Global Information Assurance Certification Paper

INDICE

1. INTRODUCCION

Para una persona común, el que pueda acceder de una manera fácil a un servicio que necesita, le es beneficioso ya que le simplifica su trabajo, evitándole pasar horas dando solución a sus búsquedas. Es allí cuando un servicio de directorio le resulta de gran utilidad, de modo que le da libertad para acceder a la información de manera ordenada.

Un ejemplo podría ser: El directorio telefónico, que le permite acceder a números de teléfonos, que están debidamente ordenados basándose en nombres, ya sea de personas físicas (Números personales) o Personas Jurídicas (Empresas), lo cual hace sencillo una búsqueda especifica. Asimismo se pueden realizar búsquedas, aunque no se conozca el nombre exacto del recurso que se necesita, de este modo si desea encontrar el numero de una línea área, de la cual no se este totalmente seguro del nombre, puede buscarse una lista de nombres que coincidan con el atributo que se conoce, para ello podría buscar todas las empresas de líneas aéreas que se encuentran en la ciudad, y terminara encontrando lo que necesita.

De igual manera dentro de una organización es importante proveer a los usuarios de un servicio que les permita localizar la información que necesitan para realizar su trabajo y mantener fuera de su alcance otros recursos no necesarios, ello incluye tanto la información más confidencial de la institución, como la propiedad personal de otros usuarios; todos ellos coinciden en que la seguridad de la información es fundamental, hasta el día en que olvidan una contraseña, y se les niega el acceso a los documentos que necesitan. En ese momento esta se convierte en un obstáculo, ya que impide que puedan realizar su trabajo, entonces culpan a los administradores de red por una seguridad excesiva; sin embargo de igual forma se quejaran de una seguridad descuidada si sus archivos llegan a ser accedidos, cambiados o destruidos, por otros usuarios.

Wndows 2000 Server, provee un servicio de directorio, denominado el Directorio Activo que proporciona la estructura y las funciones necesarias para mantener, organizar, administrar y controlar los recursos de la red, como ser (impresoras, equipos, servidores, base de datos, grupos de trabajo) y hace estos accesibles a los usuarios.

2. OBJETIVOS

El objetivo de este documento es realizar una introducción y descripción del Directorio Activo y sus componentes para recalcar la importancia de su uso dentro de una organización, las ventajas que proporcionan para Configurar una infraestructura de red simple, también mostrar un panorama general sobre los aspectos básicos de seguridad con la aplicación de políticas de grupo y cómo afectan en el acceso a los recursos.

Pero este documento no ahondará en la información técnica detallada, que se va a utilizar al considerar la Implementación, como planear la estructura de DNS, Opciones de Instalación, tecnologías soportadas por el directorio activo, replicacion y su funcionamiento, así como la descripción de la nomenclatura de nombres a usarse en los componentes.

3. INTRODUCCION A LA ESTRUCTURA DEL DIRECTORIO ACTIVO

Todo proyecto comienza con la planificación minuciosa del diseño, antes de implementarse en una organización, para comprender el alcance que se desea lograr.
En este caso es importante conocer las características del directorio activo, ya que así como puede proveer una estructura sencilla de red, para que los usuarios accedan a los recursos, y los administradores controlen dicho acceso.
También pude ser demasiado complejo su uso, si no se tiene claro varios aspectos, basados en la estructura de la organización como ser los grupos administrativos ya existentes.
Para ello primero se debe diseñar el ámbito, es decir organizar los recursos de la red, decidir el numero de dominios, arboles o Ou's que se creara, así como los nombres que se desea dar a cada uno, también definir dónde y cuando ocurrirá el trafico de logon y replicacion, todo esto debe ser comprendido en su descripción a fin de que se utilice apropiadamente
Es así que el Directorio Activo se divide en dos estructura, claramente definidas como son:
La Estructura Lógica y la Estructura Física.

1.- Estructura Lógica.-

Es flexible y proporciona un método de diseño y jerarquía de directorio, que se usa para organizar los recursos de la red. Tiene como componentes:

a) Dominio.- Unidad básica de organización de seguridad en el Directorio Activo, todos los objetos son mantenidos en un dominio y este guarda la información solo de los objetos que contiene. Cada dominio tiene sus propias políticas de seguridad y las relaciones de confianza de seguridad con otros dominios. El administrador de un dominio tiene los permisos y derechos necesarios para desempeñar las tareas de administración en ese dominio.

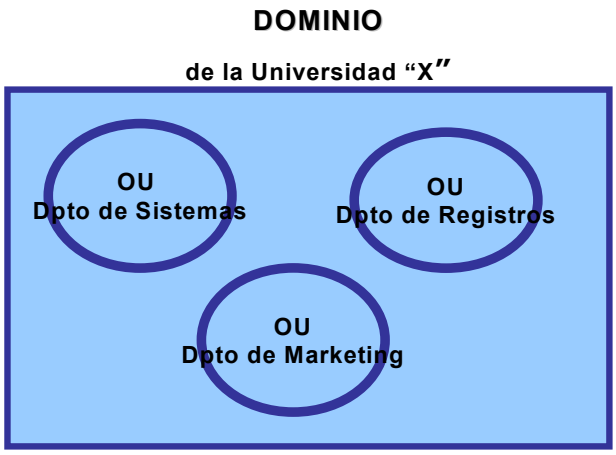

Imagen1: El cuadrado representa el dominio, y los círculos que están dentro de el, las Ou's por las cuales esta conformado. Ej.: En este caso las Ou's están divididas por departamentos.

a) Unidades Organizacionales.-

Una Unidad Organizacional (OU) es un objeto contenedor que se usa para organizar objetos (como cuentas de usuario, grupos, equipos, impresoras y otras OU´s.) dentro de un dominio. Las OU proveen un mecanismo sencillo para agrupar usuarios y es la unidad más pequeña a la que se le pueden asignar configuraciones de Políticas de grupo.

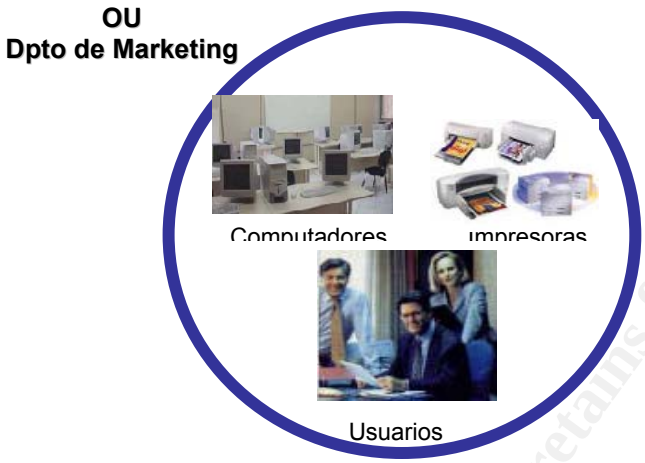

Imagen2: Muestra un circulo y dentro de el a los objetos que podrían agruparse, en una OU.

c) Árboles.-

Son una recopilación jerárquica de los dominios, los que comparten un espacio para nombres común. Cuando se añade un dominio a un árbol existente, el nuevo dominio es un dominio hijo de un dominio padre existente, y se establece automáticamente una relación de confianza Kerberos; lo cual de una manera simple es, sí el Dominio A confía en el Dominio B y el Dominio B confía en el Dominio C, entonces el Dominio A confía en el Dominio C. Muchos dominios pueden formar un árbol de dominio.

Por ejemplo: Para la Universidad X su nombre en el Directorio Activo es X.edu. Sin embargo se han adquirido dos nuevas sucursales, una en Cochabamba y otra en La Paz, y se decide crear dos nuevos dominios al árbol ya existente. Los dominios resultantes serían a.X.edu y b.X.edu.

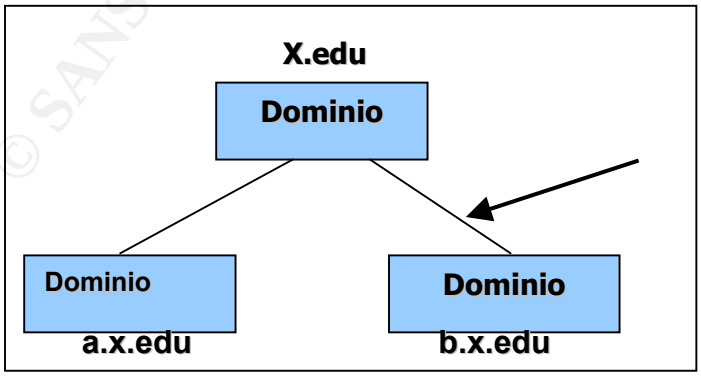

Imagen3: Representa un árbol de dominio, en el que el primer dominio es la raíz, y se crean los nuevos dominios, adjuntándole a los nuevos dominios el nombre del dominio principal.

b) Bosques.-

Está formado por varios árboles los cuales no comparten un nombre común. Cada árbol de un bosque tiene su propio nombre de espacio único.

Por ejemplo: La Universidad X crea una organización separada llamada Y
X decide crear un nuevo nombre de dominio del Directorio Activo para Y, llamado Y.edu
Aunque las dos organizaciones no comparten un espacio de nombres común, al añadir el nuevo dominio del Directorio Activo como un árbol nuevo dentro del bosque existente, las dos organizaciones podrán compartir recursos y funciones administrativas.

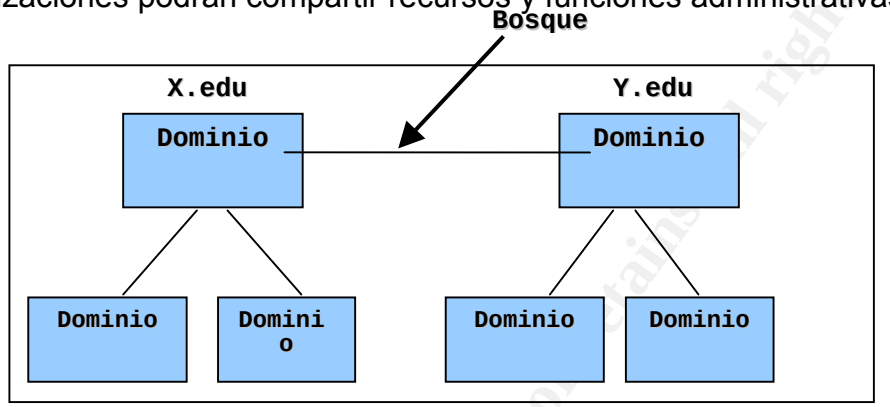

Imagen4: Representa un bosque de dominios, que se forma de varios arboles, pero con su propio nombre cada dominio raíz.

2) Estructura Física

Se usa para configurar y administrar el tráfico de red. Entender los componentes de la estructura física del Directorio Activo es importante para optimizar el tráfico de red y el proceso de logon.
Se compone de:

a) Sitios

Determina la forma que debe replicarse la información de directorio y como debe tratarse las solicitudes de servicio de equipos los que son asignados a sitios, estos son una combinación de una o más subredes IP conectadas en enlaces de alta velocidad, las cuales constituyen una forma sencilla y eficaz para representar agrupamientos en la red.

a) Controlador de Dominio

Es un equipo que ejecuta Windows 2000 Server donde se almacena una copia del directorio, y que almacenan datos y administran las interacciones entre el usuario y el dominio, como los procesos de inicio de sesión, la autenticación y las búsquedas de directorio También administra los cambios del directorio y los replica a otros controladores de dominio del mismo dominio.

4. DESCRIPCIÓN DEL DIRECTORIO ACTIVO

Ya se realizo una introducción a los componentes del directorio activo, ahora se tratara de describir cada uno.

a) La creación de dominios:

Permite organizar los objetos al utilizar las unidades organizativas OU's
Proporciona seguridad, al aplicar Políticas de grupo al dominio se establece la forma de acceso, la configuración y el uso de los recursos.
Permite duplicación

b) Unidades Organizativas O's.- Se pueden crear OU's

Para reflejar la estructura organizacional como departamento.
Que representen grupos de objetos similares como Usuarios, Computadoras, Impresoras,
Que permitan organizar datos de proyectos, de forma temporal

c) Arboles.-

Los árboles definen la mayoría de la estructura del directorio activo y el uso del dominio.

d) Boques.-

El primer dominio de un bosque se conoce como dominio raíz del bosque.
Un bosque proporciona los vínculos para muchas de las funciones que existen dentro de Directorio activo como la seguridad, convenciones y catálogo global.
El uso del bosque puede originarse de la necesidad de mantener arboles separados.

e) Sitios.-

En pequeñas empresas, las definiciones de sitio serán fáciles y estarán basadas en la conectividad de velocidad LAN.
En grandes empresas con muchas ubicaciones, definir los límites de sitios será más difícil debido a la variación de las condiciones de ancho de banda de los vínculos de red,
Los sitios aumentan la eficacia de estos dos tipos de operaciones: Solicitud de un Servicio y la replicacion de la información.

f) Controlador de dominio.-

** Una función específica del controlador de dominio, es el Catálogo global, el cual es una base de datos centralizada de todos los objetos del bosque y sus atributos

** Otra es el maestro de operaciones: que tiene cinco tipos los cuales se detallaran a grandes rasgos

1) Maestro de esquema.- Cada controlador de dominio sabrá cómo se ve el esquema y Necesita saber qué tipos o clases de objetos se pueden crear. Para evitar los conflictos originados por distintas personas que cambiarlo en tiempos diferentes, sólo un equipo debe ser una copia de leer/escribir de esa base de datos de esquema.

2) Maestro de nombre de dominio

Es el equipo que asegura que no tenga dos dominios en el mismo árbol con el mismo nombre.

3) Maestro de RID

Los Controladores de dominio de reserva necesitan ver los SID (Identificadores de seguridad) consecutivos, y depende del Maestro de RID asegurar que eso suceda. Cuando crea un usuario, ese usuario irá al Maestro de RID para obtener el siguiente SID disponible.

4) Emulador PDC

Puede crear objetos en un dominio Windows 2000, pero cuando los controladores de reserva necesiten obtener los cambios, no se dirigen al controlador de dominio; sólo saben dirigirse al Emulador PDC.
5) Maestro de infraestructura
Realiza un seguimiento del movimiento de los objetos. Si mueve un usuario de un dominio o OU a otro, parte del nombre del usuario cambiará. Este hara que el grupo en donde el usuario se encuentra refleje ese cambio de nombre lo más pronto posible.

5. VENTAJAS DEL DIRECTORIO ACTIVO

Entre las ventajas que puede proporcionar su uso, dentro de una organización, esta:

- . La seguridad de la información.- El control de acceso se puede definir no sólo para cada objeto del directorio, sino también para cada una de las propiedades del objeto.
- . La administración basada en políticas.- Establece un conjunto de normas de la empresa
- . La capacidad de ampliación.- Ya que los administradores tienen la posibilidad de agregar nuevos objetos al esquema y nuevos atributos.
- . La replicacion de la información.- Permite actualizar el directorio en cualquier controlador de dominio.
- Integración con DNS.- Usa el Sistema de nombres de dominio. Que es un servicio estándar de Internet que traduce nombres de equipos host, a direcciones IP numéricas.
- Las consultas flexibles.- Los usuarios y administradores pueden utilizar el comando Buscar, para encontrar rápidamente un objeto en la red por sus propiedades.

6. PAUTAS PARA LA PLANIFICACION DEL DIRECTORIO ACTIVO

El Directorio Activo aumenta no sólo la forma de administrar, sino también la complejidad de la red. Por ello, la correcta planificación de esta infraestructura se debe hacer de una forma minuciosa.
Algunos de los factores que deben tomarse en cuenta son:
El contorno
Consiste en diseñar el modo de organizar los recursos de red, para ello es preciso decidir el número de dominios, unidades Organizacionales, árboles de dominios y bosques que se van a crear, así como los nombres que se desea dar a los mismos
Estructura de la organización.
Es mejor respetar las divisiones administrativas que existen en la organización y diseñar una estructura de acuerdo a sus necesidades.
Dimensión de la organización
Antes de iniciar el diseño es importante conocer la dimensión de la organización, si es Una empresa mediana, pero con aspiraciones de llegar a ser una multinacional. En habrá que diseñar el entorno teniendo muy en cuenta las perspectivas de crecimiento del directorio activo más allá de las fronteras nacionales.
Factores técnicos.
Es preciso conocer a fondo las limitaciones que presenta el directorio activo antes de iniciar el diseño del entorno de trabajo, así como la forma en que se

utilizan las políticas de grupo y el modo en que éstas pueden afectar al diseño.

Se dice que cuando sólo existe un dominio para la totalidad de la empresa, la administración es más fácil, sin embargo esto dependerá de la dimensión de la Empresa. Para la creación de bosques, lo aconsejable, en casi todos los casos, es que Exista un solo bosque en la Infraestructura del directorio activo.

El siguiente paso consiste en planificar a Implementación física del diseño. Entre los factores que habrá que considerar va desde los requisitos de hardware de los controladores de dominio a la topología de sitios para la replicacion del directorio activo, así como la Implementación del servicio DNS.
Los sitios determinan la forma en que se replican los datos a través de la red. Y el diseñar su topología es quizá, la parte más complicada del diseño del directorio activo, ya que ellos permiten controlar el momento la frecuencia con que se realiza la replicacion del directorio activo. También habrá que interiorizarse en algunos de los protocolos que utiliza el directorio activo, para conocer el efecto sobre él.

Como se puede percibir la Implementación del servicio, no es nada sencillo y requiere conocer de antemano cómo y cuánto se va a utilizar el directorio activo.

7. POLÍTICAS DE GRUPO

Las políticas de grupo del directorio activo definen las configuraciones de grupos de usuarios y equipos, para controlar su acceso a los recursos de red. Utilizándolas se puede crear un entorno de trabajo que se adapte a las necesidades de cada usuario.

Las políticas de grupo se definen de dos formas:

- *Configuración de equipos.*
  Especifica el proceder del sistema operativo, la apariencia del escritorio, la configuración de las aplicaciones, de seguridad y los `scripts` de iniciar y apagar la computadora. Se aplican cuando se inicia el sistema operativo.

- *Configuración de usuarios.*
  Configura información especifica del usuario, tales como acceso al panel de control, la configuración de red, de escritorio (fondo, protector de pantalla, etc.), de Internet Explorer, e instalación de software, etc. Se aplica al momento en que el usuario se conecta a una computadora con su cuenta y contraseña.

Tipos de políticas de grupo

Las políticas de grupo en Windows 2000 permiten a un administrador establecer unos requerimientos para un usuario o para un equipo a la vez, y estos requerimientos son forzosos.
Se pueden configurar las siguientes políticas de grupo:
a) Directrices administrativas. Configuraciones basados en el registro, opciones de configuración de aplicaciones, apariencia del entorno de trabajo, y el

comportamiento de los servicios del sistema
b) Configuraciones de Seguridad. Opciones para equipos locales, dominios y configuraciones de seguridad de la red.
c) Instalación del software. Administración central de instalación de software, actualizaciones y eliminaciones.(Ej: aplicaciones disponibles para usuarios y aquellos que aparecen en sus escritorios)
d) Scripts. Para cuando un equipo arranca o se apaga y para cuando un usuario inicia sesión o la termina.
e) Redirección de carpetas. Almacenamiento de las carpetas de usuario de la red.

Orden de Herencia en la aplicación de políticas de grupo

Cada objeto menor hereda permisos de un objeto mayor. En el nivel más superior, las Directivas de grupo se pueden aplicar a un sitio. El siguiente nivel que se comprueba es nivel de todo el dominio. Después las unidades organizaciones y todos sus niveles.

Los derechos de acceso se aplican a los grupos y cuentas de usuarios y autorizan al grupo o usuario a realizar ciertas operaciones. Ya que este derecho requiere la capacidad de leer todos los archivos en dichos servidores, el usuario podrá acceder los datos que de otra manera tenían acceso prohibido a través de permisos en el objeto. Los permisos son atributos de seguridad de objetos, que especifican que usuarios o grupos pueden acceder el objeto así como qué acciones pueden realizar en él.

Las políticas tratan de ayudar a proveer:
La confidencialidad de los datos. Sólo las personas autorizadas deben poder ver la Información.
La integridad de los datos. Todos los usuarios autorizados deben estar seguros de que los datos que obtienen son precisos y de que no fueron modificados de forma Inadecuada.
La disponibilidad de los datos. Los usuarios autorizados deben poder tener acceso a la Información que necesiten, en cualquier momento.

8. EJEMPLO: Creación de cuentas de usuarios y políticas de grupo en el Directorio activo para su aplicación en un centro de computo.

Este ejemplo presenta de forma resumida, como crear cuentas de usuarios en el directorio activo y también aplicar algunas políticas que considere necesarias el supervisor para el acceso de usuarios. La creación de cuentas de usuarios, es una de las opciones que permite el directorio activo.
Los supervisores de 2 centros de computo, están de acuerdo en que hacer funcionar la red en los laboratorios seria bastante tranquilo y divertido, si no fuese por esos Molestosos alumnos que tienen una asombrosa capacidad de complicar las cosas.
En este caso, si las cuentas de usuarios, y los permisos de acceso a los recursos, están Apropiadamente configurados muchos de estos problemas desaparecen.
Se necesita crear cuentas de usuarios, a todos los alumnos de la carrera de Ingeniería de sistemas, de una Universidad, ya que estos son los que mas utilizan los laboratorios, y deben almacenar sus trabajos en cuentas personales, para las cuales hay que definir

un estándar de identificación, un máximo de almacenamiento, y las políticas de grupo Para el acceso, de cada una de las cuentas. Mas adelante se realizara lo mismo para Otras carreras.

No especifica en detalles la creación del dominio, el servicio DNS, y las OU's, todos ellos se supone que ya han sido creados, para simplificar el ejemplo.
a) Se dispone de un equipo Servidor, llamado **CENTROS**, con el Sistema Operativo Windows 2000 Server, el cual tiene instalado el Servicio de Directorio activo.

b) 50 equipos cliente, los cuales utilizan el servicio DNS para identificarse mediante un nombre, y ubicar la localización del dominio, que proporciona la autenticación de los usuarios, para que puedan tener acceso a los recursos.

c) Las maquina cliente llevaran inicialmente la letra M seguida de un numero y estarán en el rango de **(M50 hasta M74)** para una OU y el rango de **(M75-M99)** para la otra OU.

d) El dominio al cual tendrán acceso las maquinas cliente será denominado **Dominiocentros.**

e) El Directorio Activo se compone de objetos que representan recursos de la red, como los usuarios, equipos e impresoras; estos se organizan en unidades organizacionales (OUs). Se han creado 2 OU's, denominadas **CENTRO306 y CENTRO307.**

f) Las cuentas para los estudiantes deberán ser creadas antes de implementar las políticas. Para ello se debe:
1) Abrir el menú de Administrative Tools, y hacer click en Active directory Users and Computer
2) Colocarse en la carpeta Users, hacer click en botón derecho y seleccionar New. Aparecerá varias opciones. Como se quiere crear un nuevo usuario, hacer click en User.
3) Aparecerán las siguientes opciones, que deberán ser llenadas con los datos del alumno.
First Name, Initials, Last Name, Full Name, User logon name (el cual deberá ser único en el directorio activo)
4) El estándar a emplearse será, el primer apellido paterno completo, la inicial del segundo apellido, y la inicial de su nombre: Cuellargv (Cuellar Gómez Verónica), en el caso de existir otro usuarios con las mismas iniciales, se colocara un numero después, para diferenciar a los estudiantes, de modo que sea único.
5) Luego hacer click en Next, y le pedirá el password y su confirmación, el cual será el Registro del estudiante dentro de la Universidad. (Ej: 76985)
6) Y tickear las opciones: User cannot change password y el Password never expires, para tener el control de la cuenta del usuario, como administrador.

Una vez creada la cuenta del usuario, se pueden personalizar una serie de opciones que complementen sus datos.
Para ello:

1) Ubicar la cuenta de usuario en el dominio, hacer click en botón derecho y elegir la opción de Properties.
2) Se abrirá una ventana con una serie de opciones para implementar.

Los grupos simplifican la administración ya que permiten dar permisos a varios usuarios, en vez de uno por uno. Un grupo puede tener hasta 5.000 usuarios como miembros.

En este caso se crearan grupos Locales, para ello:
Abrir Active Directory Users and Computers, que se encuentra en el menú Administrative Tools
Elegir la opción de Users, y hacer botón derecho para elegir New y luego Group.
Le aparecerá una ventana, con las siguientes opciones:
Group Name: Aquí se especifica el nombre del nuevo grupo, el cual debe ser único en el dominio, donde haya sido creado. (Ej: AlumnoSistemas)
Group scope: Tiene 3 opciones el Dominio local, Global y Universal.
En nuestro caso será un Dominio Local, el que se elegirá.
Group Type: Aquí aparecerán 2 opciones para seleccionarse. Security y Distribution
En nuestro caso se usara el Security Groups, ya que aquí puede se usado para asignar permisos, y puede usarse en una lista de distribución de e-mail.
Luego de elegir todo, hacer click en OK

Una vez creado el grupo, se deben adicionar los miembros al grupo de dominio. Pueden incluir cuentas de usuarios y computadoras. Para ello:
1.- Seleccionar botón derecho, al grupo que se ha creado, y hacer click en Properties y elegir la opción de Members, y luego click en Add (para adicionar).
2.- Se abrirá una nueva pantalla, en la parte superior Look in: elegir el **Dominiocentros**
3.- En la columna Name, le aparecerán la lista de todos las cuentas de usuarios, elegir las cuentas de alumnos de sistemas y click en Add.
4.- Una vez terminada la selección de todas la cuentas, Click Ok para adicionar a los miembros del grupo, y luego click OK otra vez.
Una vez definido el grupo al cual pertenecerán los usuarios, en este caso al grupo AlumnoSistemas

Se debe proveer una localización centralizada, en la cual los usuarios puedan almacenar sus trabajos. Por ello se creara un Folder de nombre ALUMNOS, y dentro de el, las carpetas para cada usuario, con el mismo nombre de su cuenta.
Lo cual se realizara en Computer Management, y luego en Shared Folders
Después de creadas las cuentas de cada usuario, se debe especificar la cantidad máxima de almacenamiento, para sus archivos. Lo cual es denominado asignar cuotas de disco.

1) En Computer Management, elegir Disk Management y seleccionar la unidad de disco, en la cual se almacenaran los folder de cuentas de usuarios.
2) Botón derecho y elegir Properties, aparecerá una pantalla, hacer click en Quota.
3) Tickear la opción Enabled Cuota Management, para que se active las demás opciones. Deny disk space to users exceeding cuota limit

4) Limitar el espacio de disco que los usuarios pueden utilizar. En nuestro caso será de: 10 MB y de 6MB para el conjunto de errores.
5) Luego click en Quota Entries, en la cual se abrirá una nueva pantalla, en la barra de menu elegir New Quota Entry.
6) En la nueva pantalla seleccionar el usuario, o el grupo al cual se le asignara la cuota, y clik en Add. Luego OK. Aparecerá una pantalla de confirmación de la cuota a implementarse.
7) Luego cerrar la ventana, y click en OK para que sea aplicada la cuota.
Cuando las carpetas hayan sido creadas y se les haya asignado un máximo de almacenamiento. Se deberá compartir el Folder ALUMNOS para que cada usuario que esta contenido allí, pueda acceder a los recursos que necesite.
1) En el Shared Folder, botón derecho y se abrirá una pantalla, elegir Sharing
2) Hacer click en Share this folder.
En share Name: ALUMNOS
Comments: Cuenta Alumnos de Sistemas
Y una opción que puede ser opcional, como es el User limit Y luego click en Permisos

En los cuales se seleccionara de Lectura, cambios, control total, escritura. Elegir los que se considere necesarios como administrador.
Como los usuarios ya tienen acceso a sus cuentas, y a las computadoras del centro de computo, es importante especificar su acceso a los recursos, establecidas por la políticas de grupo.

La sección de User configuration, tiene 3 opciones generales para las políticas de grupo

Software Settings
Windows Settings
Administrative Templates.

Para nuestro ejemplo, todas las opciones de políticas que deberán ser fijadas a los usuarios, será realizadas en el Administrative Templates, la cual provee internamente estas opciones:
Componentes de windows, Start Menu & Taskbar, El escritorio, Panel de Control., Red y Sistema.

Se puede seleccionar una serie de politicas, para proveer la seguridad en la red. Ello dependerá de las necesidades de cada organización. En el caso del ejemplo de Centro de computo, serán aplicadas estas políticas.

Política	Acción requerida
Administrative Templates/Windows Components/Internet Explorer	
Disable changing history settings	Activada
Disable changing font settings	Activada
Disable changing language settings	Activada
Disable changing Temporary Internet files settings	Activada
Administrative Templates/Windows Components/Internet Explorer /Toolbars	

Disable customizing browser toolbar buttons	Activada
Administrative Templates/Windows Components/Internet Explorer /Browser	
Tools menu: Disable Internet Options ....menu options	Activada
Administrative Templates/Desktop	
Don't save settings at exit	Activada
Remove Run menu from Start menu	Activada
Disable/Remove the shut Down command	Activada
Administrative Templates/Control Panel/Start Menu & Taskbar	
Remove Run menu from start menu	Activada
Administrative Templates/Control Panel	
Disable control panel	Activada
Disable Add/Remove Programs	Activada
Disable Display in Control Panel	Activada
Disable deletion of printers	Activada
Administrative Templates/Network	
Prohibit TCP/IP advanced configuration	Activada

Otras Medidas de Seguridad a considerarse en los centros de computo

Al implementar un Servidor, independientemente de cual sea el entorno de trabajo, es muy recomendable tomarse en serio la seguridad.
En los centros de computo se deben tomar ciertas medidas de seguridad, tanto en la parte física (Hardware), como en la parte de datos (Software) para problemas mayores que impidan el normal desarrollo de las actividades.

SERVIDOR
a) Software

Una de las principales medidas de protección contra ataques, es mantener el entorno actualizado con todas las revisiones de seguridad necesarias, las que pueden ser Aplicadas tanto para el servidor como para los clientes.
Las más fáciles de implementar sin que ello demande mucho el costo, en este caso podrían ser:

- Mantener actualizados los Parches para las distintas aplicaciones que están Instaladas en el servidor; EJ: Internet explorer.
- También es importante actualizar el **`Service Pack,`** para una mayor seguridad en el Sistema operativo. Tanto los parches como el Service Pack pueden ser bajados de la pagina de http://windowsupdate.microsoft.com/
- Verificar que no tenga los permisos por defecto que se habilitan en la instalación del Sistema Operativo, para ello revisar, a través de otro equipo: EJ: \\centros\C$
- Hacer discos espejos, ello permite mantener exactamente la misma información de la base de datos que aparecen al mundo real, como una entidad única. Windows 2000 soporta volúmenes en espejo y RAID-5 que protegen a los datos contra errores de disco.
- Hacer BackUp, Lo cual se utiliza para proteger los datos de los fallos de dispositivos

de Almacenamiento o del hardware.
- Desinstalar software innecesario.
- Evitar abrir archivos adjuntos que venga con mensajes no esperados, o de personas extrañas.
- No se debe conceder a los servicios más privilegios de los necesarios.
- Se debe tener instalado en el equipo Software Antivirus y bajar regularmente las actualizaciones, para evitar todo tipo de virus que pudiera atacar, e impedir la ejecución de archivos necesarios.

Recomendaciones a supervisores encargados

- La contraseña para el servidor debe ser bien elegida por los supervisores, es recomendable que sea una combinación de letras y números. Y mejor si se lee al lado inverso para evitar su fácil reconocimiento.
- Los supervisores no deberían reutilizar una contraseña en particular, que haya sido conocida por algún usuario externo.
- Se debe cambiar regularmente la contraseña, para evitar problemas con los usuarios molestosos.
- Se debe educar a los supervisores sobre la privacidad de las contraseñas, la cual solo deben mantener en conocimiento con sus compañeros de trabajo, y no así otras personas externas.
- Concientizar a los supervisores que deben bloquear la maquina al ausentarse de la misma, por ello es recomendable, colocar un pequeño cartel en un lugar visible, que haga referencia a esta acción.
- Las copias de seguridad del sistema, que se realicen en Cd's deben ser guardadas en un lugar cercano, y bajo llave.

9. CONCLUSIÓN

La seguridad es una parte importante de una organización, ya que un sistema de información con una seguridad débil llegará a verse comprometido. Muchas empresas consideren que el peligro de violar la seguridad es poco probable que se de a un nivel interno. Por ello no se dan el trabajo de ser minuciosos en proveer solo la información que necesitan sus usuarios. Y solo cuando sucede algo grave es cuando toman medidas necesarias para disminuir el daño.

La puesta en práctica de las políticas del grupo, en el directorio activo ayuda a los administradores a crear los ambientes de escritorio adaptados a la responsabilidad del trabajo de cada usuario, que proporciona el acceso a los recursos de una manera específica.

10. REFERENCIAS

[1] No author. 1.2 SANS Security Essentials II: Basic Security Policy. SANS Institute.
[2] No author. 5.3 SANS Security Essentials V: Windows 2000 Security. SANS Institute.
[3] Documento Pedro Gómez. Grupo Eidos. Windows 2000 Madrid (España), 2000.
URL: www. grupoeidos.com
[4] Implementing and Administering Microsoft Windows 2000 Directory Services
[5] URL: http://club.telepolis.com/jlrosalesf/articulo_w2000c11.htm
[6]
URL: http://www.softdownload.com.ar/cursos/windows2000/directorio_activo.zip
[7]URL:http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGW01/CENTRAL_directorio_activo_y_la_seguridad.htm#Ventajas%20de%20la%20administración%20de%20cuentas%20de%20directorio%20activo
[8]
URL:http://www.windowstimag.com/atrasados/2000/48_dic00/articulos/especial.htm
[9]
URL: http://www.windowstimag.com/atrasados/2000/39_feb00/articulos/directorio.htm
[10]
URL:http://www.microsoft.com/spain/technet/recursos/articulos/welcome3.asp?opcion=18
[11]
URL:http://www.microsoft.com/spain/download/servidores/windows2000/Estructura-del-Directorio-Activo.doc
[12]
URL:http://www.microsoft.com/spain/download/servidores/windows2000/Directorio-Activo.doc
[13]
URL:http://www.microsoft.com/spain/download/servidores/windows2000/Active-Directory-Design.doc

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event