

# **CURSO 2016-2017**

**SISTEMAS OPERATIVOS EN RED (160 horas)**

**Matea Calleja**



## 3- Gestión de usuarios, grupos y equipos

- Disponemos del dominio sor.es
  - IP 10.0.0.1
  - Incorporar 2 clientes W7 a dominio (PC1 y PC2)

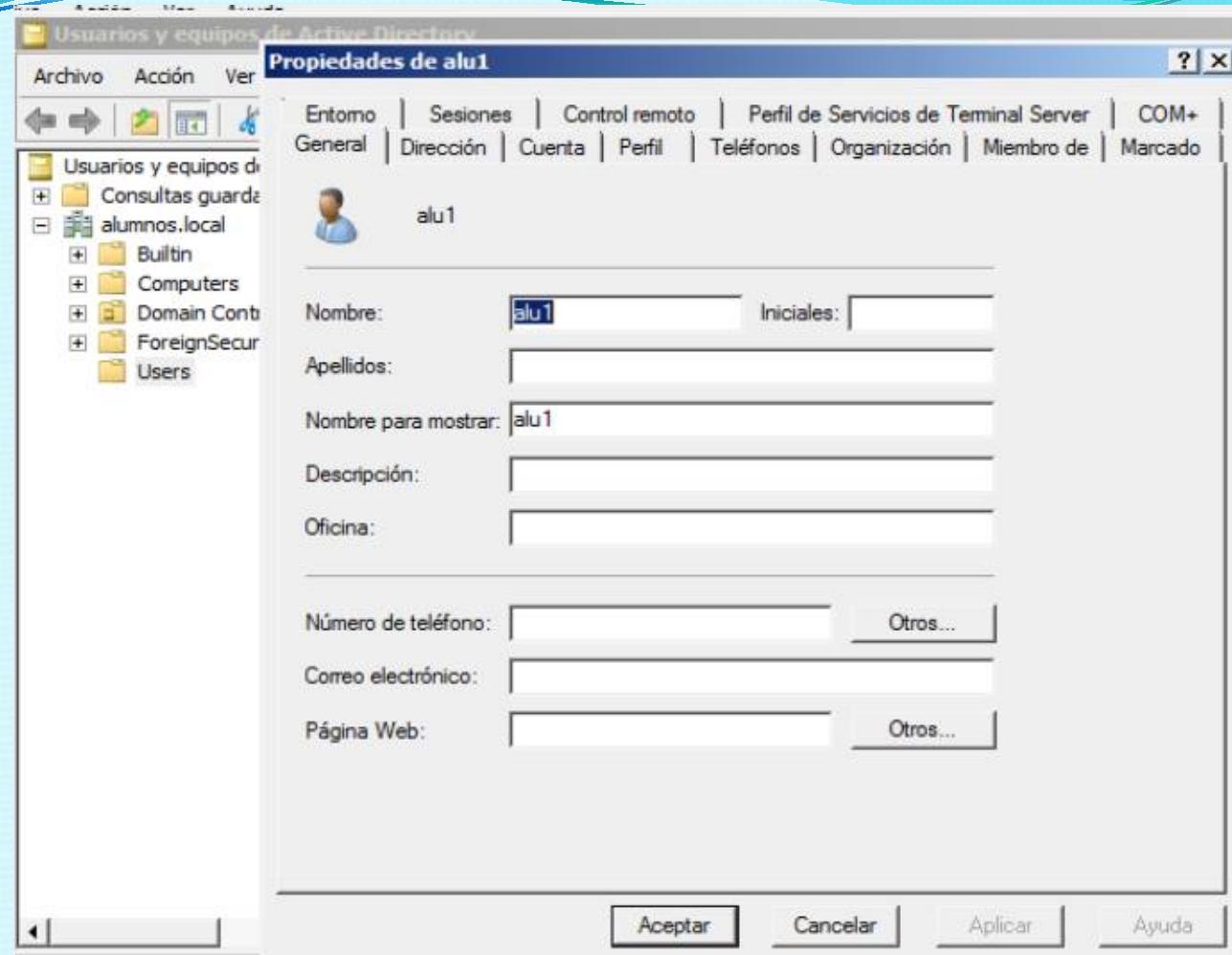
# 1. USUARIOS

## 1.1 Clasificación

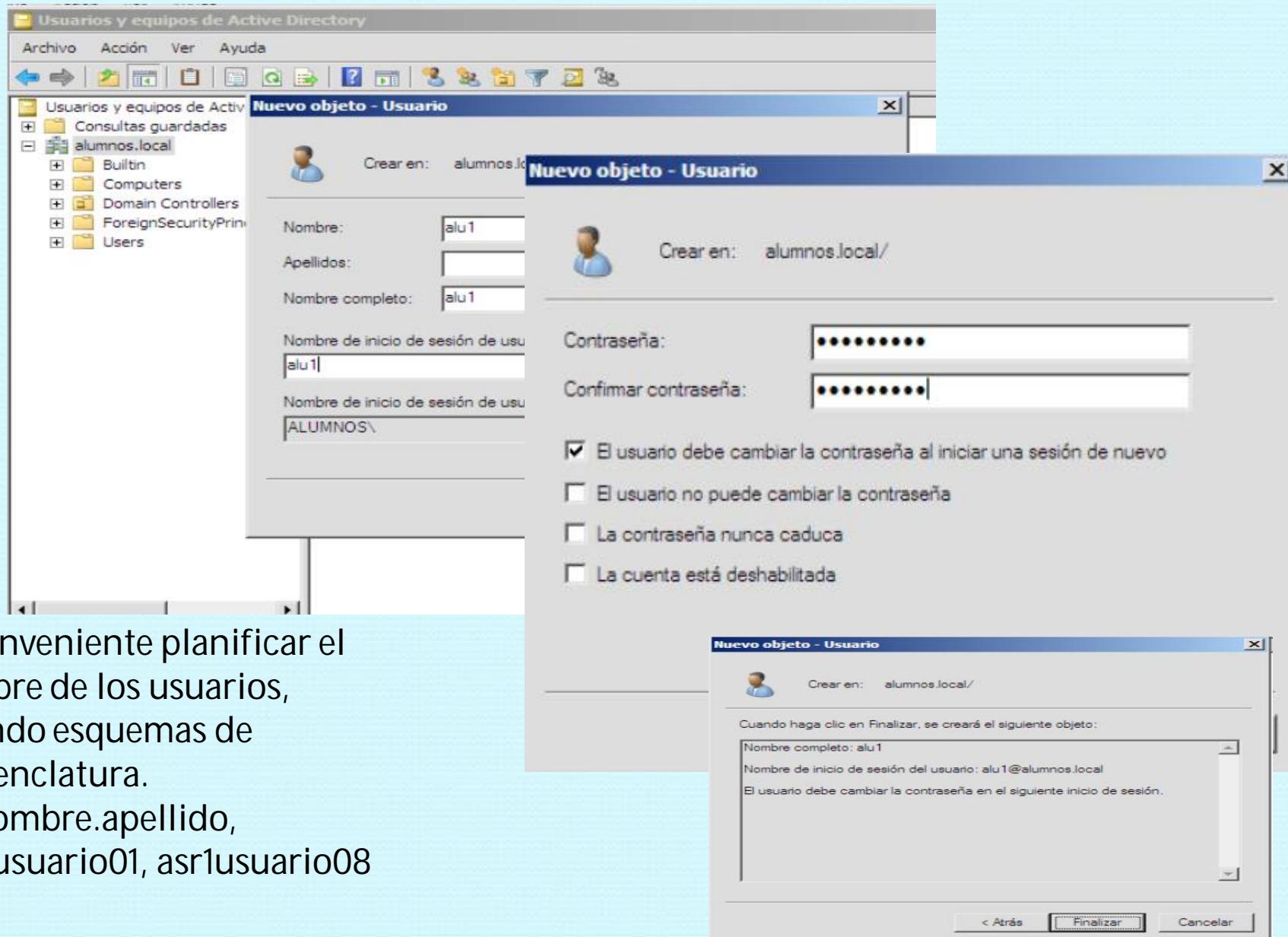
- **Usuario predeterminado:** (por el sistema loc/dom), se crea cuando se configura el dominio, pueden verse en el contenedor users.
- **Usuario local:** es el usuario de un equipo que no pertenece a un dominio
- **Usuario (de dominio),** residen en la base de datos de AD. Sus cuentas son comunes a todos equipos del dominio.
- **InetOrgPerson:** compatibilidad con LDAP (protocolo ligero de acceso a directorio)
- **Contacto:** cuentas únicamente de correo electrónico

## Usuarios predeterminados

- **Administrador:** esta cuenta tiene todos los privilegios sobre el dominio, por defecto es miembro de todos los grupos predeterminados del dominio.
- **Invitado:** es una cuenta para utilizar personas que no tienen cuenta en el dominio, por defecto está deshabilitada. Se la pueden conceder más permisos y derechos.



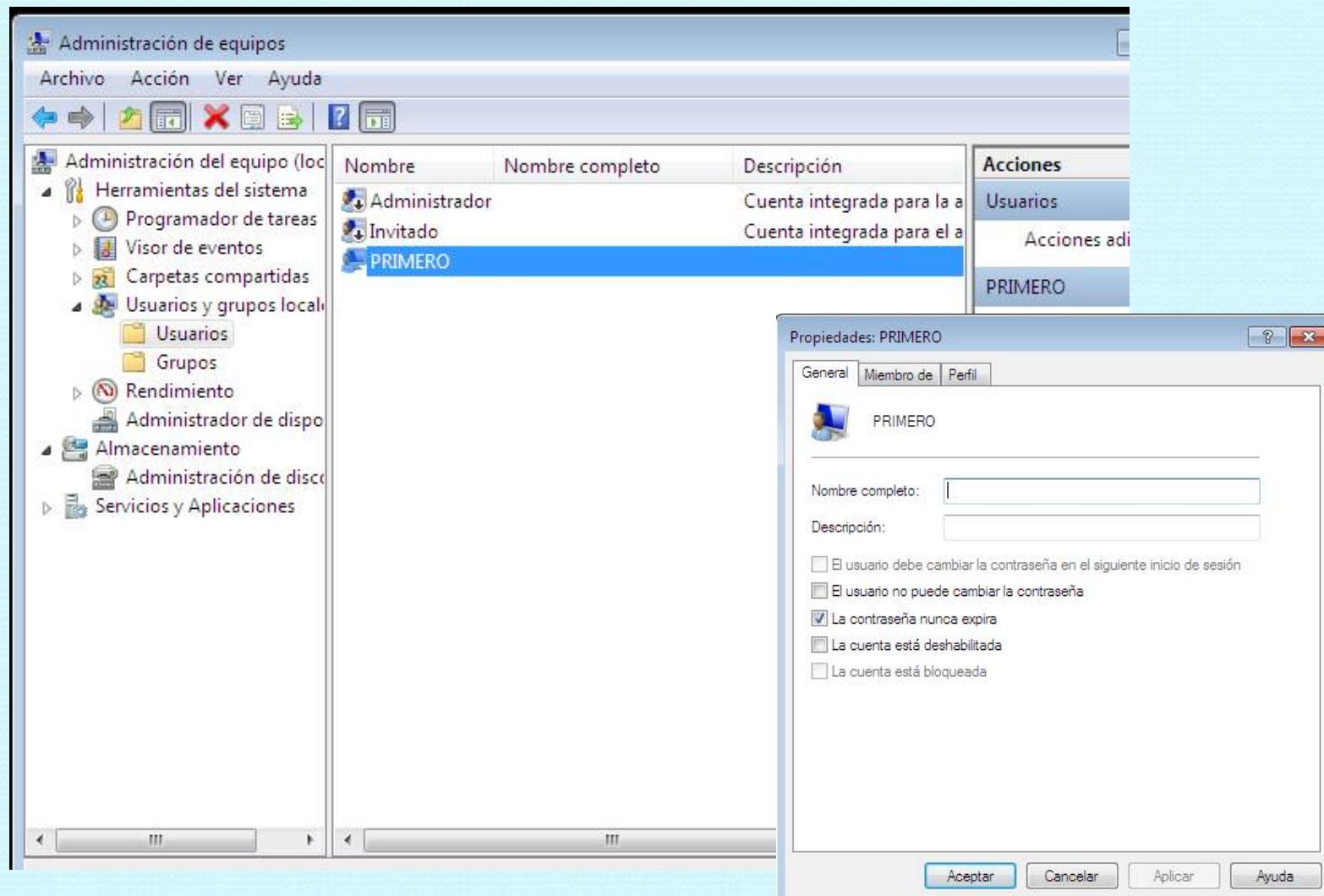
## 1.2 Crear usuarios



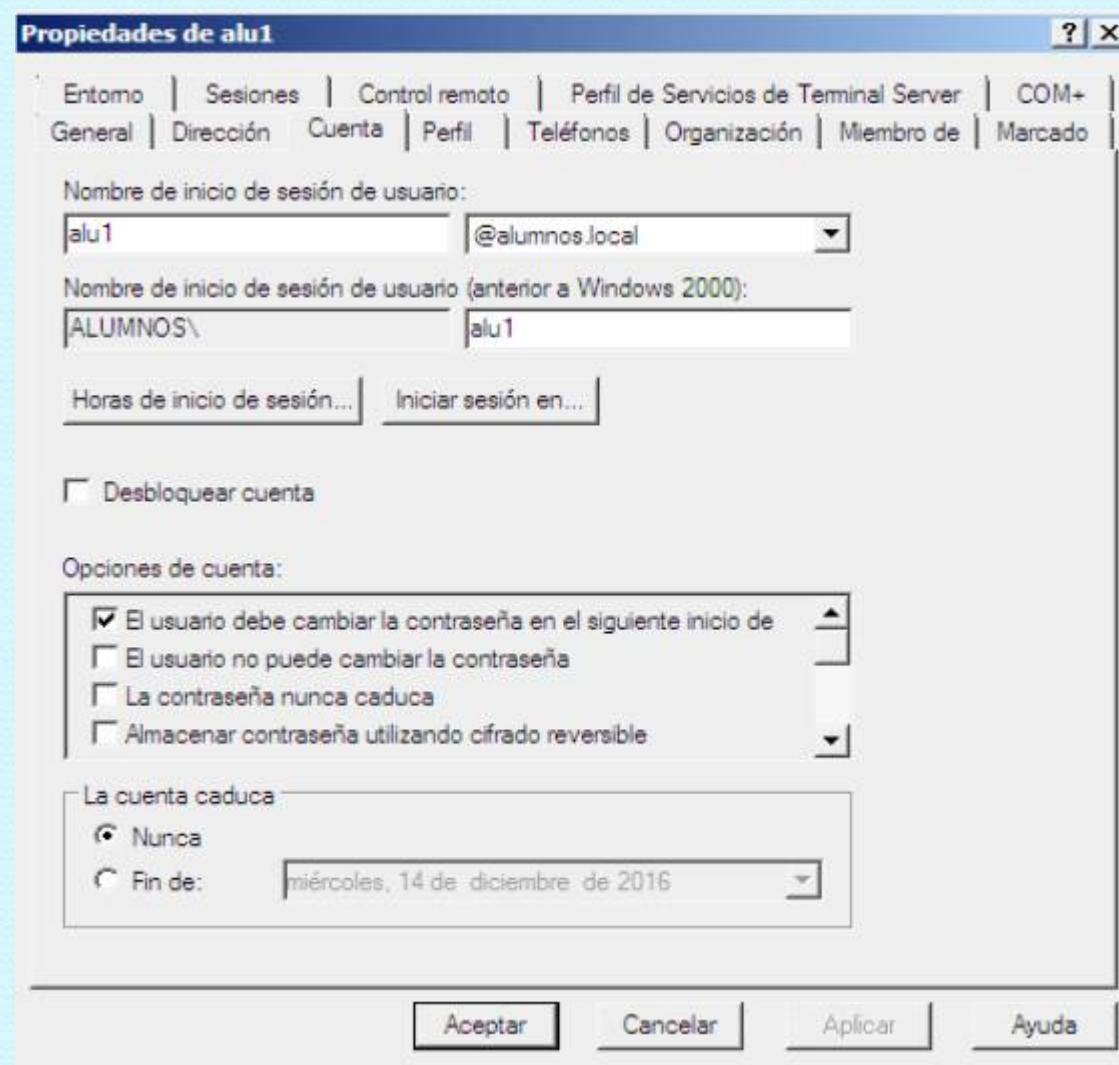
### 1.3.- Ambitos

- Un Controlador de dominio sólo tiene usuarios del dominio (no locales).
- Un equipo dentro del dominio puede definir además usuarios locales para acceso a sus recursos.
- Un equipo no incorporado a dominio sólo podrá tener usuarios locales.

Los usuarios locales de un equipo los podemos ver a través de la herramienta “Administración de equipos”



## 1.4.- Opciones de las cuentas de usuario (dominio)



Properties of alu1

Entorno | Sesiones | Control remoto | Perfil de Servicios de Terminal Server | COM+ General | Dirección | Cuenta | Perfil | Teléfonos | Organización | Miembro de | Marcado

Nombre de inicio de sesión de usuario:  
alu1 @alumnos.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):  
ALUMNOS alu1

Horas de inicio de sesión... Iniciar sesión en...

Desbloquear cuenta

Opciones de cuenta:

El usuario debe cambiar la contraseña en el siguiente inicio de sesión  
 El usuario no puede cambiar la contraseña  
 La contraseña nunca caduca  
 Almacenar contraseña utilizando cifrado reversible

La cuenta caduca  
 Nunca  
 Fin de: miércoles, 14 de diciembre de 2016

Almacenar contraseña utilizando cifrado reversible

La tarjeta inteligente es necesaria para un inicio de sesión interactivo

La cuenta es importante y no se puede delegar

Usar tipos de cifrado DES de kerberos para esta cuenta

Esta cuenta admite cifrado AES de Kerberos de 128 bits.

Esta cuenta admite cifrado AES de Kerberos de 256 bits.

**La cuenta está deshabilitada o bloqueada:** A veces, un usuario introduce su contraseña de forma errónea en varios intentos. Esto provoca el bloqueo de su cuenta. En este caso, esta casilla aparecerá habilitada. Para desbloquear la cuenta, un Administrador debe desmarcar esta casilla.

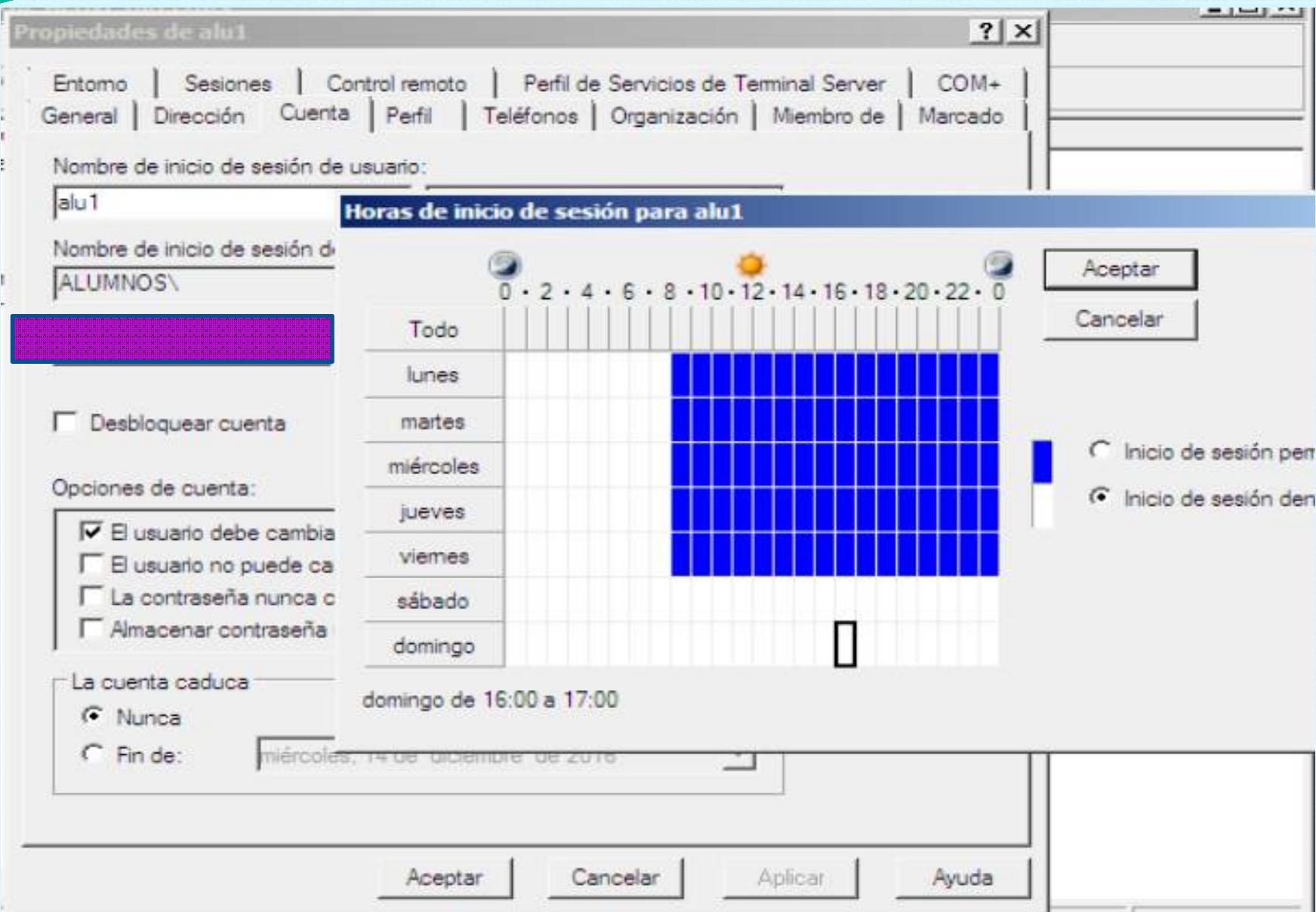
**El usuario debe cambiar la contraseña en el próximo inicio de sesión:** Si esta casilla está marcada, el sistema obligará al usuario a cambiar la contraseña la próxima vez que inicie sesión. Esto es muy útil para obligar a los usuarios y usuarias a cambiar la contraseña de vez en cuando, o a establecer una contraseña propia, desconocida para el administrador, la primera vez que utilizan el sistema.

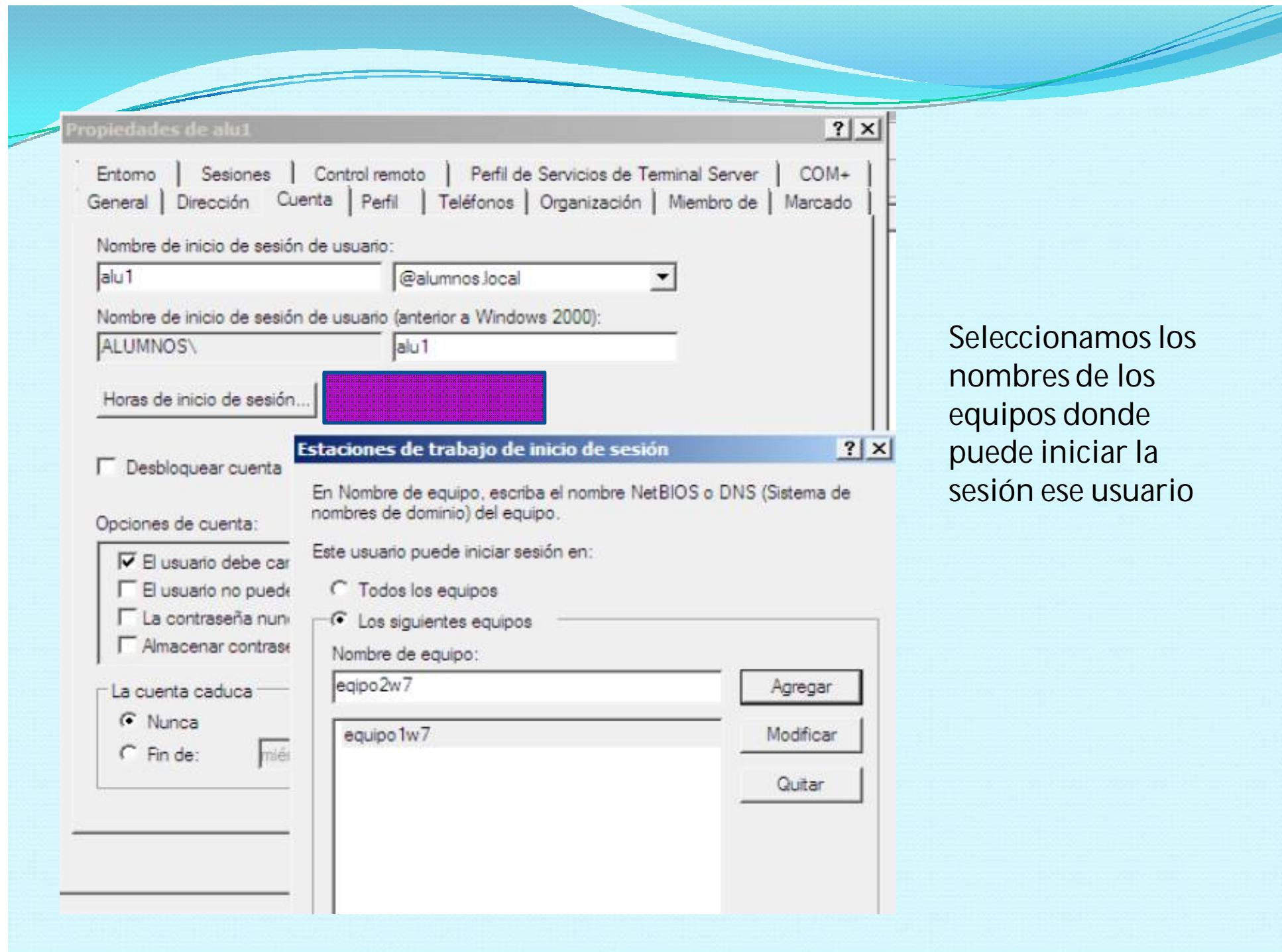
**El usuario no puede cambiar la contraseña:** Si se marca, el usuario no puede cambiar su propia contraseña.

**La contraseña nunca caduca:** Hace que, para esta cuenta de usuario, no se tenga en cuenta el tiempo de caducidad de la contraseña. Si no está marcada esta opción, el usuario o la usuaria estará obligado a cambiar la contraseña cada cierto tiempo.

**Almacenar la contraseña utilizando cifrado reversible:** Algunos sistemas operativos, como por ejemplo los de Apple, pueden almacenar las contraseñas en texto plano. En caso de tener ese tipo de sistemas en nuestro do

**La cuenta expira:** Si se establece una fecha de expiración, la cuenta se deshabilitará automáticamente llegado ese día.





Seleccionamos los nombres de los equipos donde puede iniciar la sesión ese usuario

## Iniciar sesión en equipo local W7

Como usuario local:

EQUIPO\usuariolocal

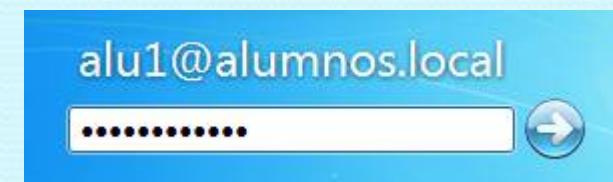
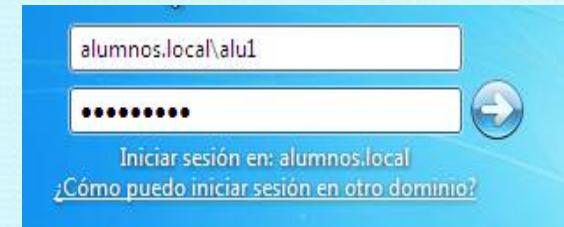


Como usuario del dominio:

DOMINIO\usuariodomínio

Ó

usuariodomínio@dominio



- Ejercicio:

- Dominio sor.es con 2 clientes W7
- Crear usuarios: alu01, alu02, profe01 y profe02. Comprobar que pueden entrar desde cualquier equipo miembro del dominio
- Configurar “Estaciones de trabajo de inicio de sesión” para que el usuario solo pueda entrar en el equipo que le corresponda
  - PC1:
    - Alu01
    - Alu02
  - PC2:
    - Profe01
    - profe02
- Restringir el acceso en la hora actual y probar que no puede entrar.
- Poner una fecha de deshabilitación y reactivar la cuenta.

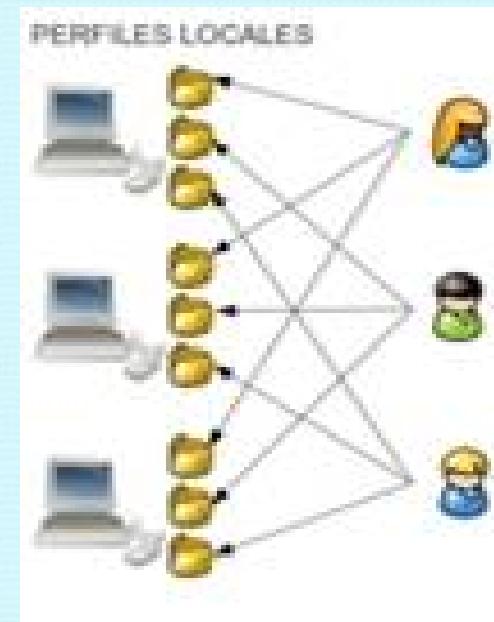
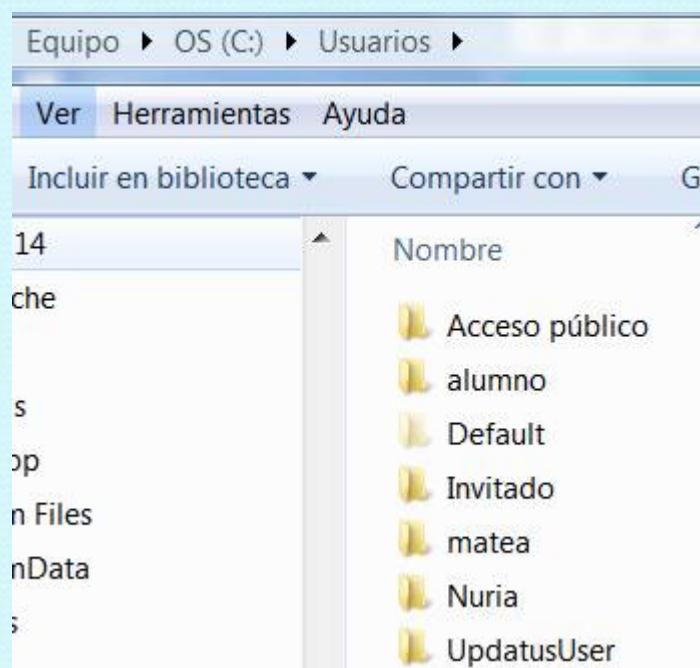
## 2. -Perfiles de usuario.

- Contiene opciones globales e información de configuración, normalmente referidos al escritorio, la barra de tareas y el menú inicio. Cuando un usuario cambia el aspecto, comportamiento, etc. de alguno de estos elementos, esos cambios se almacenan en su perfil.
- Existen tres tipos de perfiles:
  - **Locales**
  - **Móviles**
  - **Obligatorios**

## 2.1- Tipos de perfiles de usuario. Perfiles Locales.

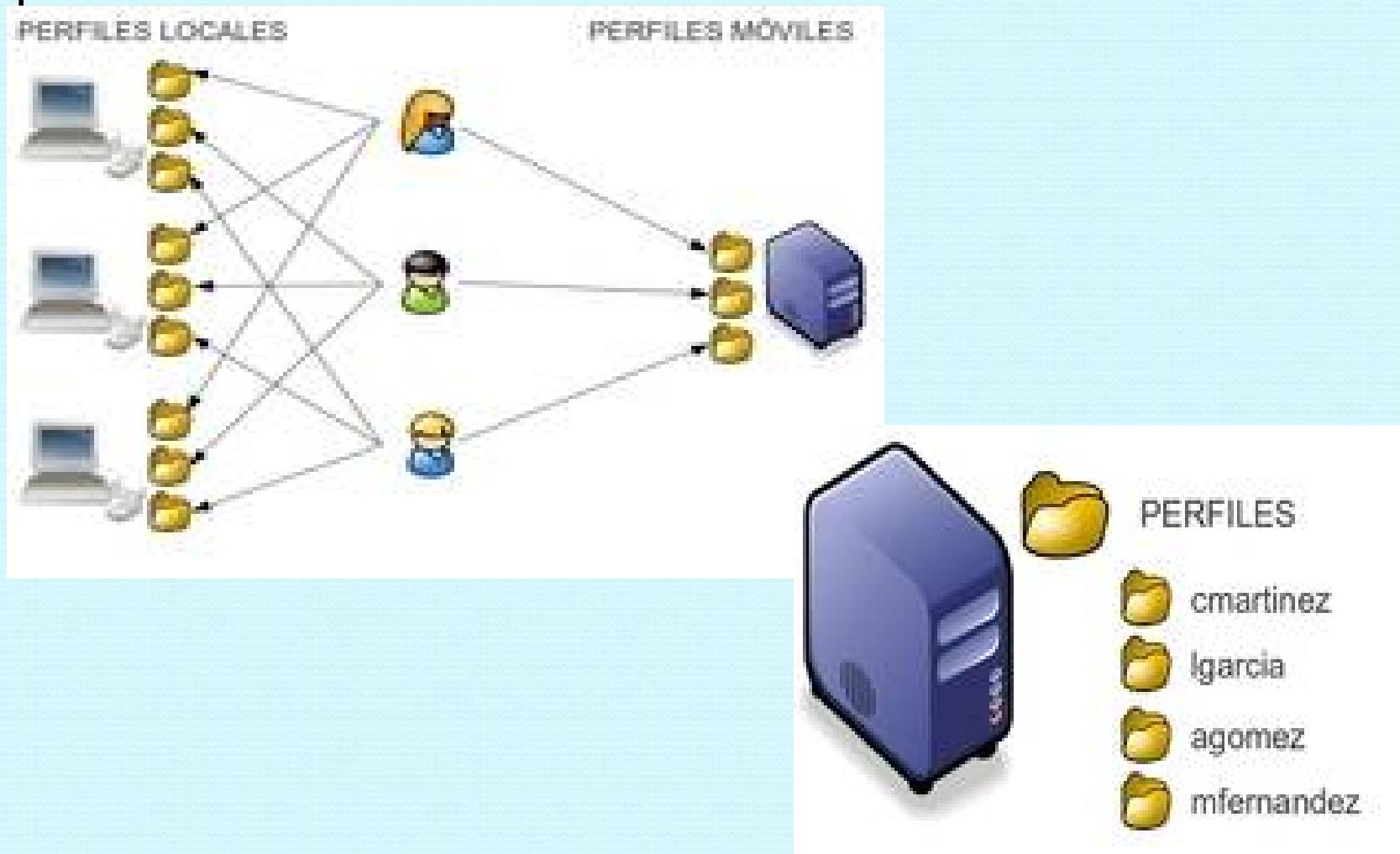
El perfil de usuario es el conjunto de configuraciones personalizadas que el usuario hace en el sistema de operativo para sus sesiones de usuario: escritorio, fuentes, configuración de programas...

- Por defecto se almacena en "C:\Users".

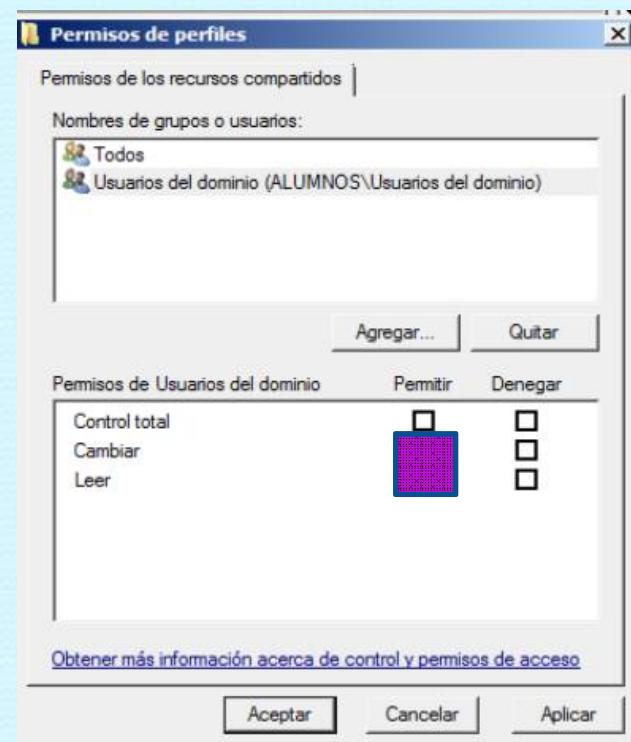
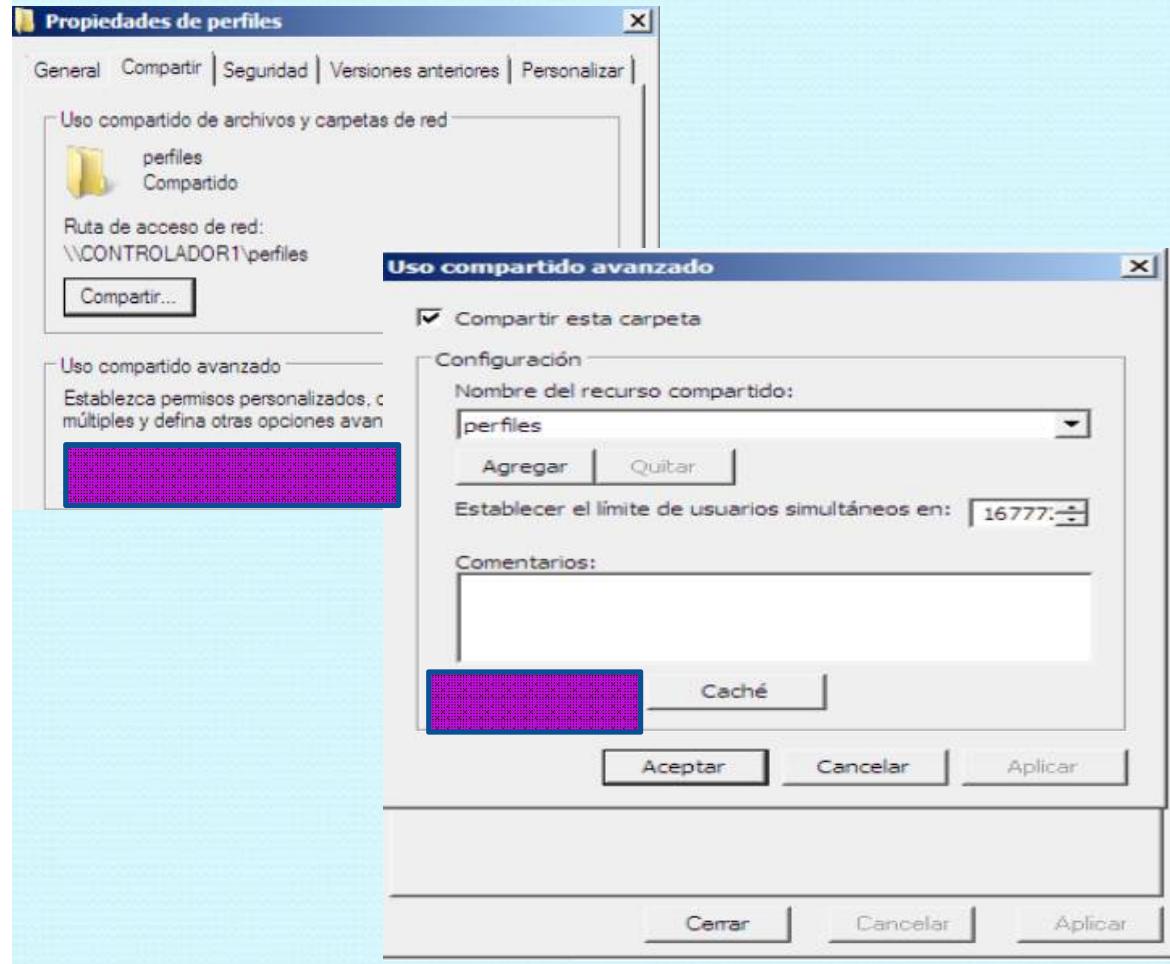


## 2.2 -Perfiles móviles.

Un perfil móvil es un perfil guardado en el dominio en una carpeta compartida, que se exporta a todo equipo en el que el usuario inicie sesión.



Para almacenar el perfil, debemos tener una carpeta compartida en un servidor. Creamos una carpeta **PERFILES** (puede tener otro nombre en el dominio y la compartimos (Todos ->Control Total)



## Administradores -> Control Total Usuarios del Dominio-> Lectura/Escritura

General Compartir Seguridad Ver  Propiedades de perfiles

Uso compartido de archivos y carpetas  
perfiles  
Compartido  
Ruta de acceso de red:  
\\CONTROLADOR1\perfiles  
Compartir...

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: C:\perfiles

Nombres de grupos o usuarios:

- CREATOR OWNER
- SYSTEM
- Administradores (ALUMNOS\Administradores)
- Usuarios (ALUMNOS\Usuarios)

Para cambiar los permisos, haga clic en Editar.

Permisos de Usuarios Permitir Denegar

Control total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modificar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lectura y ejecución	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mostrar el contenido de la carpeta	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lectura	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ecritura	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Obtener más información acerca de control y permisos de acceso

Acceptar Cancelar Aplicar

Permisos de perfiles

Seguridad

Nombre de objeto: C:\perfiles

Nombres de grupos o usuarios:

- CREATOR OWNER
- SYSTEM
- Administradores (ALUMNOS\Administradores)
- [REDACTED]

Agregar... Quitar

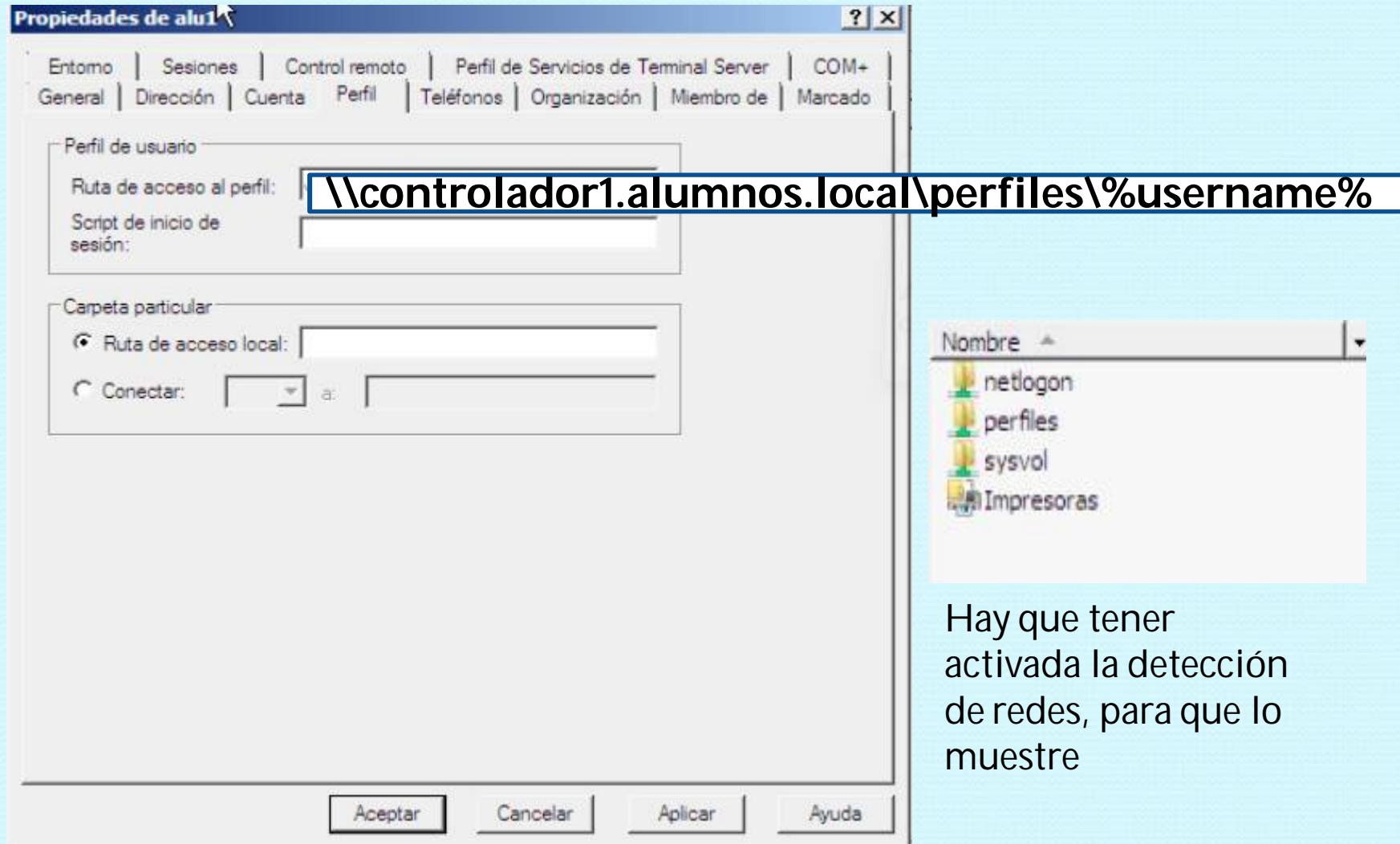
Permisos de CREATOR OWNER Permitir Denegar

Modificar	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lectura y ejecución	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mostrar el contenido de la carpeta	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lectura	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ecritura	<input type="checkbox"/>	<input checked="" type="checkbox"/>

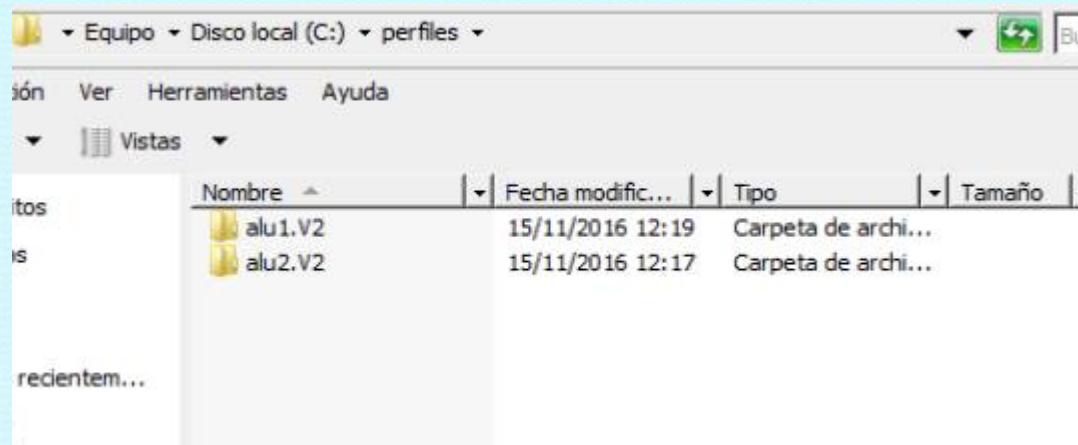
Obtener más información acerca de control y permisos de acceso

Acceptar Cancelar Aplicar

Modificamos en la cuenta del usuario su ruta de acceso al perfil:

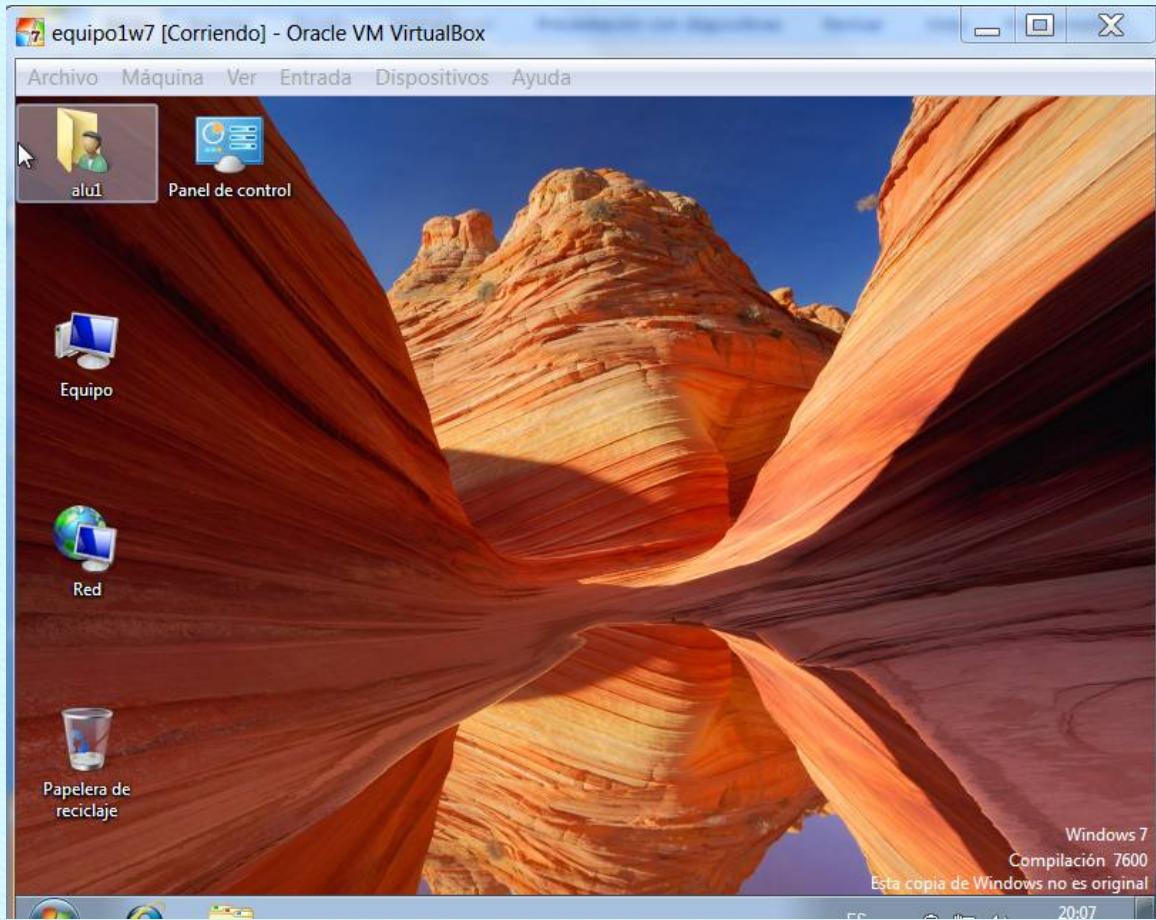


Para comprobar, entramos como usuario "alu1" en un cliente del dominio, y modificamos el escritorio (iniciamos sesión para comprobar que lo guarda ) y que se almacena en el servidor:



Cerramos sesión, y veremos como se crea el perfil en la carpeta compartida

~~COMPROBACIÓN (2): Entramos como “alu1” en el otro equipo cliente, y vemos que se traen los ficheros del perfil~~



PROBLEMA:

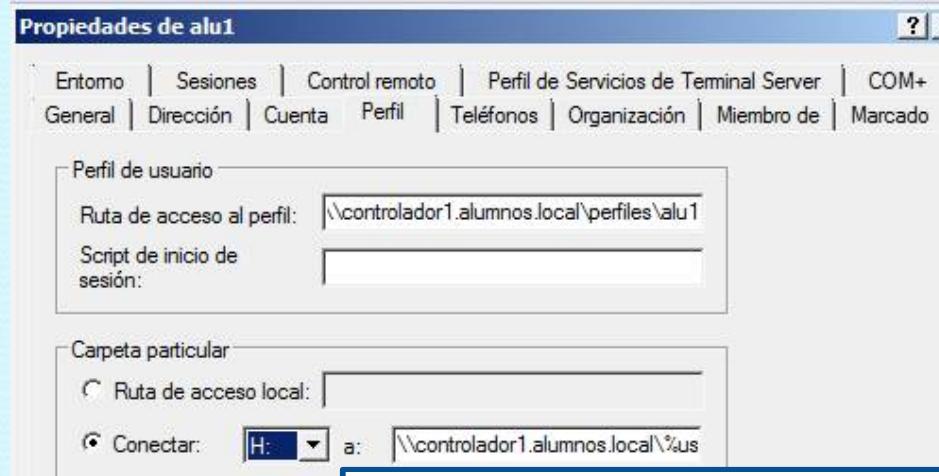
Si los ficheros son grandes, podemos saturar la red y el servidor.

Creamos una nueva carpeta compartida para las carpetas particulares de los usuarios

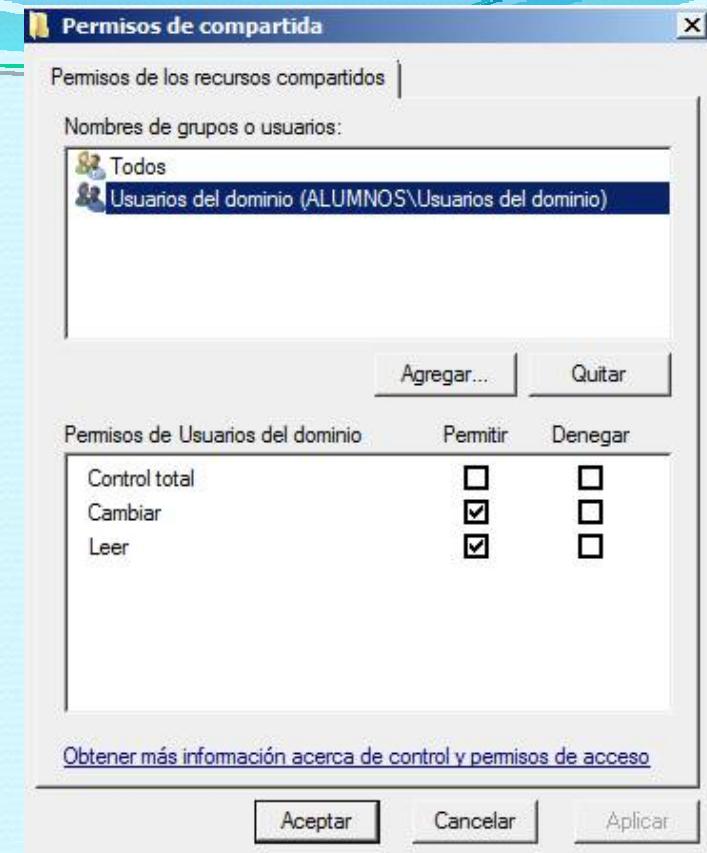
`\controlador1.alumnos.local\COMPARTIDA`

- Permisos de red:  
Todos -> Control Total
- Pestaña de seguridad:  
Administradores -> Control Total  
Usuarios del Dominio -> Lectura/Escritura

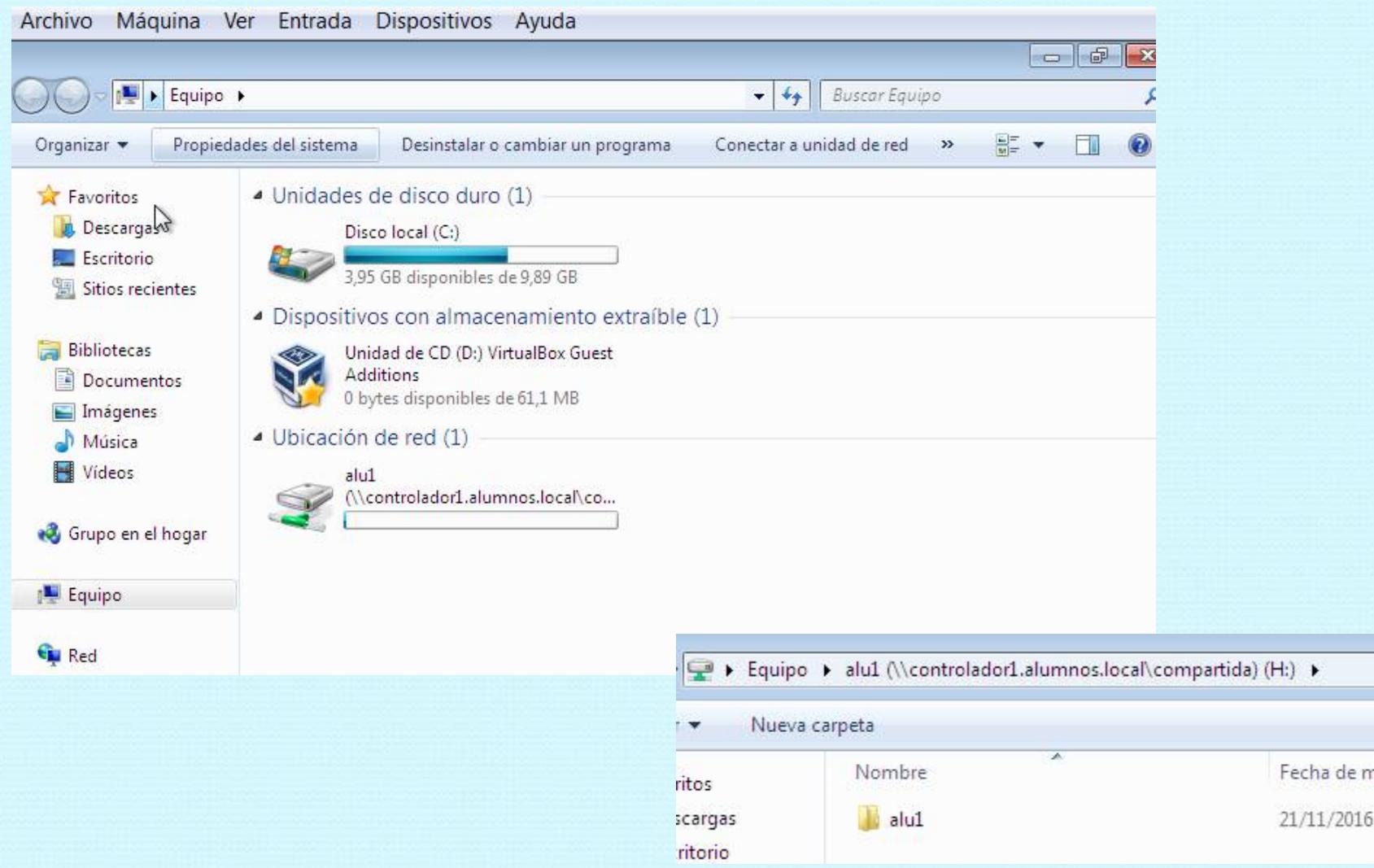
En el perfil de cada usuario asignamos una unidad de red a la carpeta compartida



`\controlador1.alumnos.local\compartida\%username%`



COMPROBACIÓN: iniciando la sesión, veremos que tenemos una unidad de red vinculada a una subcarpeta en COMPARTIDAS.



## RESUMIENDO PERFILES MÓVILES:

- Permiten trasladar la configuración a través de distintos clientes del dominio, almacenando el perfil en una carpeta compartida.

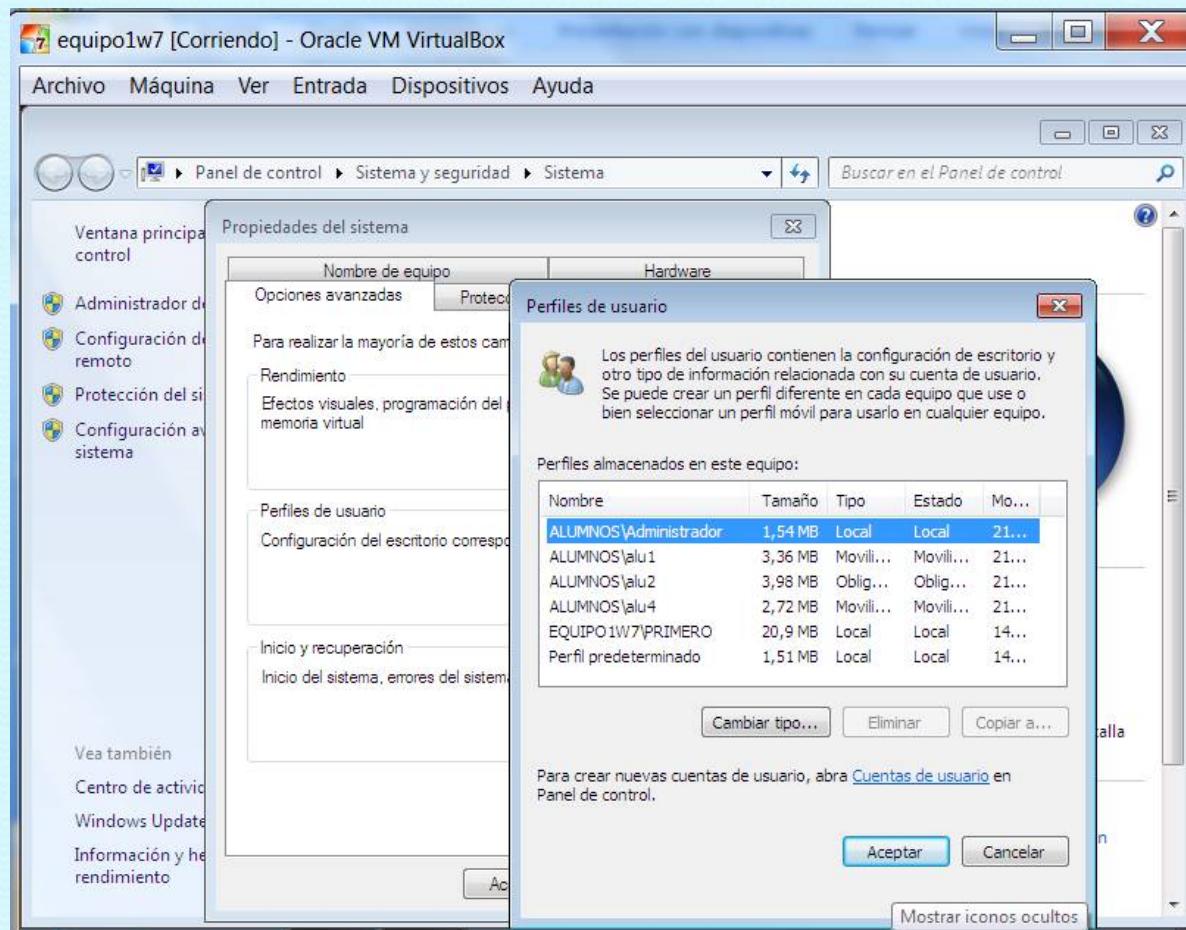
PROBLEMA: el tamaño del perfil puede ocasionar saturaciones (tráfico de red, saturación de almacenamiento).

SOLUCIÓN (PARCIAL): incluir en el perfil unidades de red a carpetas compartidas de usuario (mejoramos tráfico de red, sigue el posible problema de la saturación)

Inconvenientes:

- sólo permite una unidad de red hacia carpeta privada

Podemos ver que usuarios han iniciado la sesión en un equipo y el perfil que han utilizado para cada conexión. Podemos verlo desde configuración avanzada del sistema\opciones avanzadas\perfiles



## ALTERNATIVA A PERFILES MÓVILES:

### 1) PERFILES OBLIGATORIOS:

Son perfiles móviles que no se pueden variar. Configuraciones congeladas que se distribuyen por los distintos equipos. Para ello vamos a la carpeta del perfil del usuario y cambiamos el nombre

**netuser.dat por netuser.man**

(Hay que recuperar el control sobre la carpeta como administrador, desmarcar ocultar carpetas protegidas del sistema operativo y configurar para que se vean las extensiones y archivos ocultos).

### 2) POLITICAS DE GRUPO:

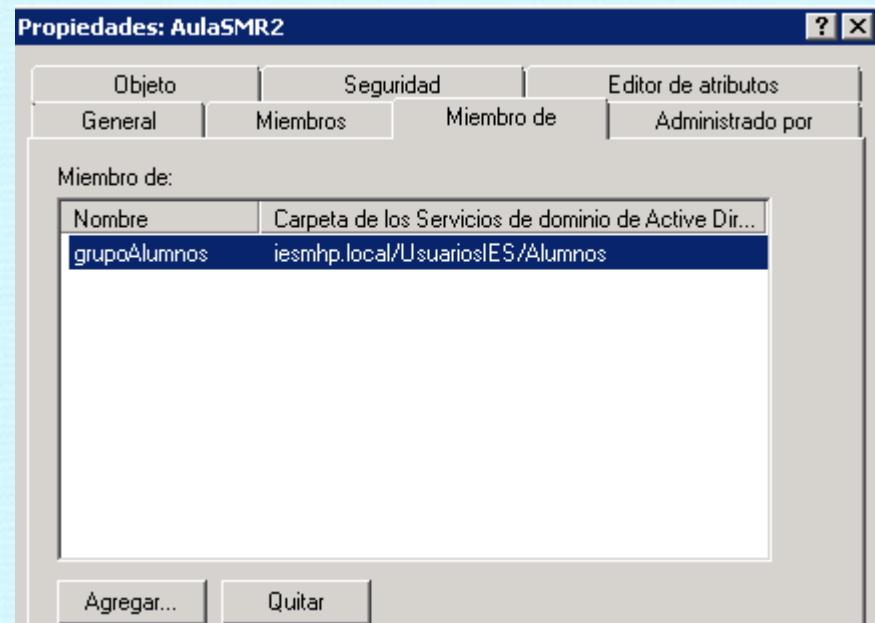
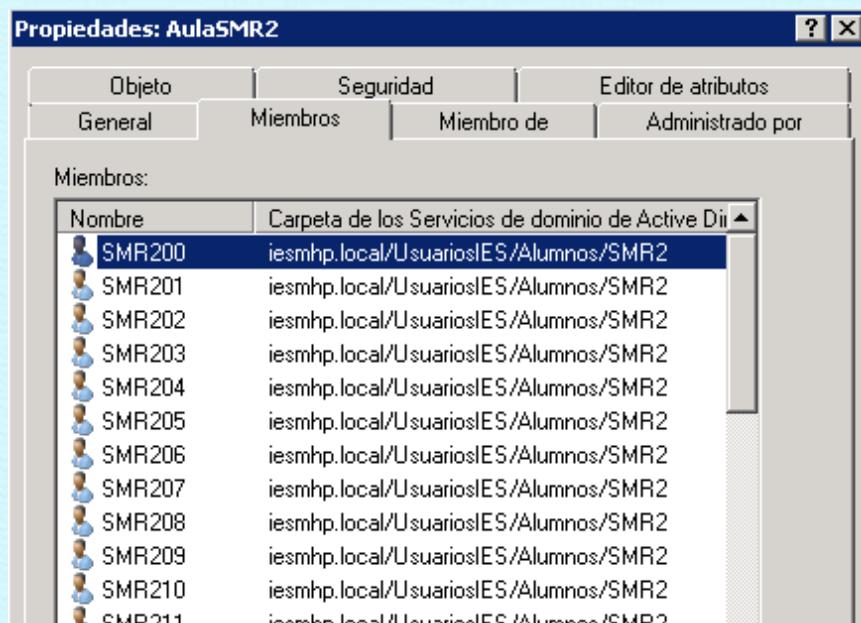
Permiten aplicar configuraciones de usuarios por unidades organizativas.

Mas flexibles que las propiedades de cuenta

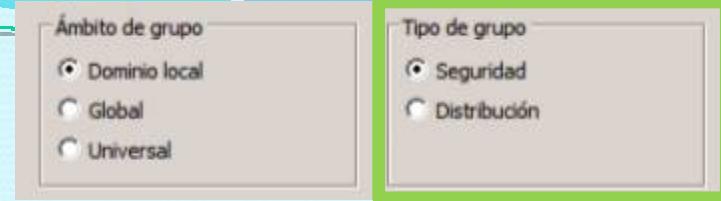
### 3. – Gestión de grupos. Tipos y ámbitos. Propiedades.

#### GRUPOS

- Un grupo es una recopilación de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una unidad individual.
- Los usuarios y los equipos que pertenecen a un grupo determinado se denominan miembros del grupo (MEMBRESIA)



### 3.1 Tipos de Grupos de usuarios



- **Grupos de distribución:**

Sólo se pueden utilizar con aplicaciones de correo electrónico (Exchange: agrupan contactos). No tienen habilitada la seguridad.

- **Grupos de seguridad:**

Permite establecer que puede hacer cada usuario del grupo en los distintos recursos del directorio.

## 3.2 – Ambitos.

Ámbito de grupo

Dominio local

Global

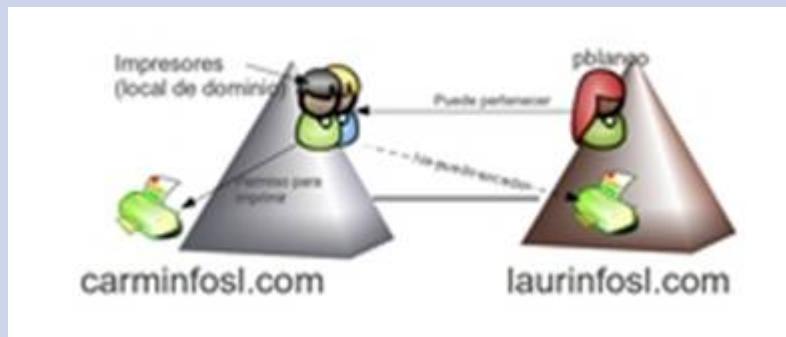
Universal

Tipo de grupo

Seguridad

Distribución

Ambito	Miembros...	Permisos en...
Dominio local	Cuentas de cualquier dominio Grupos globales de cualquier dominio Grupos universales de cualquier dominio Grupos locales de dominio pero sólo del mismo dominio que el grupo local de dominio principal	Los permisos de miembro sólo se pueden asignar en el mismo dominio que el grupo local de dominio principal
Global	Las cuentas del mismo dominio que el grupo global principal Los grupos globales del mismo dominio que el grupo global principal	Los permisos de miembro se pueden asignar en cualquier dominio del bosque.
Universal	Las cuentas de cualquier dominio del bosque en el que se encuentra este grupo universal. Los grupos globales de cualquier dominio del bosque en el que se encuentra este grupo universal. Los grupos universales de cualquier dominio del bosque en el que se encuentra este grupo universal.	Puede asignar permisos de miembro a cualquier dominio, e incluir miembros de cualquier dominio (siempre dentro del mismo bosque).

Ambito	
Dominio local	 
Global	
Universal	