openSUSE 13.1 con Active Directory

Guía Ilustrada

openSUSE™

samba

Eduardo Adolfo Sotomayor G.

Configuración inicial del SO

Instalación de samba 4.x

Provisionamiento de samba 4.x

Configuración de DNS

Configuración de Kerberos

Configuración de ntp

Ajustes de seguridad

Configurando el servicio samba

Compartiendo Archivos

Configurando el Firewall

Uniendo estaciones de trabajo al dominio

Usando las RSAT (Remote Server Administration Tools)

El entorno de red.

DNS

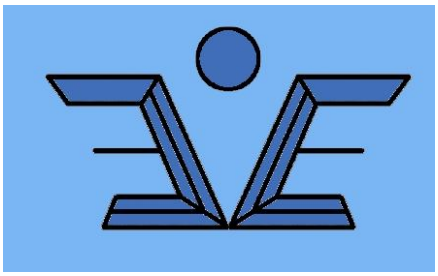
DHCP

Permisos locales

En este manual se explica paso a paso con ilustraciones como instalar un controlador de dominio con samba 4.1 en openSUSE 13.1 con BIND como backend para DNS, en este caso se explica una implementación para la empresa SIENIC (Sistemas Informáticos de Entretenimiento) que cuenta con una red de 125 computadoras, a lo largo del manual se explica desde la instalación de samba 4.1 hasta la configuración y creación de políticas de grupo, delegación de privilegios, creación de grupos de seguridad, creación de usuarios, el manejo del DNS y DHCP, tratando de cubrir todos los aspectos básicos que se requieren para empezar a utilizar un controlador de dominio.

Esta guía no pretende ser una Biblia de samba 4.1 ni de Active Directory, pero si una herramienta que ayudara al administrador de red a tener una visión amplia de las cosas que se pueden hacer con Active Directory y tener una idea clara de que dirección tomar una vez terminada la implementación.

Samba es un proyecto que está evolucionando rápida y constantemente por lo que se recomienda estar al pendiente de nuevas versiones en el sitio oficial, para estar al día con estos cambios.

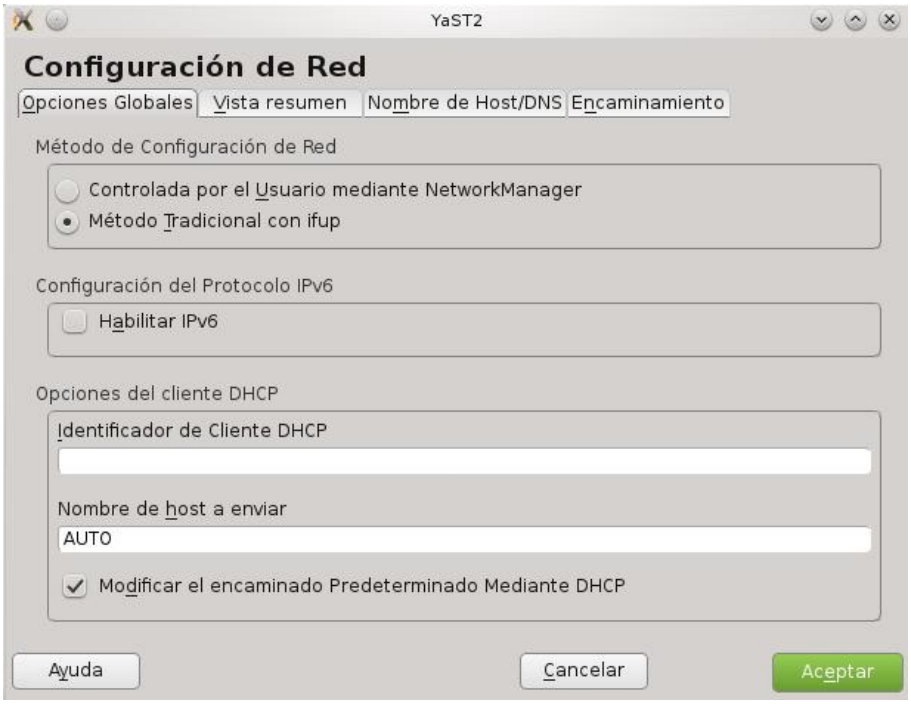


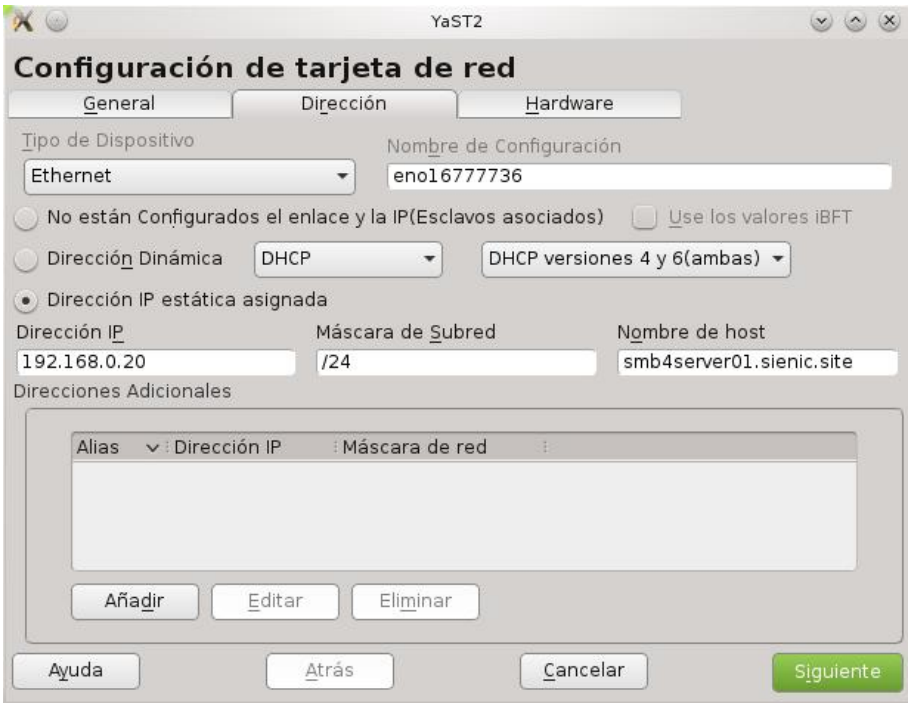
http://easgs.wordpress.com/

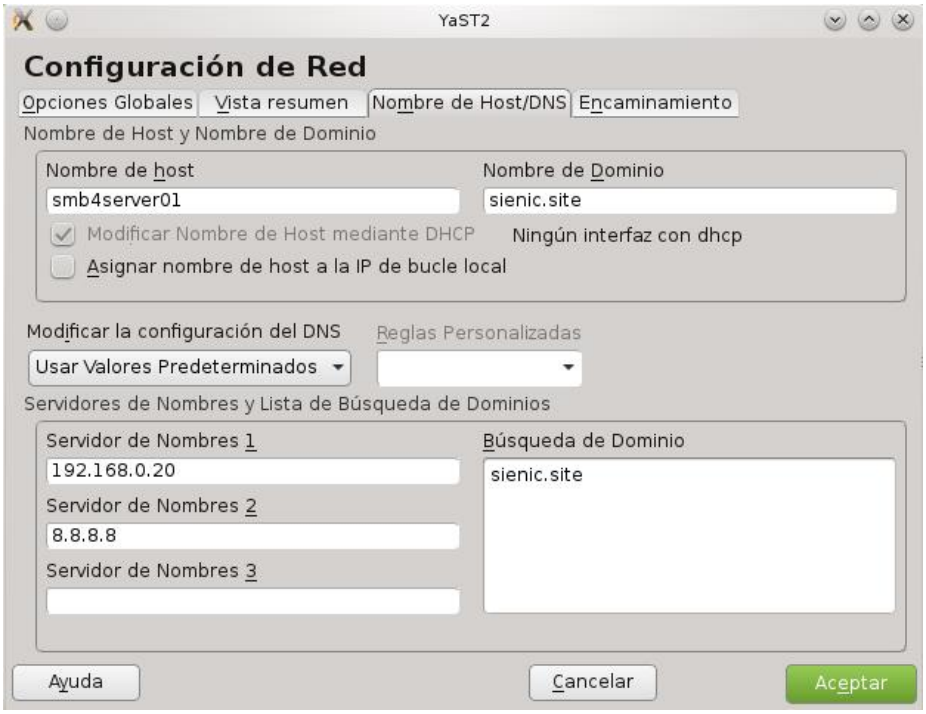
Configuración inicial del SO

Configuración de la red

Lo primero que hay que hacer es configurar una dirección IP estática para ello nos vamos a **Yast/Dispositivos de red/Configuración de red** y realizamos las configuraciones que se muestran a continuación adecuando las opciones a su respectivo caso.

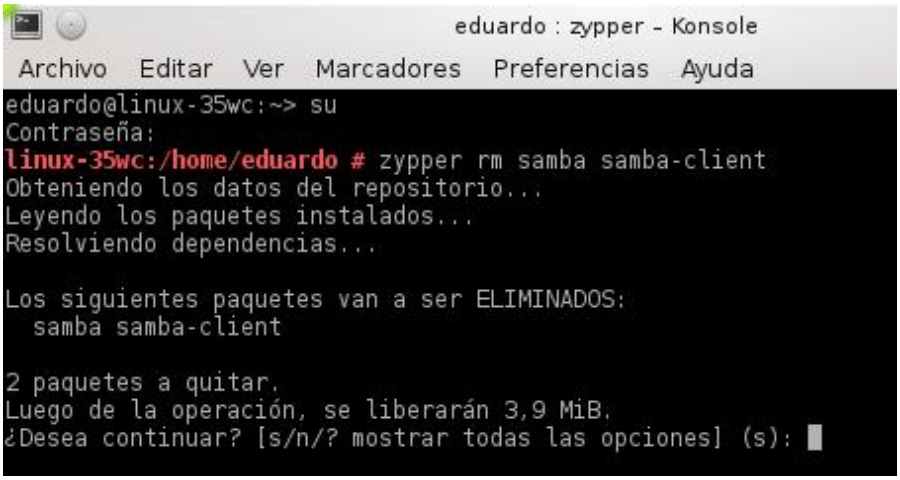






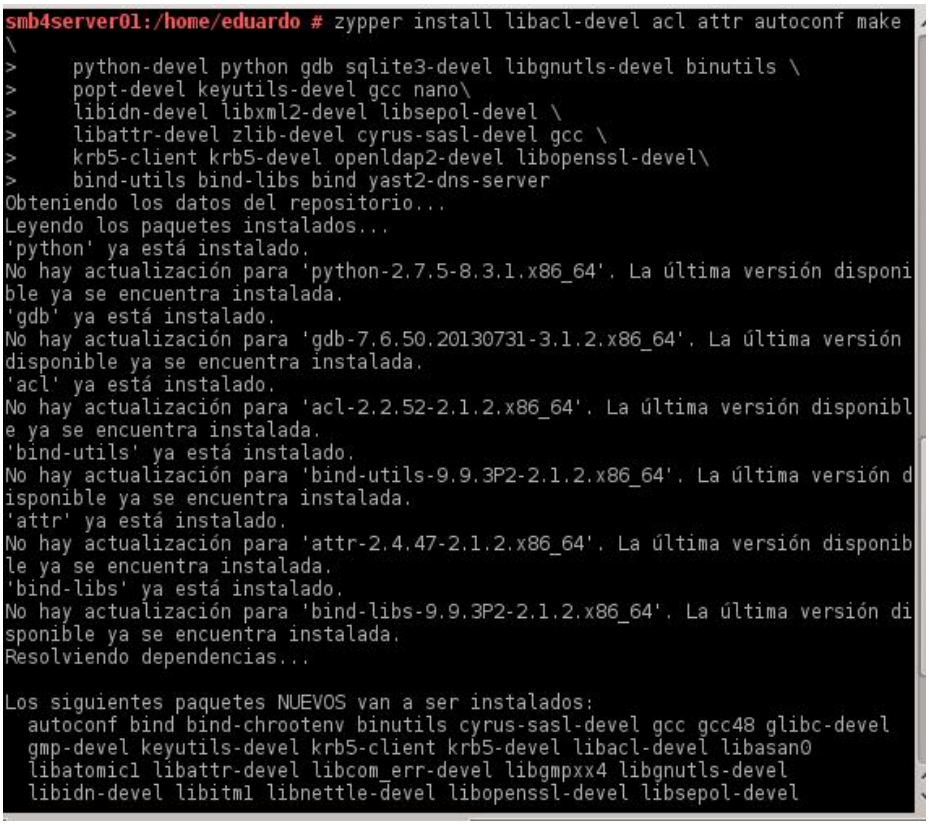
Desinstalar los paquetes samba que vienen con la distribución

zypper rm samba samba-client



Instalar los paquetes necesarios.

```
zypper install libacl-devel acl attr autoconf make \
    python-devel python gdb sqlite3-devel libgnutls-devel binutils \
    popt-devel keyutils-devel gcc \
    libidn-devel libxml2-devel \
    libattr-devel zlib-devel cyrus-sasl-devel gcc \
    krb5-client krb5-devel openldap2-devel libopenssl-devel\
    bind-utils bind-libs bind yast2-dns-server
```



Instalación de samba 4.x

Descargar samba 4.x

http://www.samba.org/samba/ftp/stable/samba-4.1.3.tar.gz

Instalar samba

tar -xzvf samba-4.1.3.tar.gz

cd samba-4.1.3

./configure && make && make install

Editar los PATH

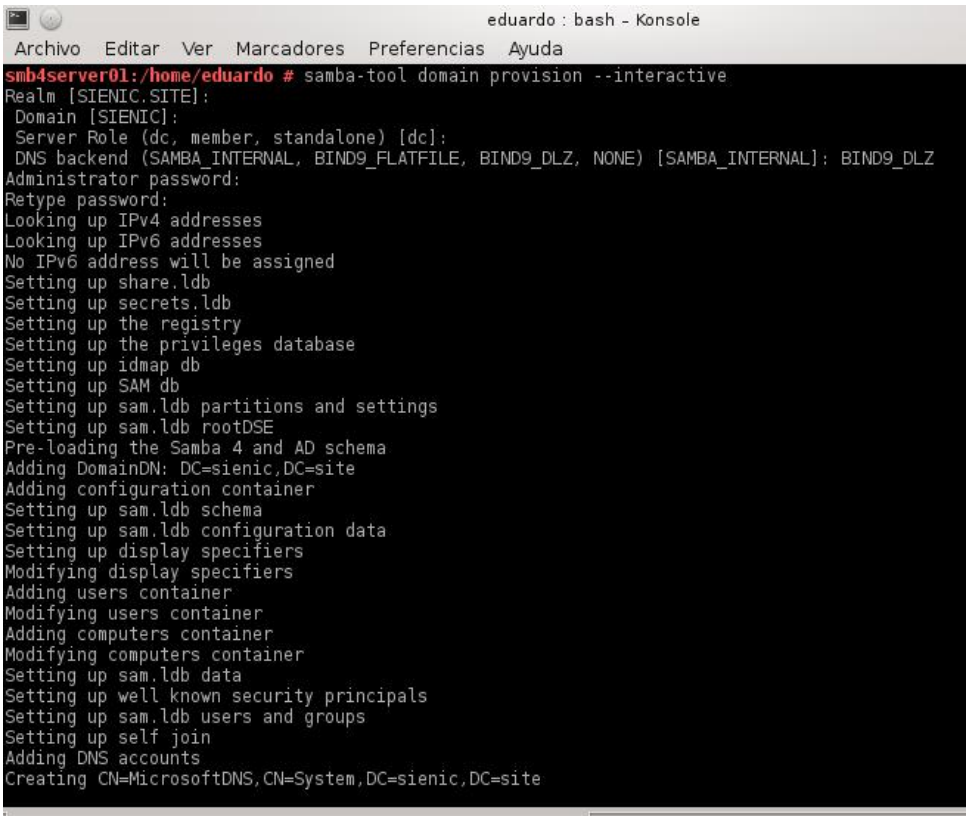
Editar el archivo ~/.bashrc y agregar lo siguiente al final

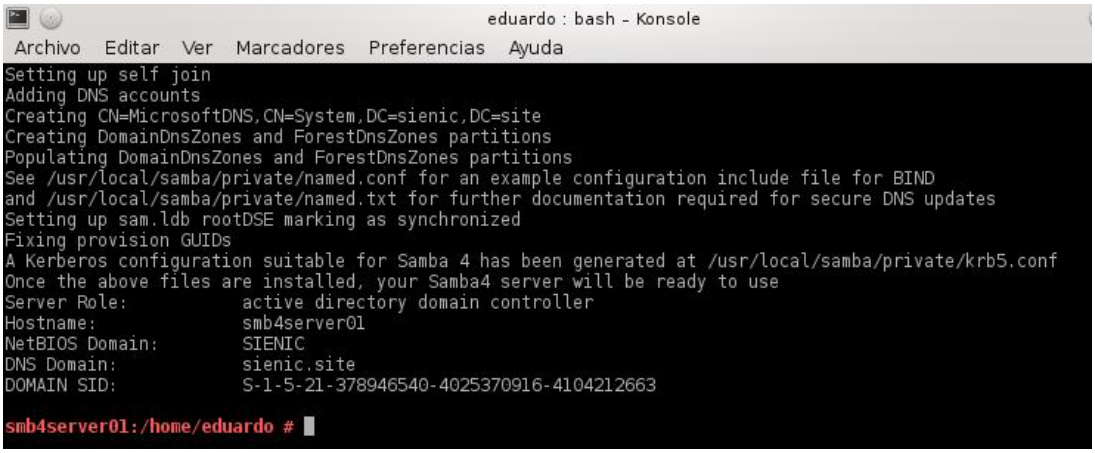
export PATH=$PATH:/usr/local/samba/sbin:/usr/local/samba/bin

Provisionamiento de samba 4.x

Provisionar samba

```
samba-tool domain provision --interactive
```





Iniciar samba

Es necesario iniciar samba manualmente

samba

Reiniciar samba

Estos son los comandos necesarios en caso que necesitemos reiniciar samba

```
killall samba
samba
```

Volver a leer la configuración de smb.conf

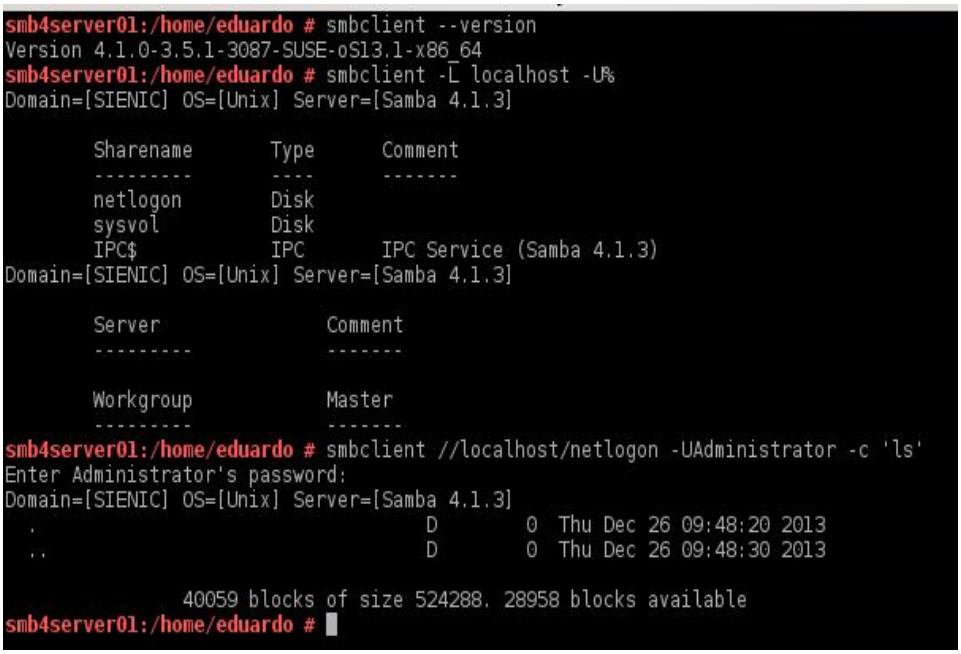
```
smbcontrol all reload-config
```

Probar conectividad

Los siguientes comando nos sirven para probar el servidor, el primero es para verificar la versión de samba, el segundo es para listar los recursos compartidos en el servidor, el ultimo es para probar la autenticación conectándonos a netlogon usando las credenciales de administrator.

```
smbclient --version
smbclient -L localhost -U%
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

La salida de estos comandos debe ser similar a la mostrada en la siguiente imagen

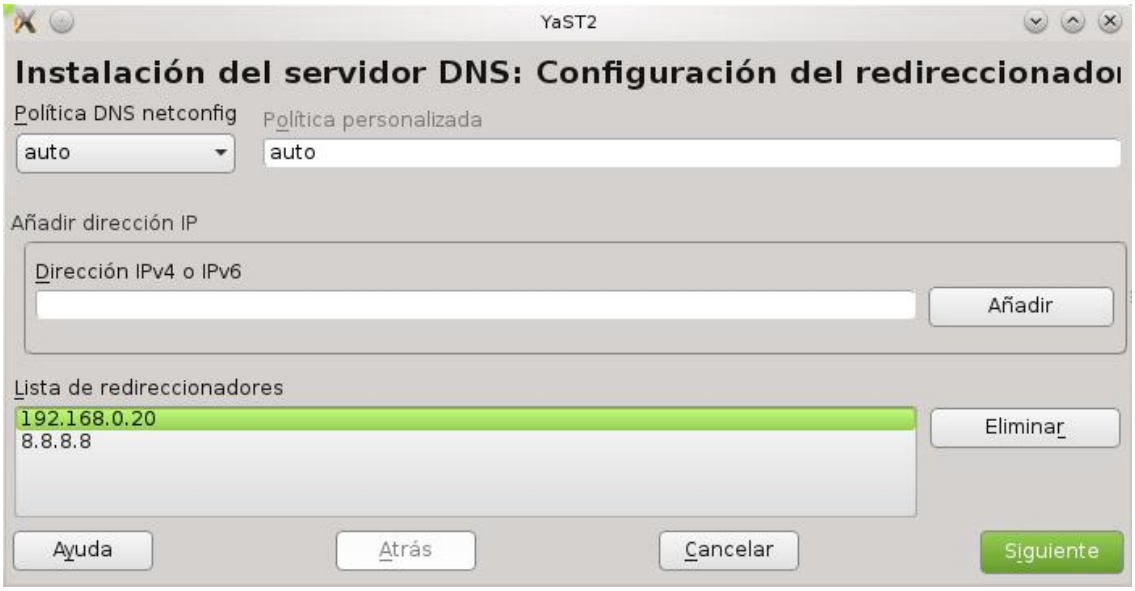


Configuración de DNS

Configurar Bind

Yast/servicios de red/servidor DNS

En **Lista de redireccionadores** poner el ip de este servidor DNS y del servidor DNS del ISP o el que convenga y clic en añadir.



Hacemos clic en **Siguiente** y procedemos a eliminar la zona ipv6 que aparece en la lista de zonas si no hacemos uso de ipv6 y damos clic en **siguiente**.

En esta pantalla seleccionamos las opciones a como se muetran en la siguiente imagen y damos clic en **terminar**.

Ahora nos vamos a **Yast/Seguridad y Usuarios/Configuracion Apparmor**

Seleccionamos **Configuracion** y hacemos clic en **ejecutar**

Quitamos el check a **Habilitar AppArmor**

Le damos los permisos adecuados a la carpeta /usr/local/samba/private/dns

chown named:named -R /usr/local/samba/private/dns

Ahora procederemos a editar el archivo /etc/named.conf y agregamos lo siguiente en la sección de opciones:

```
tkey-gssapi-keytab "/usr/local/samba/private/dns.keytab";
```

Luego agregamos esto al final del archivo

```
include "/usr/local/samba/private/named.conf";
```

Editamos el archivo /usr/local/samba/private/named.conf y habilitamos la sección

database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so";

Y comentamos la opción que estaba habilitada por defecto que es

database "dlopen /usr/local/samba/lib/bind9/dlz_bind9.so";.

El archivo debe quedar a como se muestra en la siguiente ilustración

```
# This DNS configuration is for BIND 9.8.0 or later with dlz_dlopen support.
#
# This file should be included in your main BIND configuration file
#
# For example with
# include "/usr/local/samba/private/named.conf";

#
# This configures dynamically loadable zones (DLZ) from AD schema
# Uncomment only single database line, depending on your BIND version
#
dlz "AD DNS Zone" {
    # For BIND 9.8.0
    #database "dlopen /usr/local/samba/lib/bind9/dlz_bind9.so";

    # For BIND 9.9.0
     database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so";
};
```

Editamos el archivo /etc/sysconfig/named y modificamos las siguientes opciones para que queden asi:

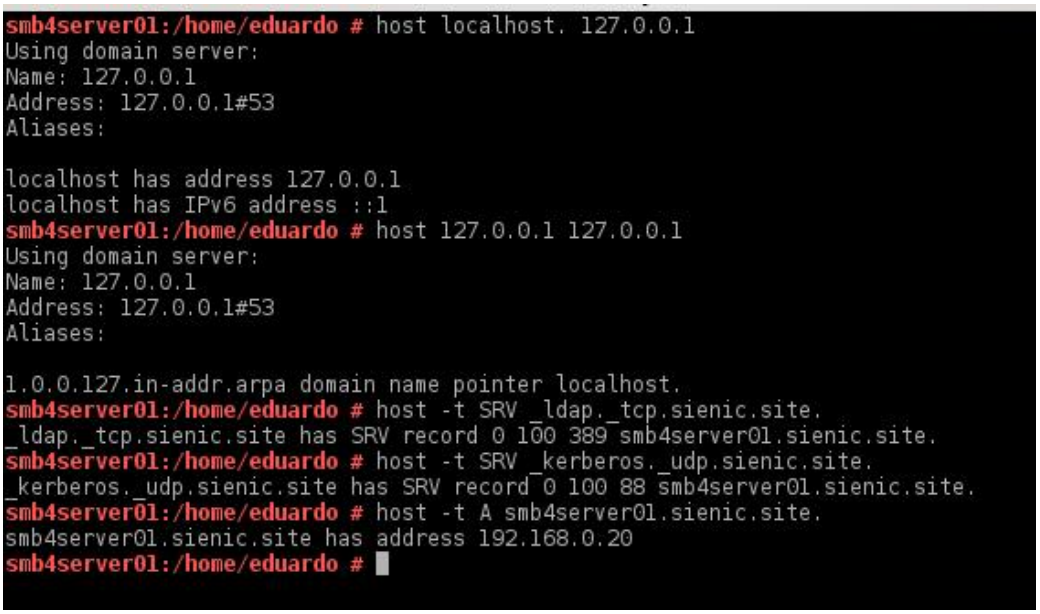
```
NAMED_RUN_CHROOTED="no"
```

Opcionalmente podemos deshabilitar el uso de ipv6 si no lo utilizamos en nuestra red.

```
NAMED_ARGS="-4"
```

Probando DNS

```
# host localhost. 127.0.0.1
# host 127.0.0.1 127.0.0.1
# host -t SRV _ldap._tcp.sienic.site.
# host -t SRV _kerberos._udp.sienic.site.
# host -t A smb4server01.sienic.site.
```



Configuracion de Kerberos

Configurar Kerberos

Editamos el archivo /etc/krb5.conf y le ponemos el siguiente contenido suponiendo que el nombre del realm es SIENIC.SITE, este tiene que estar escrito en mayúsculas.

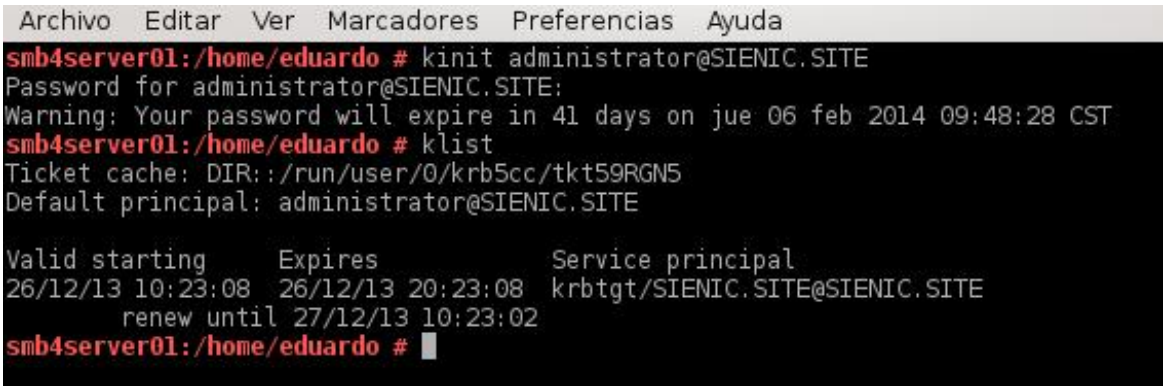
[libdefaults]

default_realm = SIENIC.SITE
dns_lookup_realm = false
dns_lookup_kdc = true

Probando kerberos

 # kinit administrator@SIENIC.SITE

 # klist



Configuración de ntp

Configurar ntp

Nos vamos a la ruta /usr/local/samba/var/lib/ y cambiar los permisos del directorio ntp_signd

chgrp -R ntp /usr/local/samba/var/lib/*ntp_signd*

chmod -R 750 /usr/local/samba/var/lib/*ntp_signd*

Editamos el archivo /etc/ntp.conf y le ponemos el siguiente contenido:

```
server 127.127.1.0
fudge 127.127.1.0  stratum 12
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
restrict default mssntp
```

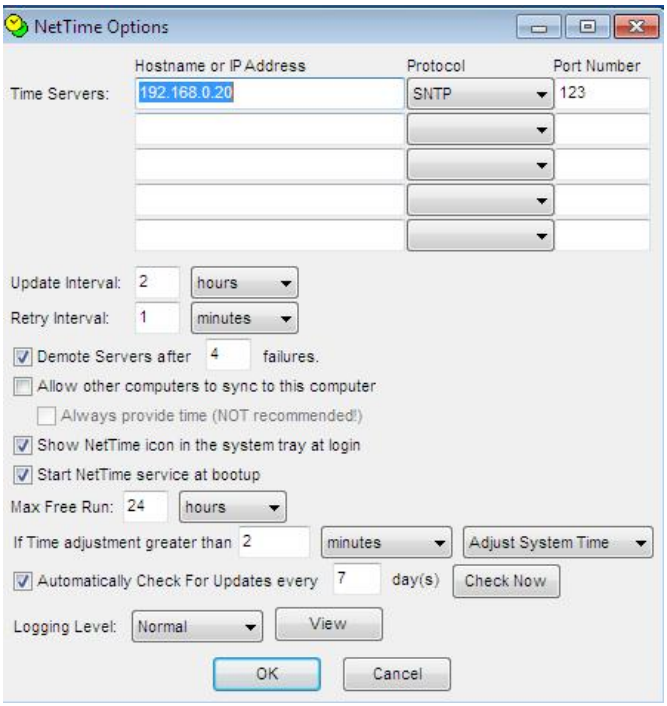
Habilitar y arrancar el servicio ntp

Los comando para habilitar y arrancar el servicio NTP son:

systemctl enable ntp.service

systemctl start ntp.service

Sugerencia: Una excelente herramienta para mantener sincronizados los relojes en las estaciones de trabajo con Windows es http://www.timesynctool.com/



Ajustes de seguridad

Cambiar políticas de complejidad de password

samba-tool domain passwordsettings set --complexity=off

samba-tool domain passwordsettings set --min-pwd-length=5

samba-tool domain passwordsettings set --history-length=0

samba-tool domain passwordsettings set --min-pwd-age=0

samba-tool domain passwordsettings set --max-pwd-age=0

Para ver las políticas actuales.

samba-tool domain passwordsettings show

```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
smb4server01:/home/eduardo # samba-tool domain passwordsettings set --complexity=off
Password complexity deactivated!
All changes applied successfully!
smb4server01:/home/eduardo # samba-tool domain passwordsettings set --min-pwd-length=5
Minimum password length changed!
All changes applied successfully!
smb4server01:/home/eduardo # samba-tool domain passwordsettings set --history-length=0
Password history length changed!
All changes applied successfully!
smb4server01:/home/eduardo # samba-tool domain passwordsettings set --min-pwd-age=0
Minimum password age changed!
All changes applied successfully!
smb4server01:/home/eduardo # samba-tool domain passwordsettings set --max-pwd-age=0
Maximum password age changed!
All changes applied successfully!
smb4server01:/home/eduardo # samba-tool domain passwordsettings show
Password informations for domain 'DC=sienic,DC=site'

Password complexity: off
Store plaintext passwords: off
Password history length: 0
Minimum password length: 5
Minimum password age (days): 0
Maximum password age (days): 0
smb4server01:/home/eduardo #
```

Cambiar la clave de Administrator

samba-tool user setpassword administrator

Agregar permisos administrativos varios al grupo Domain Admins

net rpc rights grant 'SIENIC\Domain Admins' SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege -Uadministrator

```
smb4server01:/home/eduardo # net rpc rights grant 'SIENIC\Domain Admins' SeM
achineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOp
eratorPrivilege SeRemoteShutdownPrivilege  -Uadministrator
Enter administrator's password:
Successfully granted rights.
smb4server01:/home/eduardo #
```

Para listar los permisos asignados escribimos

net rpc rights list accounts –Uadministrator

Cuenta administradora de dominio alterna.

Se recomienda crear una cuenta administradora alterna que pertenezca únicamente al grupo Domain Admins y desde esta cuenta administrar los recursos compartidos, políticas de seguridad y unir máquinas, esto se puede hacer desde RSAT en Windows, para más información de RSAT pasar a la sección Herramientas de administración remota del servidor para Windows en la pagina.

Configurando el servicio samba

Configurando el servicio samba

El siguente paso es configurar el servicio samba para que arranque automaticamente con el servidor, asi como poder detenerlo, reiniciarlo y arrancarlo, para esto creamos un archivo de texto con el nombre samba.service en la ruta `/usr/lib/systemd/system/` con el siguiente contenido.

```
[Unit]
Description=Samba AD Daemon
After=syslog.target network.target

[Service]
Type=forking
PIDFile=/usr/local/samba/var/run/samba.pid
LimitNOFILE=16384
EnvironmentFile=-/etc/sysconfig/samba
ExecStart=/usr/local/samba/sbin/samba $SAMBAOPTIONS
ExecReload=/usr/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

Luego ejecutamos el siguiente comando

```
ln -s /usr/lib/systemd/system/samba.service /etc/systemd/system/samba.service
```

ahora procedemos a habilitar el servicio

```
systemctl enable samba
```

Ahora para administrar el servicio usaremos los siguientes comandos:

Detener el servicio.

```
systemctl stop samba.service
```

Arrancar el servicio.

```
systemctl start samba.service
```

Reiniciar el servicio.

```
systemctl restart samba.service
```

Ver estado del servicio.

```
systemctl status samba.service
```

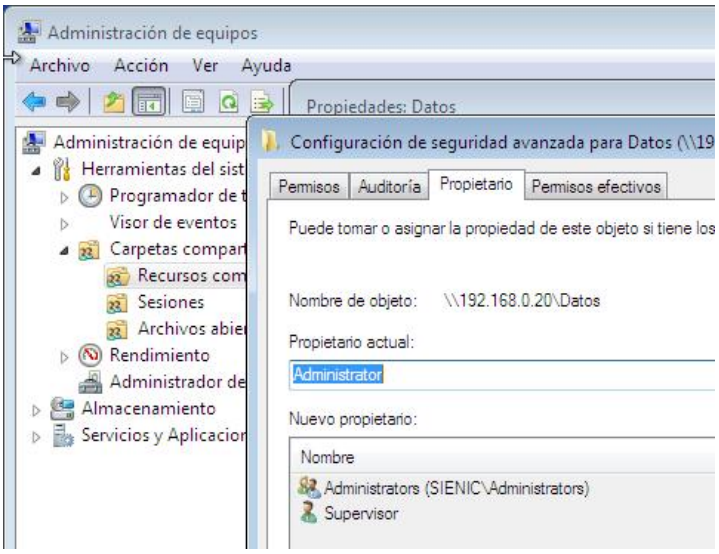
Compartiendo Archivos

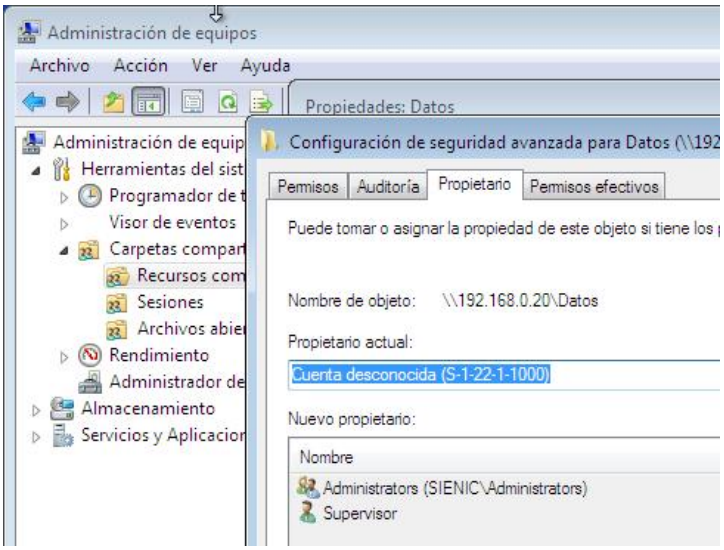
Compartir archivos

Para compartir una carpeta en red es necesario crear la carpeta y asignarle los siguientes permisos, en este ejemplo el nombre de la carpeta es datos, cabe mencionar que el sistema de archivos que tiene la partición donde vamos a compartir los archivos esta formateada con el sistema de archivos XFS.

chown root:root datos

Si no le ponemos como propietario root:root en las propiedades en lugar de administrator va a salir cuenta desconocida.

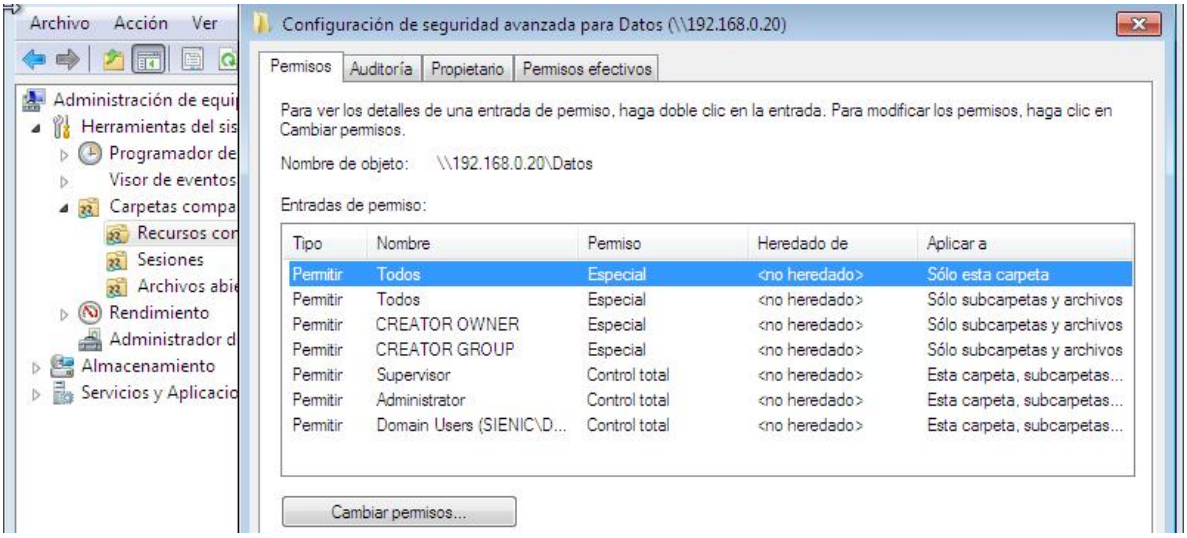


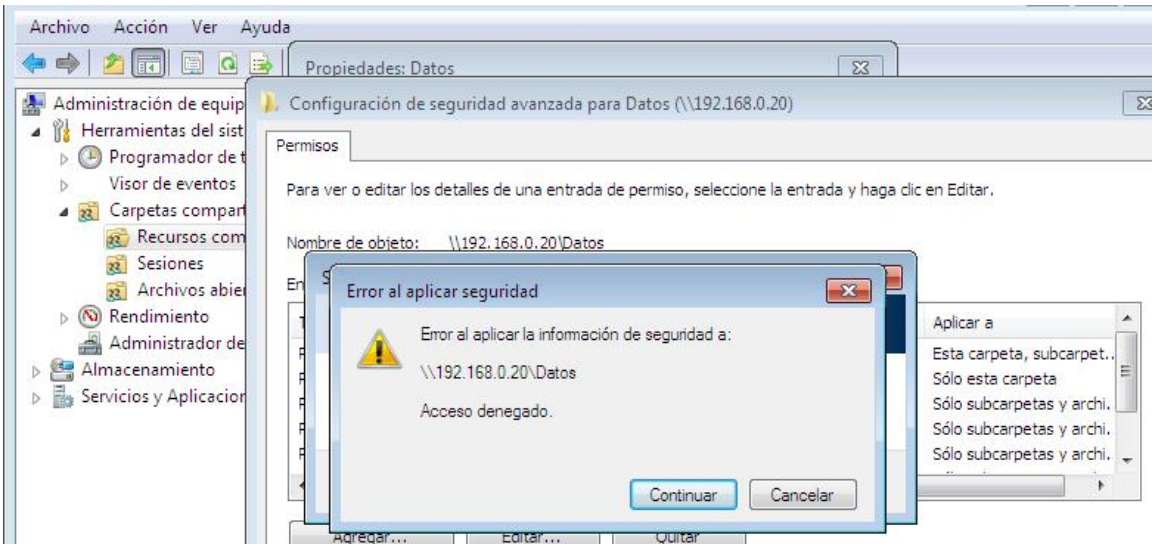


Luego le damos los permisos necesarios.

chmod 777 datos

Si no le damos los permisos 777 y en su lugar le damos algo como 775 no nos permitirá hacer modificaciones a los permisos de configuración de seguridad avanzada.





Luego editamos el archivo /usr/local/samba/etc/smb.conf y creamos la sección del recurso compartido, en adelante todos los permisos se van a administrar desde un equipo con Windows con una cuenta administrativa de dominio.

```
[Datos]
     path = /home/eduardo/datos/
     read only = no
```

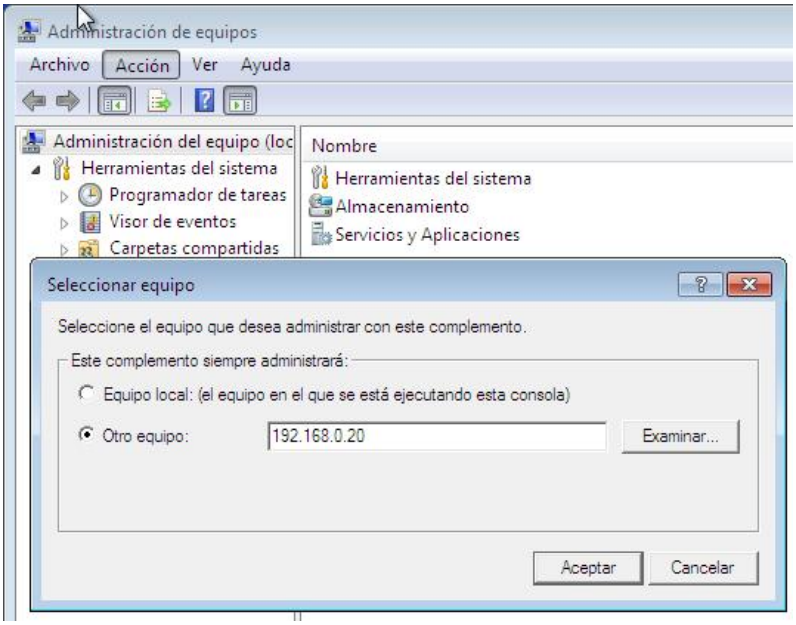
Luego ejecutamos el comando.

```
smbcontrol all reload-config
```

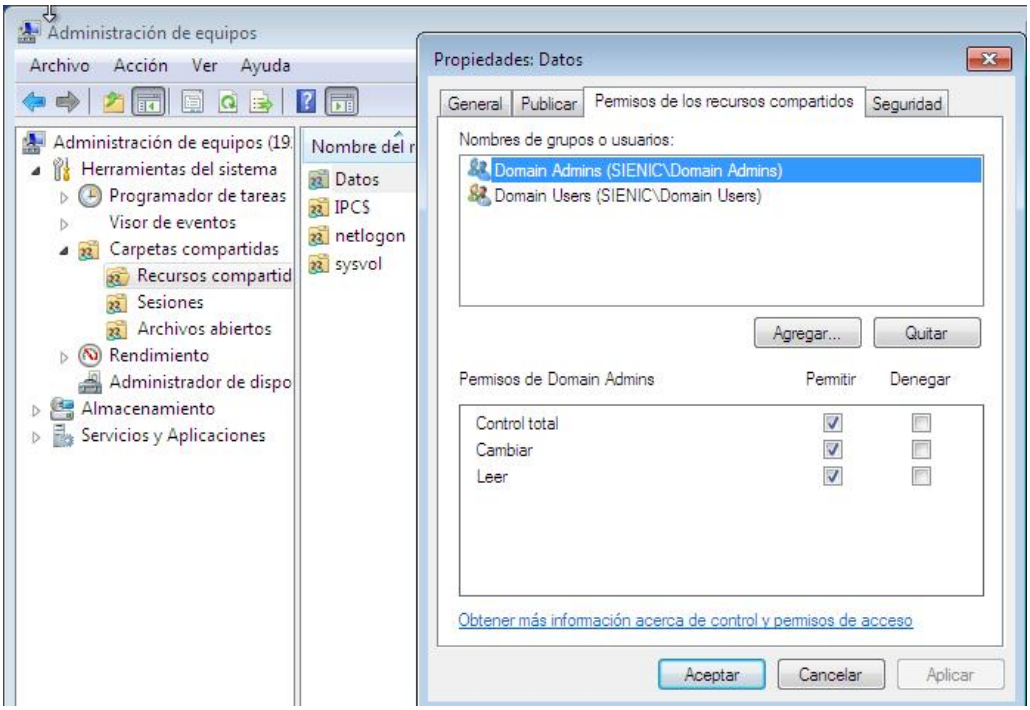
Este comando hace que se vuelva a leer la configuración del archivo smb.conf para que se hagan efectivos los cambios.

Modificar los permisos del recurso compartido.

En una pc con Windows nos vamos a **Administración de equipos/Acción/Conectar con otro equipo** y en el cuadro de dialogo ponemos el IP del servidor y luego damos clic en **aceptar**.



Luego nos vamos a **Herramientas del sistemas/Carpetas compartidas/Recursos compartidos** y seleccionamos la carpeta que configuramos en el servidor le damos con el boton secundario del mouse y seleccionamos **propiedades**, una vez en propiedades podemos configurar los permisos en las solapas "**Permisos de los recursos compartidos**" y "**Seguridad**".



Nota: Para realizar estos cambios la maquina debe estar unida al dominio y la sesion debe ser con una cuenta administrativa.

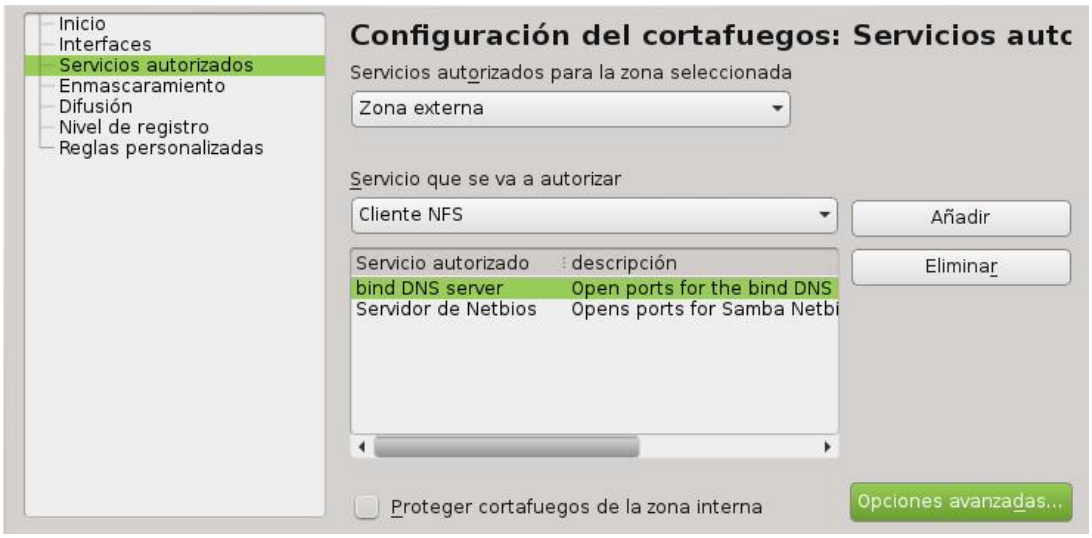
Configurando el Firewall

Abrir los puertos correspondientes en el firewall

Yast/Seguridad y usuarios/Cortafuegos.

Servicios autorizados y de la lista desplegable seleccionamos **Servidor de Netbios** y hacemos clic en **Añadir**

Despues hacemos clic en **opciones avanzadas**.



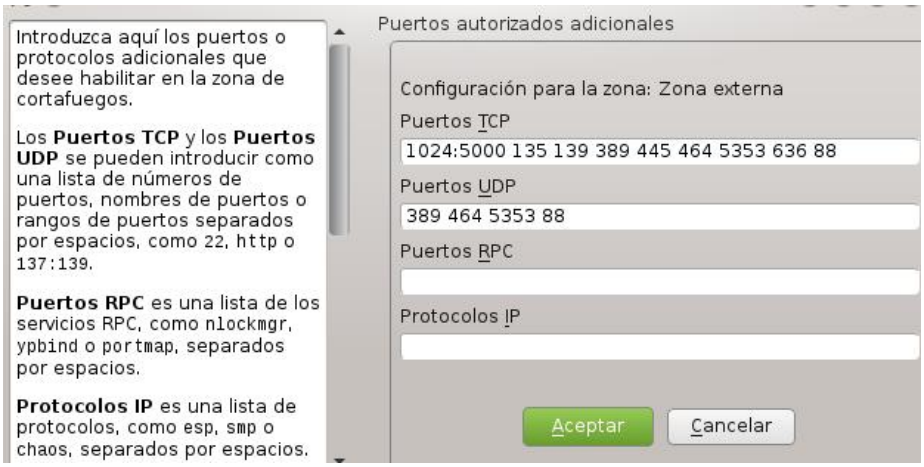
Y procedemos a abrir los siguientes puertos

Puertos TCP

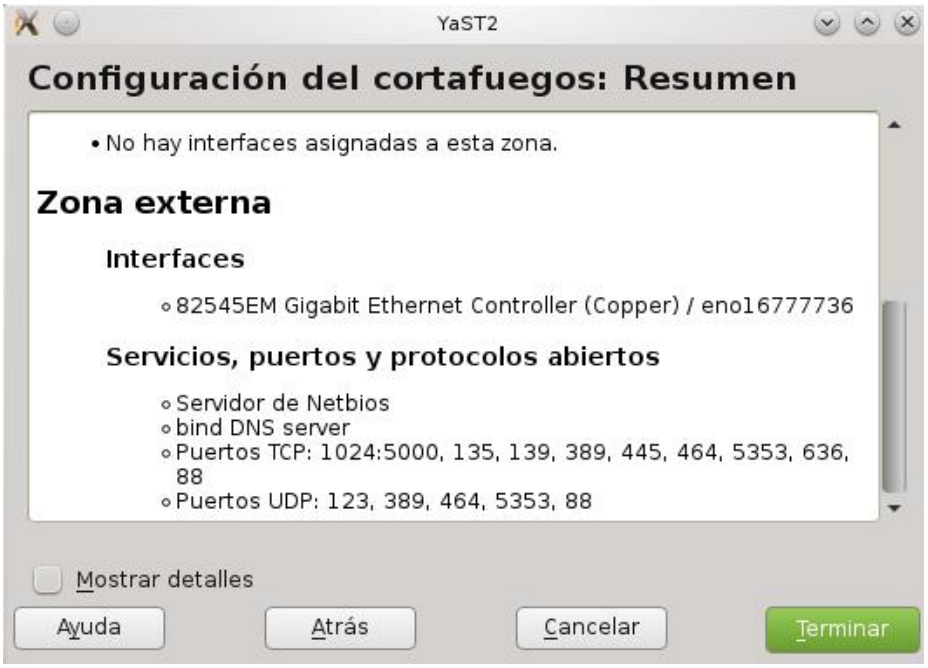
1024:5000 135 139 389 445 464 5353 636 88

Puertos UDP

123 389 464 5353 88



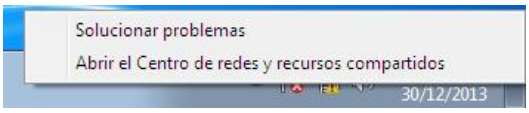
Hacemos clic en **Aceptar/Siguiente/terminar.**



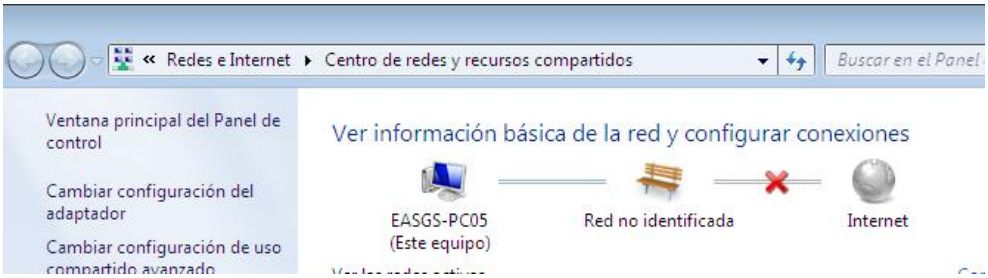
Uniendo estaciones de trabajo al dominio

Unir las estaciones de trabajo al nuevo dominio.

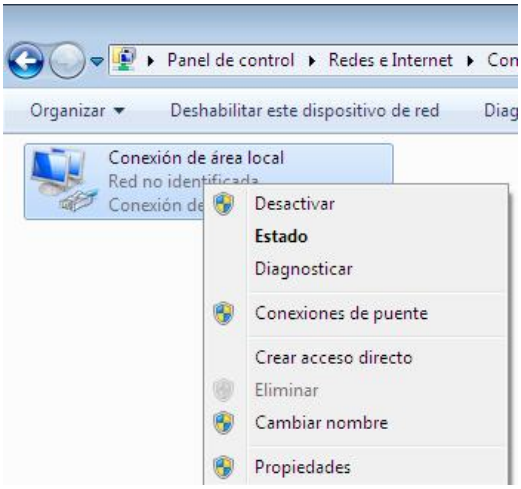
Para unir una maquina al dominio lo primero que hay que hacer es configurar una ip que este dentro de la red en la estacion de trabajo, para ello damos clic derecho sobre el icono de la red y seleccionamos **Abrir el centro de redes y recursos compartidos**.



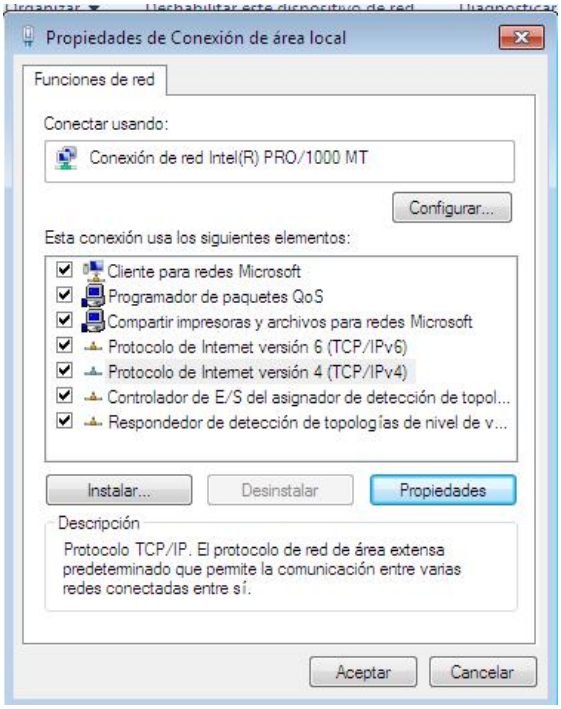
Luego damos clic en **Cambiar configuracion del adaptador**.



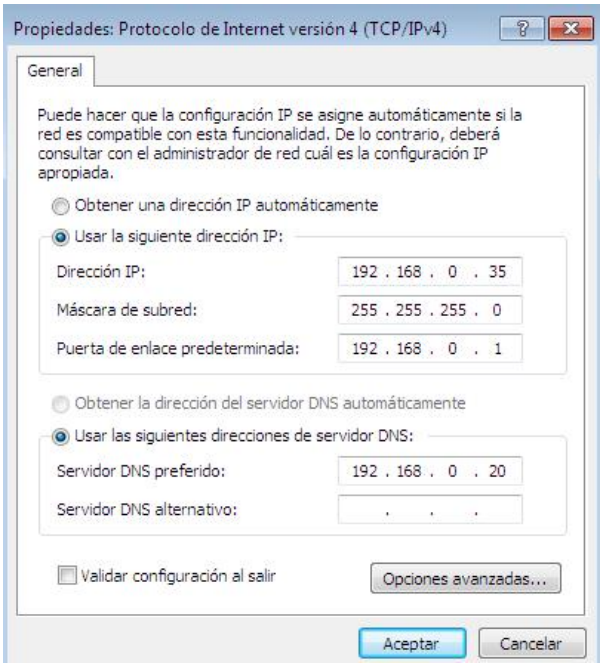
Seleccionamos el adaptador que vamos a usar y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades**



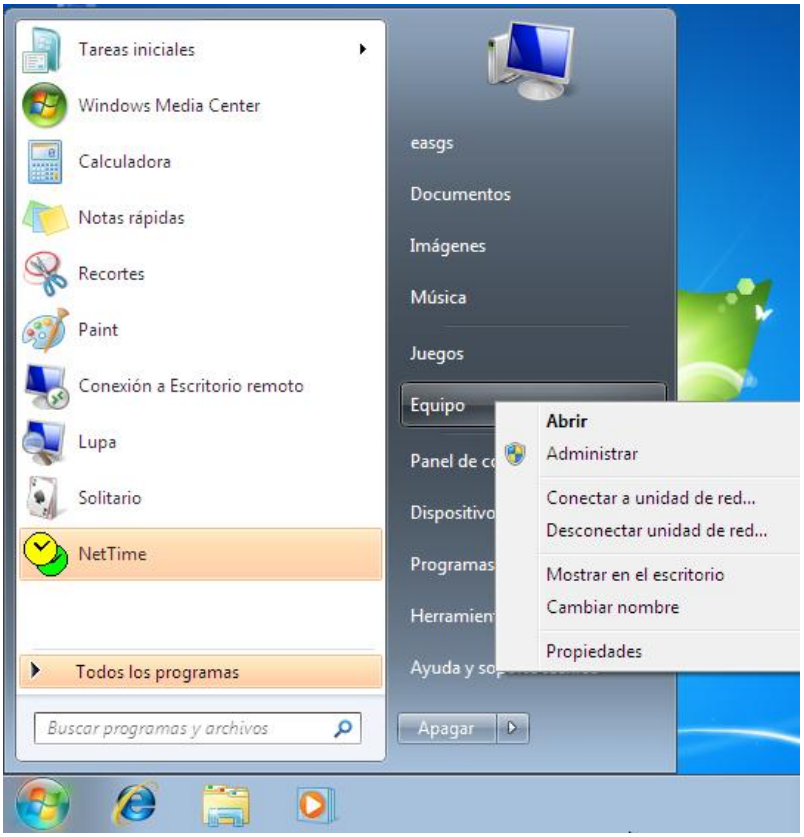
En este cuadro seleccionamos **Protocolo de internet version 4** y le damos clic en **propiedades**.



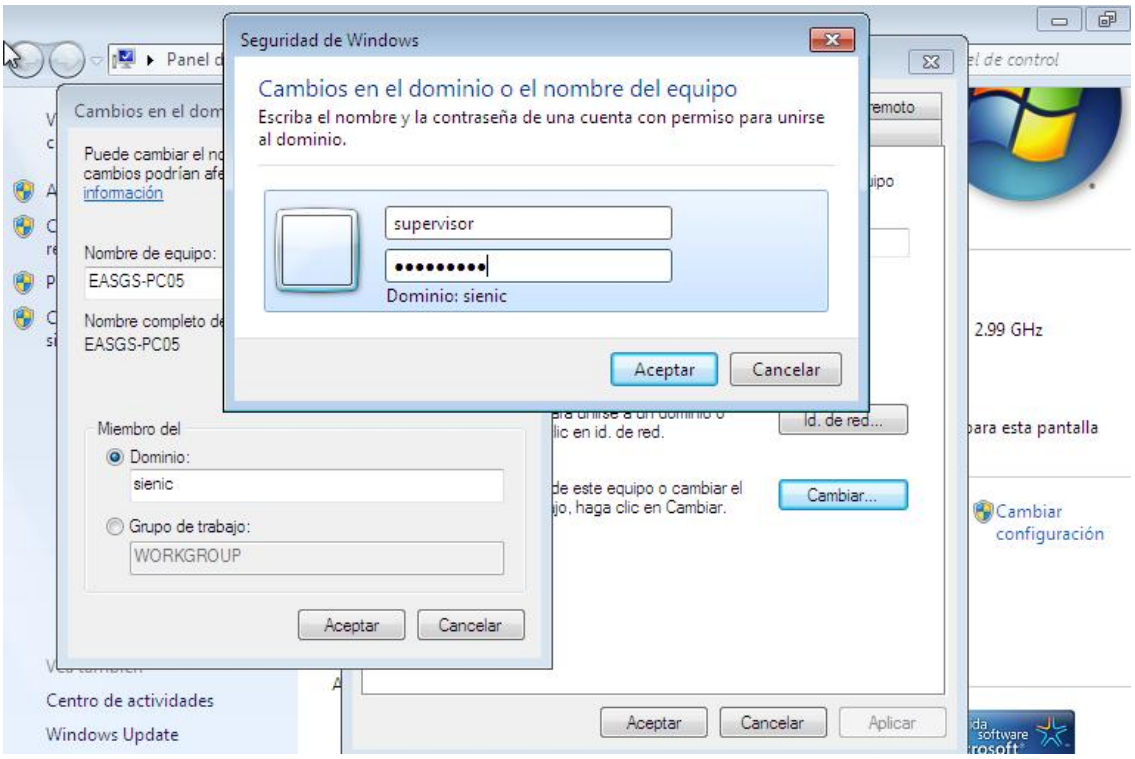
Luego llenamos los datos con los numero ip que correspondan a la red, en Direccion IP ponemos una direccion IP que este libre en la red, en mascara de subred ponemos la que corresponda a la red, en puerta de enlace ponemos la direccion del router y en DNS nos aseguramos de poner la direccion IP del servidor samba y le damos **aceptar**.



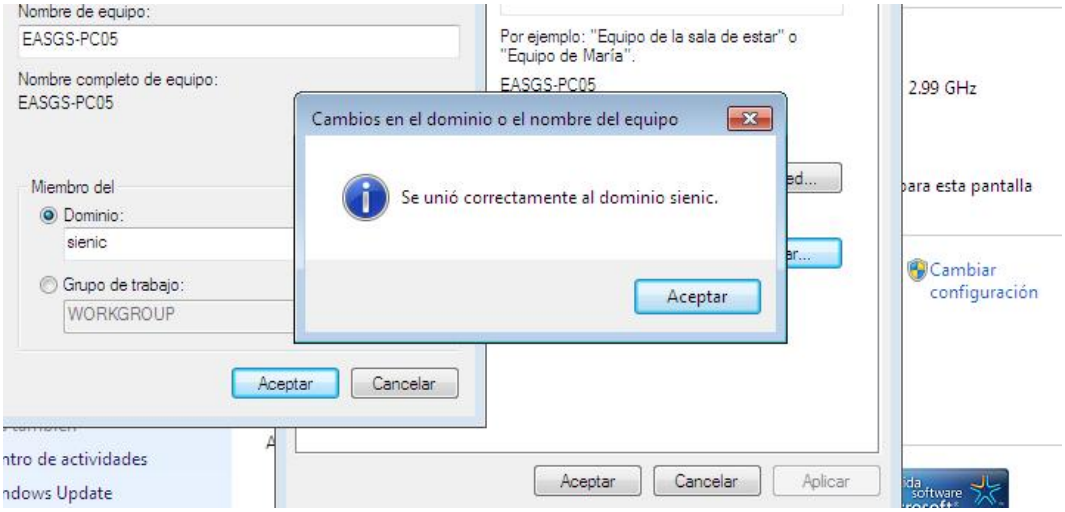
El siguiente paso es unir la maquina al dominio para esto no vamos a **Inicio** y le damos clic con el boton secundario del mouse a **Equipo** y luego seleccionamos **propiedades**.



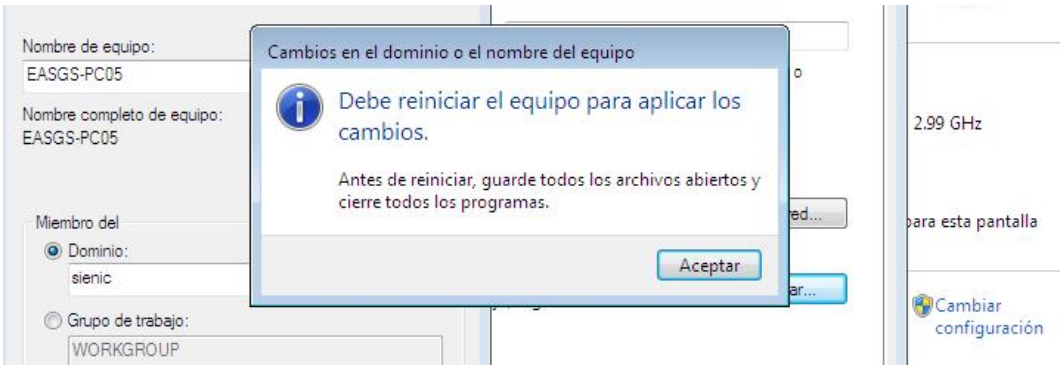
En la siguiente pantalla damos clic en **Cambiar configuracion**, despues en el siguiente cuadro de dialogo seleccionamos **Cambiar**… y en el siguiente cuadro en el campo **Dominio** ponemos el nombre del dominio y damos clic en **aceptar**, nos va a pedir las credenciales de una cuenta administrativa con permisos para agregar maquinas al domino, introducimos los datos y damos clic en **aceptar**



Nos mostrara un cuadro informativo que la maquina se a unido al dominio exitosamente



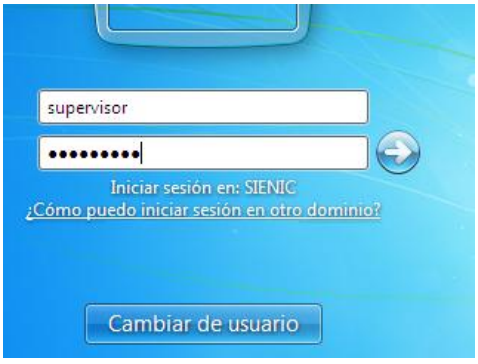
El siguiente cuadro nos dice que tenemos que reiniciar la maquina para que los cambios surtan efecto.



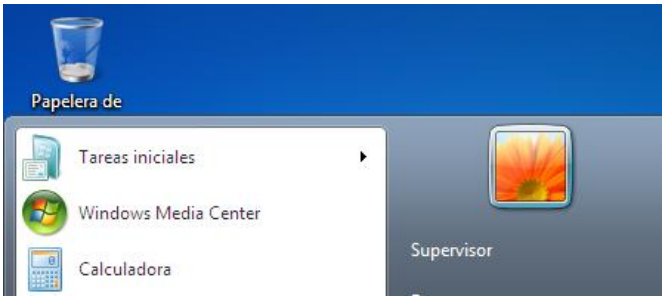
Cuando reinicie la maquina le damos clic en **cambiar de usuario**

Damos clic en **otro usuario**.

Introduciomos los datos del usuario de dominio y damos **enter**.



Con esto ya hemos iniciado sesion dentro del dominio



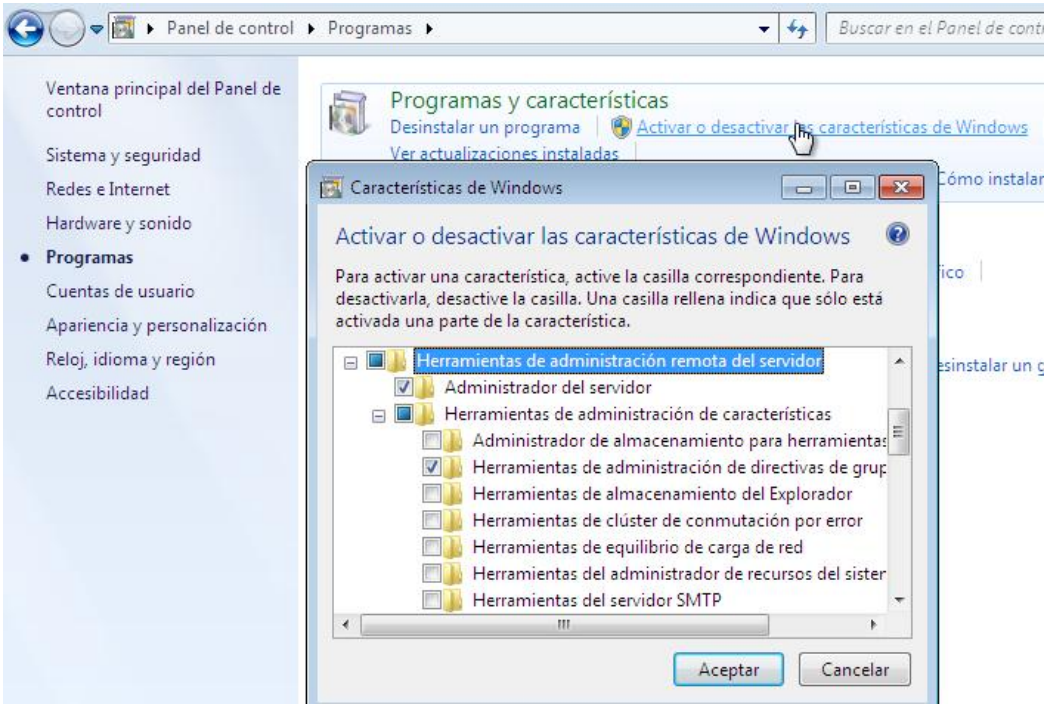
Usando las RSAT (Remote Server Administration Tools)

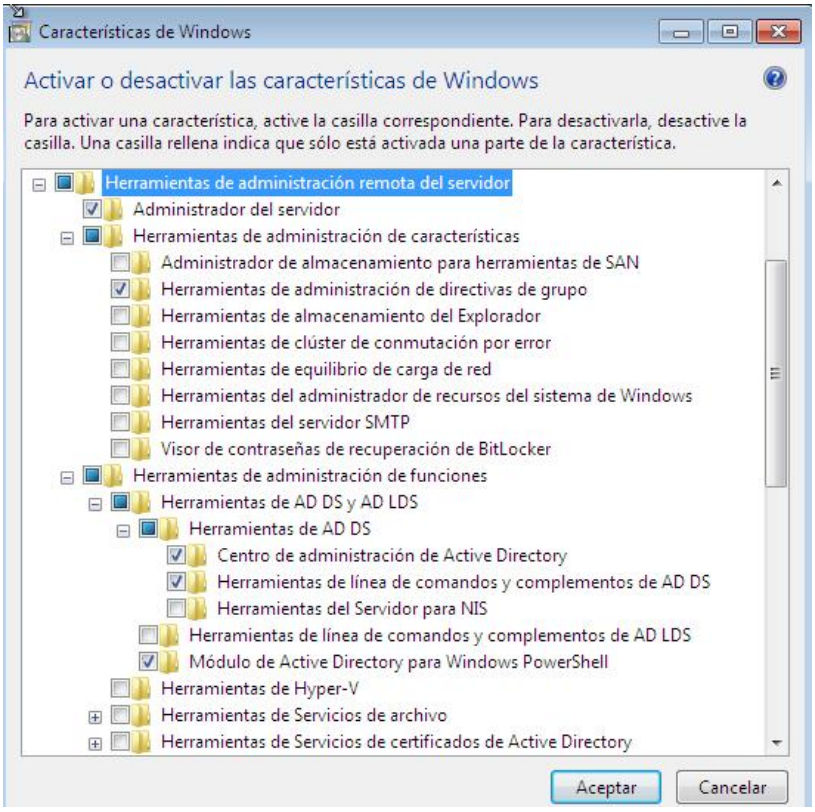
Herramientas de administración remota del servidor para Windows

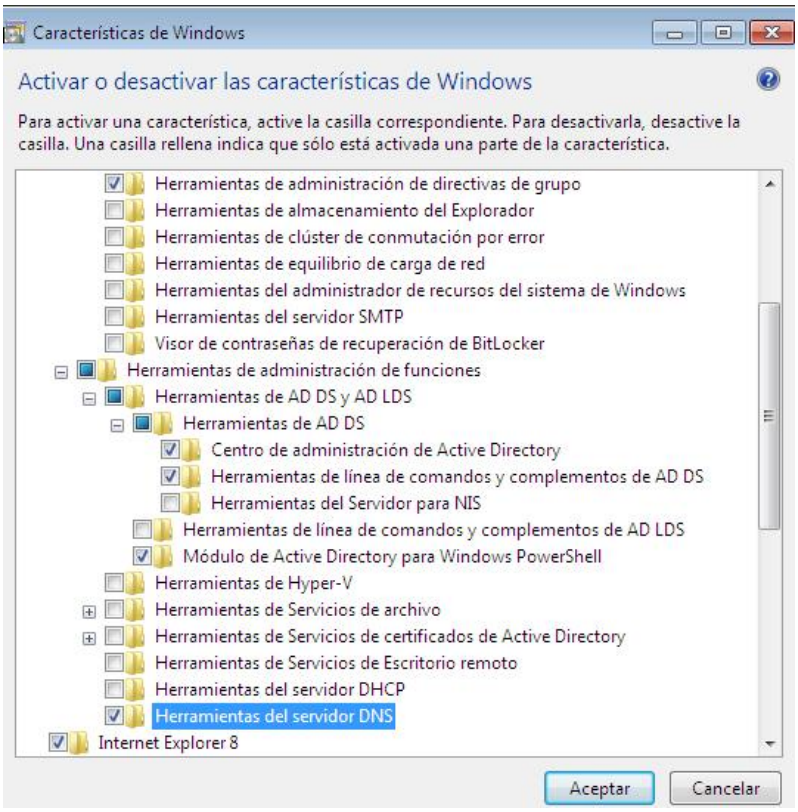
La administracion de Usuarios y Grupos, Unidades organizativas, Directivas de grupo, DNS y recursos compartidos entre otros pueden hacerse desde una estacion de trabajo con Windows XP/Vista/7/8/8.1 instalado, para esto se deben descargar e instalar las Herramientas de administración remota del servidor para Windows, estas se pueden descargar de los siguientes enlaces:

- http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en (Vista)
- http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en (Windows 7)
- http://www.microsoft.com/download/details.aspx?id=28972 (Windows 8)
- http://www.microsoft.com/en-us/download/details.aspx?id=39296 (Windows 8.1)

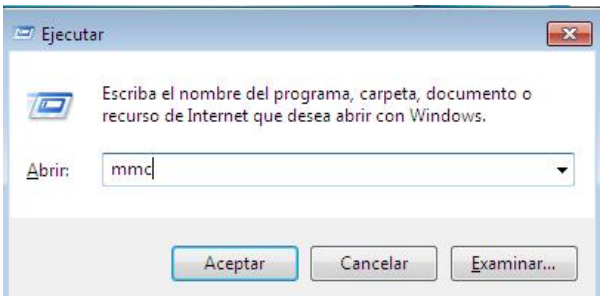
La instalacion es como cualquier otro paquete de windows, una vez instaladas las herramientas hay que habilitarlas, para eso nos vamos **a panel de control/Programas/Activar o desactivar las caracteristicas de Windows** y seleccionamos las opciones a como se muestra en las siguientes imágenes.


Panel de control ▸ Programas ▸
Buscar en el Panel de cont
Ventana principal del Panel de control
Sistema y seguridad
Redes e Internet
Hardware y sonido
Programas
Cuentas de usuario
Apariencia y personalización
Reloj, idioma y región
Accesibilidad
Programas y características
Desinstalar un programa
Activar o desactivar las características de Windows
Ver actualizaciones instaladas
Características de Windows
Activar o desactivar las características de Windows
Para activar una característica, active la casilla correspondiente. Para desactivarla, desactive la casilla. Una casilla rellena indica que sólo está activada una parte de la característica.
Herramientas de administración remota del servidor
Administrador del servidor
Herramientas de administración de características
Administrador de almacenamiento para herramientas
Herramientas de administración de directivas de grup
Herramientas de almacenamiento del Explorador
Herramientas de clúster de conmutación por error
Herramientas de equilibrio de carga de red
Herramientas del administrador de recursos del sister
Herramientas del servidor SMTP
Aceptar
Cancelar

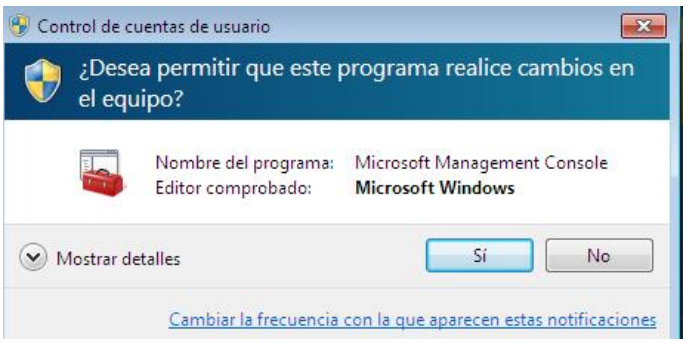

Características de Windows
Activar o desactivar las características de Windows
Para activar una característica, active la casilla correspondiente. Para desactivarla, desactive la casilla. Una casilla rellena indica que sólo está activada una parte de la característica.
Herramientas de administración remota del servidor
Administrador del servidor
Herramientas de administración de características
Administrador de almacenamiento para herramientas de SAN
Herramientas de administración de directivas de grupo
Herramientas de almacenamiento del Explorador
Herramientas de clúster de conmutación por error
Herramientas de equilibrio de carga de red
Herramientas del administrador de recursos del sistema de Windows
Herramientas del servidor SMTP
Visor de contraseñas de recuperación de BitLocker
Herramientas de administración de funciones
Herramientas de AD DS y AD LDS
Herramientas de AD DS
Centro de administración de Active Directory
Herramientas de línea de comandos y complementos de AD DS
Herramientas del Servidor para NIS
Herramientas de línea de comandos y complementos de AD LDS
Módulo de Active Directory para Windows PowerShell
Herramientas de Hyper-V
Herramientas de Servicios de archivo
Herramientas de Servicios de certificados de Active Directory
Aceptar
Cancelar



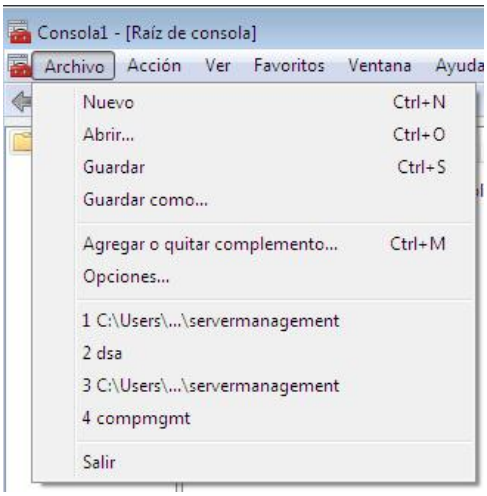
Una vez habilitadas las funciones presionamos la tecla **Windows + R** y escribimos **mmc**



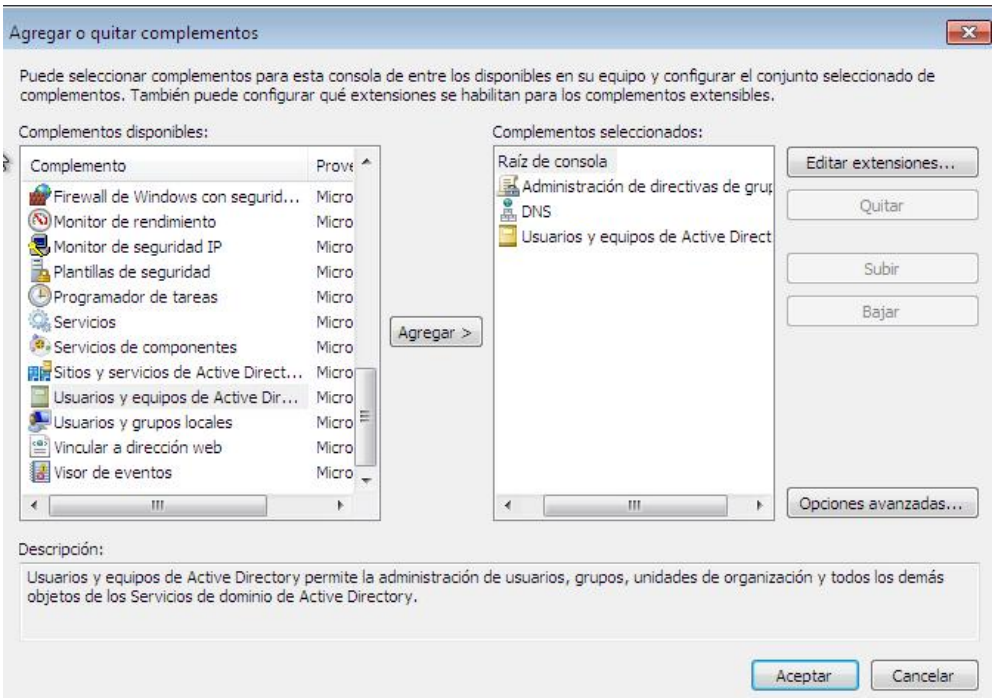
En el siguiente cuadro de dialogo le damos clic en "**Si**"

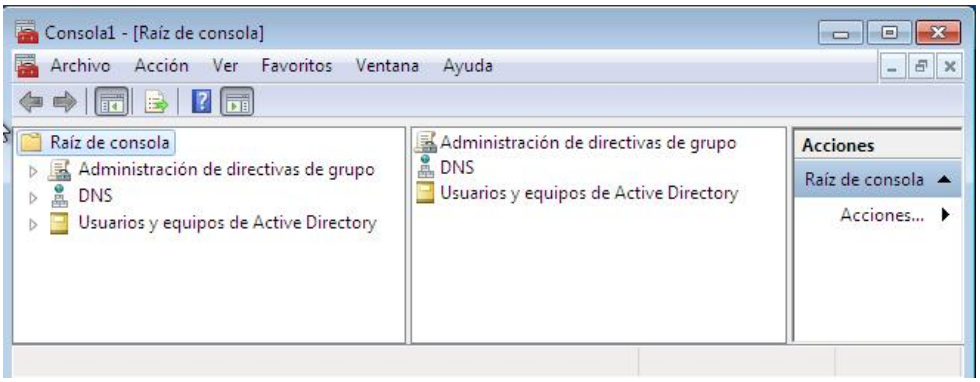


En la Raiz de consola damos clic en **Archivo/agregar o quitar complemento**.

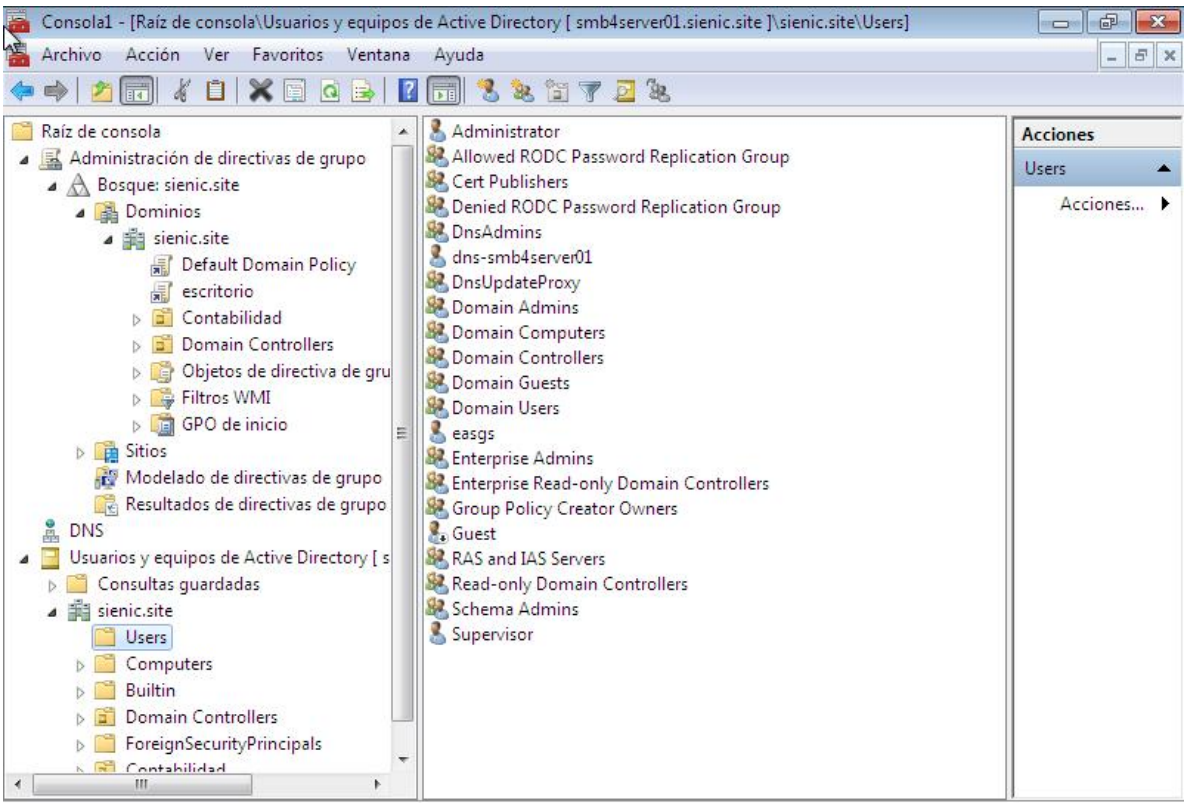


Seleccionar **Administracion de directivas de grupo, DNS y Usuarios y equipos de Active Directory** y le damos clic en **aceptar**.

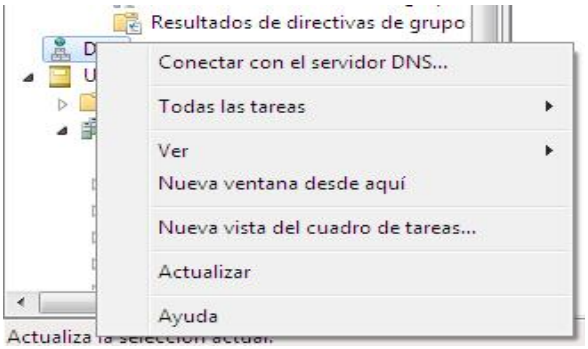




Desde esta consola podremos administrar todas las funciones mencionadas anteriormente.

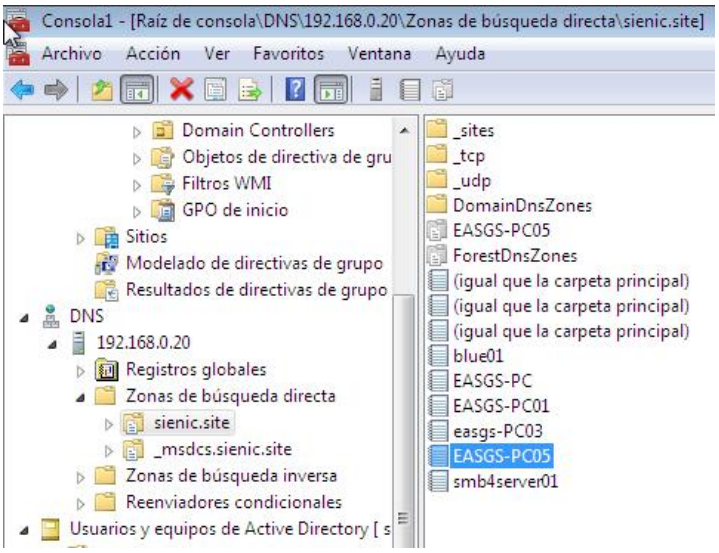


Para administrar el DNS del servidor damos clic derecho sobre la opcion **DNS** y seleccionamos **Conectar con el servidor DNS**.

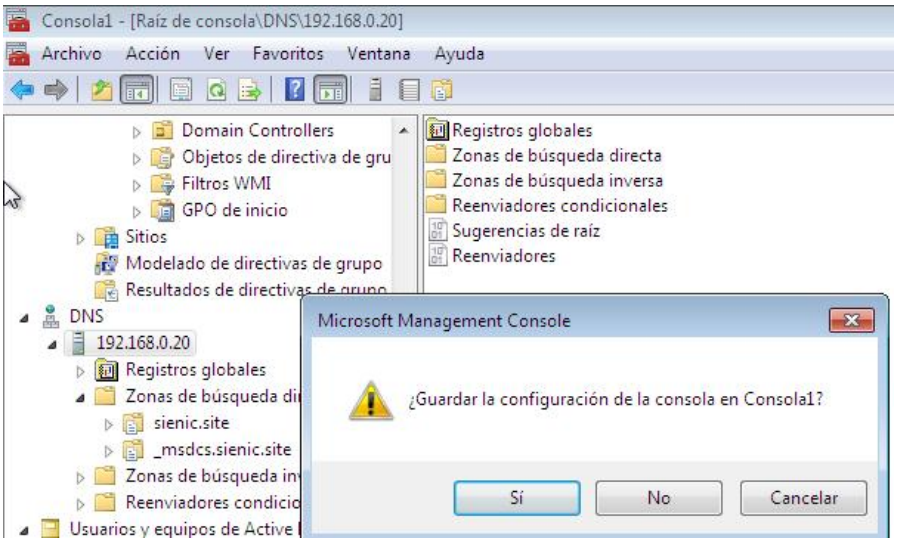


En el siguiente cuadro de dialogo seleccionamos la opcion "**El Siguiente equipo**" y escribimos la direccion IP del servidor samba y damos clic en **aceptar**.

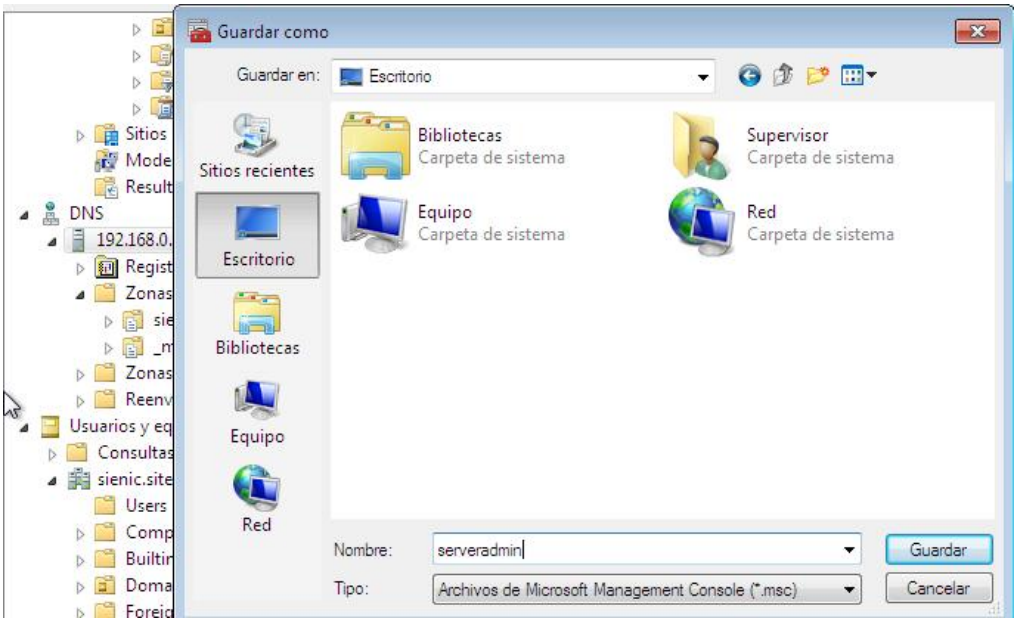
Una vez realizada la conexión podremos administrar el servidor DNS desde la RSAT



Cuando cerremos la consola no preguntara si deseamos guardar, le damos clic en **si**.



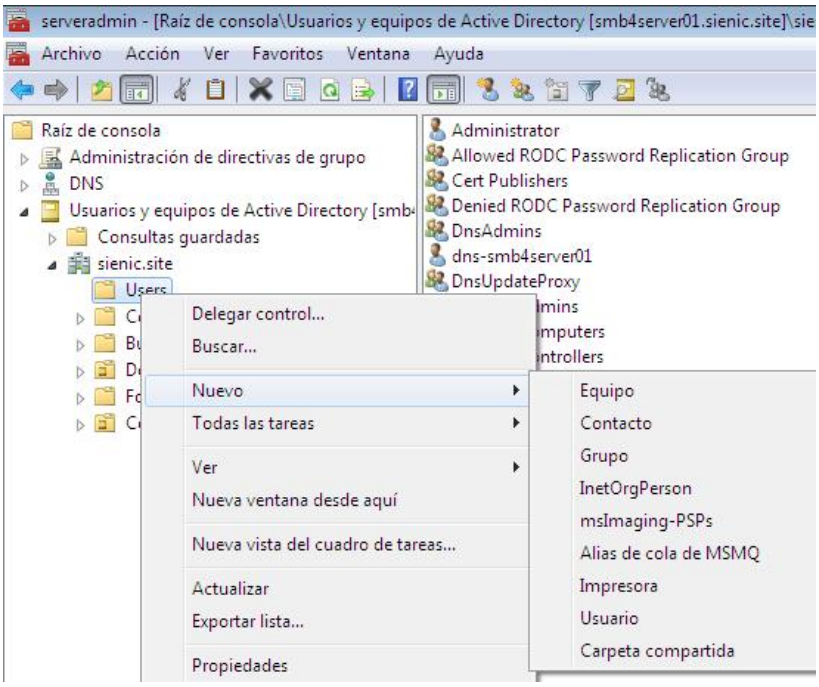
Le ponemos un nombre descriptivo y la guardamos en el escritorio.



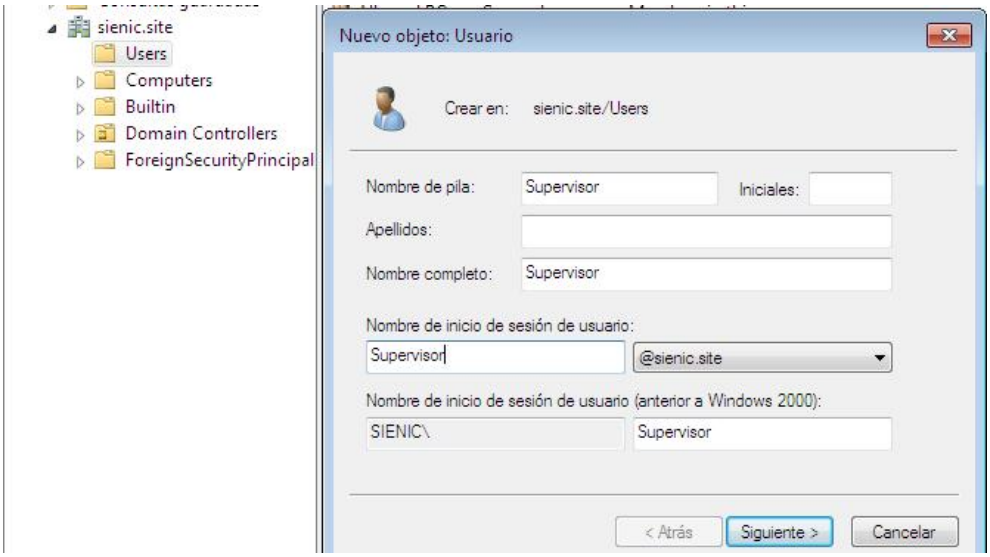
Ahora con solo dar clic en el icono podremos acceder a las opciones de administracion del servidor previamente configuradas.

Creando cuenta administradora de dominio alterna.

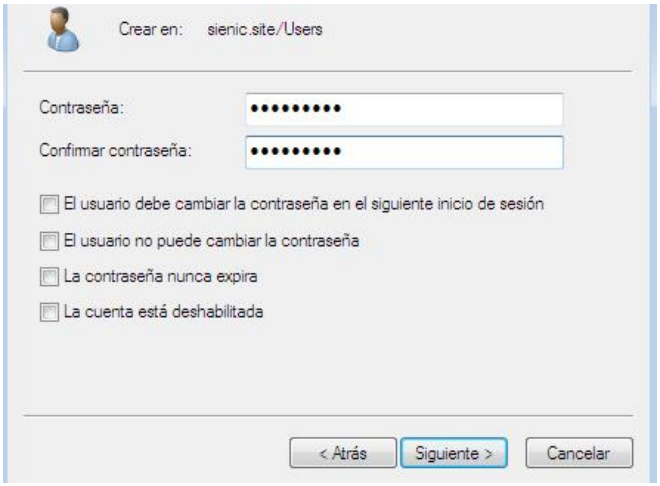
Para crear un usuario administrador alterno nos vamos a **Usuarios y equipos de Active Directory/sienic.site** damos clic derecho en **Users** seleccionamos **Nuevo/Usuario**.



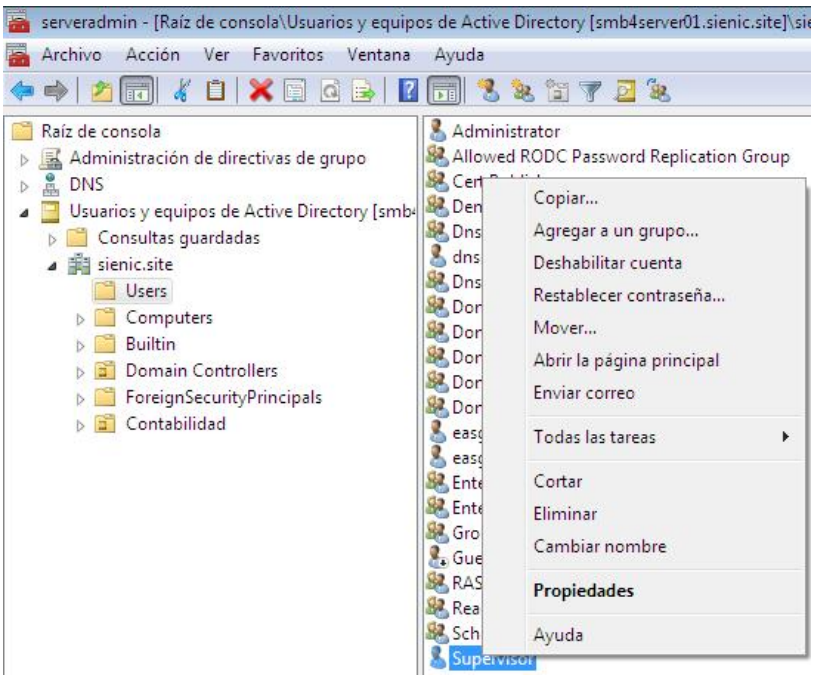
Llenamos los datos Nombre de pila, Nombre completo y nombre de inicio de sesion de usuario y clic en **siguiente**.



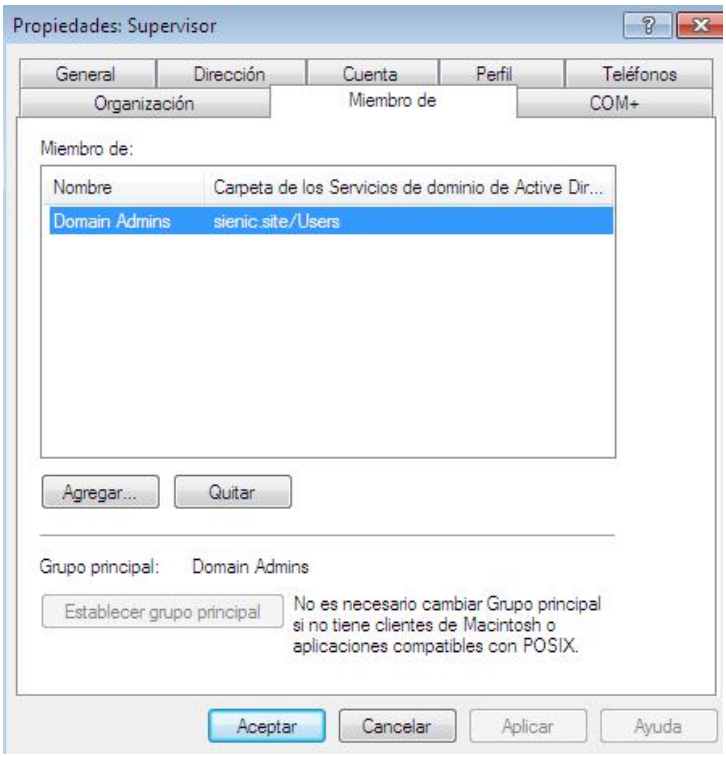
Ponemos la clave y dejamos las demas opciones a como se muestra en la siguiente imagen y clic en **siguiente**.



Una vez creado el usuario lo seleccionamos y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades**



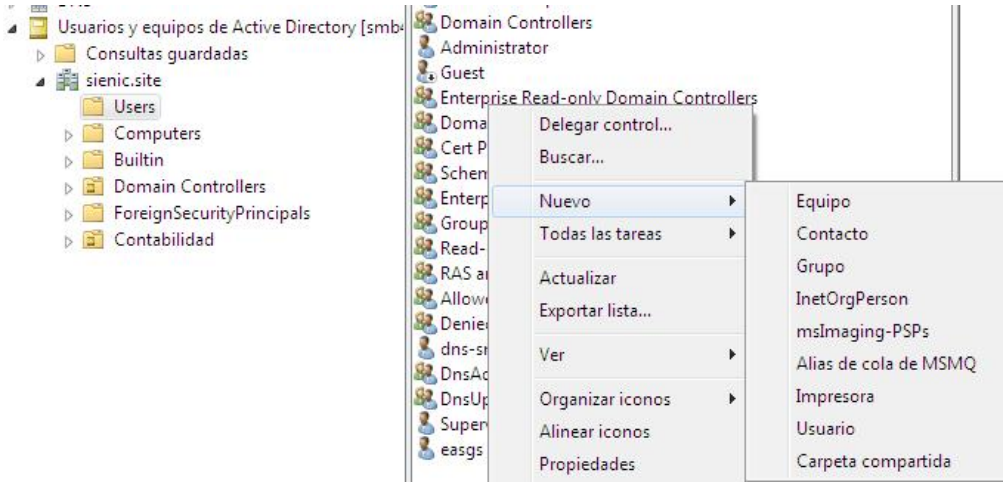
Seleccionamos la solapa **Miembro de** y lo hacemos miembro del grupo “Domain Admins” unicamente y le damos clic en **aceptar**.



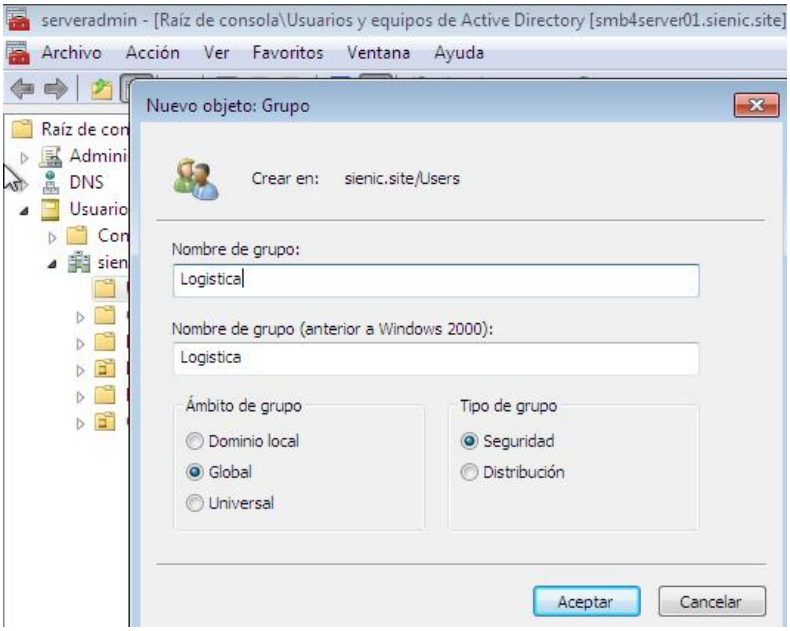
El proceso es similar para cualquier tipo de usuario excepto la parte donde lo hacemos miembro de un grupo ya que los grupos deben corresponder a los privilegios de cada usuario.

Creando Grupos de Seguridad.

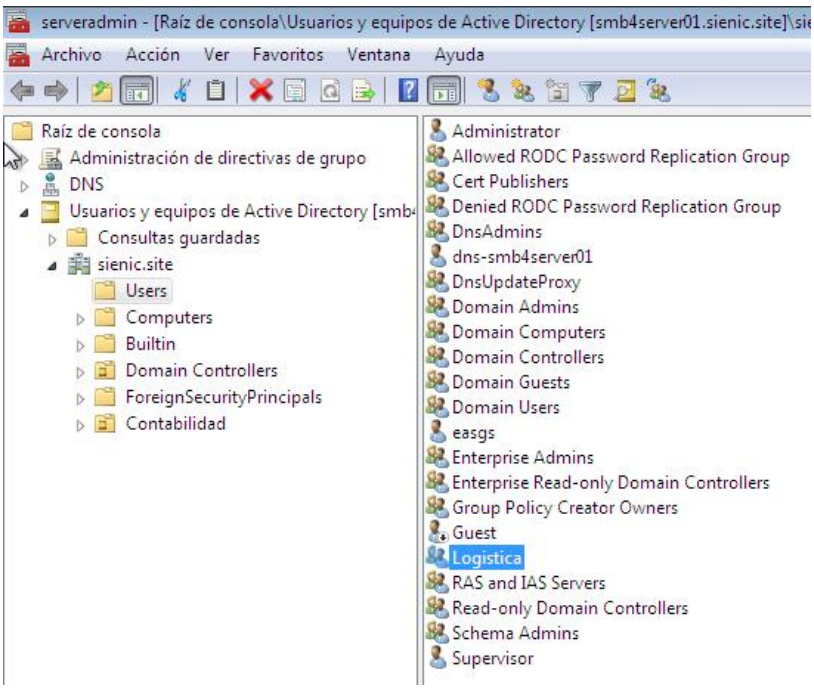
Para crear un grupo nos vamos a **Usuarios y equipos de Active directory/Users** damos clic con el boton secundario seleccionamos **Nuevo/Grupo**.



Ponemos nombre al grupo y en ambito seleccionamos **Global** en tipo de grupo seleccionamos **Seguridad**.

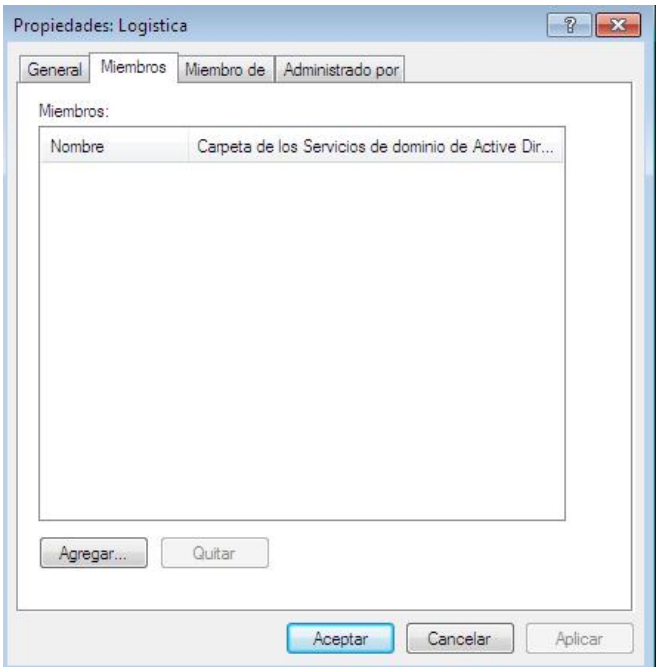


Damos clic en **aceptar** y con esto ya tenemos creado el grupo de seguridad.

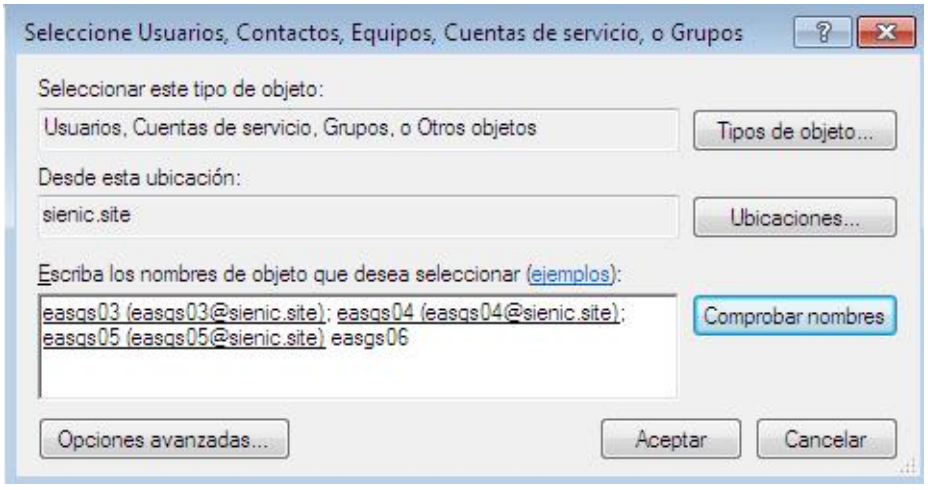


Agregando usuarios a un grupo de seguridad.

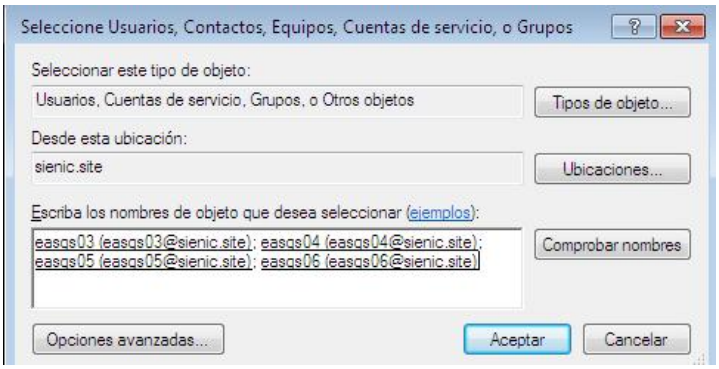
Para agregar usuarios a un grupo de seguridad damos clic con el boton secundario del mouse sobre el grupo de seguridad y damos clic en **propiedades**, en el cuadro de propiedades seleccionamos la solapa **Miembros** y damos clic en **agregar**.



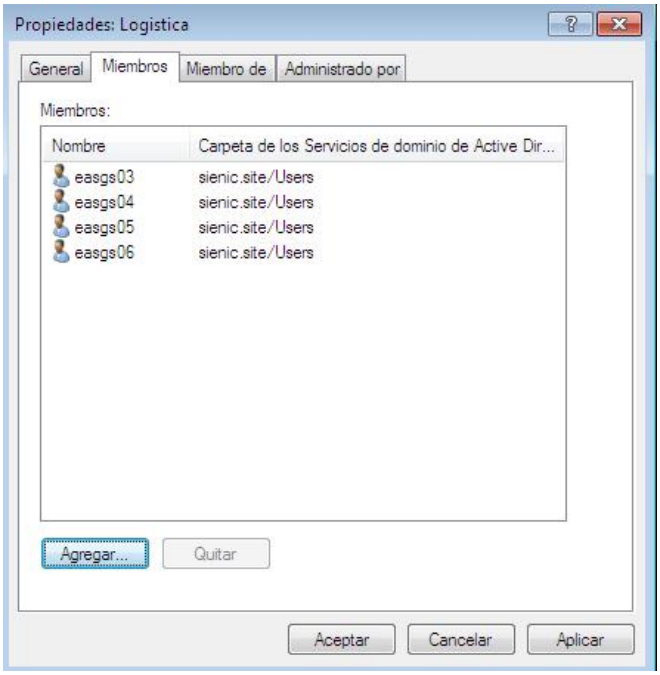
En el siguiente cuadro vamos escribiendo los nombre de usuarios que van a pertenecer al grupo y vamos dando clic en **comprobar nombre.**



Cuando ya tengamos a todos los usuarios requeridos damos clic en **aceptar**.

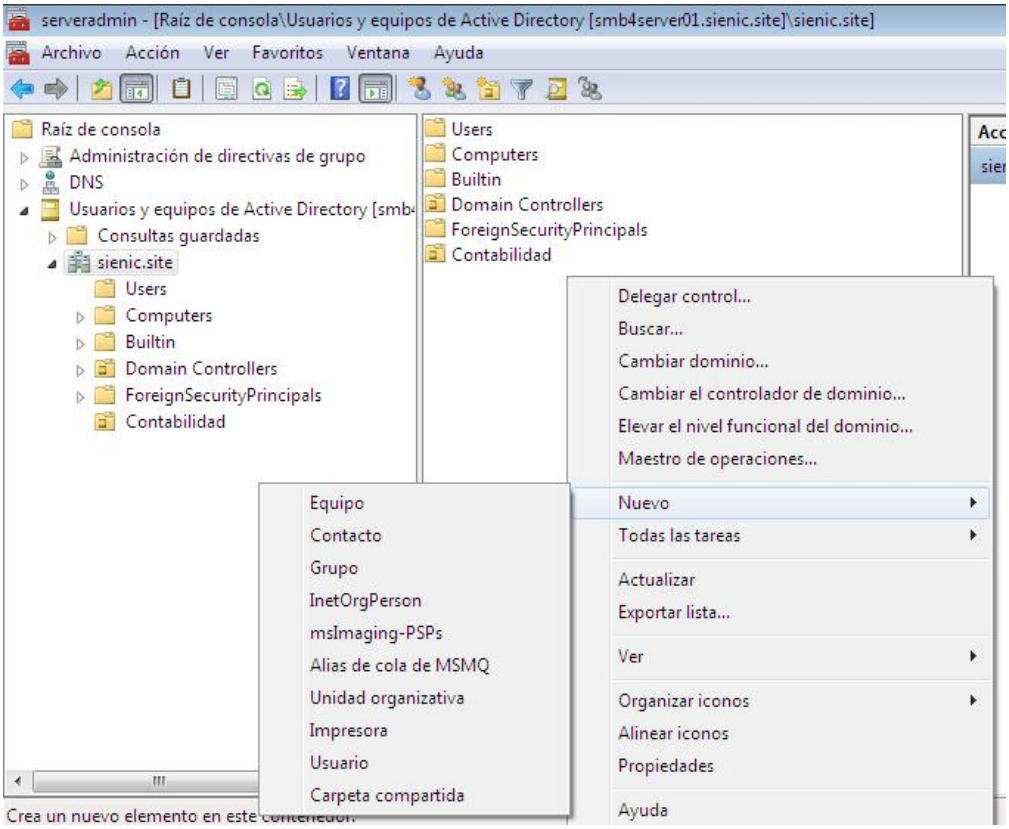


En el siguiente cuadro damos clic en **aceptar**.

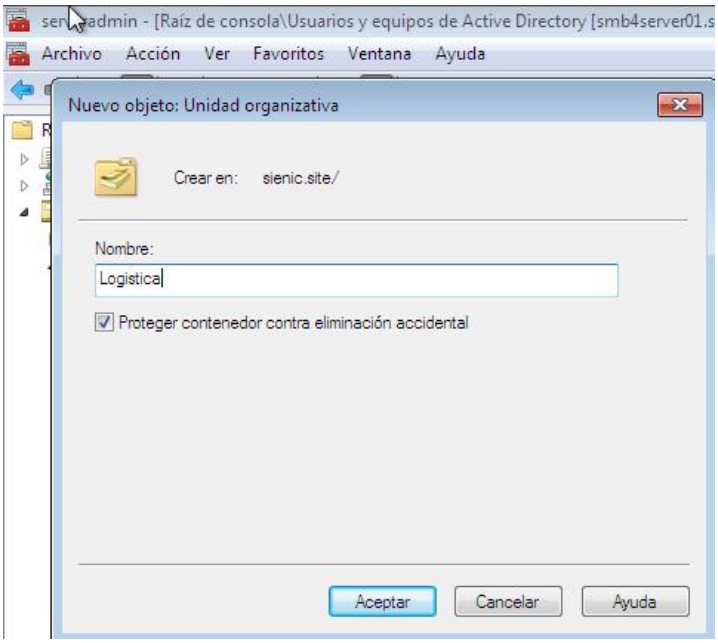


Creando unidades organizativas.

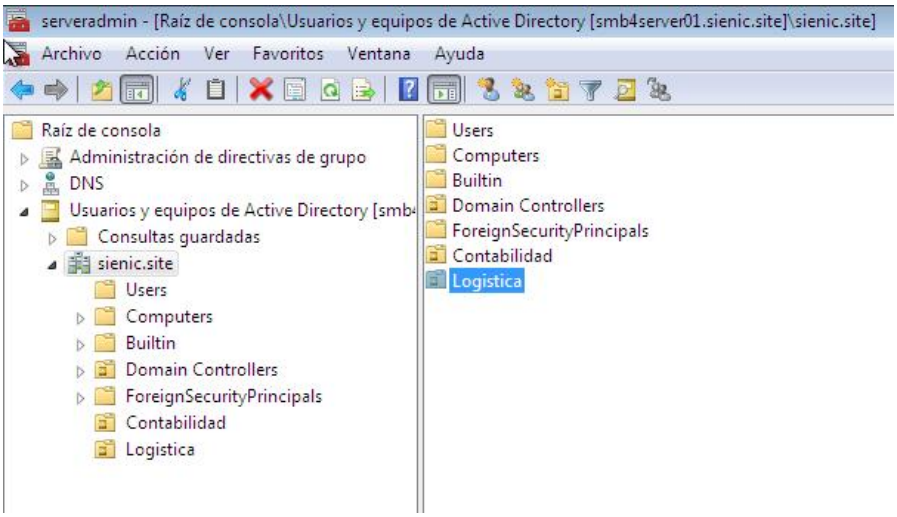
Para crear una unidad organizativa, nos vamos a **Usuarios y equipos de Active Directory** y damos clic con el boton secundario del mouse sobre el dominio, seleccionamos **Nuevo/Unidad Organizativa.**



Ponemos un nombre descriptivo a la Unidad organizativa y damos clic en **aceptar**.

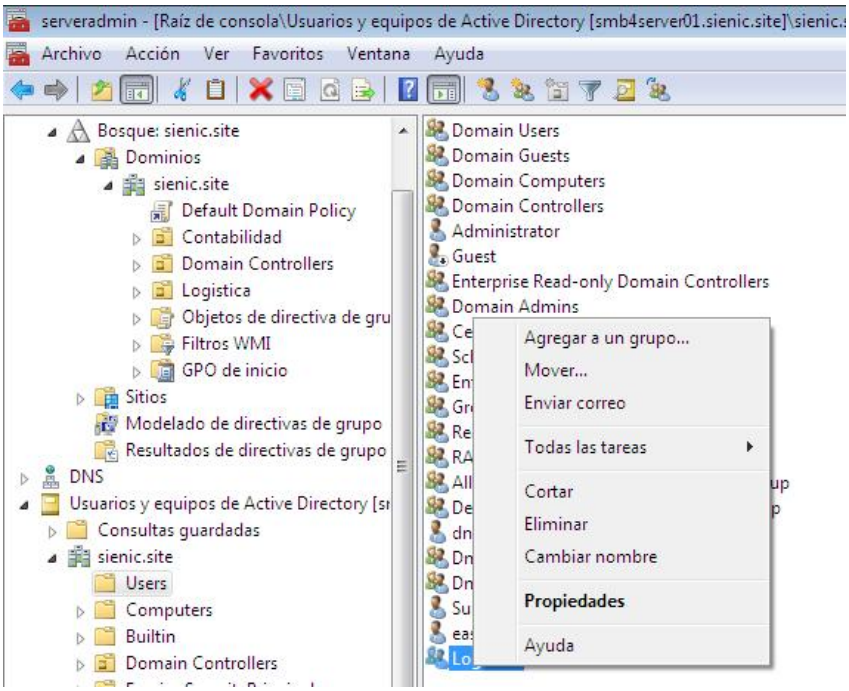


Ahora la nueva unidad organizativa se mostrara dentro del dominio.

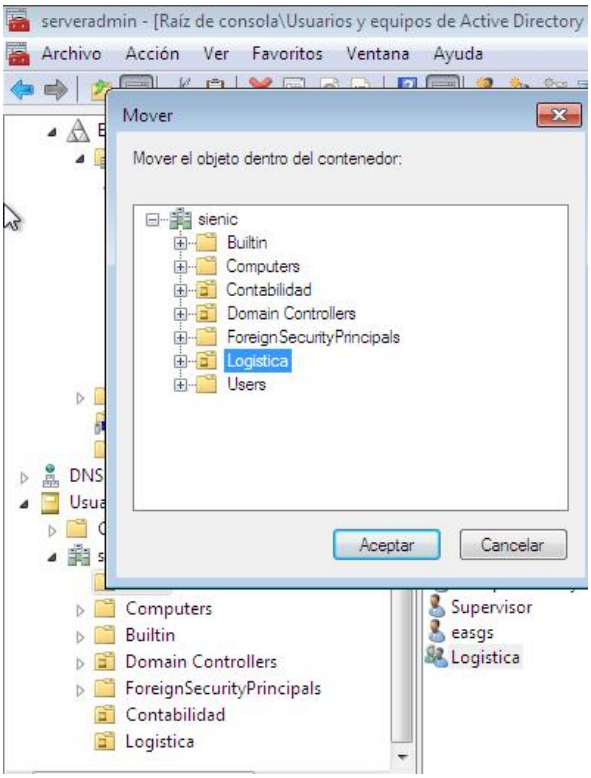


Mover un Grupo a una Unidad Organizativa.

Damos clic con el boton secundario del mouse sobre el grupo que queremos agregar a la unidad organizativa y seleccionamos **Mover**.



En el siguiente cuadro seleccionamos la Unidad Organizativa a la que queremos mover el grupo y clic en **aceptar**.

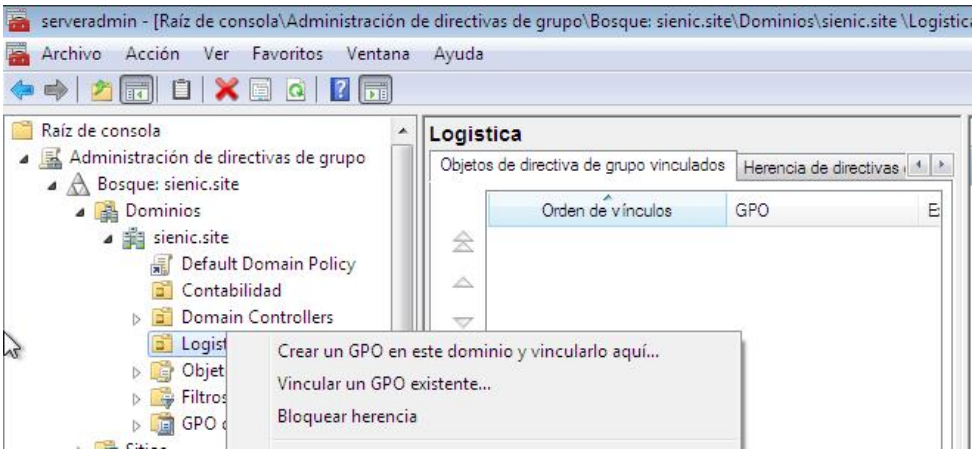


Con esto el grupo aparecera en el active directory dentro de la unidad organizativa seleccionada

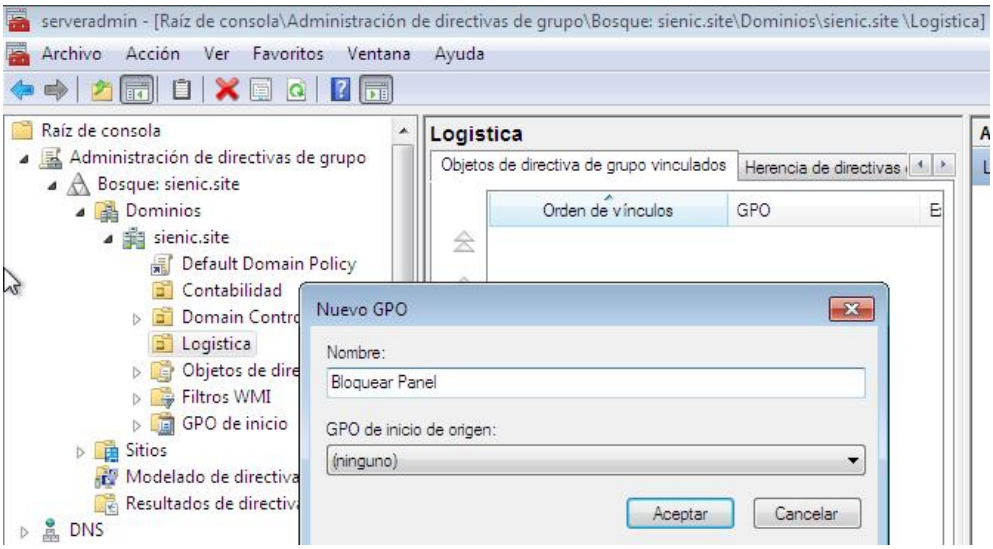
El procedimiento es el mismo para un usuario tambien podemos arrastar los objetos.

Creando GPO para restringir el uso del panel de control

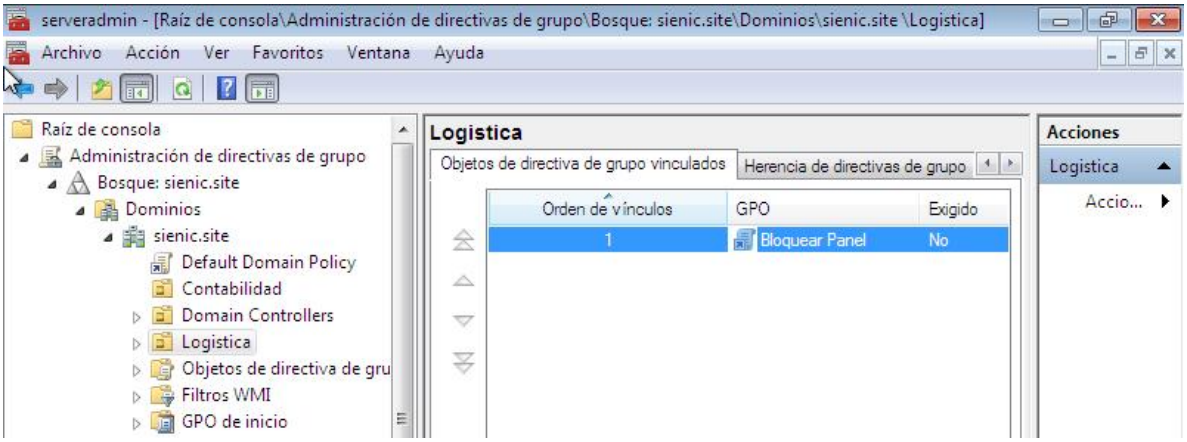
Para crear una GPO nos vamos a Administracion de directivas de grupo, nos vamos al dominio y hacemos clic con el boton secundario del mouse sobre la unidad organizativa a la que vamos a aplicar la politica de seguridad, en el menu seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



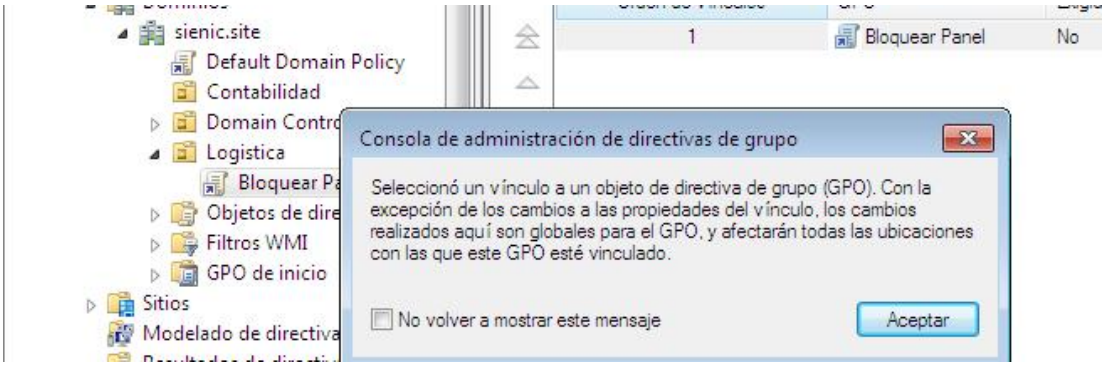
Ponemos un nombre descriptivo a la nueva politica de grupo y damos clic en **aceptar**.



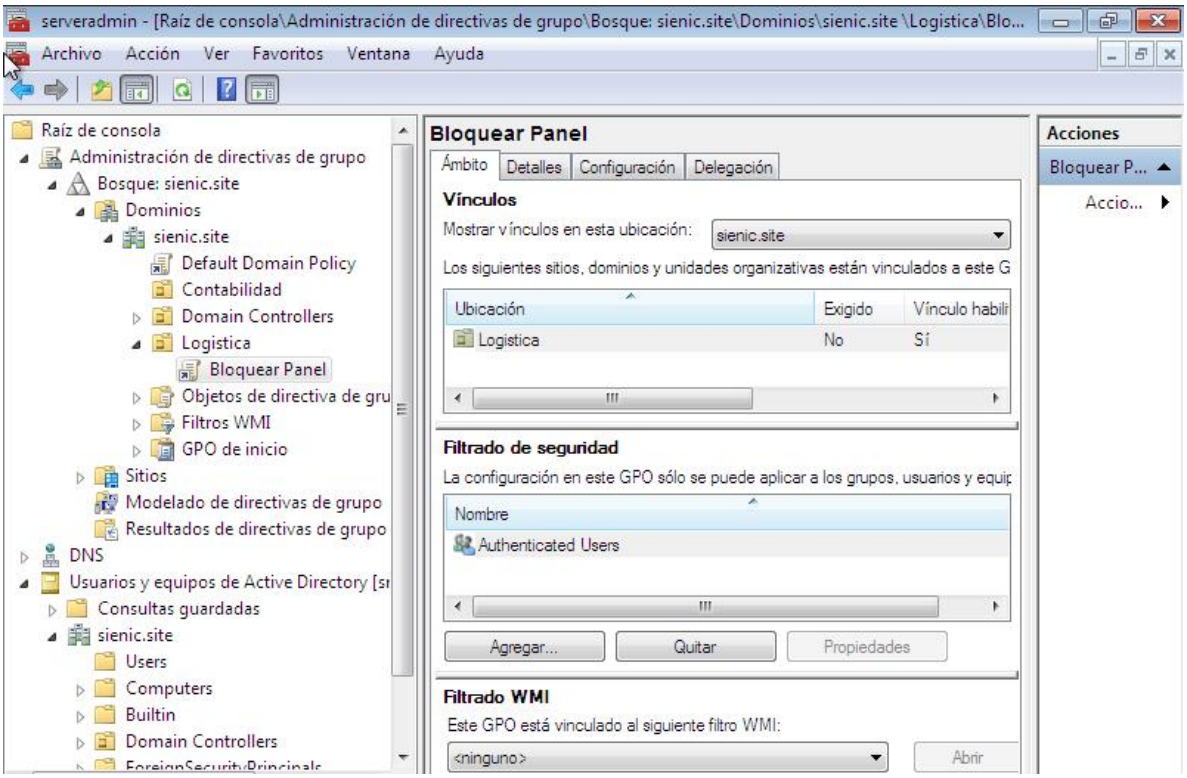
En el panel derecho damos doble clic sobre la nueva politica.



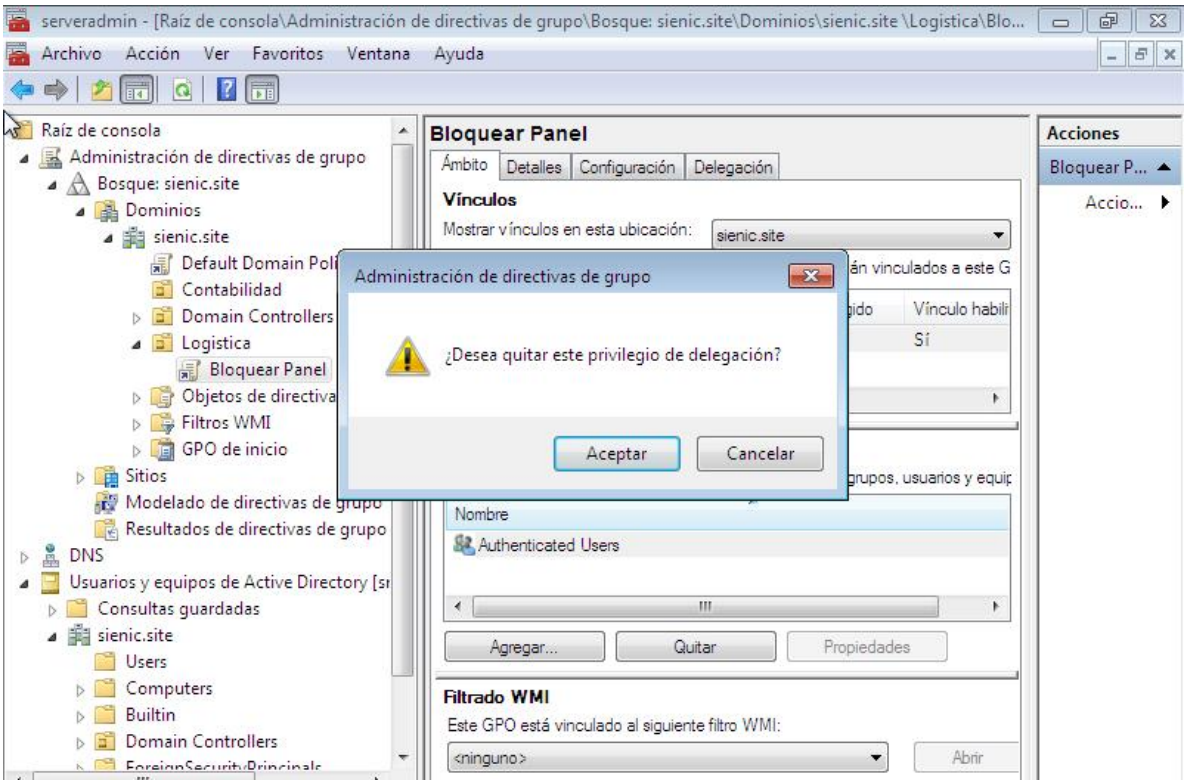
Nos va a aparecer un aviso como el de la siguiente imagen damos clic en **aceptar**.



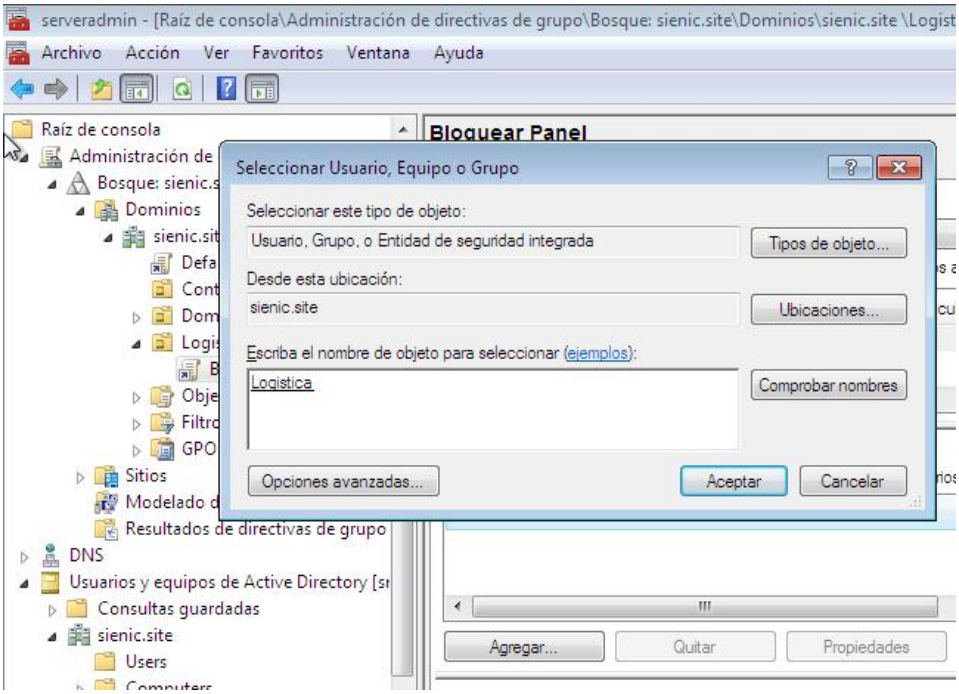
Aquí podemos ver que en **filtrado de seguridad** por default nos aparece el grupo Authenticated Users, pero digamos que queremos que esta GPO se aplique a otro grupo, entonces seleccionamos el grupo y damos clic en **quitar**.



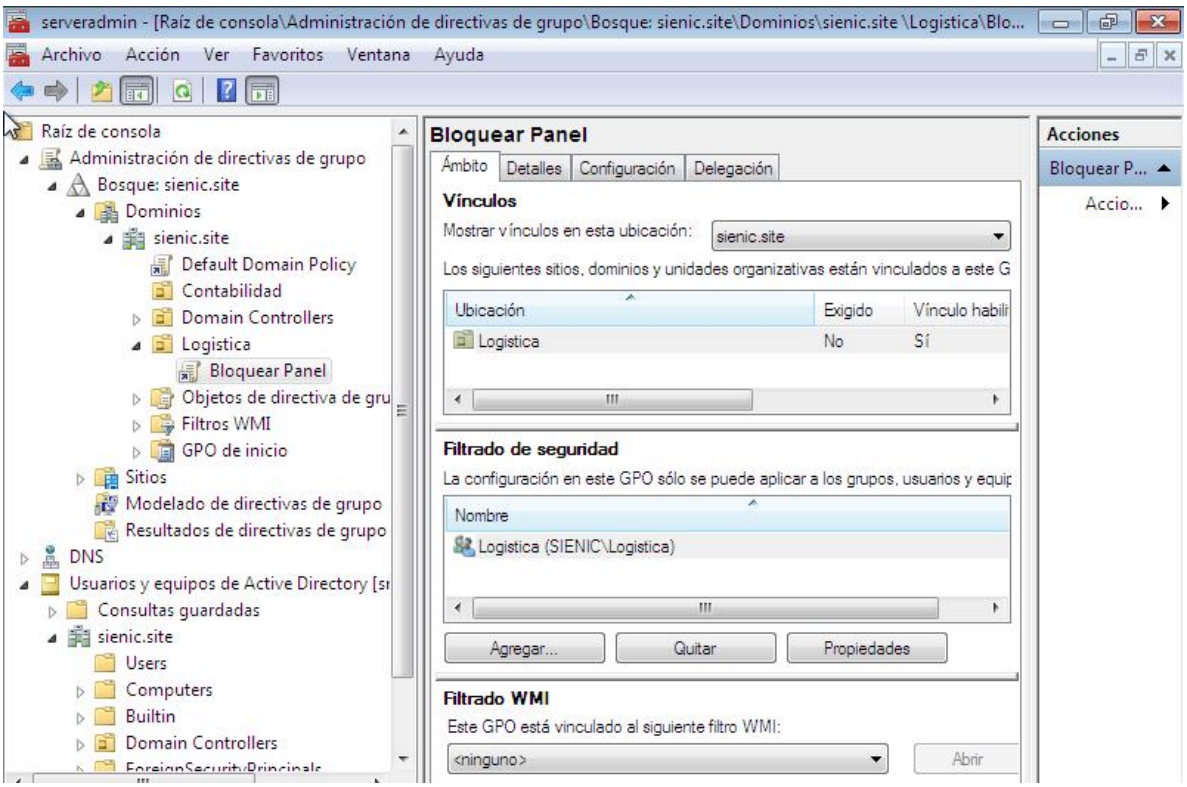
En el cuadro de dialogo de confirmacion damos clic en **aceptar**.



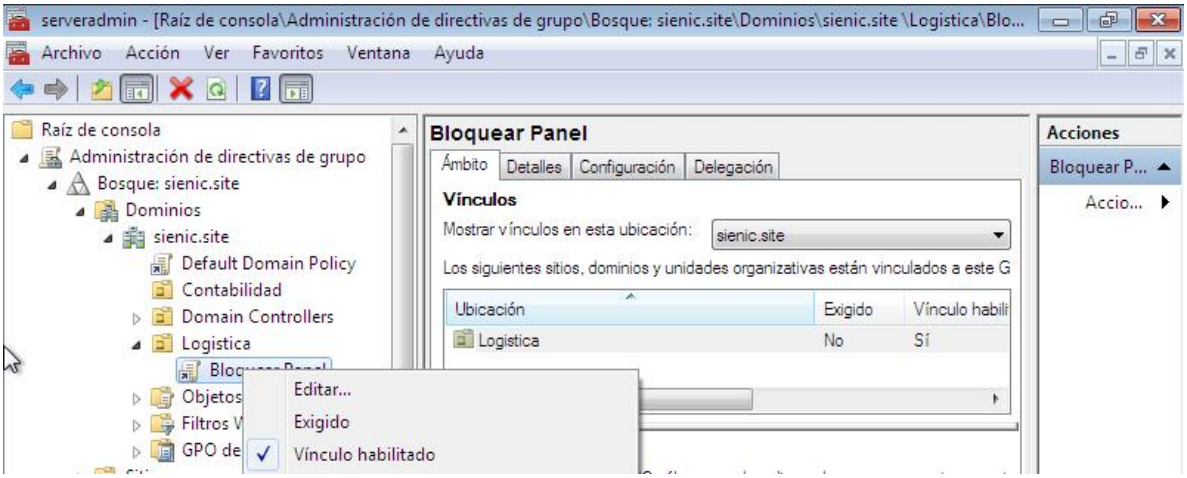
Ahora que hemos removido el grupo por default debemos agregar el grupo al que queremos aplicar la politica, damos clic en **agregar** y escribimos el nombre del grupo deseado luego damos clic en **comprobar nombre** y finalmente clic en **aceptar**.



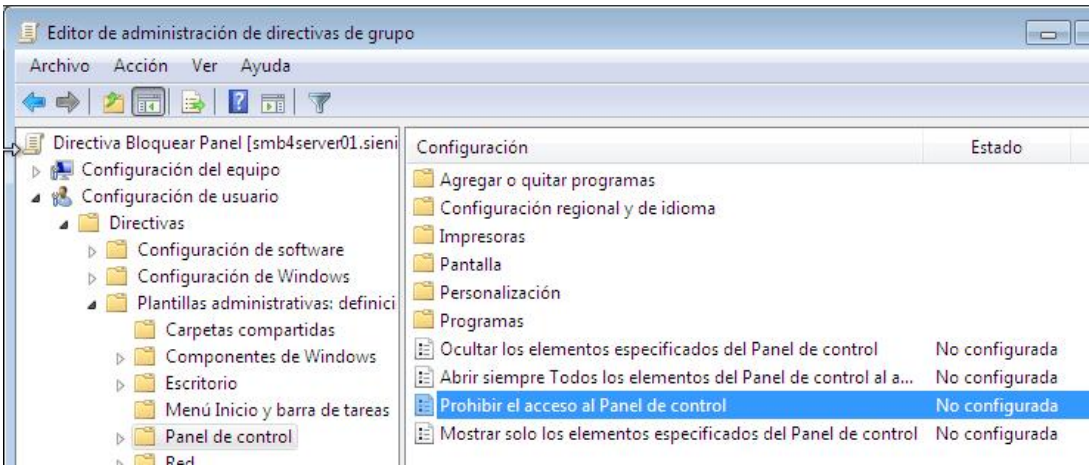
Ahora ya nos aparece reflejado el grupo deseado.



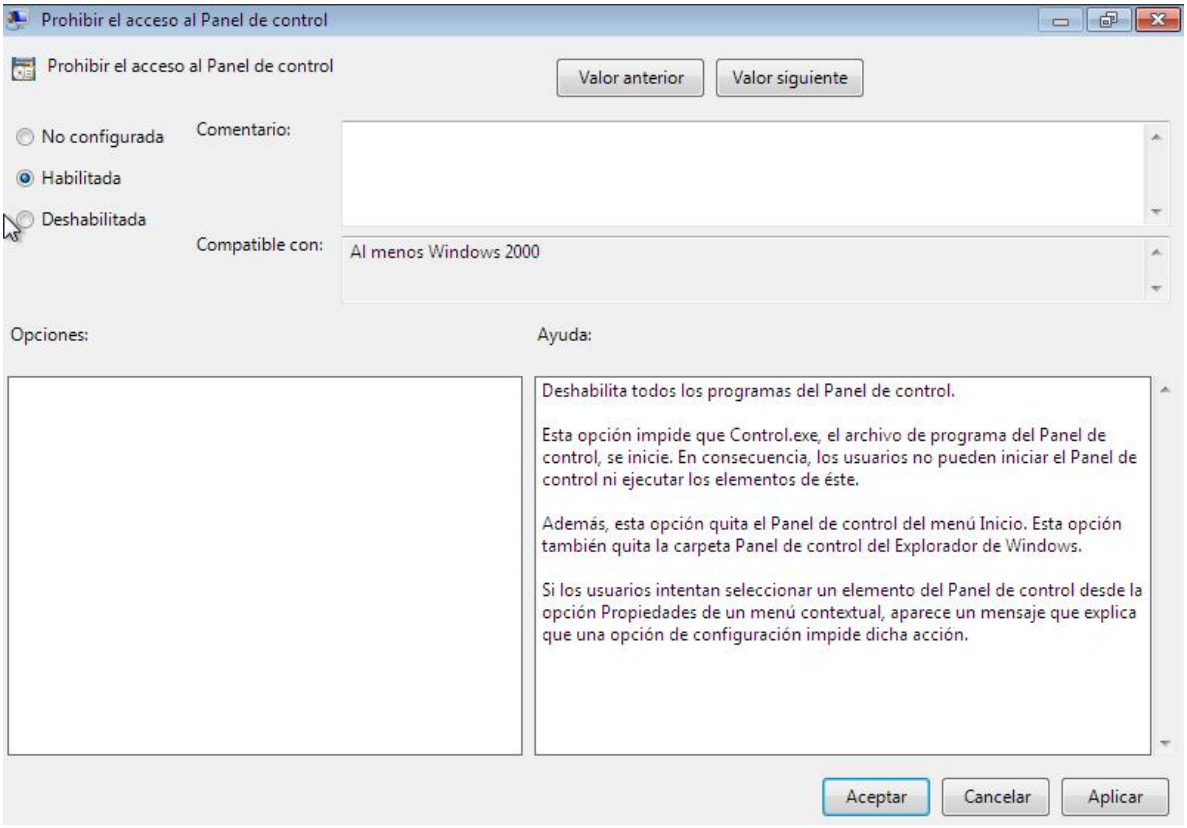
Ahora para configurar la nueva politica le damos clic con el boton secundario del mouse y seleccionamos **editar**.



En el editor de administracion de directivas de grupo nos vamos a **Configuracion de usuario/Directivas/Plantillas administrativas/Panel de control** y en el panel derecho le damos doble clic a la opcion **Prohibir el acceso al panel de control**.

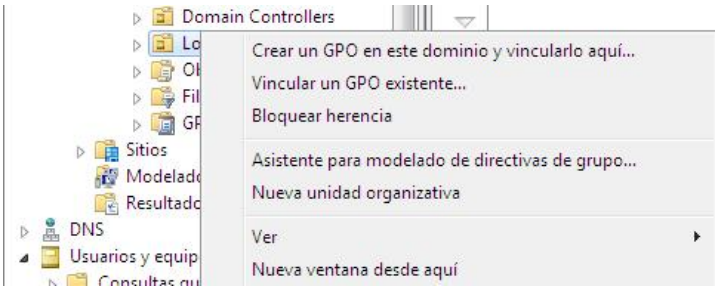


En la siguiente ventana seleccionamos **Habilitada** y damos clic en **aceptar**.

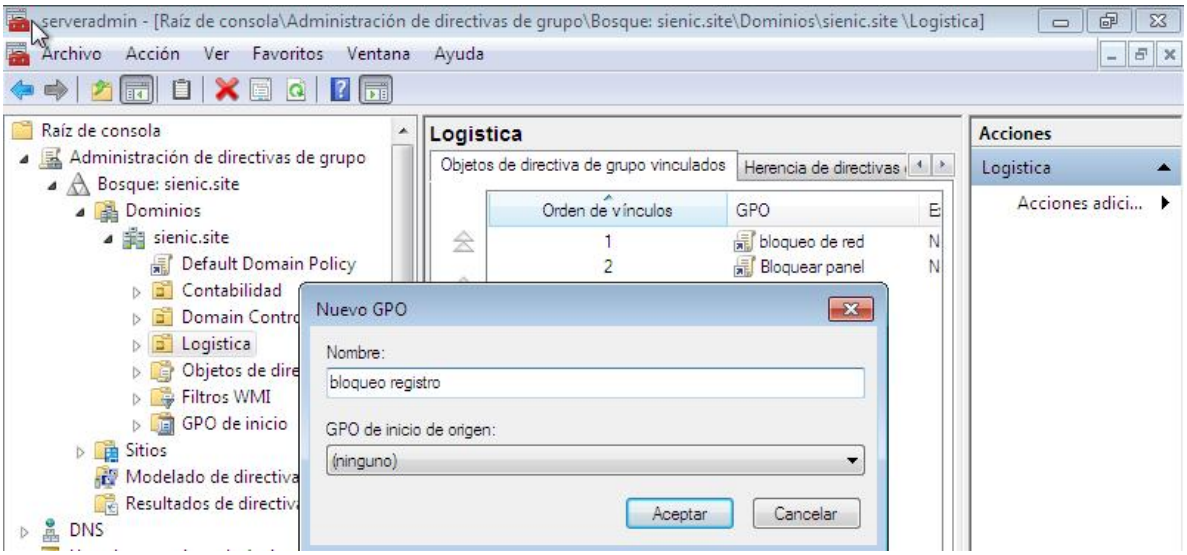


Crear una GPO para restringir el acceso al regedit.

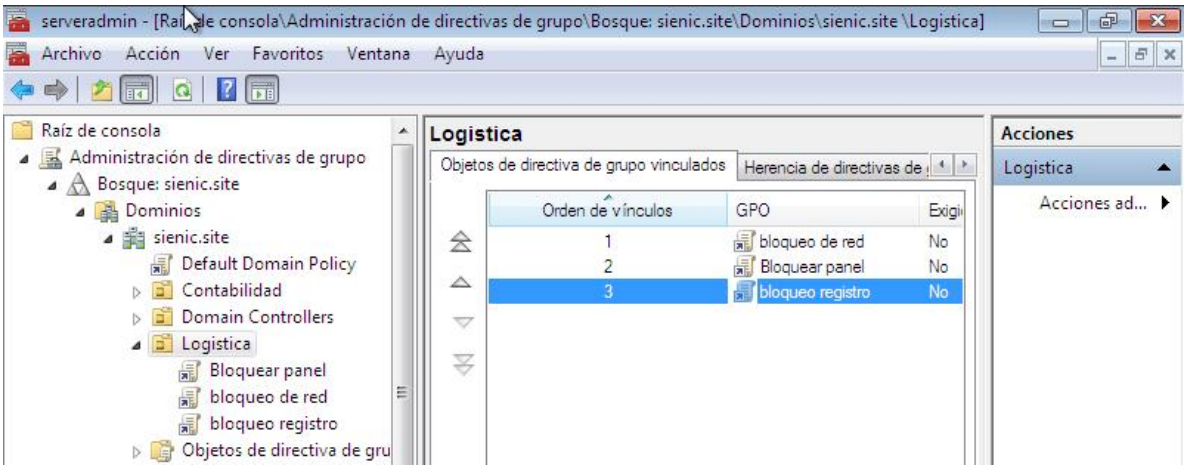
Para crear una GPO para restringir el acceso al registro de Windows seleccionamos la OU a la que deseamos aplicar la politica y le damos clic con el boton secundario del mouse, luego seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



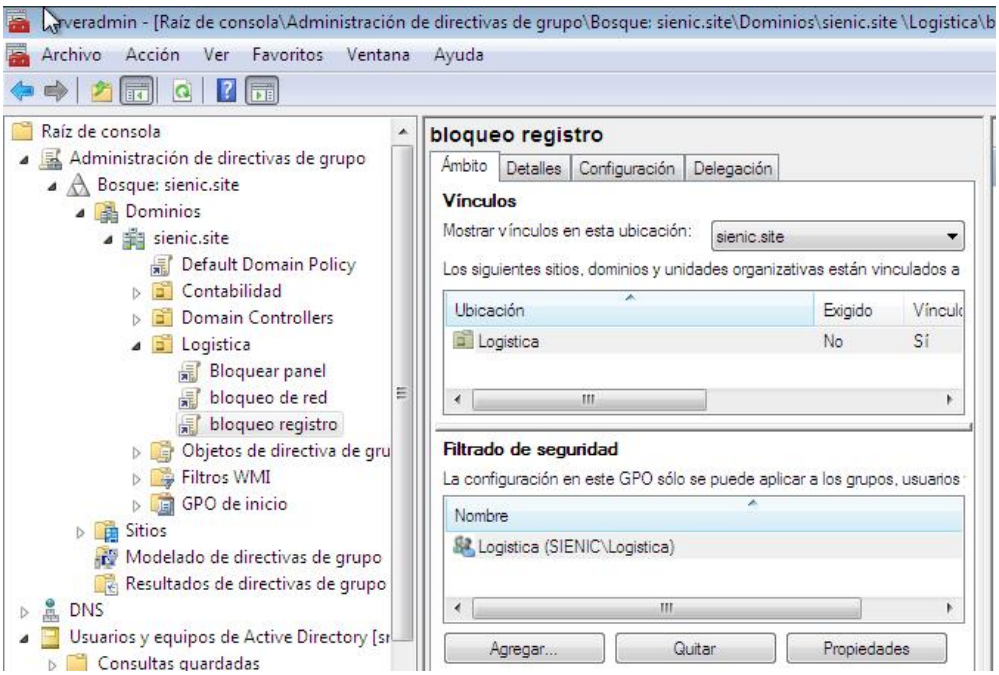
En el siguiente cuadro le ponemos un nombre descriptivo para tener una referencia clara de lo que hace la politica y damos clic en **aceptar**.



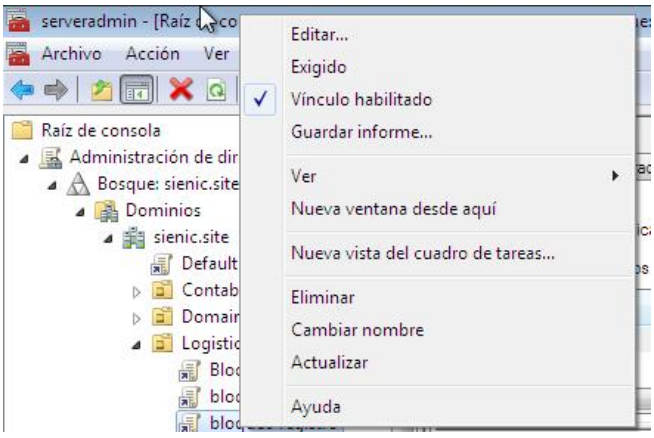
En la lista de GPO asignados a esta OU hacemos doble clic sobre la GPO recien creada.



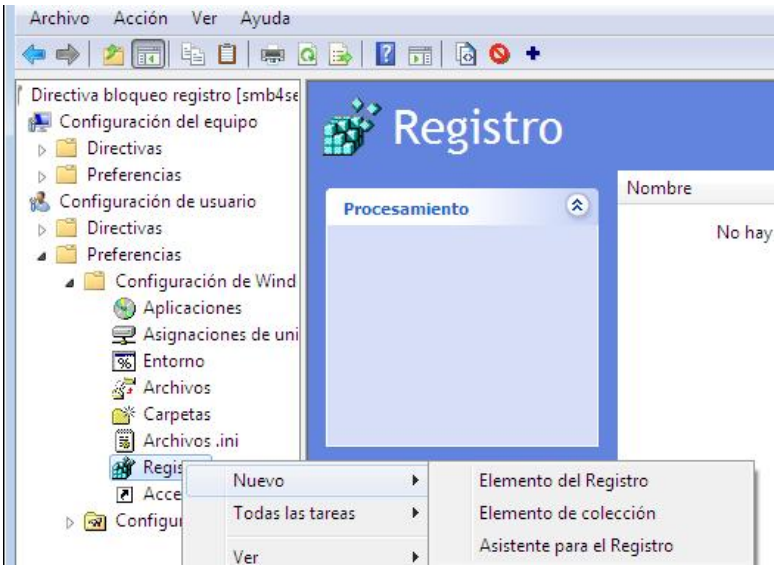
En esta pantalla nos aseguramos que en **filtrado de seguridad** este el grupo al que deseamos aplicar la politica.



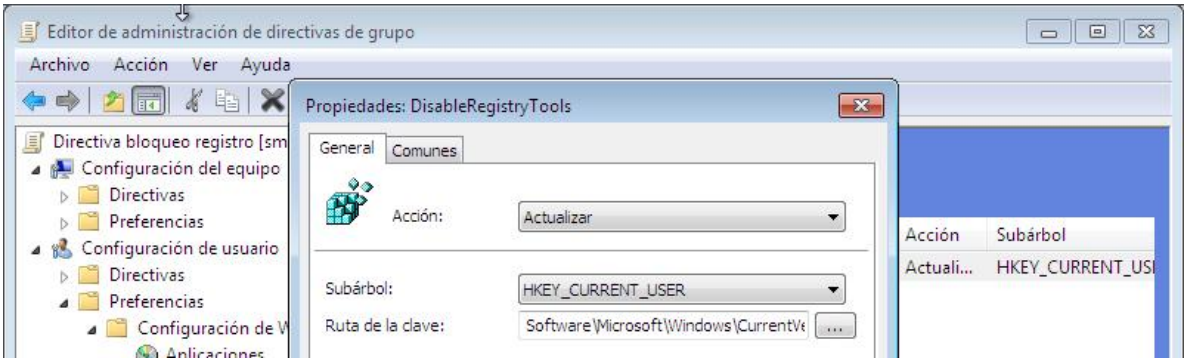
Ahora seleccionamos la GPO y le damos clic con el boton secundario del mouse y seleccionamos **editar.**

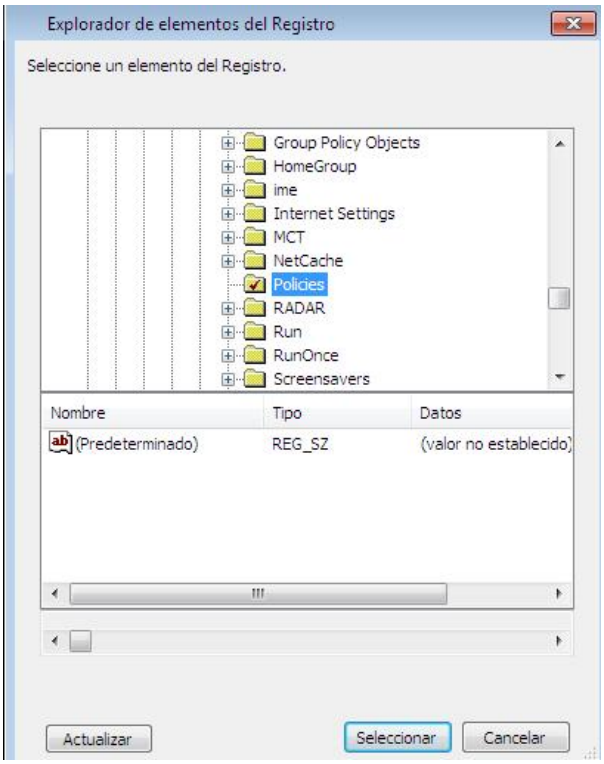


En el editor de politicas de grupo nos vamos a **configuracion de usuario/Preferencias/Configuracion de Windows/Registro**, hacemos clic con el boton derecho sobre este ultimo y seleccionamos **Nuevo/elemento del registro.**

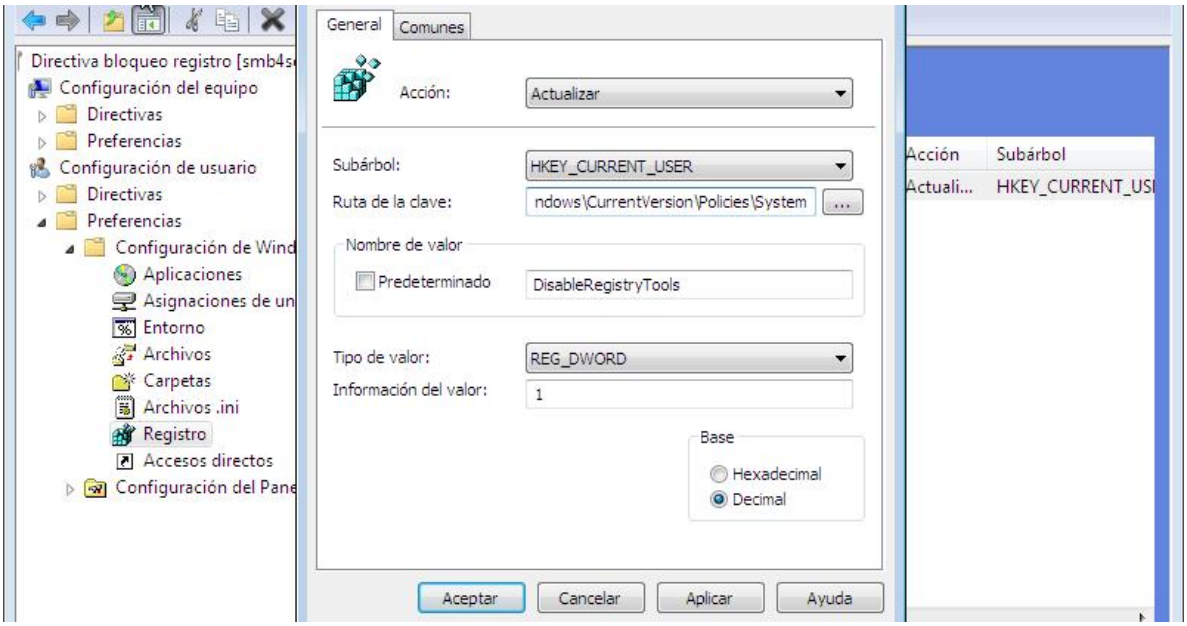


En la siguiente ventana en subarbol seleccionamos **HKEY_CURRENT_USER** y en **ruta de la clave** nos vamos a **Software\Microsoft\Windows\CurrentVersion\Policies** y al final agregamos **System**



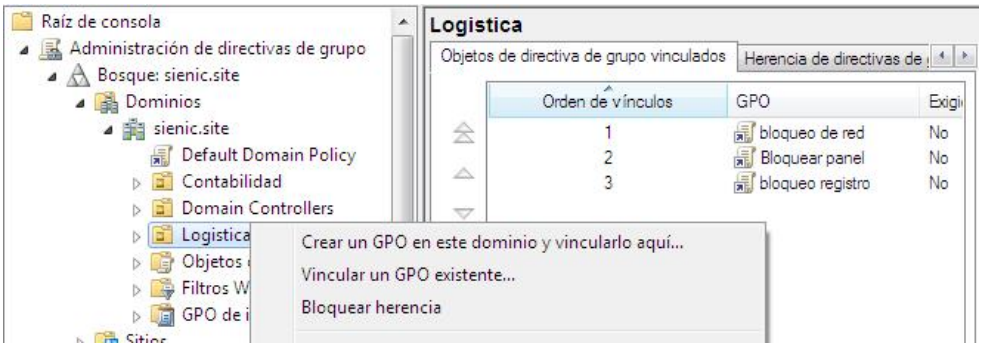


En nombre del valor ponemos **DisableRegistryTools** en tipo de valor seleccionamos **REG_DWORD** y en informacion del valor ponemos **1**, en base debe estar **Decimal**, al final se debe mostrar como la siguiente imagen, al final damos clic en **aceptar**.

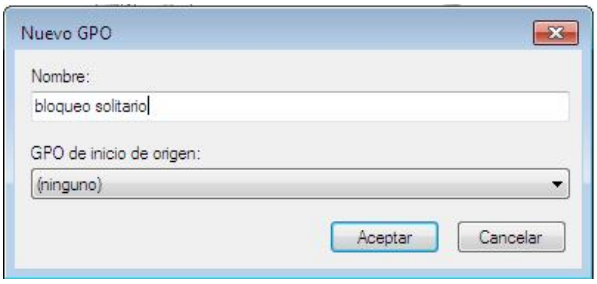


Bloquear un programa por medio de una GPO.

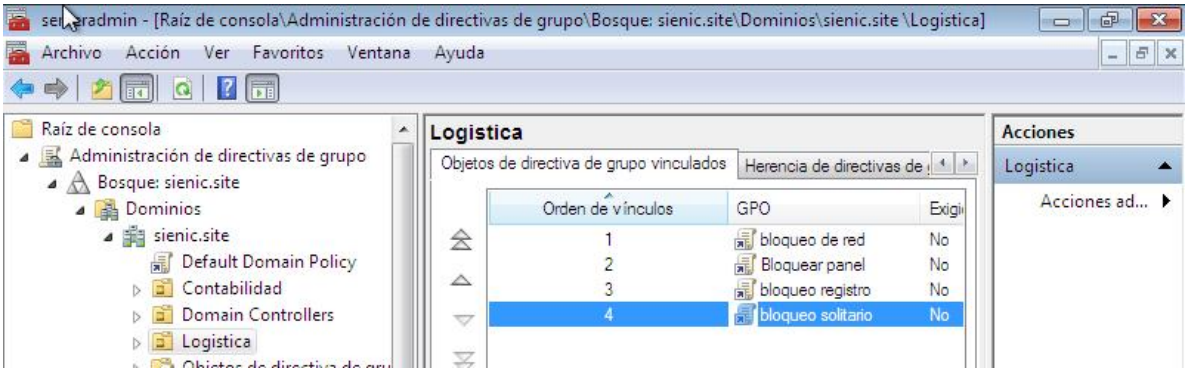
En ocaciones es necesario bloquear un programa ya sea poque se trata de un juego o un programa que genera algun tipo de trafico en la red y los usuarios estan abusando del uso de este, para esto nos vamos a la OU a la que le vamos a aplicar la politica le damos clic con el boton secundario del mouse y seleccionamos **Crear un GPO en este dominio y vincularlo aquí**.



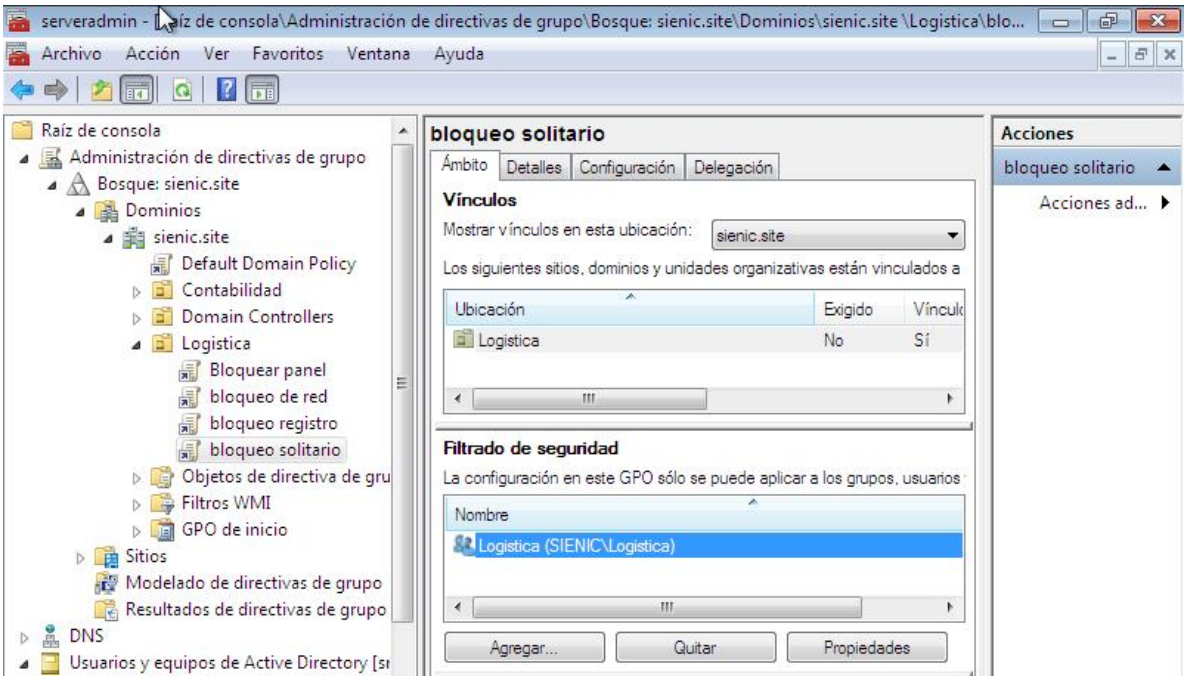
En el siguiente cuadro poner un nombre descriptivo para llevar un control de lo que hacen las GPO que tenemos en el servidor y clic en **aceptar**.



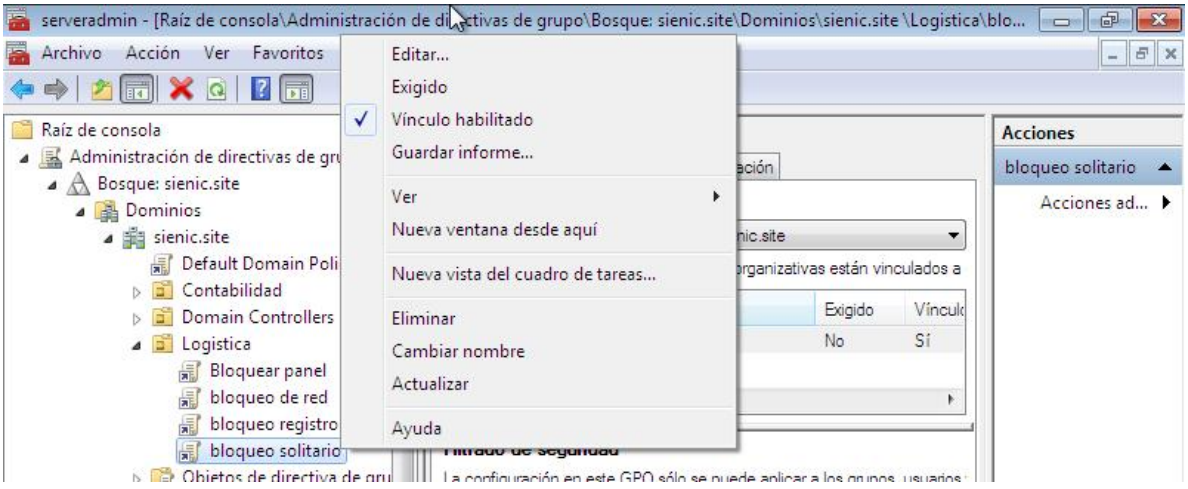
En la lista de GPO damos doble clic sobre la que acabamos de crear.



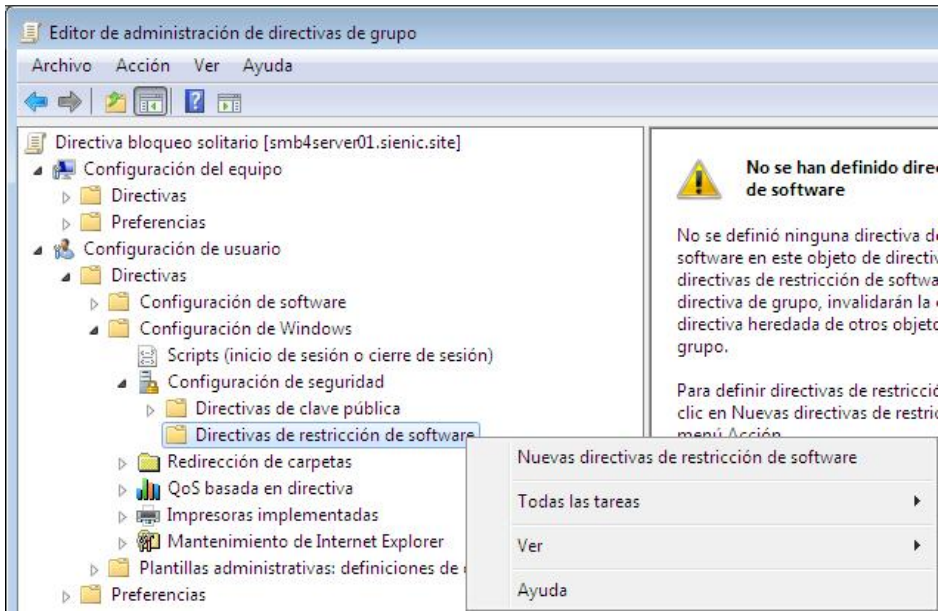
Nos aseguramos que en **filtrado de seguridad** este el grupo o los grupos correspondientes.



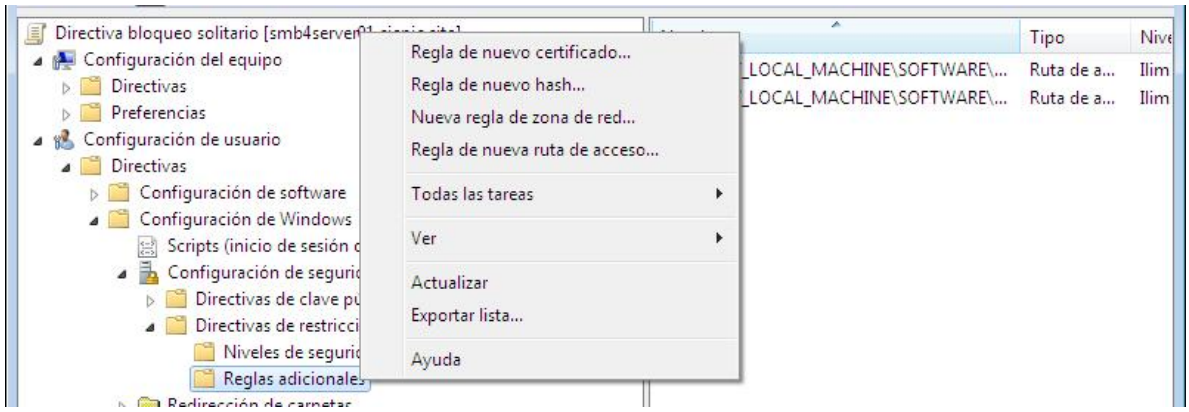
Hacemos clic con el boton secundario del mouse sobre la GPO y seleccionamos **Editar**.



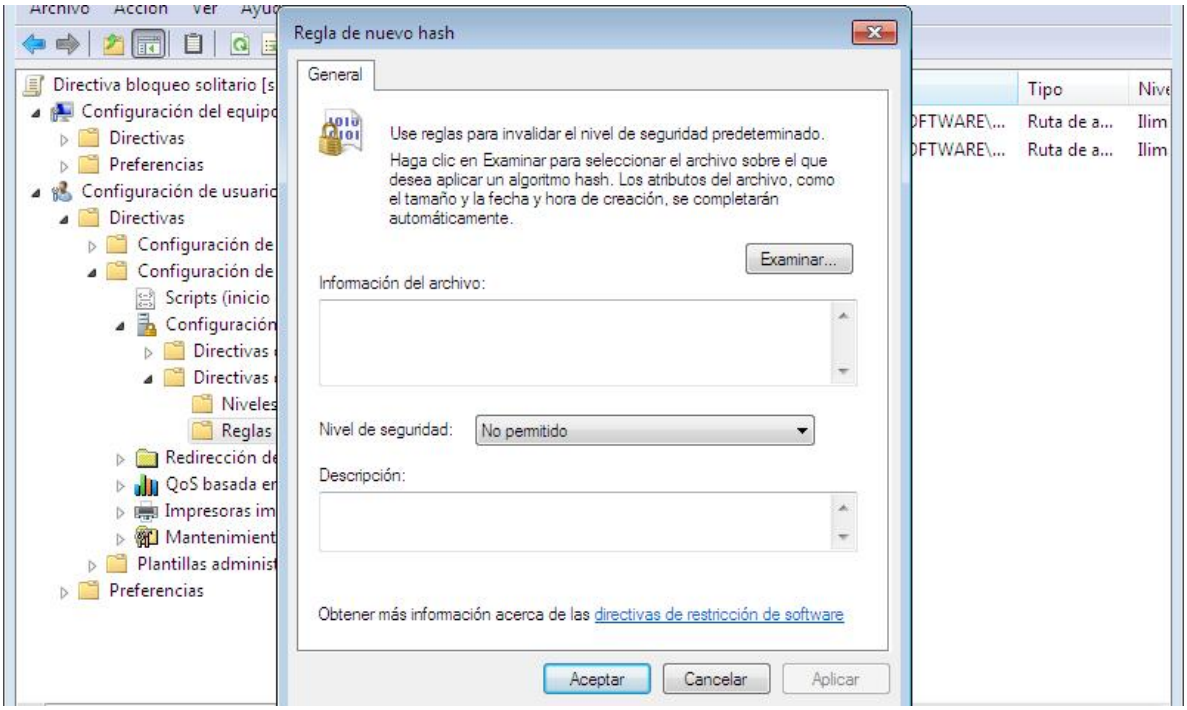
Luego nos vamos a **Configuracion de usuario/Configuracion de Windows/Directivas de restriccion de software** damos clic con el boton secundario del mouse y seleccionamos **Nuevas directivas de restriccion de software.**



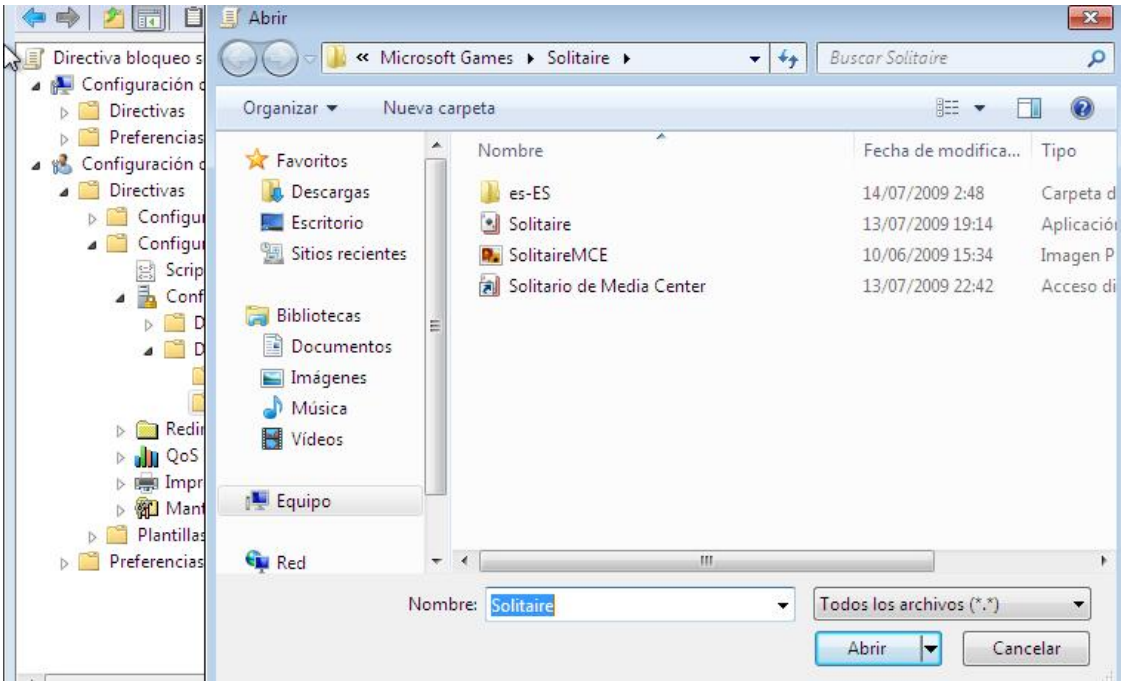
Hacemos clic con el boton secundario sobre **Reglas adicionales** y seleccionamos **Regla de nuevo hash.**



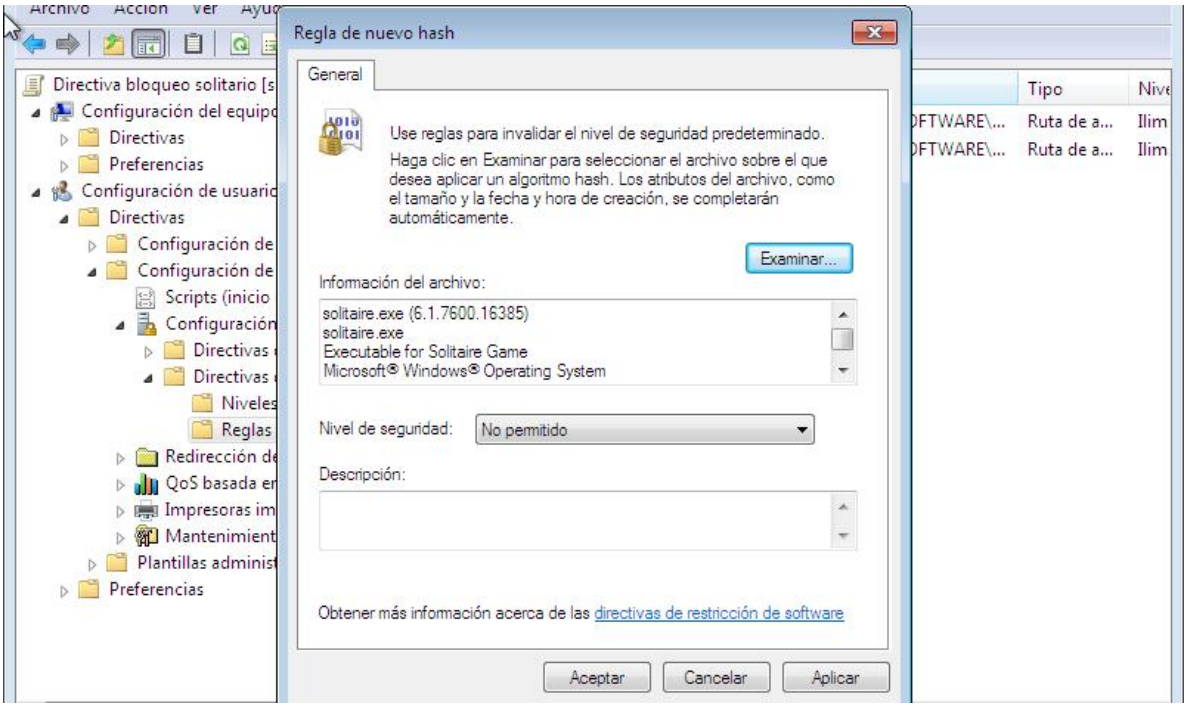
En el siguiente cuadro hacemos clic en **examinar**.



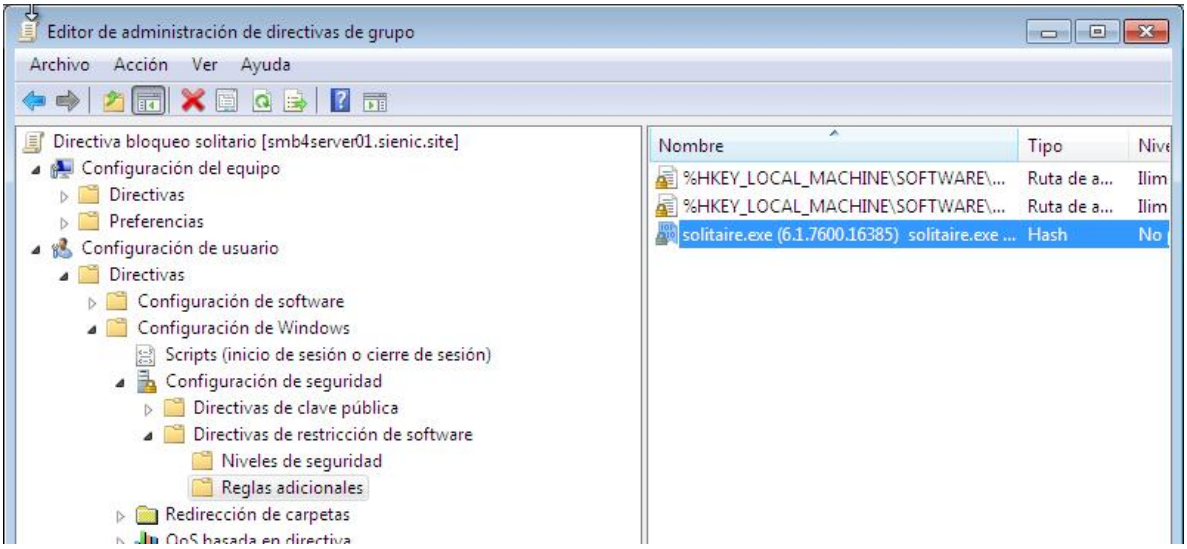
Buscamos la ruta del ejecutable del programa que deseamos bloquear lo seleccionamos y damos clic en **aceptar**.



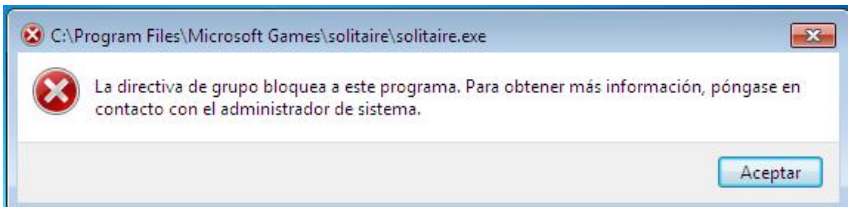
En el siguiente cuadro se muestra toda la informacion del ejecutable, damos clic en **aceptar**.



Ahora se nos muestra el ejecutable en el panel derecho.

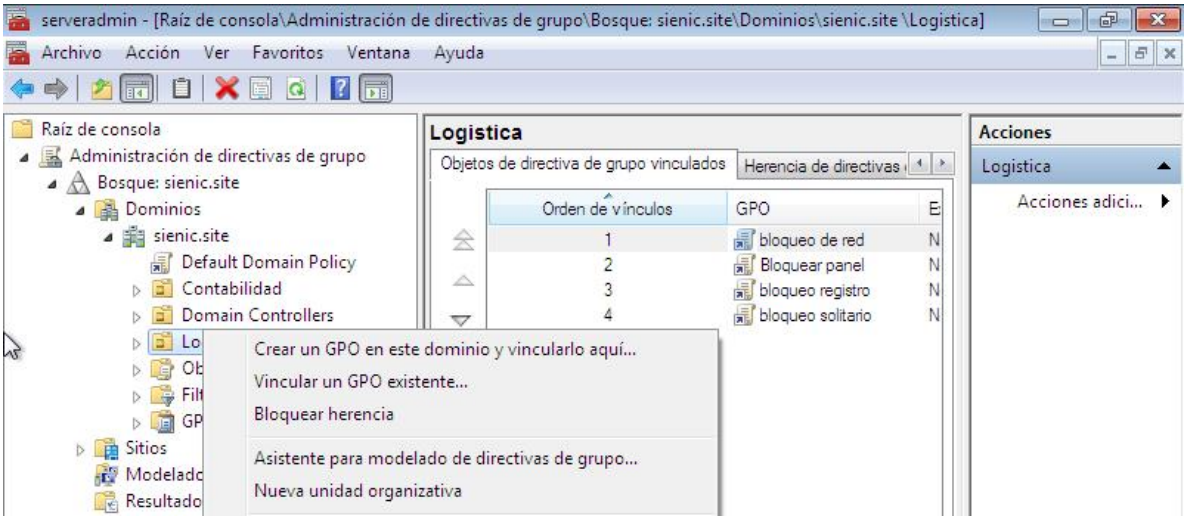


Ahora cuando el usuario trate de ejecutar el programa le aparecera este cuadro de dialogo.

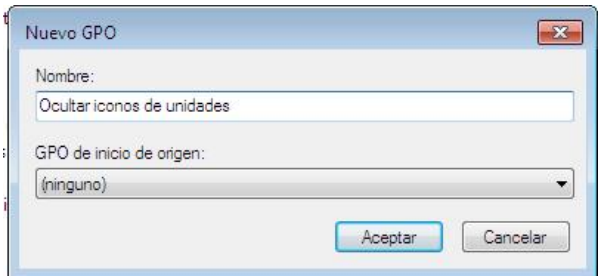


Ocultar Unidades en Mi Pc.

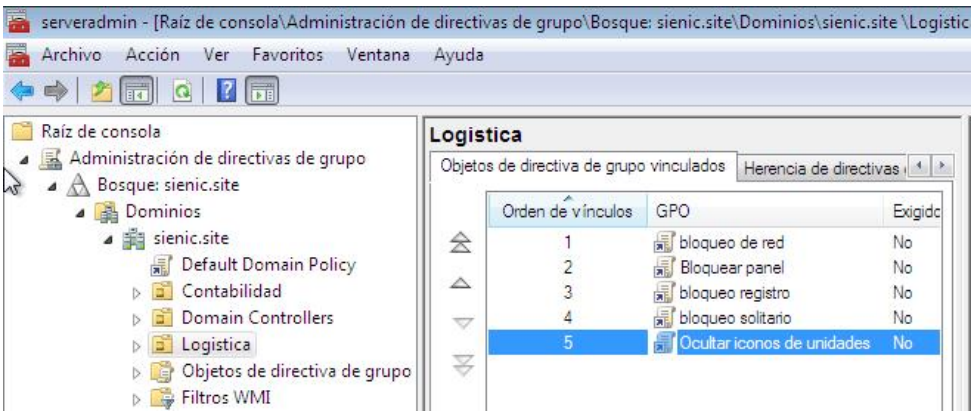
En este ejercicio vamos a ocultar las unidades A, B, C Y D para que el usuario no pueda verlar cuando haga doble clic sobre el icono Mi PC, para esto nos vamos a la OU a la que vamos a aplicar la politica hacemos clic con el boton derecho del raton y seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



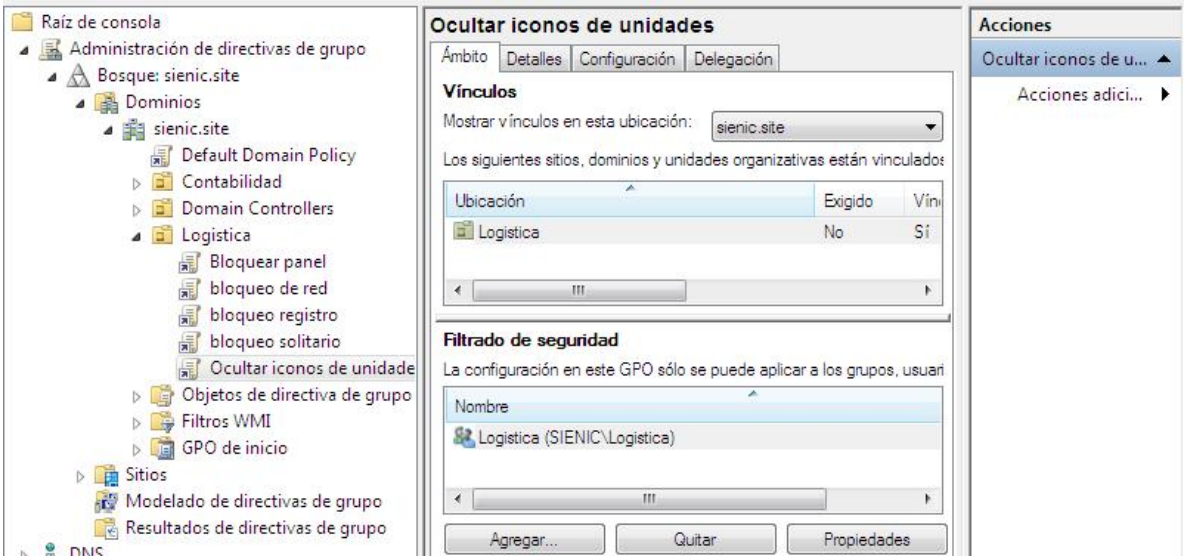
En el siguiente cuadro le ponemos un nombre descriptivo a la GPO y clic en **aceptar**.



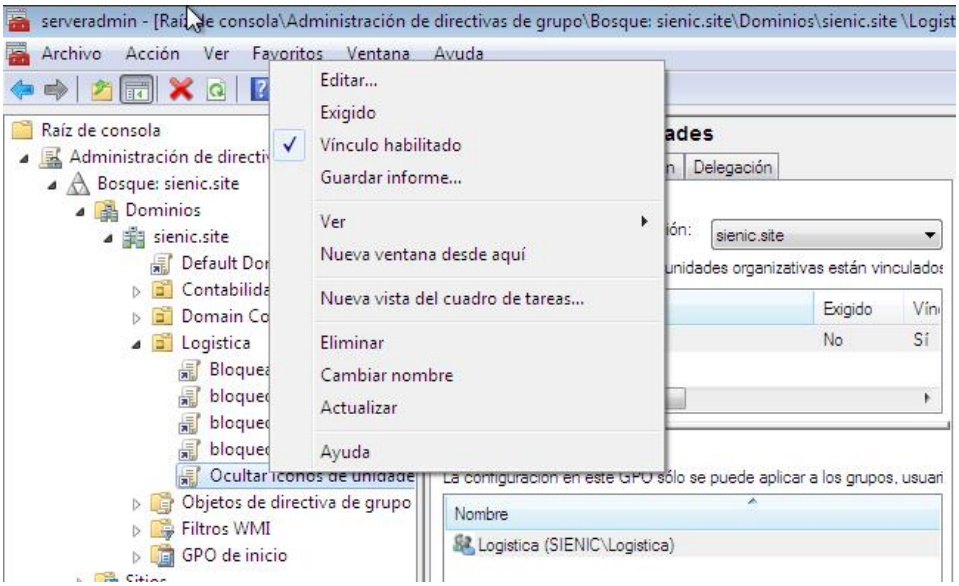
Hacemos doble clic sobre la GPO



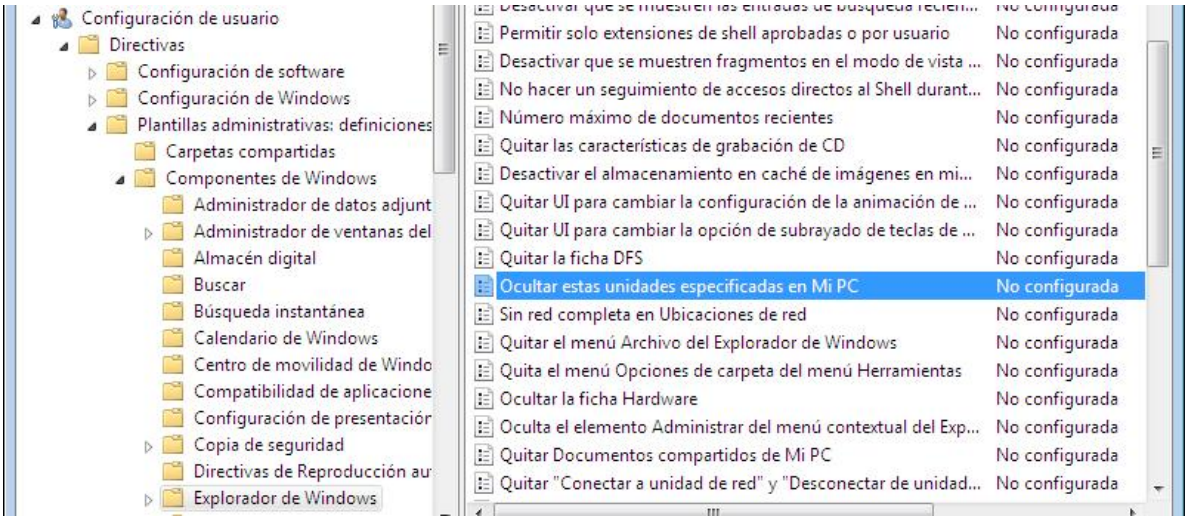
En la siguiente ventana nos aseguramos que en **filtrado de seguridad** esten los grupos a los que deseemos aplicar la politica de seguridad.



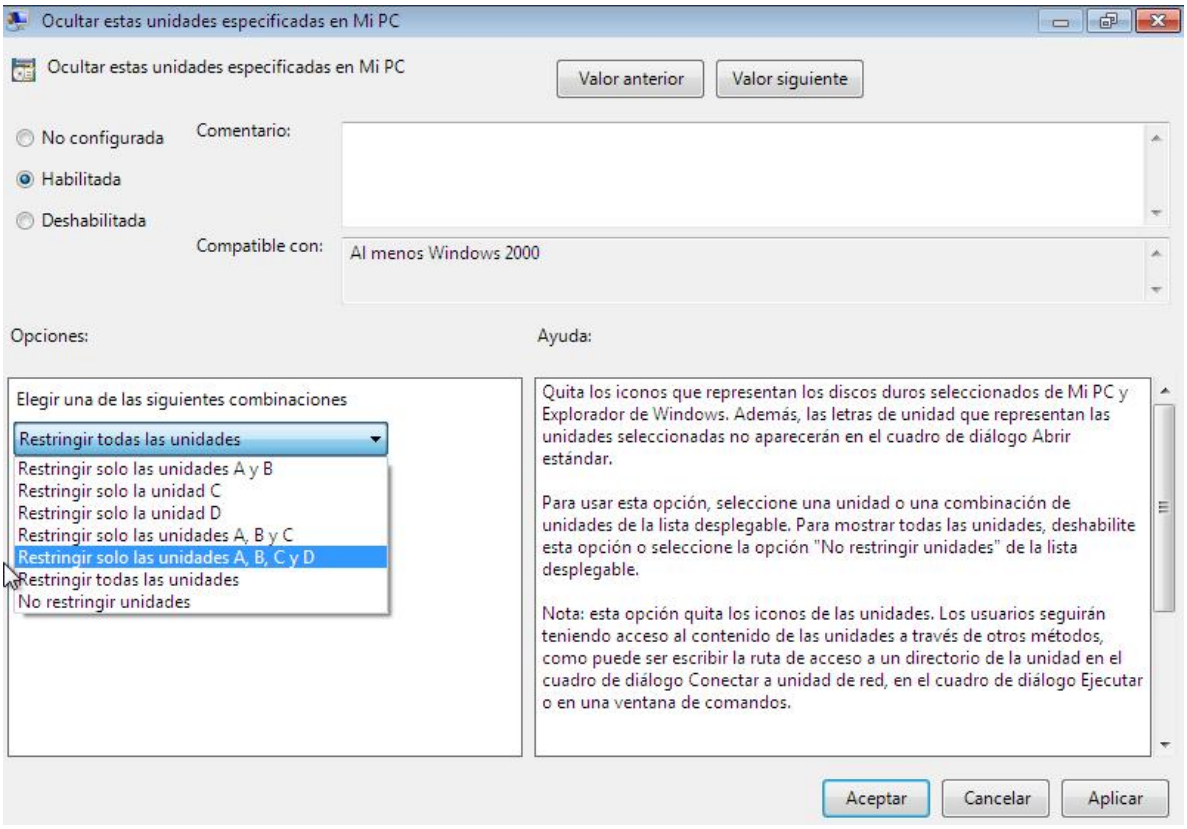
El siguiente paso es hacer clic con el boton secundario del mouse sobre la GPO y seleccionamos **Editar**.



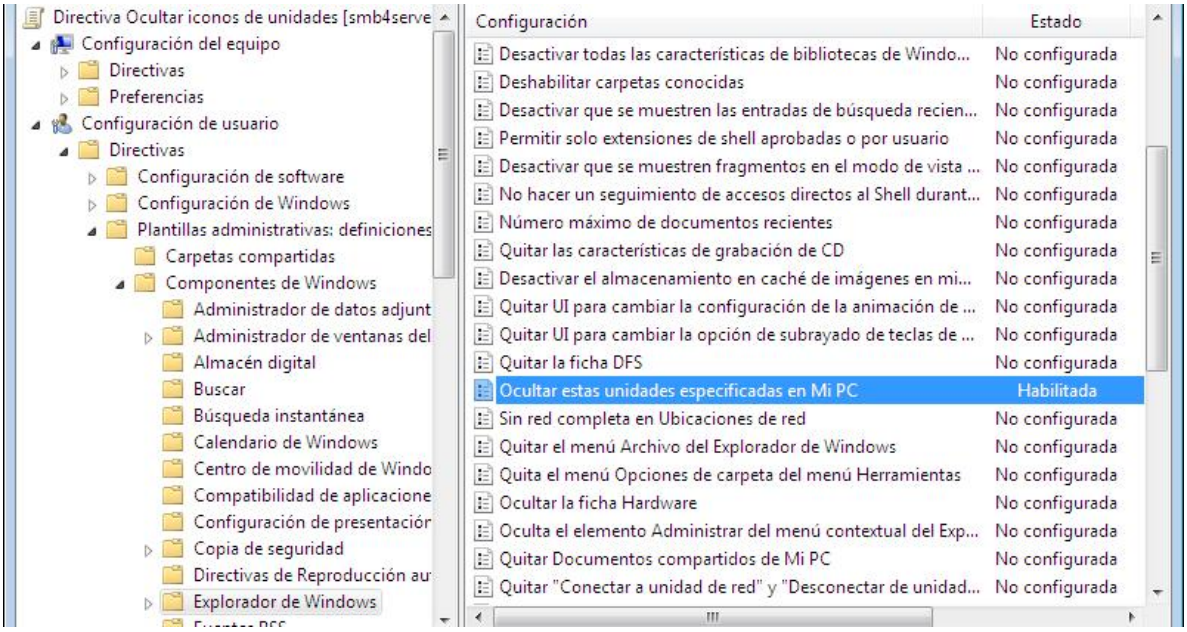
Luego nos vamos a **Configuracion de usuario/Plantillas administrativas/Componentes de Windows/Explorador de Windows** y hacemos doble clic sobre la opcion **Ocultar estas unidades especificadas en Mi PC**.



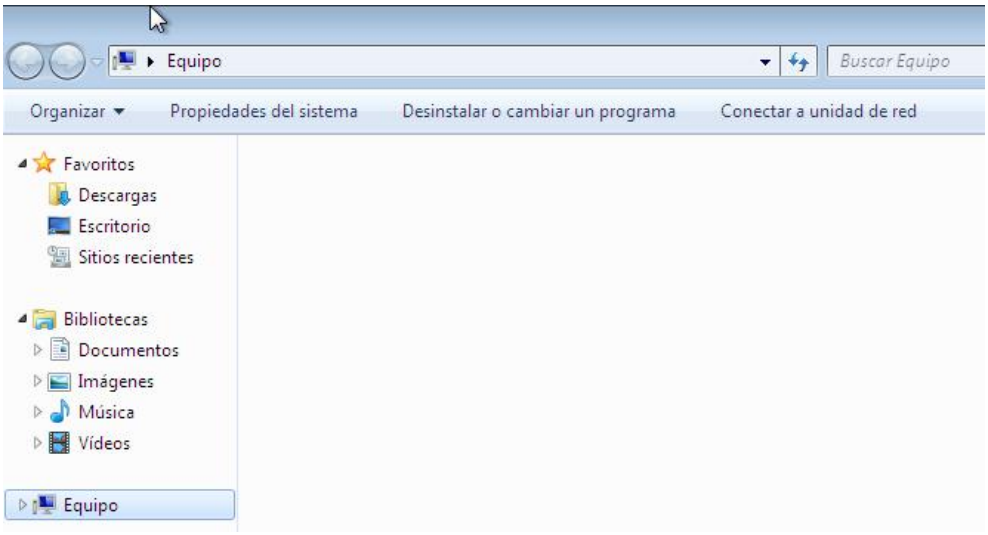
En este cuadro seleccionamos la opcion **Habilitada** y en **Elegir una de las siguientes combinaciones** seleccionamos **Restringir solo las unidades A, B, C y D.**



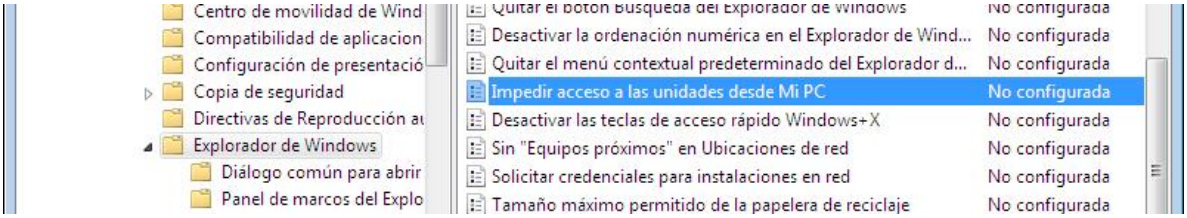
Damos clic en **aceptar**, con esto ya tenemos configurada la GPO.



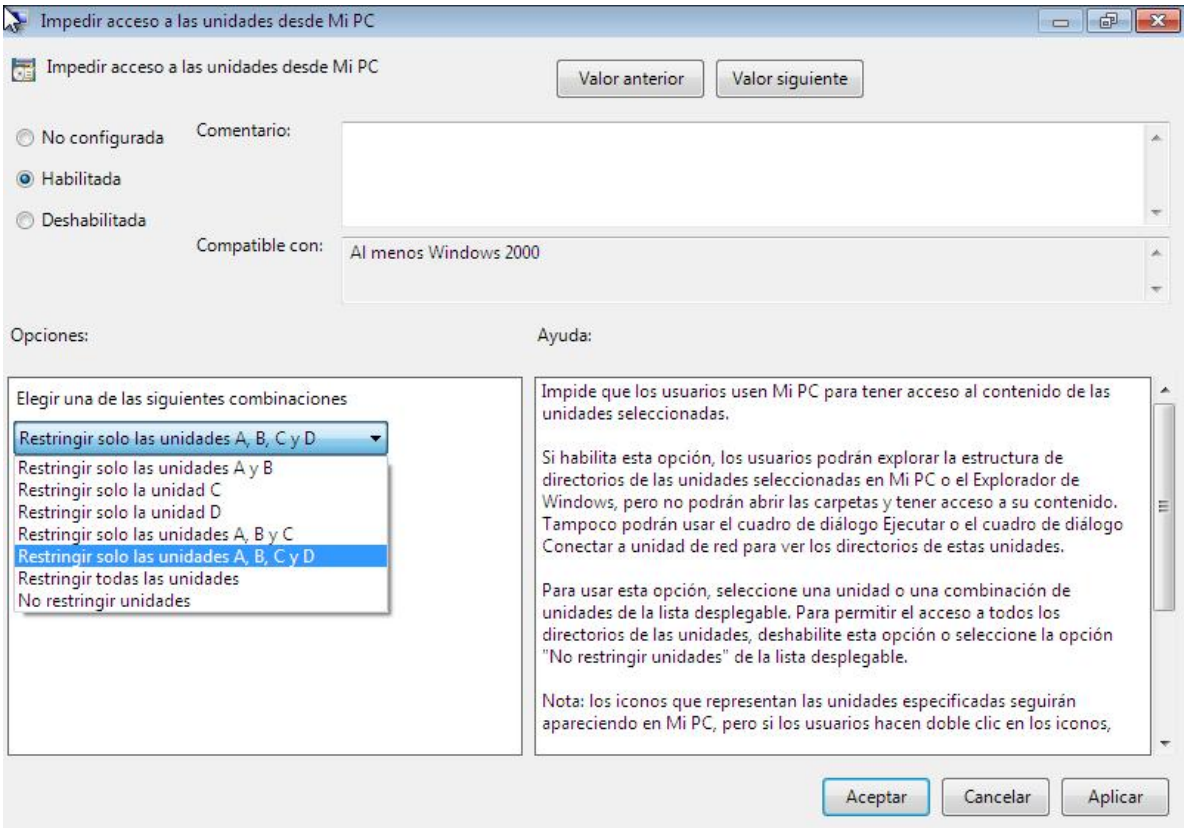
A como podemos ver en la siguiente imagen no se muestra nada cuando hacemos doble clic sobre el icono Mi PC.



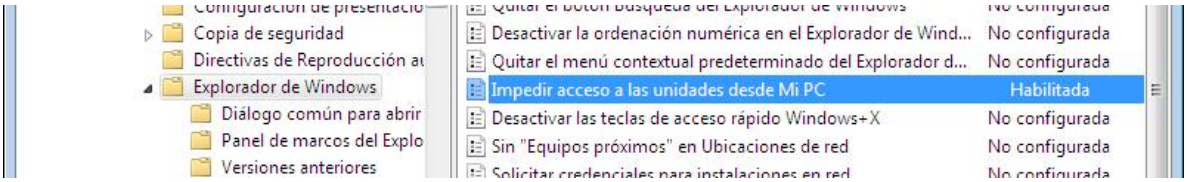
Esta ultima configuracion solo oculta las unidades pero el usuario podra entrar a la unidad de red si escribe la ruta en el cuadro de dialogo ejecutar o si escribe la ruta en la barra de direcciones del explorador de Windows, para impedir que el usuario tenga acceso a las unidades espeficicadas hay que usar la opcion **Impedir acceso a las unidades desde mi PC**.



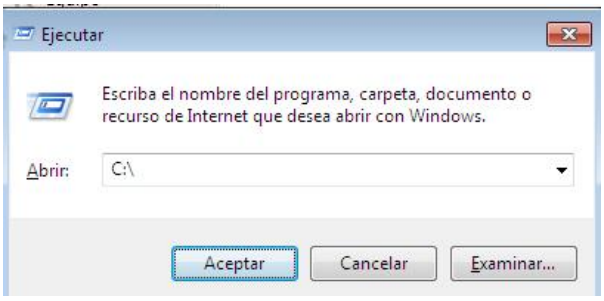
Habilitamos la opcion y seleccionamos las unidades que queremos bloquear, luego le damos clic en **aceptar**.

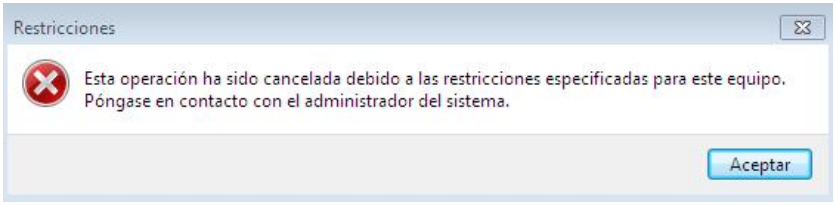


Con eso ya tenemos habilitada la opcion para que los usuarios no puedan entrar a las Unidades que hemos bloqueado.



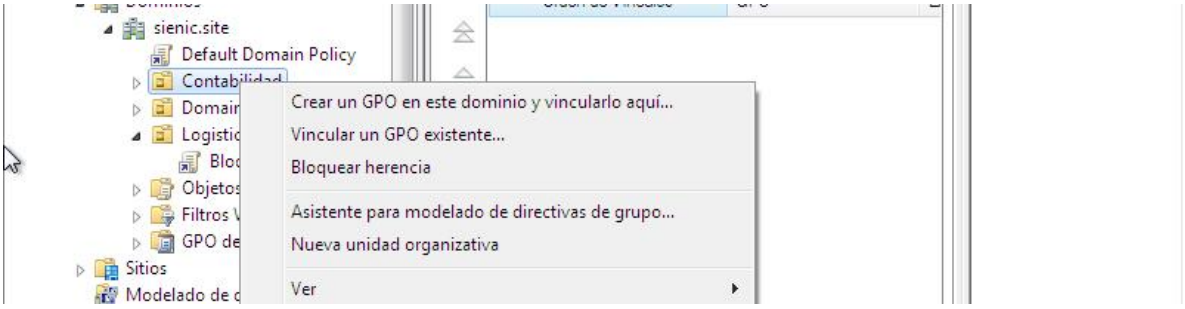
Si el usuario escribe la ruta ya sea en Ejecutar o en la barra de direcciones de Windows explorer recibira un error.



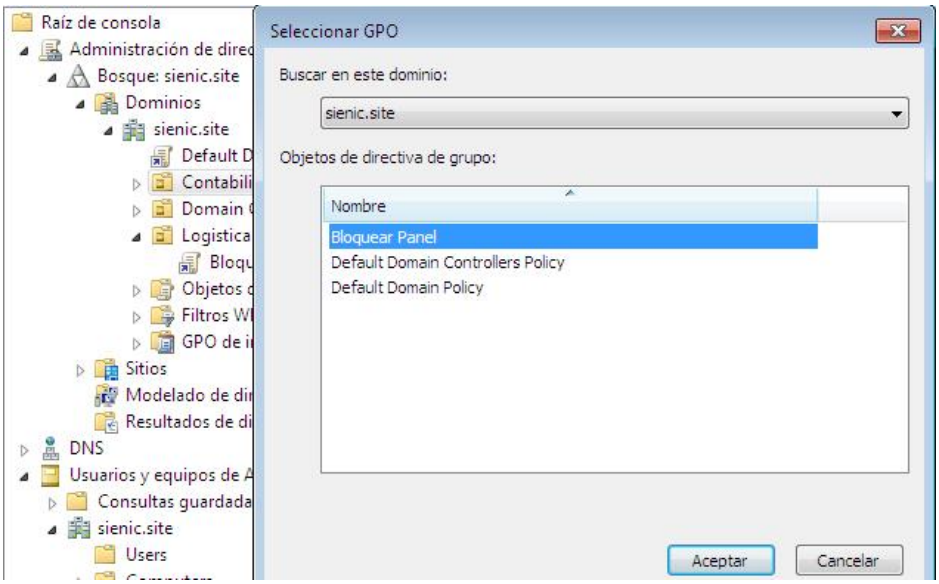


Vincular un GPO existente a una unidad organizativa.

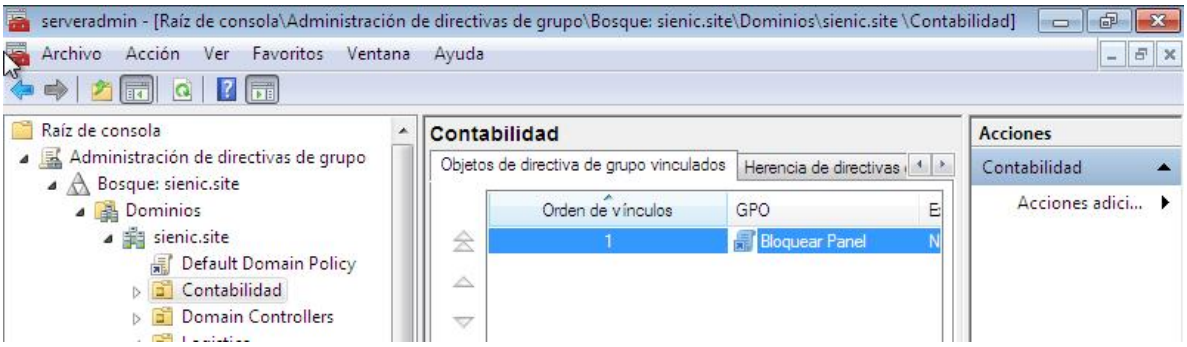
En ocaciones es necesario aplicar un GPO existente a otra unidad organizativa, esto nos permite aplicar politicas de seguridad a otros usuarios de otros departamentos sin necesidad de volver a crear otra politica con los mismos parametros evitando asi redundancia, para llevar a cabo esta tarea, nos vamos a la OU a la que deseemos aplicar la directiva ya existente y le damos clic con el boton derecho del mouse, luego seleccionamos **Vincular un GPO existente**.



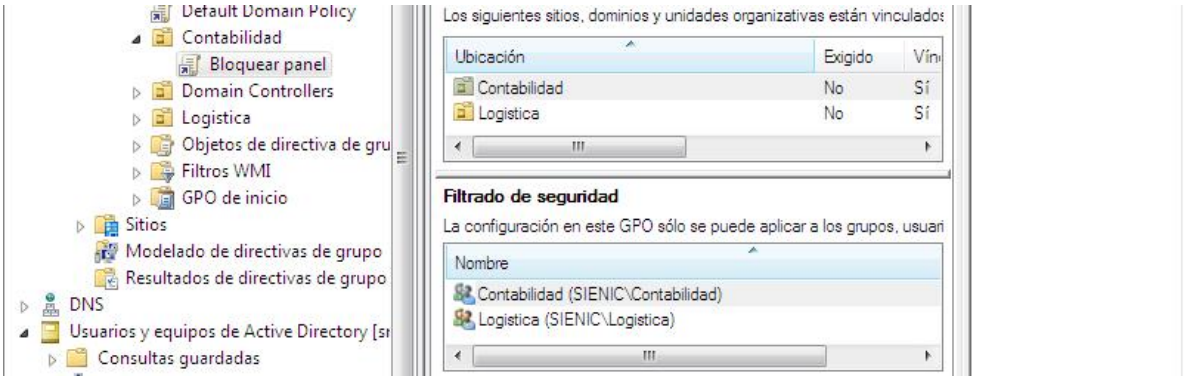
En la siguiente ventana seleccionamos la GPO que deseamos aplicar y damos clic en **aceptar**.



Ahora podemos ver que la GPO aparece en la lista de objetos vinculados a esta OU a como se muestra a continuacion, es importante saber que esto es solo un vinculo a un objeto GPO, por lo que si la borramos lo que estamos borrando es un acceso directo no la GPO en si.



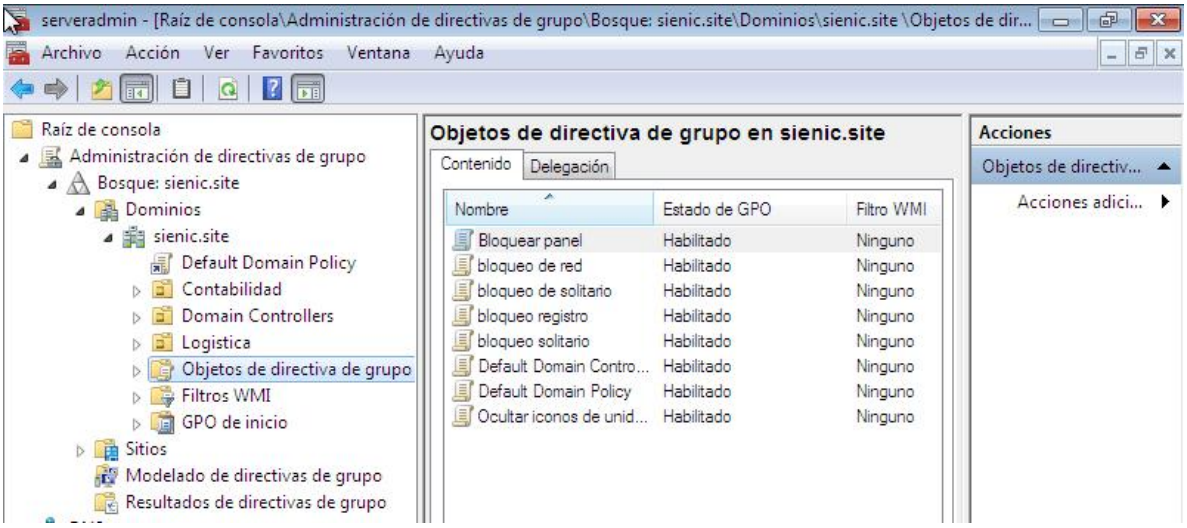
Hacemos doble clic sobre la GPO y agregamos los grupos de usuarios correspondientes en este caso el grupo contabilidad.



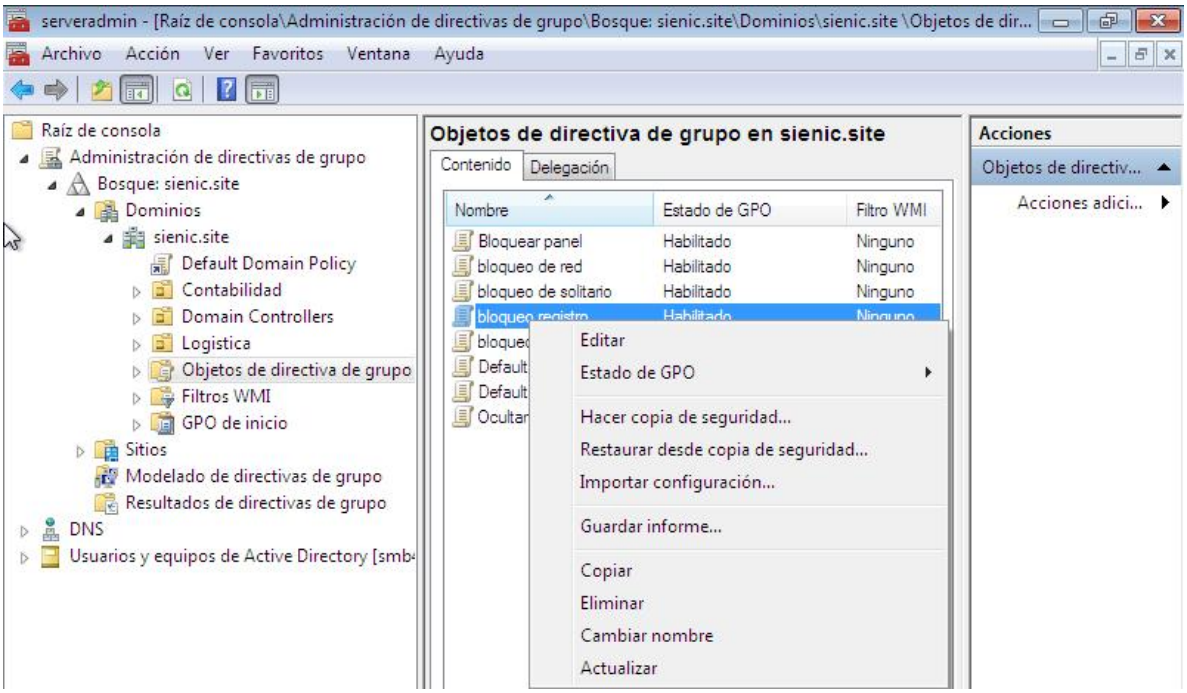
Aunque en el filtrado de seguridad este agregado el grupo, si no se vincula la GPO a la OU los parametros no se van a aplicar, la GPO tiene que estar vinculada a la OU y el grupo agregado para que esto funcione.

Eliminar una GPO.

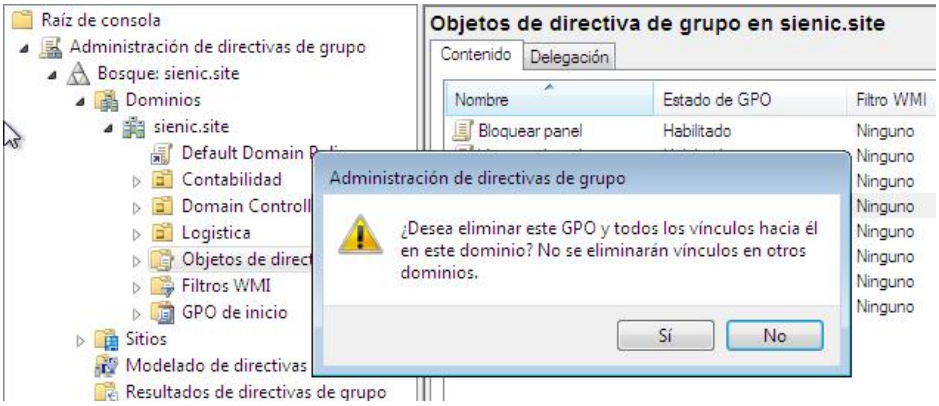
Para eliminar una GPO nos vamos a **Administracion de directivas de grupo**, seleccionamos el dominio y luego **Objetos de directiva de grupo**, en el panel derecho se mostraran todas las GPO creadas.



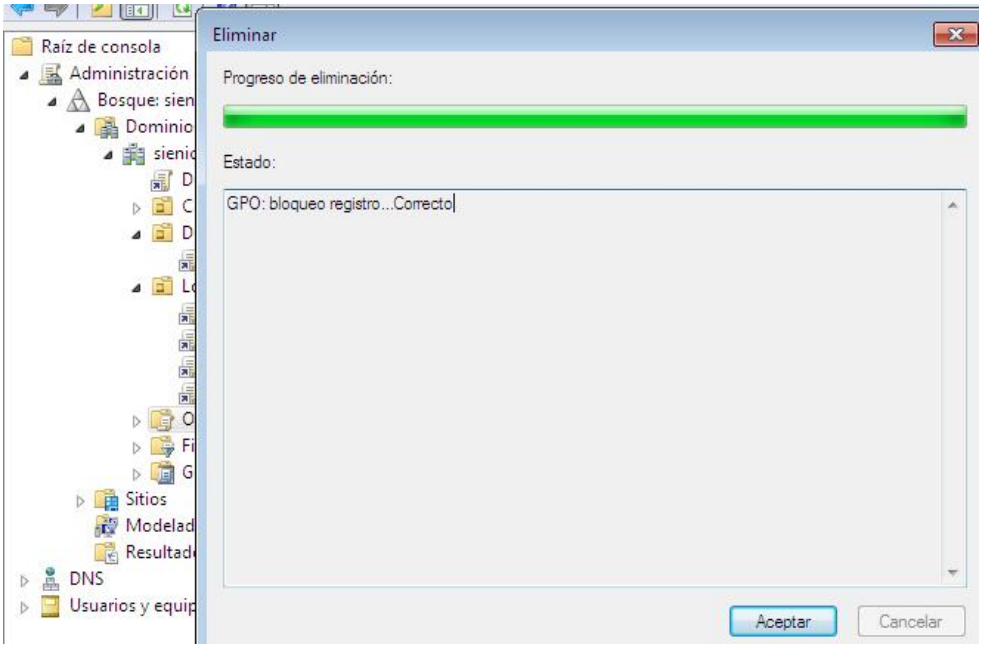
Seleccionamos la GPO que deseamos eliminar y hacemos clic con el boton secundario del mouse luego seleccionamos **Eliminar**.



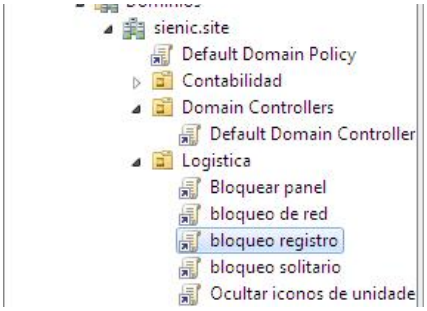
Nos va a a aparecer una cuadro de confirmacion donde se nos indica que si borramos la GPO tambien se eliminaran todos los vinculos a OU que hayamos creado.



Damos clic en **si** y se nos mostrara esta pantalla al terminar damos clic en **aceptar**.



En la siguiente imagen se muestra un vinculo a la GPO que estamos borrando que es bloqueo de registro y que esta vinculado a la OU Logistica.



Aquí se muestra que despues de borrar el objeto GPO tambien se elimina automaticamente el vinculo de las OU.

Delegar Control sobre una Unidad organizativa.

Para hacer efectiva una delegacion de control, los objetos a administrar deben estar dentro de la unidad organizativa, esto es que si existe un usuario que pertenece a un grupo que esta dentro de

la unidad organizativa, pero el usuario en si no esta dentro de la OU, no se podra administrar este usuario a menos que se incluya explicitamente dentro de la OU.

Lo primero que debemos hacer para poder delegar control sobre una OU es modificar el archivo `/usr/local/samba/etc/smb.conf` y agregar la opcion

acl:search=false

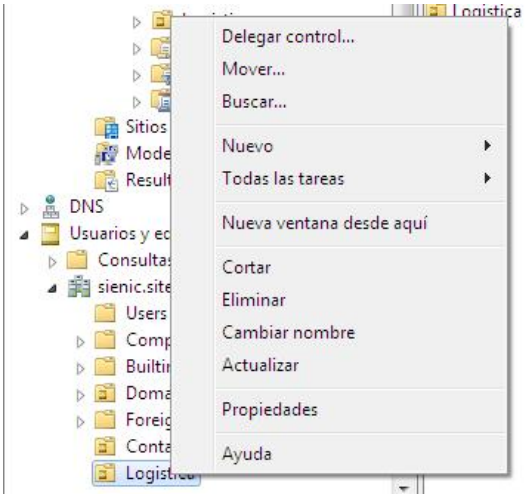
Luego ejecutamos el comando

```
smbcontrol all reload-config
```

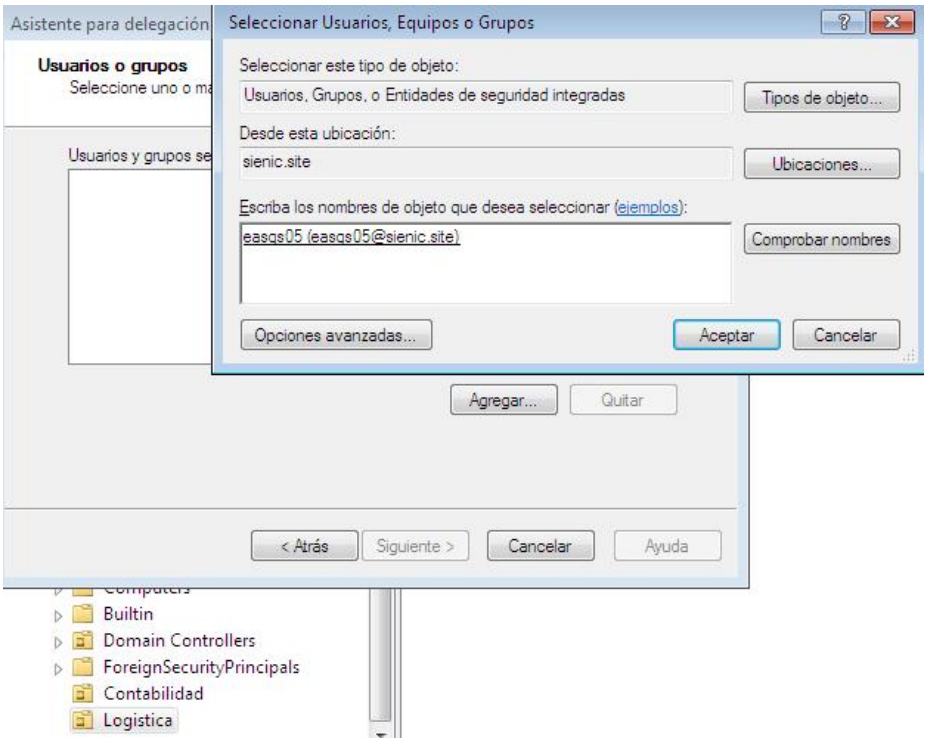
Para revisar que la configuración del archivo smb.conf este bien ejecutamos el comando.

```
samba-tool testparm –v
```

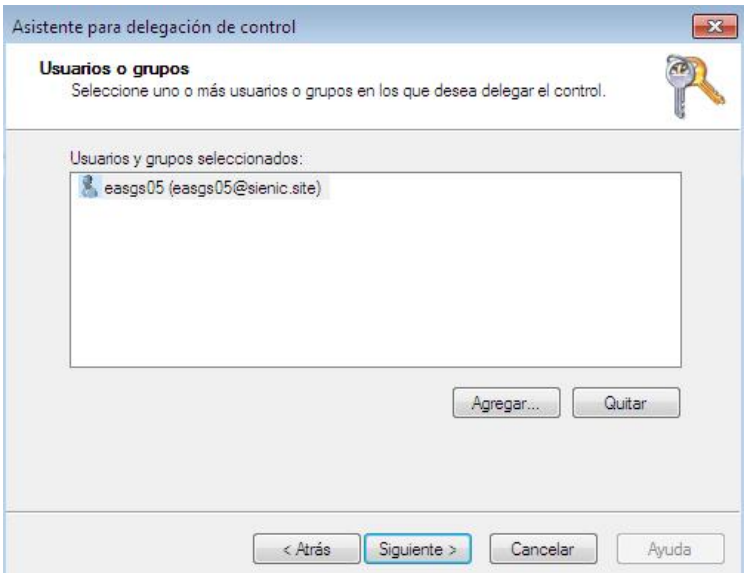
Luego en **Usuarios y equipos de active directory** damos clic derecho sobre la OU en la que deseamos delegar control y en el menu desplegable seleccionamos **Delegar Control**, en el siguiente cuadro damos clic en **siguiente**.



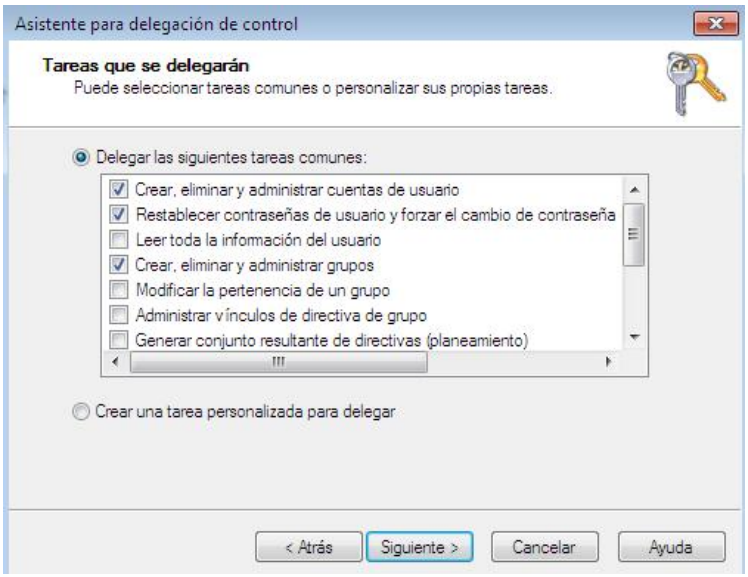
En la siguiente ventana damos clic en **Agregar** y en el cuadro introducimos el usuario al que deseemos delegar control en esta OU, damos clic en **Comprobar nombre** y luego en **aceptar**.



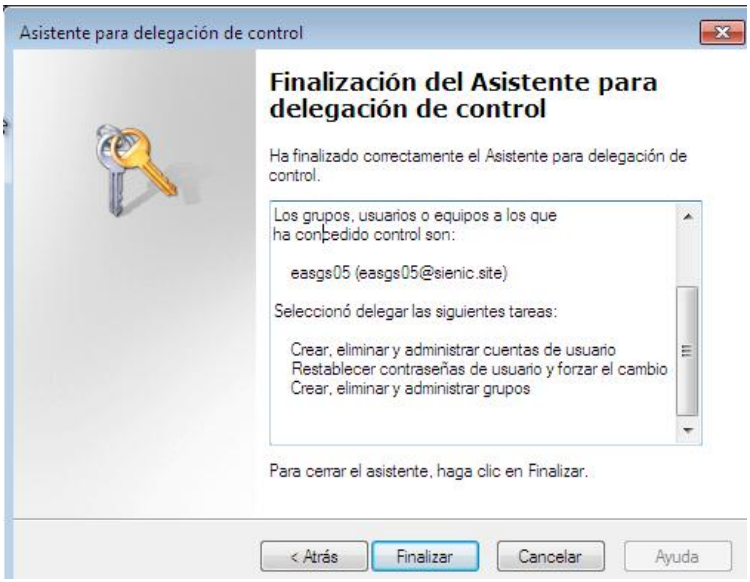
Damos clic en **siguiente.**



En este cuadro seleccionamos las tareas que vamos a delegarle al usuario, damos check a las que deseemos.



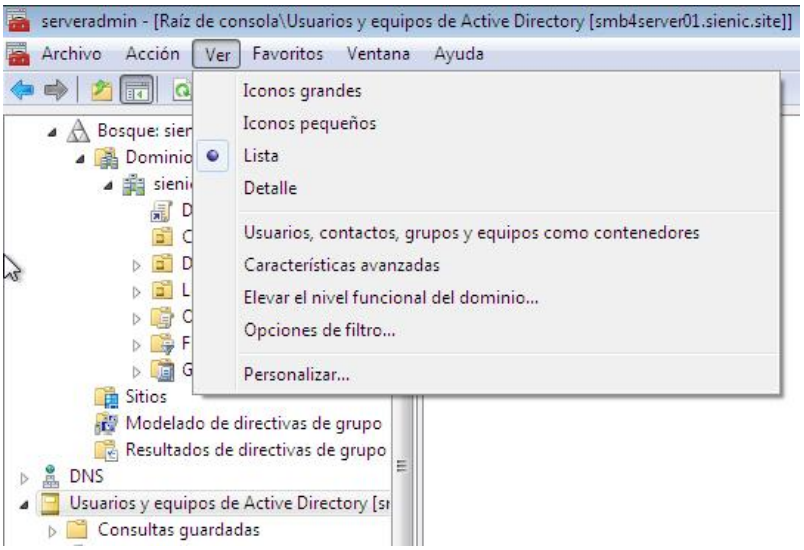
Al terminar el asistente le damos clic en **finalizar**.



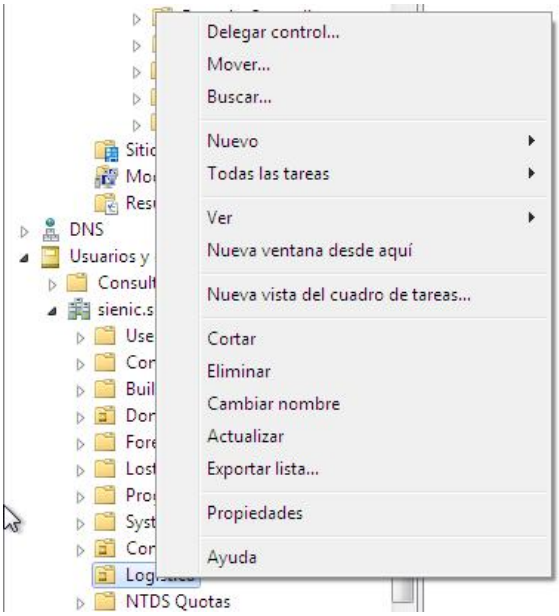
Con esto el usuario podra hacer las todas tareas especificadas dentro de esta OU.

Revisar los permisos delegados.

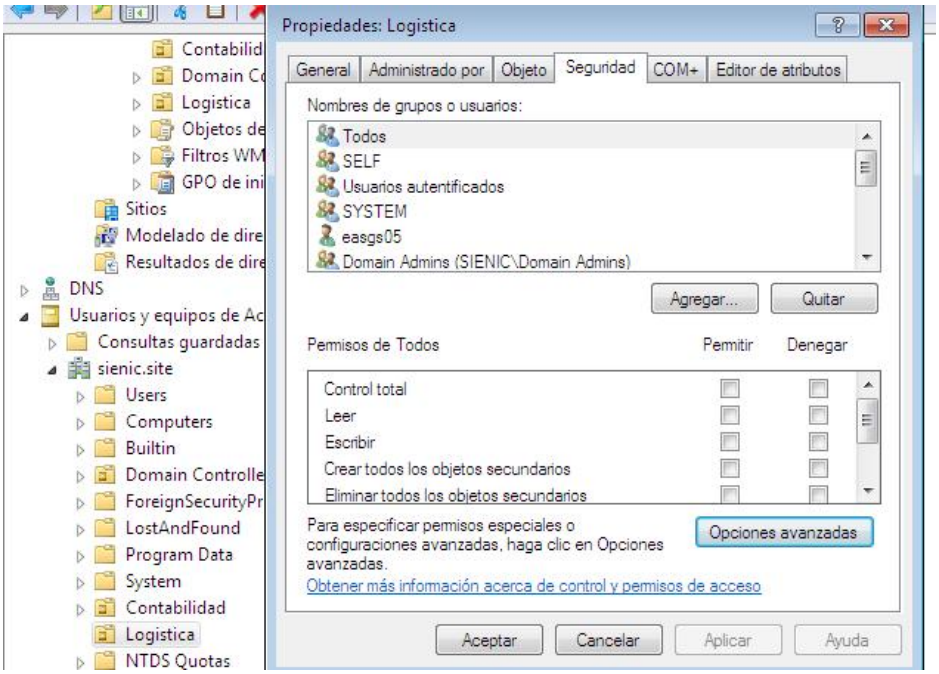
Para revisar los permisos que hemos delegado en una unidad organizativa nos vamos a **Usuarios y equipos de Active Directory/Ver/Caracteristicas avanzadas.**



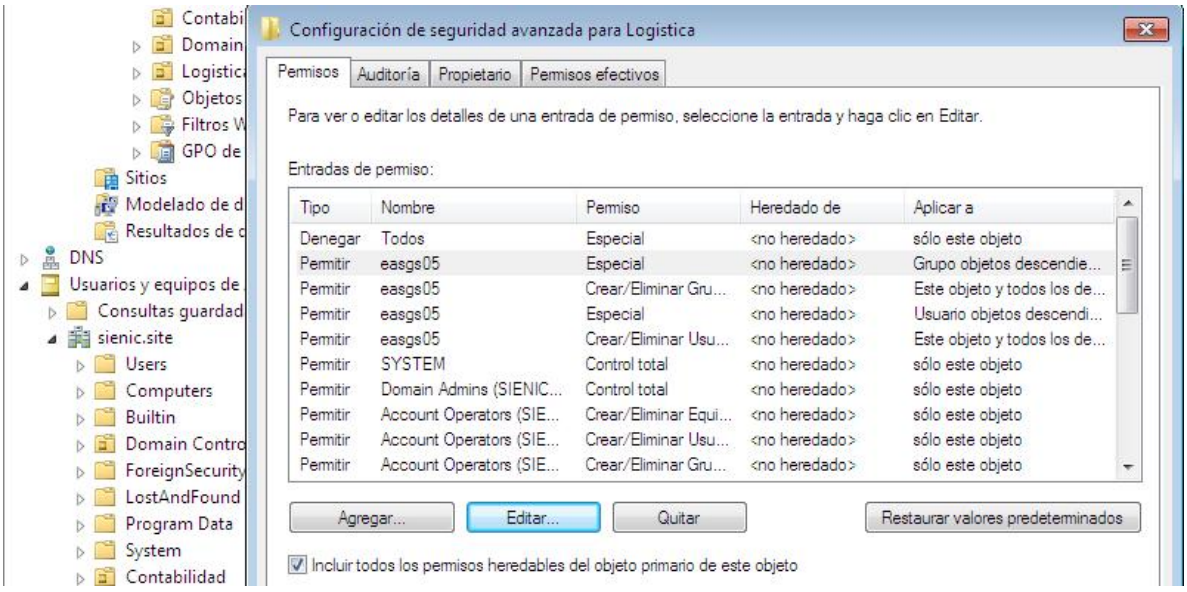
Seleccionamos la OU y le damos clic con el boton secundario del mouse y damos clic en **propiedades**.



En el cuadro de propiedades seleccionamos la solapa **Seguridad** y damos clic en **opciones avanzadas**.

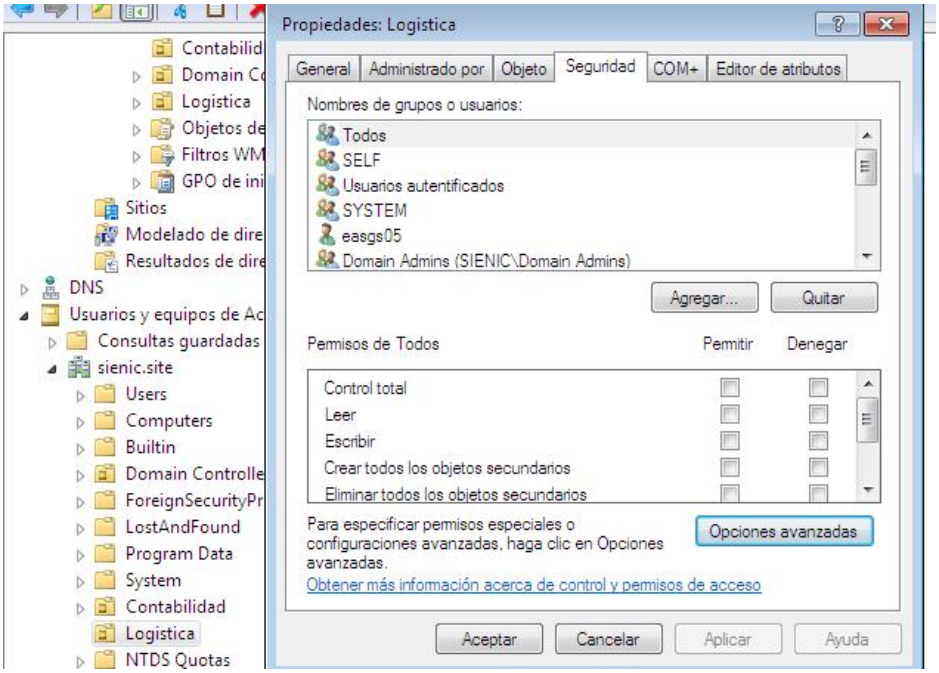


En este cuadro se muestran los permisos asignados al usuario en esta OU.



Revocar los permisos delegados.

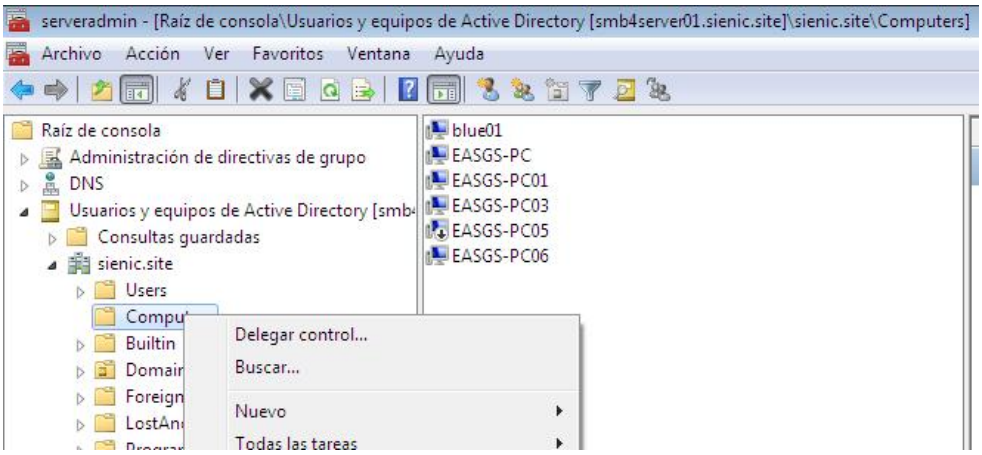
Para revocar una delegacion basta con eliminar el usuario de la solapa **seguridad** de las **propiedades** de la unidad organizativa.



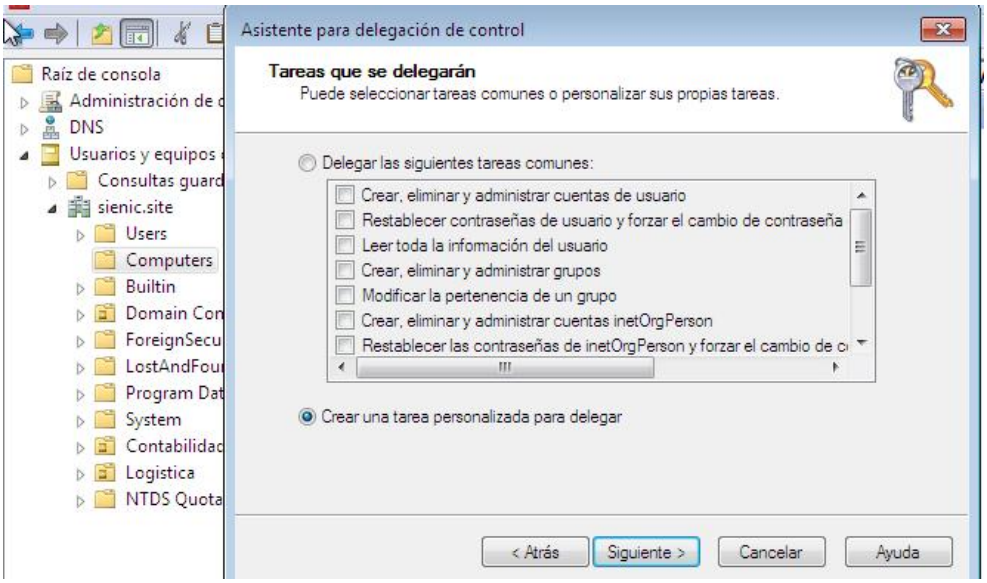
Delegar control para unir maquinas al dominio.

Esta delegacion solo se puede asignar sobre el contenedor Computers y se puede aplicar ya sea a un grupo o a un usuario.

Para llevar a cabo esto nos vamos a **Usuarios y equipos de Active Directory** y damos clic con el boton secundario del mouse sobre el contenedor **Computers**, luego seleccionamos **Delegar control** y damos clic en **siguiente** en el primer cuadro de asistente.

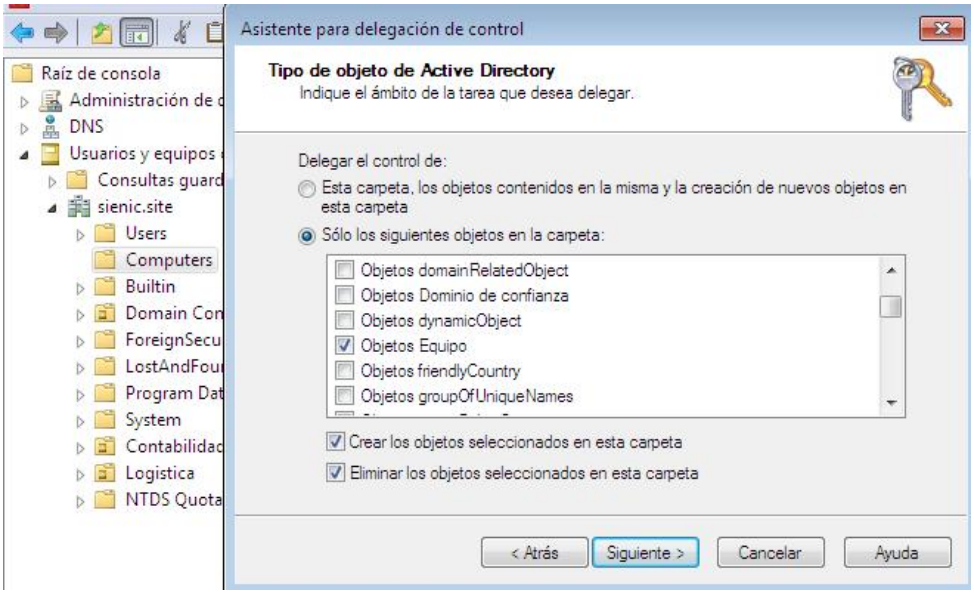


En la siguiente pantalla damos clic en **agregar**, escribimos el nombre del usuario o grupo y damos clic en **comprobar nombre** y clic en **aceptar** y despues en **siguiente**, en la siguiente pantalla seleccionamos la opcion **Crear una tarea personalizada para delegar** y clic en **siguiente**.



En la siguiente pantalla seleccionamos la opcion **Solo los siguientes objetos en la carpeta**, y checamos **Objetos Equipo**, tambien checamos las otras dos opciones, **Crear los objetos**

seleccionados en esta carpeta y **Eliminar los objetos seleccionados en esta carpeta** y luego damos clic en **siguiente**.



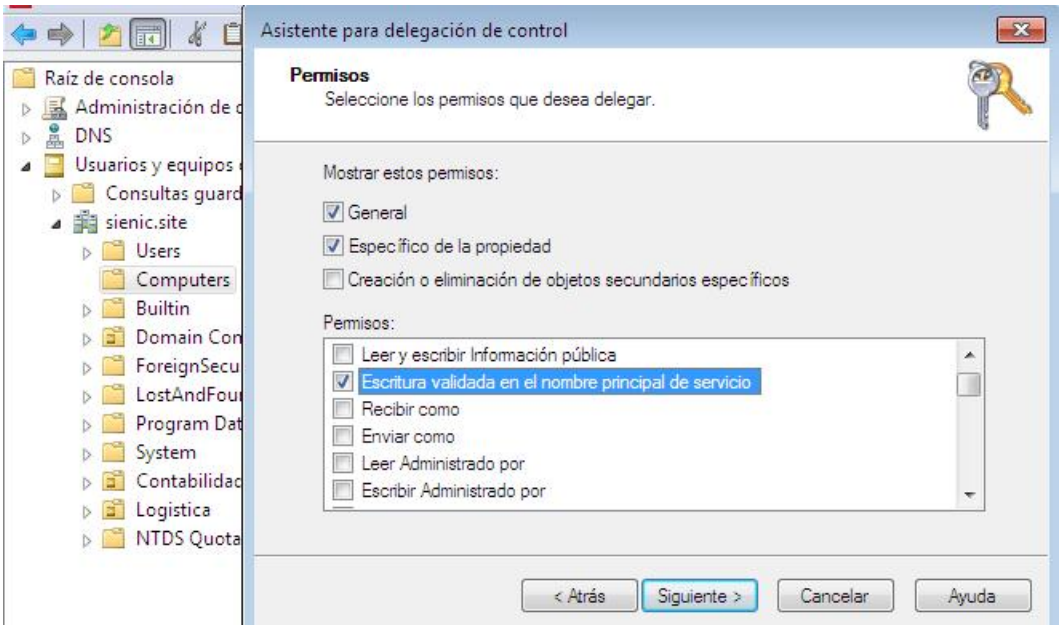
En la siguiente pantalla checamos las opciones **General** y **Especifico de la propiedad** y de la lista de opciones seleccionamos las siguientes opciones.

Lista en español:

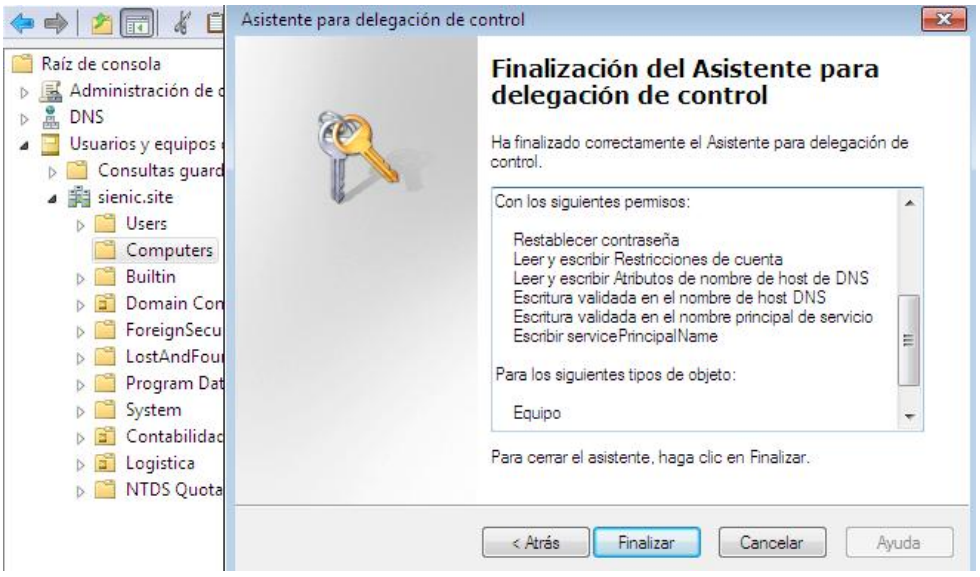
Restablecer contraseña
Leer y escribir restricciones de cuenta
Leer y escribir atributos de nombre de host de DNS
Escritura validada en el nombre de host DNS
Escritura validada en el nombre principal de servicio
Escribir servicePrincipalName

Lista en Ingles:

Reset password
Read and write account restrictions
Read and write DNS host name attributes
Validated write to DNS host name
Validated write to service principal name
Write servicePrincipalName



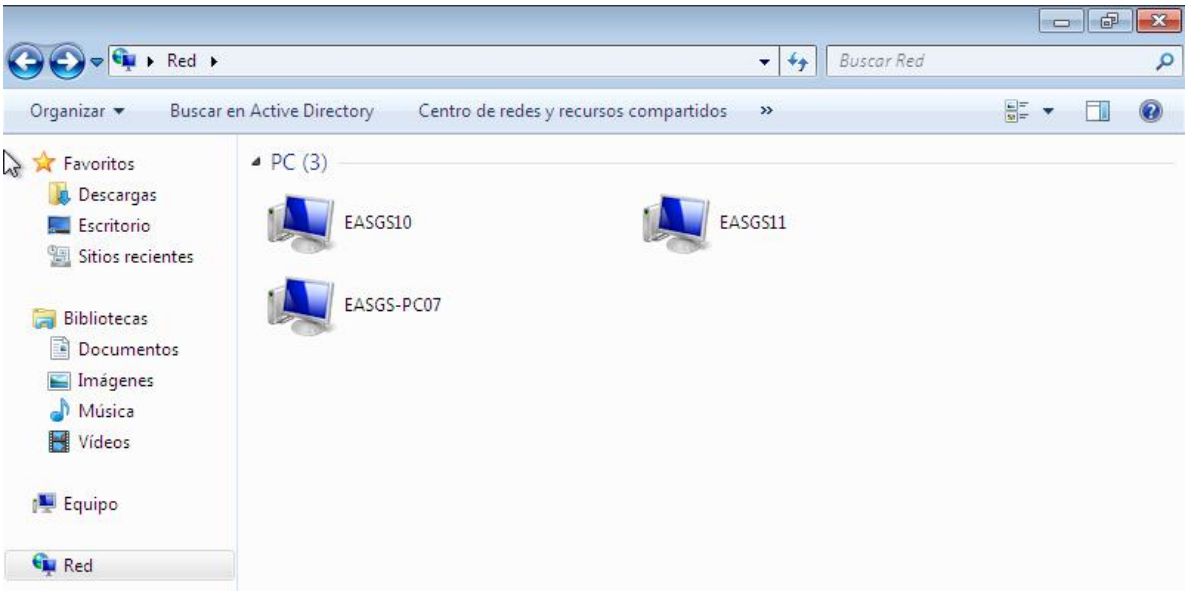
Damos clic en **siguiente** y se nos mostrara una pantalla con un resumen de lo que hemos configurado y damos clic en **finalizar**.



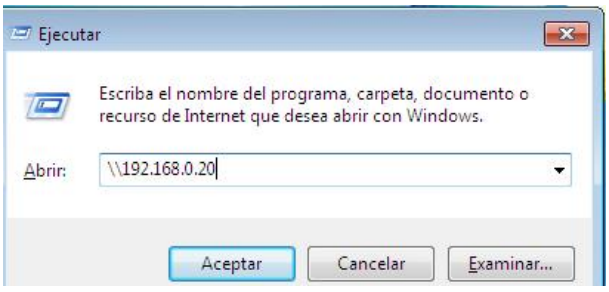
Entorno de red.

En cuanto al entorno de red, por el momento esperemos ver todos los equipos menos el servidor samba en el entorno de red, a como se muestra a continuacion el nombre del servidor de dominio samba es smb4server01

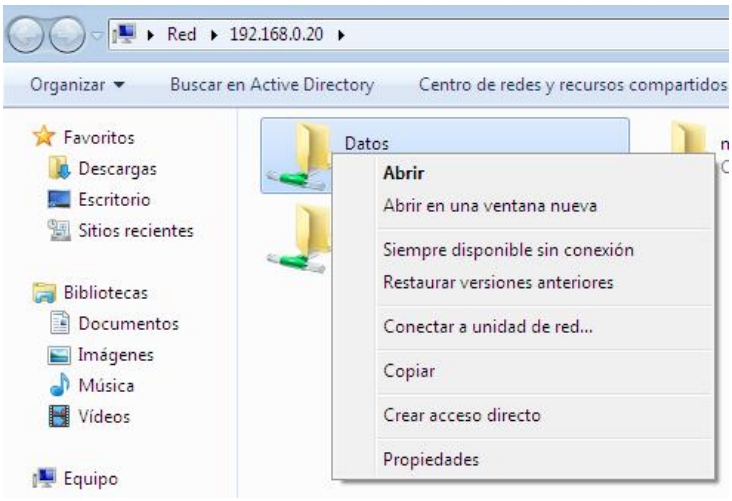
Pero en la siguiente imagen del entorno de red en una estacion con Windows 7 pro, podemos ver que todos los demas equipos se muestran menos el servidor de dominio samba.



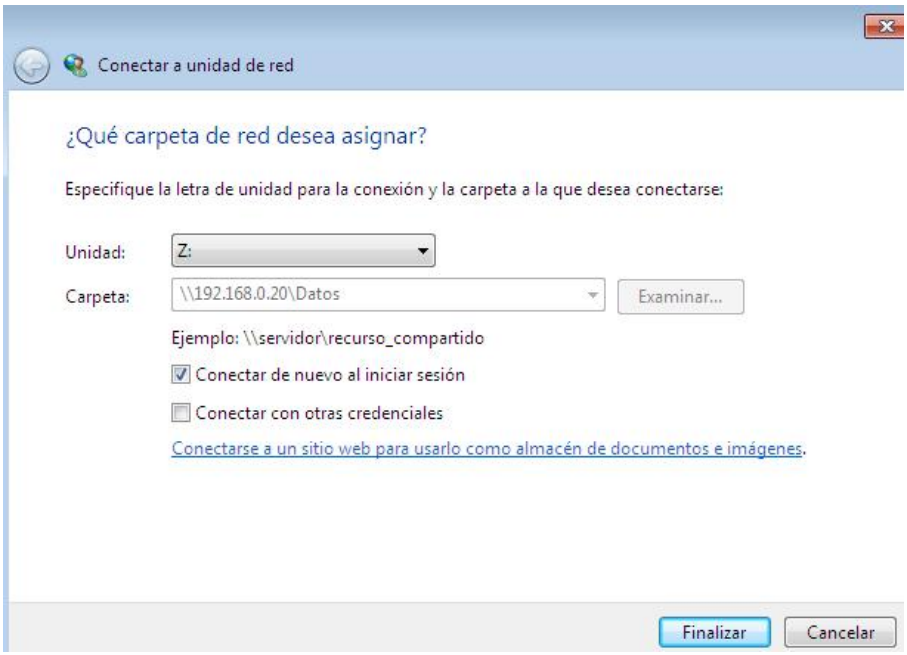
Esto significa que para acceder a un recurso compartido en el servidor deberemos introducir la direccion ip del servidor ya sea usando windows+R o en la barra de ubicación.



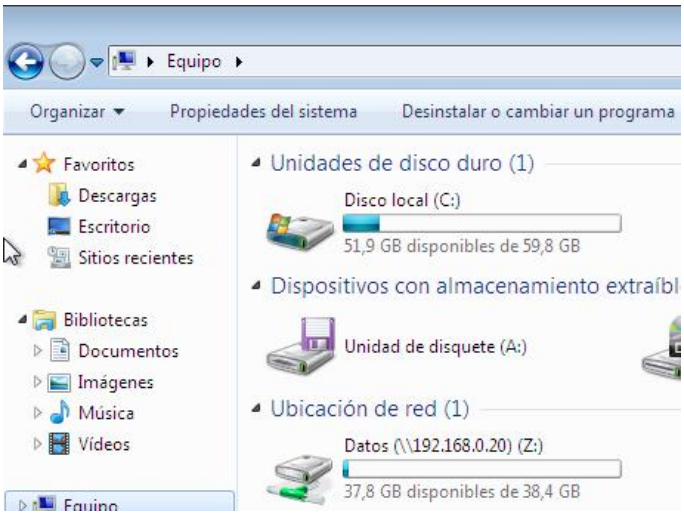
Si queremos que el recurso este disponible cada vez que arranque el equipo le damos clic con el boton secundario del mouse y seleccionamos **conectar a unidad de red.**



En la siguiente pantalla seleccionamos la letra de unidad que le queremos asignar y checamos Conectar de nuevo al iniciar sesion.



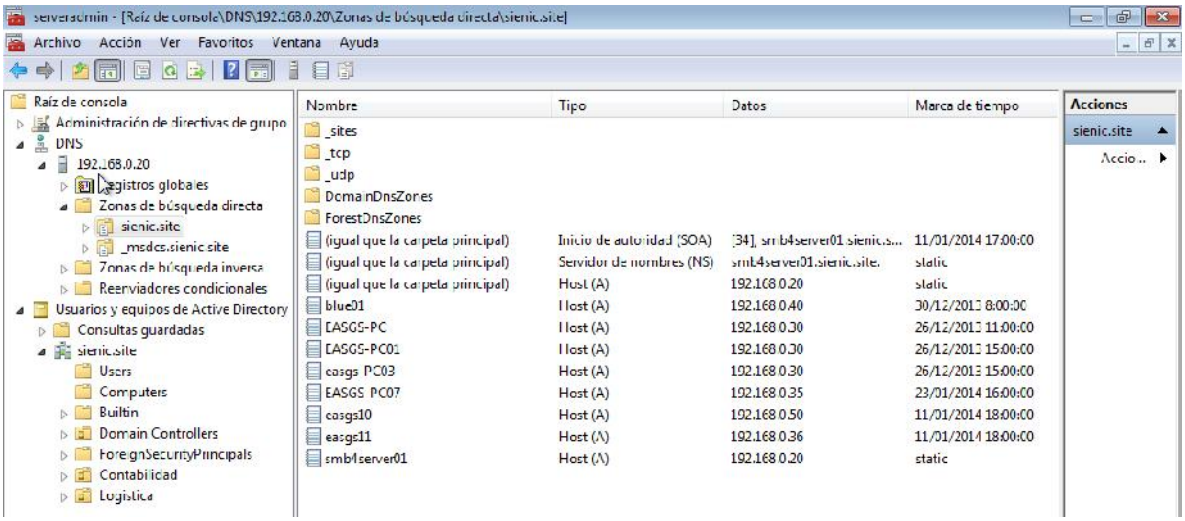
Ahora cada vez que queramos acceder a este recurso no vamos a equipo y damos doble clic sobre la letra de unidad que le asignamos al recurso compartido.



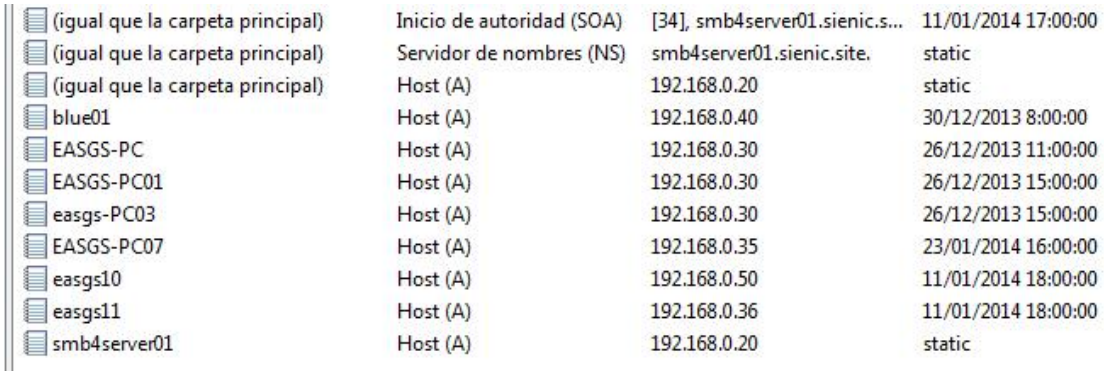
DNS

DNS

El servicio DNS es vital para el funcionamiento de Active Directory, por eso es importante conocer los tipos de registros que debemos manejar para su buen funcionamiento, bajo condiciones normales no deberiamos tener la necesidad de hacer algun tipo de tarea en el DNS ya que las actualizaciones las hace el servidor automaticamente cuando agregamos un equipo a la red, pero en el caso por ejemplo que tuvieramos que formatear una maquina o cambiarle el nombre deberemos borrar el registro en el DNS para mantener nuestro servidor lo mas ordenado posible, para entrar al DNS nos vamos a **DNS/IP_DEL_SERVIDOR/Zonas de busqueda directa/sienic.site**.

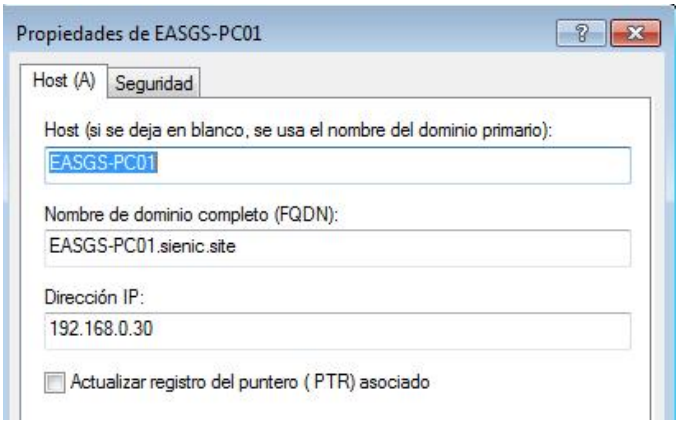


En esta ventana se nos muestran los diferente tipos de registros que tenemos en nuestro servidor DNS, un registro (A) para cada computadora de la red, estos registros estan asociados a la direccion IP de cada maquina, en este ejemplo podemos ver que hay varios registros (A) para una misma direccion IP, esto es debido a que se le a cambiado el nombre a la PC en varias ocaciones, este tipo de registros son los que debemos ir eliminando para que no causen confusion en el DNS, no es mandatorio y de hecho todo va a funcionar debidamente si no se hace, pero conforme pasa el tiempo la lista se puede ir haciendo mas grande de manera innecesaria, otro tipo de registro que tenemos es el servidor de nombre NS y la Inicio de Autoridad (SOA).

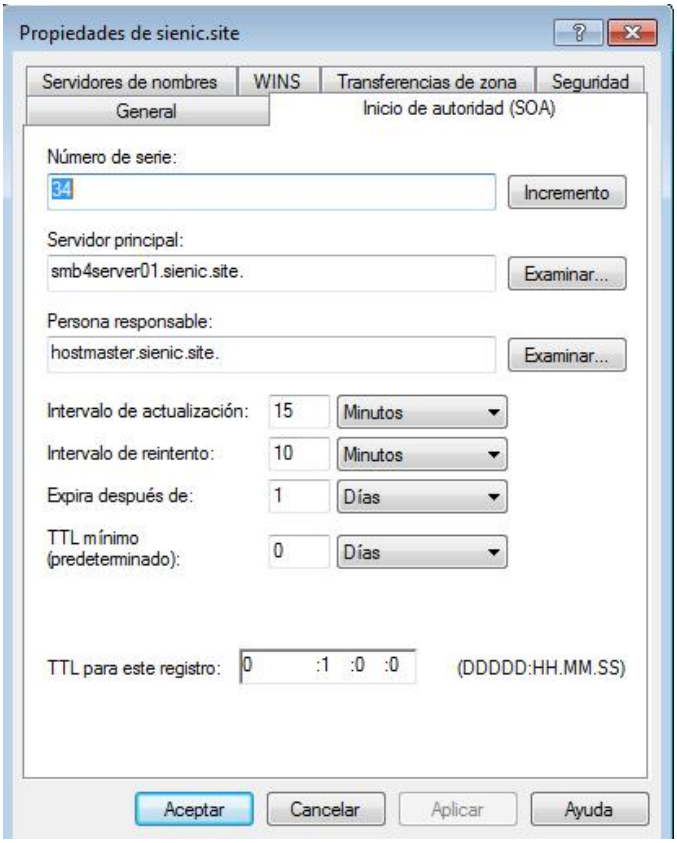


(igual que la carpeta principal)	Inicio de autoridad (SOA)	[34], smb4server01.sienic.s...	11/01/2014 17:00:00
(igual que la carpeta principal)	Servidor de nombres (NS)	smb4server01.sienic.site.	static
(igual que la carpeta principal)	Host (A)	192.168.0.20	static
blue01	Host (A)	192.168.0.40	30/12/2013 8:00:00
EASGS-PC	Host (A)	192.168.0.30	26/12/2013 11:00:00
EASGS-PC01	Host (A)	192.168.0.30	26/12/2013 15:00:00
easgs-PC03	Host (A)	192.168.0.30	26/12/2013 15:00:00
EASGS-PC07	Host (A)	192.168.0.35	23/01/2014 16:00:00
easgs10	Host (A)	192.168.0.50	11/01/2014 18:00:00
easgs11	Host (A)	192.168.0.36	11/01/2014 18:00:00
smb4server01	Host (A)	192.168.0.20	static

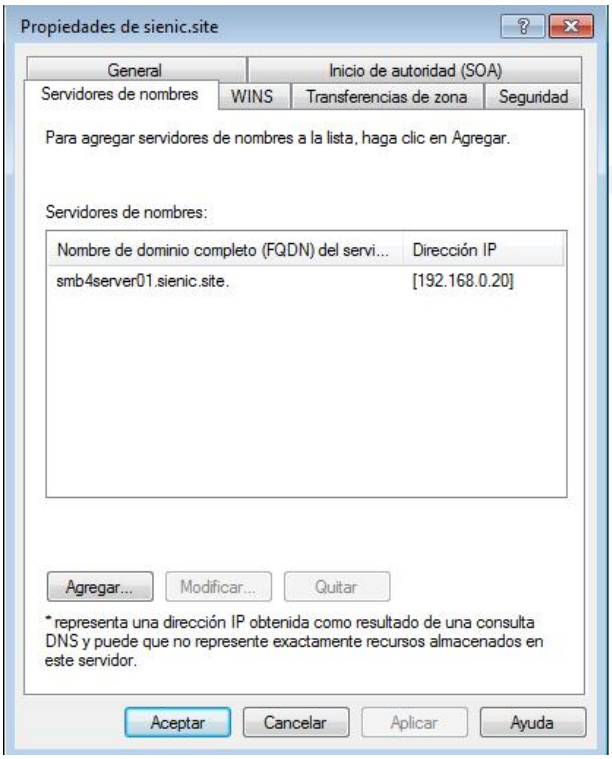
En la siguiente imagen podemos ver un registro (A) en detalle, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando **propiedades**, este registro es de una computadora con el hosname EASGS-PC01, generalmente este registro se crea automaticamente al unir la maquina al dominio.



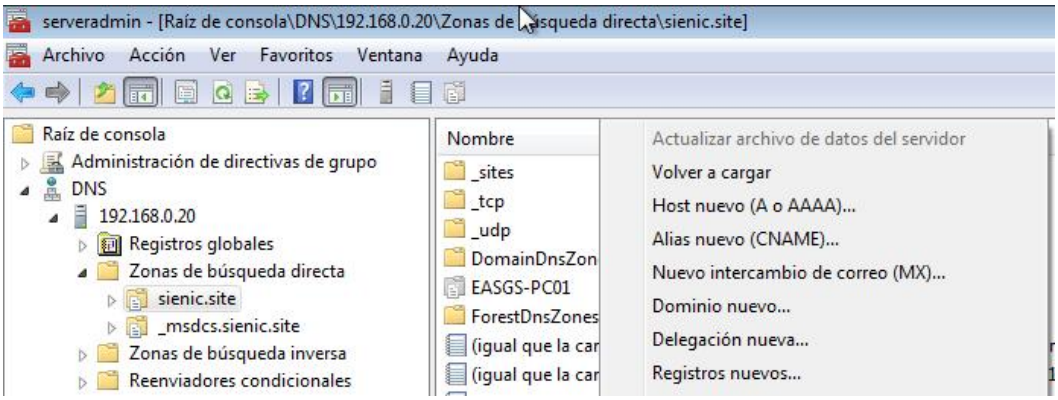
En la siguiente imagen vemos con detalle el registro (SOA) que contiene informacion acerca de la zona DNS, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando propiedades.



En la siguiente imagen se muestra informacion detallada del registro NS, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando propiedades.

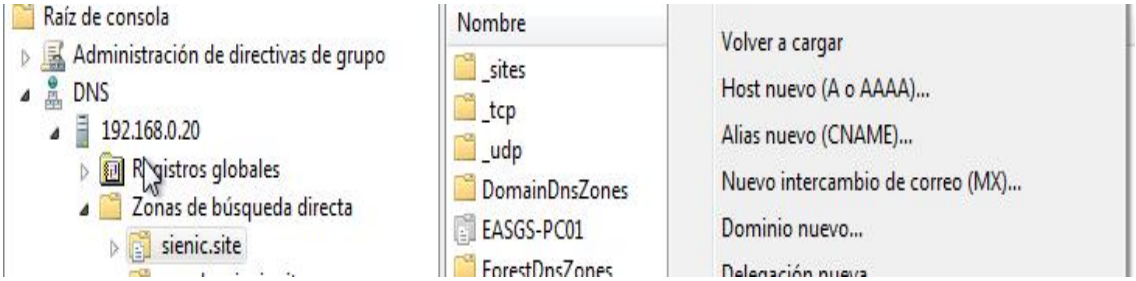


Al hacer clic con el boton secundario del mouse sobre la zona se mostrara un meno desplegable que nos da la opcion de agregar Registro A, CNAME y MX, los registro MX son para los servidores de correo electronico.

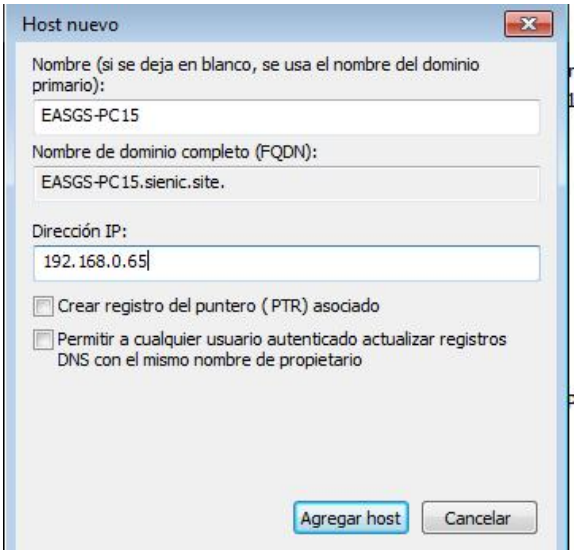


Agregando un registro (A)

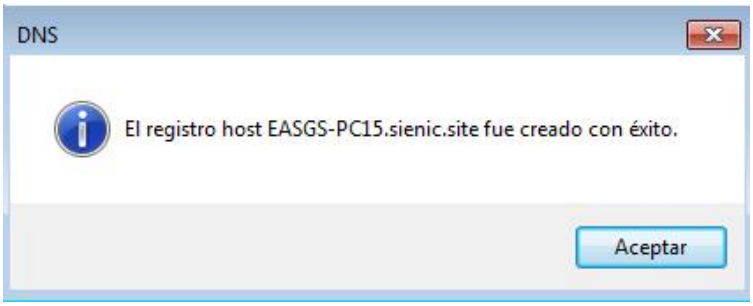
Para agregar un nuevo registro (A) damos clic con el boton secundario del mouse sobre la zona seleccionamos la opcion **Host nuevo (A o AAA)**.



En la siguiente ventana ponemos el nombre de la PC en el campo **Nombre**, en **Direccion IP** ponemos la direccion IP que tiene la maquina y damos clic en **Agregar Host**



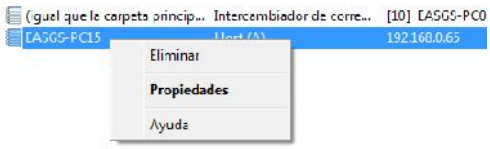
Nos aparecera un cuadro de dialogo como el siguiente, damos clic en **aceptar**.



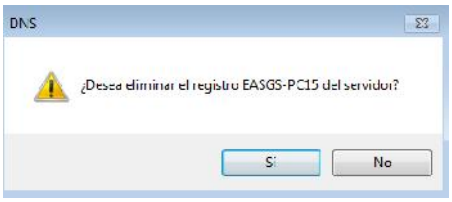
Nota: Los registros A se crean automaticamente cuando se une un PC al dominio.

Eliminar un registro (A)

Para eliminar un registro (A) seleccionamos el registro y le damos clic con el boton secundario del mouse, luego seleccionamos **Eliminar**

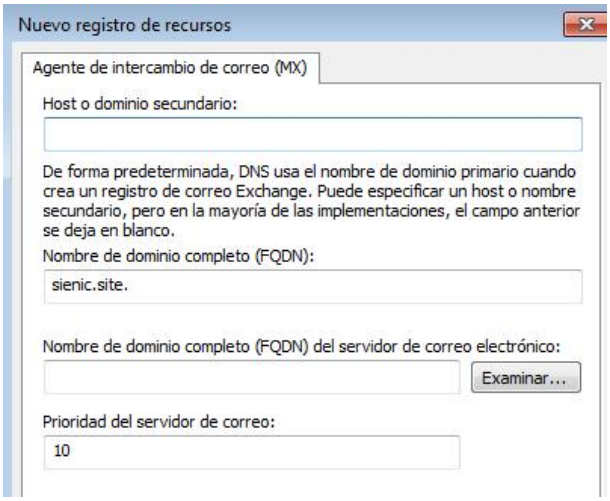


En el siguiente cuadro de dialogo damos clic en **Si**

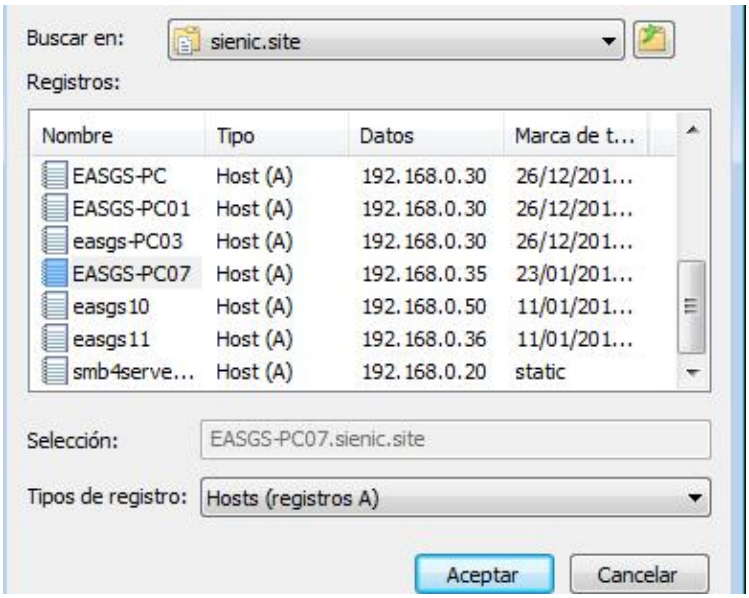


Agregando un registro (MX)

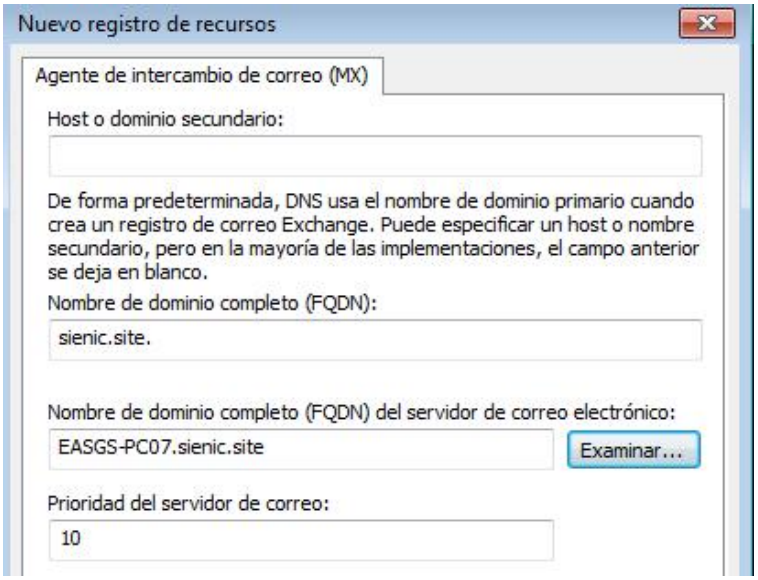
Para agregar un registro MX primero debemos crear el registro (A) luego seleccionamos **Nuevo intercambio de correo (MX)** del menu desplegable, se mostrara un cuadro de dialogo como el que se muestra a continuacion, en este cuadro damos clic en **examinar** y buscamos el registro (A) del servidor que sera el encargado de manejar el correo.



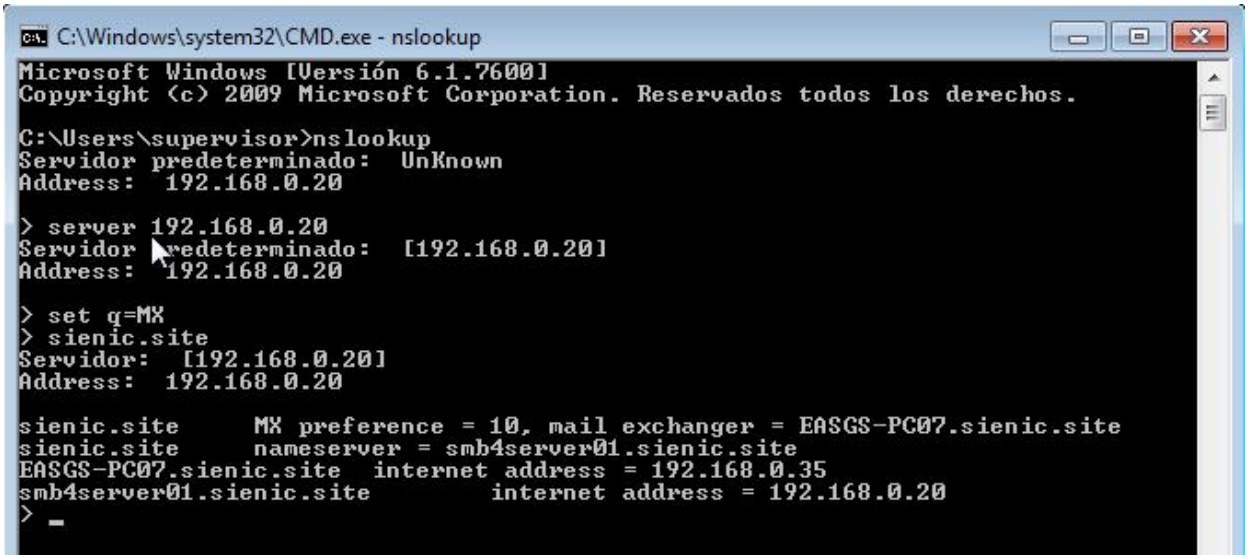
Una vez encontrado el registro (A) damos clic en **aceptar**



Luego ponemos la **prioridad** que tendra el servidor de correo y damos clic en **aceptar**, con eso ya tenemos nuestro registro (MX)



En la siguiente pantalla utilizamos nslookup para verificar que el registro MX este correcto.



DHCP

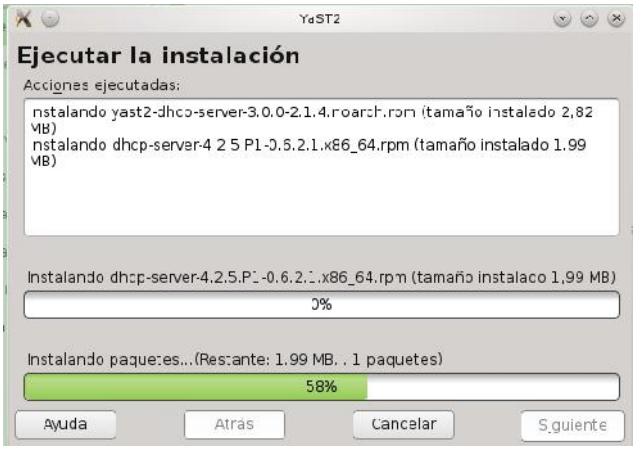
Instalacion y configuracion del DHCP

El servicio DHCP nos permite brindar direcciones IP de manera automatica asi como tambien otros parametros a las estaciones de trabajo ahorrandonos asi la tarea de estar configurando cada PC de la red de manera manual, para configurar el servicio DHCP nos vamos a **Yast/Software/Instalar / desinstalar software**.

Damos clic en **Ver** y seleccionamos la opcion **Patrones**

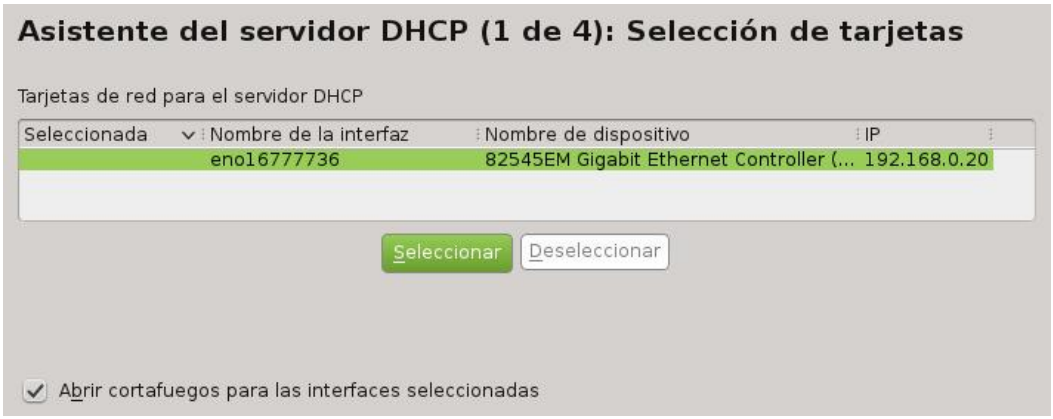
En patrones seleccionamos **Servidor DHCP y DNS** y en el panel derecho seleccionamos los paquetes **dhcp-server** y **yast2-dhcp-server.**

Se mostrara una ventana msotrando el progreso de la instalacion.



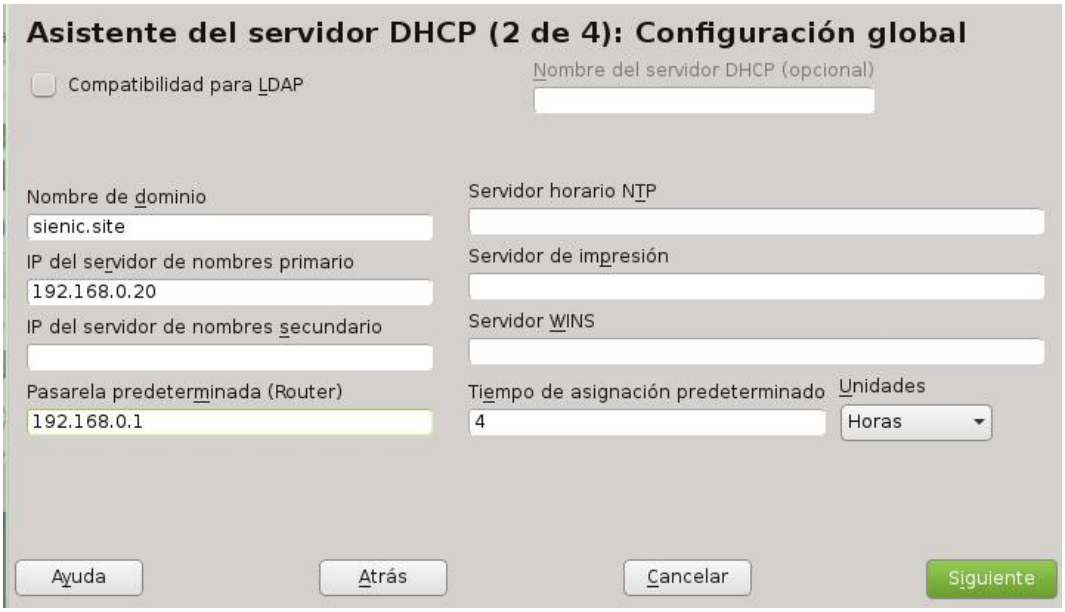
Una vez instalados los paquetes nos vamos a **Yast/Servicios de red/Servidor DHCP**

En la siguiente ventana seleccionamos la interface por medio de la cual vamos a asignar las direcciones IP y damos clic en **Seleccionar** y checamos la opcion **Abrir cortafuegos para las interfaces seleccionadas.**



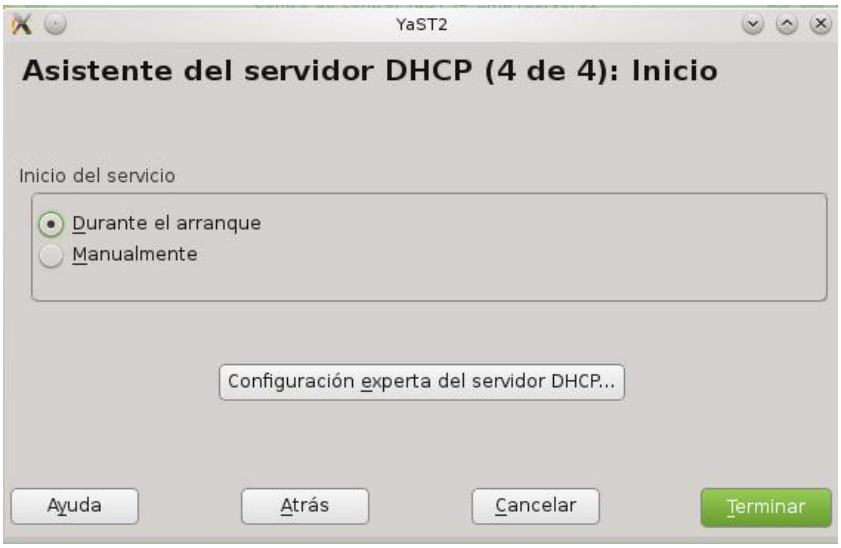
Damos clic en **siguiente**.

En la siguiente ventana ponemos las opciones tal a como se muestran en la siguiente figura y damos clic en **siguiente**, adaptando las opciones a sus necesidades.

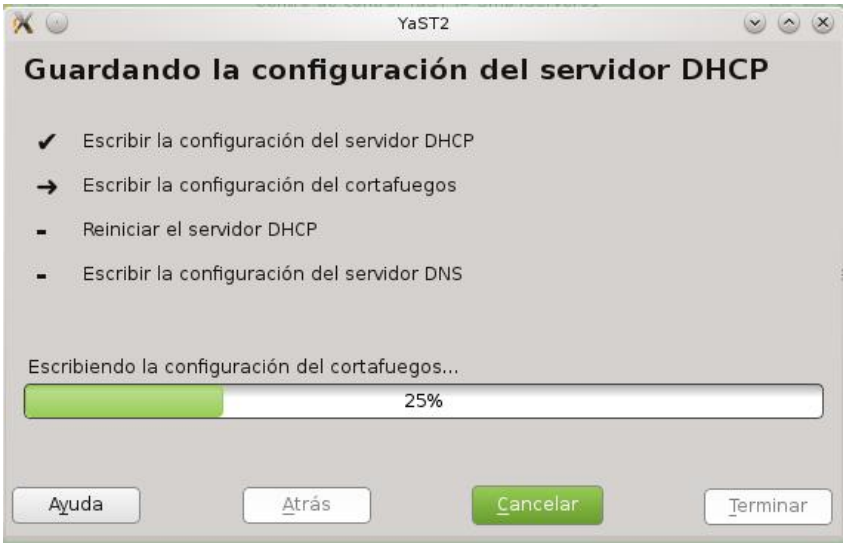


En esta ventana se configura el ambito de direcciones IP que asignara este servidor, ponemos la **Primera direccion IP** y la **Ultima direccion IP** del rango que deseamos configurar y damos clic en siguente.

En la siguiente ventana configuramos el servicio para que arranque junto con el sistema operativo y damos clic en **terminar**.

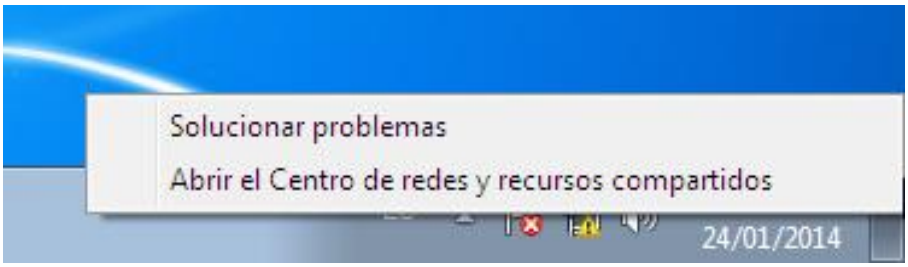


Se mostrara una ventana con el progreso de las configuraciones.

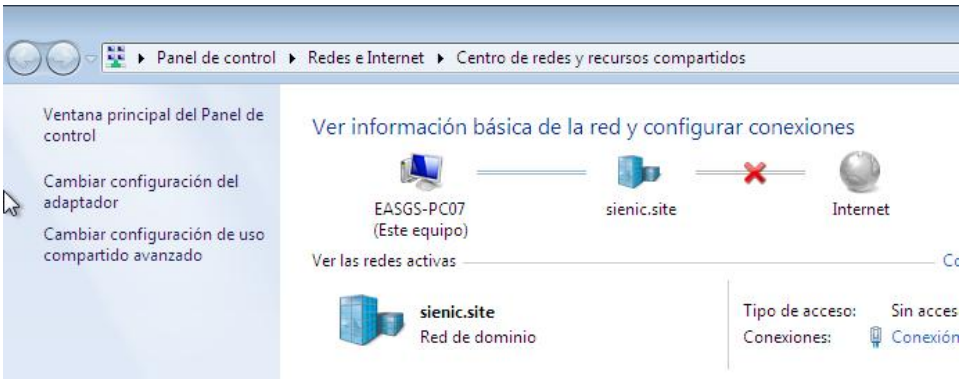


Configurar las estaciones de trabajo como clientes DHCP.

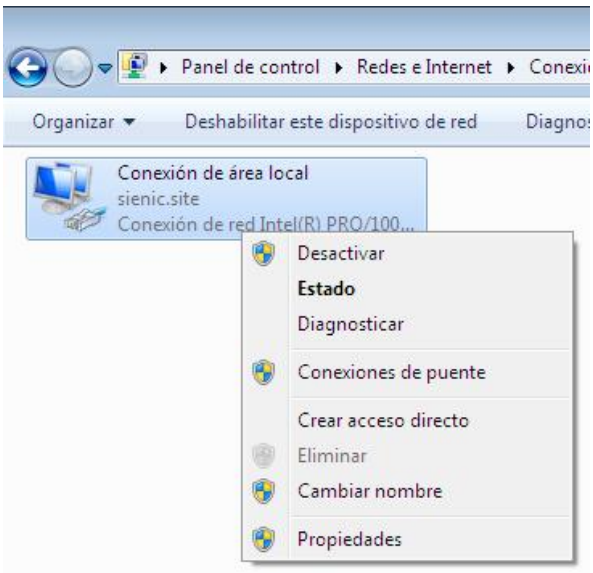
El siguiente paso es configurar las estaciones de trabajo para que hagan uso del servidor DHCP, para esto damos clic con el boton secundario del mouse sobre el icono de red y seleccionamos **Abrir el Centro de redes y recursos compartidos**.



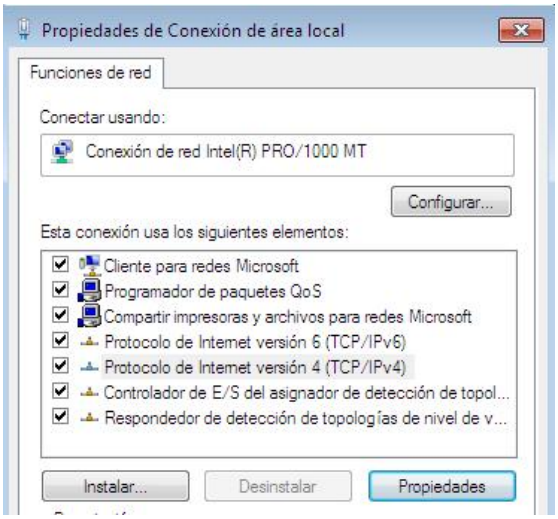
En la siguiente ventana hacemos clic en la opcion **Cambiar configuracion del adaptador**.



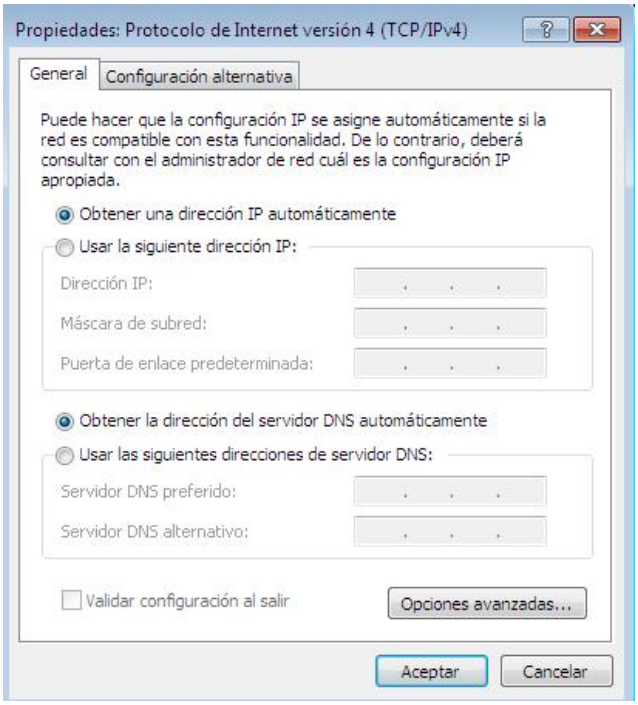
Seleccionamos la conexión que deseamos configurar y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades** del menu desplegable.



Luego seleccionamos **Protocolo de Internet version 4 (TCP/IPv4)** y damos clic en **propiedades.**



El la siguiente ventana seleccionamos las opciones **Obtener una direccion IP automaticamente** y **Obtener la direccion del servidor DNS automaticamente.**

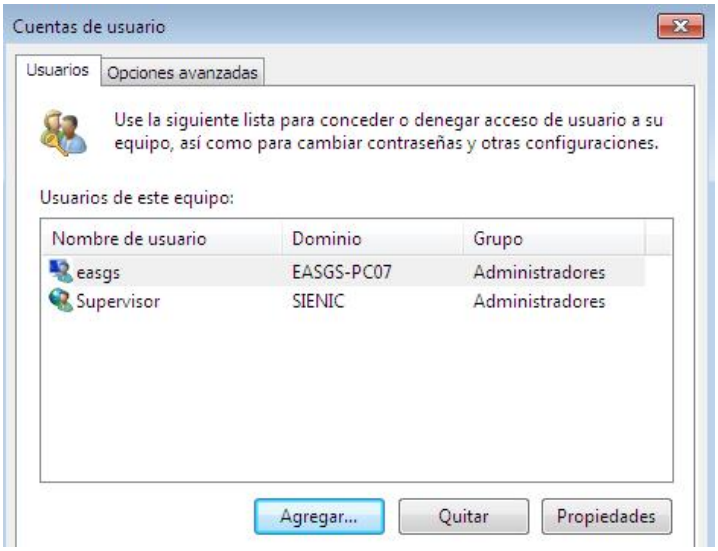


Permisos locales

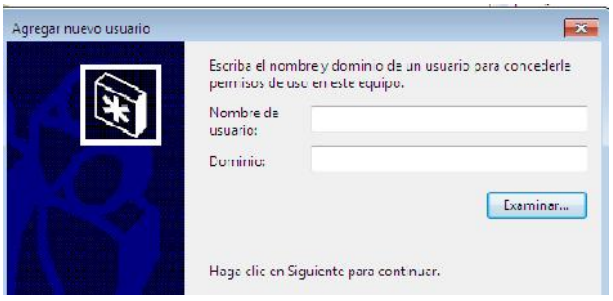
Permisos locales

En algunas ocaciones necesitamos que un usuario tenga permisos locales administrativos en la estacion de trabajo, esto debido a alguna aplicación que asi lo requiera o por cualquier otro motivo, el problema es que si el usuario no pertenece al grupo Domain Admins su sesion se iniciara con permisos limitados, el problema es que no podemos andar agregando usuarios al grupo de Domain Admins, para resolver este problema vamos a configurar permisos locales con la cuenta de dominio del usuario.

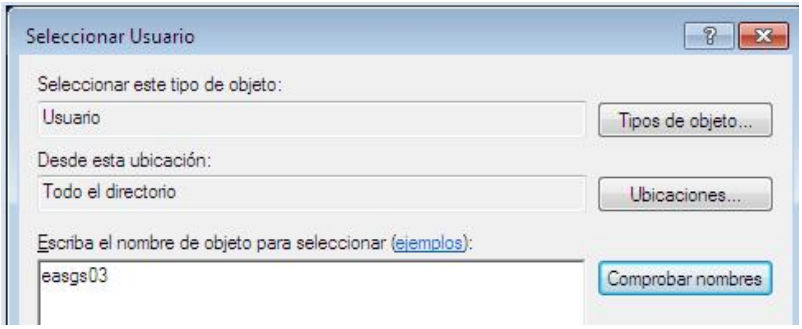
Para configurar los permisos locales con la cuenta de dominio nos vamos a **Panel de control/Cuentas de usuario/Cuentas de usuario/Administrar cuentas de usuario** y damos clic en **agregar**.



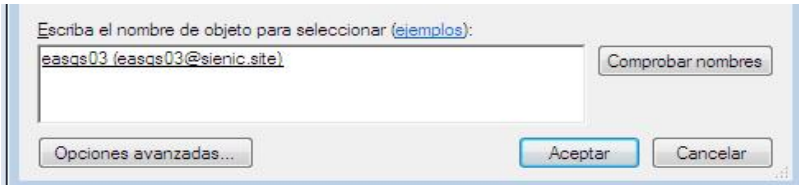
En la siguiente ventana damos clic en el icono **Examinar**.



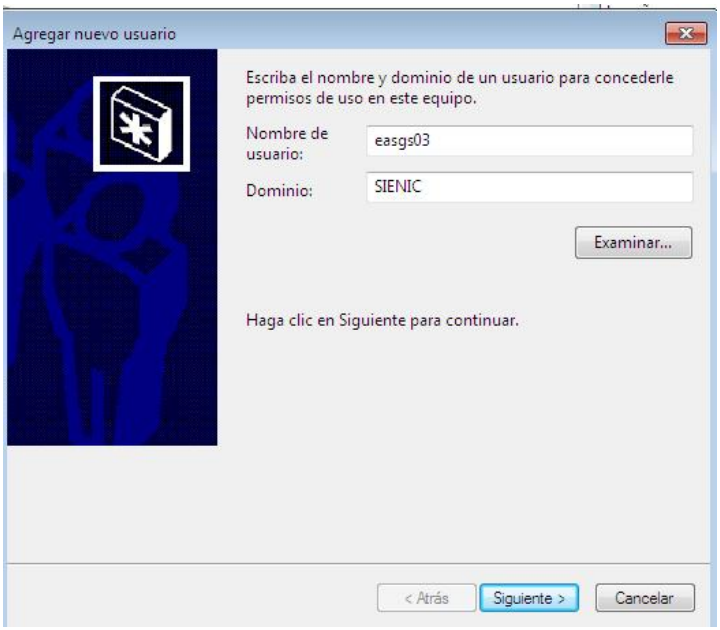
Escribimos el nombre de la cuenta de usuario de dominio y damos clic en **Comprobar nombres**.



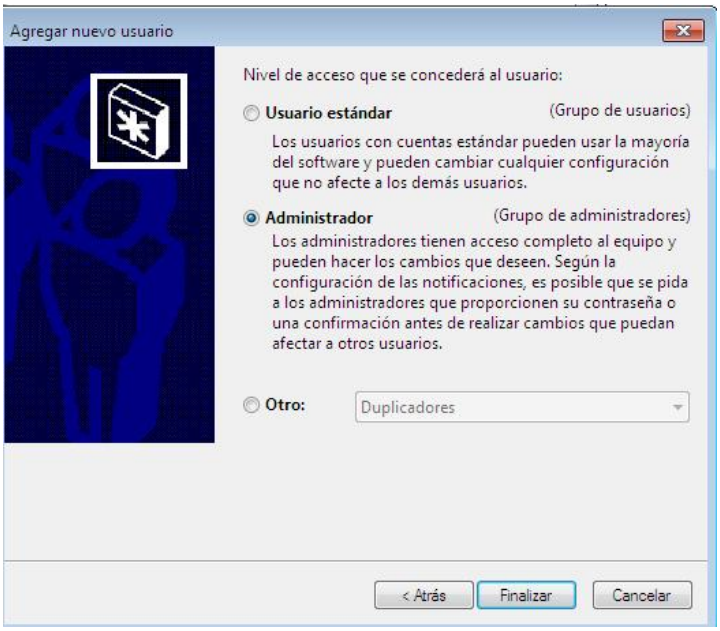
Una vez comprobado el nombre damos clic en A**ceptar**.



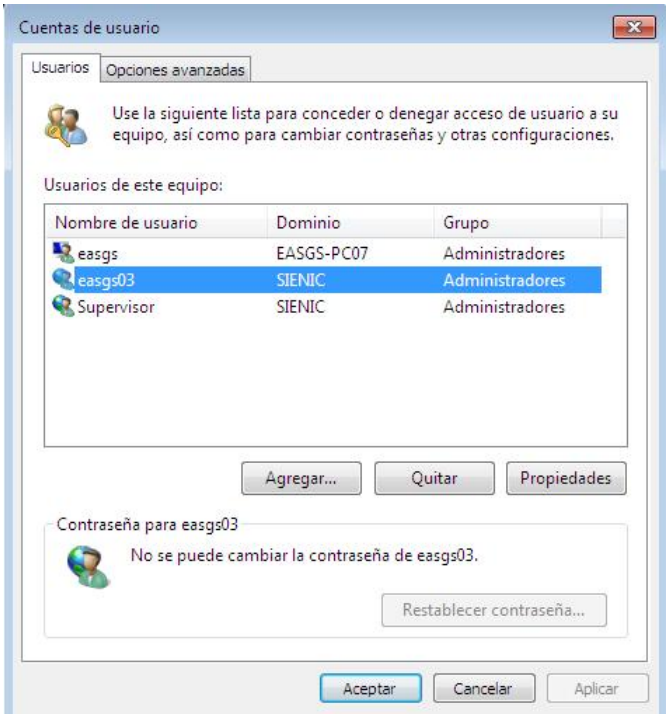
En la siguiente ventana nos mostrara el nombre de usuario y automaticamente el dominio, damos clic en **Siguiente.**



En esta ventana vamos a seleccionar el nivel de permisos locales que va a tener el usuario, seleccionamos **Administrador** si damos clic en **Otro** y abrimos la lista deplegable se nos mostraran mas opciones, una vez hecha nuestra selección damos clic en finalizar.



En la siguiente ventana se muestra el usuario ya agregado a la lista de usuarios, podemos ver que este es miembro del grupo local de la estacion de trabajo Administradores, damos clic en **Aceptar**.



Ahora este usuario tendra permisos de administrador local en esta estacion de trabajo, por lo que si una aplicación tiene este requierimiento funcionara sin problema, sera responsabilidad del administrador del dominio implementar las politicas de seguridad o GPO necesarias para limitar el acceso de este usuario a las unidades del sistema, panel de control , conexiones de red etc.

Creditos

Este manual no hubiera sido posible sin la información contenida en los siguientes sitios, ni la ayuda brindada por los autores y participantes:

https://lists.samba.org/

http://wiki.samba.org/index.php/Samba

http://easgs.wordpress.com/2009/11/23/opensuse-11-2-con-samba-guia-ilustrada/

http://conradjonesit.wordpress.com

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection

http://forums.opensuse.org

La portada gracias a:
Daniel Salazar
ADNX

Para comentarios y preguntas contactar al autor:
Eduardo Adolfo Sotomayor G.
adolfo2007@starlinux.net
http://easgs.wordpress.com