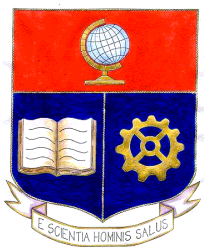

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

PILOTO DE MIGRACIÓN DESDE WINDOWS NT 4.0 HACIA WINDOWS 2003 PARA UNA RED WAN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES DE INFORMACIÓN

MARCO PATRICIO CHIRIBOGA PINTO

DIRECTOR: ING. JUAN HERRERA S.

Quito, Abril - 2005

DECLARACIÓN

Yo, Marco Patricio Chiriboga Pinto, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

MARCO PATRICIO CHIRIBOGA PINTO

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Marco Patricio Chiriboga Pinto, bajo mi supervisión.

_____

Ing. Juan Herrera S.

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Mi especial reconocimiento a DIOS, quien ha sido luz en la oscuridad, fortaleza en mis momentos de debilidad y quien me ha levantado cuando me he sentido vencido.

A mi esposa e hijos, que con sus corazones generosos han sabido apoyar mis necesidades y comprender mis aspiraciones.

A mi querida Escuela Politécnica Nacional, en cuyas aulas fui forjando la semilla del saber y que ahora al culminar la carrera se ve reflejado sus frutos no sólo entregando profesionales, sino seres humanos.

Mi sincera gratitud al Director de Tesis Ing. Juan Herrera S, por haber transmitido sus importantes conocimientos que sirvieron como guía para la feliz culminación del presente proyecto de titulación.

A la Compañía PRONACA, un valioso reconocimiento por haber permitido llevar a cabo el presente proyecto de migración; así como a todos sus directivos y empleados por la colaboración y apoyo brindados en todo momento que se lo ha requerido.

GRACIAS.

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

PRESENTACIÓN

El presente proyecto de titulación se refiere a un Piloto de Migración Windows NT 4.0 hacia Windows 2003 para una red WAN enfocado a la Compañía INDUSTRIAX.

INDUSTRIAX por ser líder en la industria de alimentos, requiere contar con tecnología de punta en su infraestructura con el propósito de garantizar la seguridad, integridad y disponibilidad de sus operaciones; por ésta razón, sus representantes han tomado la decisión de actualizar su plataforma Microsoft de Windows NT Server 4.0 a Windows 2003 Server para aprovechar las bondades que especialmente en tareas de seguridad y administración brinda este nuevo sistema operativo para servidores.

Al momento se dispone de un esquema multidominio, el cual se reemplazará por un esquema de un sólo dominio para disponer de un esquema de administración centralizada, lo que ayudará a conseguir una administración homogénea de los recursos. También se requiere pasar los servicios DNS y DHCP que actualmente están en Linux, hacia Windows 2003 Server.

Todo este cambio va a exigir mayores recursos de Hardware por lo que algunos equipos que actualmente se encuentran trabajando como servidores tendrán que ser reemplazados por unos nuevos. Por otro lado, las estaciones de trabajo mantendrán su configuración actual ya que si es posible la convivencia de Windows Server 2003 con sistemas Windows 95, Windows 98, Windows 2000 Profesional y Windows XP.

Los diseños que se seleccionen para la implementación de la presente migración, serán previamente implementados y probados en un laboratorio de pruebas con el propósito de disminuir el impacto de posibles fallas en la migración desde Windows NT 4 a Windows Server 2003.

OBJETIVOS

OBJETIVO GENERAL

Realizar un piloto de migración de dominios de Windows NT 4.0 a Windows 2003 en un ambiente WAN.

OBJETIVOS ESPECÍFICOS

- Definir la infraestructura básica para la adopción de nuevas tecnologías basadas en Windows 2003.

- Establecer estándares que faciliten la integración y la renovación de los servicios de red a utilizar en la WAN.

- Establecer un piloto de migración de dominios basados en la red actual Windows NT 4.0 a Windows 2003 para su operación sobre una WAN.

CAPÍTULO 1.

1. DEFINICIONES BÁSICAS DEL PROYECTO

1.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

1.1.1. DIRECCIONAMIENTO IP

Al momento las redes LAN[1] de Quito y Guayaquil se encuentran utilizando un direccionamiento IP[2] clase "C" para redes privadas. Las subredes están distribuidas de la siguiente manera:

CIUDAD	QUITO	GUAYAQUIL
SUBRED 1	192.168.1.0	192.168.5.0
SUBRED 2	192.168.20.0	

Tabla 1.1. Direccionamiento IP de INDUSTRIAX.

FUENTE: Inventario de recursos de red, Anexo 1

1.1.2. ENLACES

El enlace de datos que permite la comunicación entre Quito y Guayaquil es un enlace satelital Frame Relay[3] cuyo proveedor es Impsat. Este enlace tiene las siguientes características:

ENLACE	CAPACIDAD	PROVEEDOR	TECNOLOGIA
QUITO	384 Kbps	IMPSAT	FRAME RELAY
GUAYAQUIL	128 Kbps	IMPSAT	FRAME RELAY

Tabla 1.2. Enlaces WAN de IDUSTRIAX.

FUENTE: Inventario de recursos de red, Anexo 1

[1] Ver en siglas y símbolos
[2] Ver en siglas y símbolos
[3] Ver glosario de términos

1.1.3. ESTRUCTURA DE DOMINIOS

En la actualidad la compañía tiene una infraestructura de multidominios, los cuales se han creado de acuerdo a las necesidades del negocio. Esta situación ha provocado una falta de estandarización y organización, es decir, cada dominio tiene su nomenclatura, reglas y configuración propias.

A continuación se detalla la distribución de los dominios en las ciudades de Quito y Guayaquil que son el motivo de este piloto de migración.

CIUDAD	QUITO	GUAYAQUIL
NOMBRE DE DOMINIO	DOM_UIO	DOM-GYE
NOMBRE DE DOMINIO	PECUARIA	
NOMBRE DE DOMINIO	DOM_RH	

Tabla 1.3. Dominios existentes en INDUSTRIAX.

FUENTE: Inventario de recursos de red, Anexo 1

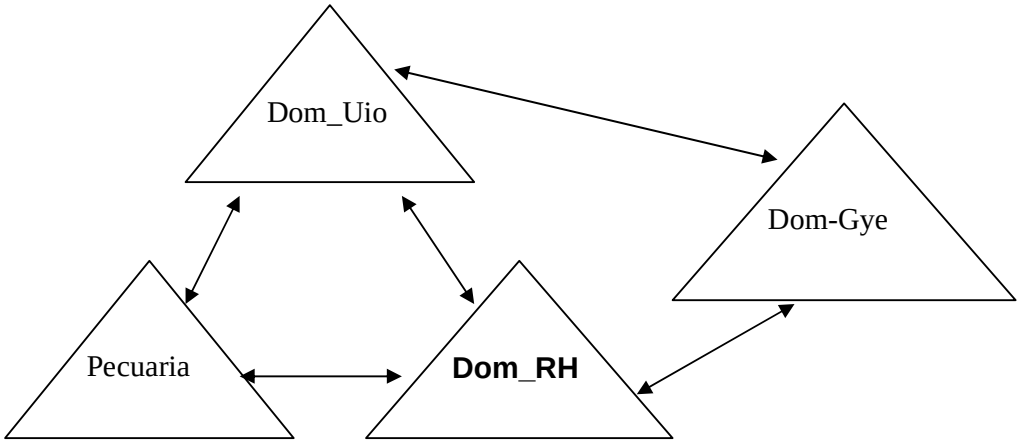

Figura 1.1. Dominios Existentes en INDUSTRIAX.

FUENTE: Inventario de recursos de red, Anexo 1

Los tres dominios en Quito están dispuestos en una LAN (red de área local) y enlazados al de Guayaquil por una WAN (red de área amplia). Todos los dominios están enlazados por relaciones de confianza bidireccionales[4], de tal manera que los usuarios de un dominio puedan acceder a los recursos de otro.

[4] Ver glosario de términos

1.1.4. CORREO ELECTRÓNICO

Este servicio de red es provisto por un servidor de correo Lotus Domino 5.0, el cual se ejecuta en un servidor de Windows 2000 con dirección IP 192.168.1.2 y maneja la base de datos de todos los usuarios a nivel nacional. Este servidor no será migrado ya que en el presente piloto de migración se han considerado únicamente los servidores controladores de dominio. Luego de la migración, todas las estaciones de trabajo deberán poder conectarse a este servidor para descargar el correo.

1.1.5. SERVICIO WINS

Este servicio está levantado en el controlador principal del dominio Dom_uio y contiene la base de equipos a nivel nacional, su dirección IP es 192.168.1.244 y si será migrado.

1.1.6. SERVICIO DNS

Actualmente esta manejado por un servidor Linux cuya dirección IP es 192.168.1.250, pero este servicio deberá ser migrado a Windows 2003 ya que es mandatorio para el correcto funcionamiento del Directorio Activo (Active Directory).

1.1.7. SERVICIO DE IMPRESIÓN

Este servicio es suministrado por una compañía tercerizadora a través de un convenio IN-HOUSE[5] y por lo tanto no será migrado. El sistema operativo en el cual se ejecuta este servicio es Windows 2000.

1.1.8. SERVICIO DE INTERNET

Este servicio está instalado en un servidor Linux y está administrado por el

[5] Ver glosario de términos

servidor Proxy de este sistema operativo. La dirección IP es 192.168.1.250 y el puerto es 3128. Este servicio se mantendrá invariable.

1.1.9. ESTACIONES DE TRABAJO

En lo que se refiere a las estaciones de trabajo se tiene un ambiente mixto compuesto por estaciones Win95, Win98, Win2000 y WinXP. Y se deberá probar la convivencia de las mismas con Windows 2003 previamente a la migración.

1.1.10. SISTEMA ERP

El sistema que maneja las transacciones comerciales de la compañía es Baan[6] y se ejecuta en un servidor IBM RS600 con sistema operativo IBM AIX y con dirección IP 192.168.1.1. Las estaciones de trabajo se conectan a este servidor a través del programa Reflection y el protocolo TCP/IP[7].

1.2. INVENTARIO DE RECURSOS, USUARIOS Y GRUPOS

El piloto de migración de Windows NT 4.0 a Windows 2003 cubrirá las localidades de Quito y Guayaquil de INDUSTRIAX, por lo que a continuación se presenta un resumen del inventario de recursos, usuarios y grupos de las localidades antes mencionadas.

En la localidad de Quito, que es la matriz de INDUSTRIAX, existen 3 dominios denominados *DOM_UIO*, *PECUARIA* Y *DOM_RH*, los cuales manejan 350, 20 y 15 usuarios respectivamente. En cuanto a los servidores, se encuentran 7 servidores; de éstos, 3 son controladores de dominio y 4 son servidores de aplicación. Respecto a las estaciones de trabajo se cuenta con 350 estaciones, conformadas de la siguiente manera: 31 estaciones de trabajo con Windows 95, 59 estaciones de trabajo con Windows 98, 12 estaciones de trabajo con Windows

[6] Ver glosario de términos
[7] Ver en siglas y símbolos

Milenium, 73 estaciones de trabajo con Windows 2000 y 175 estaciones de trabajo con Windows XP.

En la localidad de Guayaquil, que es la sucursal de INDUSTRIAX, se encuentra el dominio DOM-GYE con 50 usuarios, 1 servidor controlador de dominio y 1 servidor de aplicación. En cuanto a las estaciones de trabajo, existen 12 con Windows 95, 17 con Windows 98, 2 con Windows Milenium, 3 con Windows 2000 y 16 con Windows XP.

En vista de que la aplicación que procesa todas las transacciones del negocio es el sistema Baan, el mismo que tiene su propia administración de accesos, los grupos de usuarios que se han creado en Windows NT 4.0 están orientados a controlar el acceso especialmente a servidores de archivos. Los grupos existentes son:

- En Quito: Todos, Soporte Usuarios, Ejecutivos, RRHH y Contabilidad.
- En Guayaquil: Todos, Soporte Usuarios.

Con respecto a los recursos compartidos, tanto en Quito como en Guayaquil, se tienen: carpetas de respaldo, impresoras, carpetas para distribución de software y carpetas para transferencia de archivos.
Esta información se encuentra detallada en el anexo 1.

1.3. ANÁLISIS DE LOS OBJETIVOS DEL NEGOCIO.

Para INDUSTRIAX, el objetivo es renovar sus servicios de autenticación y control de estaciones de trabajo, mediante la actualización de la plataforma de servidores Windows NT 4.0 a Windows Server 2003, para así poder aprovechar las características que en cuanto a seguridad de la información brinda este nuevo sistema operativo y de esta manera conseguir el ambiente adecuado para posteriormente implementar políticas que permitan definir entornos de trabajo seguros para los usuarios en base a las funciones que estos desempeñan dentro

del negocio.

Para alcanzar este objetivo se han definido los siguientes lineamientos:

- Enfocar los esfuerzos de todo un equipo de trabajo en el proyecto para implementar la migración a Windows Server 2003 con el menor impacto posible en las operaciones de la Compañía; de tal manera que permita mantener al máximo la continuidad de las actividades que al momento dependen de la infraestructura de servidores con Windows NT 4.0.
- Optimizar el modelo de dominios para que cumpla los requerimientos de simplicidad, administración centralizada y posibilidad de delegación de tareas.
- Centralizar las Políticas Seguridad.
- Considerar en el diseño un nivel de escalabilidad, que sea capaz de atender la carga generada por los usuarios actuales y que considere un crecimiento futuro de hasta el 50%.
- Considerar en el diseño un nivel de disponibilidad tal que, permita mantener la operación de los servicios básicos de infraestructura en el esquema 24X7.
- Mantener al menos los mismos niveles de servicio, funcionalidad e interoperabilidad[8] actuales, con otras plataformas como: BAAN, Lotus Notes y Linux[9].

1.4. ANÁLISIS DE RIESGOS DEL PROYECTO

Los integrantes del equipo y los principales patrocinadores del proyecto mediante una serie de discusiones abiertas identifican y clasifican los riesgos que pueden aparecer en el desarrollo del proyecto y luego realizan una declaración de los mismos en una lista de riesgos que además incluye el plan de mitigación, para reducir la probabilidad de ocurrencia.

[8] Ver glosario de términos
[9] Ver glosario de términos

1.4.1. RIESGO

Es la probabilidad de que ocurra alguna circunstancia adversa.

1.4.2. CUANTIFICACIÓN DE LA PROBABILIDAD DE OCURRENCIA

Es necesario cuantificar la probabilidad de que un riesgo se haga o no efectivo. Para esto es necesario realizar frecuentes discusiones entre los principales responsables del proyecto para determinar si existe una probabilidad alta media o baja de que el riesgo ocurra. Y si el riesgo ocurre, determinar si el impacto para el negocio es alto medio o bajo.
La escala de cuantificación se muestra en la siguiente tabla:

PROBABILIDAD / IMPACTO	VALOR
Alto	3
Medio	2
Bajo	1

Tabla 1.4. Ponderación de riesgos.

FUENTE: Risk Management Guide for Information Technology Systems

En base a esta escala de medición se valorará tanto la probabilidad como el impacto de cada riesgo y se calculará la exposición, la cual será el producto del valor del riesgo por el valor del impacto y podrá ir en una escala del 1 al 9, como se muestra en la tabla siguiente:

EXPOSICION	RANGO	OBSERVACIONES
Alto	6 – 9	Es considerada de alto riesgo. El sistema como tal puede seguir adelante, pero se debe tomar acciones correctivas para ser puestas en práctica tan pronto como sea posible.
Medio	3 – 6	Es considerada de riesgo medio. Se deben tomar acciones correctivas mediante un plan a ejecutarse dentro de un período de tiempo razonable.
Bajo	1 – 3	Es considerada de bajo riesgo. El Product Manager debe decidir si se toman acciones correctivas o se acepta el riesgo.

Tabla 1.5. Ponderación de la exposición.

FUENTE: Risk Management Guide for Information Technology Systems

1.4.3. DECLARACIÓN DE RIESGOS

- **Que no se cumpla el contrato**. Es posible que por varias causas no se cumpla con el contrato establecido entre INDUSTRIAX y la compañía consultora para normar la ejecución del proyecto.
  - PROBABILIDAD: 1
  - IMPACTO: 2
  - EXPOSICION: 2
  - PLAN DE MITIGACION: Redactar el contrato de una forma cuidadosa, asegurándose que todos los compromisos que contiene sean factibles.
    Renegociar el contrato o los plazos de entrega.

- **Retrasos en el avance del proyecto**. Debido a una subestimación de trabajo, una mala planificación, o la aparición de algún otro riesgo, se pueden producir retrasos.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Realizar una buena planificación.
    Aumentar el período de trabajo.

- **Dedicación no exclusiva al proyecto**. Cada miembro del grupo realiza distintas actividades y esto provoca la dedicación a tiempo parcial de los miembros del equipo al proyecto.
  - PROBABILIDAD: 3
  - IMPACTO: 2
  - EXPOSICION: 6
  - PLAN DE MITIGACION: No tener una única persona por rol.
    Repartir equitativamente el trabajo.

- **Baja temporal de algún miembro del equipo**. Todos los miembros del equipo cumplen con actividades adicionales en su lugar de trabajo, por lo que

es posible que en algún momento no se pueda contar con uno de los miembros del equipo de trabajo.

- PROBABILIDAD: 1
- IMPACTO: 3
- EXPOSICION: 3
- PLAN DE MITIGACION: No tener una única persona por rol.
  Cubrir el rol de la persona ausente distribuyendo las tareas al resto de miembros

- **Bajo nivel de conocimiento de los miembros del equipo**. Al desconocer la funcionalidad de la nueva plataforma se podrían cometer errores que comprometan la correcta implementación y administración de los procesos.
  - PROBABILIDAD: 3
  - IMPACTO: 3
  - EXPOSICION: 9
  - PLAN DE MITIGACION: Definir un plan de capacitación mínimo.
    Buscar materiales que permitan un auto estudio.
    Contratar la asesoría de expertos en el tema.

- **Limitación de Recursos de hardware en los servidores actuales**. Es posible que los servidores no dispongan de los requerimientos que la nueva plataforma exige.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Realizar inventario de hardware de los servidores.
    Determinar las características del servidor que esta nueva plataforma requiere, mediante un proceso de dimensionamiento de acuerdo al tamaño del negocio.
    Actualizar los servidores existentes o comprar nuevos equipos.

- **Limitación de recursos para disponer de un laboratorio de desarrollo y pruebas**. Para instalar un laboratorio adecuado para el ambiente de desarrollo

será necesario contar con 3 servidores y 3 estaciones de trabajo con Windows 98, 2000 y XP. Es necesario contar con todos estos recursos para validar de manera correcta todos los diseños y procedimientos de migración propuestos.

- PROBABILIDAD: 1
- IMPACTO: 3
- EXPOSICION: 3
- PLAN DE MITIGACION: Dar las especificaciones de los equipos necesarios para el ambiente de desarrollo lo antes posible para que INDUSTRIAX los pueda proporcionar.

- **Incompatibilidad de Equipos con la plataforma MS**. Que muchos de los equipos no puedan ser actualizados por bajas características en hardware y que los nuevos equipos se encuentren dentro de la lista de compatibilidad de hardware.
  - PROBABILIDAD: 2
  - IMPACTO: 3
  - EXPOSICION: 6
  - PLAN DE MITIGACION: Revisar lista de compatibilidad de hardware con Windows.
    Inventario de equipos que van a ser reutilizados.

- **Incompatibilidad parcial de los sistemas operativos actuales con la nueva plataforma**. Durante el proceso de migración, las estaciones de trabajo no serán actualizadas y por tanto no podrán usar características como Kerberos, IPSec, políticas, etc.
  - PROBABILIDAD: 3
  - IMPACTO: 2
  - EXPOSICION: 6
  - PLAN DE MITIGACION: Enfocarse en usar las características que sean compatibles con Windows 98 o inferiores.
    Instalar el programa DSClient[10] en las estaciones Windows98 o inferiores, para conseguir la compatibilidad de estas con el Directorio Activo.

[10] Ver glosario de términos

- **Limitación en los enlaces de datos de la red WAN que no permitan una replicación eficiente del Directorio Activo**. Para facilitar la localización de recursos de la red y la autenticación es necesario distribuir controladores de dominio en los diferentes sitios o localidades geográficas. Esto requiere de replicación entre los distintos controladores de dominio y por tanto se necesita de un ancho de banda disponible para el efecto.
  - PROBABILIDAD: 3
  - IMPACTO: 3
  - EXPOSICION: 9
  - PLAN DE MITIGACION: Analizar las capacidades y nivel de utilización de los enlaces existentes.

    Realizar un plan de horarios de replicación de tal manera de optimizar la utilización del ancho de banda existente.

- **Que la migración de Windows NT4.0 a Windows 2003 Server afecte a las operaciones del sistema Baan**. La migración no debería afectar las operaciones del sistema Baan, ya que las estaciones de trabajo acceden directamente a este sistema a través del protocolo TCP/IP, sin embargo debido a que este sistema es crítico para las operaciones del negocio se debe realizar una prueba de funcionamiento en el laboratorio.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Realizar pruebas en el laboratorio, simulando el acceso de una estación de trabajo al servidor Baan en un ambiente Windows 2003 Server.

- **Que el servicio DNS no registre los nombres de los servidores existentes al momento en INDUSTRIAX**. El servicio DNS tiene que ser migrado de Linux a Windows 2003 y no va a poder registrar automáticamente los nombres de servidores no Windows, lo cual afectaría al servicio de Internet.
  - PROBABILIDAD: 2

- IMPACTO: 3
- EXPOSICION: 6
- PLAN DE MITIGACION: Inventario de registros del servidor actual de DNS, para ingresarlos posteriormente en el nuevo servidor de DNS.
  Realizar procedimiento de migración del servicio de DNS y probarlo en el laboratorio.

- **Que el servicio DNS no se configure correctamente y por lo tanto genere inconvenientes en la operación de aplicaciones basadas en este servicio, como son, Internet y Correo Electrónico**. Al fallar el servidor DNS, las estaciones de trabajo no van a poder ubicar a los servidores de Internet y de Lotus Notes, los cuales están registrados con un nombre DNS.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Realizar un procedimiento de configuración de DNS para la nueva plataforma y luego generar un ambiente muy semejante al real en el laboratorio de pruebas.

- **Que el servicio WINS de la nueva plataforma no funcione correctamente**. En la base de datos de WINS se registran los nombres netBIOS de los dominios, servidores y estaciones de trabajo. Al no trabajar correctamente va a provocar errores graves como: la ruptura de las relaciones de confianza entre dominios, la imposibilidad de que estaciones de trabajo Windows 98 o inferiores puedan autentificarse en el dominio y que por lo tanto no puedan acceder a los servicios de correo, impresión y archivos compartidos.
  - PROBABILIDAD: 2
  - IMPACTO: 3
  - EXPOSICION: 6
  - PLAN DE MITIGACION: Inventario de registros del servidor actual de WINS, para que de ser necesario se los ingrese manualmente en el nuevo servidor de WINS.
    Pruebas de instalación y configuración del Servicio WINS en el laboratorio.

- **Que el servicio DHCP de la nueva plataforma no funcione correctamente**. Por una configuración inadecuada del servicio DHCP, algunas estaciones de trabajo no recibirían una dirección IP y por lo tanto no podrían acceder a los servicios de la red.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 6
  - PLAN DE MITIGACION: Respaldo de configuración del servidor actual de DHCP (ámbitos, exclusiones, rangos, etc.).
    Realizar pruebas del servicio DHCP en el laboratorio.

- **Que las aplicaciones críticas del negocio como Norton Antivirus, no puedan ser movidas a Member Servers y deban mantenerse en controladores de dominio**. Pueden Existir aplicaciones críticas que al momento se encuentren en un Controlador de Dominio y que deban de ser movidas a Servidores Miembro con el fin de no sobrecargar las características de los controladores de dominio.
  - PRBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Inventario completo de aplicaciones.
    Probar diferentes ambientes con los nuevos roles de los servidores.

- **Imposibilidad de regresar al ambiente anterior en caso de falla durante la migración, por falta de respaldos y procedimientos definidos para recuperación de desastres**. No existen procesos formales de recuperación de desastres que protejan la información y esquemas de seguridad definidos actualmente en el negocio.
  - PROBABILIDAD: 1
  - IMPACTO: 3
  - EXPOSICION: 3
  - PLAN DE MITIGACION: Definir un plan de recuperación de desastres

mínimo para poder hacer un procedimiento de retorno al estado anterior (rollback) en caso de presentarse problemas en la migración.

- **Que los usuarios tengan dificultades en el uso de la red y las nuevas facilidades**. Es posible que existan ciertas dificultades con el manejo de las estaciones de trabajo por los cambios aplicados en ciertos procedimientos de operación (consolidación de varios dominios en uno solo).
  - PROBABILIDAD: 3
  - IMPACTO: 3
  - EXPOSICION: 9
  - PLAN DE MITIGACION: Definir un plan de capacitación para los usuarios críticos, en base a las nuevas funcionalidades.

    Implantar nuevas funcionalidades que no impliquen cambios sustanciales en el modo de trabajo actual de los usuarios.

    Aplicar paulatinamente las restricciones mediante el uso de políticas.

CAPÍTULO 2.

2. METODOLOGÍA FRAMEWORK DE MICROSOFT

2.1. DESCRIPCIÓN DE LA METODOLOGÍA FRAMEWORK

Luego de analizar los riesgos que conlleva realizar el Piloto de Migración desde Windows NT 4.0 hacia Windows 2003 para una red WAN para las operaciones del negocio, se ve la necesidad de apoyarse en una metodología que permita cumplir con este objetivo de una manera organizada, minimizando la presencia de problemas y resultados no deseados durante el proceso de implementación del mencionado proyecto.

En este sentido INDUSTRIAX aceptó la sugerencia de la Corporación Microsoft, de adoptar la metodología Microsoft Solution Framework (MSF), por tratarse de un producto del mismo fabricante de Windows Server 2003.
Esta metodología va a permitir determinar acciones concretas en las tareas a realizarse, así como estimar la carga de trabajo en términos de tiempo y número de personas implicadas y perfil de las mismas.

Con el fin de tener una visión más amplia, a continuación se describen los pasos que debería cumplir un proyecto según la metodología de desarrollo de proyectos de Microsoft MSF[11]:

“Fase 1: Estrategia y Alcance
Fase 2: Planificación y Prueba de Concepto
Fase 3: Estabilización

[11] Ver en siglas y símbolos

Fase 4: Despliegue”[12]

Figura 2.1. Ciclo de MSF.
FUENTE: www.informatizate.net

2.1.1. FASE 1: ESTRATEGIA Y ALCANCE

En esta fase deberían tener lugar los siguientes trabajos:

- Elaboración y aprobación de un “Documento de Alcance y Estrategia”, el mismo que debe ser un documento de consenso con la participación del mayor número de agentes implicados en el proyecto. En este documento quedarán reflejados las funcionalidades y servicios que, ineludiblemente, debe ofrecer la solución a implantar.
- Formar un “Equipo de Trabajo” para distribuir competencias y responsabilidades para cubrir áreas como: la de Diseño de Arquitectura, Pruebas de Laboratorio, Documentación, Logística y Coordinación.
- Elaborar un “Plan de Trabajo” en el cual deben marcarse fechas y contenidos para esta fase y las siguientes.
- Elaboración de una “Matriz de Riesgos” que contenga los principales riesgos detectados y un plan de mitigación.

Para un proyecto de migración a Windows 2003 se puede requerir la intervención de un Consultor de Microsoft junto con el equipo de trabajo que formen el Cliente y el socio de negocios.

En nuestro caso en particular el alcance está especificado en el plan del proyecto

[12] www.microsoft.com, Metodología Microsoft Solution Framework, http://www.microsoft.com/latam/technet/fases/msf.asp

de titulación.

2.1.2. FASE 2: PLANIFICACIÓN Y PRUEBA DE CONCEPTO.

Debe realizarse una planificación para el desarrollo del proyecto, la cual va a generar cierta documentación:

- Documento de Planificación y Diseño de Arquitectura, es el documento donde se describen en detalle los aspectos funcionales y operativos de la nueva plataforma. Si en el curso de las fases sucesivas fuera necesario revisar estos contenidos, se deberá hacer por acuerdo y conocimiento de todo el equipo de trabajo y se llevará un registro de versiones o cambios realizados.
- Documento de Plan de Laboratorio y Prueba de Concepto, contiene los diversos escenarios a simular, los criterios de validez, el control de incidencias. Es un documento dinámico, en el que se recoge la idea y la experiencia práctica al llevarla a cabo en un entorno controlado y aislado. La etapa de prueba de laboratorio concluye cuando la maqueta ofrece todos los servicios y funciones descritos en el Documento de Alcance y Estrategia.

Esta fase permitió decidir entre varios diseños de los diferentes servicios, realizar las pruebas respectivas del diseño elegido y planear como aplicarlo al negocio.

2.1.3. FASE 3: ESTABILIZACIÓN

La solución implantada en la maqueta se pasa a un entorno real de explotación, restringido en número de usuarios y en condiciones tales que se pueda llevar un control efectivo de la situación. Los objetivos fundamentales de esta fase son:

- Selección del entorno de prueba piloto. Se acordará la composición y ubicación del conjunto de máquinas y usuarios que entrarán en la prueba. Esta selección se recomienda que se haga atendiendo a la mayor variedad posible de casos, de manera que puedan aflorar el máximo de incidentes potenciales en el menor tiempo posible; sin perder de vista que la prueba piloto no es el

despliegue propiamente, sino una fase de observación en la que es absolutamente crítico establecer las causas de los errores.

- Gestión de Incidencias, ya que el éxito de la prueba piloto dependerá de que se forme un sistema que permita recoger los incidentes y la resolución de problemas para documentarlos (versionado de la plataforma).
- Revisión de la documentación final de Arquitectura ya que el documento de Planificación y Diseño de Arquitectura se puede ver alterado parcialmente como resultado de ésta fase. El documento final, aprobado por consenso, supone el principal documento del Proyecto y la culminación de los trabajos de diseño, al menos en sus líneas principales. Este documento se considerará definitivo cuando la solución puesta en marcha se muestre estable y el número de incidencias graves sea nulo.
- Elaboración de la documentación de Formación y Operaciones, con vistas al soporte post proyecto y los programas de formación a usuarios y administradores, en esta fase deben elaborarse las Guías de Usuario, de Administración y otras, cuyos contenidos deben acordarse previamente.
- Elaboración del Plan de Despliegue, en el cual se debe consensuar la fecha de finalización de la fase Piloto, y las condiciones de calidad que debe cumplir la solución final para iniciar el despliegue. En el Plan deben identificarse las fases, estrategias de implantación, fechas, tareas a realizarse, procedimientos de validación y métodos de control de incidencias.
- Elaboración del Plan de Formación, para lo cual con anterioridad al despliegue definitivo, debe haberse aprobado el Plan de Formación orientado a usuarios finales y administradores, y debe hacerse compatible con los ritmos acordados en el Plan de Despliegue.

El tiempo necesario para abordar esta fase es variable y depende en parte de factores ajenos a la complejidad de la propia solución, como es la adecuada selección del entorno de prueba y el momento del año en que tenga lugar (evitando que coincida con periodos de vacaciones o puntos de trabajo críticos como Fin de Año).

En base a esta fase se realizará un proceso de premigración para poner a prueba

el procedimiento de migración en un número reducido de equipos (departamento de sistemas). Los problemas presentados se recopilarán para posteriormente realizar las correcciones necesarias.

Debido a que los cambios se realizarán a nivel de servidores, el efecto hacia el usuario, de acuerdo a lo planificado, deberá ser mínimo; pues procesos como la autentificación van a seguir igual, por lo que las tareas con el usuario se reducirán a enviar comunicaciones mediante el correo electrónico con propósitos de información. Por otro lado para el personal de sistemas encargado de la administración de la plataforma Windows 2003, se contemplará un curso de instalación y administración del sistema operativo Windows 2003.

2.1.4. FASE 4: DESPLIEGUE

Se llevarán a cabo en esta fase los planes diseñados en la anterior fase, principalmente el de despliegue y el de formación. Los principales trabajos a conseguir son en este caso, además de los obvios (implantación de la plataforma, puesta en servicio de todas las funciones, formación a los usuarios y administradores), los siguientes:

- Continuación con las labores de recepción de incidencias, clasificación, tratamiento, resolución y distribución de fixes[13] o intervención en el sitio.
- Registro de mejoras y sugerencias, funcionalidades no cubiertas y novedades a incorporar en sucesivas versiones de la plataforma, incluyendo mejoras aportadas por los fabricantes de software (nuevas versiones o Service Packs[14], por ejemplo)
- Revisión de las Guías y manuales de usuario, rectificación de errores y obtención de los documentos de formación definitivos.
- Entrega de los documentos definitivos acordados como "deliverables"[15] en la fase de Visionamiento.
- Revisión (si procede) de la matriz de riesgos y métricas de calidad.

[13] Ver glosario de términos
[14] Ver glosario de términos
[15] Ver glosario de términos

- Finalmente, entrega del Proyecto y cierre del mismo, con o sin apertura de nuevo proyecto en base a la información y experiencia obtenidas.

La duración de la fase de despliegue, puesto que debe planificarse, no puede establecerse a priori. Depende de numerosos factores externos al propio proyecto (incluyendo factores de oportunidad política o de negocio) que pueden retardar o acelerar la conclusión.

La experiencia demuestra que no hay una relación directa entre número de máquinas y tiempo necesario para el despliegue. Los factores más relevantes en el cálculo suelen ser la dispersión o concentración geográfica, la complejidad del proceso de migración, el grado de automatización alcanzado, la experiencia y nivel de los técnicos que realizan la operación y condicionantes de calendario.

2.2. CONFORMACIÓN DEL EQUIPO DE TRABAJO

Para este proyecto se usarán los lineamientos de Microsoft Solutions Framework. Esto permitirá un mejor control y administración del proyecto debido a una forma unificada de comunicación entre los miembros del equipo de trabajo y una adecuada planeación de las fases que se deben considerar para la consecución del proyecto. Por este motivo se ha planteado la estructura del equipo de trabajo que se detalla en la siguiente tabla:

ROL	RESPONSABLE	RESPONSABILIDADES
Product Manager	Gerente Técnico de INDUSTRIAX	Conducir en la visión y alcance del proyecto. Administrar la definición de los requerimientos del cliente así como sus expectativas. Tomar decisiones, relacionando características vs. Agenda vs. recursos
Program Manager	Consultor Microsoft	Conducir los procesos de desarrollo para encajar el producto sobre el tiempo, manteniendo un reporte del avance del proyecto Administrar las especificaciones del producto Administrar y conducir

ROL	RESPONSABLE	RESPONSABILIDADES
		los riesgos del proyecto
Development	Partner (Binaria Sistemas)	Especifica las características del diseño físico. Estima tiempo y esfuerzo para completar cada característica. Prepara el producto para el despliegue o implementación
Test	Soporte Técnico de INDUSTRIAX	Asegura que todos los inconvenientes sean conocidos. Realiza las pruebas de los diseños planteados en la parte de desarrollo.
Logistic	Soporte Técnico de INDUSTRIAX	Provee de los recursos necesarios para realizar las tareas de desarrollo, prueba e implementación del producto.
User Education Manager	Gerente Técnico de INDUSTRIAX	Administra e implementa un plan de entrenamiento para los usuarios, sobre el producto.

Tabla 2.1. Conformación del Equipo de trabajo.

FUENTE: Microsoft Solution Framework, white paper

El equipo de trabajo es multidisciplinario e involucra a varias compañías, por este motivo el Product Manager deberá poner especial énfasis en un plan de comunicaciones eficientes, para garantizar una adecuada sincronización de los esfuerzos.

Todas las personas que han sido designadas en los diferentes roles han recibido una introducción a los principios de MSF y han comprendido sus responsabilidades dentro del equipo de trabajo.

2.2.1. DIMENSIONAMIENTO DEL CONTROLADOR DE DOMINIO

Previo a ubicar un controlador de dominio en los sitios asignados, se debe determinar el número de controladores de dominio requeridos y el hardware para cada controlador de dominio. Un planeamiento de capacidad de un controlador de dominio ayuda a colocar el número adecuado de controladores de dominio en los sitios y estimar los requerimientos de hardware para minimizar costos y mantener un nivel de servicio efectivo para los usuarios.

La Figura 2.2 muestra los aspectos que se deben considerar para completar el planeamiento de capacidad del Controlador de Dominio basado en Windows Server 2003.

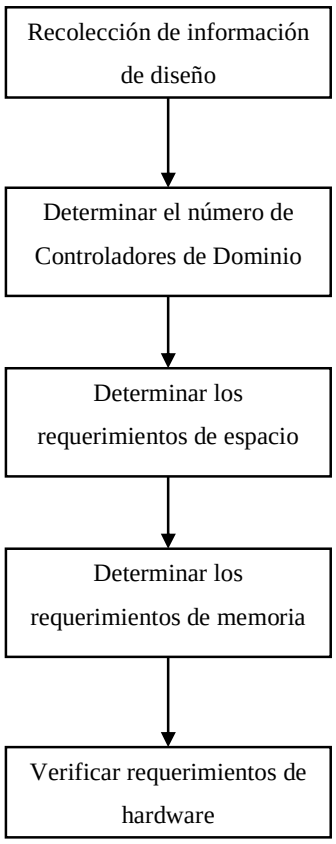

Figura 2.2. Proceso de dimensionamiento de capacidad para un controlador de dominio.
FUENTE: Microsoft Windows Server 2003 Deployment Kit

2.2.1.1. Recolección de información de diseño

Varios factores influyen en la planeación de capacidad de un controlador de dominio, incluyendo el tamaño del dominio, el número de usuarios a conectarse al dominio, el rol del controlador de dominio y los servicios instalados en este, por lo que es necesario recolectar cierta información de diseño. Esto incluye:

NUMERO DE DOMINIOS	UNO
NOMBRE DE DOMINIO	INDUSTRIAX.CORP
NOMBRES DE CADA SITIO	MATRIZ, REGIONAL GYE
NUMERO DE USUARIOS	500 USUARIOS
SERVICIOS DE RED	DNS, DHCP, WINS

Tabla 2.2. Información para dimensionar un controlador de dominio.

FUENTE: Inventario de recursos de red, Anexo 1

2.2.1.2. Determinar el mínimo número de controladores de dominio requeridos

Se puede determinar el mínimo número de controladores de dominio requeridos basados en el número de usuarios de cada sitio. Para realizar cálculos de planeamiento de capacidad, se utilizará la herramienta Adsizer[16] (Active Directory Sizer Tool) la misma que permite estimar los requerimientos de hardware para desplegar el Directorio Activo en una organización. Este estimado esta basado en los perfiles de uso de la organización y permite trabajar en base a tablas de referencia.

La Tabla 2.3 indica el CPU y la memoria que cada controlador de dominio requiere en base al número de usuarios; y cuántos de ellos se deben configurar como servidores de catálogo global.

USUARIOS EN EL SITIO	NUMERO DE CONTROLADORES DE DOMINIO	CATALOGO GLOBAL	CPU's	MEMORIA
1 – 499	Se requiere 1	El Controlador de Dominio es Catálogo Global.	1 PIII 500MHz o superior	512 MB
500 – 999	Se requiere 1	El Controlador de Dominio es Catálogo Global.	2 PIII 500MHz o superior	1 GB
1,000 – 10,000	Se requieren 2	Ambos controladores de dominio son catálogos globales.	4 PIII, XEON o superior	2 GB

[16] Ver glosario de términos

USUARIOS EN EL SITIO	NUMERO DE CONTROLADORES DE DOMINIO	CATALOGO GLOBAL	CPU's	MEMORIA
> 10,000	Se requiere 1 por cada 5,000 usuarios.	La mitad de todos los controladores de dominio son servidores de catálogo global con un mínimo de dos catálogos globales.	4 PIII, XEON o superior	2 GB

Tabla 2.3. Determinación de los Requerimientos CPU y Memoria para un Controlador de Dominio basado en el Número de Usuarios.
FUENTE: Microsoft Windows Server 2003 Deployment Kit

Basados en la tabla anterior y considerando que uno de los objetivos del negocio es la disponibilidad de servicios, el direccionamiento del CPU quedaría de la siguiente manera:

NUMERO DE USUARIOS EN DOMINIO O SITE	NECESIDADES DEL NEGOCIO	CATALOGO GLOBAL	NUMERO DE CONTROLADO-RES DE DOMINIO	CPU's
500 USUARIOS	DISPONIBLIDAD , FLEXIBILIDAD	SI	Se requieren 2	2 PIII 500MHz o superior

Tabla 2.4. Dimensionamiento del Procesador para un Controlador de Dominio.
FUENTE: Microsoft Windows Server 2003 Deployment Kit

2.2.1.3. Determinar los requerimientos de espacio en disco.

Para determinar el espacio en disco, se calcula el mínimo espacio en disco requerido para las funciones de controladores de dominio en sí y entonces se añade espacio en disco por cada función adicional alojada tal como: el catálogo global, el servicio de DNS o las particiones de directorio para aplicaciones.

Como mínimo, un controlador de dominio requiere espacio de disco para el sistema operativo, los archivos de eventos del Directorio Activo, la base de datos del Directorio Activo y el SYSVOL. A continuación veamos como determinar cuánto espacio en disco requieren estas funciones:

- En el drive que contendrá la plantilla de base de datos del Directorio Activo, NTDS.dit, se requiere un espacio disponible igual al 10% del tamaño de la base de datos existente o al menos 250MB.
- En el drive que contiene los archivos de eventos de transacción del Directorio Activo, se requiere por lo menos 50MB de espacio disponible.
- En el drive que contiene la carpeta compartida SYSVOL, requiere al menos 100MB de espacio disponible.
- En el drive que contiene el sistema de archivos Windows Server 2003, requiere por lo menos 200MB de espacio disponible.
- Con respecto a las funciones de controlador, se provee 0.4 GB de almacenamiento por cada 1000 usuarios.
- También se debe añadir espacio en disco para los controladores de dominio que quieran usarse como servidores de catálogo global. Si un bosque contiene solo un dominio, el habilitar el servicio de catálogo global en un controlador de dominio no incrementa el tamaño de la base de datos. Si el bosque contiene más de un dominio, cada dominio añade un 50% de su propio tamaño de base de datos al catálogo global.
- Adicionalmente para prevenir fallas de disco, muchas organizaciones usan arreglos redundantes de discos (RAID). Para la determinación del nivel da RAID se debe considerar que el sistema operativo demanda operaciones de lectura y escritura, los archivos de Log demandan operaciones de escritura y la Base de Datos y SYSVOL demandan principalmente operaciones de lectura. Para controladores de dominio que alojan un dominio con menos de 10, 000 usuarios, todos los cuatro componentes pueden residir en un solo arreglo RAID 1.

Con estas consideraciones, para éste caso particular, el dimensionamiento de la capacidad de almacenamiento quedaría como se muestra en el siguiente cuadro:

NUMERO DE DOMINIOS	1
NUMERO DE USUARIOS	500
PLANTILLA DE LA BASE DE DATOS DEL DA	250 MB
ARCHIVOS LOG	50 MB

CARPETA COMPARTIDA SYSVOL	100 MB
ARCHIVOS DEL SISTEMA OPERATIVO	200 MB
FUNCIONES DE CONTROLADOR DE DOMINIO	200 MB
CATALOGO GLOBAL	0 MB
NIVEL RAID	RAID 1
CAPACIDAD	2 DISCOS DE 18 GB EN RAID 1

Tabla 2.5. Dimensionamiento del disco duro para el Controlador de Dominio.

FUENTE: Microsoft Windows Server 2003 Deployment Kit

2.2.1.4. Determinar los requerimientos de memoria

Luego de determinar el número de controladores de dominio y el espacio en disco requerido, se debe determinar los requerimientos de memoria para cada controlador de dominio. La Figura 2.2 muestra los requerimientos de memoria como un paso en el proceso de planeación de la capacidad.

La Tabla 2.6 muestra un estimado comparativo del requerimiento de memoria para un controlador de dominio.

NÚMERO DE USUARIOS EN DOMINIO O SITE	NECESIDADES DEL NEGOCIO	CATÁLOGO GLOBAL	NÚMERO DE CONTROLADORES DE DOMINIO	MEMORIA
500 USUARIOS	DISPONIBLIDAD, FLEXIBILIDAD	SI	Se requieren 2	512 MB

Tabla 2.6. Requerimiento de memoria para un Controlador de Dominio.

FUENTE: Microsoft Windows Server 2003 Deployment Kit

En resumen el dimensionamiento de los equipos para el proyecto de Migración a Windows Server 2003 en base al diseño de planeamiento de capacidad y considerando la disponibilidad de equipos en el mercado, queda de la siguiente manera:

CONTROLADOR DE DOMINIO PRINCIPAL	
Tipo	2GHz/400MHz-512KB L2 Cache Upgrade con Procesador Xeon
Número de Procesadores	2
RAM	512 MB ampliable a 3 GB

CONTROLADOR DE DOMINIO PRINCIPAL	
Arreglo de Discos	RAID 1 de 2 discos
Tamaño de los discos	18 GB
Tarjetas de Red	2 de 100 Mbps

Tabla 2.7. Controlador de Dominio Principal.

CONTROLADOR ADICIONAL DE DOMINIO	
Tipo	Pentium III Xeon 933 MHz
Número de Procesadores	1
RAM	512 MB ampliable a 2 GB
Arreglo de Discos	RAID 1 de 2 discos
Tamaño de los discos	18 GB
Tarjetas de Red	1 DE 100 Mbps

Tabla 2.8. Controlador Adicional de Dominio.

CAPÍTULO 3.

3. PLANEACIÓN Y DISEÑO

3.1. DISEÑO DE PLAN DE BOSQUES

Introducción

Dentro del proceso de planificación de migración de INDUSTRIAX a Windows Server 2003, se requiere diseñar la estructura de bosques más adecuada que se adapte y cubra las necesidades del negocio. Para esto es necesario revisar algunos términos que van a ayudar al momento de decidir.

3.1.1. DEFINICIONES

3.1.1.1. Bosque

Un bosque es una colección de uno o más dominios del Directorio Activo. Los bosques sirven para dos propósitos principales: simplificar la interacción de los usuarios con el directorio y permitir que los dominios compartan una misma configuración, esquema y catálogo global.

3.1.1.2. Esquema Único

El esquema del Directorio Activo, define las clases de objeto y los atributos de las clases de objeto que se pueden crear en el directorio. Las clases de objeto definen a su vez los tipos de objetos que se pueden crear en el directorio. El esquema existe como un contexto de clasificación que se replica en todos los controladores de dominio del bosque.

3.1.1.3. Contenedor único de configuración

Las aplicaciones que usan el directorio almacenan información en el contenedor Configuración, la misma que se aplica a todo el bosque. Por ejemplo: el Directorio Activo almacena información acerca de la red física en el contenedor Configuración y la usa para guiar la creación de conexiones de replicación entre los controladores de dominio.

3.1.1.4. Relaciones completas de confianza

El Directorio Activo crea automáticamente relaciones transitivas y bidireccionales entre los dominios de un bosque. Los usuarios y los grupos de cualquier dominio pueden ser reconocidos por cualquier equipo miembro del bosque y se pueden incluir en grupos o listas de control de acceso (ACL).

3.1.1.5. Catálogo global único

El catálogo global contiene una copia de cada objeto de todos los dominios del bosque pero sólo incluye un conjunto seleccionado de los atributos de cada objeto. El catálogo global permite efectuar búsquedas rápidas y eficaces que abarcan todo el bosque.

3.1.1.6. Proceso de diseño del bosque

Las consideraciones principales para crear un diseño de bosques para una organización son los siguientes:

- Determinar si se requiere limitar el alcance de una relación de confianza.
- Cada usuario del bosque puede estar incluido en una lista de control de acceso en cualquier equipo del bosque. Si desea evitar que se concedan permisos a ciertos usuarios para el acceso a determinados recursos, esos usuarios deben residir en un bosque diferente del de los recursos.

3.1.1.7. Determinar el número de bosques de una red

Dependiendo de las necesidades se pueden tener entornos con único bosque o con varios bosques.

En el primer caso las tareas de administración son más sencillas. Todos los usuarios ven un único directorio en el catálogo global y si fuese necesario agregar un dominio nuevo al bosque, no se requiere efectuar la configuración de ninguna relación de confianza adicional.

El segundo caso es útil en organizaciones con sociedades conjuntas en las cuales cada administrador requiere manejar su propia configuración y por ende su propio bosque.

Otras situaciones en las cuales se requieren varios bosques pueden ser cuando hay un excesivo requerimiento de creación o eliminación de múltiples objetos produciendo que las réplicas saturen el ancho de banda y por tanto se genere una denegación de servicio.

Un bosque único es suficiente en muchas situaciones, sin embargo, si se decide la creación de bosques adicionales, los mismos deberán tener una justificación técnica válida.

3.1.2. DISEÑO DEL PLAN DE BOSQUES EN EL CASO DE ESTUDIO INDUSTRIAX

Para determinar el esquema de bosques a implementarse en INDUSTRIAX, se tiene que recordar que entre las principales necesidades del negocio están el tener una administración centralizada que permita manejar configuraciones idénticas tanto en Quito como en Guayaquil. Las tareas de administración deben ser sencillas; además los recursos de red tales como servidores de archivos e impresión deben estar disponibles a nivel nacional.
Por lo tanto, una vez que se han revisado los tipos de esquemas de bosques

disponibles, se ve que el que más se ajusta a las necesidades del negocio es “el esquema de único bosque” el cual consolidará todos los recursos, sitios y cuentas de usuario del negocio a nivel nacional. Así lo representa el gráfico que a continuación se incluye.

Figura 3.1. Diagrama de Plan de Bosques INDUSTRIAX.

3.2. DISEÑO DEL PLAN DE DOMINIOS

Introducción

Una vez definido el esquema de bosque de Windows Server 2003 es necesario determinar cuál va a ser la estructura de dominios a implantarse en INDUSTRIAX, Las definiciones que se detallan a continuación muestran las diferentes opciones para la creación de dominios.
En este documento se determinan tanto el nombre del dominio, nombre NetBIOS y nombre DNS.

3.2.1. DEFINICIONES

3.2.1.1. División en particiones del bosque

Los bosques del Directorio Activo son bases de datos distribuidas cuyas particiones son definidas mediante dominios. La división de una base de datos en partes más pequeñas y la colocación de dichas partes donde los datos son más útiles, permiten distribuir de forma eficaz la base de datos en una red de gran

tamaño.

3.2.1.2. Controladores de dominios

Al igual que en la plataforma basada en Windows NT 4.0, los servidores donde se ejecuta Windows 2003 que contienen una base de datos con los objetos del dominio y que realizan la función de autenticación se denominan controladores de dominio. Adicionalmente estos contienen una copia de los contenedores Configuración y Esquema.

3.2.1.3. Proceso de diseño del plan de dominios

Las siguientes son algunas consideraciones a tomarse en cuenta para el diseño de la estructura de dominios:

- **Alcance de la administración y políticas**
  Cada dominio tiene un grupo de administradores de dominio. Los administradores de dominio tienen un control total sobre cada objeto del dominio y estos derechos sólo son válidos dentro del dominio y no se propagan a otros dominios. Así también la Política de grupo (Group Policy Object, GPO) asociada con un dominio no se propaga automáticamente a otros dominios del bosque.
  Existen casos en los cuales se necesita que un grupo de usuarios tengan una política de seguridad diferente a la política de seguridad aplicada al resto de usuarios. Por ejemplo, los administradores podrían necesitar tener una política de contraseñas más restrictiva, por lo cual se los debería colocar en un dominio independiente que tenga relaciones de confianza con el dominio raíz.

- **Capacidad de la base de datos SAM (Administración de Cuentas de Seguridad)**
  En versiones anteriores de Microsoft Windows NT Server, la base de datos SAM tenía una limitación práctica de aproximadamente 40.000 objetos por dominio. El Directorio Activo puede llegar a usar fácilmente millones de objetos

por dominio.

- **Capacidad de delegación de la administración dentro de un dominio**
  En las versiones anteriores de Windows NT Server, para delegar la administración se usaban grupos locales integrados como el grupo de operadores de cuentas o se creaban múltiples dominios con distintos grupos de administradores de dominio. Así por ejemplo, para delegar la administración sobre los servidores de impresión o de archivos, se creaban dominios de recursos. En Windows 2003, es posible delegar la administración de un dominio a través de las unidades organizacionales (OU), las cuales son más fáciles de usar, mover, eliminar y modificar; que los dominios.

- **Diferenciar los nombres de dominio de la Internet y de la Intranet**
  Si la organización INDUSTRIAX decide denominar a un dominio en la Intranet como INDUSTRIAX.corp, no debería crear un dominio en Internet que también se llame INDUSTRIAX.corp, ya que si un cliente de INDUSTRIAX.corp se conecta a la Intranet y a la Internet a la vez, seleccionaría el dominio que conteste primero durante la búsqueda del localizador. Para el cliente esta selección cambiaría de forma aleatoria y no se tendría la certeza de que sea la correcta.

- **Elegir un dominio raíz del bosque**
  Tras determinar cuántos dominios se colocarán en el bosque, se decidirá qué dominio será la raíz. El dominio raíz del bosque es el primero que se crea en un bosque. Los dos grupos válidos en todo el bosque, administradores de empresa (Enterprise Admins) y administradores del esquema (Schema Admins), residirán en este dominio. Si el bosque contiene sólo un dominio, éste será la raíz del bosque.

3.2.2. DISEÑO DEL PLAN DE DOMINIOS PARA EL CASO DE ESTUDIO INDUSTRIAX

Para determinar el esquema de dominios que mejor se ajuste a los requerimientos

de INDUSTRIAX, es necesario recordar que entre las necesidades del negocio está el manejar un entorno centralizado con configuraciones homogéneas a lo largo de toda la red, tanto en Quito como en Guayaquil, en donde los recursos puedan estar disponibles a nivel nacional, estableciendo para esto obviamente su respectivo control de acceso.

Así también las tareas de administración deben ser sencillas (cada dominio adicional supone una carga administrativa). Por lo tanto, se ha definido implementar un esquema de un solo dominio el cual consolidará todos los recursos, sitios y cuentas de usuario del negocio a nivel nacional y nos permitirá aprovechar su característica "Delegación de Administración" para delegar funciones administrativas al administrador de Guayaquil y disminuir la carga de trabajo en Quito.

De esta manera el dominio que administra las cuentas de usuarios de INDUSTRIAX actual en Windows NT 4.0 se mantendrá y será actualizado a Windows 2003, mientras que los dominios que almacenan recursos de red adicionales serán eliminados y sus cuentas o recursos serán consolidados en el primer dominio migrado.

Con respecto a los controladores de dominio, con el propósito de disminuir el tráfico en la red WAN y conseguir que las autenticaciones de los usuarios y equipos se realicen localmente, aquellos serán dispuestos de la siguiente manera:

CANTIDAD	CIUDAD	ROL
1	Matriz Quito	Controlador Principal de Dominio
1	Matriz Quito	Controlador Adicional de Dominio
1	Regional Guayaquil	Controlador Adicional de Dominio

Tabla 3.1. Roles de los servidores de INDUSTRIAX.

De acuerdo a la tabla anterior, el segundo servidor ubicado en Quito va a ayudar a incrementar la disponibilidad, pues hará las funciones de respaldo del servidor principal.

Adicionalmente se habilitará el catálogo global en cada controlador de dominio

existente en los principales lugares de INDUSTRIAX (Quito y Guayaquil).

En lo que tiene que ver con el nombre, en vista de que el dominio INDUSTRIAX.com ya existe publicado en Internet, se ha determinado que el nombre del dominio de Windows sea industriax.corp.

Una vez que se ha definido el número de dominios del bosque es necesario definir el dominio raíz, el cual para este caso y por tener un solo dominio, será el ya existente, es decir el dominio industriax.corp.

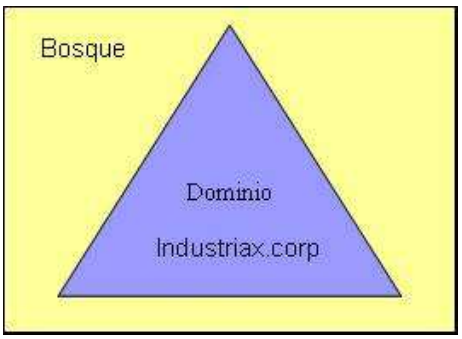

Figura 3.2. Diagrama del Plan de Dominios para IDUSTRIAX.
FUENTE: Elaborado por el autor

3.3. DISEÑO DEL PLAN DE OUs[17]

3.3.1. DEFINICIONES

3.3.1.1. Unidad Organizativa (OU)

Una Unidad Organizativa es un objeto del Directorio Activo contenido en el dominio, muy útil porque permite agrupar y organizar objetos para propósitos administrativos tales como, delegar derechos administrativos y asignar políticas.

Muchas tareas administrativas pueden simplificarse con una adecuada

[17] Ver en siglas y símbolos

distribución de los objetos en el directorio activo.

Por otro lado, para la administración de una empresa, se puede escoger entre crear una estructura de unidades organizativas (OU) o una estructura de dominios, pero hay que considerar que es mucho más eficiente manejar una estructura de Unidades Organizativas que una estructura de multidominios.

3.3.1.2. Delegación de control o administración

Sobre una Unidad Organizativa, se puede delegar un control total o parcial. Como ejemplo de una delegación total se podría tener la asignación de permisos de "Acceso Total" sobre todos los objetos de una OU; y como ejemplo de una delegación parcial podríamos tener la asignación únicamente de permisos para "Modificar" los objetos de una OU, a uno o más usuarios o grupos. Con lo que los administradores pueden disponer de la habilidad de conceder a ciertos usuarios derechos específicos, sin asignar controles totales de administración.

3.3.1.3. Jerarquía de OUs basada en funciones

Esta se basa en las funciones de trabajo de la organización sin importar la ubicación geográfica y requiere de ciertas consideraciones:

- No debe ser afectada por la reorganización de la empresa.
- Puede ser necesario crear capas adicionales para poder manejar ciertos objetos o recursos tales como usuarios, impresoras, servidores, etc.
- Esta estructura es adecuada para pequeñas organizaciones en donde el número de departamentos o funciones es reducido.

3.3.1.4. Jerarquía de OUs basada en localidades

Si la organización es centralizada y la administración de la red es geográficamente distribuida, es recomendable usar esta estructura. Presenta los siguientes beneficios:

- No es afectada por la reorganización de la empresa ya que los departamentos pueden cambiar pero las localidades muy rara vez.
- Si una organización se fusiona con otra es fácil integrar la nueva localidad dentro la estructura de dominios o unidades organizacionales.
- Esta estructura normalmente se acopla a la topología de la red, por lo tanto toma ventaja en redes donde el ancho de banda es reducido.

3.3.1.5. Jerarquía basada en una estructura combinada

Esta estructura hace uso de una combinación de las anteriores para cubrir de mejor manera las necesidades de la organización. En esta estructura se puede tener primero una distribución por localidad y luego por funciones o departamentos con lo cual se puede aplicar una delegación de administración de los recursos.

3.3.2. PROCESO DE DISEÑO DEL PLAN DE OUs.

Las siguientes son algunas consideraciones a tomarse en cuenta para el diseño de la estructura de OUs:

3.3.2.1. Decidir entre Unidades Organizacionales y Dominios

Un dominio en Windows Server 2003 es la principal unidad administrativa de la red, es usado para organizar, almacenar y dar seguridad a los recursos existentes; pero implementar una estructura de dominios, genera un nivel de administración muy complejo. Por esta razón seleccionar un modelo de unidades organizacionales podría simplificar la administración de nuestra empresa. Esto se puede observar en la siguiente figura:

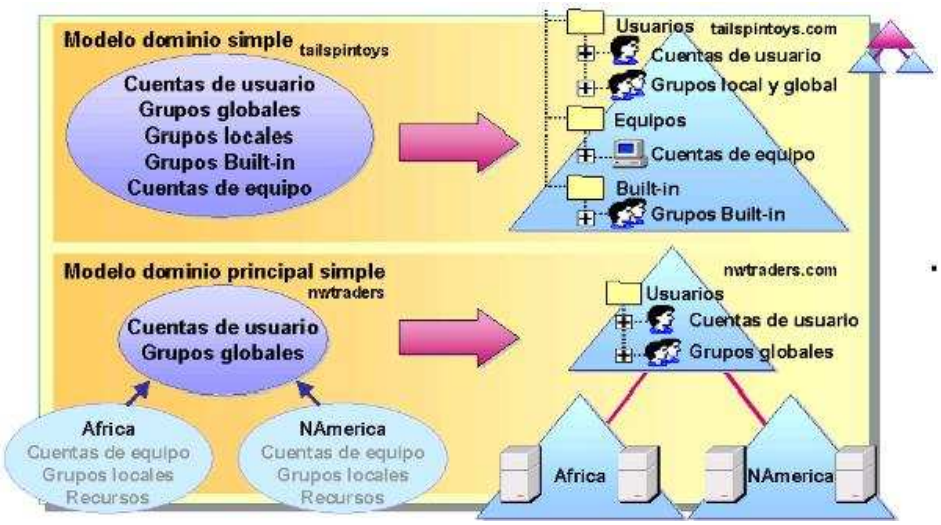

Figura 3.3. Diseño de Dominio vs. OU.

FUENTE: Managing a Microsoft Windows Server 2003 Enviroment

3.3.2.2. Determinar los niveles de la estructura de las OUs

El número de niveles de una estructura puede variar de acuerdo a la clasificación jerárquica que se escoja y de acuerdo a los requerimientos que el negocio tenga en cuanto a la aplicación de políticas y a la selección de una administración centralizada o descentralizada. Hay que recordar que mientras menor sea el número de niveles más sencilla será la administración.

3.3.2.3. Establecer el Modelo de Delegación de la Administración

En la estructura de OUs tenemos que definir el modelo de delegación de la administración, para esto tenemos que saber cuantos administradores van a ser los responsables de manejar los usuarios y los recursos de las diferentes localidades de la WAN y el rol que cada uno de ellos va a desempeñar.

Adicionalmente en este punto también se tiene que considerar si el negocio decide manejar una administración centralizada o distribuida con sus consiguientes ventajas y desventajas, pues en una administración centralizada se consigue homogeneidad y mayor restricción, mientras que en una administración distribuida se consigue reducir los tiempos y costos.

3.3.3. DISEÑO DEL PLAN DE OUS EN EL CASO DE ESTUDIO INDUSTRIAX

De acuerdo a las necesidades de la organización y a los recursos de los cuales se dispone, se ha considerado como la estructura más adecuada, una estructura de OU's mixta o híbrida compuesta de varios niveles, la misma que esta orientada a facilitar la administración y aplicación de políticas.

En el primer nivel se tiene una organización por ubicación geográfica que contempla dos unidades organizativas para Quito y Guayaquil respectivamente.

En el segundo nivel existe una organización por funciones que consta de tres unidades organizativas, una para equipos, otra para usuarios y la tercera para grupos.

Finalmente tenemos un tercer nivel compuesto por las siguientes unidades organizativas:

- Dentro de la OU *usuarios*, se tienen unidades organizativas por pisos (primero, segundo, etc.).
- Dentro de la OU *equipos*, se tienen unidades organizativas por tipo de equipo (estaciones de trabajo, portátiles, etc.).
- Dentro de la OU *grupos*, se tienen unidades por funciones (sistemas, gerentes, etc.).

Una vez definida la estructura de las unidades organizativas, se define el diseño de delegación de administración el cual va a depender de la estructura geográfica que se dispone, para nuestro caso queda definido que los administradores de Quito y Guayaquil tengan control total en las unidades organizativas Quito y Guayaquil respectivamente y que a su vez el administrador de Quito tenga un control total sobre el dominio.

El gráfico que a continuación se presenta resume la estructura de unidades organizativas que se ha definido para INDUSTRIAX:

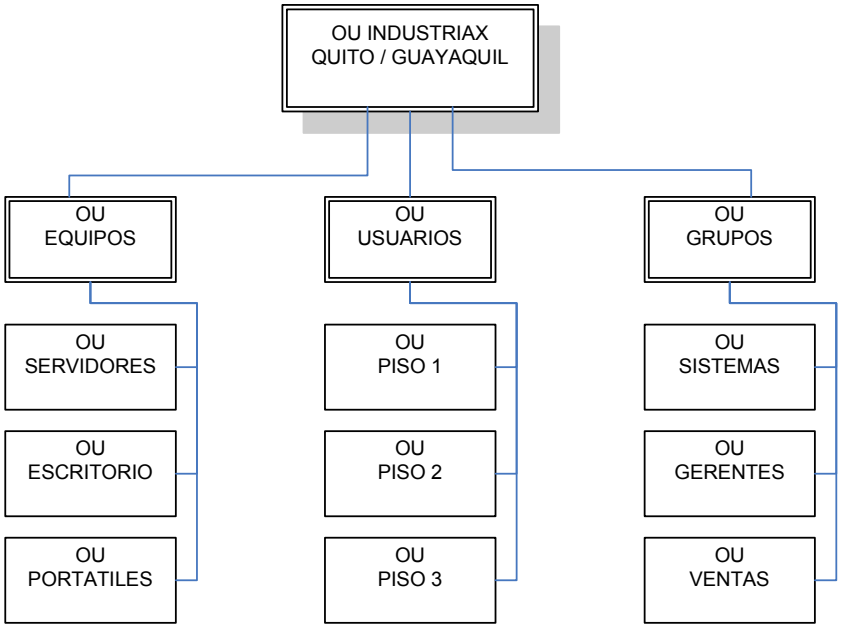

Figura 3.4. Diagrama del Plan de Unidades Organizativas para IDUSTRIAX.

FUENTE: Elaborado por el autor

3.4. DISEÑO DE TOPOLOGÍA DE REPLICACIÓN DE SITIOS

Introducción

INDUSTRIAX tiene oficinas en varias localidades distribuidas geográficamente en Ecuador, por lo que es necesario diseñar un plan de sitios que permita realizar una adecuada distribución de los Controladores de Dominio de tal manera que la autenticación de los clientes se realice localmente y en lo posible no atraviese la red WAN por un lado y por otro lado permita optimizar la ruta y el tiempo de réplica del Directorio Activo a lo largo del bosque de Windows Server 2003.

3.4.1. DEFINICIONES

3.4.1.1. Sitio

Los sitios en el directorio activo representan la estructura física (topología) de la red. El directorio activo utiliza información de topología, almacenada como objetos

de sitio y de vínculos a sitios en el directorio, para crear la topología de replicación más eficaz. Un sitio es un conjunto de subredes correctamente conectadas. Los sitios son diferentes a los dominios; los primeros representan la estructura física de la red, mientras que los segundos representan la estructura lógica de la organización.

3.4.1.2. Vínculo a sitios

Objeto del directorio activo que representa un conjunto de sitios que se pueden comunicar a un costo uniforme mediante un transporte entre sitios. Un vínculo a sitios típico conecta dos sitios a través de una WAN.

3.4.1.3. Puente de vínculo a sitios

Objeto del directorio activo que representa un conjunto de vínculos a sitios que se pueden comunicar mediante algún tipo de transporte. Son conjuntos de vínculos a sitios que se pueden tratar como una ruta única.

3.4.1.4. Replicación dentro de un sitio

El directorio activo trata la replicación en un sitio o la replicación dentro de un sitio de un modo distinto a la replicación entre sitios, porque el ancho de banda en un sitio siempre tiene una disponibilidad más inmediata. El Comprobador de coherencia de la información (KCC) del directorio activo crea la topología de replicación dentro del sitio mediante un diseño de anillo bidireccional. La velocidad de la replicación dentro del sitio se optimiza y las actualizaciones del directorio en el sitio se realizan automáticamente basándose en la notificación de cambio. A diferencia de los datos de replicación que se desplazan entre sitios, las actualizaciones de directorio dentro de un sitio no están comprimidas.

3.4.1.5. Replicación entre sitios

El directorio activo trata la replicación entre sitios de un modo distinto a la

replicación dentro de un sitio, porque el ancho de banda entre sitios suele ser más limitado. El Comprobador de coherencia de réplica (KCC) del directorio activo crea la topología de replicación entre sitios mediante un diseño de árbol de expansión con el mínimo costo. La replicación entre sitios se optimiza en vistas a la eficacia del ancho de banda y las actualizaciones del directorio entre sitios se realizan automáticamente basándose en una programación configurable. Las actualizaciones de directorio replicadas entre sitios están comprimidas para preservar el ancho de banda.

3.4.1.6. KCC[18]

El comprobador de coherencia de Réplica (KCC), es un proceso del sistema operativo que se ejecuta en todos los controladores de dominio, encargado de generar la topología de replicación del directorio activo a lo largo del bosque. La creación de la topología de replicación va a depender de si la replicación se está realizando dentro de un sitio o entre sitios.

3.4.2. UTILIDAD DEL DISEÑO DE LA TOPOLOGIA DE SITIOS

El diseño ayuda a enrutar eficientemente los requerimientos de los clientes y el tráfico de replicación del directorio activo. Un buen diseño ayudará a la organización a alcanzar los siguientes beneficios:

- Minimizar el costo de replicación de los datos del directorio activo.
- Disminuir el esfuerzo administrativo requerido para dar mantenimiento una topología de sitios.
- Programar la réplica del directorio activo entre localidades con enlaces de baja velocidad, para que se realice fuera de las horas pico y así evitar interferencia con transacciones del negocio como Baan.
- Optimizar la habilidad de los computadores clientes para localizar recursos próximos, como controladores de dominio, reduciendo el tráfico sobre los enlaces WAN y mejorando los procesos de inicio y finalización de sesión de

[18] Ver en siglas y símbolos

usuario.

3.4.3. USO DE SITIOS

Los sitios facilitan diversas actividades dentro del directorio activo, como por ejemplo:

- **Replicación.** El directorio activo sopesa la necesidad de información de directorio actualizada con la necesidad de optimización de ancho de banda replicando información dentro de un sitio con más frecuencia que entre sitios. También puede configurar el costo relativo de conectividad entre sitios para optimizar aún más la replicación.
- **Autenticación.** La información del sitio acelera y hace más eficaz la autenticación. Cuando un cliente inicia una sesión en un dominio, en primer lugar busca un controlador de dominio en su sitio local para autenticarse. Mediante el establecimiento de varios sitios, puede garantizar que los clientes se autentiquen en los controladores de dominio más cercanos a ellos, con lo que se reduce la latencia de replicación y se evita el tráfico en las conexiones WAN.
- **Replicación de SYSVOL.** El volumen del sistema SYSVOL, es una colección de carpetas del sistema, existentes en todos los controladores de dominio, que sirven como una localidad por omisión, a ciertos archivos que deben ser replicados a lo largo del dominio, como por ejemplo: políticas y scripts
- **Otros servicios proporcionados.** El directorio activo proporciona otros servicios que pueden aprovechar la información de sitios y de subred para que los clientes encuentren fácilmente los proveedores de servidor más cercanos.

3.4.4. TOPOLOGÍA DE RED

La topología del sitio de una red consiste de una o varias redes LANs y acoplamientos WAN que las conecten. La red que apoya INDUSTRIAX consiste en un grupo de LANs conectadas por acoplamientos de la red de área amplia (WAN) con un punto central en una nube frame relay, según lo mostrado en la

siguiente figura:

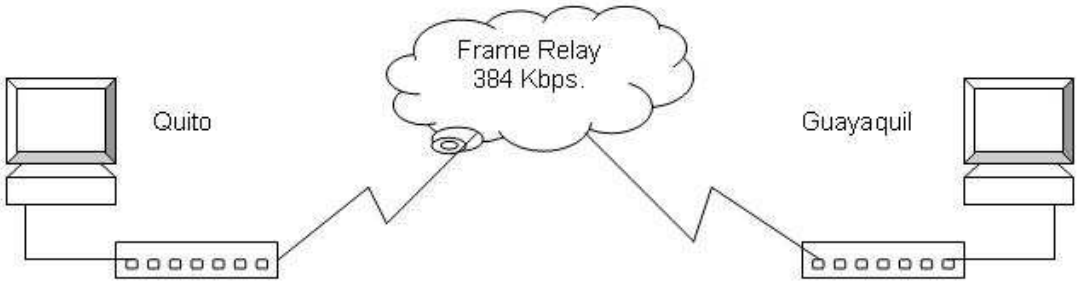

Figura 3.5. Mapa simplificado de la red WAN de INDUSTRIAX.corp.

FUENTE: Elaborado por el autor

3.4.5. DISEÑO DE LA TOPOLOGÍA DE SITIOS EN EL CASO DE ESTUDIO INDUSTRIAX

Para establecer la topología de sitios es necesario recolectar cierta información que nos va a ayudar a tomar decisiones importantes, tales como el manejo del horario de replicación y la definición de localidades como sitios.

LOCALIDADES	Quito	Guayaquil
ENLACES (Kbps)	384 Frame Relay	128 Frame Relay
SUBREDES	192.168.1.0 – 192.168.20.0	192.168.5.0
MASCARA DE SUBRED	255.255.255.0	255.255.255.0
DOMINIO	Industriax.corp	Industriax.corp
USUARIOS	350	50

Tabla 3.2. Datos necesarios en la definición de sitios.

FUENTE: Inventario de recursos de red, Anexo 1

3.4.5.1. Determinando la ubicación de los controladores de dominio

Se aconseja ubicar los controladores de dominio en localidades con un significativo número de usuarios para evitar de esta manera que se cargue el tráfico de la red con información de autenticación de usuarios.

En INDUSTRIAX, considerando que la matriz aloja a 350 clientes de red, se ha decidido que debe contener el primer controlador de dominio (1S1-DC1) para

atender los requerimientos de esta localidad. Adicionalmente se ubicará un controlador de dominio adicional (1S1-DC2) para aumentar la disponibilidad se servicios y establecer un nivel tolerancia a fallas.
En cuanto a la localidad de Guayaquil, la cual aloja a 50 usuarios, se ha decidido implementar el servicio de autenticación local a través de la ubicación de un controlador de dominio adicional (5S1-DC1), para no cargar el tráfico en la WAN.

Una vez definida la ubicación de los servidores, es importante también definir los roles que estos deben cumplir en las diferentes localidades. Así, el rol “catálogo global”, será habilitado en todos los servidores, pues este, facilita el proceso de autenticación de usuarios y las búsquedas a lo largo del bosque, sin afectar a la carga del procesador, al espacio en disco duro o al tráfico en la WAN.
El rol “emulador PDC”, que permite la compatibilidad con sistemas inferiores a Windows 2000 y que debe estar en la localidad con mayor número de usuarios, se habilitará obviamente en el controlador de dominio de Windows 2003 1S1-DC1.

Finalmente el rol “maestro de operaciones”, el cual permite aceptar ciertos requerimientos específicos como añadir o remover dominios al bosque, es habilitado por omisión en el primer controlador de dominio instalado, es decir en el controlador de dominio 1S1-DC1 ubicado en la matriz.

LOCALIDAD	Quito	Quito	Guayaquil
DOMINIO	Industriax.copr	Industriax.copr	Industriax.copr
USUARIOS	350	350	50
SUBREDES	192.168.1.0, 192.168.20.0	192.168.1.0, 192.168.20.0	192.168.5.0
NOMBRE DEL SERVIDOR	1S1-DC1	1S1-DC2	5S1-DC1
ROL MAESTRO DE OPERACIONES	Si	no	No
ROL CATALOGO GLOBAL	Si	Si	Si
ROL EMULADOR PDC	Si	no	No

Tabla 3.3. Ubicación de servidores y asignación de roles.

FUENTE: Elaborado por el autor

3.4.5.2. Asignación de localidades como sitios

Una condición para que una localidad pueda ser considerada como un sitio es que al menos disponga de un controlador de dominio, por lo tanto, de han definido como sitios, la localidad de Quito y la localidad de Guayaquil, en función del número de usuarios que estas localidades alojan.

SITIO	LOCALIDAD	SUBREDES	USUARIOS
Matriz_uio	Quito	192.16.1.0 192.168.20.0	350
Regional_gye	Guayaquil	192.168.5.0	50

Tabla 3.4. Definición de sitios.

3.4.5.3. Creación del diseño de enlaces a sitios

Es necesario conectar los sitios con enlaces a sitios, ya que esto va a permitir definir el método a utilizarse para transferir el tráfico de replicación del directorio activo. Hay que tener en cuenta que todo sitio debe estar incluido en un enlace a sitio para que pueda realizar la replicación.

Para INDUSTRIAX se ha definido crear el enlace a sitio llamado “matriz_uio-regional_gye”, el cual va a conectar los sitios matriz_uio y regional_gye.

3.4.5.4. Configuración de las propiedades del enlace a sitio

En vista de que cada enlace a sitio representa la conexión WAN entre dos o más sitios, es importante determinar cual será la configuración que más se adecue a las necesidades del negocio.
Los parámetros o propiedades a considerarse son los siguientes:

- Determinar el costo asociado a la ruta de replicación.
- Calenda rizar la réplica, decir determinar el tiempo en el que ésta se realizará.
- Determinar el intervalo de tiempo o frecuencia con la que deben realizarse las réplicas.

3.4.5.4.1. Determinando el costo

El costo de un enlace a sitio es usado en varios casos. Por ejemplo permitirá determinar qué controlador de dominio alternativo debe ser utilizado por un cliente si el de su sitio al momento no esta disponible, la selección se realizará de acuerdo al enlace a sitio que menor costo tenga.

Hay que considerar que el costo de un enlace a sitio no solamente depende del ancho de banda, sino también de la disponibilidad y latencia del enlace de datos.

Para determinar el costo de un enlace a sitios basado en la velocidad del enlace WAN, se debe utilizar la siguiente tabla:

ANCHO DE BANDA DISPONIBLE (Kbps)	**COSTO**
9.6	1042
19.2	798
38.4	644
56	586
64	567
128	486
256	425
512	378
1024	340
2048	309
4096	283

Tabla 3.5. Costos referenciales basados en la velocidad del enlace WAN.
FUENTE: Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003: A Guide for Small and Medium Organizations.

En cuanto a la confiabilidad, los enlaces menos confiables deberán tener un costo alto. Así por ejemplo, si tenemos un enlace telefónico WAN calloso, se lo debería configurar como altamente costoso para disminuir la presencia de problemas de replicación.

3.4.5.4.2. Determinación de la calendarización de replicación

Mediante la calendarización se puede controlar el horario de replicación para manejar la disponibilidad del enlace a sitio y el tráfico de replicación para evitar cargar al enlace WAN en horas pico. Tomar en cuenta que al disminuir el horario de replicación se aumenta la latencia.[19]

La calendarización definida para INDUSTRIAX se muestra en la figura de abajo. La consideración que se ha tomado en cuenta es, evitar afectar el tráfico WAN de otras aplicaciones existentes, como por ejemplo el sistema Baan.

ENLACE A SITIO	HORARIO	INTERVALO
Matriz_uio-regional_gye	18H00 – 6H00	180 min.

Tabla 3.6. Horario e intervalo de replicación de un enlace a sitio

3.4.5.4.3. Determinación del intervalo de replicación

Una vez que se ha determinado el horario de replicación es necesario indicar con que frecuencia se tiene que realizar la replica. Para establecer esta frecuencia se sugiere tener en cuenta los siguientes criterios:

- Un intervalo corto disminuye la latencia, pero incrementa tráfico en la WAN.
- Si se quiere mantener actualizadas las particiones del directorio del dominio, es preferible configurar una latencia baja.
- Si existen varios sitios, la latencia máxima de la red es la suma de las latencias de cada sitio. Por ejemplo, si la máxima latencia entre Quito y Cuenca es de 3 horas y la máxima latencia entre Quito y Guayaquil es de 4 horas, entonces la latencia máxima de la red será de 7 horas.

En INDUSTRIAX, en vista de que tanto en la localidad de Quito como en la de Guayaquil existe al menos un controlador de dominio para responder requerimientos de autenticación localmente, se ha decidido establecer el intervalo de replicación en 180 minutos, con el propósito de no sobrecargar el tráfico en la

[19] Ver glosario de términos

WAN. Este parámetro se lo puede ver en la tabla 3.6.

3.5. DISEÑO DEL PLAN DE POLITICAS (Group Polices Object, GPO)

Introducción

Los costos involucrados en administración de redes de computadores citan la pérdida de productividad de usuarios, como uno de los mayores costos en la operación de las corporaciones. Esta pérdida de productividad es frecuentemente atribuida a errores de usuario que pueden ser tan sencillos como, modificar la configuración del escritorio, o tan complejos como la no disponibilidad de aplicaciones esenciales en el desempeño del negocio.
Una de las formas de reducir este costo (Total Cost Operation, TCO) es usar Políticas de Grupo para crear entornos de clientes a la medida de sus responsabilidades. En Windows Server 2003, los administradores pueden manejar clientes de manera centralizada, usando el servicio de Directorio Activo y su soporte Políticas de Grupo.

3.5.1. DEFINICIONES

Es importante contar con varias definiciones, las mismas que van a facilitar la comprensión del presente tema. Las definiciones señaladas a continuación, han sido traducidas al español y resumidas del manual “Managing a Microsoft Windows Server 2003 Environment”.

3.5.1.1. Políticas de Grupo (Group Polices Object, GPO)

El servicio de Directorio Activo utiliza Políticas de Grupo para tres propósitos, administrar usuarios y computadores de una red, distribuir software y redireccionar carpetas como “Mis Documentos”. Al usar esta propiedad se puede definir el ambiente de trabajo de un usuario por una sola vez y luego confiar en que Windows continuamente forzará la aplicación de las configuraciones antes

definidas. La configuración de una Política de Grupo se puede aplicar a toda una organización o a grupos específicos de usuarios y computadores.

3.5.1.2. Configuración de Usuario

Es una de las opciones de Políticas de Grupo a través de la cual se puede configurar el comportamiento del sistema operativo, la apariencia del escritorio, las aplicaciones, el redireccionamiento de carpetas y la ejecución de scripts. Las políticas de usuario se aplican al momento de realizar un inicio de sesión. Contiene las siguientes opciones:

- **Configuración de Software**
  Es una carpeta que esta dentro de la opción Configuración de Usuario y que contiene los valores que serán aplicados a los programas sin importar el equipo en el que se haya iniciado sesión. Esta carpeta puede también contener los valores de instalación de los programas.

- **Configuración de Windows**
  Es una carpeta que también se encuentra dentro de la opción Configuración de Usuario y que contiene los valores que serán aplicados al sistema operativo sin importar el equipo en el que se haya iniciado sesión. Esta carpeta contiene a su vez los siguientes ítems: valores de seguridad, scripts y redireccionamiento de carpetas.

3.5.1.3. Configuración de Computador

Es la segunda opción de Políticas de Grupo a través de la cual se puede definir el comportamiento del sistema operativo, el comportamiento del escritorio, los valores de seguridad, scripts de inicio y apagado del equipo y configuración de aplicaciones. Las políticas de computador son aplicadas en el momento en el que el sistema operativo se inicializa y tienen precedencia sobre las políticas de usuario. Contiene las siguientes opciones:

- **Configuración de Software**

  Es una carpeta que se encuentra bajo el ítem Configuración de Computador y que contiene las configuraciones de software que se aplicarán a todos los usuarios que hagan logon en el computador. Así también contiene las configuraciones de instalación de software.

- **Configuración de Windows**

  Esta carpeta también esta dentro de Configuración de Computador y contiene los seteos del sistema operativo que se aplicaran a todos los usuarios que hagan logon en el computador. Este fólder también contiene ítems como: scripts y seteos de seguridad.

- **Configuración de Seguridad**

  Esta opción está disponible bajo la carpeta Configuración de Windows tanto en la Configuración de Usuarios como en la de Computadores y está compuesta de reglas o políticas que se pueden configurar para proteger los recursos sobre un computador o sobre la red. Con esta opción se pueden establecer las políticas de seguridad para una unidad organizacional, dominio o sitio.

3.5.1.4. Enlace de una Política de Grupo

Todas las políticas están almacenadas en un contenedor del Directorio Activo llamado Objeto de Políticas de Grupo (GPO). Para que una política pueda ser usada o aplicada a un sitio, dominio o unidad organizacional, la política debe ser enlazada desde el contenedor GPO. Como resultado de esto se puede conseguir administrar centralizadamente la aplicación de políticas a muchos dominios o unidades organizacionales.

3.5.1.5. Consola de Administración de Políticas (GPMC)

La herramienta Consola de Administración de Políticas de Grupo (GPMC) es usada para crear, ver y administrar GPOs, de esta manera simplifica la administración al ofrecer un único punto de acceso para la administración de

Políticas. Se Resaltan las siguientes funcionalidades:

- Una interfase de usuario que permite un uso mucho más fácil.
- Respaldo/restauración de GPOs.
- Importar/exportar y copiar/pegar GPOs.
- Reportes HTML de las configuraciones de GPO.

3.5.1.6. Jerarquía de Políticas de Grupo

Por defecto, las políticas de grupo son jerárquicas y acumulativas y afectan a todos los computadores y usuarios en un contenedor del Directorio Activo. Las GPOs son procesadas de acuerdo al siguiente orden:

1. **Política Local GPO.** Cada computador tiene exactamente un GPO almacenado localmente compartido por todos los usuarios de ese computador.

2. **Política de Sitio.** Cualquier GPO que ha sido asociado al sitio en el que el computador esté pegado es el que se procesa a continuación. Este proceso se ejecuta en el orden que ha especificado el administrador, dentro del *tab Linked Group Policy Objects*. El GPO con el menor link order es procesado al final y tiene la mayor precedencia.

3. **Política de Dominio.** El procesamiento de múltiples GPOs enlazadas al dominio se realiza en el orden especificado por el administrador.

4. **Política de Unidades Organizacionales.** Las GPOs que están enlazadas a la unidad organizacional de mayor jerarquía dentro del Directorio Activo son procesadas primero antes que las GPOs que están enlazadas a sus unidades organizacionales hijos y así sucesivamente.

3.5.2. PROCESO DE DISEÑO DEL PLAN DE POLITICAS DE GRUPO (GPO)

La delegación de autoridad, la separación de tareas administrativas, la

administración central versus la distribuida y la flexibilidad de un diseño, son factores importantes y necesarios a considerar cuando se diseña el Plan de Políticas.

3.5.2.1. Relación entre la Estructura de Unidades Organizacionales y el Uso de Políticas

De cómo se diseñe la estructura de unidades organizacionales y la aplicación de las Políticas, va a depender el buen funcionamiento administrativo de la corporación. Es por esto que en el diseño es necesario tomar en cuenta las consideraciones abajo mencionadas:

- Determinar la dimensión de la estructura de OU's, ya que en la mayoría de organizaciones, la estructura de unidades organizacionales encaja en una de las siguientes categorías:

    - Estructura de Unidades Organizacionales Planas: 1 o 2 niveles.
    - Estructura de Unidades Organizacionales Estrechas: 3 a 5 niveles.
    - Estructura de Unidades Organizacionales Profundas: Más de 5 niveles.

- Para organizaciones con requerimientos de una administración simple, es recomendable que los administradores usen un modelo simple en el cual una estructura de unidad organizacional plana con GPOs enlazadas al dominio o unidad organizacional es suficiente.
- Para organizaciones con requerimientos de administración moderada, es recomendable que los administradores usen una estructura de unidad organizacional estrecha en la que las GPOs están enlazadas al sitio, dominio o unidad organizacional con un carácter de necesario.

Además se recomienda tener en cuanta las siguientes consideraciones:

- Usar opciones de *Block Policy Inheritance*, *Enforce Policy*, *Grupos de Seguridad o Filtros WMI* para filtrar GPOs.

- Separar Usuarios y Computadores en Unidades Organizacionales Diferentes para facilitar la aplicación de políticas.
- Evitar aplicar políticas sobre los contenedores que alojan a usuarios y grupos de alta seguridad tales como *Domain Admins*, *Schema Admins*, o *Enterprise Admins*.
- Evitar Editar la GPO de Dominio por Defecto, es decir en lugar de editar la GPO de Dominio por defecto, es aconsejable crear una nueva GPO, enlazarla a la GPO de dominio y configurarla para que la nueva GPO tenga precedencia sobre la GPO de dominio por defecto.

3.5.3. DISEÑO DEL PLAN DE POLÍTICAS DE GRUPO EN EL CASO DE ESTUDIO INDUSTRIAX

Como se ha explicado anteriormente la estructura de Unidades Organizacionales asumida por INDUSTRIAX contiene 3 niveles, por lo que la podemos clasificar como una estructura estrecha. Adicionalmente a esto tenemos que recordar que entre los requerimientos del negocio están el conseguir una administración sencilla y el establecer una administración centralizada a nivel de dominio con delegación a nivel de regionales. De tal manera podemos conseguir una aplicación de políticas tanto a nivel de dominio, sitios y unidades organizacionales.

Para el caso de la compañía INDUSTRIAX, por sugerencia del Consultor Microsoft, se ha definido implementar una plantilla básica de políticas orientadas especialmente a controlar la validación de usuarios; las mismas se muestran en la tabla adjunta.

El nivel de seguridad de las políticas de cuenta se ha establecido en un estado medio para no causar un alto impacto en los usuarios de la red.
Puesto que el manejo de políticas es muy amplio y de alto impacto, el resto de políticas serán implementadas posteriormente a la migración, y solo después de un amplio análisis de requerimientos que el negocio lo realice.

3.5.3.1. Configuraciones de Seguridad en la Política de Dominio por Defecto

POLITICA	VALOR ESTABLECIDO	COMENTARIO
Políticas de Cuenta		
Enforce password history	4 password remembered	Mantiene un historial de claves
Maximum password age	90 days	Es la duración de la clave
Minimum password age	30 days	Es la duración mínima de la clave
Minimum password length	6 characters	Define la longitud mínima de la clave
Passwords must meet complexity requirements	Disabled	Si se habilita, la clave debe contener caracteres alfanuméricos
Store password using reversible encryption for all users in the domain	Disabled	La clave se guarda encriptada
Account Lockout Threshold	3	Número de intentos fallidos antes de que se bloquee la cuenta

Tabla 3.7. Políticas establecidas a nivel de password.

FUENTE: Managing a Microsoft Windows Server 2003 Enviroment

POLITICA	VALOR ESTABLECIDO	COMENTARIO
Políticas de Auditoría		
Audit Account Logon events	No Auditing	Audita los eventos de logon de cuentas
Audit Account Management	No Auditing	Audita la gestión de cuentas
Audit Directory Service Access	No Auditing	Audita el acceso al directorio activo
Audit Logon Events	No Auditing	Audita los evento de logon
Audit Object Access	No Auditing	Audita el acceso a los objetos
Audit Policy Change	No Auditing	Audita el cambio de políticas
Audit Privilege Use	No Auditing	Audita el uso de privilegios
Audit Process Tracking	No Auditing	Realiza un seguimiento a los procesos
Audit System Events	No Auditing	Audita los eventos del sistema

Tabla 3.8. Políticas establecidas a nivel de auditoria.

FUENTE: Managing a Microsoft Windows Server 2003 Enviroment

POLITICA	VALOR ESTABLECIDO	COMENTARIO
Políticas de Registro de Eventos		
Maximum application log size	10240 KB	Especifica el tamaño máximo a ser utilizado por el registro de eventos de aplicación
Maximum security log size	10240 KB	Especifica el tamaño máximo a ser utilizado por el registro de eventos de seguridad
Maximum system log size	10240 KB	Especifica el tamaño máximo a ser utilizado por el registro de eventos del sistema
Restrict guest access to application log	Enabled	Evita que la cuenta de invitado accede al registro de eventos de aplicación
Restrict guest access to security log	Enabled	Evita que la cuenta de invitado accede al registro de eventos de seguridad
Restrict guest access to system log	Enabled	Evita que la cuenta de invitado accede al registro de eventos del sistema
Shut down the computer when the security audit log is full	Disable	Si el log de auditoria se llena, el computador se apaga

Tabla 3.9. Políticas establecidas a nivel de registro de eventos.

FUENTE: Managing a Microsoft Windows Server 2003 Enviroment

POLITICA	VALOR ESTABLECIDO	COMENTARIO
Políticas de derechos de usuario		
Access this computer from the network	Administrators, Authenticated Users, Everyone	Define los usuarios y grupos que tendrán acceso al servidor desde la red. Cuando un controlador de dominio de Windows NT 4.0 es actualizado a Windows 2003, se asignan automáticamente estos derechos al grupo “usuarios autentificados”.
Add workstations to the domain	Domain Admins, technical support	Permite definir usuarios y grupos con derechos para crear cuentas de computadores.
Back up files and directories	Administrators, Backup Operators, Server Operators	Determina que usuarios pueden respaldar archivos
Bypass traverse checking	Administrators, Authenticated Users, Everyone	Determina que usuarios pueden ejecutar el asistente de instalación del directorio activo y luego son removidos

POLITICA	VALOR ESTABLECIDO	COMENTARIO
Change the system time	Administrators, Server Operators	Determina los usuarios que pueden cambiar la hora del sistema
Create a pagefile	Administrators	Determina los usuarios que pueden crear un archive de paginación
Force shutdown from a remote system	Administrators, Server Operators	Determina qué usuarios pueden apagar una estación desde una ubicación remota
Generate security audits		Determina qué cuentas pueden ser usadas por un proceso para añadir entradas al registro de eventos de seguridad
Load and unload device drivers	Administrators	Determina qué usuarios pueden cargas y descargar controladores de dispositivos
Log on locally	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	Define los grupos o usuarios que pueden iniciar una sesión local en el servidor.
Modify firmware environment variables	Administrators	Determina que usuarios pueden modificar valores de ambiente
Profile system performance	Administrators	Determina los usuarios que pueden usar herramientas de monitoreo de rendimiento
Restore files and directories	Administrators, Backup Operators, Server Operators	Determina qué usuarios pueden restaurar archivos
Take ownership of files or other objects	Administrators	Determina qué usuarios pueden tomar posesión de archivos y otros objetos
Deny Logon Locally		Determina qué usuarios no pueden realizar logon local
Deny Access to this computer from network		Determina qué usuarios no pueden acceder al computador desde la red
Remove Computer from Docking Station	Administrators	Determina los usuarios que pueden desconectar un computador portátil de la base, sin cerrar la sesión
Synchronize directory service data	Administrators	Establece quienes tienen derecho para sincronizar todos los datos del directorio activo
Shut down the system	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	Permite definir los usuarios y grupos que al iniciar una sesión en el servidor, disponen de la opción de apagar el servidor.

Tabla 3.10. Políticas establecidas a nivel de derechos de usuario.

FUENTE: Managing a Microsoft Windows Server 2003 Enviroment

3.6. DISEÑO DE ARQUITECTURA DNS

Introducción

El servicio de resolución de nombres permite que un computador, sea este una estación de trabajo o un servidor, pueda ser ubicado en la red o en el Internet por su nombre DNS y no por su dirección IP, facilitando de esta manera el acceso de los usuarios a un determinado computador.

Windows Server 2003 utiliza DNS para la resolución de nombres en lugar del Servicio de nombres de Internet de Windows (WINS) NetBIOS que utilizan las redes basadas en Windows NT 4.0.

Sigue siendo posible utilizar WINS para aplicaciones que la requieran; sin embargo, el Directorio Activo requiere DNS. El Directorio Activo utiliza los servicios de resolución de nombre que proporciona DNS para permitir a los clientes ubicar los controladores de dominio y permitir que éstos almacenen el servicio de directorio para comunicarse entre sí.

3.6.1. DEFINICIONES

Es importante contar con varias definiciones, las mismas que van a facilitar la comprensión del presente tema. Las definiciones señaladas a continuación, han sido traducidas al español y resumidas del manual “Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003. A Guide for Small and Medium Organizations”, el cual es utilizado en los cursos de entrenamiento y certificación del programa Microsoft Oficial Curriculum.

3.6.1.1. Servidor DNS Autoritario

Es un servidor DNS que hospeda una copia primaria o secundaria de los datos de la zona. Cada zona tiene al menos un servidor DNS autoritario

3.6.1.2. Redireccionamiento Condicional

Es una característica de DNS que habilita a un servidor a rutear un requerimiento de un particular nombre a otro servidor, especificando el nombre y la dirección IP. Por ejemplo el servidor DNS de industriax.corp puede ser configurado para que redireccione consultas de nombres de impsat.com a un servidor DNS que hospede la zona impsat.com.

3.6.1.3. Espacio de nombres DNS

Es la estructura jerárquica de nombres del árbol de dominios. Cada nivel de dominio que es usado en un nombre de dominio plenamente calificado (FQDN), indica un nodo o rama en el árbol de dominios. Por ejemplo, host1.industriax.corp es un FQDN que representa el nodo Host1, bajo el nodo industriax, bajo el nodo com, bajo la raíz del DNS.

3.6.1.4. Servidor DNS

Es un computador que hospeda los datos de la zona DNS, resuelve las consultas DNS y almacena temporalmente las respuestas de estas consultas.

3.6.1.5. Árbol de Dominios

En DNS, es la estructura de árbol jerárquica invertida que es usada para indexar nombres de dominio dentro de un espacio de nombres. Un árbol de dominio es similar al concepto del árbol de directorios en un sistema de archivos.

3.6.1.6. Nombre de Dominio Completamente Calificado (FQDN)

Es un nombre DNS que identifica de manera única a un nodo en el espacio de nombres DNS. El FQDN de un computador es la concatenación del nombre del computador (ejemplo, cliente1), el sufijo DNS primario del computador (ejemplo, industriax.com) y un punto final (ejemplo, Industriax.com.).

3.6.1.7. Servidor DNS Primario

Es un servidor DNS que hospeda copias de lectura - escritura de los datos de la zona, tiene una base de datos DNS con registros de los recursos y resuelve consultas DNS.

3.6.1.8. Servidor DNS Secundario

Es un servidor DNS que hospeda copias de lectura-escritura de los datos de la zona. Pero un servidor DNS secundario revisa periódicamente los cambios realizados en la zona del servidor primario y efectúa transferencias de zona de manera incremental o total, dependiendo de las necesidades que se tenga.

3.6.1.9. Zona

Es una porción contigua del árbol de dominios de la base de datos DNS que es administrada por un servidor DNS como una entidad separada. La zona contiene los registros de todos los nombres encontrados dentro de esta.

3.6.1.10. Zona de Búsqueda Inversa

Es una zona DNS autoritaria que es usada principalmente para resolver una dirección IP al nombre de un recurso de la red.

3.6.2. PLAN DE DISEÑO DEL SERVICIO DNS EN EL CASO DE ESTUDIO INDUSTRIAX

Para iniciar el diseño es necesario examinar el ambiente DNS que al momento se encuentra implementado en INDUSTRIAX. La compañía tiene una conexión al Internet de alta velocidad, un dominio registrado en Internet y el servidor DNS ejecutándose en un servidor Linux, de acuerdo al siguiente detalle:

Proveedor de Internet	Impsat
Servidor DNS del proveedor	200.31.6.34
Enlace hacia el proveedor	Frame Relay de 384 Kbps
Nombre de dominio de Internet asignado	Industriax.com
Dirección IP asignada	200.31.27.98/255.255.255.224
Dirección de Puerta de Enlace	200.31.27.97
Servidor DNS de IDUSTRIAX	192.168.1.250/255.255.255.0
Espacio de nombres actual	Industriax.com

Tabla 3.11. Parámetros del servidor DNS actual.

FUENTE: Inventario de recursos de red, Anexo 1

Es necesario también realizar un inventario de los registros existentes en el servidor DNS actual que resuelve los nombres DNS de la red local y que se ejecuta sobre el sistema operativo Linux. Los registros se detallan en la siguiente tabla:

NOMBRE	DIRECCION IP	DESCRIPCION
S_notes	192.168.1.2	Servidor de correo Quito
Server_rh	192.168.1.81	Servidor de la Intranet
Proxy	192.168.1.250	Servidor de acceso a Internet
Vanguard_6520	192.168.1.254	Ruteador o puerta de enlace
Server_gye	192.168.5.2	Servidor de correo Gye

Tabla 3.12. Registros del servidor DNS actual.

FUENTE: Inventario de recursos de red, Anexo 1

3.6.2.1. Definición de espacio de nombres

A continuación se va a determinar el espacio de nombres. Para esto se debe tomar en cuenta la estructura de dominios del directorio activo y la existencia o no de un dominio DNS externo. En el caso de INDUSTRIAX, la estructura del directorio activo consta de un solo dominio a nivel nacional; y sí existe un dominio DNS externo cuyo espacio de nombres es industriax.com, por lo que se ha decidido manejar un esquema de dos dominios DNS, uno interno y otro externo, para esto es necesario crear un espacio de nombres para manejar el dominio interno y que se lo llamará industriax.corp.

Se aconseja no reutilizar nombres existentes en Internet para nombrar los espacio

de nombres internos, ya que esto puede ocasionar errores en la resolución de nombres.

3.6.2.2. Convención de nombres

Para establecer la convención de nombres de computadores de la red, se debe considerar que éstos sean fáciles de recordar para simplificar el acceso a los recursos. En el caso de INDUSTRIAX se ha establecido la siguiente nomenclatura:

Subred del equipo, Tipo de equipo – Usuario al que pertenece el equipo

Ejemplo: **5p-jperez**

En el tipo de equipo se utiliza la “p” para describir a una estación de trabajo y la “s” para describir a un servidor, por lo tanto en el ejemplo significa que el equipo pertenece a la subred 5, que es una estación de trabajo y que pertenece al usuario jperez.

3.6.2.3. Redireccionamiento Condicional

Si un servidor DNS no tiene la información en su cache[20] o en los datos de la zona para resolver una consulta, éste redirecciona la consulta a otro servidor DNS, conocido como redireccionador (forwarder).
Como en INDUSTRIAX no se ha definido una raíz interna, se debe configurar un servidor DNS interno, para que redireccione hacia el Internet (forwarding), las consultas que no se pueden resolver localmente.

INDUSTRIAX usa el nombre industriax.com externamente y el nombre industriax.corp internamente. El servidor que hospede la zona industriax.corp va a ser el 1S1-DC1.

[20] Ver glosario de términos

Para simplificar la administración de los servidores DNS y los clientes, se ha decidido usar el redireccionamiento condicional, configurando el servidor 1S1-DC1 de la siguiente manera:

Los requerimientos que tengan como destino industriax.corp son resueltos por el servidor 1S1-DC1, mientras que todos los otros requerimientos incluyendo los que tengan como destino insdutriax.com, son redireccionados al servidor DNS del proveedor del servicio de Internet.

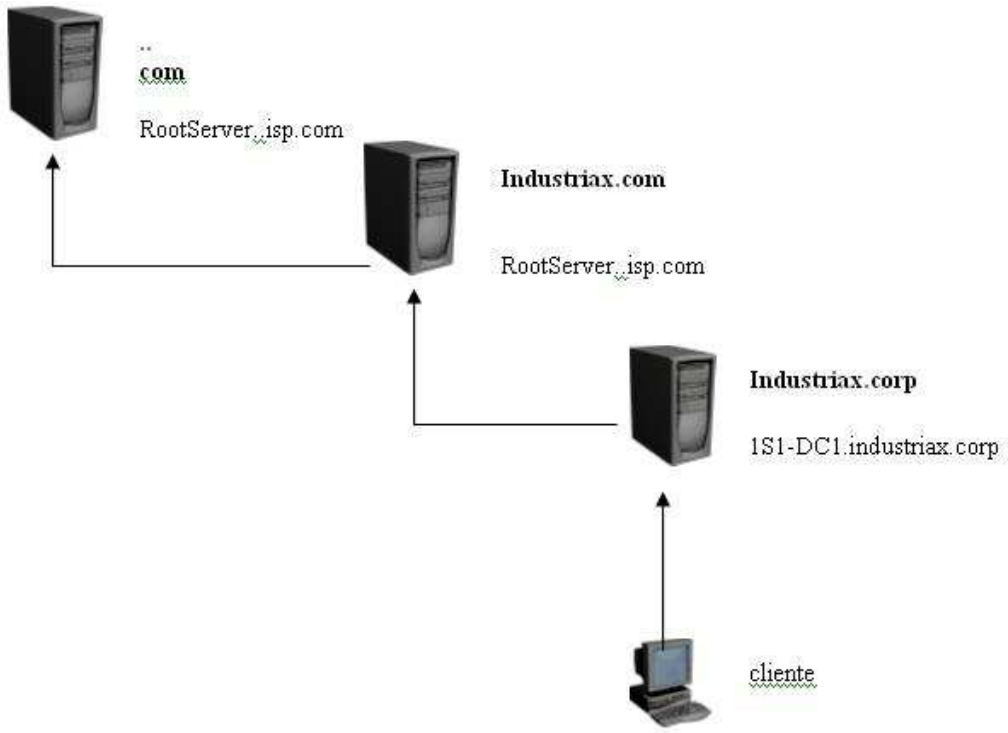

Figura 3.6. Servidor de redireccionamiento.
FUENTE: Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003.

3.6.2.4. Determinación del número de Servidores DNS

Para disminuir la carga administrativa es aconsejable utilizar el menor número de servidores posible. En este caso se utilizarán dos servidores DNS autoritarios en Quito para tener tolerancia a fallas y disponibilidad de servicios; y con el propósito de reducir el tráfico en la red entre localidades remotas, se añadirá un servidor en Guayaquil y se lo configurará como un servidor DNS secundario.

Se necesitarían añadir servidores secundarios, si la relación de servidores DNS a

clientes es muy baja y se experimentan retardos significativos en la resolución de nombres.

El servicio DNS en Windows 2003 es capaz de responder a más de 10.000 consultas por segundo sobre un procesador Pentium III de 700 MHz.

El servicio DNS se va a levantar en los controladores de dominio 1S1-DC1 y 1S1-DC2 para de esta manera poder activar la integración de zonas con el directorio activo. La distribución de los mismos se muestra en la tabla siguiente:

CIUDAD	SERVIDOR PRIMARIO	SERVIDOR SECUNDARIO
Quito	1S1-DC1 (192.168.1.244)	1S1-DC2 (192.168.1.29
Guayaquil	5S1-DC1 (192.168.5.3)	

Tabla 3.13. Distribución de servidores DNS en INDUSTRIAX.

3.6.2.5. Zonas integradas con el directorio activo

INDUSTRIAX ha elegido implementar el esquema de zonas integradas al directorio activo.
El integrar las zonas con el directorio activo permite almacenar los datos de la zona en la base de datos del directorio activo, de esta manera se aprovecha la característica de replicación multi maestro que el directorio activo tiene, es decir cualquier actualización que se haga en un controlador de dominio es replicada a todos los controladores de dominio del bosque o dominio, incluyendo la información de la zona del servidor DNS primario. Esto nos permite tener tolerancia a fallas y reducir el tráfico ya que todos los servidores DNS que están ejecutándose sobre controladores de dominio van a actuar como servidores primarios de la zona y van a aceptar actualizaciones dinámicas

3.6.2.6. Configuración y Administración de clientes DNS

Al configurar los parámetros DNS en las estaciones de trabajo es necesario especificar una lista de servidores destinados a resolver los nombres DNS. También hay que especificar la lista de sufijos que utilicen los usuarios cuando

efectúen consultas DNS de nombres de dominio no calificados.
En INDUSTRIAX se ha definido que los clientes DNS deben ser configurados con los parámetros indicados en la siguiente tabla:

PARAMETRO	QUITO	GUAYAQUIL
Servidor DNS Preferido	192.168.1.244	192.168.5.3
Servidor DNS Alternativo	192.168.1.29	192.168.1.244
Sufijo DNS	Industriax.corp	Industriax.corp

Tabla 3.14. Parámetros a configurarse en un cliente DNS.

3.7. DISEÑO DE ARQUITECTURA DHCP

Introducción

Para desarrollar este tema se han tomado ciertas definiciones, las mismas que han sido traducidas al español y resumidas del manual “Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003. A Guide for Small and Medium Organizations”.

Los computadores y otros dispositivos de red como impresoras, requieren de una dirección IP única para poder trabajar en una red corporativa. La familia de sistemas operativos Microsoft Windows Server 2003, incorpora el servicio de configuración automática del protocolo TCP/IP para clientes de red (DHCP), el cual permite tener una administración automática y centralizada de las direcciones IP y otros parámetros TCP/IP en la red.

El Implementar una solución DHCP confiable y escalable, permite reducir dramáticamente la carga administrativa y eliminar la presencia de errores comúnmente generados en la configuración del protocolo TCP/IP, tales como, direcciones IP duplicadas, máscaras de subred inválidas, etc.

La información de configuración del protocolo TCP/IP consiste de una única dirección IP, una máscara de subred, una puerta de enlace, dirección del servidor

DNS y dirección de servidor WINS. Siempre estas opciones de configuración cambian, y la configuración IP debe ser actualizada.

La implementación del servicio DHCP en una organización involucra pasos importantes como la planificación, el diseño y la implementación

3.7.1. DISEÑO DEL SERVICIO DHCP

El diseño del servicio DHCP debe cubrir las necesidades de la organización en términos de funcionalidad, disponibilidad e interoperabilidad, por lo que es necesario considerar la ubicación del servidor y la disponibilidad y desempeño del servicio.

Uno de los beneficios de ejecutar el servicio DHCP en Windows Server 2003, es tener la posibilidad de beneficiarse de las funcionalidades del servicio de Directorio Activo, tales como: actualizaciones dinámicas seguras de la base de datos DNS.

3.7.2. OPTIMIZACION DEL SERVIDOR DHCP

Demasiados requerimientos de los clientes pueden llegar a cargar excesivamente el canal de datos y la operación del servidor DHCP, por lo que se necesita optimizar el rendimiento del servidor DHCP en la organización, extendiendo el periodo de arrendamiento de la dirección IP o disponiendo de un disco duro rápido en el servidor con suficiente memoria RAM.

El extender el periodo de arrendamiento de la dirección IP hace que los requerimientos de los clientes disminuyan; y que el tráfico en la red, de esta manera, no sea exageradamente alterado. Hay que tener cuidado de no extender demasiado el periodo de arrendamiento, ya que en ciertos casos donde hay mucha rotación de equipos como por ejemplo los portátiles, se podrían llegar a agotar las direcciones IP.

3.7.3. DETERMINANDO EL NÚMERO DE SERVIDORES

En la mayoría de casos es suficiente tener un servidor DHCP, sin embargo si el número de clientes DHCP es alto y el ancho de banda en la WAN es reducido, habrá que pensar en utilizar más servidores.

Para tener una idea de cómo impacta el servicio DHCP en el hardware, consideremos que un arrendamiento requiere de aproximadamente 600 bytes para la base de datos, más 1200 bytes para respaldos.

3.7.4. INTEGRANDO DHCP CON OTROS SERVICIOS

Si se va a utilizar el servidor DHCP con clientes Microsoft, se debe usar un servicio de resolución de nombres. En este caso como se tienen clientes Windows 95, Windows 98, Windows 2000 y Windows XP, es necesario implementar tanto el servicio de resolución de nombres DNS como el servicio WINS.

DHCP y DNS trabajan juntos para efectuar actualizaciones dinámicas, así también DHCP trabaja con el directorio activo para realizar actualizaciones dinámicas DNS seguras, lo cual elimina la necesidad de actualizar manualmente los registros de la base de datos DNS cuando se han realizado cambios en la dirección IP de un cliente. DHCP también trabaja con el directorio activo para prevenir la presencia de servidores DHCP no autorizadas y de esta manera evitar que se produzcan asignaciones incorrectas de direcciones IP.

Como las versiones inferiores a Windows 2000 no soportan actualizaciones dinámicas es necesario configurar el servicio de DHCP para que actualice los registros de recursos A y PTR.

3.7.5. DFINICION DEL AMBITO DE ARRENDAMIENTO DE DIRECCIONES IP

Previo a que los clientes DHCP puedan usar un servidor DHCP para configurar dinámicamente sus parámetros TCP/IP, se debe definir y activar un ámbito para

los clientes.

Un ámbito es un rango completo de direcciones IP posibles para una subred y es utilizado para administrar la distribución de direcciones IP y la configuración de opciones DHCP.

En el proceso de definición es necesario crear un ámbito, configurar rangos de exclusión de direcciones, determinar el tiempo de arrendamiento y activar las opciones de DHCP.

3.7.5.1. Creando un ámbito de arrendamiento de direcciones IP[21]

Se debe crear un ámbito por cada subred de la red, que contenga un solo rango continuo de direcciones IP.

3.7.5.2. Rangos de Exclusión

Para evitar conflictos de direcciones IP se deben excluir las direcciones IP de dispositivos que se hayan configurado estáticamente, para que estas no sean entregadas a otros clientes DHCP. Por ejemplo se tiene que excluir la dirección del servidor DHCP,

3.7.5.3. Determinando la duración del arrendamiento

Al momento de crear un ámbito, el tiempo de arrendamiento es ajustado por omisión a ocho días, sin embargo puede ser necesario cambiar este parámetro, ya que influye en el rendimiento de la red y de los clientes DHCP.

Es aconsejable aumentar el tiempo de arriendo cuando se tienen suficientes direcciones disponibles y pocos cambios o rotación de clientes DHCP, consiguiendo de esta manera reducir el tráfico de red.

Por el contrario se sugiere reducir el tiempo de arriendo si existe un número limitado de direcciones IP disponibles y los cambios de configuración o de

[21] Ver glosario de términos

ubicación de los clientes es muy frecuente. Esto producirá un incremento en el tráfico de la red.

Duración de la Asignación	Tráfico de la Red	Liberación de IP
Incremento	Decrementa	Es más tardía
Decremento	Incrementa	Es más temprana

Tabla 3.15. Efectos de modificar el tiempo de asignación DHCP.

FUENTE: Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003.

3.7.5.4. Configurando las Opciones de DHCP

DHCP usa opciones para pasar parámetros IP adicionales a los clientes de la red. Estos parámetros incluyen: dirección IP de la puerta de enlace, dirección IP del servidor WINS, dirección IP del servidor DNS y nombre del dominio.

Los valores que se configuran manualmente en el cliente, sobrescriben las opciones DHCP de cualquier tipo.

En los clientes DHCP lo único que se debe hacer es marcar la opción “obtener una dirección IP automáticamente”

3.7.6. CREACION DE RESERVAS EN DHCP

Para los clientes que necesitan una dirección IP fija se necesita reservar dicha dirección en el servidor DHCP, realmente es un arrendamiento permanente que se utiliza para garantizar que un determinado cliente puede utilizar siempre la misma dirección IP en la red. Esta opción esta orientada para clientes que necesitan tener siempre la misma dirección. Por ejemplo: Servidor WINS, Servidor DNS, Servidor FIREWALLS, etc.

3.7.7. DISEÑO DEL SERVICIO DHCP EN EL CASO DE ESTUDIO INDUSTRIAX

En INDUSTRIAX, el servicio DHCP se encuentra actualmente levantado en un servidor Linux; pero, este deberá ser deshabilitado, para levantar el servicio en

Windows Server 2003, el cual se implementara de una manera distribuida, es decir existirá un servidor DHCP ubicado en Quito y otro en Guayaquil, para de esta manera conseguir disponibilidad, reducir el tráfico en la red y mejorar el desempeño del servicio.

El servicio DHCP se integrará con DNS para que las actualizaciones sean dinámicas, así también DHCP estará integrado con el directorio activo para prevenir la presencia de servidores DHCP no autorizadas y de esta manera evitar que se produzcan asignaciones incorrectas de direcciones IP.

UBICACIÓN	NOMBRE	DIRECCION IP	SUBRED MANEJADA
Matriz_uio	1S1-DC1	192.168.20.244	192.168.20.0
Regional_gye	5S1-DC1	192.168.5.3	192.168.5.0

Tabla 3.16. Asignación de servidores DHCP.

Con respecto a la creación de los ámbitos, estos serán dos y serán definidos de acuerdo a la siguiente tabla:

CIUDAD	Quito	Guayaquil
NOMBRE	Ámbito uio	Ámbito gye
DESCRIPCION	Subred 20	Subred 5
DIRECCION INICIAL	192.168.20.1	192.168.5.10
DIRECCION FINAL	192.168.20.253	192.168.5.253
MASCARA	255.255.255.0	255.255.255.0

Tabla 3.17. Definición de ámbitos.

En lo referente a los rangos de exclusión se ha definido excluir únicamente la dirección del servidor DHCP de Quito (192.168.20.244). Además se han considerado por el momento no utilizar las reservas de direcciones IP, pues para el caso de los servidores se ha decidido manejar direcciones fijas mediante la configuración manual de los parámetros IP en la subred 192.168.1.0, la cual maneja direcciones fijas de Quito. Y en Guayaquil se han dejado disponibles las 10 primeras direcciones de la subred 192.168.5.0 para asignarlas a equipos que puedan necesitar una dirección IP fija.

Los parámetros considerados para configurarse como opciones de DHCP, se muestran en la tabla siguiente:

OPCIONES	VALORES	VALORES
Localidad	Quito	Guayaquil
Servidor WINS primario	192.168.1.244	192.168.5.3
Servidor WINS secundario	192.168.1.29	192.168.1.244
Servidor DNS primario	192.168.1.244	192.168.5.3
Servidor DNS secundario	192.168.1.29	192.168.1.244
Dominio DNS	Industriax.corp	Industriax.corp
Puerto de enlace	192.168.1.254	192.168.5.254

Tabla 3.18. Opciones que el servidor DHCP las configura automáticamente.

En INDUSTRIAX se ha decidido mantener el tiempo de arriendo en 8 días ya que si hay disponibilidad de direcciones IP; pues se manejan 3 subredes: la 1 que es estática, la 20 que es dinámica para Quito y la 5 que es dinámica para Guayaquil.

3.8. DISEÑO DE ARQUITECTURA WINS

Introducción

El Servicio de nombres Internet de Windows (WINS) provee una solución dinámica para resolución de nombres NETBIOS (sistema de entrada/salida básico de red) en una red corporativa. Las organizaciones que aún trabajan con Windows 95, Windows 98, Windows Milenium Edition o Windows NT 4.0 deben implementar mandatoriamente una solución WINS.

3.8.1. INTERACCIÓN CON EL CLIENTE DE WINS

Debido a que el propósito de WINS es resolver nombres NetBIOS, WINS debe soportar las funciones primarias encontradas en el protocolo NetBIOS. WINS administra la funcionalidad de NetBIOS a través de cuatro distintas interacciones con el cliente WINS. La siguiente tabla lista las interacciones y describe cada una

de ellas.

INTERACCIONES	DESCRIPCION
Registrar	Durante el inicio del proceso, los clientes de WINS informan al servidor WINS por sus nombres NetBIOS y direcciones IP asociadas.
Resolver	Los clientes de WINS envían un nombre NetBIOS al servidor WINS, el servidor WINS realiza una consulta de la base de datos de WINS y entonces devuelve la dirección IP asociada con el nombre de NetBIOS.
Renovar	Los clientes de WINS contactan el servidor de WINS para prevenirlo de la expiración del registro de clientes. Cuando el registro expira, el servidor WINS automáticamente remueve la información del cliente WINS.
Liberar	Durante el proceso de apagado, los clientes WINS informan al servidor WINS la desactivación de los nombres NetBIOS asociados con el cliente de WINS.

Tabla 3.19. Interacción de los clientes WINS con el servidor.

FUENTE: Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003.

3.8.2. CONSTRUYENDO LA ESTRATEGIA DEL SERVIDOR WINS

Esto implica saber cuantos servidores WINS utilizar, y como una estrategia puede incrementar la disponibilidad y optimizar el rendimiento de WINS.

En lo referente al hardware; la velocidad del procesador y del disco duro van a influenciar el rendimiento de este servicio.

En cuanto al número de servidores requeridos, va a depender del número de usuarios existentes y de la topología de la red.

Un servidor de WINS puede típicamente puede registrar 1.500 nombres por minuto y contestar 2.500 consultas por minuto. Esto significa que un servidor

sencillo puede servir adecuadamente hasta a 10.000 clientes.

Se sugiere instalar servidores adicionales en localidades separadas por un enlace WAN de baja velocidad para reducir el tráfico en la red.

3.8.2.1. Diseño de WINS para tener alta disponibilidad

Un diseño que provea alta disponibilidad debe tener más de un servidor WINS y considerar puntos potenciales de riesgo de falla (ruteadores, servidores y enlaces) que permitan establecer la implementación de sistemas redundantes con tolerancia a fallas. Por ejemplo se podrían tener dos servidores redundantes ubicados en localidades diferentes para que de esta manera si uno falla aun se tenga disponible el segundo para atender los requerimientos de los clientes.
Al tener varios servidores se consigue disponibilidad, tolerancia a fallas y balanceo de rendimiento, en contraste con el costo y la manejabilidad.

3.8.2.2. Replicación de servidores WINS

Al utilizar dos servidores, estos se pueden configurar para que la réplica entre ellos sea: o como asociado de inserción (push) o como asociado de extracción (pull).
Cuando un servidor WINS es configurado como asociado de extracción, este periódicamente consulta al servidor socio por algún cambio disponible y se actualiza. Se sugiere utilizarlo si:

- La velocidad de WAN es baja.
- Se desea reducir el tráfico de replicación.
- Se desea una actualización de la base WINS de manera programada.

Cuando un servidor WINS es configurado como asociado de inserción, este notifica al servidor asociado que existen actualizaciones disponibles y las replica. Está orientado a utilizarse cuando:

- Se dispone de una conexión WAN de lata velocidad.
- La frecuente replicación de actualizaciones, no es crítica para el tráfico de red.
- Se requiere que las actualizaciones se reciban tan pronto como sea posible.

3.8.3. OPTIMIZANDO EL RENDIMIENTO DEL SERVICIO WINS

El servicio WINS va a generar un incremento en el tráfico entre servidores y clientes debido a la existencia de peticiones de resolución de nombres netBIOS. Esto es particularmente crítico si se usa WINS sobre redes TCP/IP ruteadas, por lo que es necesario conocer cuales son los factores que van a influir en el rendimiento del servidor, para de esta manera optimizar su operación.
Los factores son:

- Cantidad de nombres netBIOS registrados por los clientes WINS.
- Renovaciones y registros de recursos, generados por el inicio diario de los clientes.
- Efecto de usuarios móviles al moverse dentro de la red ruteada.

3.8.3.1. Reducción del tiempo de respuesta

Una de las opciones para mejorar el rendimiento es reducir el tiempo de respuesta del servidor WINS. Además debido a que el tráfico sobre la WAN en horas pico es alto, es necesario incrementar el periodo de renovación de registro de nombres netBIOS, para reducir el tráfico de renovación cliente-servidor y así mejorar el desempeño. El periodo por omisión esta configurado en seis días.

3.8.3.2. Consolidación de subredes

Si se disponen de pequeñas oficinas remotas, se aconseja no utilizar múltiples subredes, ya que esto generaría tráfico de ruteo. Por el contrario, estas oficinas remotas se deben consolidar en una sola subred mediante el uso de redes virtuales, para de esta manera reducir el tráfico asociado a WINS sobre la WAN.

3.8.3.3. Configuración de control de ráfagas

Los servidores WINS ahora permiten el control de ráfagas. Las ráfagas se producen cuando un gran número de clientes WINS intentan registrar activa y simultáneamente sus nombres locales en WINS, como cuando hay una interrupción en el suministro eléctrico. Cuando se restablece el suministro, muchos usuarios empiezan a registrar sus nombres simultáneamente en la red, lo que crea altos niveles de tráfico WINS. Gracias a la compatibilidad con el modo por ráfagas, un servidor WINS puede responder adecuadamente a estas solicitudes de los clientes, incluso antes de procesar y agregar físicamente dichas actualizaciones en la base de datos del servidor WINS.

3.8.4. INTEGRACION DE WINS CON OTROS SERVICIOS

El servicio WINS esta estrechamente relacionado con otros servicios como DNS y DHCP, por lo cual es necesario determinar de qué manera van a interactuar estos servicios.

3.8.4.1. Integración de WINS con DNS

Si la mayoría de los clientes utilizan netBIOS y los servidores tienen levantado el servicio DNS, se puede habilitar la opción “operación de búsqueda WINS” sobre el servidor DNS, para que el servidor WINS resuelva algunos nombres que el servidor DNS no encuentra en sus registros.

3.8.4.2. Integración de WINS con DHCP

Si se utilizan DHCP y WINS juntos en la red, se pueden utilizar las opciones adicionales de DHCP, para registrar los servidores WINS primario y secundario en los clientes DHCP.

Cuando se configuran estos dos servicios, hay que tomar en cuenta que el periodo de arrendamiento del servidor DHCP sea igual o mayor que el periodo de

renovación de WINS para evitar una situación en la cual el servidor WINS no note que un cliente ha liberado la dirección DHCP asignada y por lo tanto no pueda registrar este cambio en la base de datos WINS, generando una inconsistencia.

3.8.5. DISEÑO DEL SERVICIO WINS EN EL CASO DE ESTUDIO INDUSTRIAX

Actualmente en INDUSTRIAX, el servicio WINS se encuentra levantado en el controlador de dominio de respaldo SERVER2, sobre Windows NT 4.0, dando este servicio a nivel nacional, lo cual es poco funcional, por lo que es necesario rediseñarlo.

En el nuevo diseño es necesario considerar la estrategia de replicación, la cual debe ir de acuerdo a la topología o distribución física de la red, por lo tanto se ha decidido colocar dos servidores en Quito para implementar tolerancia a fallas y un servidor en Guayaquil para reducir el tráfico en la WAN y aumentar la disponibilidad. El tipo de replicación seleccionado se muestra en la siguiente tabla:

UBICACIÓN	Quito	Quito	Guayaquil
NOMBRE	1S1-DC1	1S1-DC2	5S1-DC1
DIRECCION IP	192.168.1.244	192.168.1.29	192.168.5.3
REPLICACION	Servidor Principal	Asociado Inserción/Extracción con 1S1-DC1	Asociado Inserción/Extracción con 1S1-DC1
ENLACE	Matriz	100 Mbps (LAN)	384 Kbps (WAN)
Nro. DE CLIENTES	500	500	500

Tabla 3.20. Tabla de Replicación entre servidores WINS.

En cuanto a la ubicación del servicio WINS, en vista de que se dispone de 500 clientes y un servidor de mediano tamaño puede atender hasta 10.000 clientes, este va a ser levantado en los controladores de dominio arriba mencionados.

Adicionalmente se ha considerado configurar el periodo de renovación, que tiene que ser menor que el periodo de arrendamiento DHCP, en el valor por omisión que es 6 días. Y se ha decidido habilitar la opción “control de ráfagas” para disminuir el tráfico en la red. Así como también la opción “operación de búsqueda

WINS" sobre el servidor DNS para aumentar la funcionalidad en la resolución de nombres.

Una vez que en el presente capítulo han sido definidos los diseños de los servicios de red DNS, DHCP y WINS; se puede resumir que los servidores estarán determinados como se muestra en la tabla siguiente:

SERVIDOR	SERVICIOS	DIRECCION IP	PUERTA DE ENLACE
1S1-DC1	DC Principal, DNS, DHCP, WINS	192.168.1.244/24	192.168.1.254
1S1-DC2	ADC, DNS, WINS	192.168.1.29/24	192.168.1.254
5S1-DC1	ADC, DNS, DHCP, WINS	192.168.5.3/24	192.168.5.254

Tabla 3.21. Roles y características TCP/IP de los servidores del dominio INDUSTRIAX.

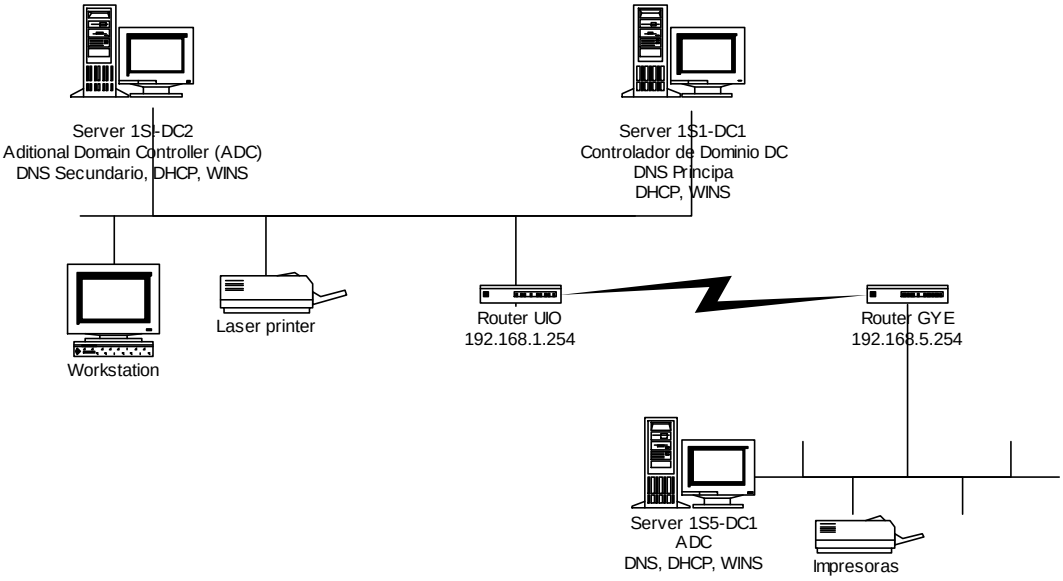

Figura 3.7. Distribución de Servicios de DNS, DHCP, WINS.

FUENTE: Elaborado por el autor

CAPÍTULO 4.

4. TEST E IMPLEMENTACÍON DEL DISEÑO

4.1.- CONSTRUCCÍON DEL LABORATORIO DE DESARROLLO

El objetivo del laboratorio de desarrollo es recrear con la mayor fidelidad parte del entorno real de producción de INDUSTRIAX, para determinar cuáles serán las fases de implantación de la estructura de Windows 2003 y así garantizar un plan que permita que el personal de Sistemas lleve a cabo una instalación exitosa de todo lo que previamente ya se ha implementado en este laboratorio.

Es por esto que se considerarán todos los casos posibles de falla y recuperación ante cualquier riesgo que se presentara.

Este documento describe todos los pasos para la consecución de este laboratorio y los requerimientos mínimos de hardware para las diferentes pruebas a realizarse. Tanto las tareas, como los requerimientos de hardware mencionados, han sido establecidos por la consultaría de Microsoft Ecuador.

4.1.1. TAREAS A REALIZARSE

1. Instalar un Controlador de Dominio de Respaldo (BDC) del Controlador Principal de Dominio (PDC) en producción y replicar las cuentas de usuarios.
2. Separar el servidor BDC del entorno de producción y promoverlo a PDC dentro del entorno de laboratorio. Este servidor se llamará SERVER1
3. Instalar un BDC del PDC de Guayaquil en producción y replicar las cuentas de usuarios.
4. Separar el servidor BDC del entorno de producción y promoverlo a PDC dentro del entorno de laboratorio. Este servidor se llamará PCSERVER315
5. Establecer la comunicación entre SERVER1 y PCSERVER315 mediante dos

ruteadores, simulando la velocidad de conexión real (128Kbps)

6. Instalar un BDC del SERVER1 y replicar cuentas de usuarios para poder hacer un rollback.
7. Unir tres estaciones de trabajo con Sistemas Operativos Windows 95/98, Windows 2000 y Windows XP.
8. Implementar los diseños establecidos en el capítulo 3 y verificar su funcionalidad

4.1.2. REQUERIMIENTOS PARA EL AMBIENTE DE LABORATORIO

Los recursos necesarios para armar el laboratorio de desarrollo se detallan en la siguiente tabla:

EQUIPOS	REQUERIMIENTOS HW	S. O.	ROL
SERVER1	Pentium III o Superior	Windows NT4.0	PDC
	256 MB RAM	Windows 2003	
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
BACKUP	Pentium III o Superior	Windows NT4.0	BDC
	256 MB RAM		
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
PCSERVER315	Pentium III o Superior	Windows NT4.0	PDC
	256 MB RAM	Windows 2003	
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		

EQUIPOS	REQUERIMIENTOS HW	S. O.	ROL
	Teclado		
	Mouse		
PC1	Pentium o Superior	Windows 95	Cliente
PC2	Pentium o Superior	Windows 2000	Cliente
PC2	Pentium o Superior	Windows XP	Cliente
	256 MB RAM		
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
Switch	8 Puertos o más		
Routers	1 puerto WAN, 1 puerto LAN		
	2 Cables DCE a DTE		
Varios	8 Cables de Red		
	Una Unidad CD Writer		
	1 punto de conexión a Internet		
	2 supresores de corriente		
	Una línea telefónica para conexión RAS		

Tabla 4.1. Recursos que conforman el laboratorio de desarrollo.

FUENTE: Requerimientos establecidos por la Consultaría de Microsoft Ecuador.

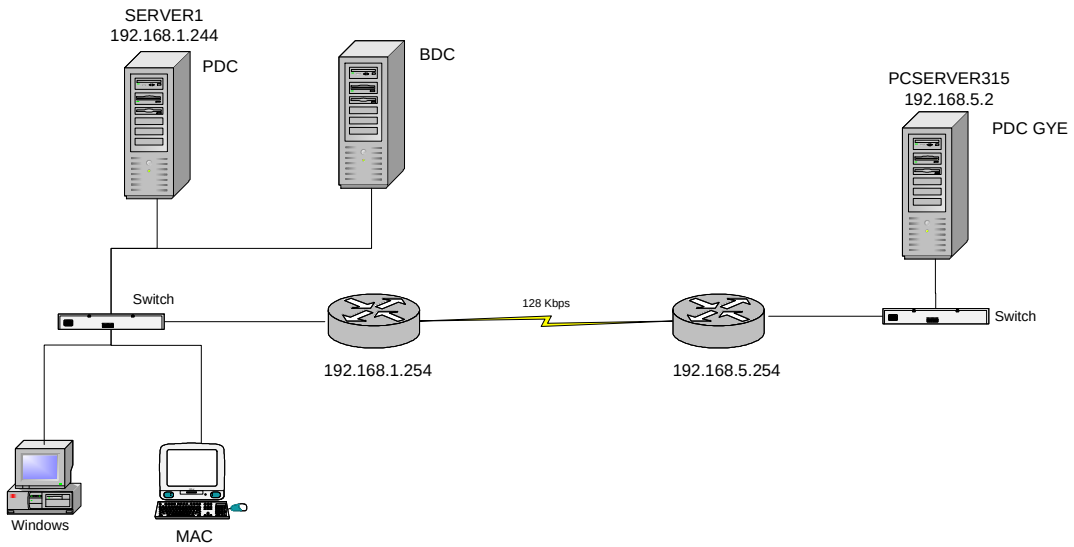

Figura 4.1. Diagrama de Entorno Inicial de Laboratorio.

FUENTE: Elaborado por el autor

4.2. CONSTRUCCIÓN DEL LABORATORIO DE PRUEBAS

Como lo indica la fase 2, “Planificación y Prueba de Concepto” de la metodología “Microsoft Solution Framework” (MSF), en el capítulo 2 del presente documento; la intención del laboratorio de pruebas es recrear parte del entorno real de producción de INDUSTRIAX en base a los diseños obtenidos en el capítulo 3, para de esta manera en primer lugar determinar que los mensionados diseños funcionan correctamente y en segundo lugar probar las diferentes fases de implantación de la estructura de Windows 2003 y así garantizar que el personal de Sistemas lleve a cabo una instalación exitosa de todo lo que previamente ya se ha probado en este laboratorio.

Es por esto que se prueban todas las fases de la implantación y en caso de que existieran errores se comunica al equipo de desarrollo para que sean resueltos a tiempo y así conseguir disminuir el impacto en las operaciones del negocio.

4.2.1. TAREAS A REALIZARSE

1. Instalar un Controlador de Dominio de Respaldo (BDC) del Controlador Principal de Dominio (PDC) en producción y replicar las cuentas de usuarios.
2. Separar el servidor BDC del entorno de producción y promoverlo a PDC dentro del entorno de laboratorio. Este servidor se llamará *SERVER1*
3. Instalar un BDC del PDC de Guayaquil de producción y replicar las cuentas de usuarios.
4. Separar el servidor BDC del entorno de producción y promoverlo a PDC dentro del entorno de laboratorio. Este servidor se llamará *PCSERVER315*
5. Establecer la comunicación entre *SERVER1* y *PCSERVER315* mediante dos ruteadores simulando la velocidad de conexión real (128Kbps)
6. Instalar un BDC del *SERVER1* y replicar cuentas de usuarios para poder hacer un rollback.
7. Unir tres estaciones de trabajo con Sistemas Operativos Windows 95/98, Windows 2000 Windows XP.

8. Implementar los procedimientos establecidos en el capítulo 3 y verificar su correcto funcionamiento.

4.2.2. REQUERIMIENTOS PARA EL AMBIENTE DE LABORATORIO

EQUIPOS	REQUERIMIENTOS HW	S. O.	ROL
SERVER1	Pentium III o Superior	Windows NT4.0	PDC
	256 MB RAM	Windows 2003	
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
BACKUP	Pentium III o Superior	Windows NT4.0	BDC
	256 MB RAM		
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
PCSERVER315	Pentium III o Superior	Windows NT4.0	PDC
	256 MB RAM	Windows 2003	
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		
	Monitor		
	Teclado		
	Mouse		
PC1	Pentium o Superior	Windows 95	Cliente
PC2	Pentium o Superior	Windows 2000	Cliente
PC3	Pentium o Superior	Windows XP	Cliente
	256 MB RAM		
	40Gb		
	Tarjeta de Red 10/100		
	CDROM		

EQUIPOS	REQUERIMIENTOS HW	S. O.	ROL
	Monitor		
	Teclado		
	Mouse		
Switch	8 Puertos o más		
Routers	1 puerto WAN, 1 puerto LAN		
	2 Cables DCE a DTE		
Varios	8 Cables de Red		
	Una Unidad CD Writer		
	1 punto de conexión a Internet		
	2 supresores de corriente		
	Una línea telefónica para conexión RAS		

Tabla 4.2. Recursos que conforman el laboratorio de pruebas.

FUENTE: Requerimientos establecidos por la Consultaría de Microsoft Ecuador.

4.3. PROCEDIMIENTO DE RECUPERACIÓN DE DESASTRES WINDOWS 2003

Introducción

Este documento nos proporciona información acerca de cómo prepararse para solucionar los problemas de arranque del sistema operativo y cómo utilizar las opciones de reparación y recuperación disponibles en Windows Server 2003. Esta información ha sido traducida y resumida del manual “Managing and Maintaining a Microsoft Windows Server 2003 Environment”.

4.3.1. PREVENCIÓN DE PROBLEMAS

Si ciertos tipos de archivos del sistema operativo se dañan, pueden surgir problemas en la operación del servidor. Estos tipos de archivos pueden ser: controladores de dispositivos, registro del sistema operativo, archivos de información del sector de inicio y archivos de arranque del sistema operativo.

Para ayudar a prevenir problemas causados por daños en archivos, realice los

pasos siguientes:

- Proteja el equipo contra variaciones e interrupciones de la alimentación eléctrica, que pueden dañar los archivos cuando se están escribiendo en el disco duro.
- Antes de instalar o implementar configuraciones poco usuales de dispositivos, controladores o configuraciones del Registro, obtenga información detallada del fabricante del dispositivo y de la Ayuda de Windows Server 2003.
- Realice copias de seguridad regulares, incluidas las copias de seguridad del Estado del sistema.

4.3.2. MÉTODOS DE RECUPERACIÓN

El sistema operativo Windows Server 2003 provee de varias herramientas de recuperación de errores, las mismas que se detallan a continuación:

- Copias de seguridad.
- Copia de seguridad del registro.
- Crear discos para iniciar un sistema deshabilitado.
- Consola de recuperación.
- Modo a prueba de fallas.
- Disco de reparación de emergencia.

4.3.2.1. Copias de seguridad

Windows Server 2003 incluye Copia de seguridad, un programa gráfico para hacer copias de seguridad y restaurar datos del usuario.

Para iniciar Copia de seguridad:

- Haga clic en *Inicio*, seleccione *Programas*, *Accesorios*, *Herramientas del sistema* y haga clic en *Copia de seguridad*, para iniciar el asistente.

- El asistente le permitirá realizar una copia de seguridad o restaurar los archivos de configuración como se muestra en la figura 4.2 (Para que este asistente siempre esté presente chequear el visto en la opción “empezar siempre en modo de asistente”).

Figura 4.2. Asistente de copia de seguridad.

- El asistente permitirá realizar una copia de seguridad de archivos, configuración del sistema y además del Estado del Sistema. Luego permitirá escoger entre toda la información del equipo (en este caso el respaldo es general de todo el disco duro, datos y disco de recuperación del sistema) o elegir lo que se desea incluir en la copia de seguridad, como se observa en la figura 4.3.

Figura 4.3. Selección de modo de respaldo.

- La opción “*elegir*” nos permitirá realizar un backup de forma selectiva de lo que deseo respaldar, con todos los servicios dentro de nuestro controlador de

dominio como se observa en la figura 4.4.

Figura 4.4. Elementos a incluir.

- En la figura 4.5 se observara la descripción del respaldo con su respectivo destino, nombre y tipo de copia de seguridad.

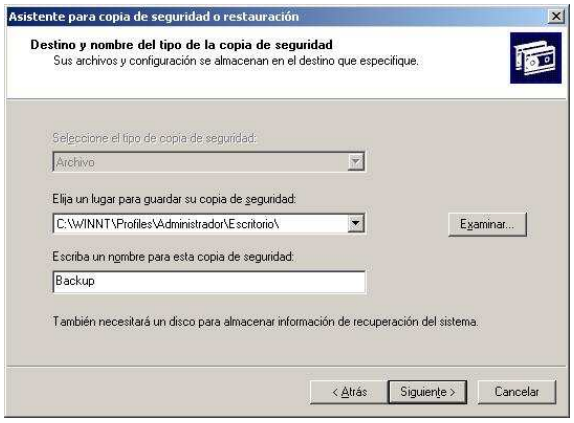

Figura 4.5. Destino y Nombre de copia de seguridad.

- Y como ultima instancia presenta el asistente de finalización incluyendo la configuración creada para la copia de seguridad como se observa en la figura 4.6.

Figura 4.6. Finalización y resumen.

4.3.2.2. Copia de seguridad del Registro

El programa Copia de seguridad para Windows Server 2003 Server incluye la opción de copia de seguridad del Estado del sistema. Al seleccionar esta opción se realiza una copia de seguridad de los siguientes elementos: archivos del sistema, registro del sistema y otros componentes del sistema como el servicio de directorio. La manera de obtener la copia se observa en la figura 4.7.

Figura 4.7. Copia de Seguridad del Estado del Sistema.

El Registro, es una base de datos estructurada jerárquicamente, que contiene información acerca de la configuración de un equipo, archivos de inicio (necesarios para iniciar el equipo) y archivos de sistema (necesarios para ejecutar el sistema operativo).

Si se trata de un controlador de dominio, encontraremos la carpeta *Sysvol* y la

base de datos de información utilizada por el directorio activo.

4.3.2.3. Creación de discos para iniciar un sistema deshabilitado

Para prepararse ante la posibilidad de que se produzca un error de sistema en un equipo que no admite el inicio desde la unidad de CD-ROM, cree discos que podrá utilizar para iniciar el equipo. Después de iniciar un equipo desactivado desde discos, tiene la opción de utilizar la Consola de recuperación o el disco de reparación de emergencia.

Puede crear discos para iniciar un sistema deshabilitado con el disco compacto de instalación de Windows Server 2003 en cualquier equipo que ejecute una versión de Windows o MS-DOS. Necesitará cuatro discos en blanco, con formato, de 3,5 pulgadas y 1,44 MB. Asígneles las etiquetas *Disco de inicio de instalación de Windows Server 2003, Disco de instalación de Windows Server 2003 nº 2, Disco de instalación de Windows Server 2003 nº 3 y Disco de instalación de Windows Server 2003 nº 4.*

No se puede utilizar discos de inicio creados a partir del disco compacto de Windows Server 2003 Professional para iniciar Windows Server 2003 Server. Los discos de inicio deben coincidir con el sistema operativo del equipo que desea iniciar.

Para crear discos para iniciar un servidor hacer lo siguiente:

1. Inserte un disco en blanco, con formato, de 1,44 MB en la unidad de disco de un equipo que esté ejecutando cualquier versión de Windows o MS-DOS.
2. Inserte el disco compacto de Windows Server 2003 Server en la unidad de CD-ROM.
3. Haga clic en *Inicio* y, después, en *Ejecutar*.
4. En *Abrir*, escriba *d:\bootdisk\makeboot a:* (donde d: es la letra asignada a la unidad de CD-ROM) y, a continuación, haga clic en *Aceptar*.
5. Siga las instrucciones que aparecerán en la pantalla.

4.3.2.4. Menú de opciones avanzadas de Windows

Windows Server 2003 proporciona una gran variedad de opciones para utilizar cuando un sistema no se inicia correctamente. En las siguientes secciones se describen las opciones que se presentan al presionar *F8* en el momento en que inicia Windows.

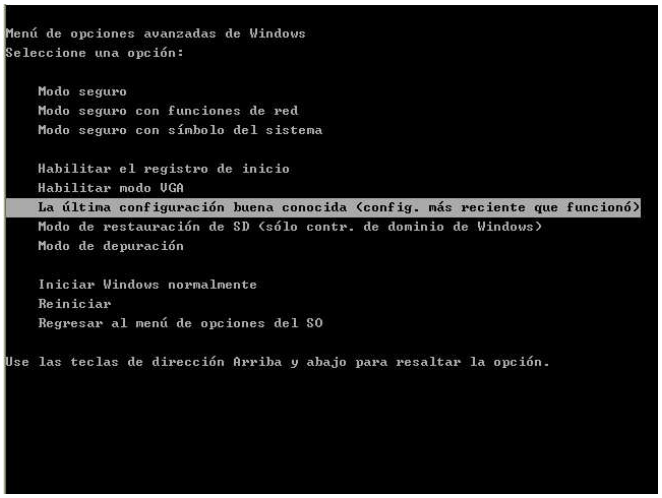

Figura 4.8. Consola de recuperación.

4.3.2.4.1. Modo a prueba de errores

Inicia Windows Server 2003 sólo con los archivos y controladores básicos, sin acceso a la red. Los controladores y archivos utilizados son para el mouse, el monitor, el teclado, el almacenamiento masivo, el vídeo base y los servicios predeterminados del sistema. El modo a prueba de errores también permite cambiar la configuración del sistema para corregir el problema (por ejemplo, quite o vuelva a configurar los controladores instalados recientemente que puedan haber causado el problema).

El modo a prueba de errores permite el acceso a todas las particiones, independientemente del sistema de archivos que se utilice: FAT, FAT32 o NTFS.

4.3.2.4.2. Modo a prueba de errores con red

Inicia Windows Server 2003 sólo con los archivos y controladores básicos, pero también incluye acceso a la red. El modo a prueba de errores con red también guarda el registro de inicio.

4.3.2.4.3. Sólo símbolo del sistema en Modo a prueba de errores

Inicia Windows Server 2003 sólo con los archivos y controladores básicos, sin acceso a la red, y muestra únicamente el símbolo del sistema. Sólo símbolo del sistema en Modo a prueba de errores también guarda el registro de inicio.

4.3.2.4.4. Habilitar el registro de inicio

Crea un registro de inicio de los dispositivos y servicios que se están cargando. El registro se guarda en un archivo denominado Ntbtlog.txt en la raíz del sistema (la carpeta en la que está instalado Windows Server 2003, que suele ser \Winnt).

4.3.2.4.5. Habilitar Modo VGA

Inicia Windows Server 2003 con el controlador básico VGA (vídeo). Este modo es útil cuando se ha instalado un nuevo controlador de tarjeta de vídeo u otro dispositivo impiden que Windows Server 2003 se inicie correctamente.

4.3.2.4.6. Última configuración válida conocida

Inicia Windows Server 2003 con la configuración (información del Registro) que Windows guardó la última vez que se cerró. Utilice la Última configuración válida conocida sólo en casos de configuración incorrecta. No se solucionan problemas causados por controladores o archivos dañados o perdidos.
Importante: Si utiliza Última configuración válida conocida, se perderán los cambios en la configuración del sistema que sean posteriores al último inicio correcto.

4.3.2.4.7. Modo Restauración de servicios de directorio

Restaura el directorio activo en un controlador de dominio. (No puede utilizar esta opción ni en Windows Server 2003 Professional ni en servidores miembros.)

4.3.2.4.1. Modo de depuración

Inicia Windows Server 2003 mientras envía información de depuración a otro equipo a través de un cable serie.

4.3.2.5. La Consola de recuperación

Si el modo a prueba de errores y otras opciones de inicio no funcionan, puede utilizar la Consola de recuperación. Sin embargo, este método sólo se recomienda si es usted es un usuario avanzado o un administrador que puede utilizar comandos básicos para identificar y localizar archivos y controladores con problemas. La Consola de recuperación es una consola de línea de comandos que puede utilizar después de iniciar el equipo con el disco compacto de instalación (si la unidad de CD-ROM del equipo lo permite) o con los discos que creó a partir del disco compacto. Para poder utilizar la Consola de recuperación, deberá iniciar una sesión con la cuenta Administrador. Entre los comandos que proporciona esta consola se incluyen comandos que permiten realizar operaciones simples como cambiar a un directorio distinto o ver un directorio, y operaciones más complejas como reparar el sector de inicio del disco duro. Para ver la Ayuda de los comandos de la Consola de recuperación, escriba *help* en el símbolo del sistema de la Consola de recuperación.

Con la Consola de recuperación, puede iniciar y detener servicios, leer y escribir datos en una unidad local (incluso en unidades con formato NTFS), copiar datos de un disco, dar formato a unidades, reparar el registro de inicio principal y realizar otras tareas administrativas. La Consola de recuperación es particularmente útil cuando hay que copiar un archivo desde un disco o CD-ROM

al disco duro para reparar el sistema o si es necesario volver a configurar un servicio que impide que el equipo se inicie correctamente. Por ejemplo, puede utilizar la Consola de recuperación para reemplazar un archivo de controlador sobrescrito o dañado por una copia en buen estado.

Para iniciar el equipo y utilizar la Consola de recuperación realice los siguientes pasos:

1. Inserte el CD-ROM de instalación de Windows Server 2003, o el primer disquete creado a partir del CD-ROM, en la unidad correspondiente. Para los sistemas que no pueden iniciarse desde la unidad de CD-ROM, debe utilizar un disquete.
2. Reinicie el equipo y, si está utilizando discos, responda a las indicaciones que solicitan cada uno de los discos por orden.
3. Cuando comience la parte de texto del programa de instalación, siga las instrucciones. Seleccione la opción de reparación; para ello presione *R*.
4. Cuando se le indique, elija la Consola de recuperación; para ello presione *C*.
5. Siga las instrucciones para volver a insertar uno o más de los discos que creó para iniciar el sistema.
6. Si utiliza un equipo con más de un sistema operativo instalado, elija la instalación de Windows Server 2003 a la cual necesita obtener acceso desde la Consola de recuperación.
7. Cuando se le indique, escriba la contraseña de Administrador.
8. En el símbolo del sistema, escriba comandos de la Consola de recuperación y, a continuación, escriba *help* para obtener una lista de comandos o *“help Nombre Comando"* para obtener ayuda acerca de un comando determinado.
9. Para salir de la Consola de recuperación y reiniciar el equipo, escriba *exit*.

4.3.2.6. El Disco de recuperación automática del Sistema.

Con “Recuperación automática del sistema” (ASR) puede crear conjuntos ASR periódicamente como parte de un plan general para recuperar el sistema en caso de que se produzca un error. Utilice ASR como último recurso para recuperar el

sistema, sólo después de haber intentado las demás opciones, como las opciones de inicio en modo de prueba de errores y la última configuración válida conocida. ASR no incluye archivos de datos. Haga copia de seguridad de los archivos de datos por separado periódicamente y restáurelos cuando el sistema esté en funcionamiento.

ASR acepta volúmenes FAT16 de hasta 2,1 GB. Si su sistema contiene particiones FAT16 de 4 GB, conviértalas de FAT16 a NTFS antes de utilizar ASR.

Los pasos siguientes pueden crear un disquete de ASR a partir de una operación de copia de seguridad de ASR:

1. Formatee un disquete de 1,44 MB e insértelo en la unidad de disquetes del equipo.
2. En *Herramientas del sistema*, inicie el programa *Copia de seguridad*. Cuando aparezca el Asistente para copia de seguridad y restauración, haga clic en *Siguiente*.
3. Haga clic en *Restaurar archivos y configuraciones* y, a continuación, en *Siguiente*.
4. En el cuadro de diálogo *Elementos a restaurar*, seleccione el medio que contiene la copia de seguridad de ASR. Asegúrese de que el medio está insertado.
5. Expanda el “Conjunto de copia de seguridad de recuperación automática del sistema” correspondiente al disquete de ASR que desea crear.
6. Expanda la segunda instancia de la letra de unidad que contiene los archivos de sistema. Expanda la carpeta *Windows / Repair*.
7. Haga clic en los archivos *Asr.sif* y *Asrpnp.sif* de esta carpeta de reparación y, después, haga clic en *Siguiente*.
8. En la pantalla “Completando el Asistente para copia de seguridad o restauración”, haga clic en *Avanzadas*.
9. En la pantalla *Dónde restaurar*, establezca *Restaurar archivos en Carpeta única* y establezca como nombre de carpeta a la raíz de la unidad de disquetes; por ejemplo, "A:\".

10. Haga clic en *Siguiente*. Las otras opciones de este asistente son opcionales y no afectan a la transferencia de archivos al disco. Cuando el asistente termine, los archivos se copiarán a la ubicación especificada previamente. El disquete de ASR ya puede utilizarse para una operación de restauración de ASR.

4.4. PROCEDIMIENTO DE MIGRACIÓN A WINDOWS 2003

Introducción

Basado en el manual "Migrating from Microsoft Windows NT Server 4.0 to Windows Server 2003. A Guide for Small and Medium Organizations" y en la experiencia de los Consultores de Microsoft Ecuador. Este documento se genera como una herramienta para mitigar los riesgos en una actualización del ambiente Windows NT Server 4.0 a Windows Server 2003. Consta de varios procedimientos y recomendaciones que ayudarán en la preparación de un dominio, previo a su actualización. Una de las tareas indispensables es conocer todos los diseños previamente preparados y aprobados para la creación del Dominio y el Bosque de INDUSTRIAX, saber las definiciones de nombres DNS y los principales servicios a implementar, las definiciones de políticas y la estructura organizativa de la compañía.

4.4.1. CONSIDERACIONES PRELIMINARES

4.4.1.2. Preparación del Dominio para la Actualización

Antes de actualizar el dominio Windows NT 4,0 de INDUSTRIAX a una estructura de Windows Server 2003 con Directorio Activo, se debe realizar un proceso de preparación. Para comenzar este proceso de preparación se deberá completar los siguientes procedimientos:

- Extraer las Cuentas de la Base de Datos de la SAM.
- Limpiar la Base de Datos de la SAM.

- Preparar el controlador de dominio para la actualización.
- Asegurar el entorno de Windows NT 4,0 antes del procedimiento de migración de servicios.
- Asegurar que la implementación del DNS soporte el directorio activo.

4.4.1.2.1. Extraer las Cuentas de la Base de Datos de la SAM

En primera instancia se partirá con la base de usuarios existente donde hay la mayor cantidad de cuentas para luego chequear, comparar, y aumentar las cuentas de otros dominios.

4.4.1.2.2. Limpiar la Base de Datos de la SAM

Los usuarios o equipos que pueden ser eliminados serán aquellos que se consideren están dentro de las siguientes consideraciones:

- Duplicación de cuentas de usuarios generadas por rotación de personal en los distintos sitios de trabajo.
- Cuentas de empleados que han dejado la organización.
- Cuentas de uso temporal que ya no se utilizan.
- Grupos de cuentas para recursos que no existen.
- Cuentas de computador sin utilizar.

4.4.1.2.3. Preparar el controlador de dominio para la actualización

Antes de actualizar un dominio a Windows Server 2003, se debe preparar el PDC y todos los BDCs en ese dominio.
Para realizar una adecuada preparación de un servidor de controlador de dominio se realizarán las siguientes tareas:

- Chequear la presencia de virus mediante el escaneo de la información con las últimas definiciones.
- Respaldar en cintas u otro dispositivo magnético o de red la información del

servidor PDC (archivos de cuentas, servicios etc.)

- Realizar un upgrade de hardware y software; este chequeo se lo hace comparando con la Hardware Compatibility List (HCL) de Windows Server 2003 y la respectiva actualización de BIOS, controladores, etc.
- Descomprimir drives: Descomprimir cualquier unidad de disco a la que se haya realizado un DriveSpace, Doublespace o software de terceros.
- Remover cualquier administrador de energía o herramientas administrativas de discos.
- Desconectar alguna Unidad de Energía Ininterrumpida (UPS) que tenga conectado vía puertos seriales.
- Deshabilitar software de terceros por ejemplo antivirus.

4.4.1.2.4. Asegurar Ambiente de Windows NT 4.0

Antes de pasar a la fase de migración de un ambiente de Windows NT 4,0 a Windows Server 2003 se deberá asegurar todo este ambiente; esto se lo define como un periodo de replicación a todos los controladores y los servidores de reserva.

4.4.1.2.5. Asegurar que la implementación del DNS soporte directorio activo

La estructura de Windows Server 2003 tiene una dependencia del Servicio de DNS, por esta razón es importante asegurarse que el DNS pueda soportar el Directorio Activo.

4.4.2. PROCEDIMIENTOS DE ACTUALIZACION

4.4.2.1. Procedimiento de Actualización desde un dominio Windows NT 4.0 a Windows Server 2003

Los pasos para llevar a efecto el procedimiento de actualización del controlador de dominio de Windows NT 4.0 a Windows Server 2003, son los que se listan a continuación:

- Asegurarse de haber cumplido con todos los pasos descritos anteriormente para la preparación del dominio Windows NT 4.0 a migrar.
- Colocar el CD de Windows Server 2003. Esto desplegará una pantalla de

  bienvenida. Se aconseja previo a ejecutar la actualización realizar un chequeo de compatibilidad del hardware.
- Una vez realizado este chequeo proceder con la ejecución de la opción de instalación. Esta acción despliega la siguiente pantalla:

Figura 4.9. Pantalla de bienvenida a la instalación.

- A continuación aparece el recuadro de Instalación de Windows preguntando el tipo de instalación que se va a realizar, escoja la opción Actualización en el cuadro de opciones y a continuación siga los pasos del asistente de la instalación.

Cabe anotar que el password de administrador una vez actualizado el Sistema operativo, sigue siendo el mismo del entorno Windows NT 4.0.

Figura 4.10. Pantalla del asistente de instalación.

4.4.2.2. Procedimiento de Actualización de la SAM de Windows NT 4.0 al directorio activo Windows Server 2003

A continuación se detallan los procesos realizados durante la actualización de la SAM de Windows NT 4.0 a Windows Server 2003 directorio activo.

- Una vez culminada la actualización del Sistema Operativo, automáticamente se da inicio al Asistente para Instalación del directorio activo. Este Asistente completará la actualización del controlador de dominio y convertirá el dominio INDUSTRIAX en un dominio del directorio activo.

Figura 4.11. Asistente para la instalación del directorio activo.

- Durante este proceso de instalación del Directorio Activo, aparece la pantalla que solicita instalar y configurar un nuevo servidor DNS. Como el directorio activo requiere que el Servicio de DNS se ejecute en este equipo, se selecciona la opción “No, sólo instalar y configurar DNS en este equipo” para que se instale este servicio y se pulsa siguiente como se muestra en la siguiente figura.

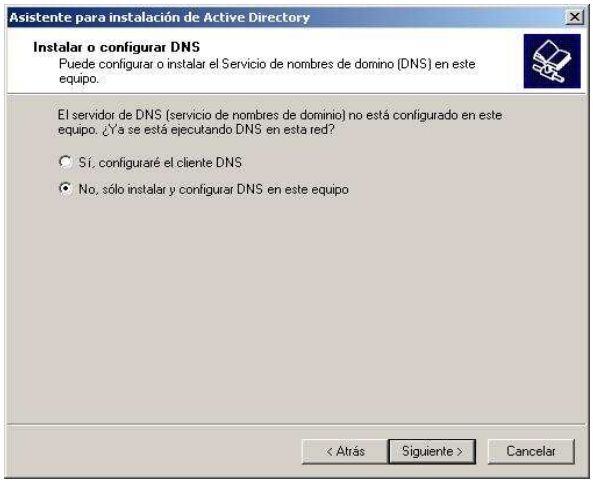

Figura 4.12. Instalación del servicio DNS.

- A continuación se especifica el nombre del nuevo espacio de nombres DNS. Por decisión de diseño, este será industriax.corp. Ingrese este nombre en el casillero dispuesto para el efecto y pulse Siguiente para continuar.
- El nivel de funcionalidad del bosque es solicitado. Se escogerá la opción de Windows 2000 para mantener la convivencia del controlador de dominio Windows Server 2003 con los dominios Windows NT 4.0 que aún permanezcan operando.
- Finalmente, se despliega un resumen de toda la configuración realizada para promover el directorio activo y completar la instalación.

Figura 4.13. Pantalla de sincronización del directorio activo.

4.5.- PROCEDIMIENTO DE ROLLBACK A WINDOWS NT 4.0

Introducción

Es importante tener presente que muchas ocasiones en los procesos de actualización, un equipo o un sistema pueden presentar problemas que eviten que la actualización sea exitosa. Para mitigar los efectos causados por estos inconvenientes es necesario contar con un proceso de RollBack o retorno al estado anterior, el mismo que debe permitir especificar los criterios a considerarse para poner en marcha el procedimiento de rollback.

4.5.1. PLAN DE RECUPERACION PARA LA ACTUALIZACION DEL DOMINIO WINDOWS NT 4.0

Un plan de recuperación o Rollback se emplea cuando en el proceso de actualización del Dominio aparecen problemas y es necesario regresar al estado operativo anterior. Por esa razón se empleará un Servidor de Reserva adicional para el dominio a migrar.

El plan de recuperación para INDUSTRIAX consiste de los pasos abajo detallados:

- Recolectar información del controlador principal de dominio de acuerdo a la siguiente tabla:

NOMBRE	Server1
LOCALIDAD	Matriz Quito
DOMINIO	DOM_UIO
ROL	Controlador principal de dominio
MEMORIA	512 MB
DISCO DURO	9 GB
DIRECCION IP	192.168.1.10
MASCARA DE SUBRED	255.255.255.0
PUERTA DE ENLACE	192.168.1.254
DIRECCION WINS	192.168.1.244
DIRECCION DNS	192.168.1.250
SERVICIOS	Autenticación
APLICACIONES	SP6
RECURSOS COMPARTIDOS	No disponible

Tabla 4.3. Recolección de datos del controlador principal de dominio.

- Generar un controlador de dominio de reserva (1S1-BDC1) a partir a partir del controlador principal de dominio *SERVER1*. Este servidor tendrá la dirección IP *192.168.1.200*.
- Revisar la información de la tabla 4.3 para Instalar aplicaciones, importar archivos de datos y levantar servicios en el servidor *1S1-DC1*, de tal manera que tenga la misma información que el servidor *SERVER1*.
- Realizar la sincronización del servidor *1S1-PDC1* con el servidor *SERVER1* para que se actualice la base de datos SAM.
- Desconectar el servidor *1S1-PDC1* de la red y guardarlo en un lugar seguro del centro de cómputo y proceder a la actualización del servidor *SERVER1*.
- Si se presentan problemas en el proceso de actualización, se procederá a conectar el controlador de dominio de reserva *1S1-BDC1* en la red.
- Configurar los valores de nombre y parámetros TCP/IP de acuerdo a la tala 4.3.
- Finalmente promover el servidor *1S1-PDC1* a controlador principal de dominio.

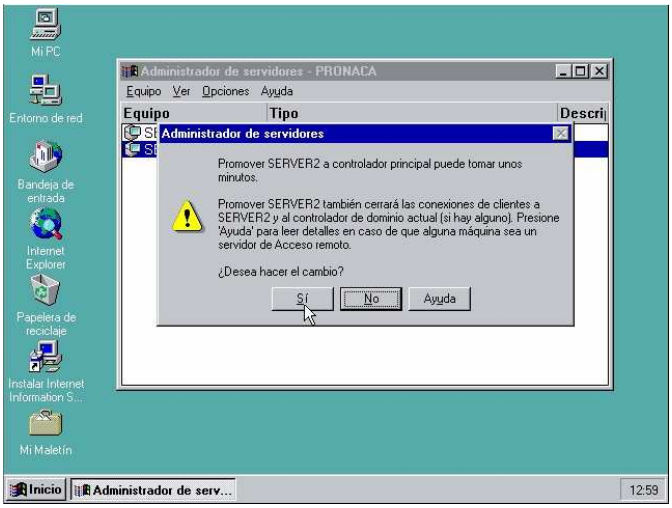

Figura 4.14. Promoción de BDC a PDC.

Este plan de recuperación se ha considerado que se debe aplicar en los siguientes casos:

- Si se supera el periodo de tiempo establecido para el proceso de migración del dominio.
- Si no llegaran a funcionar los servicios de red tales como: DHCP, DNS, WINS, y autenticación.
- Si los usuarios no pueden acceder a los sistemas críticos del negocio, tales como: sistema Baan, sistema de correo electrónico y Power Play.

4.6. CONFIGURACIÓN DE DNS

Introducción

El servicio de resolución de nombres de dominio en Windows Server 2003 es requisito obligatorio para que el servicio del directorio activo funcione correctamente, por lo tanto en el proceso de diseño del servicio DNS se decidió deshabilitarlo en el servidor Linux y levantarlo en la nueva plataforma Windows 2003.

4.6.1. INSTALACION DEL SERVICIO DNS EN WINDOWS 2003

El servicio DNS en Windows 2003 se puede instalar de dos maneras, la primera forma, es directamente durante el proceso de instalación del sistema operativo Windows Server 2003. Y la segunda, mediante un proceso adicional luego de que se ha concluido con la instalación del sistema operativo.

Debido a que el primer método ya ha sido descrito en el capítulo 4 numeral 4.4.2.2. “Procedimiento de Actualización de la SAM de Windows NT 4.0 al directorio activo de Windows Server 2003”, aquí, únicamente se revisará el segundo método.

4.6.1.1. Instalación de DNS desde panel de control.

Una vez que se ha concluido con la instalación del sistema operativo Windows Server 2003, se puede adicionar el servicio de DNS completando los siguientes pasos:

- Haga clic en *Inicio*, seleccione *Panel de control* y, a continuación, haga clic en *Agregar o quitar programas*.
- Haga clic en *Agregar o quitar componentes de Windows*. Ver figura 4.16.

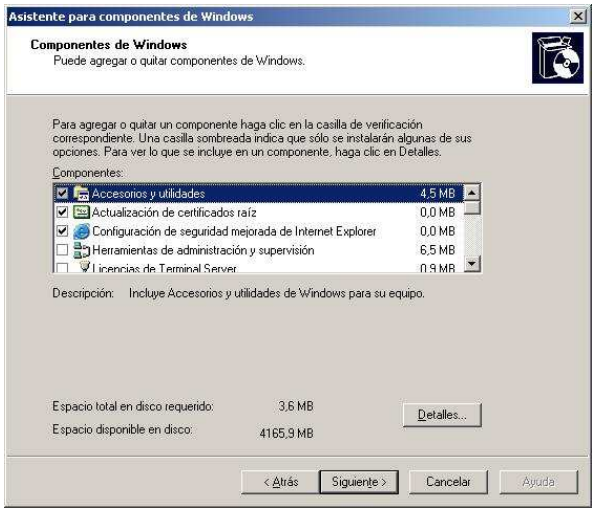

Figura 4.15. Componentes de Windows.

- En la lista Componentes, haga clic en *Servicios de red* (pero no active ni desactive la casilla de verificación) y, después, haga clic en Detalles. Ver figura 4.16.

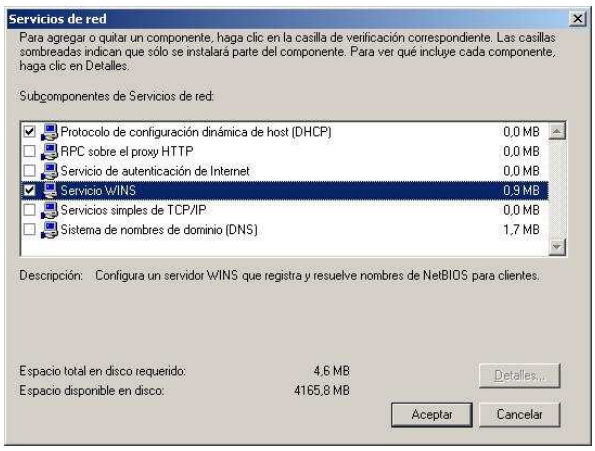

Figura 4.16. Servicios de Red.

- Active la casilla de verificación *Sistema de nombres de dominio (DNS)* y, después, haga clic en *Aceptar*.
- Haga clic en *Siguiente*.
- Cuando se solicite, introduzca el disco compacto de Windows Server 2003 en la unidad de CD-ROM o DVD-ROM del equipo.
- En la página *Finalización del Asistente para componentes de Windows*, haga clic en *Finalizar* cuando se haya completado la instalación.
- Haga clic en *Cerrar* para cerrar la ventana Agregar o quitar programas.

De esta manera ha quedado instalado el servicio DNS, pero seguidamente a esto será necesario configurarlo.

4.6.2. CONFIGURACION DE PARAMETROS DNS

La configuración de los parámetros del servidor DNS debe realizarse en base a las decisiones de diseño establecidas en el capítulo 3, las cuales se resumen en el siguiente cuadro:

LOCALIDAD	Matriz Quito	Regional Guayaquil
NOMBRE DEL SERVIDOR	1S1-DC1	5S1-DC1
DOMINIO	Industriax.corp	Insdustriax.corp
ESPACIO DE NOMBRES EXTERNO	Industriax.com	Industriax.com
ESPACIO DE NOMBRES INTERNO	Insdustriax.corp	Insdustriax.corp
ZONA PRIMARIA	Insdustriax.corp	Insdustriax.corp
TIPO DE ACTUALIZACIONES	Dinámicas	Dinámicas
RESOLUCION DE NOMBRES EXTERNOS	Por redireccionamiento	Por redireccionamiento
SERVIDOR REENVIADOR	200.31.6.34	200.31.6.34

Tabla 4.4. Parámetros a configurarse en el servidor DNS.

Para acceder a la consola de administración del servidor DNS, ir a *menú inicio*, *herramientas administrativas*, *DNS*. Y proceder a configurar los parámetros de la tabla 4.4 de acuerdo al manual adjunto en el anexo 2.

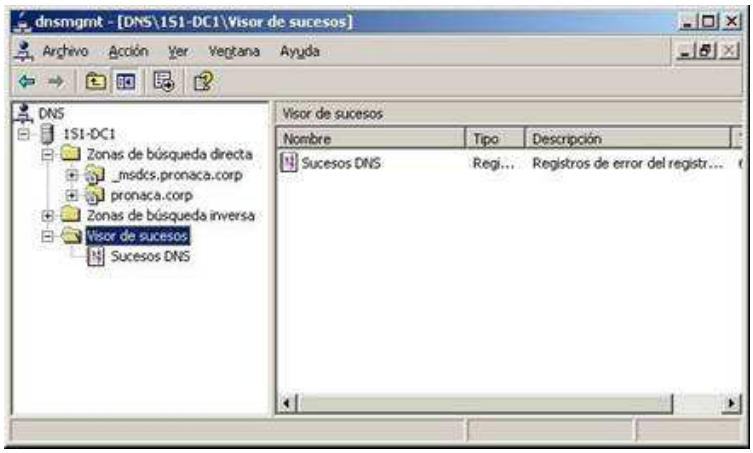

Figura 4.17. Configuración de Parámetros DNS.

4.6.3. PRUEBAS DEL SERVIDOR DNS

Luego de que se ha configurado el servidor DNS es aconsejable probar que la resolución de nombres DNS esté funcionando correctamente, esto se lo puede hacer a través del comando “nslookup”, como se muestra en la siguiente figura.

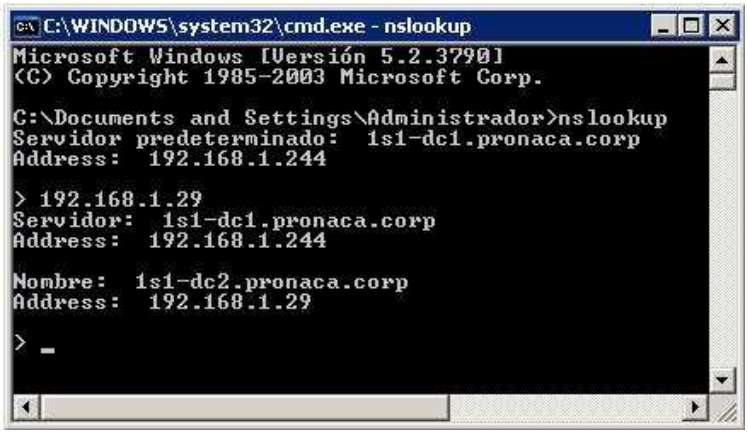

Figura 4.18. Prueba de resolución de nombres DNS.

4.7. CONFIGURACIÓN DE WINS

Introducción

En este documento se describe cómo instalar el servicio de nombres de Internet de Windows (WINS) en un equipo que ejecuta Windows Server 2003. WINS proporciona resolución de nombres NetBIOS. La instalación del Servicio WINS incluye dos procedimientos. En el primero se configuran los valores TCP/IP estáticos para el servidor y en el segundo, se instala WINS. Previo a estos procedimientos se detalla la información necesaria para configurar este servicio.

4.7.1. INFORMACIÓN NECESARIA DE CONFIGURACIÓN

Antes de comenzar la instalación, recopile la información siguiente, la misma que permitirá configurar el servicio conforme a las decisiones de diseño anteriormente establecidas:

- Una dirección IP estática para el servidor WINS. Si el servidor reside en una red basada en el Protocolo de configuración dinámica de host (DHCP), tiene que excluir la dirección IP del ámbito DHCP.
- El nombre del servidor que estará dando este servicio como servidor primario

de WINS.

- La máscara de subred.
- La dirección IP de la puerta de enlace predeterminada.

Una vez revisado el diseño del servicio WINS propuesto para INDUSTRIAX, se presentan los parámetros con los que este servicio deberá configurarse, en la siguiente tabla:

Ciudad	Quito
Localidad	Matriz Quito
Nombre del servidor	1S1-DC1
Dirección IP	192.168.1.244
Máscara de subred	255.255.255.0
Puerta de enlace	192.168.1.254
Replicación	Asociado de Inserción / Extracción con 1S1-DC2 y 5S1-DC1
Periodo de renovación	6 días

Tabla 4.5. Parámetros de configuración del servidor WINS 1S1-DC1.

El servidor 1S1-DC1, es el servidor principal de este servicio a nivel nacional, pero para implementar disponibilidad, se instalará un servidor adicional de WINS en la regional Guayaquil llamado 5S1-DC1, el mismo que atenderá requerimientos locales y que además replicará periódicamente con el servidor principal.

4.7.2. INSTALACION DE WINS

Para la instalación de WINS, una vez que se ha configurado el sistema operativo, se procederá a la instalación de acuerdo a los siguientes pasos:

1. Inicie la sesión como administrador local. Haga clic en *Inicio*, seleccione *Panel de control*, haga clic en *Agregar o quitar programas* y, a continuación, haga clic en *Agregar o quitar componentes de Windows*.

   En la figura 4.19 se observa la pantalla del asistente para agregar o quitar componentes de Windows.

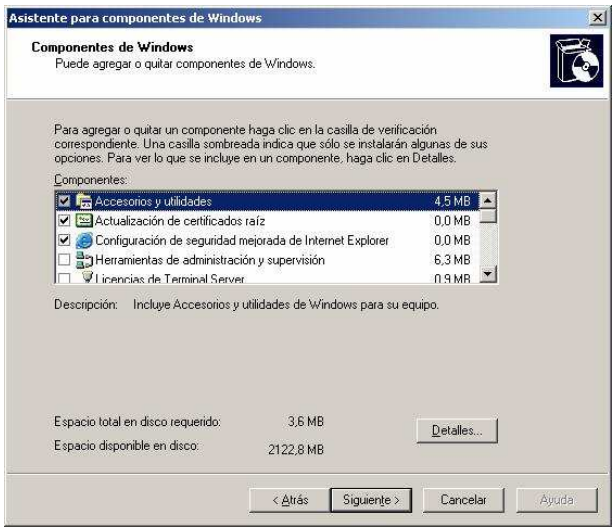

Figura 4.19. Componentes de Windows.

2. Cuando se inicie el Asistente Componentes de Windows, haga clic en *Servicios de red* (no active la casilla de verificación) y, después, haga clic en *Detalles*.
3. En el cuadro de diálogo *Servicios de red*, active la casilla de verificación *Servicio WINS* y después, haga clic en *Aceptar*, como se observa en la figura 4.20.

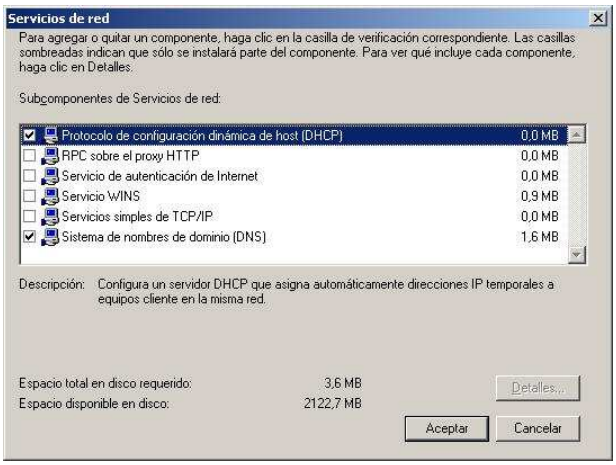

Figura 4.20. Agregar servicios de Red.

4. Haga clic en *Siguiente* y siga las instrucciones que aparecen en pantalla para completar la instalación.

5. Haga clic en *Finalizar*, cierre el cuadro de diálogo *Agregar o quitar programas* y, a continuación, cierre el *Panel de control*.

4.7.4. CONFIGURACIÓN DE WINS

Una vez instalado WINS, se procede a configurar el servicio con los parámetros descritos en la tabla 4.5, mediante la consola de administración de WINS. Para acceder a esta consola ir a *herramientas administrativas* y luego a *WINS*. La consola se ilustra en la figura 4.21.

Se observa que el servicio de WINS es levantado automáticamente en el servidor en el cual reside.

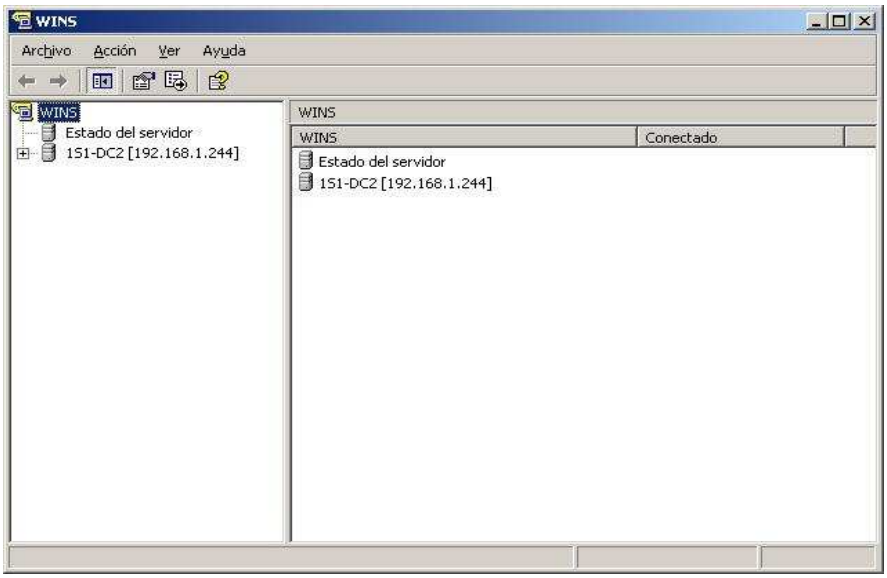

Figura 4.21. Consola de WINS.

En caso de que existan clientes que no se puedan registrar automáticamente en la base de datos WINS, como es el caso de los sistemas Linux, estas asignaciones se las puede ingresar manualmente, a través de la consola de WINS, como se observa en la figura siguiente:

Figura 4.22. Asignación estática.

En las ubicaciones que requieren alta disponibilidad puede existir más de un Servidor de WINS. Se ha diseñado un esquema de WINS Secundario manejado por *1S1-DC2* y *5S1-DC1*, estos equipos se deberán configurar como asociados de replicación del servidor principal.

En la figura 4.24 se muestra cómo añadir en el servidor *1S1-DC1* la definición de asociación de replicación de extracción/inserción.

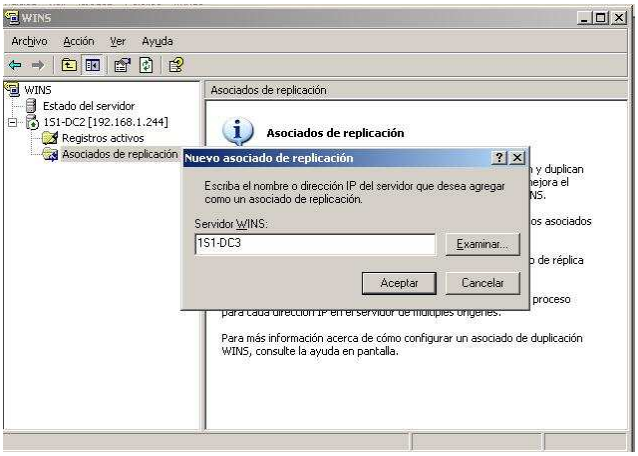

Figura 4.23. Definición de la asociación de replicación.

4.7.5. PRUEBAS DEL SERVIDOR WINS

Los clientes Windows se registran de manera automática y dinámica en la base de datos WINS, por lo que una de las maneras de probar el correcto funcionamiento de este servicio es ir a verificar que la base de datos se esté actualizando, un ejemplo se muestra en la siguiente figura:

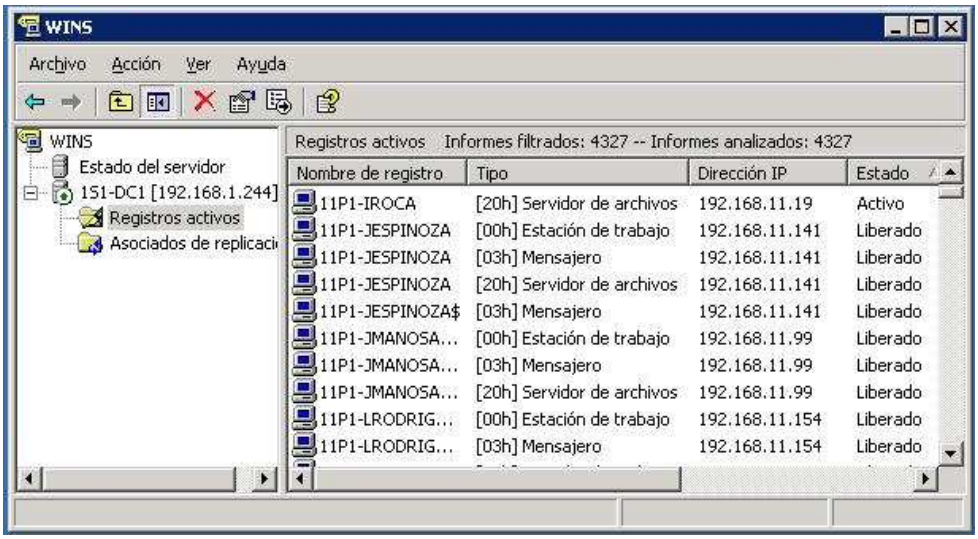

Figura 4.24. Registros de la base de datos WINS.

Otra manera de probar la resolución WINS es a través de una estación de trabajo, mediante la ejecución del comando ping a un nombre netBIOS.

4.8. IMPLEMENTACIÓN DE SERVICIOS BÁSICOS DE INFRAESTRUCTURA

4.8.1. INSTALACION DEL SERVICIO DHCP EN UN SERVIDOR WINDOWS 2003.

Introducción

Windows Server 2003 Dynamic Host Configuration Protocol (DHCP) reduce la complejidad y carga administrativa que involucra el manejar direcciones IP de clientes de red y su configuración. DHCP permite asignar direcciones IP a los clientes de la red de forma automática y dinámica, centralizando y simplificando la configuración y distribución de direcciones IP a través de la red. Esto evita errores comunes de configuración que ocurren cuando los valores son ingresados manualmente en cada computador y ayuda a prevenir conflictos de direcciones.

4.8.1.1. Instalación de DHCP

Se puede instalar DHCP durante o después de la instalación inicial de Windows Server 2003, lo que si es mandatorio que exista previamente es un servidor DNS en funcionamiento en el entorno.

Basados en la decisión de diseño de DHCP se subirán los servicios de DHCP en el servidor *1S1-DC1*.

Para instalar los servicios de DHCP en el Servidor *1S1-DC1* se deberá seguir el procedimiento detallado a continuación:

1. Comenzamos haciendo clic en el menú *Inicio*, en *Configuración* y, a continuación, en *Panel de control*.
2. Doble clic en *Agregar o quitar programas* y, después, clic en *Agregar o quitar componentes de Windows*.
3. En el *Asistente para componentes de Windows*, haga clic en *Servicios de red* en el cuadro *Componentes* y después, en *Detalles*.

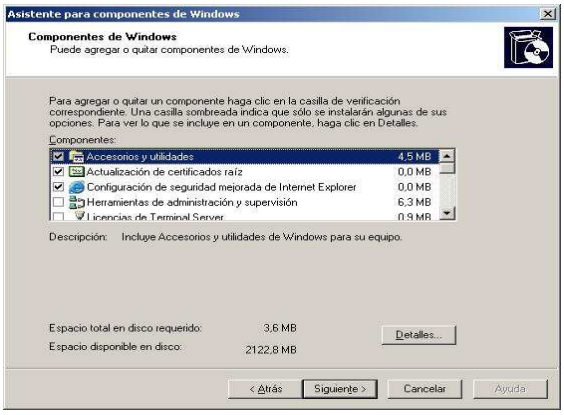

Figura 4.25. Componentes de Windows.

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

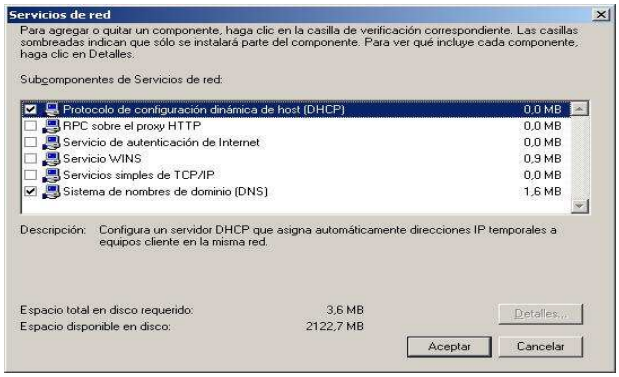

Figura 4.26. Levantar servicio DHCP.

5. En el Asistente para componentes de Windows, haga clic en *Siguiente* para iniciar la instalación de Windows Server 2003. Cuando se solicite, introduzca el CD-ROM de Windows Server 2003 en la unidad de CD-ROM o de DVD-ROM. El programa de instalación copiará en el equipo el servicio DHCP y los archivos de herramientas.
6. Cuando termine el programa de instalación, haga clic en *Finalizar*.

4.8.1.2. Configuración del servicio DHCP

Después de instalar e iniciar el servicio DHCP, es necesario crear un ámbito (un intervalo de direcciones IP válidas que se pueden conceder a los clientes de DHCP). Cada servidor DHCP del entorno debe tener al menos un ámbito que no se superponga con ningún otro servidor DHCP de su entorno. En Windows Server 2003, los servidores DHCP dentro de un dominio del directorio activo deben estar autorizados para impedir que se conecten servidores DHCP falsos.

Cuando se instala y configura el servicio DHCP en un controlador de dominio, se suele autorizar el servidor la primera vez que lo agrega a la consola de DHCP.

4.8.1.2.1. Autorizar un servidor DHCP

1. Haga clic en *Inicio*, *Programas*, *Herramientas administrativas* y a continuación, haga clic en *DHCP*.

2. En el árbol de consola del complemento DHCP, seleccione el nuevo servidor DHCP. Si hay una flecha de color rojo en la esquina inferior derecha del objeto Servidor, significa que todavía no se ha autorizado el servidor. Ver figura 4.27.

Figura 4.27. Consola de DHCP sin autorización.

3. Haga clic con el botón secundario del mouse (ratón) en el servidor y, a continuación, haga clic en *Autorizar*. Tras unos momentos, haga clic de nuevo con el botón secundario del mouse en el servidor y a continuación, haga clic en *Actualizar*.
4. Debe aparecer una flecha de color verde en la esquina inferior derecha para indicar que se ha autorizado el servidor. Ver figura 4.28.

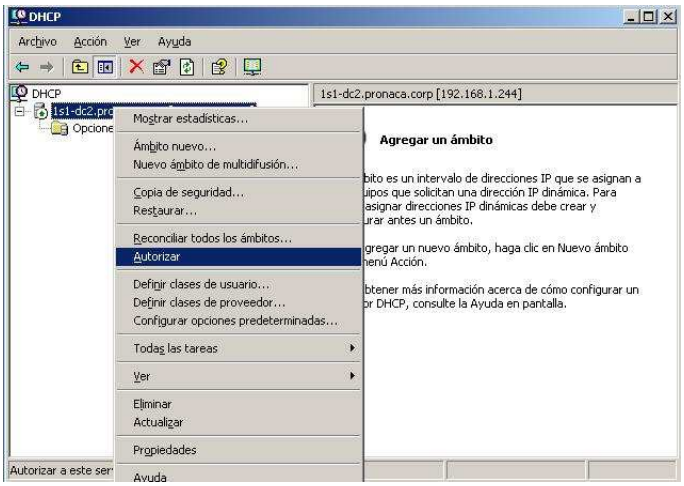

Figura 4.28. Autorizar un servidor DHCP.

4.8.1.2.2. Crear un ámbito nuevo

1. Haga clic en *Inicio*, *Programas*, *Herramientas administrativas* y, a continuación, haga clic en *DHCP*.
2. En el árbol de la consola, haga clic con el botón secundario del Mouse en el servidor DHCP en el que desee crear el nuevo ámbito DHCP y, a continuación, haga clic en *ámbito nuevo*. Refiérase a la tabla 4.6, donde se muestran las direcciones de los ámbitos a crearse y configurarse. Ver figura 4.29.

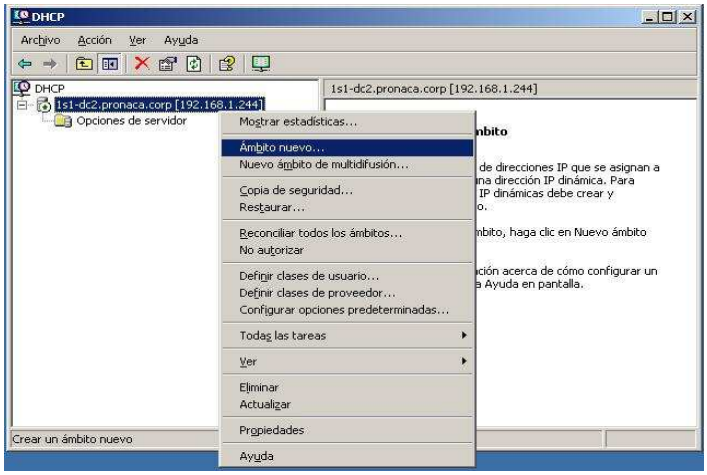

Figura 4.29. Crear un ámbito nuevo.

Nombre de ámbito	**Dirección Inicial**	**Dirección Final**	**Rango Exclusiones**	**Máscara de Subred**
Ámbito Matriz Quito Red 20	192.168.20.1	192.168.20.253	Ninguno	255.255.255.0
Ámbito Regional Guayaquil	192.168.5.10	192.168.5.253	Ninguno	255.255.255.0

Tabla 4.6. Ámbitos en Dominio INDUSTRIAX.

3. En el *Asistente para ámbito nuevo*, haga clic en *Siguiente*, y escriba un nombre y una descripción para el ámbito. Puede ser cualquier nombre que desee, pero debe ser suficientemente descriptivo como para identificar el propósito del ámbito en la red. Por ejemplo, podría utilizar Direcciones de clientes del edificio de administración. Haga clic Siguiente. Ver figura: 4.30.

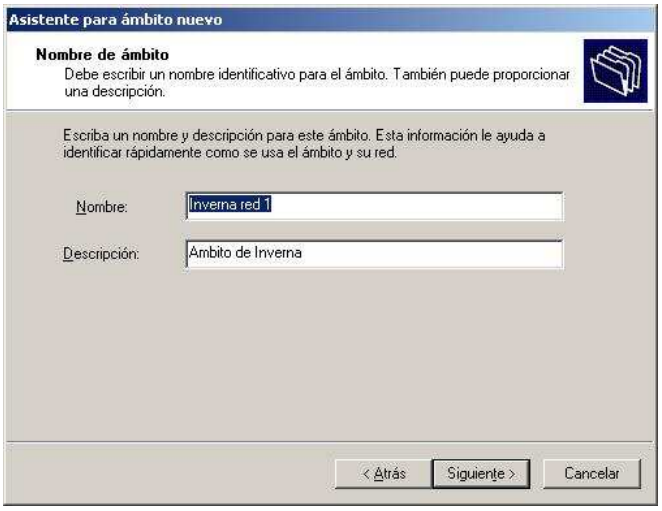

Figura 4.30. Nombre del ámbito.

4. Escriba el intervalo de direcciones que pueden concederse como parte de este ámbito, de acuerdo a la tabla 4.6.

   En el diseño de DHCP, la red 20 de la localidad Matriz_uio comienza desde la dirección *1* a la *253* y la mascara tiene un valor de *255.255.255.0*.

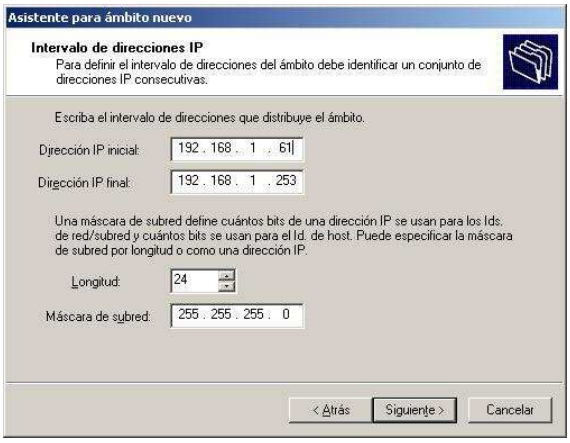

Figura 4.31. Intervalo de Direcciones IP.

5. En caso de existir, escriba todas las direcciones IP que desee excluir del intervalo especificado. Esto incluye todas las direcciones que puedan haberse asignado estáticamente a varios equipos de la organización. Haga clic en *Siguiente*. Ver figura 4.32.

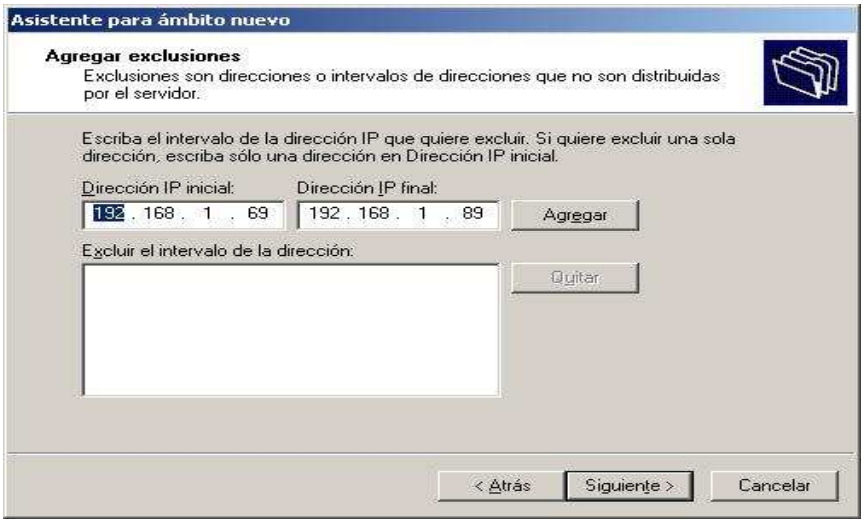

Figura 4.32. Exclusión de direcciones IP.

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

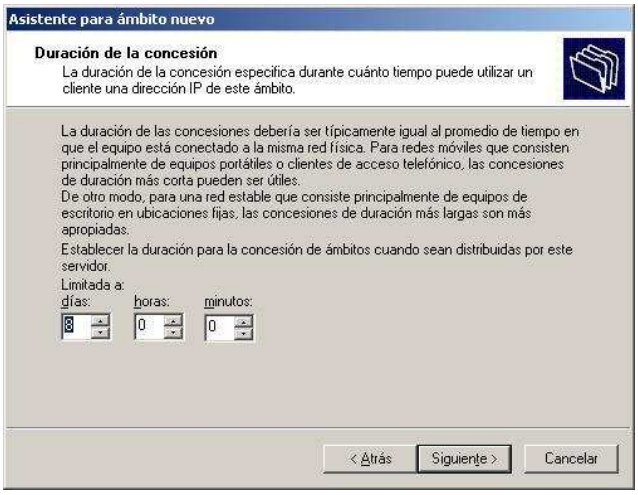

Figura 4.33. Duración de dirección asignada.

Por decisión de diseño la duración de concesión será configurada con un máximo de *8 días*, *0 horas*, *0 minutos*.

7. Haga clic en *Configurar estas opciones ahora* y en *Siguiente* para desplegar el asistente de manera que configure valores para las opciones de DHCP más

comunes tales como dirección de DNS, Gateway, WINS, etc. Ver figura 4.34.

Figura 4.34. Configuración de Opciones de DHCP.

8. Escriba los valores de dirección IP de la puerta de enlace predeterminada, servidor DNS, servidor WINS y nombre de dominio DNS; que deben utilizar los clientes que obtienen una dirección IP de este ámbito. Haga clic en *Agregar* para agregar los valores ingresados y, a continuación, haga clic en *Siguiente*. Ver figura 4.35.

Figura 4.35. Ingreso de valores de las opciones DHCP.

9. Haga clic en *Activar este ámbito ahora* para activar el ámbito y permitir que los clientes obtengan concesiones del mismo. Haga clic en *Siguiente* y, después, haga clic en *Finalizar*.

Figura 4.36. Activación del ámbito.

10. El servidor de DHCP se podrá verificar mediante la consola DHCP como se muestra en la figura 4.37. Observe que para cada nuevo ámbito existe la opción de Reservas.

Figura 4.37. Consola de manejo de DHCP.

11. El reservar direcciones IP tiene como objetivo el asignar a una estación siempre la misma dirección, por medio del MAC Address de cada tarjeta de red, este método se lo realiza mediante la opción *reservas* y *añadir una nueva reserva*. Ver figura 4.38.

Figura 4.38. Reservación de direcciones IP.

4.8.2. CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD (GPO)

Introducción

La directiva de grupo es una de las tecnologías clave de administración de cambios y configuraciones que incluye el sistema operativo Microsoft Windows Server 2003. Los administradores utilizan la directiva de grupo para especificar opciones de configuración de escritorio y sistema que se aplican a equipos y usuarios. Este documento examina las opciones de configuración de Directivas de grupo, las mismas que deberán ser activadas de acuerdo a las especificaciones realizadas en el capítulo 3.

4.8.2.1. Procedimientos para configurar las directivas de seguridad con directorio activo

La configuración de políticas de seguridad en Windows 2003 se lo puede realizar a través del complemento “Editor de objetos de directiva de grupo”, de la consola de administración Microsoft (MMC).

Para cargar el complemento Directiva de grupo de MMC:

1. En el menú *Inicio*, haga clic en *Ejecutar*. En el cuadro de texto *Abrir*, escriba: *mmc/s* y haga clic en *Aceptar*.

2. En el menú *Archivo*, seleccione *Agregar o quitar complemento* y haga clic en *Agregar*. Ver figura 4.39.

Figura 4.39. Agregar el complemento Directiva de grupo.

3. En la lista *Complementos independientes*, seleccione *Editor de objetos de directiva de grupo* y haga clic en *Agregar*.
4. En el cuadro de diálogo *Seleccionar un objeto de directiva de grupo*, haga clic en *Examinar*.

   El GPO predeterminado que se ha seleccionado al agregar el complemento directiva de grupo es *equipo local*. Ver figura 4.40.

Figura 4.40. Seleccionar un objeto Directiva de grupo.

5. En el cuadro de diálogo *Buscar un objeto directiva de grupo*, haga doble clic en la carpeta que contiene los GPO asociados con la OU “Controladores de dominio”. Ver figura 4.41.

Figura 4.41. Seleccionar la directiva de controladores de dominio que desea ver.

6. Seleccione la *Directiva predeterminada de controladores de dominio* y haga clic en *Aceptar*. Ver figura 4.42.

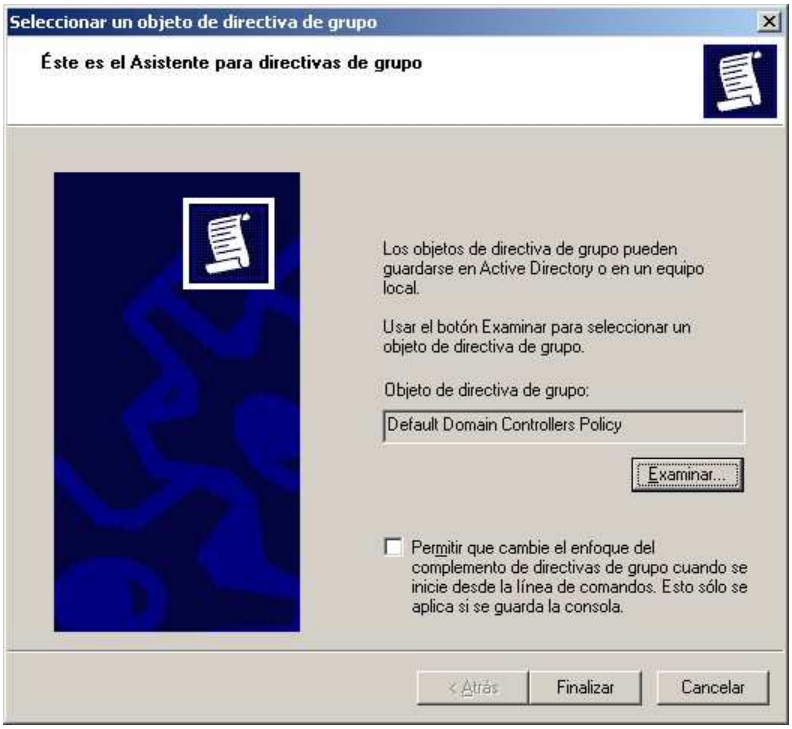

Figura 4.42. Selección de directiva de grupo.

7. En el cuadro de diálogo Seleccionar un objeto de directiva de grupo, haga clic en Finalizar, luego pulse Cerrar y finalmente Aceptar.

Para agregar una estación de trabajo a un dominio:

1. Editar la *Directiva predeterminada de controladores de dominio*.
2. En la *Consola*, vaya a *Asignación de derechos de usuario* y selecciónela.

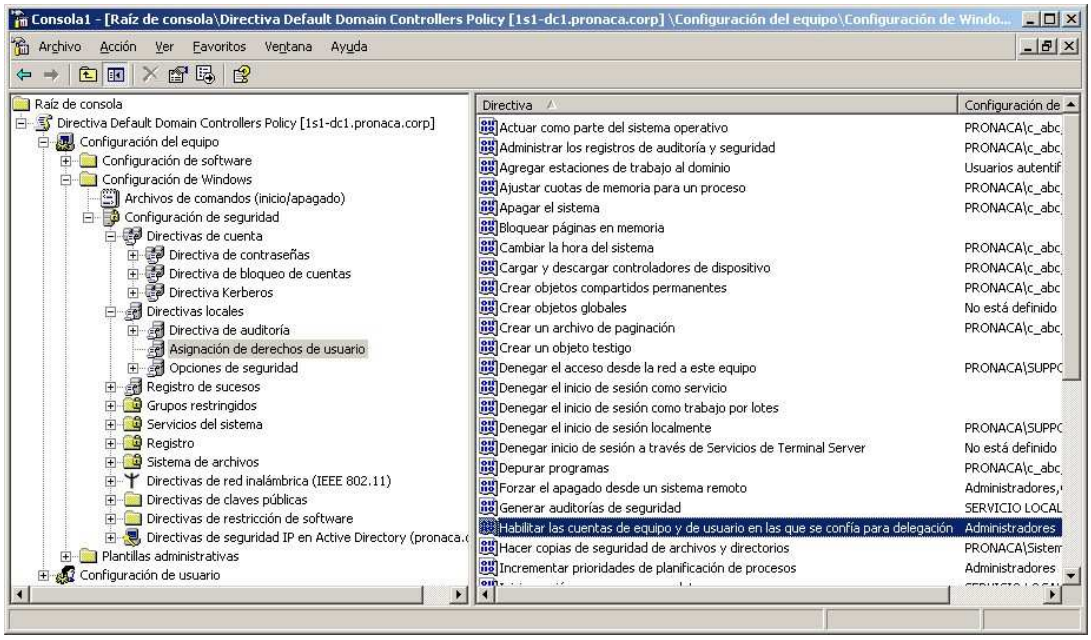

Figura 4.43. Ver las asignaciones de derechos de usuario.

3. En el panel de resultados, haga doble-clic en el derecho de usuario *Agregar estaciones de trabajo al dominio* y haga clic en *Agregar*.
4. En el cuadro de diálogo *Seleccionar usuarios o grupos*, seleccione *Administradores* y haga clic en *Agregar*. Ver figura 4.44.

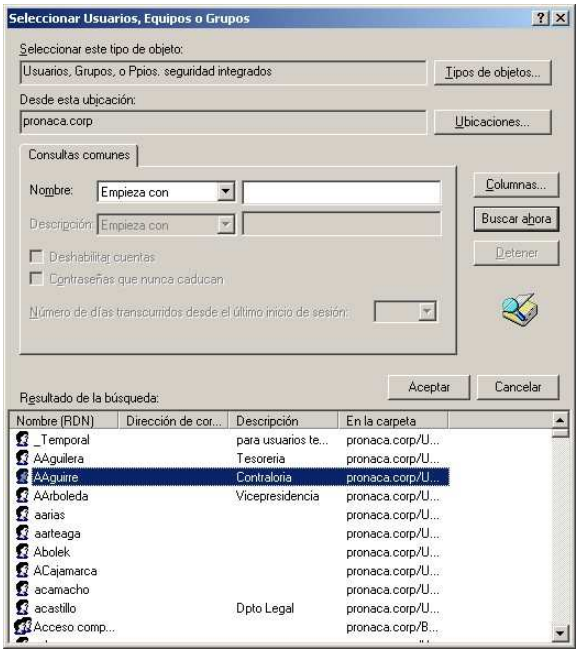

Figura 4.44. Agregar el grupo Administradores.

5. En el cuadro de diálogo *Seleccionar usuarios o grupos*, haga clic en *Aceptar*.
6. En el cuadro de diálogo *Agregar estación de trabajo a dominio*, haga clic en *Aceptar*. Ver figura 4.45.

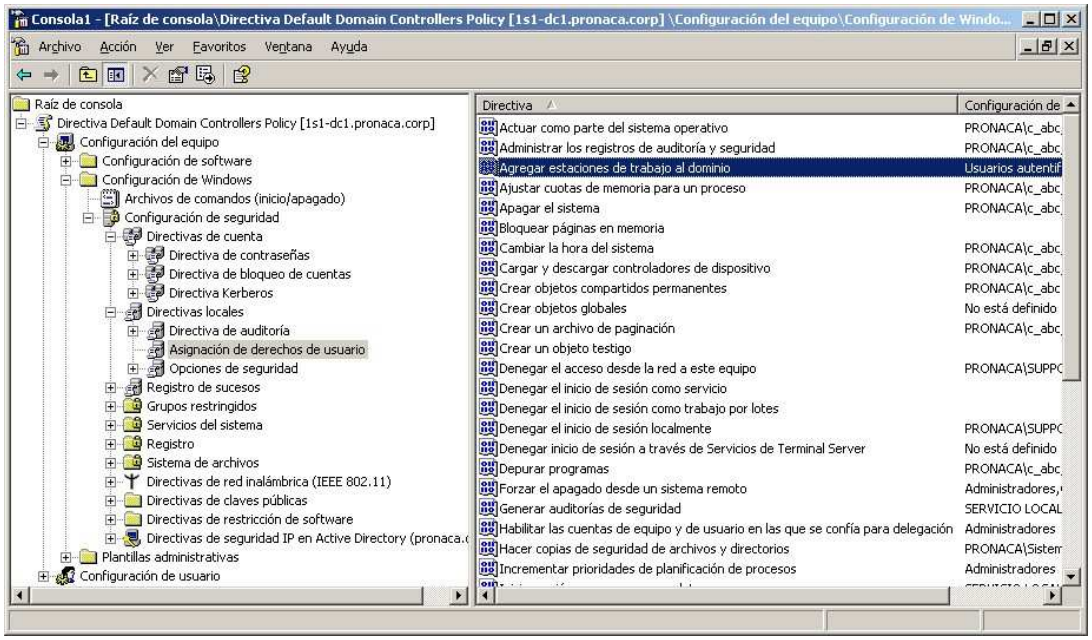

Figura 4.45. Ver los resultados de asignar un derecho de usuario a los administradores.

4.8.2.1.1. Habilitar las directivas de auditoría

Es posible modificar la directiva de auditoría de los controladores de dominio sin cambiar de consola.

Para habilitar la auditoria:

1. En el panel izquierdo de la consola, seleccione *Directiva de auditoría*.
2. En el panel de resultados, haga doble-clic en Auditar el acceso del servicio de directorio.
3. Seleccione Auditar intentos fallidos y haga clic en Aceptar. Deben actualizarse los valores del panel de resultados.
4. Cierre la consola cargada con el complemento GPO predeterminada de controladores de dominio.

5. Cuando se le pregunte si desea guardar la configuración de la consola, haga clic en *No*.

4.8.2.1.2. Establecer un mensaje de inicio de sesión para todas las máquinas del dominio

Para establecer un mensaje de inicio de sesión para todos los equipos de un dominio, debe utilizar el complemento *Equipos y usuarios de Active Directory* y su opción *Editor de directivas de grupo*.

Para establecer un mensaje de inicio de sesión:

1. En el Editor de directivas de grupo, que se encuentra en la *Directiva predeterminada de dominio*, expanda *Configuración del equipo*, después *Configuración de Windows*, vaya a *Configuración de seguridad*, después a *Directivas locales* y seleccione *Opciones de seguridad*. Ver figura 4.46.

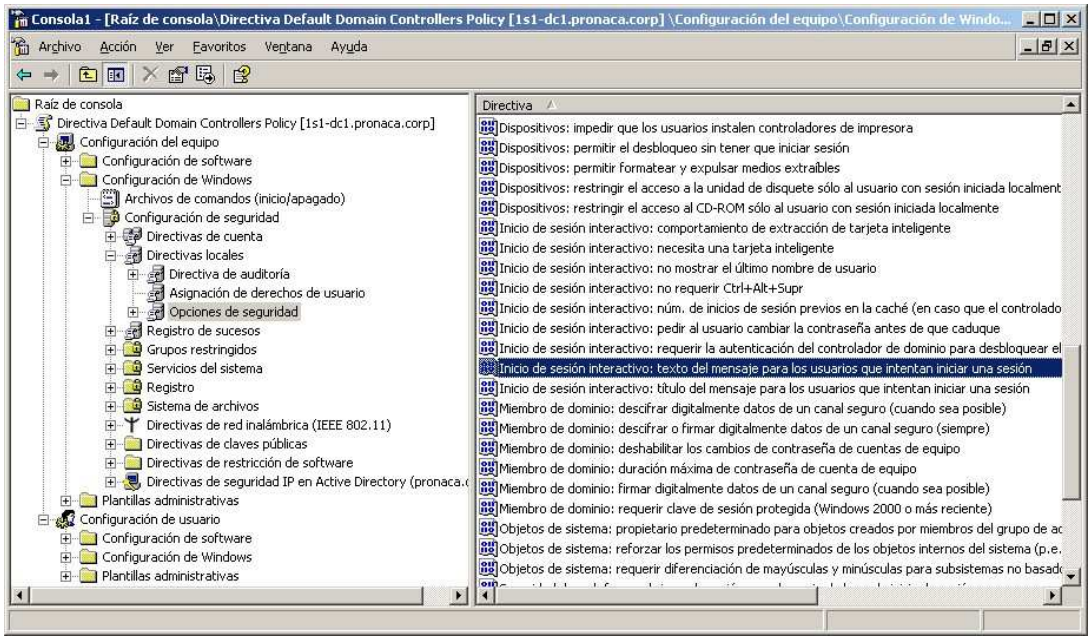

Figura 4.46. Seleccionar opciones de seguridad.

2. En el panel de resultados, haga doble-clic en *Texto del mensaje para los usuarios que intentan conectarse*.
3. Haga clic para desactivar la casilla de verificación *Excluir estos parámetros de*

la configuración.

4. Escriba el mensaje que desea que vean los usuarios cuando inicien la sesión en cualquier equipo del dominio. En este ejemplo, escriba *El jefe te vigila* y haga clic en *Aceptar*. Debe actualizarse el valor del panel de resultados. Ver figura 4.47.

Figura 4.47. Crear el texto de un mensaje.

5. Cierre el *Editor de directivas de grupo*.
6. Cierre la página *Propiedades del dominio*.
7. Cierre el complemento *Equipos y usuarios de Active Directory*.

Puesto que esta configuración de seguridad se asocia con el GPO de dominio predeterminado, se aplica a todos los equipos del dominio. Esta configuración anulará todas las directivas locales (definidas en los equipos individuales) que especifican este parámetro de seguridad.

4.8.2.1.3. Habilitar directivas de cuenta

Para activar directivas de cuenta se debe utilizar la Directiva predeterminada de dominio, puesto que estas directivas se van a aplicar a todo el dominio. El procedimiento es el siguiente:

1. En el menú Inicio, haga clic en *Ejecutar*.
2. En el cuadro de texto *Abrir*, escriba *GPEdit.msc* y haga clic en *Aceptar*.
3. En el panel izquierda de la consola del Editor de directivas de grupo, expanda la *Directiva predeterminada de dominio*, luego *Configuración del equipo*, vaya a *Configuración de Windows*, a *Configuración de seguridad* y a *Directivas de cuenta*.
4. Seleccione *Directiva de contraseñas*. Ver figura 4.48.

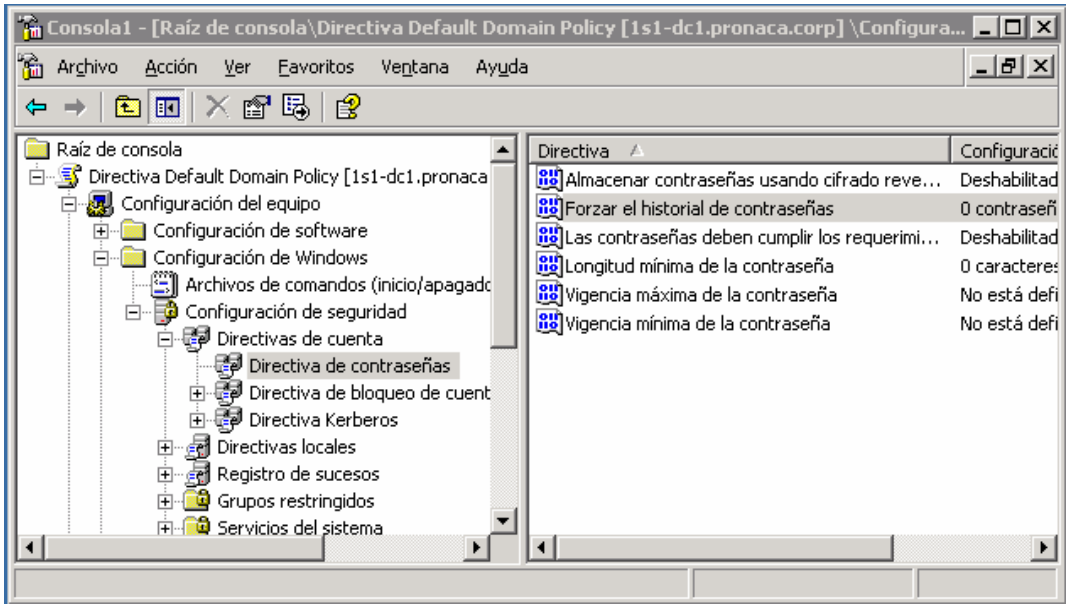

Figura 4.48. Ver la directiva de cuentas.

5. En el panel de resultados haga doble clic en la opción *Forzar historial de contraseñas* y a continuación en el cuadro de diálogo *Propiedades,* configure el valor en 4. Ver figura 4.49.

   Este valor se ha tomado de la tabla 3.7 “Políticas establecidas a nivel de password”, para completar las opciones de configuración de dicha tabla, se deberá repetir este procedimiento desde el paso 3.

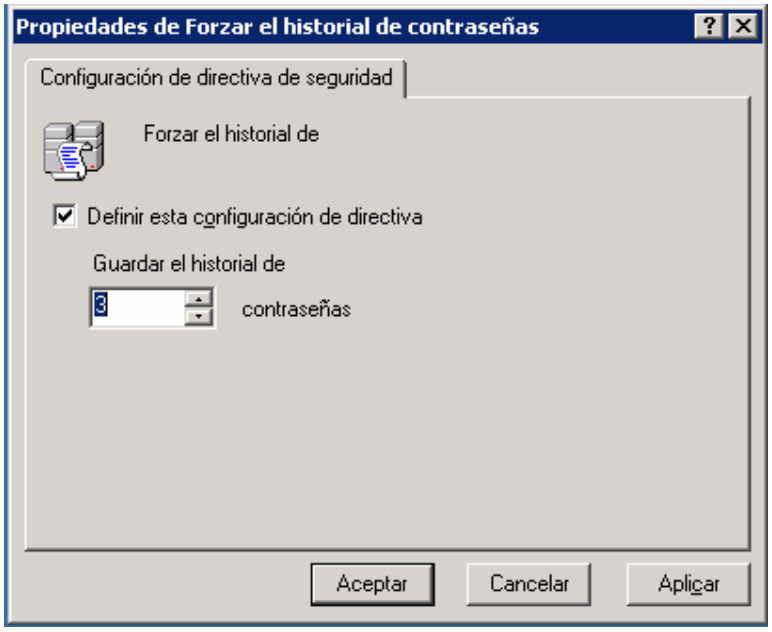

Figura 4.49. Definir la directiva de contraseñas.

6. Cierre la consola *Directiva predeterminada de dominio*, cuando se le pregunte si desea guardar la configuración de la consola, haga clic en *No*.

4.9. PRODEDIMIENTO DE CONTROLADOR ADICIONAL DE DOMINIO PARA GUAYAQUIL

El procedimiento a utilizarse para instalar el controlador adicional de dominio para Guayaquil incluye dos etapas, en la primera se instala el servidor como un servidor miembro del dominio y en la segunda etapa se lo promueve a controlador adicional de dominio.

4.9.1. INSTALACIÓN DEL SISTEMA OPERATIVO

Para instalar el sistema operativo se debe iniciar el servidor desde el disco compacto de instalación del sistema Windows Server 2003 y continuar con las instrucciones que aparecen en pantalla, estas instrucciones se encuentran detalladas en el anexo 3.

Figura 4.50. Inicio de Asistente de Instalación de Windows Server 2003.

Durante el proceso de instalación serán requeridos varios datos, los mismos que se detallan en la siguiente tabla:

UNIDAD ASIGNADA PARA LA INSTALACIÓN	C
TAMAÑO DE LA PARTICION	5 GB
SISTEMA DE ARCHIVOS	NTFS
NOMBRE DEL SERVIDOR	5S1-DC1
MODO DE LICENCIAMINETO	Por usuario
ROL	Miembro del dominio
DIRECCIÓN IP	192.168.5.3
MÁSCARA DE SUBRED	255.255.255.0
PUERTA DE ENLACE	192.168.5.254
DNS PRIMARIO	192.168.1.244
DOMINIIO	Industriax.corp
WINS PRIMARIO	192.168.1.244
SERVICIOS	DHCP, WINS, DNS

Tabla 4.6. Datos necesarios para la instalación del ADC para Guayaquil

4.9.2. PROMOCIÓN A CONTROLADOR DE DOMINIO ADICIONAL

Una vez instalado el sistema operativo se procede a promover el servidor a controlador de dominio, mediante la ejecución del comando “dcpromo”. En este proceso el servidor 5S1-DC1 va a sincronizar con el controlador principal de dominio 1S1-DC1 y va a cargar el directorio activo.

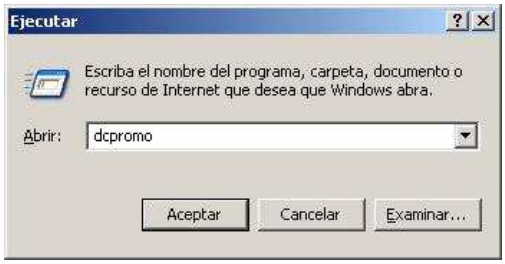

Figura 4.51. dcpromo inicia la instalación del directorio activo.

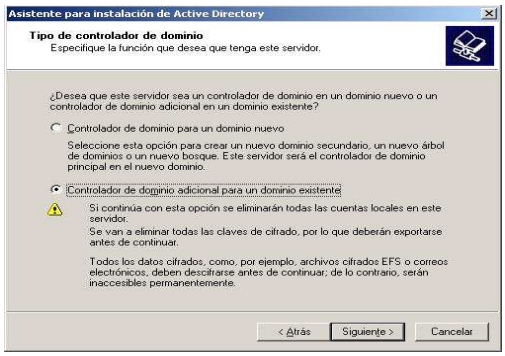

Figura 4.52. Asistente para la instalación del directorio activo.

Finalmente se procederá a instalar los servicios DHCP, WINS y DNS mediante los procedimientos anteriormente explicados en este mismo capítulo.

4.9.3. PRUEBAS DE FUNCIONAMIENTO DEL SERVIDOR ADC

Para determinar el funcionamiento correcto del servidor procedemos a abrir el directorio activo mediante la herramienta “usuarios y equipos del directorio activo” y comprobamos que se hayan cargado las cuentas de usuarios y equipos del dominio industriax.corp.

Para probar los servicios tenemos que utilizar una estación de trabajo y ejecutar los siguientes pasos:

1. ejecutar el comando “ipconfig /all”. Si la dirección IP asignada es una dirección válida (es decir pertenece a la subred 192.168.5.0), entonces el servicio DHCP, está correcto.
2. Ejecutar el comando “nslookup”. Si el nombre del servidor es resuelto

adecuadamente, entonces el servicio DNS está correcto.

3. Desde una estación con Windows 98, ejecutar el comando “ping 5S1-DC1”. Si el nombre netBIOS es resuelto, entonces el servicio WINS está correcto.

4.10. PRUEBAS DE PREMIGRACIÓN

Una vez que se han definido los diseños a implementarse en la nueva plataforma; y siguiendo con lo indicado en la Fase de Estabilización (Fase 3) de la Metodología Microsoft Solution Framework (MSF), es necesario implementar y probar los mencionados diseños en un entorno de operaciones lo más real posible, pero con un número de usuarios restringido, para de esta manera reducir el impacto que la aplicación de la actualización a Windows Server 2003 pudiera producir en las operaciones del negocio.

4.10.1. SELECCIÓN DEL ESCENARIO

El grupo de usuarios que nos va a permitir simular un ambiente real para estas pruebas es el departamento de sistemas de Quito y Guayaquil, debido a que aquí están los administradores de las diferentes aplicaciones que INDUSTRIAX dispone, tales como: Baan, Power Play, Internet y correo electrónico. Y aquí también encontramos estaciones de trabajo con todas las versiones de sistemas operativos como son: Windows 95, Windows 98, Windows 2000 y Windows XP

4.10.2. CRITERIOS DE VALIDEZ

Para considerar exitosa o no la migración de dominios de Windows NT 4.0 a Windows 2003, se deberán obtener resultados positivos en las pruebas siguientes, las cuales van a verificar que los servicios de la red estén correctamente habilitados:

- Validación de usuarios desde cada una de las versiones de sistemas operativos cliente, tales como: Windows 95, Windows 98, Windows 2000 y

Windows XP.

- Verificación de la asignación de direcciones IP a los clientes para determinar el correcto funcionamiento del servicio DHCP.
- Verificar la resolución de nombres DNS para determinar el correcto funcionamiento del servicio DNS.
- Verificar la resolución de nombres netBIOS para determinar el correcto funcionamiento del servicio WINS.
- Verificar el acceso al servicio de correo electrónico.
- Verificar el acceso al sistema Baan.
- Verificar el acceso al sistema Power Play.
- Verificar el acceso al servicio de Internet.
- Verificar el acceso al servicio de impresión y servidor de archivos.

Todas estas pruebas se deberán realizar desde las diferentes versiones de sistema operativo, es decir: Windows 95, Windows 98, Windows Milenium, Windows 2000 y Windows XP.

Para registrar los resultados de las pruebas se deberá utilizar el formulario de pruebas de migración que se adjunta en el anexo 4 (Formulario de pruebas de migración).

4.10.3. REVISIÓN DE RESULTADOS

Luego de haber registrado los resultados de las pruebas de premigración, estos deberán ser revisados para determinar los errores que se han presentado, proceder a solucionarlos y finalmente conseguir el correcto funcionamiento de todos los servicios contemplados en el proyecto.

En el caso de INDUSTRIAX los resultados recopilados en el anexo 5 (Tabulación de resultados de pruebas de migración 1), muestran que algunas estaciones con versiones de Windows inferiores a Windows 2000, no permitieron realizar la autenticación de usuarios en el dominio, porque presentaron el mensaje “no se encuentra un controlador del dominio”.

Esta novedad fue presentada al equipo de desarrollo para que proceda a investigar las causas y plantear la solución. En este caso particular, el inconveniente se resolvió instalando el programa DSclient, en las estaciones de trabajo con sistema operativo inferior a Windows 2000, para que puedan operar correctamente con el directorio activo.

Seguidamente en los 15 días posteriores se planteó repetir las pruebas con las estaciones de trabajo con sistema operativo inferior a Windows 2000; se volvieron a realizar las pruebas y se obtuvieron resultados satisfactorios, los cuales se muestran en el anexo 6 (Tabulación de resultados de pruebas de migración 2).

4.11. MIGRACIÓN

El proceso de migración de dominios de Windows NT 4.0 a Windows 2003 será realizado en dos etapas. En la primera se procederá a migrar el dominio DOM_UIO de Quito y en la segunda el dominio DOM-GYE de Guayaquil.

4.11.1. MIGRACIÓN DEL DOMINIO DOM_UIO AL DOMINIO INDUSTRIAX.CORP

Una vez que los resultados de las pruebas de premigración han sido exitosas, se procederá a realizar la actualización del dominio de DOM_UIO que actualmente se encuentra en Windows NT 4.0 al dominio industriax.corp de Windows 2003. Para esto se deberá establecer una fecha, hora y duración de este proceso y se lo deberá comunicar a todo el personal de la organización a través del Gerente Técnico, ya que se deberán suspender todos los servicios de red.

Para el caso de INDUSTRIAX, se estimó que el proceso de actualización tome 4 horas, pero por seguridad se estableció en 6 horas.

Se designo como equipo responsable de este proceso al conformado por dos

consultores de la compañía Binaria Sistemas y el Soporte Técnico de Quito de INDUSTRIAX. Los pasos para la migración se estableció que se realicen en el siguiente orden:

1. Antes de iniciar el proceso tener preparado el controlador de dominio de reserva 1S1-BDC1, que será utilizado en el proceso de rollback en caso de que se presentaran problemas durante la actualización.
2. Confirmar que se encuentren apagados los servidores y estaciones de trabajo de la localidad matriz_uio, a excepción de los servidores AIX y el controlador principal de dominio de Windows NT 4.0, SERVER1.
3. Proceder a la actualización del controlador principal de dominio, SERVER1, de acuerdo al numeral “4.4. Procedimiento de migración a Windows 2003”.
4. Configurar los parámetros del protocolo TCP/IP de acuerdo al contenido de la siguiente tabla:

OPCIONES	VALORES
Nombre de servidor	1S1-DC1
Dirección IP	192.168.1.244
Mascara de subred	255.255.255.0
Puerta de enlace	192.168.1.254
Servidor WINS primario	192.168.1.244
Servidor WINS secundario	192.168.1.29
Servidor DNS primario	192.168.1.29
Servidor DNS secundario	192.168.1.244
Dominio DNS	Industriax.corp

Tabla 4.7. Parámetros IP para configurar el servidor 1S1- DC1

5. Configurar el servicio DNS de acuerdo al numeral “4.6. Configuración de DNS”.
6. Configurar el servicio WINS de acuerdo al numeral “4.7. Configuración de WINS”.
7. Configurar el servicio DHCP de acuerdo al numeral “4.8. Implementación de servicios básicos de infraestructura”
8. Configurar las políticas de grupo de acuerdo al numeral “4.8. Implementación de servicios básicos de infraestructura”

9. Iniciar los servidores de aplicaciones Lotus Notes, Power Play, Internet, Impresión.
10. Iniciar las estaciones de trabajo del departamento de sistemas para realizar las pruebas establecidas en el formulario de pruebas de migración del anexo 13.
11. Revisar los resultados del anexo 14 (tabulación de pruebas), en caso de no existir inconvenientes proceder al encendido del resto de estaciones de trabajo y dar por concluido el proceso de migración.

4.11.2. MIGRACION DEL DOMINIO DOM_GYE AL DOMINIO INDUSTRIAX.CORP

Luego de que se considere estable la operación de la nueva plataforma Windows 2003 en la matriz_quito, se procederá a establecer la fecha, hora y duración del proceso de migración de los usuarios y recursos del dominio DOM-GYE al nuevo dominio industriax.corp. Para el caso de INDUSTRIAX se ha establecido que durará 4 horas.

Los responsables de este proceso serán: 2 consultores de la compañía Binaria Sistemas, el Soporte Técnico de Quito y el Soporte Técnico de Guayaquil de INDUSTRIAX.

Los pasos a seguir se enumeran a continuación:

1. Tener preparado el controlador de dominio de reserva 5S1-BDC2 que será utilizado en el proceso de rollback en caso de que se presentaran problemas durante la actualización.
2. Añadir las cuentas de usuarios y equipos del dominio DOM-GYE al dominio industriax.corp.
3. Preparar el servidor SERER315 como controlador adicional de dominio de acuerdo al numeral “4.9. Procedimiento de controlador adicional de dominio para Guayaquil”.
4. Iniciar y enlazar los servidores de aplicaciones y las estaciones de trabajo al dominio industriax.corp.

5. Realizar las pruebas establecidas en el formulario de pruebas de migración del anexo 13.
6. Revisar los resultados y si no existen inconvenientes dar por concluida la migración.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- El Objetivo del presente proyecto se cumplió exitosamente gracias a la ayuda de la metodología MSF, la cual permitió realizar la migración del dominio de Windows NT 4.0 a Windows 2003 de una manera organizada y con un impacto mínimo en las operaciones del negocio, debido a la realización de un análisis de riesgos y a la realización de las pruebas previas a dicha actualización.

- Con la actualización de dominios Windows NT 4.0 a Windows Server 2003, se ha logrado establecer una plataforma básica, pues los servicios de red (WINS, DHCP y DNS) para el usuario se han mantenido; y más bien se ha realizado un rediseño de las diferentes arquitecturas incluyendo la consolidación de varios dominios en uno solo. Lo que a futuro permitirá manejar de una manera estándar y centralizada todos los recursos de las diferentes localidades de la organización, consiguiendo de esta manera disminuir la carga administrativa para el personal de tecnología.

- Al tener un esquema multidominios, los servicios de red en ellos implementados, como por ejemplo DNS, DHCP, Políticas de usuario, etc.; se manejaban en forma independiente en cada dominio dificultando su uniformidad. Con el esquema de un solo dominio se ha conseguido unificar las configuraciones de estos servicios, de manera que todas las localidades se rijan por un estándar. Adicionalmente ha disminuido la carga administrativa ya que si se necesita aplicar un cambio de configuración en el sistema se lo debe aplicar a un solo dominio y no a cuatro como era el caso anterior.

- Del lado del usuario los cambios han sido mínimos, pues para realizar el proceso de validación en guayaquil lo único que se tuvo que hacer es cambiar el dominio de conexión “DOM-GYE” por “INDUSTRIAX.CORP”; y en la localidad de Quito la validación se mantuvo igual. Por otro lado al estandarizar entre otras cosas, los nombres de los equipos, se facilitó el acceso a los recursos de la red. Así también los usuarios móviles que tenían que adoptar una determinada configuración dependiendo de la localidad en la que se encuentren se ahorraron molestias, pues ahora la misma configuración de red (WINS, DNS y DHCP) les sirve en Quito o en Guayaquil

- El análisis de riesgos para determinar el impacto de la implementación de proyectos es importante para conseguir el éxito de una aplicación ya que permite determinar los inconvenientes que se van a encontrar en cada proceso; con el fin de evitar que pasen, o disminuir su efecto en las operaciones del negocio.

- El realizar un inventario de dominios permitió determinar que el esquema implementado anteriormente, no era el más óptimo pues existía un número exagerado de dominios que no estaban debidamente justificados y que lo único que hacían es aumentar la carga administrativa. Por lo que la nueva característica de OUs de Windows 2003 respecto a Windows NT 4.0 es sumamente beneficiosa e importante ya que permite: delegar la administración de la red; distribuir los recursos de manera sencilla pero mejor organizada; y, disminuir la necesidad de crear múltiples dominios, permitiendo tener un esquema centralizado y homogéneo de los recursos en la organización.

- Fue notoria la importancia de realizar las pruebas de premigración, pues durante este procedimiento, se pudo determinar que las estaciones de trabajo con sistemas operativos inferiores a Windows 2000 no podían ingresar al dominio. Esto permitió encontrar una solución temprana, antes de ir al modo de producción, evitando de esta manera afectar las operaciones del negocio.

- El haber establecido un solo dominio va a ayudar a manejar una

administración estándar en cuanto a cuentas de usuarios, passwords (duración) y cuentas de equipos. En el ambiente multidominio inicial; estos parámetros eran distintos y se manejaban de forma independiente de acuerdo al criterio de cada administrador.

- El servicio WINS se manejaba de manera distribuida, lo cual generaba problemas en los accesos a recursos de la WAN. La nueva arquitectura de Windows 2003 de extracción/inserción permite centralizar este servicio, lo cual mejora el acceso a los recursos de la WAN.

- Una de las ventajas que presenta Windows 2003 es permitir manejar varios servidores DHCP a través de la WAN, lo cual mejora la estandarización y disminuye la carga administrativa.

- En INDUSTRIAX inicialmente existía un solo servidor DNS para proveer de éste servicio a la organización a nivel nacional, lo que significaba que si habían problemas en el enlace WAN o en el servidor, los usuarios se quedaban sin servicio. Con el nuevo diseño, que permite ubicar un servidor secundario en Guayaquil, se aumenta la disponibilidad y se disminuye el tráfico en la WAN.

- Uno de los logros que se ha conseguido con el presente trabajo, es integrar a la plataforma Microsoft los servicios de WINS y DHCP, que anteriormente se encontraban trabajando en la plataforma Linux. Esto va a permitir disminuir la carga administrativa, pues el administrador va a utilizar una sola consola para tareas de administración y monitoreo.

- En nuestro país los recursos de comunicación son muy limitados y su costo es elevado. Este hecho ha sido considerado en las definiciones de diseño, las cuales han sido orientadas a disminuir el tráfico en la red, un ejemplo de esto es que se puso un controlador adicional de dominio en la regional_gye para que los requerimientos de autenticación de Guayaquil se hagan localmente, evitando que éste tráfico cargue el enlace WAN.

- El presente proyecto, ha sido personalmente muy provechoso porque se ha convertido en un aporte enriquecedor en el ámbito profesional; debido a que ha permitido cambiar la empírica concepción al hacer las cosas, pues muchas veces se instalan las aplicaciones únicamente siguiendo un instructivo, sin el análisis previo de riesgos o la elaboración de un plan de pruebas.

5.2. RECOMENDACIONES

- Se sugiere, en un futuro inmediato, migrar las estaciones de trabajo a un ambiente Windows XP, para de ésta manera aprovechar los beneficios que en cuanto a seguridad y carga administrativa ofrece el sistema operativo Windows Server 2003. Pues, actualmente, en Sistemas Windows inferiores a Windows 2000 se puede acceder a la información de la estación de trabajo sin validarse; es decir presionando “Escape” al momento que el sistema pide el “Password” de acceso a la red.

- También se sugiere que en la red LAN de la localidad matriz Quito, la cual actualmente tiene 2 subredes (una para Internet y otra para DHCP), se implemente una “Súper red” formada por las subredes: 192.168.0.0 y 192.68.1.0 eliminando la subred 192.168.20.0. De ésta manera se disminuirá el procesamiento de ruteo y se podrá crear un súper ámbito para manejar las asignaciones de direcciones IP automáticamente en su totalidad, realizando la asignación de acceso a Internet por medio de la reserva de direcciones en base a la dirección MAC de las estaciones de trabajo.

- En el análisis de situación actual que se realizó antes de la migración, se pudo apreciar que varias personas ejercían el rol de administrador, debido a la existencia de diversos dominios y cada uno de ellos con estilo diferente de administración; así por ejemplo había duplicación de usuarios y la denominación de dominios no cumplía con un estándar ya que uno se llamaba DOM-UIO y otro PECUARIA. Por tal razón se propone que la administración

se maneje en forma centralizada; es decir que una sola persona ejerza el rol de administrador y que éste delegue la administración a nivel de localidades y con los permisos más restrictivos.

- Una vez en operación puede ser necesario realizar cambios en las estructuras. Estos cambios deberían estar orientados a mantener los criterios con los que se diseñó la estructura inicial; caso contrario, los cambios se van a realizar desordenadamente y van a afectar a la administración, por ejemplo las unidades organizativas fueron diseñadas de tal manera que el nivel de profundidad sea bajo para no afectar la carga administrativa. En caso de que se necesite añadir OUs se deberá mantener éste criterio.

- Se recomienda ir a DHCP en todas las subredes, de ésta manera los usuarios móviles (viaje) van a evitar el inconveniente de estar cambiando su configuración IP cada vez que cambian de localidad.

- Los diseños establecidos en el presente proyecto han sido seleccionados por el equipo de trabajo, considerando ciertas características específicas de INDUSTRIAX tales como número de usuarios, disposición geográfica, disponibilidad, etc.; por lo que se sugiere que la documentación adjunta sea utilizada como referencia de consultas o cambios que en un futuro se presenten.

- Una de las propiedades de Windows 2003 es mantener deshabilitados los servicios que no sean necesarios, para que luego el administrador los vaya habilitando de acuerdo a las necesidades. La misma medida de prevención debería implementarse en los actuales servidores con Windows 2000 para mejorar la seguridad y evitar conflictos de ciertos servicios como DHCP.

- Se recomienda que en el futuro el servicio de correo electrónico que actualmente es manejado por la aplicación Lotus Notes, sea migrado a la plataforma Microsoft para aprovechar la funcionalidad del directorio activo y concentrar todas las cuentas de usuario en una sola base de datos, para de

esta manera activar características como single sign-on, es decir un solo password para todas las aplicaciones.

- Se recomienda que el personal que esté involucrado en la migración, administración y monitoreo del sistema Windows 2003 sea previamente capacitado, ya que este sistema requiere de un conocimiento profundo y gran destreza para aprovechar las características presentes y conseguir optima funcionalidad.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS Y MANUALES:

- Microsoft Corporation, “Centro de Ayuda y Soporte de Windows Server 2003”, Standard Edition, 2003.

- Microsoft Corporation, “Active Directory Operations Guide”, White Paper, 2002.

- Microsoft Corporation, “Managing a Microsoft Windows Server 2003 Enviroment”, Volumen I, Colombia, 2003.

- Microsoft Corporation, “Managing and Maintaining a Microsoft Windows Server 2003 Environment”, Colombia, 2003.

- Microsoft Corporation, “Migrating from Microsoft® Windows NT® Server 4.0 to Windows Server™ 2003. A Guide for Small and Medium Organizations”, U. S. A., 2002.

- Microsoft Corporation, “Microsoft Solution Framework”, White Paper, 2002.

- McCarthy, Jim, “Dynamics of Software Development”, 1995.

- McConnell, Steve, “Software Project Survival Guide”, 1997.

- Information Systems Audit and Control Association, “Manual de Preparación al Examen CISA”, Rolling Meadws, 2003.

DIRECCIONES ELECTRÓNICAS:

- Microsoft Corporation, “MSF”.

http://www.microsoft.com/MSF

- Microsoft TechNet, “Metodología Microsoft Solution Framework”. http://www.microsoft.com/latam/technet/fases/msf.asp

- McConnell, Steve, “Steve McConnell’s Survival Guide”. http://www.construx.com/survivalguide.

GLOSARIO DE TÉRMINOS

ADSIZER: (Active Directory Sizer), permite estimar el hardware requerido para implementar el directorio activo en una organización.

AMBITO: Espacio de existencia de una variable.

AUTENTIFICACION: Es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una clave.

ANÁLISIS DE RIESGO: El análisis de riesgo involucra identificar las amenazas más probables y analizar las vulnerabilidades relacionadas con las amenazas en la organización.

BAAN: es una aplicación de paquetes integrados que ayuda a la empresa a gestionar rigurosamente cada una de las áreas, en las que ésta se aplique. Es decir, área financiera, área proceso o producción, logística o distribución, transporte, etc.

BIDIRECCIONAL: La relación se establece en los dos sentidos.

BYTE: Conjunto de 8 bits el cual suele representar un valor asignado a un carácter.

CACHE: Copia que mantiene un ordenador de los datos accedidos últimamente de forma que si el procesador vuelve a solicitarlos, los mismos son leídos desde la memoria sin necesidad de tener que acceder de nuevo al disco duro.

CONTROLADOR DE DOMINIO: es el centro nervioso de un dominio Windows y tiene una serie de responsabilidades. Una de ellas es la autentificación.

CONTRASEÑA: Conjunto de caracteres alfanuméricos que le permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

DELIVERABLE: documentación que se puede entregar.

DIRECCIÓN IP: Cadena numérica que identifica a una máquina en una red IP.

DOMINIO: Son agrupaciones de redes que se gestionan desde un directorio centralizado -o Active Directory-, en el que se guardan las cuentas de usuario de toda la red y la información de seguridad. Espacio de existencia de una variable.

DOUBLE SPACE: Técnica que mediante software permite duplicar la capacidad de un disco duro.

DRIVE SPACE: Proceso basado en software, mediante el cual se incrementa la capacidad del disco duro.

DS CLIENT: Programa que se instala en sistema Windows 95,98 y para que éstos puedan operar como clientes del directorio activo.

FRAME RELAY: Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

FIX: Programa liberado por Microsoft que corrige errores de sus sistemas Operativos, también los llaman Parches.

HARDWARE: Componentes físicos de una computadora o de una red, a diferencia de los programas o elementos lógicos que los hacen funcionar.

INDUSTRIAX: Nombre de la empresa donde se efectuó el estudio y aplicación del proyecto.

INTEROPERABILIDAD: Ejercer una acción al interior de una red de computadores.

KBPS: (kilo bits por segundo), Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilo bit esta formado por mil bits.

KCC: proceso comprobador de coherencia de replicación del directorio activo.

LATENCIA: (retardo), tiempo que transcurre desde que un paquete de datos llega a un puerto hasta que se retransmite a su puerto de destino. Tiempo que una estación debe esperar cuando pide acceso a un canal de transmisión.

LINUX: Versión de libre distribución del sistema operativo UNIX el cual tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP.

LOGON: Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

MIGRACIÓN: Movimiento de recursos y servicios de una plataforma a otra.

MULTIDOMINIO: Esquema que maneja la plataforma Microsoft para distribuir los recursos y servicios en varios dominios.

NetBIOS: Network Basic Input Output System. Es una API que complementa la BIOS de DOS al agregar funciones especiales para redes locales (LAN).

PROTOTIPO: Persona o cosa que por sus características es modelo o ejemplo.

RED: Conjunto de recursos (impresoras, computadores, Internet, correo electrónico) que están comunicados entre si para compartir servicios.

RELACIONES DE CONFIANZA: Una relación de confianza es un vínculo entre dos dominios, donde el dominio que da la relación de confianza (Trus-ting Domains) permite a los miembros de otros dominios (Trusted Domains), autenticar sus contraseñas a través de él.

REPLICA: Recurso que es espejo o copia de otro para diversificar y descongestionar el acceso.

RIESGO: Probabilidad de daños, sociales, ambientales y económicos en un lugar dado y durante un tiempo de exposición determinada.

SERVICE PACK: Nombre que da Microsoft a los "parches" que corrigen errores en Windows NT o le añaden características nuevas.

SET: Dar valor a una posición de memoria. Cambiar el estado de un conmutador o una señal.

SCRIPT: Secuencia de comandos que se le dan a un módem con el propósito de configurarlo (velocidad, compresión de datos, etc.) o darle una tarea.

SOFTWARE: Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica de una computadora.

TOPOLOGIA: Se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador, una impresora, un concentrador, conmutador o un ruteador.

VULNERABILIDAD: Es la debilidad en el plan o aplicación del control dentro de un proceso, función, o facilidad que puede contribuir a una ruptura.

SIGLAS Y SÍMBOLOS

ADC	Controlador Adicional de Dominio.
ASR	Recuperación Automática del Sistema
BDC	Controlador de Dominio de Reserva.
Bps	Bits por segundo.
DNS	Servicio de Nombres de Dominio.
DHCP	Protocolo de Configuración Automática de un Cliente IP.
GPO	Políticas de Grupo.
KCC	Comprobador de Coherencia de Replicación.
LAN	Red de Área Local.
MSF	Microsoft Solution Framework
NT	Tecnología de Red (Network Technology)
OUs	Unidades Organizacionales.
PDC	Controlador Principal de Dominio.
SAM	Administración de cuentas del sistema
TCO	Costo Total de Operación
TCP/IP	Protocolo de Control de Transferencia/Protocolo de Internet.
UPS	Sistema de Energía Ininterrumpida
WINS	Servicio de Nombres de Internet de Windows.
WAN	Red de Área Amplia.

ANEXOS

Anexo 1. Inventario de recursos de red de INDUSTRIAX

Anexo 2. Manual de instalación del servicio DNS

Anexo 3. Manual de instalación del sistema operativo Windows 2003

Anexo 4. Formulario de pruebas de migración

Anexo 5. Tabulación de resultados de pruebas de migración 1

Anexo 6. Tabulación de resultados de pruebas de migración 2

Nota: Los anexos serán adjuntados en un medio magnético.