- **Conceptos de usuarios y cuentas de usuarios**
  - Un usuario se entiende como cada persona que puede entrar en el sistema
  - Para controlar la entrada y sus acciones se utiliza el concepto de "*cuenta de usuario*"

  Cuenta de usuario:

  - Es la credencial de un usuario y permite la entrada al dominio (u ordenador local) y el acceso a los recursos
  - Almacena toda la información que el sistema guarda de los usuarios:
    - Nombre + Nombre completo
    - Contraseña
    - Directorio de conexión
    - Horas de conexión
    - Activación de la cuenta
  - Internamente, el sistema operativo identifica al usuario por un número ? Identificador seguro *SID* (*Secure Identifier*)
    - Se genera cuando se crea la cuenta
    - Permanece aún cuando se renombra la cuenta

- **Tipos de cuentas de usuarios en W2k**

	Tipo de cuenta de usuario	Descripción
	Cuenta de usuario local	•Permite a un usuario entrar a un ordenador específico y acceder a los recursos de ese ordenador •La cuenta reside en la SAM (Security Accounts Manager) del ordenador
	Cuenta de usuario del dominio	•Permite a un usuario entrar al dominio y acceder a los recursos de cualquier ordenador de la red •La cuenta reside en el Directorio Activo
	Cuenta de usuario predefinida	•Permite a un usuario realizar ciertas tareas administrativas o acceder temporalmente a ciertos recursos •Hay dos cuentas básicas (no pueden ser borradas): administrador e invitado (local y del dominio) •Se crean automáticamente

- **Planificación de las cuentas de usuarios**

  Antes de crear la cuentas de usuario:

  – Adoptar una convención de nombres que asegure la unicidad y comodidad de las cuentas

  – Política de contraseñas:

    - Siempre asignar password al administrador
    - Fijar las contraseñas o dejar que los usuarios las controlen
    - Fijar la expiración de las cuentas (empleados temporales, alumnos,...)
    - Implicar al usuario en esta política:
      – Evitar nombres obvios
      – Fijar passwords largos (pueden ser hasta 128 caracteres)
      – Usar mayúsculas, minúsculas, caracteres no alfanuméricos

  – Establecer horas válidas para entrar al sistema

  – Limitar el acceso al dominio desde determinas estaciones

  – Determinar la situación de los directorios de trabajo de los usuarios:

    - En el servidor:
      – Centralización de los ficheros para la realización de copias de seguridad
      – Incrementa el tráfico de la red
    - En el cliente:
      – Mayor complejidad para la realización de las copias de seguridad
      – Reduce el tráfico en la red

- **Implementación de una política de cuentas**

  Una política de cuentas determina el nivel de seguridad que se establece en el sistema:

  – Caducidad de las contraseñas

  – Longitud mínima de las contraseñas

  – Unicidad de los passwords (recordar últimos passwords)

  – Bloqueo de cuentas

  Los cambios que se realizan sobre estas políticas tienen efecto a partir de:

  - La próxima vez que el usuario entre en el sistema
  - La próxima vez que el usuario realiza un cambio cubierto por la política.

  Ejemplo: La longitud mínima de las contraseñas no afecta a las ya existentes, pero cuando un usuario la va a cambiar, se aplicará la política.

  Planificación de una política de cuentas

  – No permitir passwords nulos

  – Requerir una longitud mínima:

  - 6-8 caracteres para una red de media seguridad (RMS)
  - 8-14 para una red de alta seguridad (RAS)
  - Obligar cambios de passwords con cierta frecuencia

    45-90 RMS, 14-45 RAS
  - No permitir contraseñas ya usadas (recordar 8)
  - Bloquear cuenta después de múltiples intentos fallidos
  - Forzar a que el administrador habilite la cuenta después
  - Fijar horarios de conexión

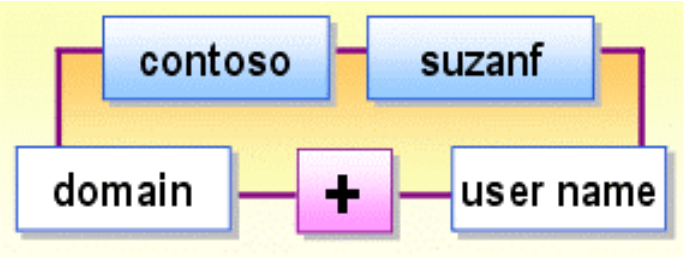
Nombres de usuario en W2k

- En el Directorio Activo, cada cuenta de usuario lleva asociada un “logon name” y un “logon name pre-Windows 2000” (que es almacenado en la SAM)
- Un usuario puede entrar al sistema indistintamente con el “*nombre principal de usuario*” o con el “nombre de usuario” (pre- Windows 2000).
- Además, cuando se crean cuentas de usuarios, también es necesario asegurar unos criterios de unicidad de las cuentas

- **Nombre principal de usuario**

- Permite al usuario entrar en cualquier ordenador del bosque
- Consta de dos partes separadas por “@”:
  - El *prefijo: suzanf*
  - El sufijo:*contoso.msft*. Por defecto, el sufijo es el nombre del dominio raíz en la red, aunque se pueden usar los otros dominios como sufijos de los nombres de usuarios (Ejemplo: para hacerlo coincidir con la dirección de correo electrónico)

- **Nombre de usuario (pre-Windows 2000)**
  - Si un usuario entra en el sistema desde un SO previo a Windows 2000, debe usar un nombre de usuario compuesto:



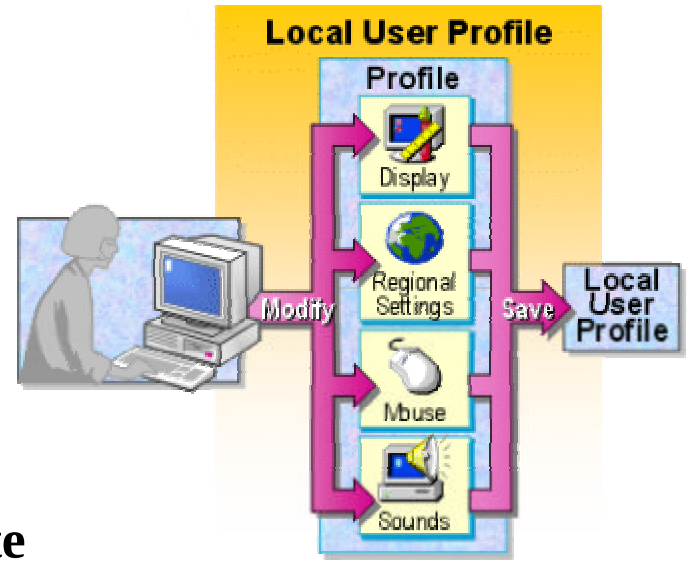
    - Cuenta de usuario: suzanf
    - Dominio en el que se encuentra la cuenta para que el controlador de dominio sepa dónde encontrar la cuenta.
- **Reglas de unicidad en los nombres de usuario**
  - El nombre completo del usuario debe ser único en el contenedor donde reside la cuenta. El nombre completo se utiliza como nombre relativo distinguido
  - El nombre principal de usuario debe ser único en el bosque
  - El nombre de usuario (pre-Windows 2000) debe ser único en el dominio.

- **Gestión del entorno de trabajo de los usuarios: perfiles**
  - El entorno de trabajo de los usuarios en W2k viene fijado por el “perfil de usuario”
  - Cada usuario necesita un perfil asociado a su cuenta para acceder al sistema
  - El perfil contiene la configuración que el usuario ha definido para su entorno de trabajo: escritorio, conexiones,...
  - El perfile se crea cuando un usuario entra a un ordenador por primera vez. La configuración se almacena en el directorio: C: :\Documents and Settings*User name*
  - Cuando el usuario abandona la sesión, se actualiza el perfil en ese ordenador
- **Tipos de perfiles de usuario**

  Perfil de usuario por defecto
  - Es la base para todos los perfiles de usuario. Inicialmente, cada usuario realiza una copia del perfil por defecto

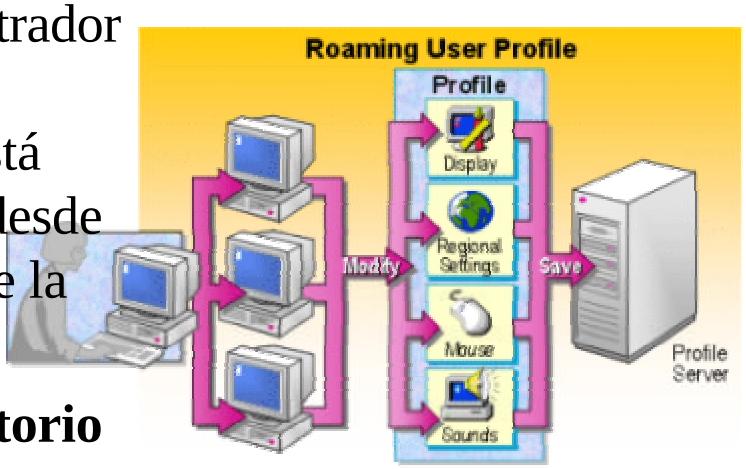
Perfil de usuario local

– Se crea la primera vez que el usuario entra en el ordenador.



Perfil de usuario flotante

– Se crea por el administrador y se almacena en un servidor. Este perfil está disponible al usuario desde cualquier ordenador de la red

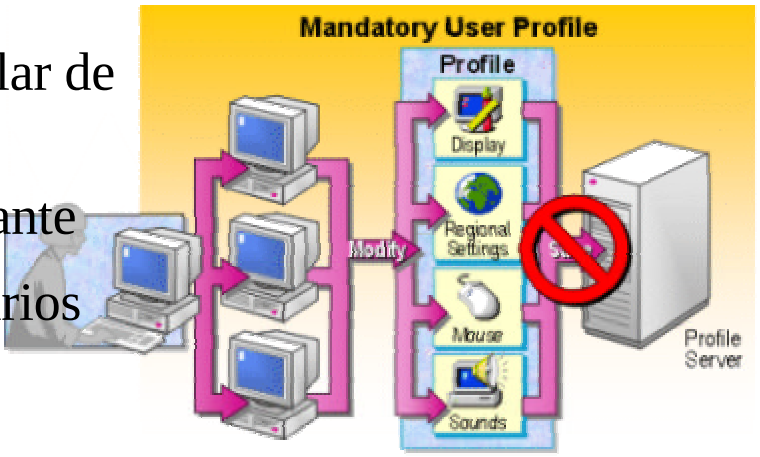


Perfil de usuario obligatorio

– Se crea por el administrador para especificar la configuración particular de los usuarios.

– Puede ser local o flotante

– No permite a los usuarios almacenar las modificaciones (ntuser.man)



- **Administración de cuentas de usuario**

  Una vez creadas las cuentas puede ser necesario realizar tareas administrativas comunes:

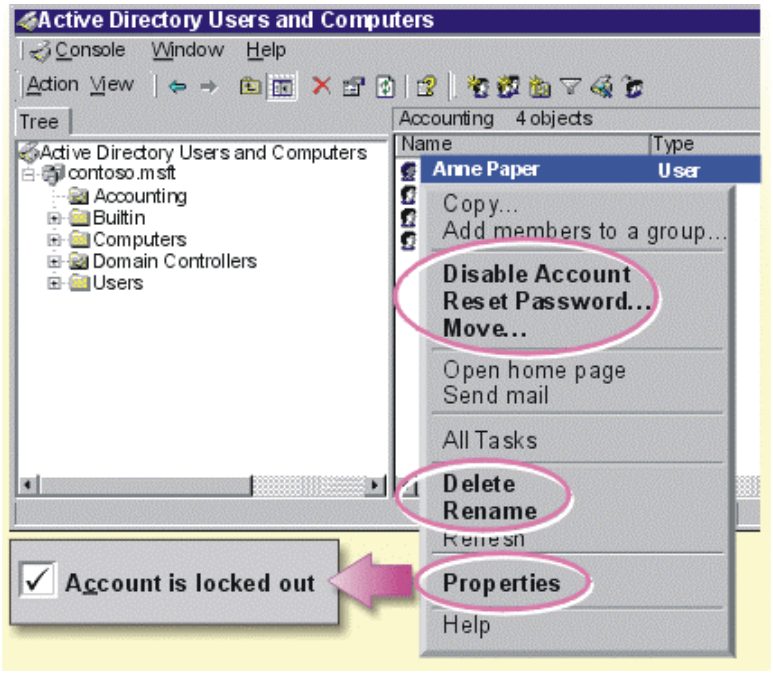
  – Habilitación/deshabilitación de cuentas

  – Modificación de contraseñas

  – Borrado/renombrado de cuentas de usuario

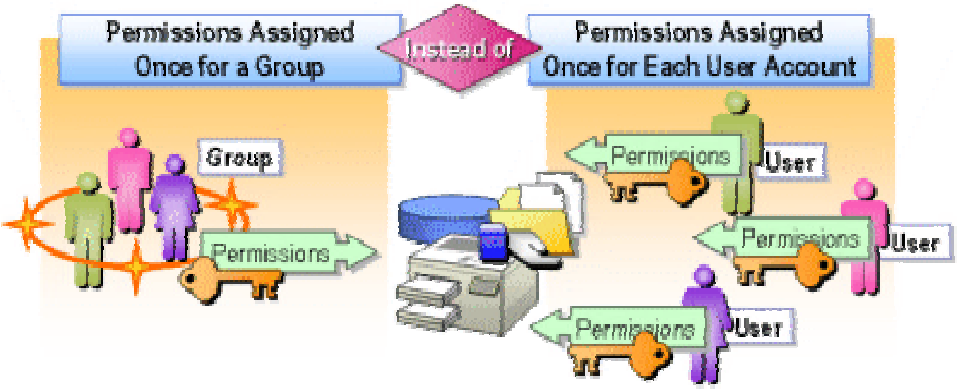
  – Desbloqueo de cuentas

  – Movimiento de cuentas en el dominio

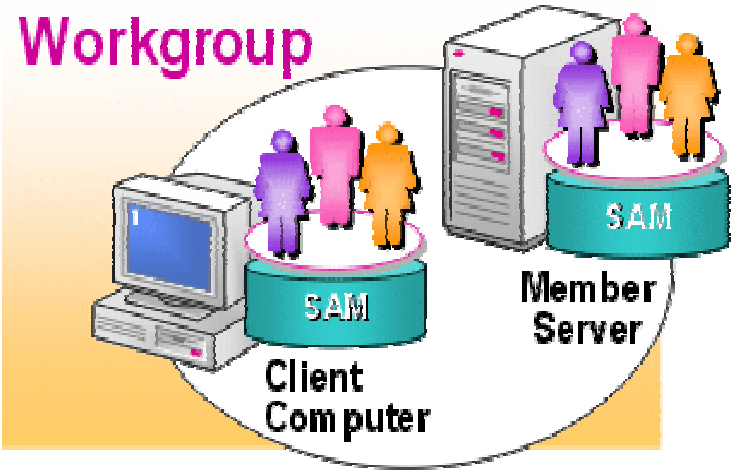


  – Puede resultar útil realizar búsquedas de objetos dentro del directorio activo: usuarios, ordenadores, impresoras, ...

- **Grupos de usuarios**
  - Un *grupo* es una colección de cuentas de usuarios.
  - Permiten simplificar la gestión del acceso a los recursos por múltiples usuarios.
  - Puesto que los grupos son una “lista de miembros”, pueden anidarse.

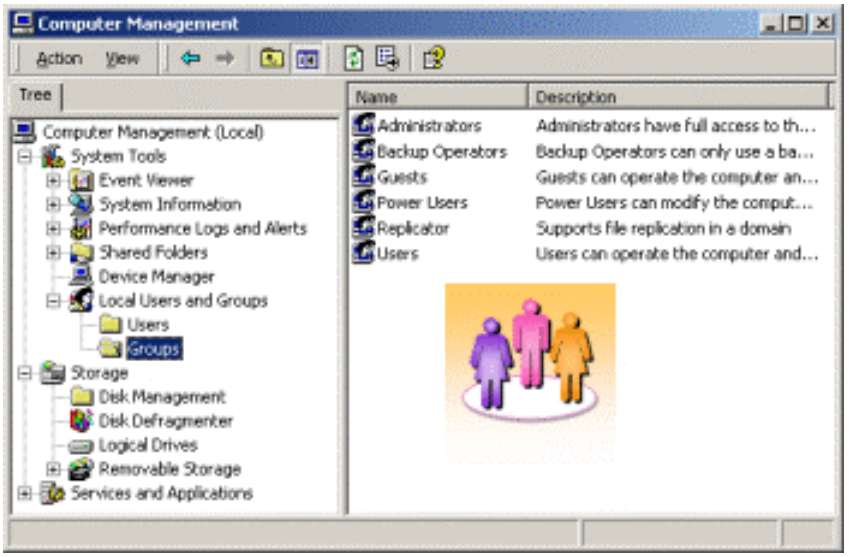


- **Grupos en “trabajo en grupo” y “dominios”**
  - **Grupos en sistemas de “trabajo en grupo”**
    - Se pueden utilizar sólo para asignar permisos en el ordenador donde se han creado
    - Son grupos locales

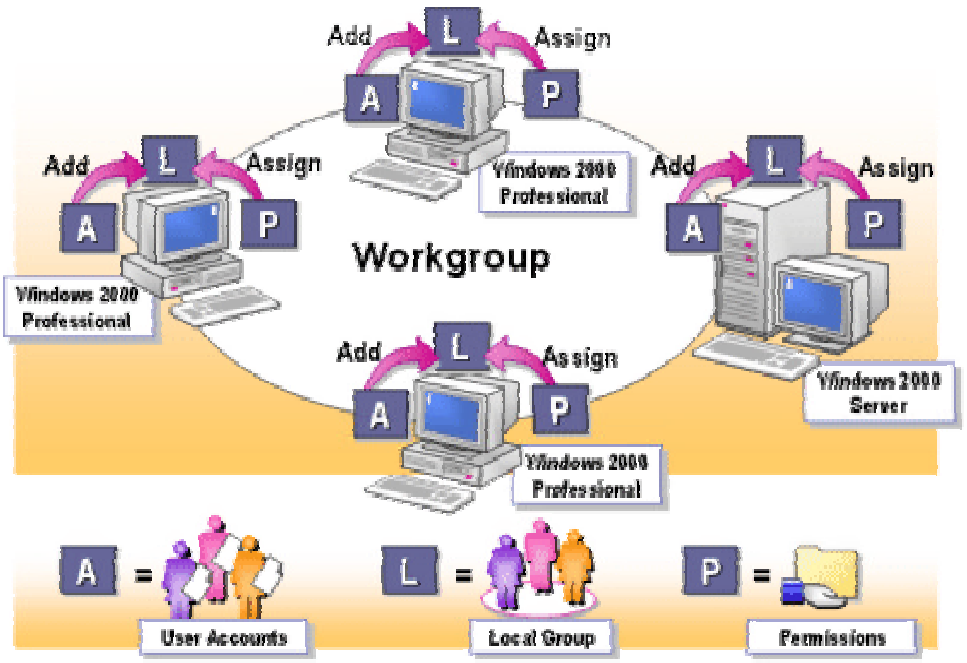


- No es aconsejable crearlos en ordenadores que formen parte de un dominio

– Grupos predefinidos

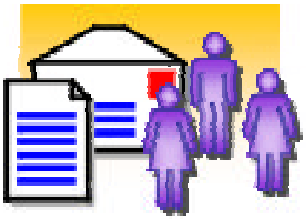


– Estrategia de creación de grupos locales



- **Grupos en “dominios”**
  - Se crean en los controladores de dominio
  - Residen en el directorio Activo
  - Se le pueden asignar permisos de acceso a todos los ordenadores del dominio
- **Tipos de grupos:**
  - ***Grupos de seguridad***: Son los grupos que se usan para todos los asuntos relacionados con la seguridad (control de acceso,...)

  - ***Grupos de distribución:*** Son listas de usuarios utilizadas para asuntos no relacionadas con la seguridad (envío de e-mail a un grupo de usuarios,...).



  No pueden ser utilizados para asignar permisos
- **Ámbito de los grupos**
  - El ámbito de un grupo determina dónde se puede utilizar un determinado grupo en la organización
  - Va a marcar cuáles son los posibles miembros que pueden formar parte así como el anidado (grupos incluidos en otros grupos).

- **Grupos globales**:

  Los grupos globales se usan para organizar usuarios que comparten las mismas tareas y necesitan requerimientos de acceso a la red similares

  – Pueden contener cuentas de usuarios y grupos globales del mismo dominio donde están definidos (sólo modo nativo)

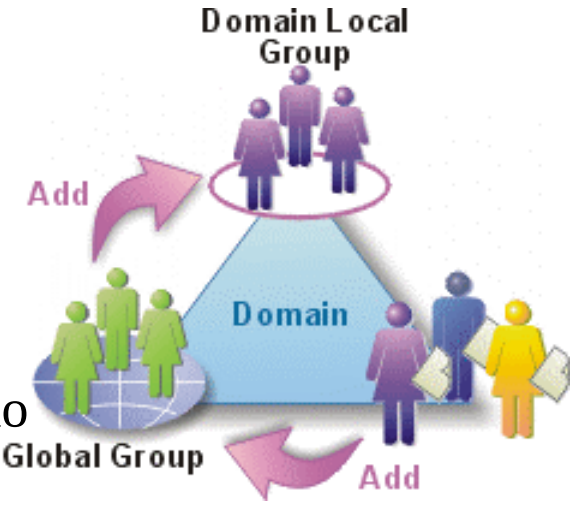
  – Pueden ser miembros de grupos universales y de grupos locales del dominio de cualquier dominio y de grupos globales del mismo dominio

  – Se le pueden asignar permisos en cualquier dominio del bosque

- **Grupos locales del dominio**

  Son usados para asignar permisos de acceso a los recursos que se encuentran en el mismo dominio donde reside el grupo

– Pueden contener cuentas de usuarios, grupos globales y grupos universales de cualquier dominio del bosque, además de otros grupos locales del mismo dominio (sólo modo nativo)



– Pueden ser miembros de otros grupos locales del mismo dominio (modo nativo)

– Se le pueden asignar permisos sólo en el dominio donde se crea.

- **Grupos Universales**

Se usan habitualmente para asignar permisos comunes a grupos de diferentes dominios.

– Pueden contener cuentas de usuarios, grupos globales y otros grupos universales de cualquier dominio del bosque.

– Pueden ser miembros de grupos locales del dominio y de otros grupos universales

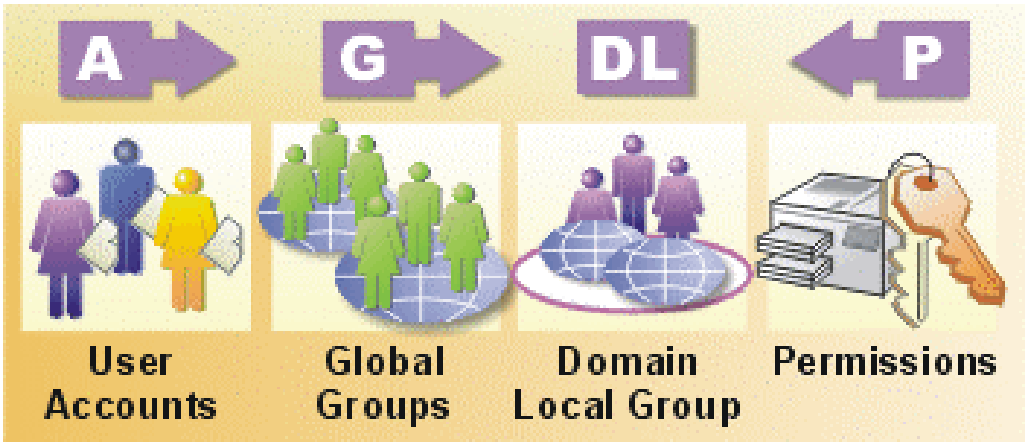
– Se le pueden asignar permisos en cualquier dominio del bosque.

– Desde el punto de vista de la eficiencia, puesto que estos grupos residen en el catálogo global, es aconsejable limitar su uso a aquellas situaciones en las que sea estrictamente necesario

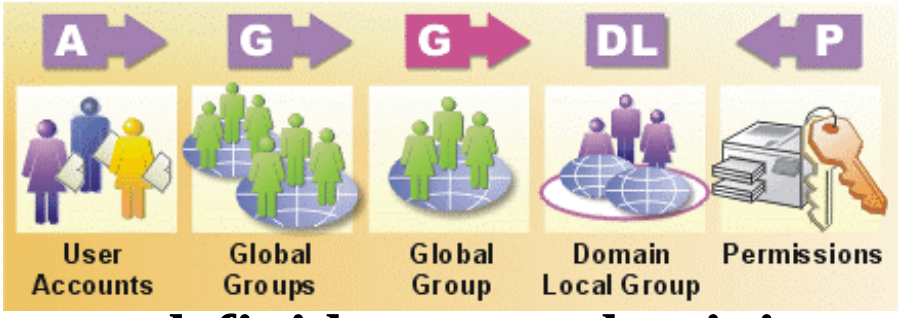
– Es aconsejable no incluir usuarios directamente en estos grupos (cualquier modificación implica la replicación del catálogo global)

- **Estrategia para la creación de grupos en un dominio**

a) Estrategia A G DL P

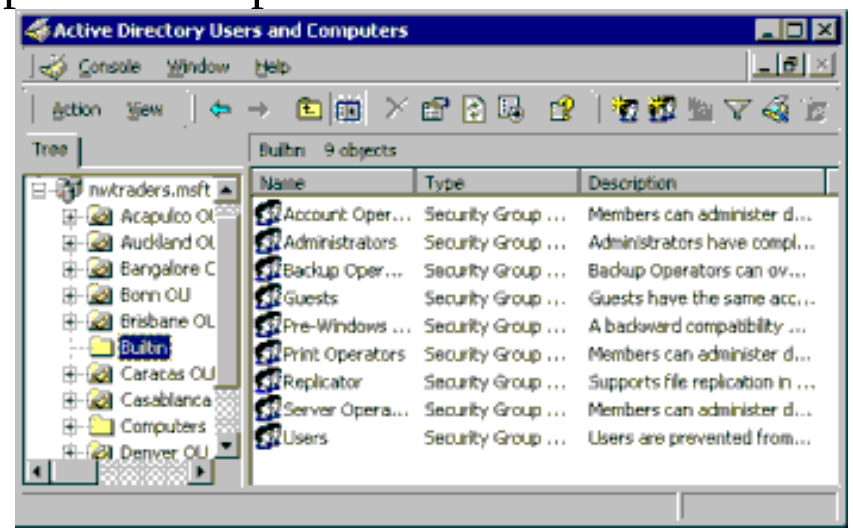


b) Estrategia A G G DL P

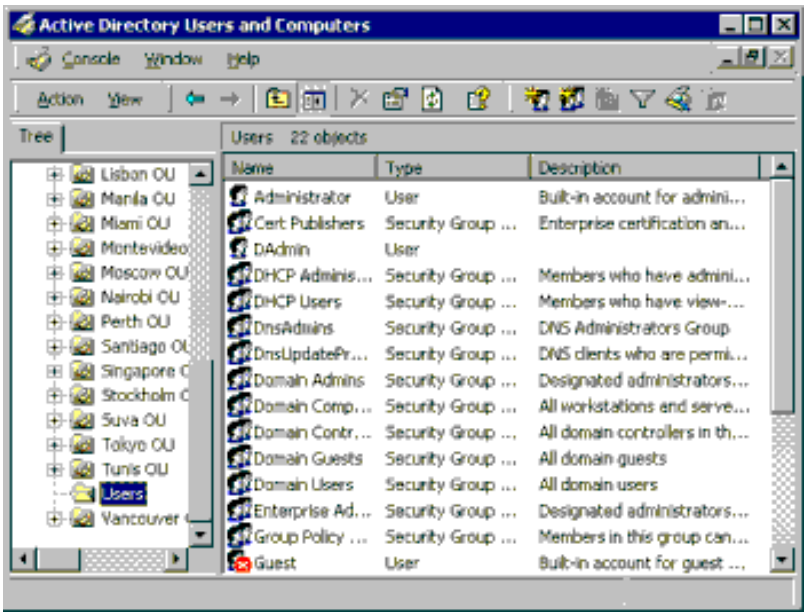


Grupos predefinidos en un dominio

a) Grupos locales predefinidos



b) Grupos globales predefinidos



- **Seguridad de los recursos de red. Carpetas compartidas**

  La compartición es una característica que permite el acceso por la red a recursos locales

  Para controlar este acceso, se establecen unos permisos que fijan lo que los distintos usuarios pueden hacer con los contenidos de ese recurso.

Permisos compartidos

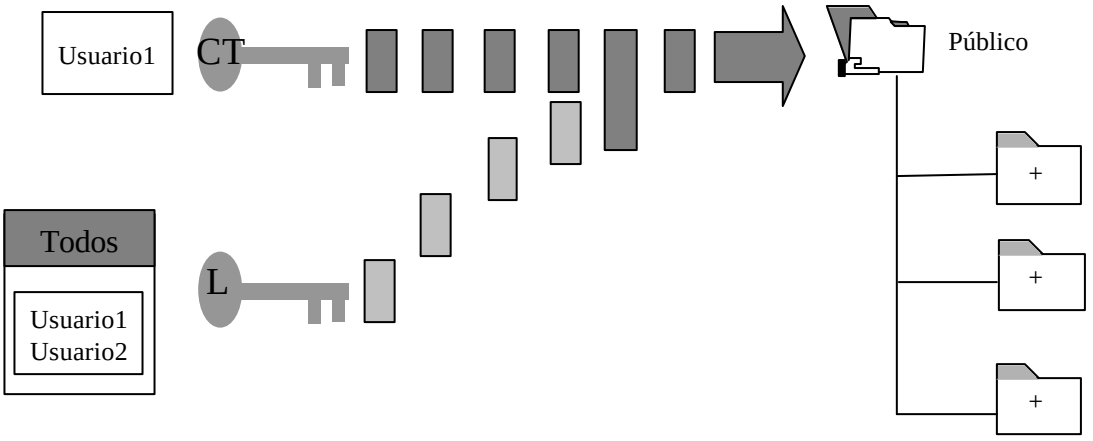
Hay que tener en cuenta las siguientes consideraciones:

- Los permisos en las carpetas compartidas se aplican a las carpetas, no a los ficheros individuales (ni subcarpetas)
- Los permisos en las carpetas compartidas no restringen el acceso a los usuarios que acceden a la carpeta de forma local
- Son la única forma de restringir el acceso a particiones FAT
- Por defecto, cuando se crea un recurso compartido se asigna el permiso control total a todos los usuarios

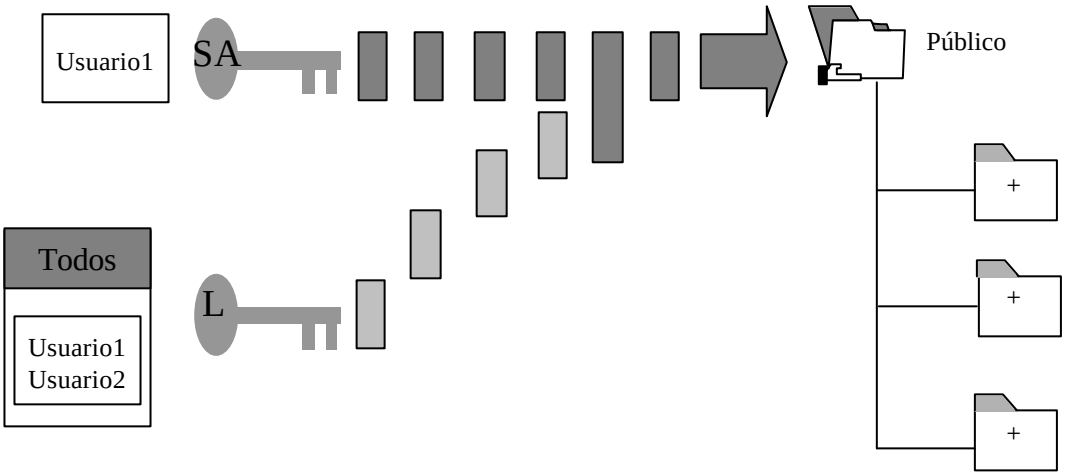
– Permisos aplicables:

Permiso	**Permite...**
Control total (por defecto)	-Igual que el derecho *cambio* - Cambiar los permisos de compartición - Apropiarse de un archivo cuando se encuentra en NTFS
Cambio	-Mismos derechos que *lectura*. - Crear, modificar o suprimir carpetas y archivos
Lectura	-Listar y recorrer las subcarpetas - Mostrar los datos y atributos de los ficheros - Ejecutar programas
Sin acceso	Se aceptan todas las conexiones pero la visualización y acceso al contenido están prohibidos

- **Aplicación de permisos**
  - Se pueden asignar permisos bien de forma individual o a través de grupos
  - El permiso efectivo es la combinación de los permisos



  - La única excepción a esta regla es el permiso "*sin acceso*". Este permiso prevalece sobre cualquier otro asignado al usuario o al grupo



- **Consideraciones para compartir carpetas**
  - Usar nombres intuitivos para las comparticiones
  - Usar nombres que puedan ser leídos por cualquier cliente
    - MS-DOS, Windows 3.x y Windows TG sólo soportan nombres 8.3
  - Organizar los recursos de disco de modo que carpetas con el mismo nivel de requerimientos de seguridad, se encuentre dentro de la misma jerarquía.
  - Asignar los permisos más restrictivos
  - Eliminar los permisos por defecto cuando se comparte una carpeta (control total por parte del grupo "*todos*"
- **Comparticiones administrativas**
  - **C$,D$,E$,…** El directorio raíz de cada unidad se comparte automáticamente para tareas administrativas
  - **Admin$** El directorio c:\winnt se comparte para administración remota

- **Seguridad local: Permisos NTFS**
  - Los permisos NTFS están disponibles sólo en unidades formateadas con NTFS.
  - Permite asignar permisos a carpetas y ficheros de forma individual
  - Permite proteger las carpetas y ficheros locales
- **Permisos en directorios**

Permisos NTFS	**Permisos asignados a los usuarios**
Leer	Ver ficheros Ver atributos de la carpeta, propietario y permisos y subcarpetas
Escribir	Crear nuevos ficheros y subdirectorios Cambiar atributos de la carpeta Ver propietario y permisos de la carpeta
Listar contenido carpeta	Ver los nombres de los ficheros y directorios en la carpeta
Leer y ejecutar	Operaciones permitidas con los permisos *Leer* y *Listar contenidos de la carpeta* Atravesar directorios (moverse a través de ellos)
Modificar	Operaciones permitidas por el permiso *escribir* y *Leer y Ejecutar* Borrar la carpeta
Control Total	Operaciones permitidas por el resto de los permisos Cambiar permisos, toma de posesión Borrar subcarpetas y ficheros

- **Permisos en ficheros**

Permisos NTFS	Permisos asignados a los usuarios
Leer	Leer el fichero, ver atributos, propietario y permisos
Escribir	Modificar el fichero Cambiar atributos del fichero, ver propietario y permisos
Leer y ejecutar	Operaciones permitidas con los permisos Ejecutar aplicaciones
Modificar	Modificar y borrar el fichero Operaciones permitidas por el permiso *escribir* y *Leer y Ejecutar*
Control Total	Operaciones permitidas por el resto de los permisos Cambiar permisos, toma de posesión

- **Listas de control de acceso (ACL)**
  - NTFS almacena una *lista de control de acceso* (*ACL*) para cada fichero y directorio de la unidad NTFS.
  - La ACL contiene una lista de todas las cuentas de usuarios y grupos a los que se le ha asignado permisos para ese directorio o fichero así como el tipo de acceso

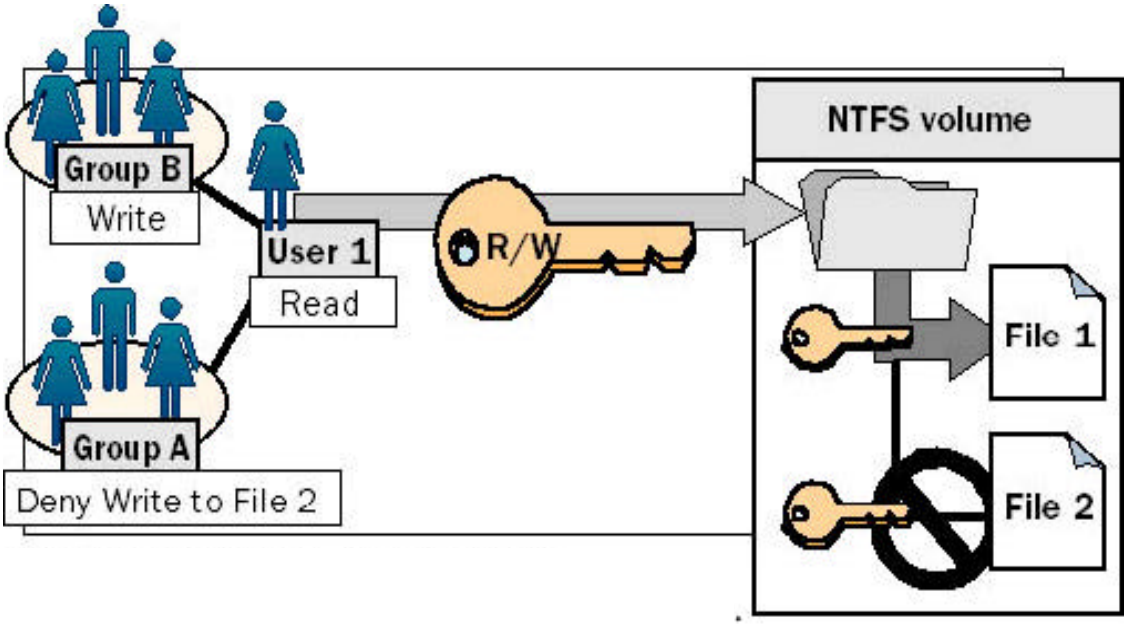
  - Cuando un usuario intenta acceder a un recurso, es necesario que éste contenga una entrada en la lista (*access control entry ACE*) para el usuario o algún grupo al que el usuario pertenece.
  - Si no existe ningún ACE para el usuario, se deniega el permiso.

- **Reglas para la asignación de permisos NTFS**

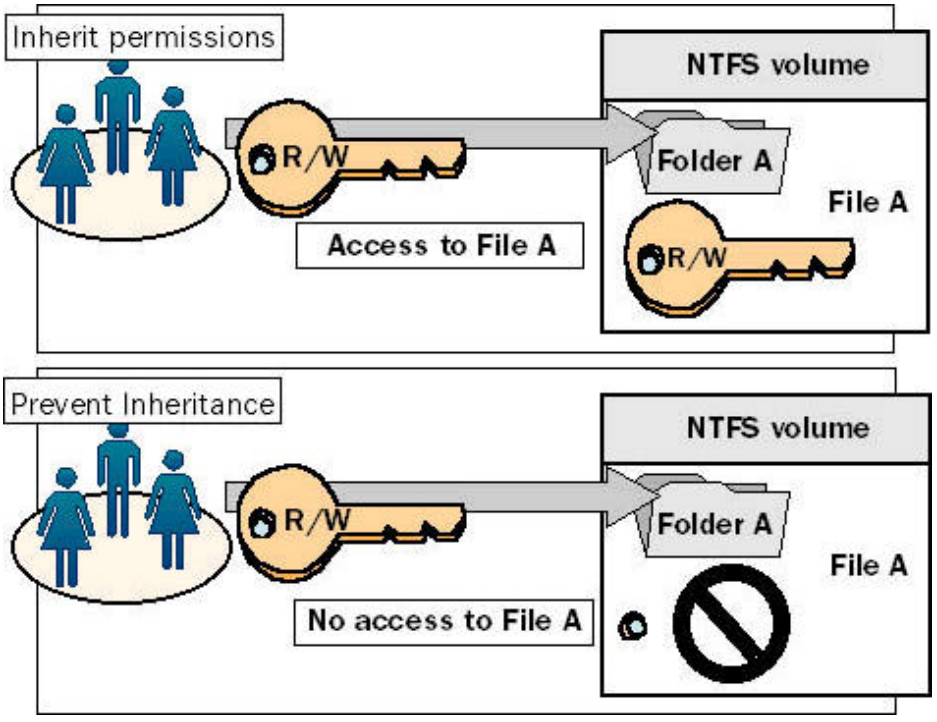
  Los usuarios pueden acceder a un determinado objeto sólo si tienen el permiso suficiente, ya como usuario individual o como miembro de algún grupo

  Los permisos son acumulativos. Si un usuario pertenece a varios grupos con distintos permisos, obtendrá la suma de ellos.

  La excepción es el permiso "*Sin acceso*" que prevalece sobre los demás



- **Herencia de permisos NTFS**
  - Por defecto, los permisos que se asignan a un directorio son heredados y propagados a los subdirectorios y ficheros que contiene.
  - Se puede prevenir que los permisos se hereden
  - Cuando se inhabilita la herencia de permisos en una carpeta, ésta se convierte en la carpeta padre, de modo que los hijos heredan sus permisos



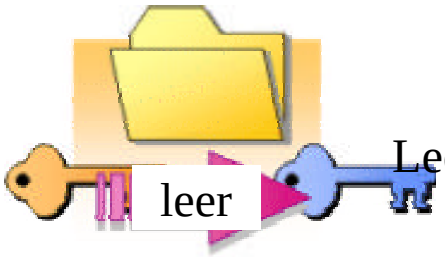
  - Opciones cuando se elimina la herencia:
    - Copiar: Copia los permisos del directorio padre y evita cualquier propagación posterior
    - Borrar: Sólo mantienen los permisos asignados explícitamente al objeto

Recomendaciones para asignación de permisos

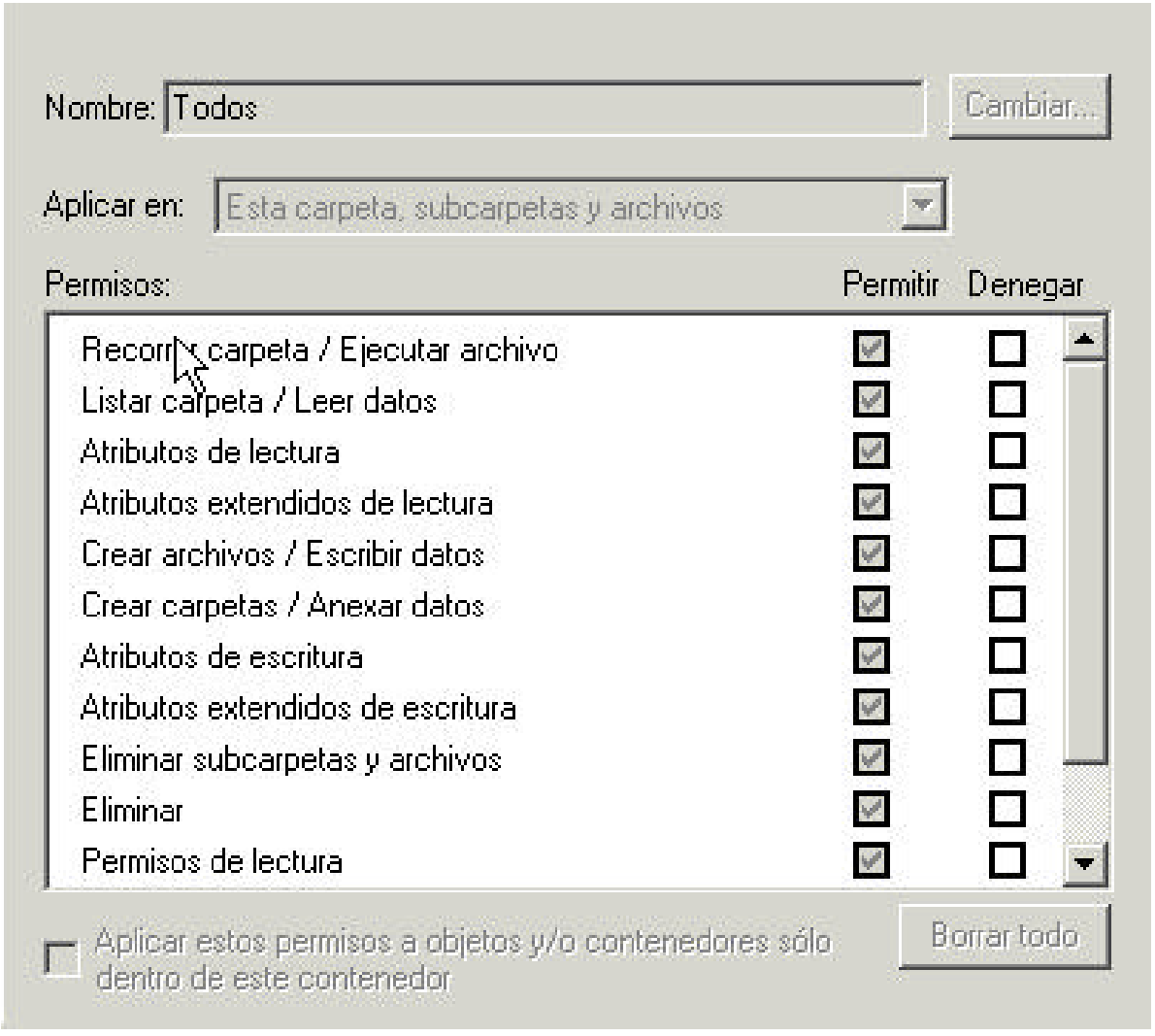
1. Agrupa los ficheros en las siguientes carpetas:
   - Aplicaciones
   - Datos
   - Directorios privados de usuarios

   Planifica la situación de estas carpetas: compartidas, distintas particiones,...
   - Asigna permisos a las carpetas, no a ficheros individuales
   - Distintas políticas de respaldo
2. Asigna los permisos más restrictivos que permitan el acceso deseado
3. Asigna los permisos a grupos en lugar de a usuarios individuales
4. Cuando se asignan permisos a carpetas de aplicación, utilizar el permiso “Leer y Ejecutar”
5. Evitar la herencia de permisos a nivel del directorio “home” de los usuarios (así se permite que los usuarios establezcan sus permisos)
6. Cuando asignes permisos a carpetas públicas, asignar los permisos “leer y ejecutar” y “escribir” a los grupos de usuarios y el permiso “control total” al grupo de sistema “CREATOR OWNER”
7. Asignar permisos sin acceso cuando se desea denegar el acceso a un usuario o grupo en concreto

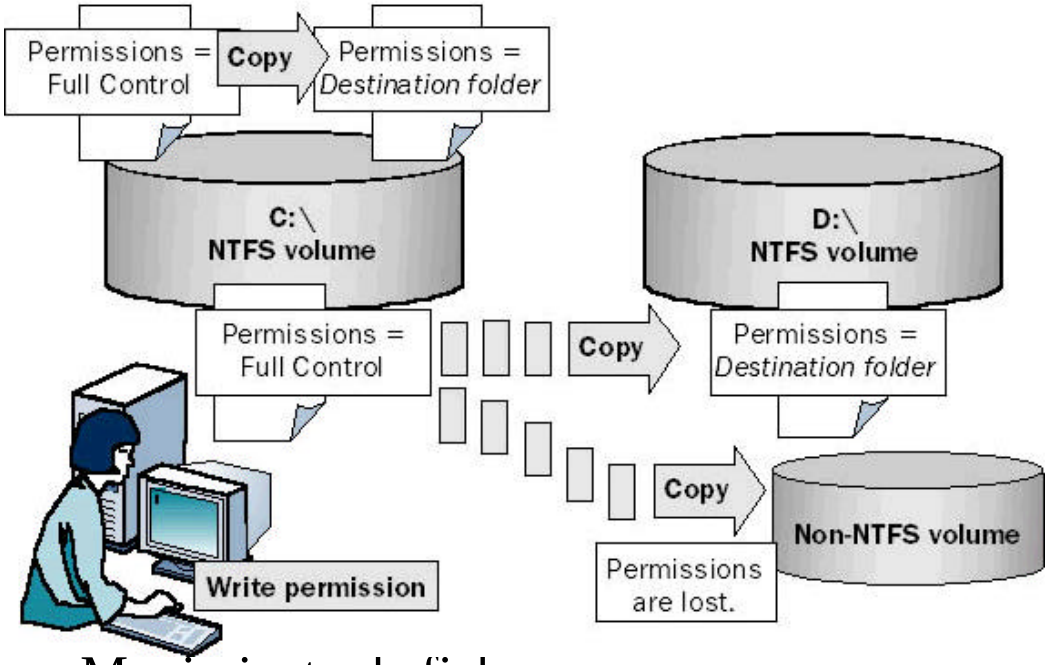
- **Permisos especiales**
  - Normalmente los permisos estándar son suficientes para la mayoría de las situaciones.
  - En caso contrario, se pueden asignar/denegar permisos individuales/especiales:



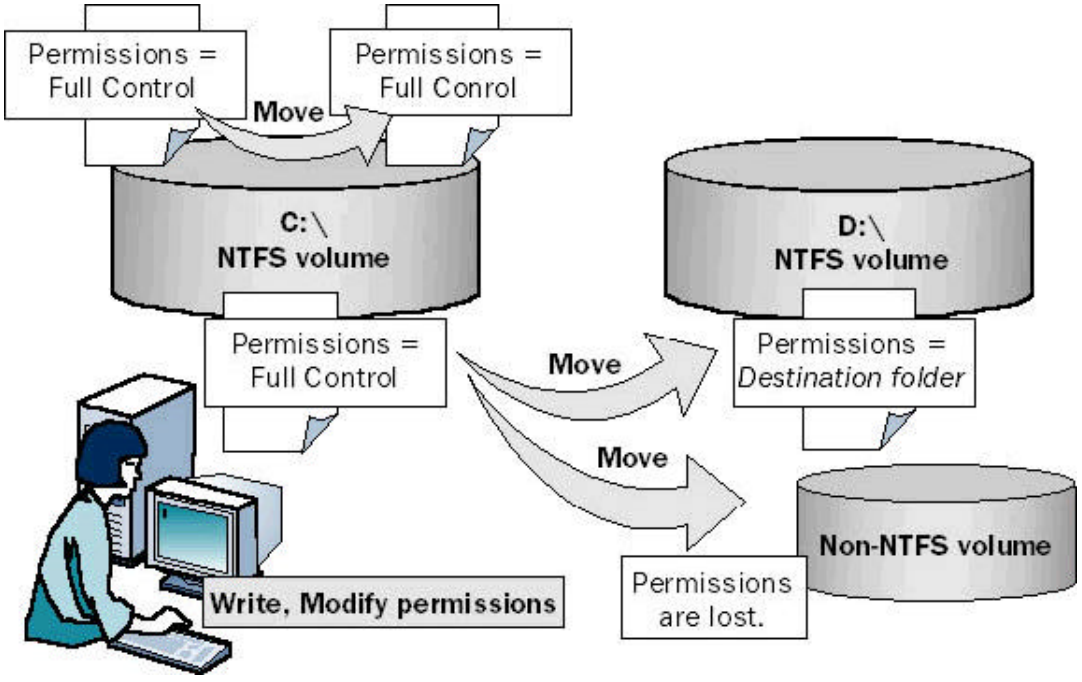
Leer datos
Lectura de atributos
Lectura extendida de atributos
Permisos de lectura



- **Copia y movimiento de ficheros**
  - Copia de ficheros: NTFS crea un nuevo fichero

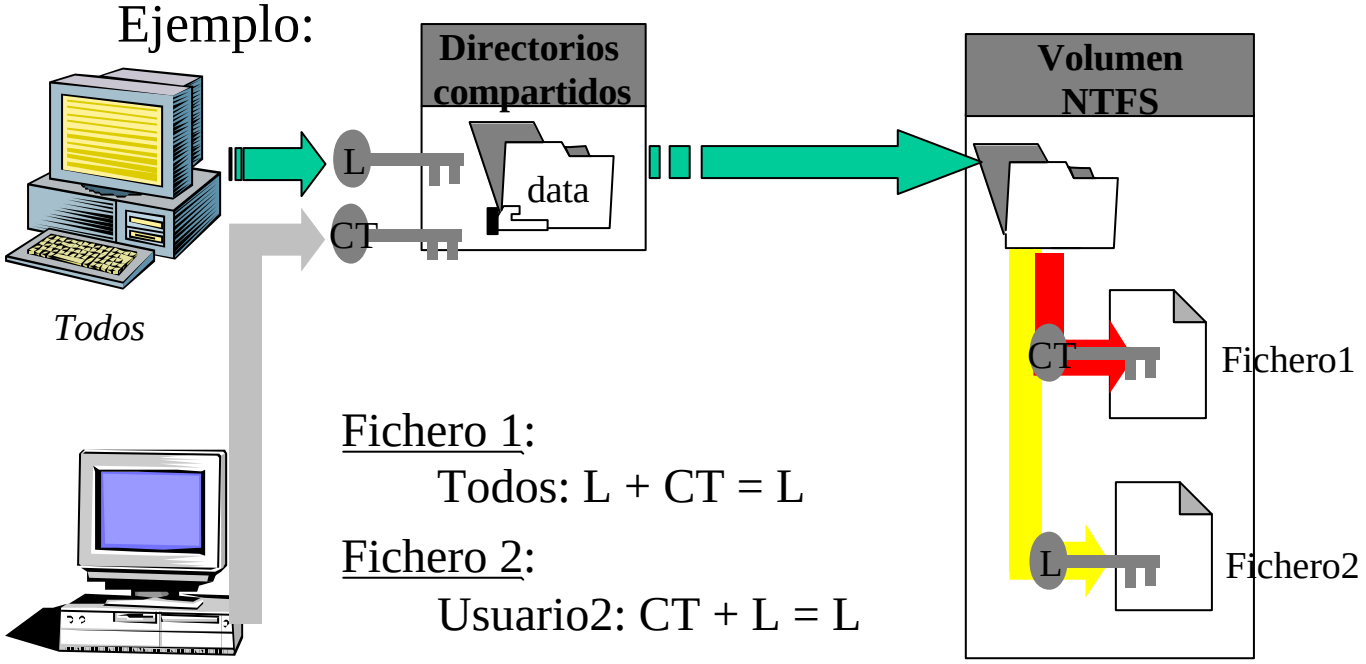


  - Movimiento de ficheros:
    - Permisos de modificación en carpeta origen
    - Permisos de escritura en carpeta destino



- **Combinación de los permisos NTFS y compartidos**
  - Sólo se aplican cuando se accede al recurso de forma remota
  - El permiso efectivo es el más restrictivo de los dos.

Ejemplo:



Fichero 1:
Todos: L + CT = L

Fichero 2:
Usuario2: CT + L = L

Recomendaciones:

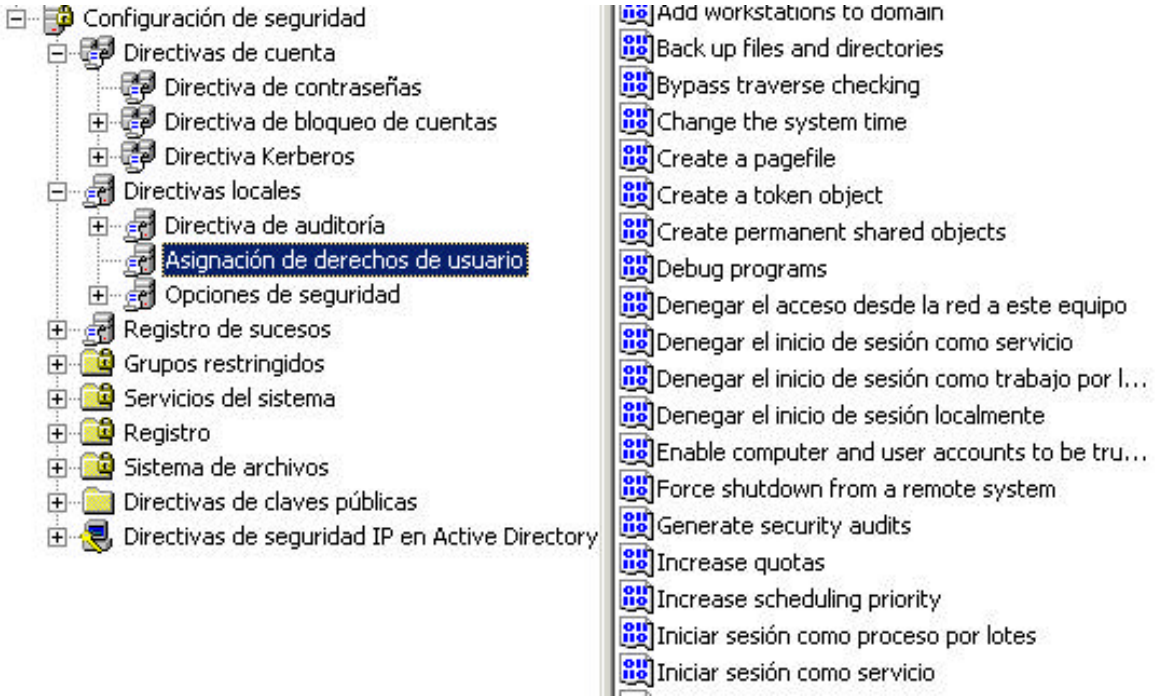
- Asignar “control total” al recurso compartido:
  - Elegir “usuarios” en lugar de “todos”
- Controlar los permisos efectivos con los NTFS

- **Introducción a la configuración de seguridad**
  - La configuración de seguridad permite establecer políticas de seguridad para el sistema (ordenadores, usuarios).
  - Estas políticas se establecen usando las “directivas de grupo” de Windows 2000
  - Existen una serie de políticas predefinidas en función de los requerimientos del sistema (por defecto se asigna una de estas políticas predefinidas)
  - Una política de seguridad está compuesta por la configuración asignada a cada una de las áreas de seguridad soportadas en W2k:
    - **Directivas de cuentas**
    - **Directivas locales**
    - **Registro de sucesos**
    - **Grupos restringidos**
    - Servicios del sistema
    - Registro
    - Sistema de ficheros
    - Directiva de claves públicas
    - Directivas de seguridad IP

- **Directivas de cuentas:**
  - Por defecto, las directivas de cuentas en el DA se heredan de las directivas aplicadas al dominio raíz
  - Cuando se aplica una directiva de cuentas en una OU, ésta afectará la directiva local de todos los **equipos** contenidos en esa OU (Ejemplo: Controladores de dominios)
  - No aplicar directiva de cuentas o OU's que sólo contengan usuarios (heredan las directivas del controlador de dominio)
  - Las directivas se aplican en el siguiente orden: primero las locales, y a continuación, las establecidas para los sitios, dominios y por último, la de las OU's
  - Esta área de seguridad controla:
  - **Directivas de contraseñas:** Duración de las contraseñas, longitud mínima, refresco,...
  - **Directivas de bloqueos de cuentas:** Determina quién y cuándo una cuenta se bloquea: número de intentos, tiempo de bloqueo,...
  - **Directiva Kerberos:** Configuración relacionada con Kerberos (tiempo de vigencia de los tickets, ...)

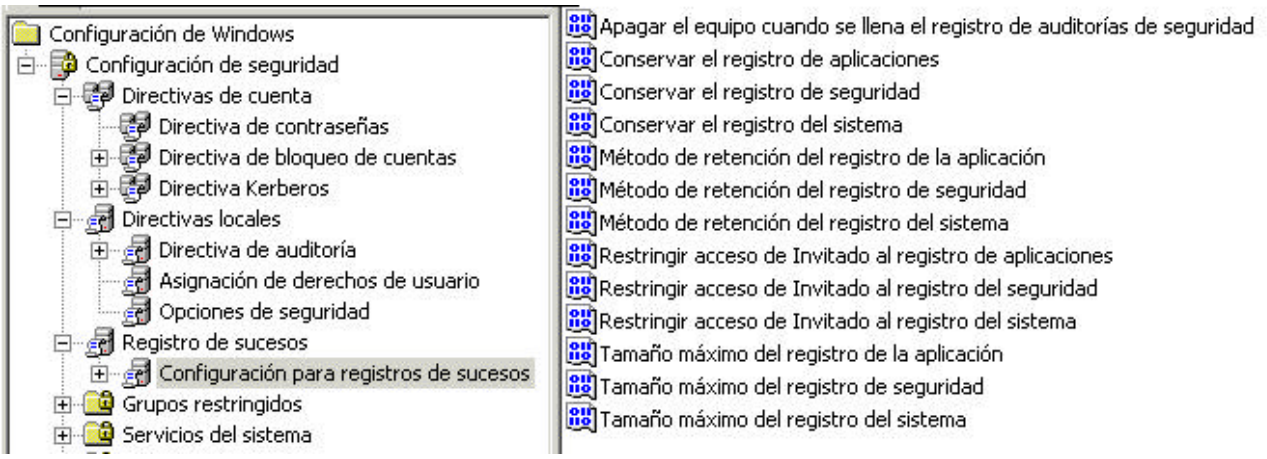
- # Directivas locales
  - Hacen referencia a configuración de seguridad que se establece al ordenador en el que el usuario hace el logon.
  - Esta área de seguridad controla:
    - **Directivas de auditoría:** Determina qué eventos de seguridad deben registrarse (intentos fallidos, accesos correctos,...). Estos eventos pueden visualizarse posteriormente con el "Visor de Sucesos"
    - **Asignación de derechos de usuarios.** Determina los usuarios con privilegios de acceso o de realización de tareas concretas en el ordenador

      Estos derechos permiten a los usuarios incluidos, a realizar ciertas operaciones: copias de seguridad, gestión de usuarios,...



- **Opciones de seguridad:** Permite establecer mecanismos de seguridad en el ordenador, tales como el cifrado de la información, los nombres para las cuentas de Administrador e Invitado, acceso a unidades extraíbles, instalación de drivers,...

- **Registro de sucesos**
  - Permite definir los atributos relacionados con los registros (logs) de sucesos:
    - Tamaño máximo
    - Derechos de acceso a los registros
    - Retención de registros



- **Grupos restringidos**
  - Permite asegurar la pertenencia de usuarios a grupos: Cuando se aplica la política, todos los usuarios y grupos no especificados, son eliminados
  - Útil para la pertenencia de grupos claves como “administradores, operadores de cuentas,...”