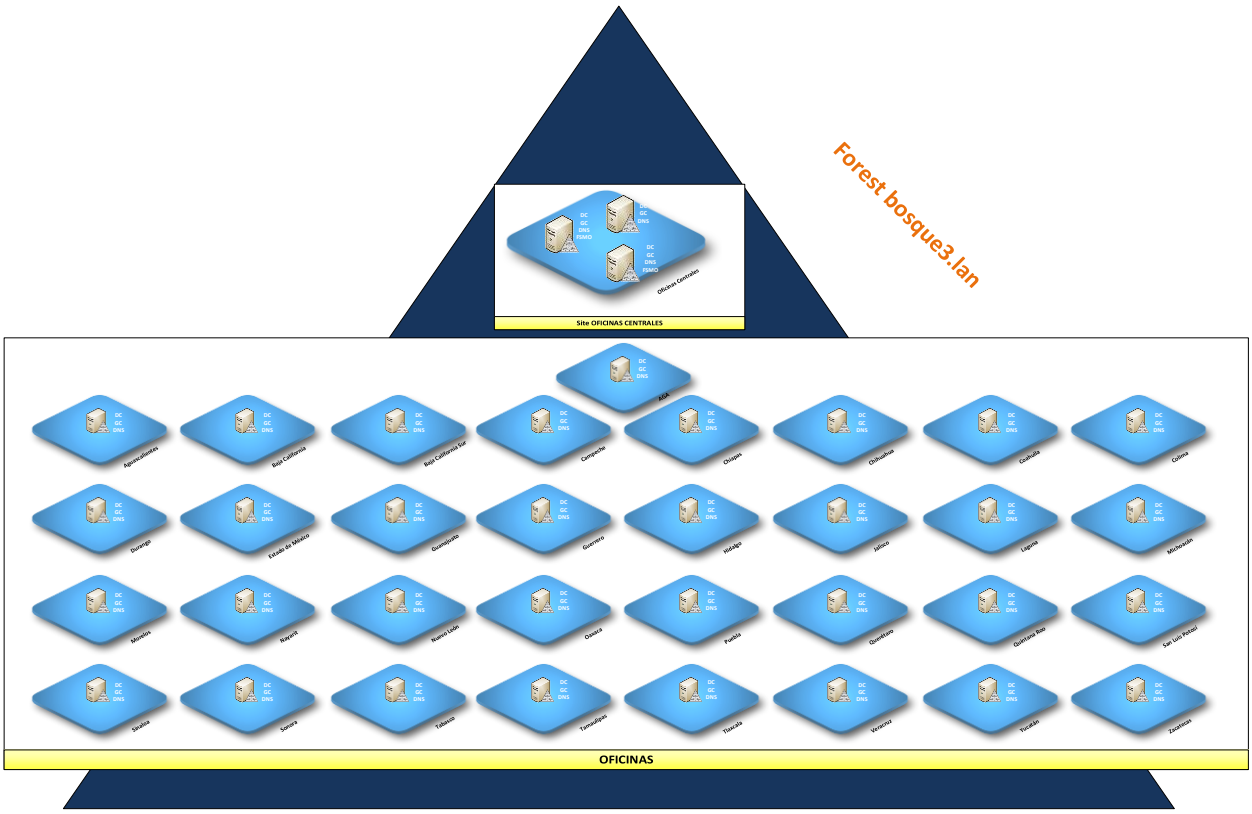


Imagen 10. Distribución de los DCs.

Como se observa en la imagen y como ya se había mencionado anteriormente, se instaló un controlador de dominio en cada una de las oficinas del cliente, estos atienden las peticiones de autenticación, resolución de nombres y servicios del AD que los equipos clientes realicen, siempre y cuando estos estén unidos al dominio. El diseño quedó basado en la asignación de subredes y en la cantidad de servidores que había adquirido el cliente.

El diseño inicial era para 33 controladores de dominio, 31 para estados y 2 para oficinas centrales, sin embargo, se detectó la necesidad de contar con un controlador de dominio en las oficinas de Comarca Lagunera, otro en sus oficinas de la zona centro del DF y otro para la demanda de servicios en oficinas centrales, por lo que, como valor agregado incluí al diseño 3 controladores de dominio, mismos que fueron instalados y configurados en una segunda etapa del proyecto.

4.9 Nomenclatura

La estandarización de los nombres asignados a los recursos del Directorio Activo proporciona beneficios administrativos, tomando esto como primicia, recomendé que todos los recursos de nueva creación se apeguen al nuevo estándar de nomenclatura que el cliente estableció.

Los recursos que tienen nombres que no se apegan a estos estándares, serán cambiados por el cliente paulatinamente, después del proyecto de directorio activo.

Como regla principal a los estándares de su nomenclatura: ***No se debe utilizar o hacer uso de caracteres especiales en los nombres de dominio y de computadoras (servidores y pc´s), tampoco se utilizarán acentos en la asignación de nombres a cualquier recurso del directorio.***

En los siguientes apartados se detalla la nomenclatura para cada objeto que compone al Directorio Activo.

4.9.1 *Convención de nomenclatura para Usuarios de Dominio*

Para generar el User ID, se recomienda tomar la siguiente cadena de texto:

Apellido_Paterno, Apellido_Materno Y Nombres

Consideraciones:

- Se cambia la letra “Ñ” por la letra “N”.
- No se toman en cuenta los acentos gramáticos.
- Se omiten los espacios en blanco.
- En la cadena NOMBRES no se toman en cuenta las palabras: “MARIA”, “JOSE”, “DE”, “LOS”, “LA” y “LAS”.
- En las cadenas APELLIDO_PATERNO y APELLIDO_MATERNO no se toman en cuenta las palabras: “Y”, “DEL”, “DE”, “LAS”, “LA”, y “LOS”.
- La longitud máxima de la firma es de 8 caracteres.

Algoritmos:

Se genera la Primera firma de la siguiente manera:

1. Se toma la primera letra de la cadena NOMBRES.
2. Se completa la firma con la cadena APELLIDO_PATERNO.
3. De ser necesario se trunca a 8 caracteres.

Si la firma no ha sido asignada se acepta la firma propuesta y se detiene el algoritmo.

Si la firma ya ha sido asignada se genera una nueva de la siguiente manera:

4. Se toma la primera letra de la cadena NOMBRES.
5. Se toma la primera letra de la cadena APELLIDO_PATERNO
6. Se completa la firma con la cadena APELLIDO_MATERNO
7. De ser necesario se trunca a 8 caracteres.

Si la firma no ha sido asignada se acepta la firma propuesta y se detiene el algoritmo.

Si la nueva firma generada es igual a la primera se detiene el algoritmo.

Si la firma ya ha sido asignada se genera una nueva de la siguiente manera:

8. Se toma la primera letra de la cadena NOMBRES.
9. Se toma la siguiente letra (segunda, tercera, cuarta, etc. Dependiendo de la iteración) de la cadena APELLIDO_PATERNO
10. Se completa la firma con la cadena APELLIDO_MATERNO
11. De ser necesario se trunca a 8 caracteres.

Si la firma no ha sido asignada se acepta la firma propuesta y se detiene el algoritmo.

Si la nueva firma generada es igual a la primera se detiene el algoritmo.

Si la firma ya ha sido asignada se genera una nueva repitiendo desde el paso 8.

Ejemplo:

RODRÍGUEZ DE LA LUZ MARIA LUISA

Resultados:

Tabla 14 Ejemplo de nomenclatura para usuario

Iteración	Cuenta de usuario sugerida
1	Lrodrigu
2	Lrluz
3	Lroluz
4	Lrodluz
5	Lrodrluz
6	Lrodrilu
7	Lrodrigl
8	Lrodrigu

4.9.2 *Convención de nomenclatura de Usuarios con otras Funciones*

La recomendación para este tipo de usuarios es que tengan dos User-ID´s, por ejemplo, uno para funciones de usuario (usuario que no tiene privilegios de administración del dominio) y otro para funciones de administrador del dominio.

Los usuarios externos también aplican en esta convención de nombres, por ejemplo, una persona que brinde sus servicios de outsourcing por tiempo limitado.

De acuerdo a las funciones que vaya a realizar se le asignarán unas letras iniciales para distinguir el tipo de usuario.

Tabla 15 Iniciales distintivas

Valor	Descripción
ADM	Administrador ó Cuenta de Servicio.
OPR	Operador
CAU	Help Desk (Centro de Atención a Usuarios)
EXT	Usuario Externo (Proveedor., etc.)

Adicional a las iniciales distintivas se deben de seguir los lineamientos que se utilizaron en la nomenclatura de usuarios:

Tabla 16 Convención de nomenclatura

Bloq.	Descripción	Valor	Separador	Límite de Caracteres	Comentarios
1	Identificador de Administración	ADM	Guion Bajo	Fijo a 3	Requerido
2	User ID Asignado al Usuario	User ID	N/A	Fijo a 8	Requerido

Ejemplos: **ADM_ Lrluz**
ADM_ Lroluz
ADM_ Lrodluz

4.9.3 *Grupos de Distribución y Seguridad*

Los grupos de distribución y seguridad son una forma de clasificar recursos, útil para asignar permisos en distintos niveles (impresoras, folders, aplicaciones, etc.), en vez de hacerlo usuario por usuario. Esto facilita la administración de los usuarios en Windows Server 2008 R2. Un usuario puede ser asignado a uno o más grupos.

Los permisos asignados a un usuario que pertenece a más de un grupo, se suman, la excepción es el permiso más restrictivo "No access" y este reemplaza cualquier otro permiso.

- **Grupos de Distribución y/o Seguridad**

Tabla 17 Nomenclatura para grupos de distribución

Bloq.	Descripción	Valor	Separador	Límite de Caracteres	Comentarios
1	Identificación de objeto Grupo	GRPO	Guion medio -	Fijo a 4	Requerido
2	Tipo de Grupo: **GG**= Global Group **DL**= Domain Local Group **UG**= Universal Group	GG,DL ó UG	Guion medio -	Fijo a 2	Requerido
3	Nombre del área o departamento	Variable	Guion medio -	Variable	Requerido, este es el primer bloque del nombre de grupo. Si el nombre es de más de una palabra.
4	Segundo criterio de agrupación	Variable	Guion medio -	Variable	Opcional, este puede ser el último bloque del nombre de grupo Si el nombre es de más de una palabra.

Ejemplo: **GRPO-GG-Finanzas**
GRPO-DL-Auditoria-General

- **Grupos de Administración del Dominio**

Se recomendó agrupar a los usuarios administradores por niveles de acuerdo a las diferentes funciones que vaya a ejercer sobre el dominio y bosque.

Tabla 18 Nomenclatura para grupos de administración

Bloq.	Descripción	Valor	Separador	Límite de Caracteres	Comentarios
1	Identificación de objeto Grupo	GRPO	Guion medio	Fijo a 4	Requerido
2	Indicador de grupo de administradores	ADM	Guion medio	Fijo a 3	Requerido
3	Nombre de la unidad de Organización que administra	Nombre de la UO	Guion medio	Variable	Si el nombre es de más de una palabra, separarlas con guiones.

Ejemplo: **GRPO-ADM-QUALITA**
GRPO-ADM-QUALITA-SERVICIOS

4.10 Nivel Funcional

El nivel funcional determina las capacidades del dominio y del bosque de Directorio Activo que está disponible. También determinan qué sistemas operativos Windows Server se pueden ejecutar en los controladores de dominio.

Los niveles funcionales no afectan a los sistemas operativos que se pueden ejecutar en las estaciones de trabajo y los servidores miembros que están unidos al dominio.

Se deben establecer los niveles funcionales de dominio y bosque en el valor más alto que admita su entorno, de esta manera, se podrán usar el mayor número de características de AD. Por ejemplo, si nunca se va a agregar al dominio controladores de dominio Windows Server 2003, se debe seleccionar el nivel funcional de Windows Server 2008 durante el proceso de implementación, sin embargo, si existe la posibilidad de conservar o agregar controladores de dominio que ejecuten Windows Server 2003, deberá seleccionar el nivel funcional de Windows Server 2003.

Nota: Una vez elevado el nivel funcional del dominio y del bosque, no se puede cambiar a un nivel funcional inferior.

Cuando se implementa un bosque nuevo se debe de indicar su nivel funcional y después el nivel funcional del dominio, no es posible establecer el nivel funcional del dominio en un valor diferente al nivel funcional del bosque, por ejemplo, si se establece el nivel funcional del bosque

en Windows Server 2008, sólo se podrá establecer el nivel funcional del dominio en Windows Server 2008.

A continuación se explican las características que están disponibles en los distintos niveles funcionales de Dominio.

Tabla 19 Características de cada nivel funcional de dominio.

Nivel funcional del dominio	Características disponibles	Sistemas operativos de controlador de dominio soportados
Windows 2000 nativo	Están disponibles todas las características predeterminadas de AD y las siguientes características de directorio: • Grupos universales para grupos de distribución y de seguridad • Anidación de grupos • Conversión de grupos, que hacen posible la conversión entre grupos de seguridad y grupos de distribución • Historial de identificadores de seguridad (SID)	• Windows 2000 • Windows Server 2003 • Windows Server 2008
Windows Server 2003	Están disponibles todas las características predeterminadas de AD, todas las características del nivel funcional de dominio nativo de Windows 2000 y las características siguientes: • La herramienta de administración de dominios, Netdom.exe, que permite cambiar el nombre de los controladores de dominio • Actualizaciones de la marca de tiempo de inicio de sesión El atributo **lastLogonTimestamp** se actualiza con la hora en que el usuario o equipo inició sesión por última vez, este atributo se replica dentro del dominio. • La posibilidad de establecer el atributo **userPassword** como la contraseña efectiva en **inetOrgPerson** y los objetos de usuario • La posibilidad de redirigir los contenedores Usuarios y equipos De manera predeterminada, se proporcionan dos contenedores conocidos para albergar cuentas de	• Windows Server 2003 • Windows Server 2008

	equipo y usuario: cn=Computers,<raíz de dominio> y cn=Users,<raíz de dominio>. Esta característica permite definir una ubicación nueva para estas cuentas. • El Administrador de autorización puede almacenar sus directivas de autorización en AD DS • Delegación restringida La delegación restringida hace posible que las aplicaciones aprovechen la delegación segura de credenciales de usuario por medio del protocolo de autenticación basado en Kerberos. La delegación se puede restringir sólo a servicios específicos. • Autenticación selectiva La autenticación selectiva hace posible especificar los usuarios y grupos de un bosque de confianza a los que se les permite autenticarse en servidores de recursos en un bosque que confía.	
Windows Server 2008	Están disponibles todas las características predeterminadas de AD, todas las características del nivel funcional de dominio de Windows Server 2003 y las características siguientes: • Compatibilidad con la replicación del Sistema de archivos distribuido (DFS) para el volumen del sistema (SYSVOL) de Windows Server 2003 La compatibilidad con la replicación DFS ofrece una replicación más sólida y detallada del contenido de SYSVOL. • Compatibilidad del Estándar de cifrado avanzado (AES 128 y AES 256) con el protocolo Kerberos • Información acerca del último inicio de sesión interactivo Información acerca del último inicio de sesión interactivo muestra la información siguiente: • La hora del último inicio de sesión interactivo correcto de un usuario • El nombre de la estación de trabajo desde la que el usuario inició sesión • El número de intentos de inicio de sesión erróneos desde el último inicio de sesión	• Windows Server 2008

	• Directivas de contraseña muy específicas Estas directivas permiten especificar directivas de contraseña y directivas de bloqueo de cuentas para usuarios y grupos de seguridad global en un dominio.	

A continuación se muestra la tabla con las características que están disponibles en cada nivel funcional de bosque.

Tabla 20 Características de cada nivel funcional de bosque.

Nivel funcional del bosque	Características disponibles	Controladores de dominio admitidos
Windows 2000 nativo	Están disponibles todas las características predeterminadas de AD.	• Windows Server 2008 • Windows Server 2003 • Windows 2000
Windows Server 2003	Están disponibles todas las características predeterminadas de AD, además de las siguientes: • Confianza de bosque • Cambio de nombre de dominio • Replicación de valores vinculados Para el almacenamiento y la replicación de valores de miembros individuales se usa menos ancho de banda de red y menos ciclos de procesador durante la replicación. Se evita la pérdida de actualizaciones al agregar o quitar varios miembros simultáneamente en distintos controladores de dominio. • Posibilidad de implementar un controlador de dominio de sólo lectura (RODC) • Mejora en la escalabilidad y los algoritmos de comprobación de coherencia de la información (KCC) El generador de topología entre sitios usa algoritmos mejorados que se escalan para admitir bosques con un número mayor de sitios de los que el AD admite en el nivel funcional de bosque de Windows 2000.	• Windows Server 2003 • Windows Server 2008

	• Posibilidad de crear instancias de la clase auxiliar dinámica llamada **dynamicObject** en una partición de directorio de dominio • Posibilidad de convertir una instancia de un objeto **inetOrgPerson** en una instancia de un objeto **User** y completar la conversión en la otra dirección • Posibilidad de crear instancias de nuevos tipos de grupo para admitir la autorización basada en funciones. • Desactivación y nueva definición de atributos y clases en el esquema	
Windows Server 2008	Todas las características disponibles en el nivel funcional del bosque de Windows Server 2003, pero no las características adicionales. Sin embargo, todos los dominios que se agreguen posteriormente al bosque funcionarán en el nivel funcional del dominio de Windows Server 2008 de manera predeterminada.	• Windows Server 2008

Para poder elevar el nivel funcional (cambiar a un nivel más alto), se deben tener en cuenta las siguientes consideraciones:

- Pertenecer al grupo Administradores del dominio para elevar el nivel funcional del dominio.
- Pertenecer al grupo Administradores de la organización para elevar el nivel funcional del bosque.
- Sólo se puede elevar el nivel funcional del dominio en el Controlador de Dominio con el rol PDC Emulator (PDC).
- El nivel funcional del bosque sólo se puede elevar en el Controlador de Dominio que cuente con el rol Schema Master.
- El nivel funcional de un dominio sólo se puede elevar si todos los controladores de dominio del dominio ejecutan la versión o las versiones de Windows que admite el nuevo nivel funcional.

- El nivel funcional de un bosque sólo se puede elevar si todos los controladores de dominio del bosque ejecutan la versión o las versiones de Windows Server que admite el nuevo nivel funcional.
- No puede establecer el nivel funcional del dominio en un valor que sea inferior al nivel funcional del bosque.
- No puede disminuir el nivel funcional del dominio o del bosque una vez que lo haya elevado.
- No puede invertir la operación de elevación de niveles funcionales de dominio y bosque. Si debe revertir a un nivel funcional inferior, debe volver a crear el dominio o el bosque, o restaurarlo desde una copia de seguridad (Reinstalación del Bosque).

El nivel funcional del Dominio y del Forest que se configuró para la infraestructura del cliente es **Windows Server 2003** debido a los requerimientos de implementación de las aplicaciones de negocio del cliente.

4.11 Diseño Físico del AD DS

Una vez que se ha diseñado la parte lógica del Directorio Activo, se debe modelar el diseño físico. Entre las cosas que se deben de tomar en cuenta en este diseño son los controladores de dominio de AD DS de cada sitio, sus características de hardware y software.

4.11.1 *Convención de Nomenclatura para Servidores*

Los servidores a los que se les instaló el rol de Directorio Activo se nombraron de acuerdo a la nomenclatura que se le recomendó al cliente.

- **Prefijo describiendo el tipo de servidor, físico o virtual**

Tabla 21 Prefijo servidor

Valor	Descripción
SF	Servidor Físico
SV	Servidor Virtual

- **Prefijo describiendo el rol que desempeña el servidor**

Tabla 22 Prefijo rol

Valor	Descripción
DC	Controlador de Dominio
HV	Host de máquinas Virtuales

- **Identificador para las oficinas**

Tabla 23 Identificador oficinas

DELEGACION	SIGLAS
Aguascalientes	AGS
Baja California	BCA
Baja California Sur	BCS
Campeche	CAM
Chiapas	CHI
Chihuahua	CHH
Coahuila -Saltillo	COA
Colima	COL
Durango	DGO
Estado de México	MEX
Guanajuato	GTO
Guerrero	GRO
Hidalgo	HGO
Jalisco	JAL
Comarca Laguna	CLG
Michoacán	MIC
Morelos	MOR
Nayarit	NAY
Nuevo León	NLN
Oaxaca	OAX
Puebla	PUE
Querétaro	QRO
Quintana Roo	QOO
San Luis Potosí	SLP
Sinaloa	SIN

Sonora	SON
Tabasco	TAB
Tamaulipas	TAM
Tlaxcala	TLX
Veracruz	VER
Yucatán	YUC
Zacatecas	ZAC
AGA	AGA
Oficinas Centrales	OFC

- **Identificador para número consecutivo, utilizado únicamente en Oficinas Centrales**

Tabla 24 Número consecutivo

Valor	Descripción
XX	**Numero Consecutivo comenzando con 01**

- **Servidores en Oficinas Centrales**

Tabla 25 Servidores en Oficinas Centrales

Bloq	Descripción	Valor	Separador	Límite de Caracteres	Comentarios
1	Prefijo	XHF, XHV	N/A	Fijo a 2	Requerido
2	Rol	DC	N/A	Fijo a 2	Requerido
3	Identificador para la localidad	OFC	N/A	Fijo a 3	Requerido
4	Número del servidor con esa función.	01, 02, 03,04,05,06	N/A	Fijo a 2	Requerido

Ejemplo: **SFDCOFC01 (Servidor Físico, Domain Controller, Oficinas Centrales, 01)**

- **Servidores en oficinas foráneas del cliente**

Tabla 26 Servidores Foráneos

Bloq	Descripción	Valor	Separador	Límite de Caracteres	Comentarios
1	Prefijo	XHF, XHV	N/A	Fijo a 2	Requerido

2	Rol o función que desempeña	DC, HV	N/A	Fijo a 2	Requerido
3	Identificador para la localidad	OFC	N/A	Fijo a 3	Requerido

Ejemplo: **SFHVGRO (Servidor Físico, Host Virtual, Guerrero)**
Ejemplo 2**: SVDCGRO (Servidor Virtual, Domain Controller, Guerrero)**

4.12 Hardware, Software y Configuración

En las siguientes tablas se muestran las características de hardware de los servidores que se asignaron en cada uno de los sitios de las oficinas del cliente.

Se dimensionó de acuerdo a los servicios que se configuraron en el Directorio Activo y a la cantidad de usuarios que lo utilizan

Tabla 27 Características de Hardware de los servidores para oficinas centrales

Numero de Servidores	Sistema Operativo	Características HW para cada uno	Opciones de Configuración:
1 Físico	**Windows Server 2008 R2 Standard Edition x64 SP1**	2 Proc. Quad Core, 8 MB cache 16 GB RAM 5x300 GB 1 RAID5	Particiones de Discos **C:** 146 GB (Sistema Operativo **D:** 900 GB (Base de Datos AD y Sysvol)
2 Virtuales	**Windows Server 2008 R2 Standard Edition x64 SP1**	4 Procesadores virtuales 8 GB RAM	VHD: **C:** 146 GB (Sistema Operativo) **D:** 146 GB (Base de datos AD y Sysvol)

Tabla 28 Características de Hardware de los servidores para oficinas foráneas

Numero de Servidores	Sistema Operativo	Características HW	Opciones de Configuración:
33	**Windows Server 2008 R2 Standard Edition x64 SP1**	2 Proc. Quad Core 8 MB cache 8 GB RAM 4x146 GB 1 RAID5	Particiones de Discos: **C:** 200 GB (Sistema Operativo) **D:** 900 GB (para almacenar máquinas virtuales)

Tabla 29 Características de las máquinas virtuales para los controladores de dominio.

Numero de Servidores	Sistema Operativo	Características HW para cada uno	Opciones de Configuración:
33 Virtuales	**Windows Server 2008 R2 Standard Edition x64 SP1**	4 Procesadores virtuales 8 GB RAM	VHD: C: 146 GB (Sistema Operativo) D: 146 GB (Base de datos AD y Sysvol)

4.13 Consideraciones de Virtualización para Directorio Activo

Ya que el cliente tomó la opción de implementar los controladores de dominio en máquinas virtuales dí a conocer las consideraciones a tomar en un ambiente virtual para su correcto funcionamiento:

- Se debe utilizar varios hosts para distribuir los controladores de dominio, esto con el fin de no mantener un solo punto de falla.

- No se debe pausar por largos periodos de tiempo el Servidor virtual, esto debido a que constantemente se escriben cambios en la base de datos de directorio Activo y al resumir la actividad se pausa la replicación de objetos con los demás Controladores de Dominio.

- No está soportado hacer la recuperación de un servidor de Directorio Activo por medio de Snapshot.

- No se recomienda virtualizar los servidores físicos de bases de datos.

- Para los controladores de dominio virtuales es recomendable que se asigne una tarjeta de red física a la tarjeta de red virtual en el servidor con el propósito de no degradar el tiempo respuesta hacia los clientes, esta asignación de tarjeta de red física vs tarjeta de red virtual debería ser 1:1.

- En general, se debe considerar de 10-12% de diferencia en rendimiento de CPU entre un servidor virtual y un servidor físico por lo que es indispensable considerar esta diferencia al momento de dimensionar el nivel de procesamiento de servidores virtuales que ejecuten Directorio Activo.

- No es recomendable asignarles memoria RAM más allá de la memoria RAM física disponible en los servidores HOST.

5 CONCLUSIONES

Migrar el **Directorio Activo Windows server 2003** a **Directorio Activo Servicios de Dominio 2008 R2** mejoró considerablemente el desempeño de la infraestructura del cliente, además de que optimizó la administración y operación de sus recursos, cubriendo así sus necesidades y rebasando sus expectativas.

En el caso particular de este cliente, la renovación, el rediseño y la implementación del AD DS con las mejores prácticas de Microsoft provocó opiniones encontradas entre los involucrados, principalmente por el impacto del cambio a los usuarios finales, quienes en mi opinión son los más importantes porque se ven afectados o beneficiados de forma directa en su trabajo del día a día. Afortunadamente, después de la implementación y de mostrar las mejoras, resultado de mi diseño pensado en el cliente, se rompieron los paradigmas y dudas al respecto. Con esta migración dejaron de enfrentarse con problemas como la pérdida de cuentas ligadas a correo electrónico, no poderse autenticar en sus equipos, no poder utilizar las aplicaciones que consumen servicios del AD DS, entre otros de menor riesgo.

Con el escenario inicial de este cliente puedo concluir que la implementación de una nueva infraestructura no garantiza mejoras, es necesario tener un diseño y una buena planeación incluyendo personas que tengan los conocimientos necesarios para realizarlo. Si no, se pueden enfrentar con problemas desde la instalación, por configuraciones mal planeadas

6 Glosario

- **Directorio Activo:** Servicio de directorio basado en Windows. Directorio Activo almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red. Directorio Activo da a los usuarios de red acceso a los recursos permitidos en cualquier punto de la red mediante un único proceso de inicio de sesión. Proporciona a los administradores de red una vista jerárquica intuitiva de la red y un punto de administración único para todos sus objetos.

- **Grupo:** Conjunto de usuarios, equipos, contactos y otros grupos. Los grupos se pueden utilizar como conjuntos de distribución de correo electrónico o de seguridad. Los grupos de distribución sólo se utilizan para correo electrónico. Los grupos de seguridad se utilizan como listas de distribución de correo electrónico y para permitir el acceso a los recursos.

- **Réplica:** En la replicación de Active Directory, una instancia de una partición lógica de Active Directory que se sincroniza por medio de la replicación entre controladores de dominio que contienen copias de la misma partición de directorios. *Réplica* hace también referencia a una instancia de un objeto o un atributo de un directorio distribuido. En el Servicio de replicación de archivos (FRS), un equipo que se ha incluido en la configuración de un conjunto de réplicas específico.

- **Directiva de Grupo (GPO Group Policy Object):** es un conjunto de una o más políticas del sistema. Cada una de las políticas del sistema establece una configuración del objeto al que afecta. Las políticas se pueden aplicar por función o por el objeto de configuración.

- **DNS (Domain Name System):** sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. Las redes TCP/IP, como Internet, usan DNS para buscar equipos y servicios mediante nombres descriptivos.

- **FSMO (Funciones Flexibles de Operaciones de un Sólo Maestro):** También conocidos como Maestros de Operaciones, roles encargados de efectuar las operaciones que actualizan los objetos que componen el Directorio Activo.

7 REFERENCIAS

1. http://technet.microsoft.com/es-es/library/cc770806(v=WS.10).aspx Planeación para implementar Directorio Activo en Windows Server 2008 R2. 13/11/2014

2. http://serversandservers.wordpress.com/2008/11/01/diseno-eficaz-de-unidades-organizativas/ Referencia de diseños para unidades organizacionales ya aplicados. 13/11/2014

3. https://msevents.microsoft.com/CUI/EventDetail.aspx?culture=es-ES&EventId=1032295636&CountryCode=ES Video donde muestran consejos y mejores prácticas para implementar Directorio Activo. 20/01/2014

4. http://www.microsoft.com/spain/windowsserver2003/technologies/directory/activedirectory/default.aspx Página donde se encuentran los documentos relacionados con el Directorio Activo para Windows Server 2003. 15/06/2014