ACTIVE DIRECTORY: IDENTIFICACIÓN Y ACCESO A LOS OBJETOS - POLÍTICAS DE GRUPO

1 OBJETIVO

El objetivo de la esta clase es presentar las características de Active Directory y la forma en que nombra y administra los objetos dentro de su estructura, para ello veremos las herramientas especializadas con que cuenta para poder administrar el acceso a estos y las políticas de grupo.

Al finalizar la clase el alumno podrá:

- ✓ Comprender la forma en que se identifican los distintos tipos de objetos y los grados de seguridad que pueden manejar.
- ✓ Diferenciar los permisos de los derechos, como y donde se aplican.
- ✓ Para que sirven las políticas y en que ámbitos se utilizan.
- ✓ Cual es la relación entre las Políticas y Equipos, Sitios, Dominios y Unidades Organizativas.
- ✓ Aprenderá a implementar políticas mediante la herramienta GPE

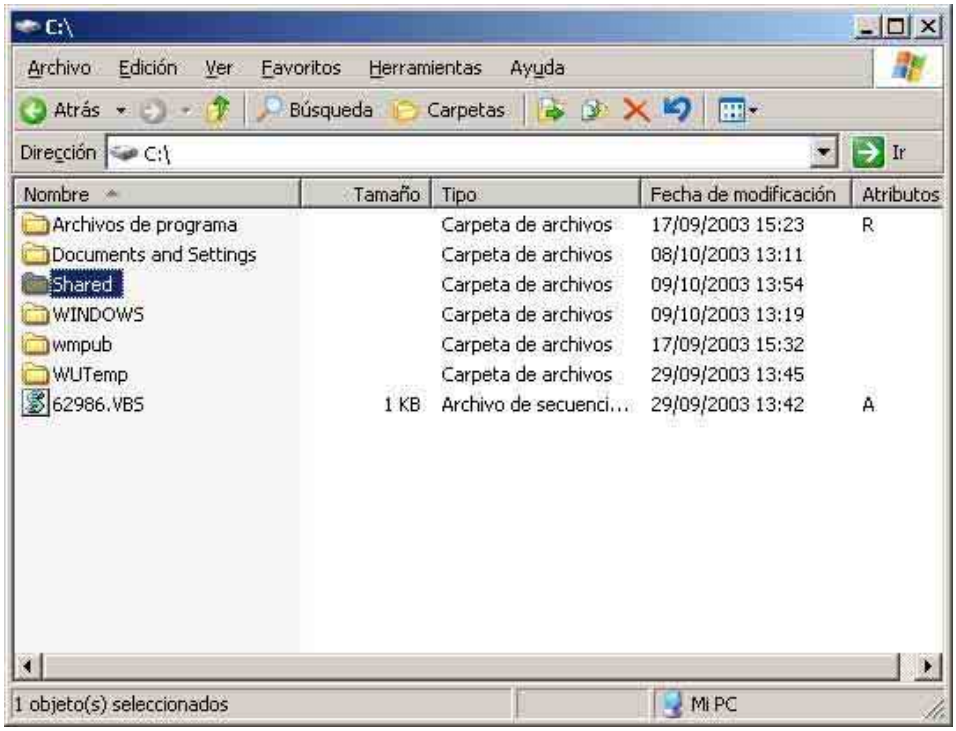
2 PERMISOS Y DERECHOS.

A modo de definición, podemos afirmar que un permiso es una regla asociada a un objeto para regular a los usuarios que pueden tener acceso al mismo y especificar de qué forma tendrán tal acceso. O sea un permiso es la facultad que un Administrador puede dar a un usuario o grupo, sobre un recurso tanto local como de red. Esto implica la posibilidad de usar, cambiar, leer, borrar o cualquier acción que pueda realizarse sobre el recurso. Un derecho tiene campo de acción a nivel dominio y refiere a acciones realizables dentro del mismo. Por ejemplo, tener derecho para iniciar sesión en un servidor y, por ende, los derechos que se tendrá sobre ese servidor.

2.1 CLASES DE PERMISOS.

Cuando hablamos de permisos, estos pueden ser analizados desde dos ángulos diferentes: Una cosa son los permisos que se pueden otorgar sobre un objeto, cuando este es un recurso compartido en la red y otra, son los permisos que un sistema de archivos que maneje seguridad (tal como NTFS) puede definir sobre un recurso.

Sobre un equipo con Windows XP instalado sobre un sistema de archivos NTFS, tomemos el ejemplo de una carpeta llamada Shared ubicada en el disco C. Si hacemos clic con el botón secundario sobre ella y seleccionamos Propiedades Podremos observar en pantalla una ventana con las propiedades de la carpeta.



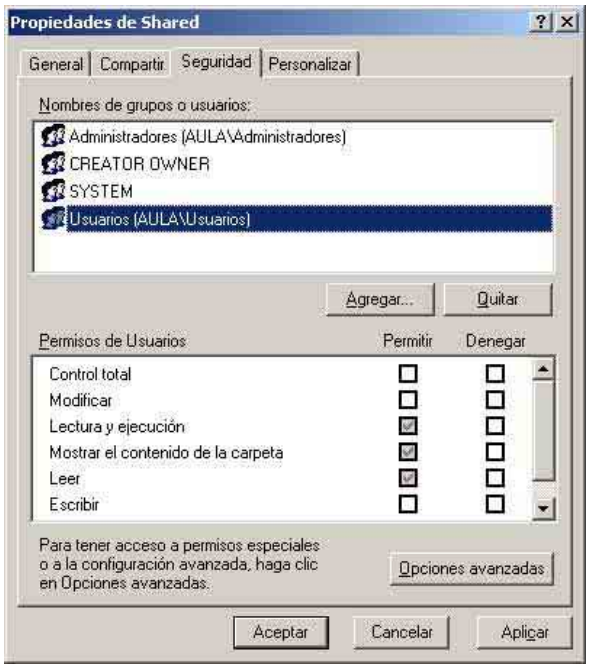
Dentro de esta podemos ver que existen diferentes lengüetas, optaremos por la que dice Compartir.

Esta solapa refiere a los permisos sobre este recurso a nivel de la red. Dentro de ella vemos que existe un campo con el nombre que tiene el recurso compartido, el cual será visto por los demás usuarios de la red. Presionaremos ahora sobre el botón Permisos.

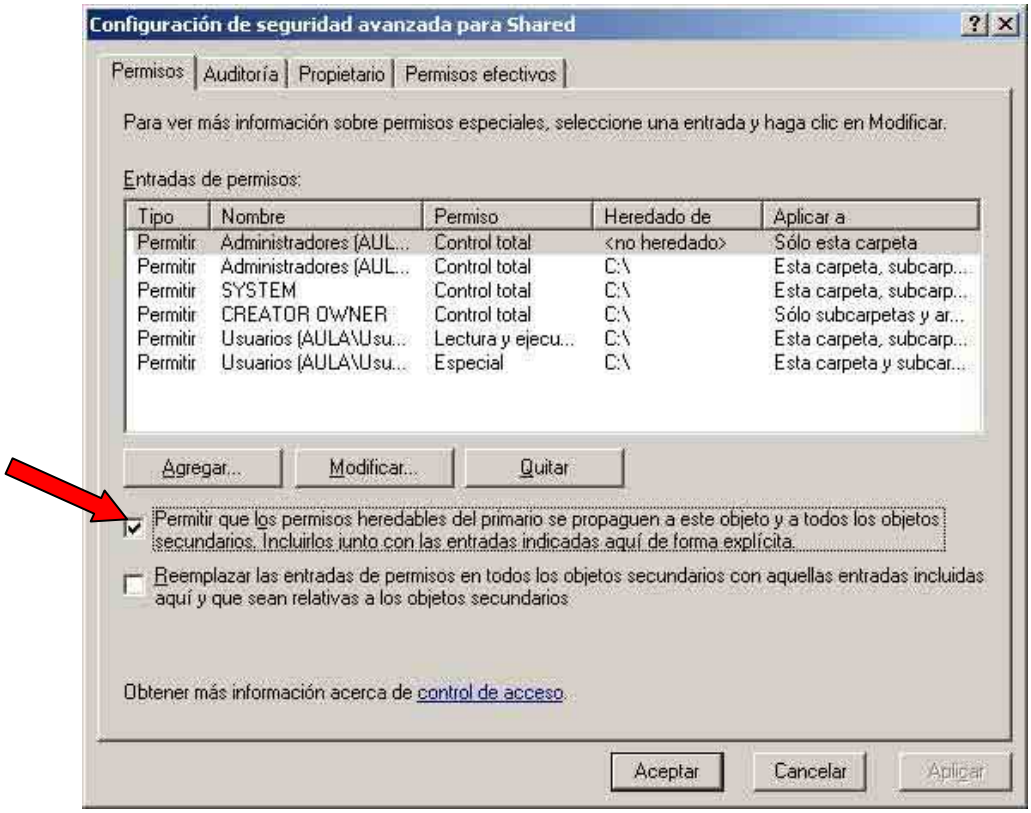
Accederemos a una nueva ventana en la que podemos visualizar los nombres de los usuarios o grupos y sus correspondientes permisos a nivel de red. Entonces y según lo que vemos en el cuadro, el grupo Todos tendrá acceso de solo lectura sobre este recurso, cuando sus miembros accedan a él a través de la red.

Si cancelamos esta ventana y entramos a la lengüeta Seguridad podremos administrar los permisos pero esta vez a nivel del sistema de archivos. Tal como vemos en la figura siguiente hay grupos como el de Administradores, que tienen permisos heredados sobre el recurso (nótese que los recuadros están grisados indicándonos esa propiedad), esto quiere decir que este objeto hereda los permisos que tiene la carpeta, unidad o recurso principal en donde se está creando este nuevo objeto. En este caso esta carpeta “hereda” los permisos que tenía el grupo Administradores sobre el directorio raíz C:.

Si seleccionamos el Grupo Usuarios, podemos ver que trae heredados varios permisos (en color grisado). Si queremos deshabilitar la herencia y asignar nuevos permisos manualmente, debemos ingresar a Opciones Avanzadas.



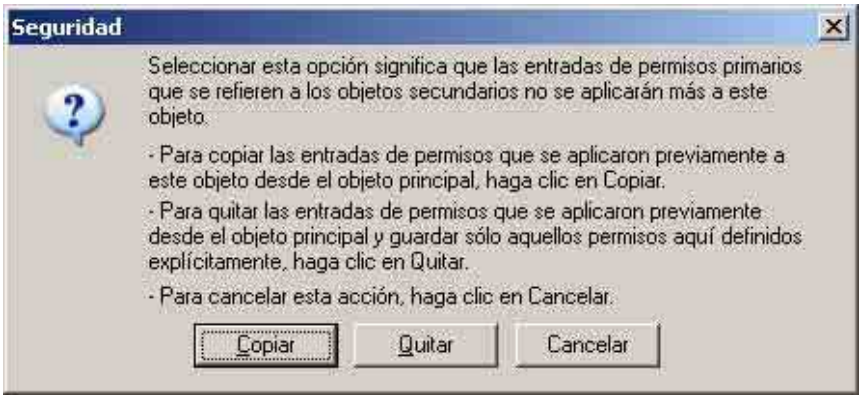
Una vez aquí, será necesario quitar la tilde a la opción Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios…



Al realizar esta tarea, veremos que aparecerá una ventana de advertencia informándonos sobre las implicancias que esto puede acarrear. Vale la pena aclarar que al efectuar esto estamos estableciendo un punto de quiebre, por lo tanto todas las modificaciones a los permisos que se realicen a partir de acá, tendrán efecto hereditario sobre todas las carpetas y subcarpetas que se creen dentro de *Shared*.

Leyendo vemos que nos da una serie de opciones. La primera permitirá que los permisos heredados ya existentes se copien, por lo tanto solo se quitará el grisado sobre los casilleros permitiéndonos luego modificar tales permisos. La segunda opción quitará todos los permisos existentes, por lo tanto empezaremos de cero y deberemos volver a incluir los grupos y usuarios que tendrán acceso al recurso y a reasignar los permisos correspondientes. Por último tenemos la opción de cancelar la operación sin modificar nada.

Optaremos por la opción copiar, por lo que los permisos heredados quedarán tildados.



En la pantalla observamos que al grupo *Usuarios* le quedaron asignados ciertos permisos, pero ya no grisados, por lo tanto podemos modificarlos a nuestra voluntad.

A partir de ahora todo objeto creado dentro de la carpeta Shared, tendrá como permisos heredado los que asignemos desde este lugar.

2.2 JERARQUÍAS ENTRE PERMISOS

2.2.1 Permisos de usuario

Tomemos el ejemplo de un usuario y los permisos que se le pueden asignar tanto a nivel del sistema de archivos (S.A.) mediante la lengüeta Seguridad, como a nivel red mediante la solapa Compartir. En cuadro podemos observar las diferentes combinaciones que pueden surgir y el resultado que realmente será aplicado como permiso cuando el usuario desee acceder a la carpeta.

Tipo de Permiso		Permiso aplicado
Nivel red	Nivel S.A.	
solo lectura	control total	solo lectura
control total	solo lectura	solo lectura
denegación	control total	denegación
control total	denegación	denegación

Como vemos, siempre los permisos más restrictivos tienen mayor peso que los más permisivos, a excepción de la denegación que es la restricción de mayor jerarquía y que está por encima de cualquier permiso.

2.2.2 Permisos de grupo

Analicemos ahora el caso de un usuario que pertenece a dos grupos diferentes y veamos con ayuda de la figura que posibilidades pueden darse y que resultantes obtendremos.

Tipo de Permiso		Permiso aplicado
Grupo 1	Grupo 2	
solo lectura	control total	control total
control total	solo lectura	control total
denegación	control total	denegación
control total	denegación	denegación

Como podemos observar cuando se tiene un usuario que pertenece a dos grupos diferentes que poseen permisos de diferente jerarquía, predomina siempre el mas "permisivo". Pero observemos que aquí también tenemos que siempre la denegación tendrá preponderancia por sobre cualquier otro permiso asignado.

Es válido recordar que si enfrentamos estos permisos de grupos entre los niveles de red y de sistema de archivos, obtendremos nuevamente el resultado que muestra la primera figura de permisos.

2.2.3 Permisos Heredados y permisos explícitos.

Recordando el tema de la herencia que tratamos anteriormente es relevante aclarar que cuando un usuario o grupo hereda ciertos permisos sobre un recurso, pero a su vez sobre este mismo recurso se han declarado permisos explícitos, estos últimos serán los de mayor peso.

Por lo tanto podemos concluir que un permiso explícito, posee mayor jerarquía que cualquier permiso heredado, por lo tanto lo explícito será lo tomado como permiso efectivo por sobre lo heredado.

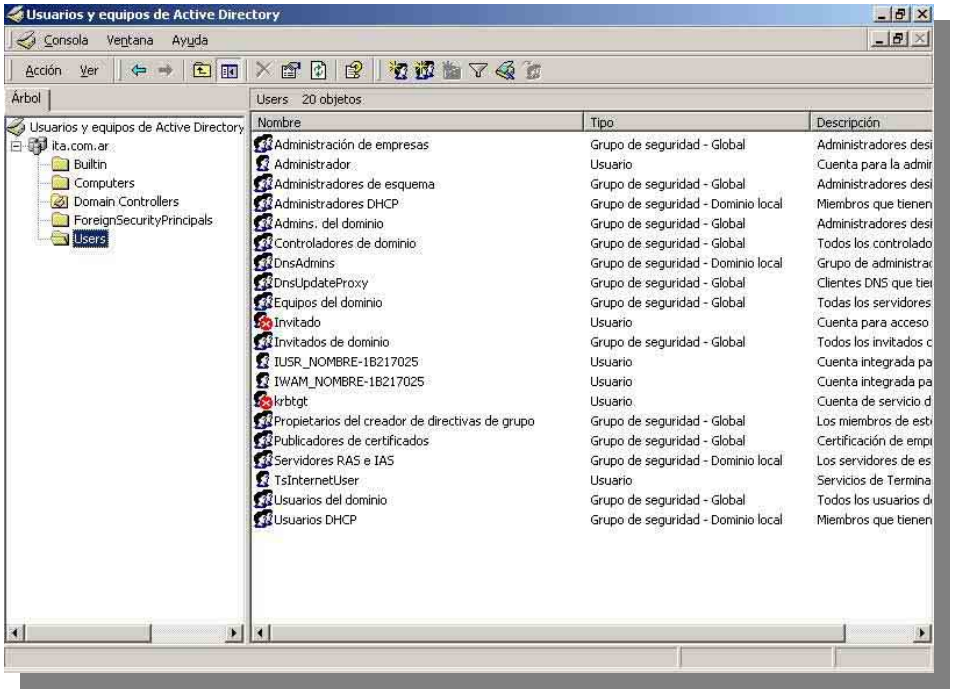
3 CREACION DE GRUPOS Y USUARIOS

3.1 CREACIÓN DE GRUPOS.

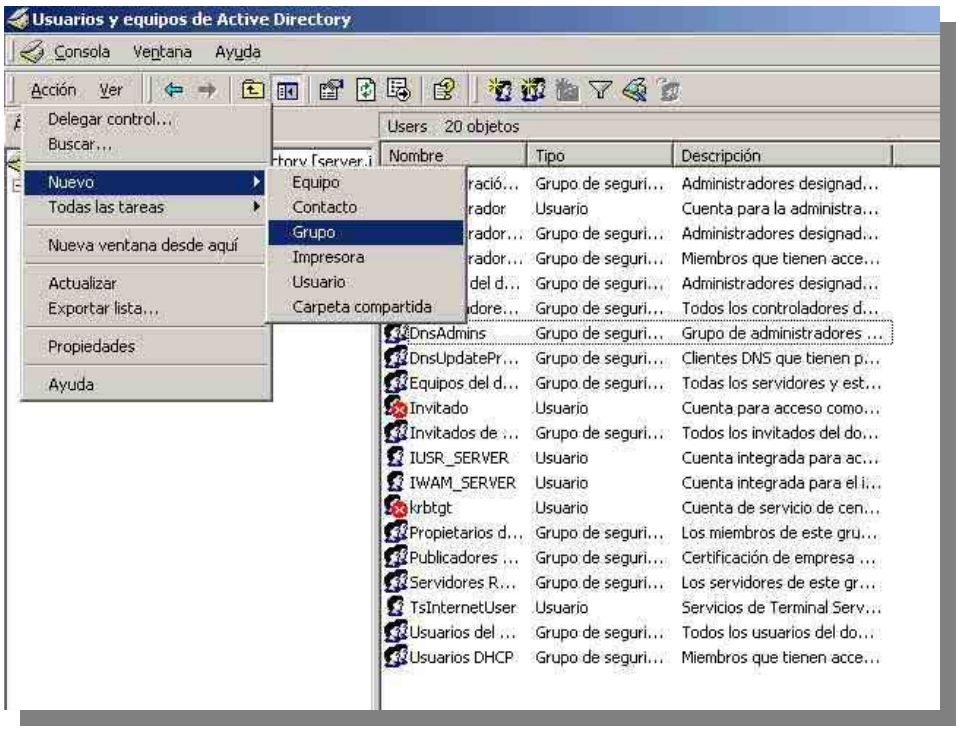
Una vez que hemos definido el tipo de grupos y usuarios que deseamos crear, es hora de empezar a generarlos, por lo tanto necesitaremos usar la herramienta Usuarios y equipos de Active Directory. Esta herramienta podemos ubicarla dentro del menú inicio, programas, herramientas administrativas.

Tal como vemos en la figura inferior, disponemos de una columna izquierda donde podemos observar los contenedores de objetos que existen dentro del dominio (en nuestro caso ita.com.ar). Por ejemplo dentro del contenedor Users pueden verse los usuarios y grupos predefinidos por el sistema.

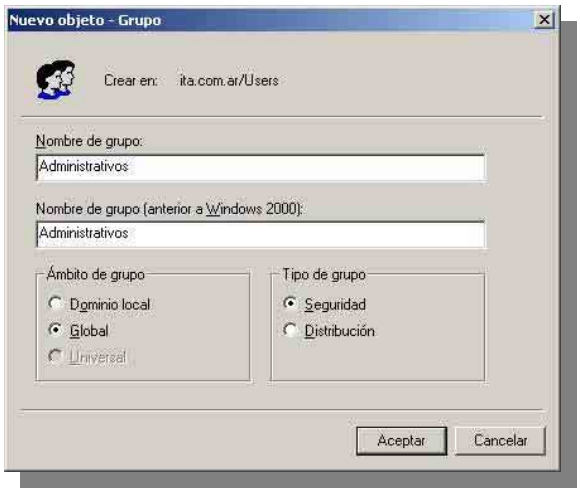
.



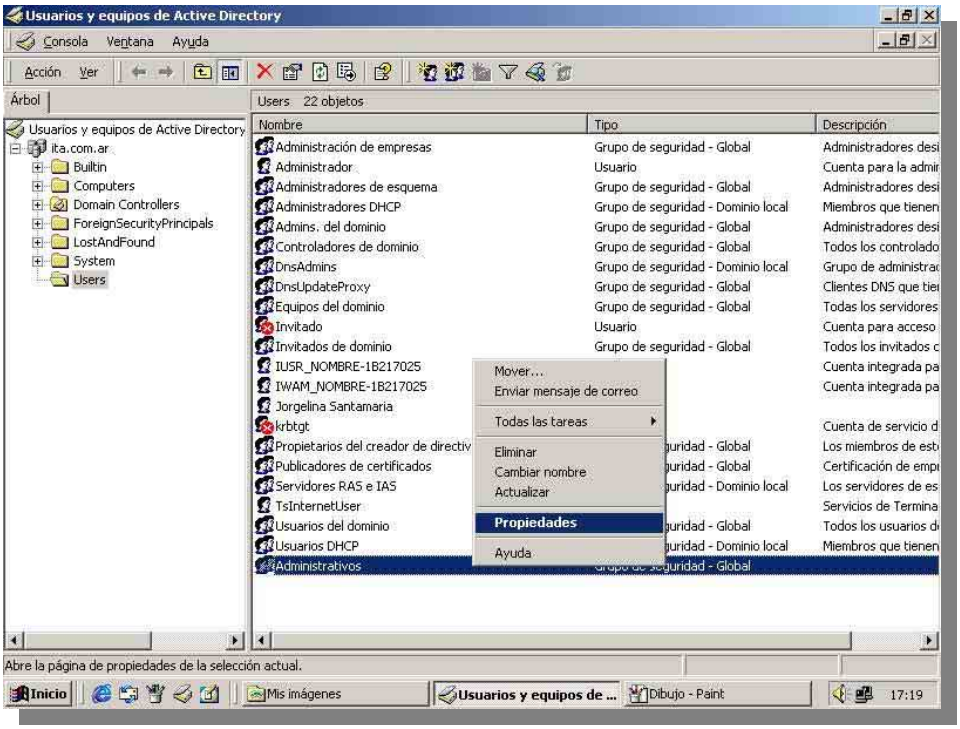
Como nuestra idea es generar un nuevo grupo dentro del contenedor Users debemos entonces seleccionar tal contenedor, y una vez allí abrimos el menú Acción, luego nuevo y por último grupos.



Desde la nueva ventana abierta debemos definir la información sobre el nuevo objeto grupo a crear. Por lo tanto es menester declarar un nombre para el nuevo grupo y también especificar que ámbito tendrá (local, global o universal) y además de que tipo de grupo se trata (distribución o seguridad).



Una vez realizadas estas tareas, el nuevo grupo deberá aparecer en la lista del contenedor users, por ejemplo podemos ver en la figura siguiente que el nuevo grupo Administrativos está presente en la lista Users. Para poder administrar este grupo será necesario presionar el botón derecho sobre el grupo y elegir Propiedades.



Luego de realizado esto, podemos ver una nueva ventana con información referente al grupo.

Nos centraremos precisamente en la lengüeta miembros, que es la que nos servirá para agregar usuarios al grupo mediante el botón Agregar.

Para poder realizar una correcta administración grupal, es preciso generar primero todos los grupos necesarios, para luego recién crear a los usuarios y agregarlos al grupo que le corresponda.

3.2 CREACIÓN DE USUARIOS

Una vez generados los grupos es necesario comenzar a crear a los usuarios que estarán incluidos en nuestro dominio. Para realizar tal tarea se debe realizar un procedimiento similar al de creación de grupos con pequeñas diferencias.

Tal como fue realizado para crear grupos, debemos seleccionar el contenedor elegido y una vez posicionados allí, debemos abrir el menú acción, nuevo pero esta vez usuario.

Nuevamente tendremos en pantalla la ventana de nuevo objeto-usuario, donde debemos ingresar información relativa a este. Esta información esta compuesta por el nombre completo del usuario, su nombre de inicio de sesión y el nombre para versiones anteriores a Windows 2003.

Una vez completados estos datos, es necesario asignar una contraseña al usuario y efectuar algunas configuraciones mas, referidas a la contraseña. Como vemos en la figura inferior tenemos una serie de cuadros que posibilitan:

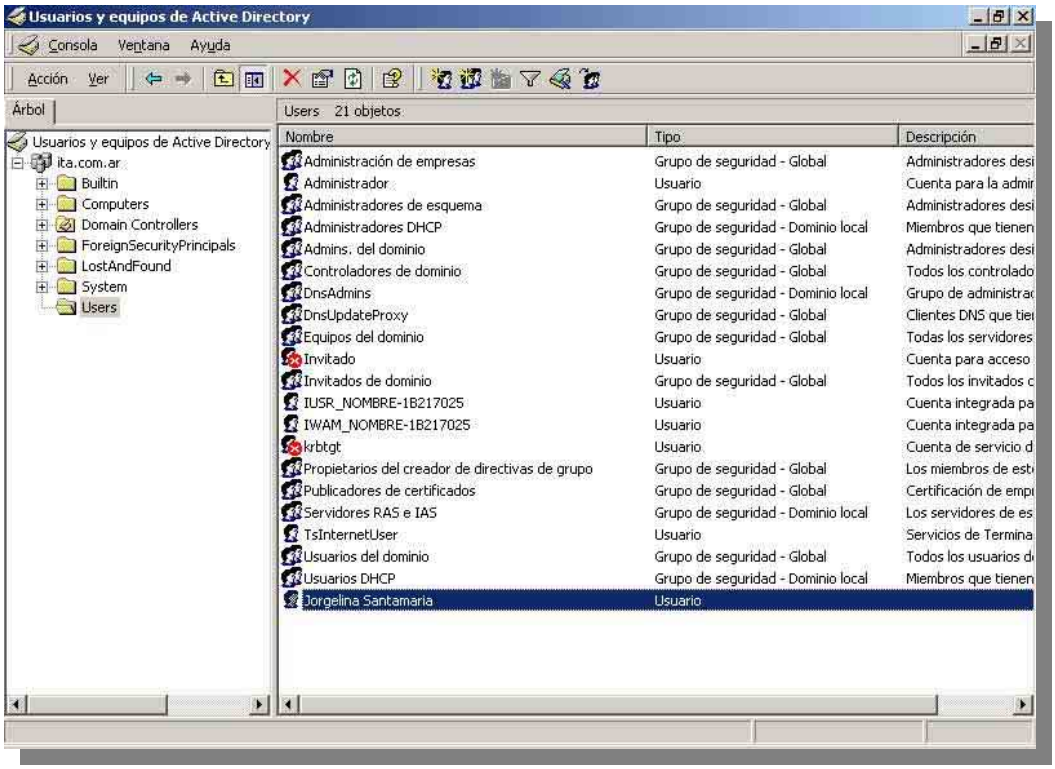
a) El usuario debe cambiar la contraseña en el siguiente inicio de sesión: si este cuadro se tilda, la primera vez que este usuario inicia sesión en el servidor, este lo obligará a cambiar su contraseña.

b) El usuario no puede cambiar la contraseña: tildando este ítem el usuario no tendrá la facultad de modificar su contraseña.

c) La contraseña nunca caduca: aquí se especificará si la contraseña tendrá fecha de caducidad y deberá ser renovada o si esta no caducará nunca.

d) Cuenta deshabilitada: como el texto nos indica, estando tildada esta opción la cuenta será deshabilitada.

Una vez más, luego de realizado este procedimiento, y habiendo aceptado el cuadro con el resumen de la información configurada del usuario, estará disponible e incluido dentro de la lista Users.



Como hemos visto la administración centralizada se basa en grupos de usuarios. De este modo toda administración se debe hacer sobre los grupos, y a cada uno de ellos asignarle los permisos correspondientes. Solo restará agregar o quitar usuarios, a medida que se vayan generando en los diferentes grupos, simplificando la tarea de la administración.

4 POLITICAS DEL SISTEMA.

Las políticas del sistema o Directivas de grupo, especifican los distintos componentes de la configuración del entorno de trabajo de un usuario. Un administrador del sistema podrá modificar los programas que se encuentran disponibles para los usuarios, lo que aparecerá en sus escritorios y las opciones del menú Inicio. Además mediante el uso de las directivas se pueden ejecutar programas al inicio de una sesión, redirigir carpetas del equipo local a ubicaciones de red, administrar aplicaciones (por ejemplo instalar programas automáticamente cuando un usuario inicia la sesión), especificar las opciones de seguridad (que puede hacer o no un usuario sobre un equipo o equipos en particular), y muchas cosas mas.

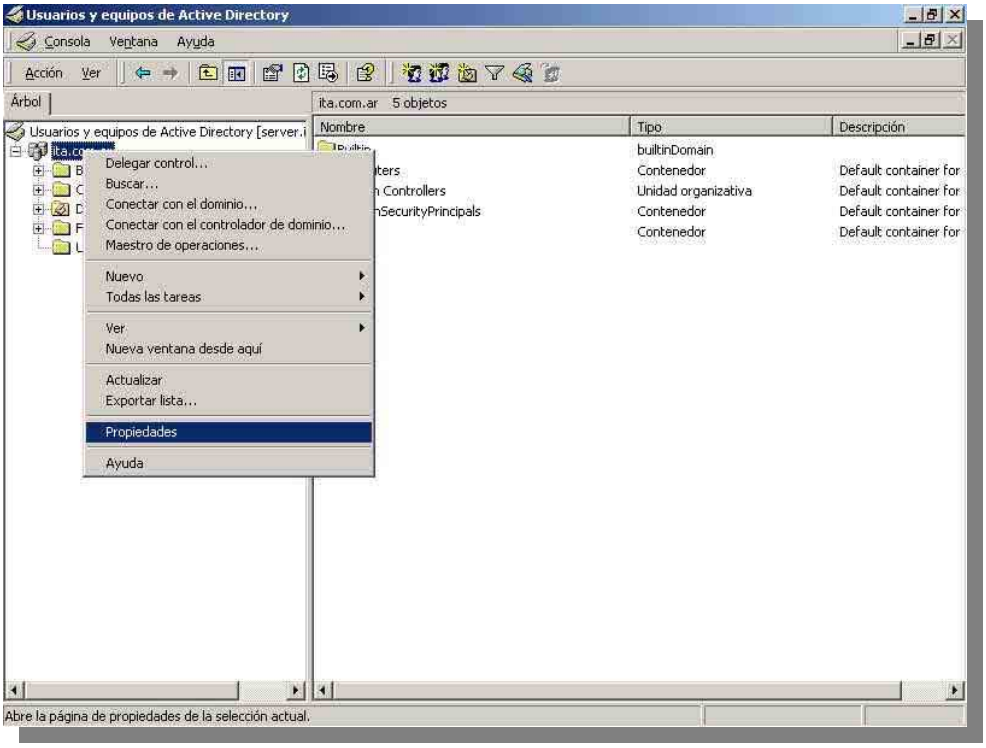
4.1 GENERACIÓN DE POLÍTICAS

Para crear una configuración específica para un grupo de usuarios en particular, se utiliza la herramienta Directiva de grupo. Mediante esta herramienta se pueden generar políticas personalizadas para grupos diferentes y controlar el entorno del usuario en los equipos en los cuales inicie sesión. Esta tarea se realiza con la ayuda de plantillas, que poseen en su interior grupos de configuraciones estándar, a partir de las cuales resulta más fácil trabajar y aplicar personalizaciones.

Existen dos tipos de directivas: directiva de usuario y de equipo. La directiva de usuario se aplica cuando un usuario inicia sesión en cualquier equipo del dominio, la directiva de equipo se aplica cuando inicia sesión sobre un equipo específico. Nos centraremos en las políticas de usuario y su configuración sobre el servidor.

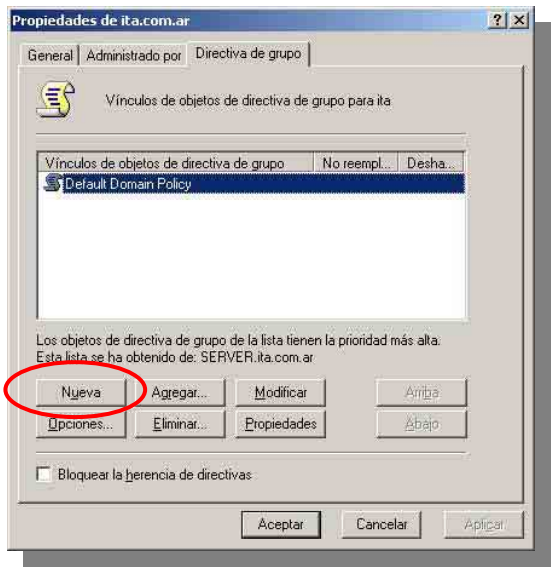
Estas políticas llamadas Directivas de Grupo en Windows 2003 se acceden desde el panel *Usuarios y equipos de Active Directory*. Seleccionando el icono de nuestro dominio se debe hacer clic con el botón derecho del mouse y seleccionar propiedades tal como muestra la imagen que se encuentra a continuación.

Una vez realizado esto veremos la pantalla de las propiedades de este dominio. A continuación será necesario ubicarse sobre la lengüeta directiva de grupo y dentro de esta solapa, encontraremos la lista de la o las directivas de grupo existentes en este dominio. Si el servidor es nuevo y no fue previamente configurado, nos encontraremos solamente con la política asignada por defecto llamada Default Domain Policy.



Volviendo sobre el concepto de administración grupal, como nuestra idea es agregar nuevas políticas adaptadas a nuestras necesidades, lo ideal será generar nuevas directivas y una vez generadas estas, poder ir agregando miembros a cada directiva en particular. De esta forma podremos crear nuevas directivas de grupo con diferentes niveles de restricción adaptadas a diferentes grupos de usuarios.

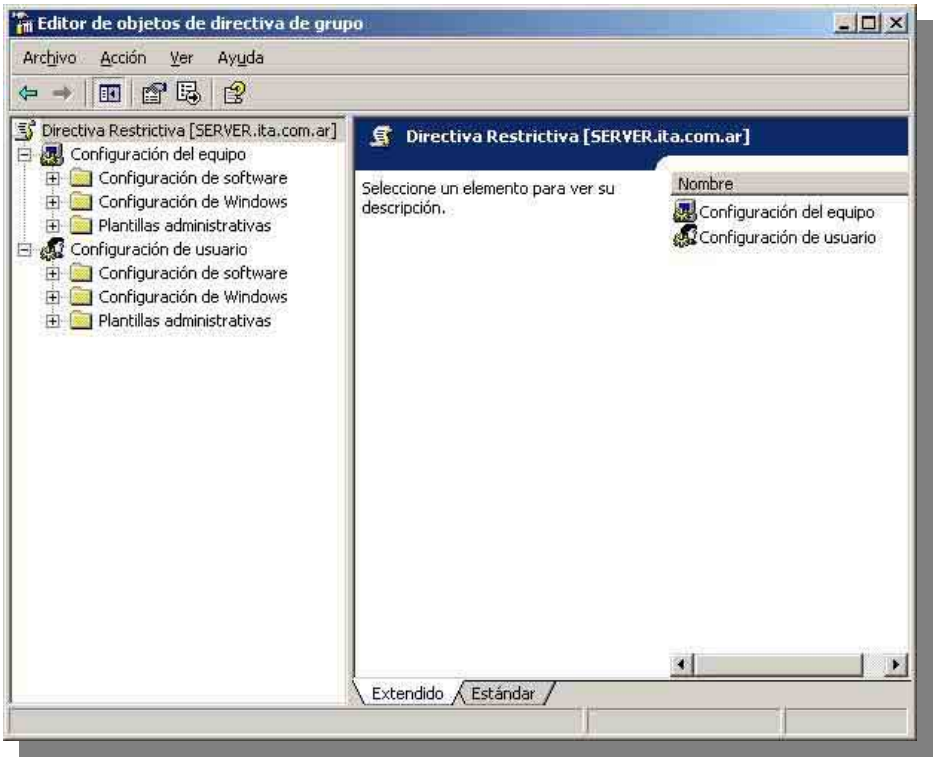
Para crearlas será necesario presionar el botón Nueva...



Luego de presionar el botón aparecerá una nueva entrada en la lista al que debemos asignarle un nombre (que en lo posible debe ser descriptivo de la directiva), para luego confirmarlo con enter.

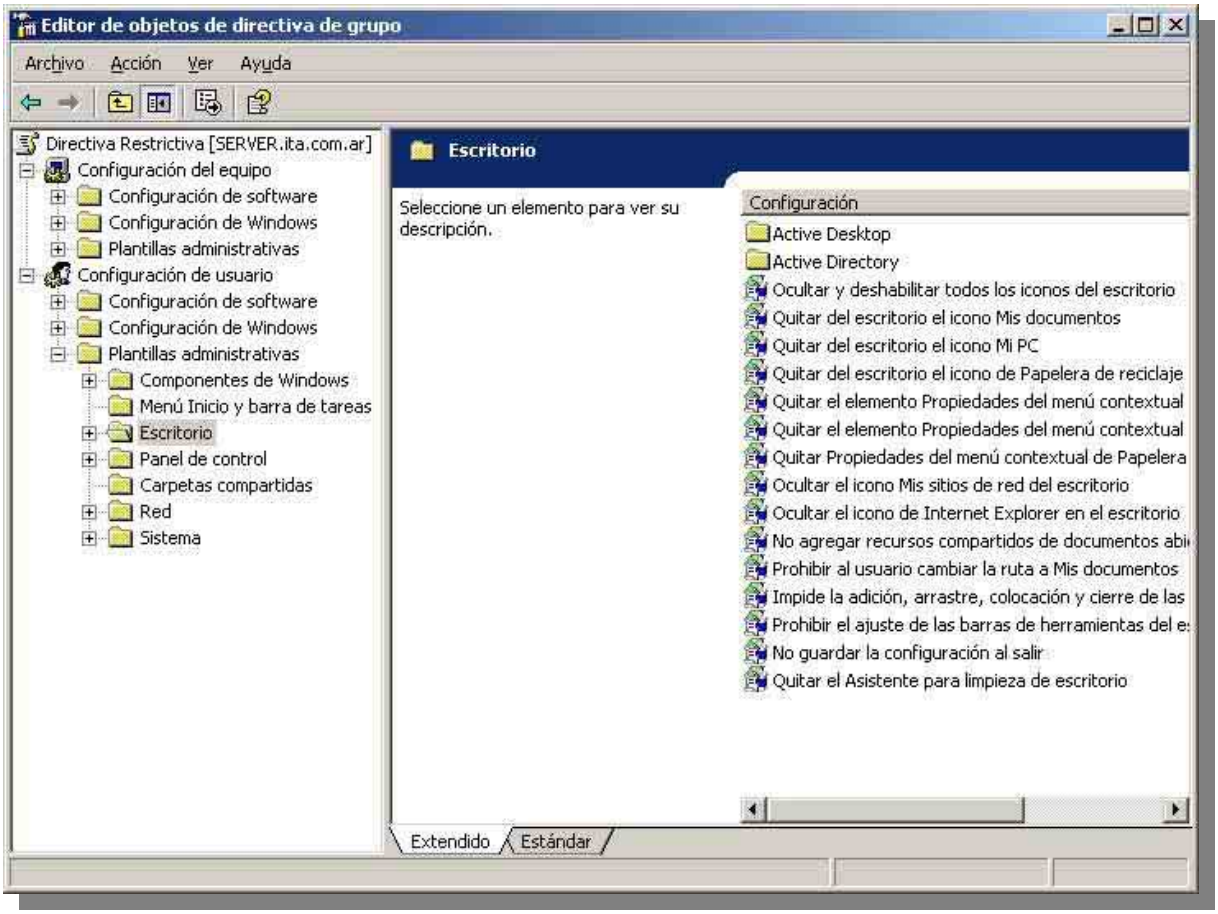
Una vez realizado esto, y una vez comprobado que el nuevo nombre figura en la lista, seleccionamos la nueva entrada y presionamos el botón modificar.

Seguidamente obtendremos la ventana de la directiva de grupo correspondiente que acabamos de crear y, como podemos observar en la siguiente figura, sobre la izquierda tenemos la entrada correspondiente a la configuración del equipo (directivas de equipo) y las que nos atañe a nosotros, configuración de usuario (o sea directivas de usuario).



Posicionándonos sobre el objeto Plantillas administrativas del contenedor Configuración de usuario, veremos una serie de contenedores con grupos de configuraciones enfocadas a diferentes aspectos del entorno de un equipo (por Ej. Escritorio, Sistema, etc.). Desde este lugar podemos personalizar y generar la política más adecuada a las necesidades de un cliente.

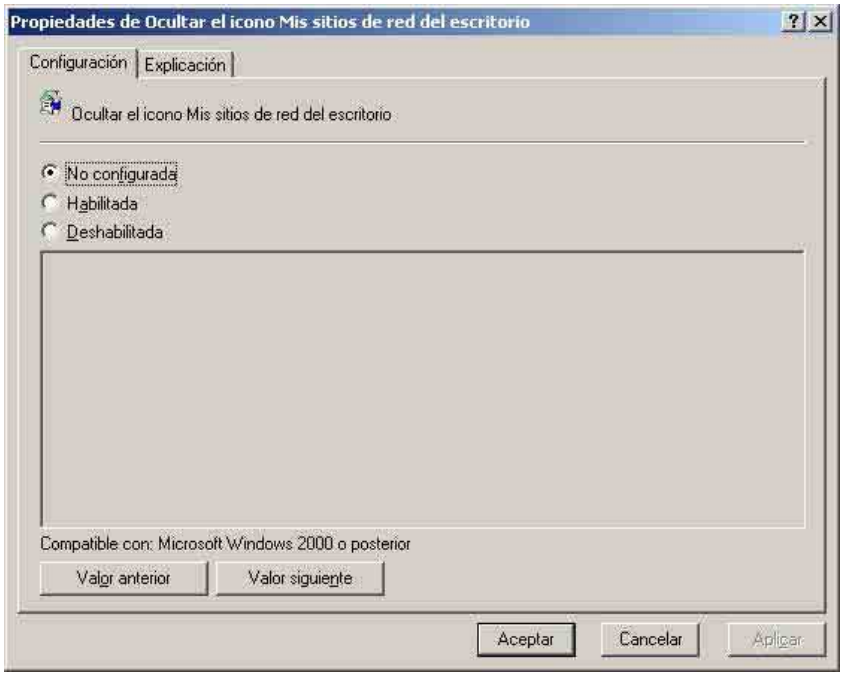
Es pertinente notar que, si observamos detenidamente la lista de de directivas, vemos que existen algunas de ellas que abarcan a las siguientes (en el orden de aparición en la lista). Por ejemplo, si prestamos atención en la figura inferior, vemos que existe una entrada Ocultar todos los íconos del Escritorio y luego existe una serie de entradas, que refieren a íconos específicos del escritorio. De este modo, si la idea es quitar todos los íconos del escritorio, usaremos la primera opción. En cambio si solo deseáramos quitar algunos, usaríamos las opciones que refieren a íconos puntuales.



Si queremos aplicar una restricción específica, por ejemplo quitar el icono Mis sitios de red del escritorio, debemos hacer doble clic sobre la directiva y, una vez abierta la ventana correspondiente, configurar el comportamiento de la directiva.

Existen tres tipos de declaración diferente de directivas:

- No configurada: opción mediante la cual determinamos que el registro no será modificado con respecto a esta directiva.
- Habilitada: el registro será modificado para que la directiva sea aplicada efectivamente a todos los usuarios afectados por la directiva de grupo.
- Deshabilitada: Especifica que no se realizará ningún cambio en el Registro en relación con este parámetro.



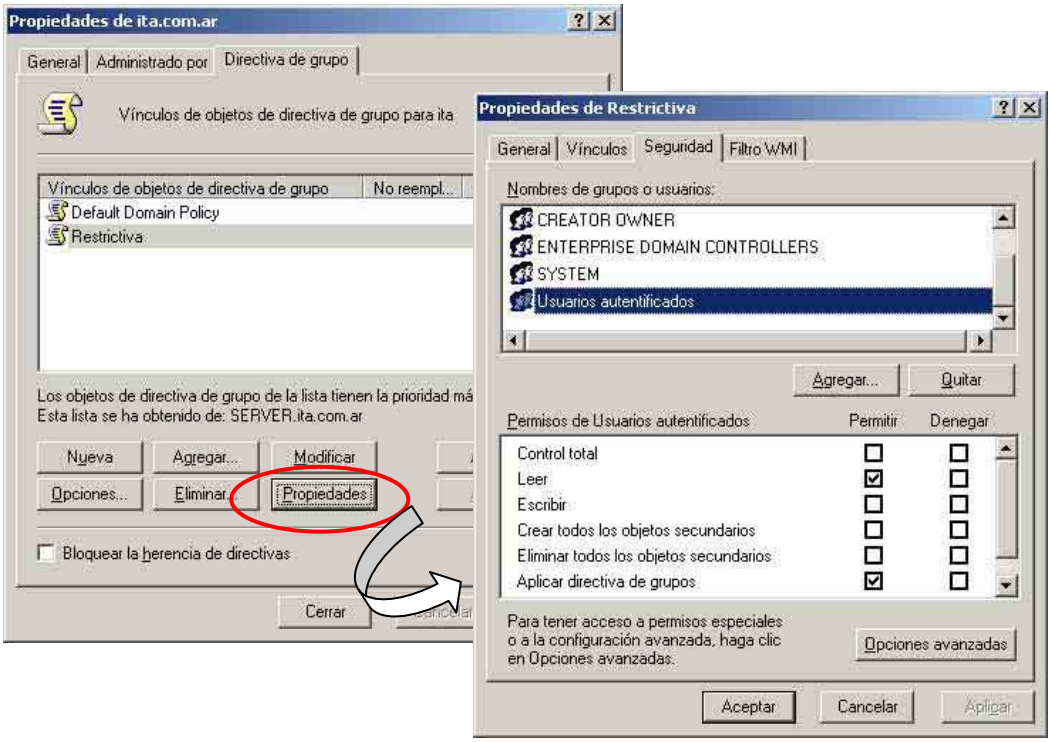
Si queremos que los usuarios afectados por esta directiva, no tengan el icono Mis sitios de red sobre el escritorio, simplemente debemos seleccionar la opción habilitada y tal configuración quedará establecida.

Una vez realizadas todas las configuraciones pertinentes dentro de nuestra Directiva de Grupo, es momento de configurar el campo de acción de la misma. Es decir que ahora, debemos determinar que grupos de usuarios quedarán afectados por la misma. Para realizar tal acción cerraremos la ventana de la nueva directiva, volveremos a la pantalla de las propiedades de nuestro dominio y, previa selección de la directiva generada, presionaremos el botón Propiedades y luego el botón Seguridad.

Desde aquí se administran los grupos (o usuarios) que serán abarcados por la directiva. Es importante tener en cuenta ciertos detalles para que a un grupo le sea aplicada la directiva.

Luego de agregado un grupo de usuarios, en la lista de permisos correspondiente deben estar tildadas dos opciones, el permiso leer y el de Aplicar directiva de grupo. Con esto permitiremos que el grupo tenga acceso de lectura a la directiva y además, que se aplique efectivamente.

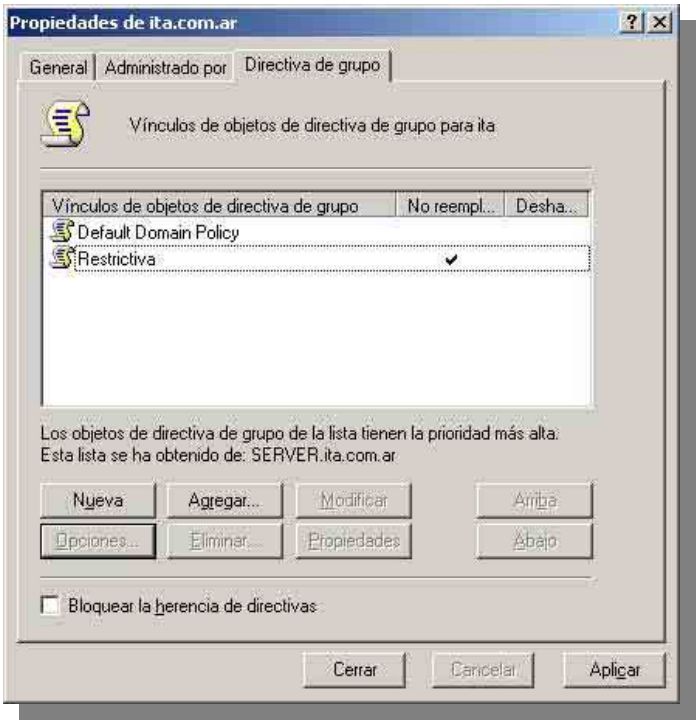
Atención: sin estas tildes la directiva no será aplicada.



4.2 JERARQUIAS ENTRE DIRECTIVAS DE GRUPO

Las directivas ubicadas en la parte superior de la lista son de mayor nivel, por lo tanto pueden anular directivas procesadas con anterioridad. En otras palabras, pueden volver a aplicar alguna directiva, que ya haya sido configurada por alguna otra directiva anterior, y por lo tanto, dejarla sin efecto. Teniendo en cuenta esto se puede notar que la ubicación dentro de la lista, dará la jerarquía a las diferentes directivas, por lo tanto si existen incoherencias entre ellas, lo valido será lo especificado por la directiva superior. No obstante, si sobre un objeto determinado de una de Directiva de grupo se activa la opción No reemplazar (haciendo clic con el botón derecho del mouse sobre la directiva y eligiendo esa opción), esa directiva no se puede volver a configurar. Por lo tanto no importará lo que otras directivas de jerarquía superior especifiquen, lo declarado por esa directiva será lo aplicado.

Finalmente y una vez realizado todo este procedimiento podemos decir que la directiva ha quedado utilizable. A partir de este momento, los usuarios pertenecientes a los grupos elegidos que inicien sesión en el dominio, serán afectados por la directiva asociada.


Propiedades de ita.com.ar
General
Administrado por
Directiva de grupo
Vínculos de objetos de directiva de grupo para ita
Vínculos de objetos de directiva de grupo
No reempl...
Desha...
Default Domain Policy
Restrictiva
Los objetos de directiva de grupo de la lista tienen la prioridad más alta.
Esta lista se ha obtenido de: SERVER.ita.com.ar
Nueva
Agregar...
Modificar
Arriba
Opciones...
Eliminar
Propiedades
Abajo
Bloquear la herencia de directivas
Cerrar
Cancelar
Aplicar

NOTAS

CUESTIONARIO CAPITULO 23

CONFIDENCIAL

1.- ¿Que diferencia hay entre un Permiso y un Derecho?

2.- ¿Cuantos tipos de directivas conoce? ¿Donde se aplican cada una de ellas?

3.- Partiendo de una Directiva creada. ¿Cual es el procedimiento para que esta se haga efectiva?

4.- ¿Que sucede si dos Políticas distintas se aplican a un mismo usuario?

5.- ¿Cuantos tipos de permisos conoce?