

ADMINISTRACIÓN DE USUARIOS, CUENTAS Y GRUPOS



1. Unidades Organizativas
 - 1.1. Diseño de las unidades organizativas
 - 1.2. Crear unidades organizativas
 - 1.3. Mover objetos dentro del dominio
2. Cuentas de usuarios
 - 2.1. Nomenclatura
 - 2.2. Contrasenñas

Restricciones de cambios de contraseñas
 - 2.3. Crear cuentas de usuario
 - 2.4. Crear cuentas de usuario locales
 - 2.5. Creación de un directorio particular para usuarios de dominio
 - 2.6. Secuencias de comandos de inicio de sesión a perfiles de usuario
 - 2.7. Perfiles de usuario

Perfiles locales

Perfiles móviles

Perfiles obligatorios
 - 2.8. Plantillas de cuentas
 - 2.9. Habilitar y desbloquear cuentas de usuarios
3. Buscar equipos y usuarios
4. Grupos
 - 4.1. Administrar grupos

Grupos globales

Grupos universales

Grupos locales del dominio
 - 4.2. Dónde crear los grupos y nomenclatura
 - 4.3. Crear grupos

1. Unidades Organizativas

Las unidades organizativas nos permiten **crear la jerarquía** de nuestra organización.

Su fin es crear una **estructura de "carpetas"** que **administrativamente organice** nuestra empresa.

Por ejemplo, crearemos una **unidad organizativa** para **cada sección o departamento** de mi empresa. Además, todos los usuarios y cuentas de equipo las crearé o moveré a este nuevo sitio así que de un vistazo cuando abra el Directorio Activo veré una estructura mucho más familiar u organizada que la predeterminada.

Además, utilizaremos las unidades organizativas para agrupar y organizar objetos, para delegar derechos administrativos y asignar directivas a una colección de objetos como una unidad única. Es decir, podemos delegar la administración de una unidad organizativa "Finanzas" a una persona de ese departamento para que administre y gestione los recursos de su departamento.

Así que utilizaremos unidades organizativas para:

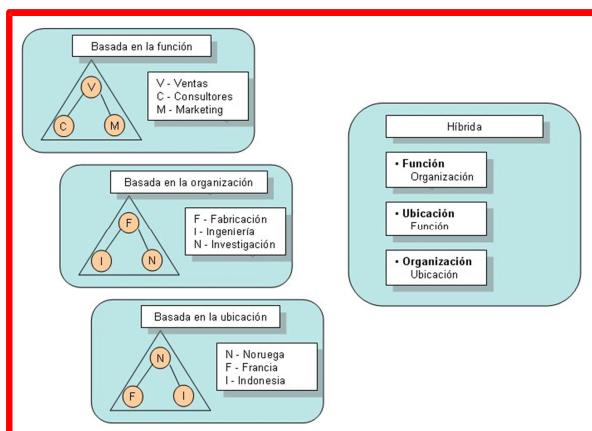
- Organizar objetos en un dominio.** Las unidades organizativas contienen objetos de dominio, como grupos y cuentas de usuario y de equipo. Los archivos e impresoras compartidos que están publicados en Active Directory también se encuentran en unidades organizativas.
- Delegar el control administrativo.** Podemos asignar control administrativo completo de todos los objetos de una unidad organizativa, como el permiso de "Control total", o asignar control administrativo limitado de los objetos de usuario en la unidad organizativa, como la capacidad de modificar la información del correo electrónico. Para delegar el control administrativo, puedes asignar permisos específicos a uno o más usuarios y grupos en una unidad organizativa y a los objetos que esta unidad contenga.
- Simplificar la administración de los recursos agrupados más utilizados.** Puedes delegar la autoridad administrativa de atributos determinados en objetos específicos en Active Directory, pero normalmente utilizarás las unidades organizativas para delegar la autoridad administrativa. Un usuario puede tener autoridad administrativa para todas las unidades organizativas de un dominio o para una única unidad. Mediante estas unidades puedes crear contenedores en un dominio que representen las estructuras jerárquicas y lógicas de tu empresa. De esta manera, puedes administrar la configuración y la utilización de las cuentas y recursos basados en tu modelo de organización.

1.1. Diseño de las unidades organizativas

¿Cómo debemos crear estas unidades organizativas?

En este caso podemos **crearlas**, luego **borrar, cambiar de nombre, moverlas** sin ningún tipo de coste de tiempo ni de cambio de configuración.

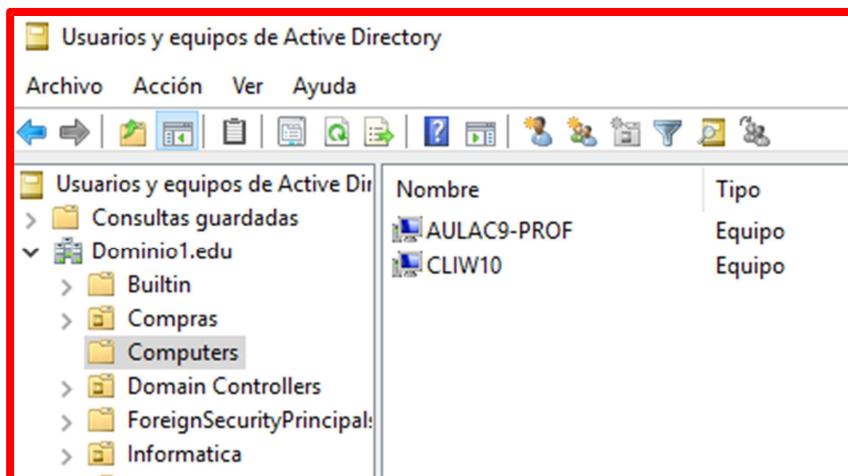
Fíjate en este gráfico:



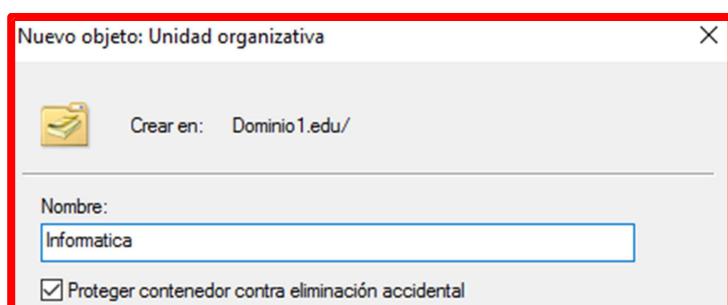
Expresa distintos criterios para crear las unidades organizativas, el diseño es ya a juicio nuestro. Por ejemplo, podemos crear una por cada departamento (Administración, Personal, Calidad, ...) y luego como tenemos dos pequeñas fábricas conectadas creamos una unidad organizativa para cada una de ellas (Barcelona, Calahorra, etc.), que es una combinación de los modelos de función y de ubicación que aparece en el gráfico.

1.2. Crear unidades organizativas

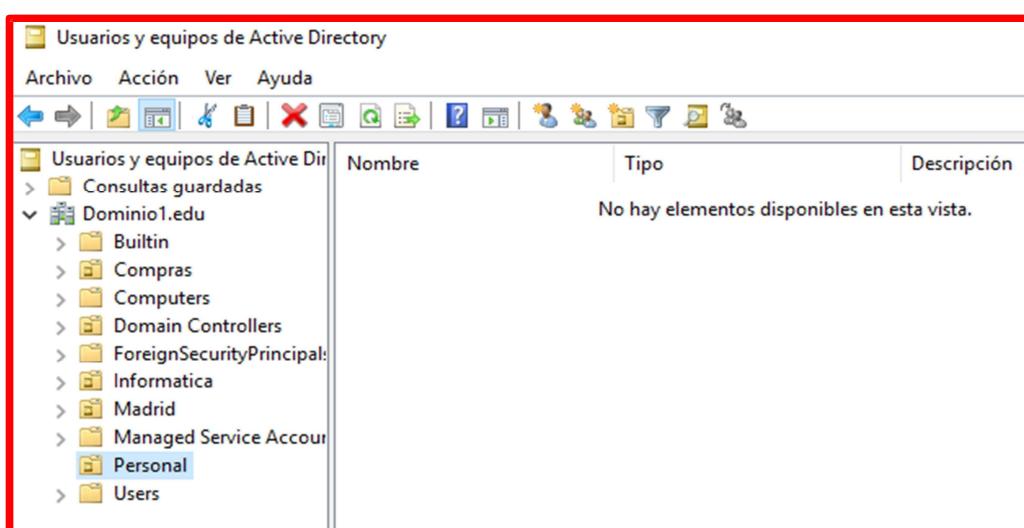
Podemos entonces crear unidades organizativas para representar una jerarquía o para administrar los objetos que deban ubicarse dentro de las unidades. Para crear una unidad organizativa nueva haremos lo siguiente. Primero abrimos la administración de usuarios y equipos (**Usuarios y equipos de Active Directory**):



Hacemos clic en el nombre de nuestro dominio "**Dominio1.edu**" y con el botón derecho seleccionamos "**Nuevo**" y luego "**Unidad Organizativa**". Aparecerá entonces esta pantalla:



Introducimos ahora el nombre de "**Informática**" y pulsamos "**Aceptar**". Repite la operación creando varias unidades organizativas más: Compras y Personal. Para que quede esto...



Como ves este es un procedimiento muy sencillo y permite organizar nuestra empresa. Por supuesto **podemos crear nuevas unidades organizativas dentro de la que hemos creado**. Por ejemplo y según la organización híbrida vista antes podemos crear una basada en la ubicación y departamento:

Nombre	Tipo	Descripción
		No hay elementos disponibles en esta vista.

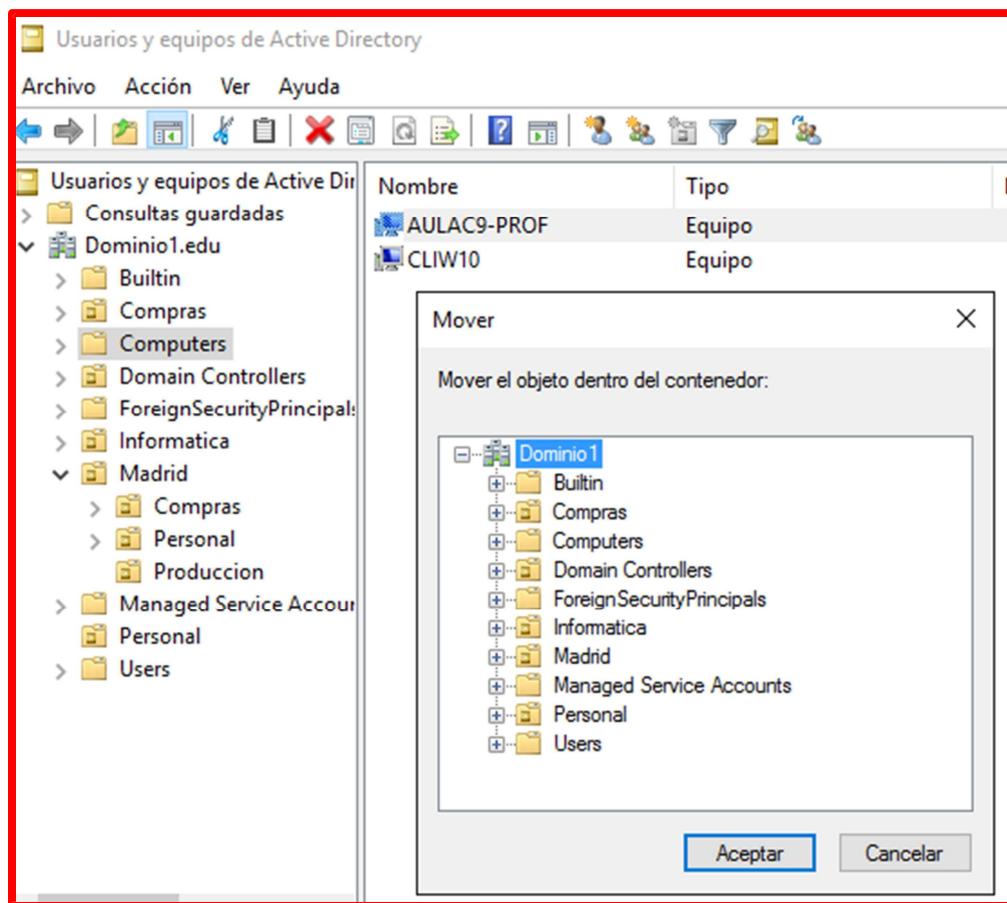
1.3. Mover objetos dentro del dominio

Podemos mover objetos entre unidades organizativas cuando haya cambios en las funciones administrativas o empresariales; por ejemplo, cuando un empleado se traslada a otro departamento. Como administrador de sistemas, nuestra tarea es la de mantener la estructura a medida que cambien las necesidades de nuestra empresa.

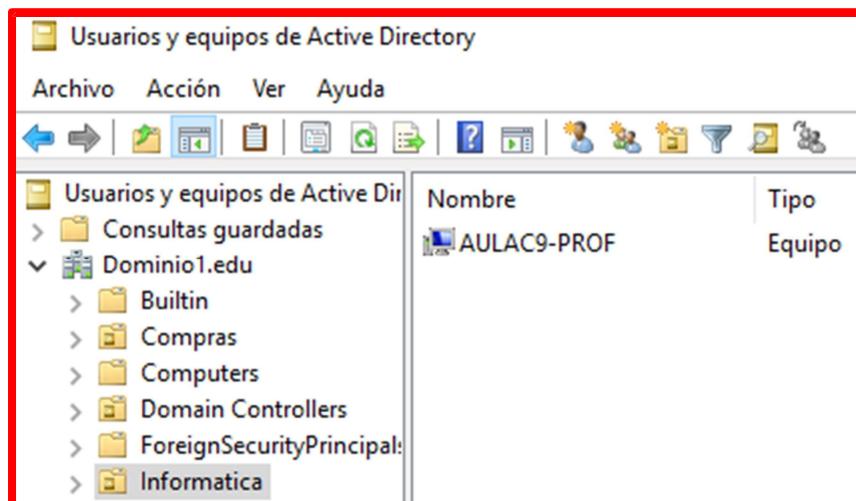
Los elementos que podemos mover dentro de la estructura del Directorio Activo son:

- Cuentas de usuario
- Cuentas de contacto
- Grupos
- Carpetas compartidas
- Impresoras
- Equipos
- Controladores de dominio
- Unidades organizativas

En nuestro ejemplo simplemente vamos a organizar los equipos registrados. Ahora que ya tenemos nuestras unidades organizativas creadas debemos mover los equipos que hemos ido registrando para ir organizando nuestros recursos. Vamos a mover el equipo **CLIENTEWIN7** a la unidad organizativa **Informatica** y el **CLIENTEW10** a la UO **Personal**. Primero vamos a la carpeta en la que se van introduciendo los equipos que se registran, recuerda: "**Computers**". En esa carpeta tenemos uno o varios equipos que queremos mover. Lo marcamos, pulsamos el botón derecho y seleccionamos la opción "**Mover**":



Nos muestra la opción de mover el objeto, seleccionamos la UO **Informatica** y pulsamos "**Aceptar**". Ahora comprueba que está en **Informatica**.



Luego, después de registrar los equipos, el primer paso es comprobar que aparecen en el Directorio Activo y luego debes moverlos a la unidad organizativa correspondiente.

Nota: Es muy importante que crees una estructura de unidades organizativas, aunque en tu empresa tengas pocos equipos. **Cuando lleguemos a las políticas (directivas) verás lo práctico que se hace luego la actualización y mantenimiento de los equipos.**

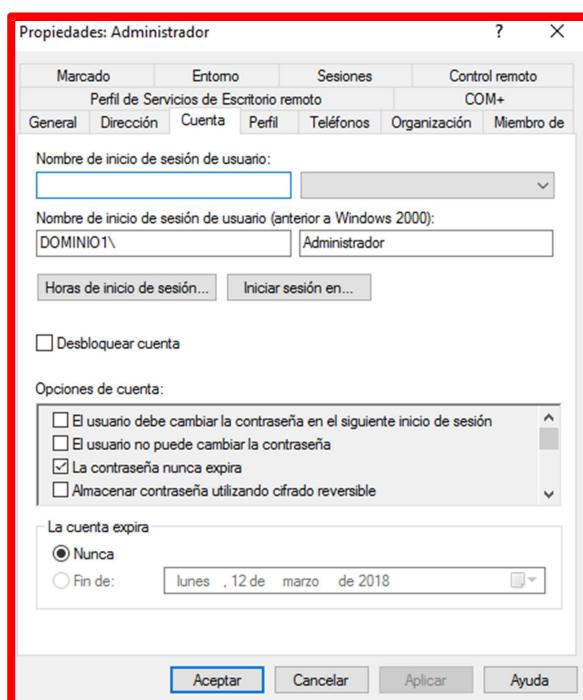
2. Cuentas de usuarios

Una cuenta de usuario es un objeto que contiene la información que define a un usuario.

Estos usuarios pueden ser **locales**, que se crean y administran en una pequeña base de datos del propio equipo o pueden ser **usuarios del dominio**. Los datos de esos usuarios están centralizados en el Directorio Activo. Obviamente lo que nos interesa son las cuentas de usuarios del dominio, pero como en ocasiones debemos tratar con cuentas locales las veremos para comprobar las diferencias.

Nota: Antes de los dominios trabajábamos con "Grupos de trabajo". En éstos al no existir un "contenedor" de cuentas como el Directorio Activo todas las cuentas de usuarios eran locales.

Este es el aspecto de las propiedades o atributos de una cuenta de usuario, luego lo veremos con más detalle:



Entre otros muchos datos contiene el **nombre de usuario** y la **contraseña** con los que el usuario inicia la sesión y los **grupos a los que pertenece**. A los datos del usuario y contraseña se les llama también las "**credenciales**" del usuario. Utilizaremos estas credenciales entre otras cosas para:

- Iniciar la sesión en un equipo.
- Permitir que los procesos y servicios se ejecuten dentro de un contexto de seguridad específico.
- Administrar el acceso de un usuario a los recursos.

Las cuentas las podemos ubicar en cualquier dominio del bosque y en cualquier unidad organizativa del dominio.

Si hemos creado nuestra estructura con departamentos crearemos las cuentas de usuario en la unidad organizativa correspondiente.

De esta forma tenemos ya en cada departamento las cuentas de equipos y las cuentas de usuario.

2.1. Nomenclatura

Igual que en el caso de las unidades organizativas vamos a ver las distintas nomenclaturas que tiene una cuenta de usuario.

Nombre	Ejemplo
Nombre de inicio de sesión de usuario	Josemari
Nombre de inicio de sesión en versiones anteriores a W2000	miempresa\josemari
Nombre de usuario principal de inicio de sesión	josemari@miempresa.com
Nombre completo relativo de LDAP	CN=josemari;CN=users;dc=miempresa;DC=com

Existen cuatro tipos de nombres asociados a las cuentas de usuario de dominio. En el Directorio Activo cada cuenta de usuario tiene:

- Un nombre de inicio de sesión de usuario.
- Un nombre de inicio de sesión de usuario de versiones anteriores a Windows 2000.
- Un nombre principal de inicio de sesión de usuario.
- Un nombre completo según el ya conocido Protocolo ligero de acceso a directorios (LDAP, Lightweight Directory Access Protocol).

Cuando se crea una cuenta de usuario, el administrador, nosotros, escribimos un nombre de inicio de sesión de usuario.

El **nombre de inicio de sesión debe ser único en el bosque** en el que se crea la cuenta de usuario (suele utilizarse como nombre completo relativo). Los usuarios utilizan este nombre sólo en el proceso de inicio de sesión. Obtienen acceso con el nombre de inicio de sesión de usuario, una contraseña y el nombre de dominio en diferentes campos de la pantalla de inicio de sesión. Es decir, los datos que ya conocemos para hacer el inicio de sesión.

Hay que tener cuidado con los nombres ya que deben cumplir que:

1. Tienen que contener hasta 20 caracteres en mayúsculas y minúsculas (ojo, el campo admite más de 20 caracteres, pero Windows Server sólo reconoce los 20 primeros).
2. Debe incluir una combinación de caracteres alfanuméricos y especiales, excepto " / \ [] : ; | = , + * ? < >.

Un nombre de inicio de sesión de usuario podría ser, "JRodriguez" o "JoseR".

En versiones anteriores a Windows 2000 hay una forma de distinguir el usuario y el dominio y es de la forma: MIEMPRESA\JOSER. El equivalente en Directorio Activo es joser@miempresa.com

Cuando instalamos el Directorio Activo nos indicó cómo se iba a llamar el dominio para equipos anteriores a Windows 2000, te recuerdo esa pantalla:



Así mismo cuando creamos las cuentas de usuario hay un nombre para el Directorio Activo y un nombre para identificar a la misma persona en equipos anteriores a Windows 2000, por coherencia se suele poner el mismo nombre. Así que la combinación de este último con esa identificación del dominio hace que se puede hacer una identificación de dominio/usuario. Esta forma de identificarse es absolutamente válida en equipos y servidores posteriores a W2000, lo que pasa es que para anteriores a este no se admitía los nuevos nombres del Directorio Activo.

El **nombre principal de usuario (UPN, User Principal Name)** está formado: el nombre de inicio de sesión de usuario y el sufijo del nombre principal de usuario, unidos por el símbolo @.

El UPN debe ser único en el bosque.

La segunda parte del UPN es el sufijo del nombre principal de usuario. Éste puede ser el nombre del dominio en el **Sistema de nombres de dominio (DNS, Domain Name System)**, el nombre DNS de cualquier dominio del bosque o un nombre alternativo creado por un administrador sólo para iniciar la sesión.

Por ejemplo "Joser@miempresa.com"

Ya a nivel más técnico y viendo cómo se almacena internamente en el Directorio Activo tenemos el nombre completo relativo según el LDAP que únicamente identifica el objeto en su contenedor primario. Los nombres completos relativos deben ser únicos en su unidad organizativa.

Ejemplos de nombres completos según el LDAP serían:

- CN=joserm,CN=users,DC=miempresa,DC=com
- CN=jrodriguez,CN=users,DC=miempresa,DC=com

En cuanto a la nomenclatura o criterio que debemos seguir es absolutamente libre pero sí se aconseja utilizar el mismo en todas las cuentas. Por ejemplo, podemos elegir poner la inicial del nombre y el primer apellido: JRodriguez, ALopez, ...

Las cuentas las podemos ubicar en cualquier dominio del bosque y en cualquier unidad organizativa del dominio. Si hemos creado nuestra estructura con departamentos crearemos las cuentas de usuario en la unidad organizativa correspondiente. De esta forma tenemos ya en cada departamento las cuentas de equipos y las cuentas de usuario.

2.2. Contraseñas

Uno de nuestros trabajos será administrar los usuarios con sus contraseñas.

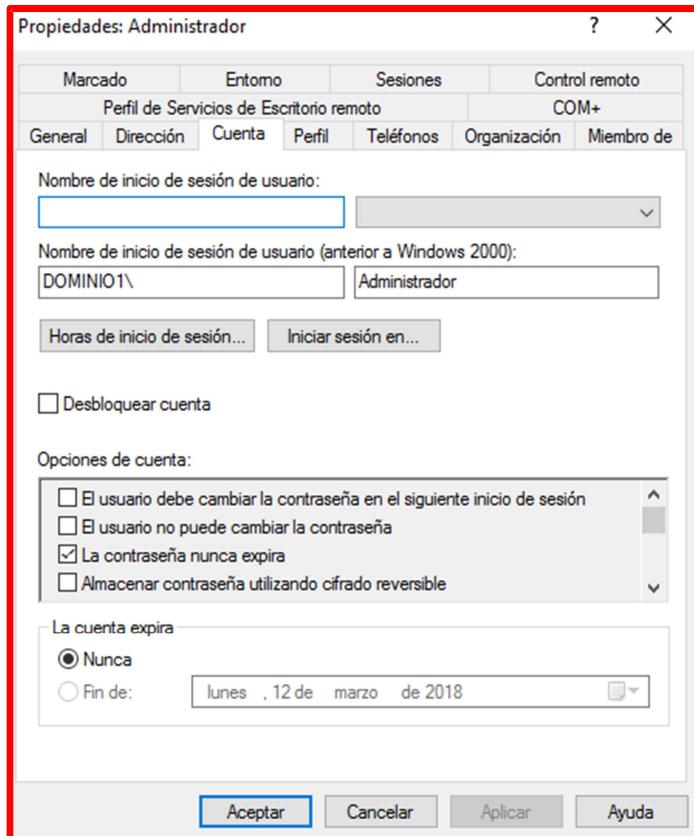
Dependiendo del nivel de seguridad que le apliquemos a nuestra red tendremos más o menos actividad con estas opciones.

Cuando veamos las políticas recomendaremos y haremos un ejemplo de un modelo de caducidad de contraseñas.

Las opciones de estas contraseñas pueden establecerse al crear la cuenta o bien a través del cuadro de diálogo **Propiedades de la cuenta de usuario**. Podremos establecer las siguientes opciones para proteger el acceso al dominio o a un equipo.

1. El usuario debe cambiar la contraseña al iniciar una sesión de nuevo. Se utiliza cuando un usuario nuevo inicia la sesión en un sistema por primera vez o cuando el administrador restablece una contraseña olvidada por el usuario.
2. El usuario no puede cambiar la contraseña. La usaremos cuando queramos controlar el momento en el se puede cambiar la contraseña de una cuenta.
3. La contraseña nunca caduca. Esta opción evita que caduque la contraseña. No debemos utilizar esto ya que nada impediría que un usuario estuviese probando distintas contraseñas sin ninguna posibilidad de que se le bloquee la cuenta

4. La cuenta está deshabilitada. Evita que el usuario inicie la sesión Estas opciones están en esta solapa:



Restricciones de cambios de contraseñas

Una de las principales recomendaciones en temas de seguridad es hacer que las contraseñas caduquen, de esta forma el usuario debe cambiarla regularmente y hace que disminuyan las posibilidades de que se conozcan esas contraseñas. En el tema de las políticas configuraremos nuestro entorno para que esto sea obligatorio en nuestro dominio, estableciendo una política de contraseñas.

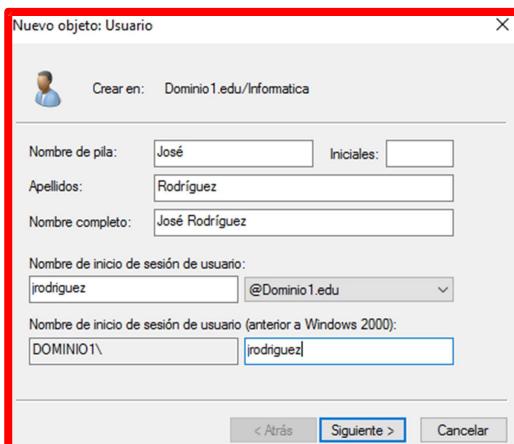
Opción	Utilizaremos esta opción cuando...
Cambio de contraseña	<ul style="list-style-type: none"> • Creemos nuevas cuentas de dominio • Queremos restablecer las contraseñas
Restringir cambio de contraseña	<ul style="list-style-type: none"> • Creemos las cuentas de servicio de dominio y locales • Creemos nuevas cuentas locales que no se inicien de forma local

2.3. Crear cuentas de usuario

Ya tenemos nuestras unidades organizativas creadas y los ordenadores en ellas, ahora queda la creación de los usuarios. Hay tres tipos de cuentas de usuario:

1. **Cuentas de usuario del dominio.** Son las utilizadas para proporcionar acceso al Directorio Activo y sus recursos. Es la cuenta de usuario habitual en las redes.
2. **Cuentas de usuario locales.** Se crean cuando no existe un dominio que centralice los recursos y se mantienen dentro de cada equipo. Se pueden crear en los equipos clientes y en los servidores independientes. El usuario solo podrá acceder a los recursos locales que se le asignen.
3. **Cuentas de usuario "built-in" o incorporadas.** Son las cuentas que el Directorio Activo crea de forma predeterminada para accesos especiales, por ejemplo, la de *Administrador*.

Vamos a crear primero la cuenta y luego comentaremos algunas cosas sobre esta pantalla. Vamos a la unidad organizativa **Informatica** donde queremos crear el usuario y con el botón derecho le decimos que "**Nuevo**" y "**Usuario**".

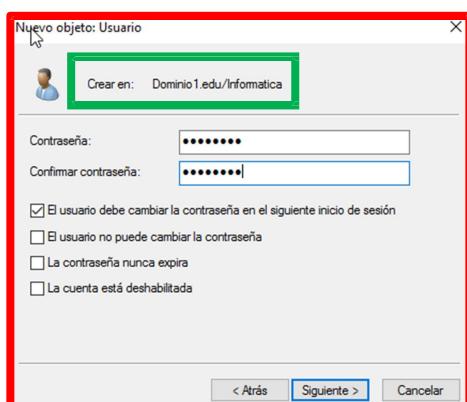


Por un lado, tenemos los datos del nombre y apellidos, el campo de iniciales no es importante, esto lo utilizan más los americanos. A medida que vamos escribiendo el nombre vemos que nos sugiere un nombre de usuario para la red en "*Nombre de inicio de sesión de usuario*". Como queremos poner la inicial del Nombre más el Apellido como sistema para llamar a los usuarios, lo modiflico para que aparezca "*jrodriguez*". Luego en la identificación, los nombres de usuario pueden ir en mayúsculas o minúsculas indistintamente, es en la contraseña donde sí se distinguen estos caracteres.

También puedes observar algo muy importante y es la forma de llamar a las cuentas de usuario según utilicemos un sistema de Windows 2000 o XP o con versiones anteriores. En la parte inferior nos avisa de esto, donde podemos poner un nombre distinto que servirá para que este usuario se identifique correctamente si está utilizando sistemas operativos anteriores a W2000. Lo mejor es que estas dos identificaciones sean iguales. Luego pueden causar problemas y nunca necesitarás recordar ese segundo nombre. Es decir, si dejamos el mismo nombre nos evitamos problemas, su nombre de cuenta de usuario es "*jrodriguez*" para todos los sistemas y ya está. Luego la forma de identificarse sería:

Sistema operativo	Nombres para identificarse en la red
Windows XP, 2000, 2003, Vista, 2008, 2010,	<u>jrodriguez@Dominio1.edu</u> Dominio1.edu\jrodriguez
Windows 95, 98, ME y NT 4.0	Dominio1.edu\jrodriguez

En la creación del nuevo Usuario nos dice dónde está creando este objeto, que, en este caso, es una cuenta de usuario. El destino es "**Dominio1.edu/informatica**".

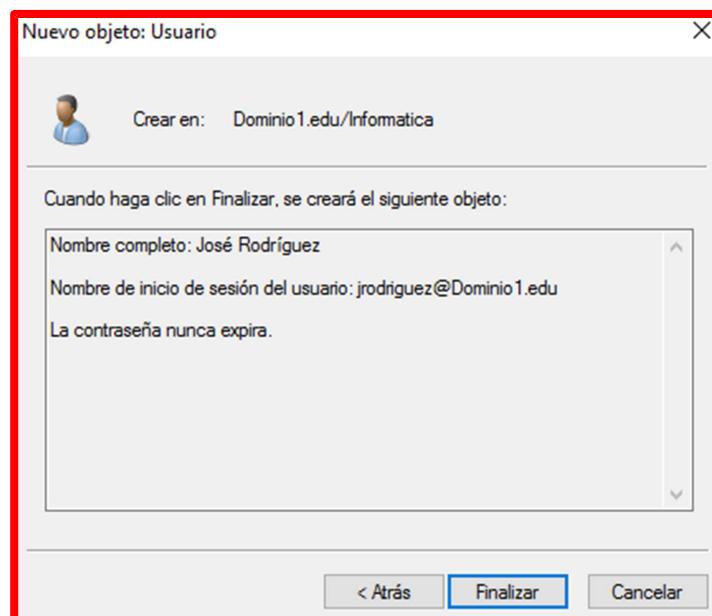


Ahora me pide la contraseña y escribiremos "12345678" en las dos casillas. Debajo tenemos las opciones que ya comentamos antes.

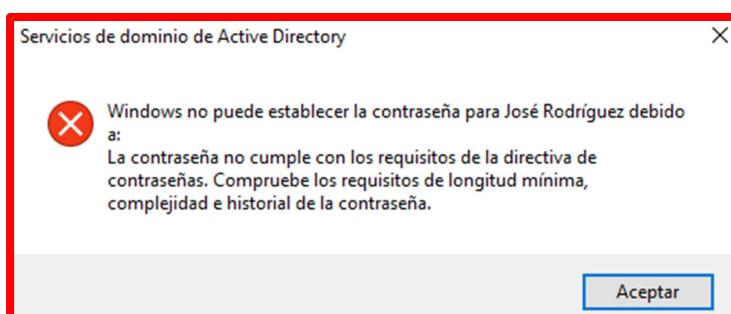
Lo natural es que a los usuarios les pongamos una contraseña genérica y dejemos activada la primera opción así cuando entre en un equipo identificándose con el usuario y contraseña que le hemos proporcionado el dominio le dirá que debe cambiar la contraseña, el usuario escribirá una nueva y así mantenemos la obligada confidencialidad en estos datos. Las otras opciones las dejamos:

- "El usuario no puede cambiar la contraseña". Esto lo dejaremos para alguna cuenta de usuario especial, por ejemplo, un usuario que utilicemos para realizar las copias de seguridad.
- "La contraseña nunca caduca". Es una opción que suele ir ligada a la anterior, así dejamos una cuenta permanente para alguna acción especial. Es muy peligroso tener esta combinación así que utilízala en situaciones imprescindibles.
- Podemos deshabilitar cuentas en determinadas ocasiones, bien porque no queremos que el usuario esté ya operativo o porque ese usuario causa baja y debemos detener esa cuenta inmediatamente."

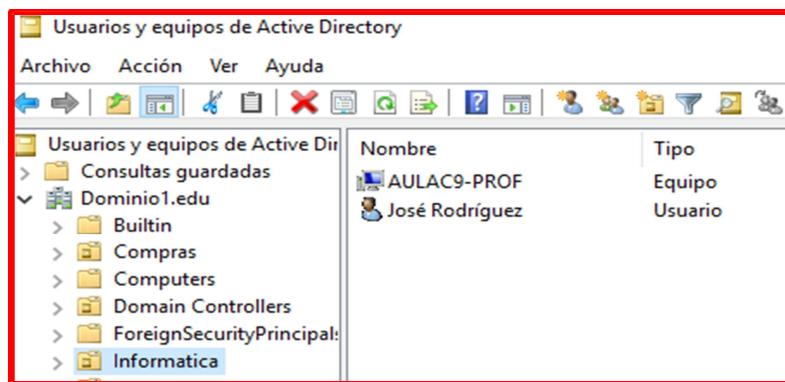
Pulsemos en "*Siguiente*" para continuar...



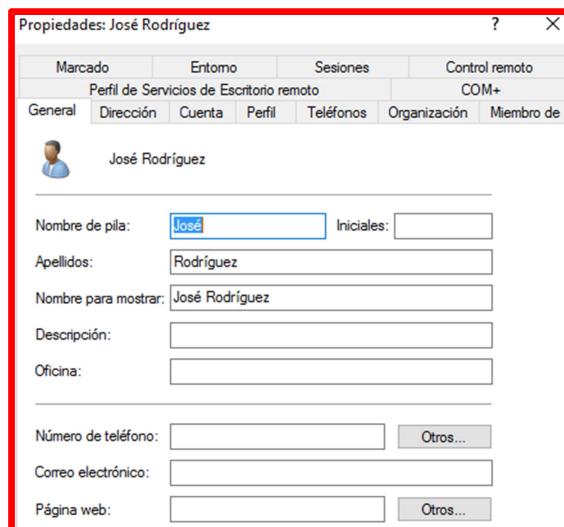
El sistema nos avisa ya de que tiene todos los datos para crear la cuenta así que nos toca "*Finalizar*":



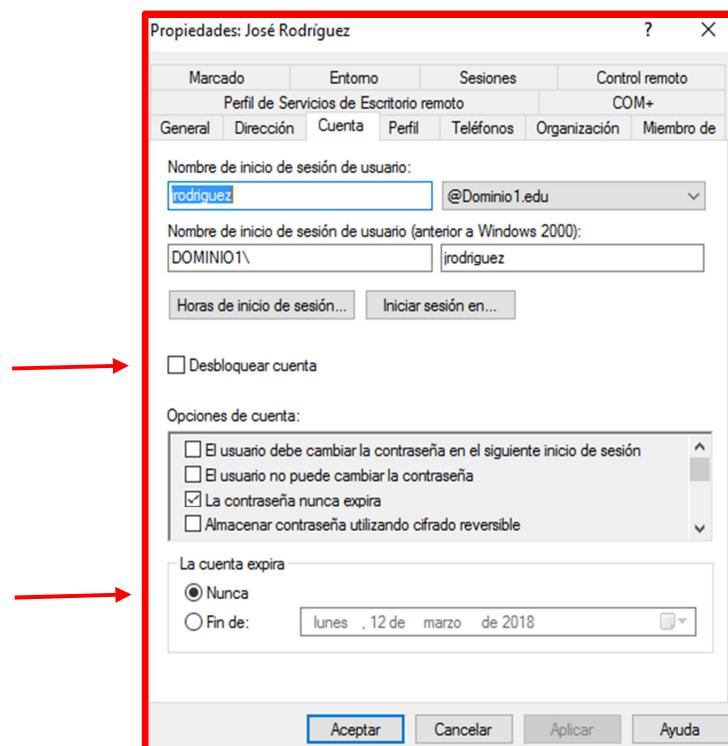
Sucede que en Windows 2016 Server por defecto tiene activado que las contraseñas sean complejas, es decir debemos poner una contraseña que tenga una combinación de letras en minúsculas, mayúsculas y números. Por ejemplo "p@ssw0rd". Ya cambiaremos esto más adelante. Vuelve hacia atrás en este asistente pon una contraseña completa (por ejemplo, la anterior) y termina de crear la cuenta.



Si hacemos clic en la unidad organizativa "**Informatica**", que es donde he creado el usuario veremos que está ya el icono del equipo y del usuario. Haz clic con el botón derecho sobre ese nombre de usuario, en **Propiedades**, para ver la ficha completa:



En esta primera pestaña aparecen los datos básicos de identificación, cuanto más completo lo hagamos mejor, así cuando hagamos inventarios o consultas nos aparecerán más datos sobre los usuarios. Hay muchas solapas con información de todo tipo sobre este usuario. Ahora nos interesa la que se llama "**Cuenta**", así que haz clic sobre ella:



La primera parte ya la conoces, es la identificación del dominio.

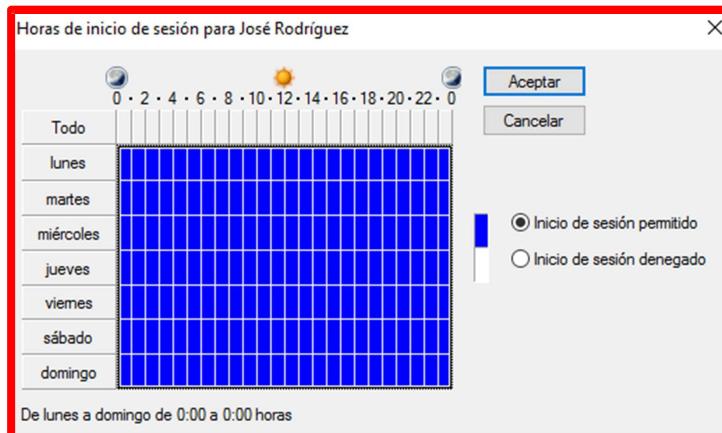
Luego tenemos unas "**Opciones de cuenta**" que son algunas más de las que vimos antes.

También tenemos una opción que pone "**La cuenta está bloqueada**" que se produce cuando el usuario hace varios intentos de entrar equivocados y a la tercera el sistema le bloquea por seguridad el acceso al dominio. En esta situación debemos venir a esta pantalla, buscas esa casilla y desactivarla para desbloquearle el acceso a la red.

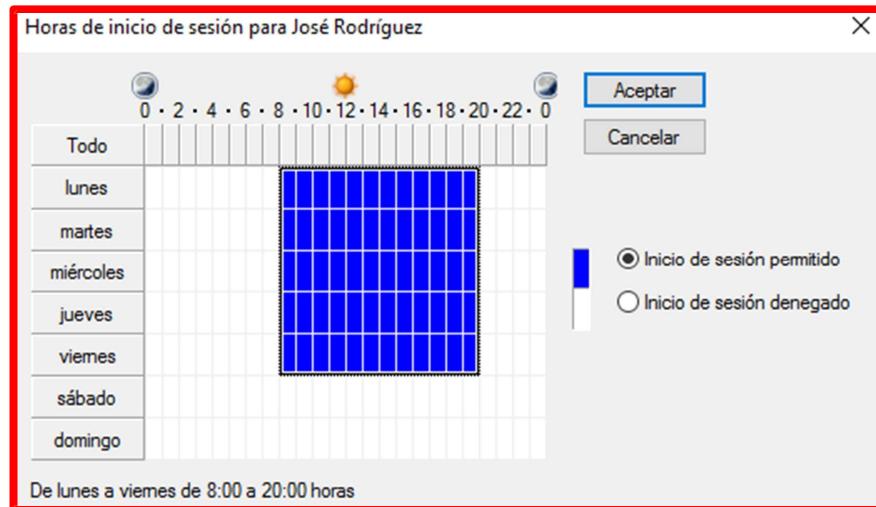
Debajo tenemos que "**La cuenta caduca**", es una opción muy interesante porque se la aplicaremos por ejemplo a alguien que vaya a estar temporalmente en nuestra empresa, así sólo tendrá esa duración.

Más opciones interesantes, supongamos que el horario de trabajo de nuestra empresa es de 8:00 a 20:00

h. aproximadamente y sólo de lunes a viernes. En este caso podemos pulsar el botón de "**horas de inicio de sesión**":



Podemos marcar con el ratón las horas de "**Inicio de sesión denegado**" de la parte de la derecha para borrar esa zona horaria que queremos que no tengan acceso. O más fácil, marcamos todo le negamos a todo el acceso para borrarlo. Luego marcamos desde las 8:00 hasta las 20:00 h. de lunes a viernes y hacemos clic en "**Inicio de sesión permitido**":



A continuación, actualizamos Dominio1.edu e iniciamos sesión el dominio, desde el equipo CLIENTEWIN7, con este usuario y una de las dos formas de identificación: **jrodriguez@Dominio1.edu** o **Dominio1.edu\jrodriguez**

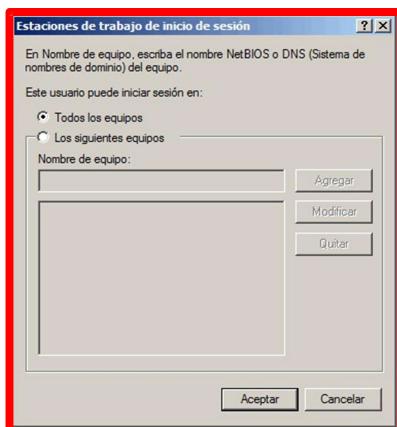


Ahora cambiaremos la hora del servidor (fuera del rango permitido para acceder que tiene asignado José Rodríguez). Veremos que no podemos entrar.



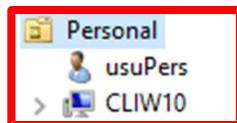
Con esto nos aseguramos que los usuarios no puedan entrar a la red fuera de las horas permitidas y aumentamos la seguridad además de no permitir por ejemplo el uso de Internet y demás recursos. Otra razón por ejemplo es la habilitación de una cuenta sólo para usuarios de turnos de noche, así no se pueden utilizar el resto del día.

Además, nos queda el botón de "Inicio de sesión en":

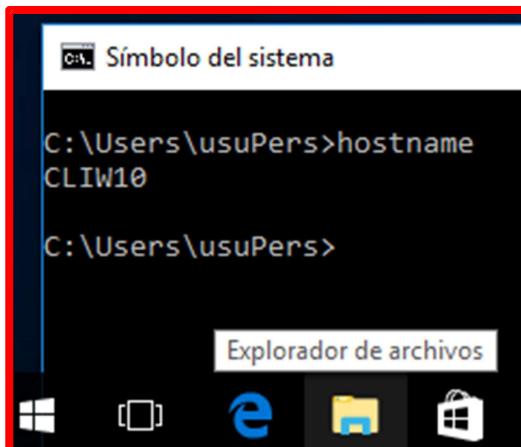


que nos permite que ese usuario sólo pueda entrar en determinados equipos. Por ejemplo, los usuarios del departamento de Personal sólo entrarán en los equipos de ese departamento así que enumeraré aquí la lista de equipos. El inconveniente de esto es que hay que mantener esta lista, si añadimos alguno nuevo al dominio debemos ir a estas listas de los usuarios y añadirlo aquí también si queremos hacer este tipo de control. Si no, dejamos que entren a todos y luego el control de acceso a los recursos de los próximos temas limitará el acceso a la red.

Ejercicio: Crea un usuario llamado usuPers en la UO Personal y que sólo pueda iniciar sesión desde el equipo CLIENTEW10 (este equipo está en esta UO Personal).



Intenta iniciar sesión con este usuario desde los equipos CLIENTEW10 y CLIENTEWIN7.



Nos deja en el cliente W10, pero no en el W7:



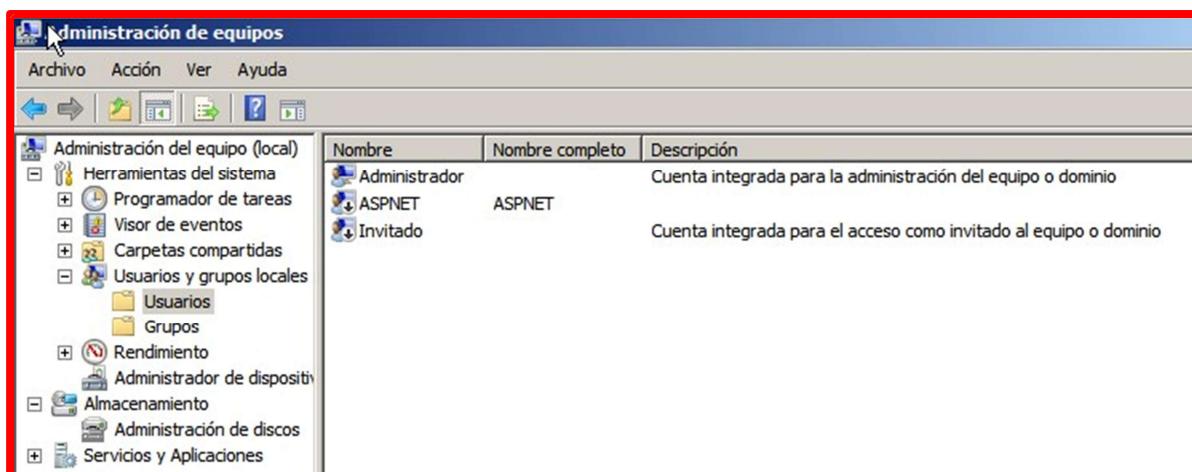
2.4. Crear cuentas de usuario locales

En ocasiones tendremos que crear una **cuenta de usuario sólo para un ordenador y no para el dominio**.

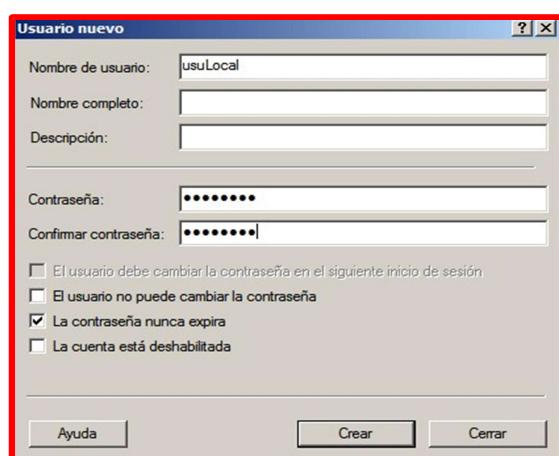
En este caso **las cuentas de usuario no residen en el Directorio Activo** sino en los propios equipos y sólo va a valer para el equipo donde se crea. Por ejemplo, podemos instalar un programa que requiera la instalación de un servicio, en ese caso seguramente nos dirá que necesita crear una cuenta de usuario local para asociarla con el servicio del programa.

Podemos hacerlo **en Servidores 2016, que no sean Controladores de Dominio**. Una vez iniciada la sesión de nuestro Servidor 2016, en el dominio (como Administrador) iremos al panel de control que tenemos y a la carpeta de "**Herramientas administrativas**":

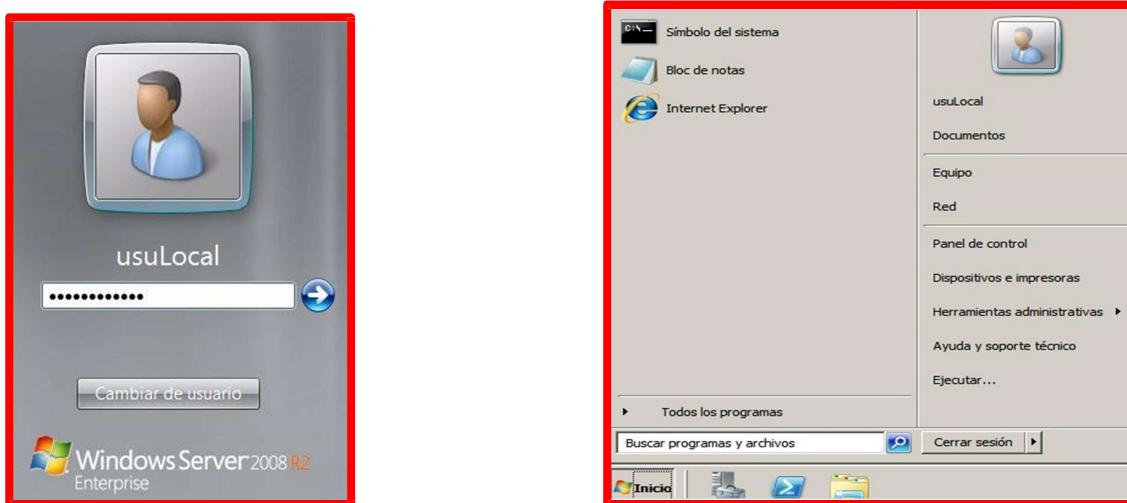
Ahí tenemos la opción de "**Administración de equipos**" donde podremos realizar distintas operaciones, entre ellas la de creación de cuentas locales (comprueba que en el Controlador de Dominio no tenemos esta opción):



Abrimos el árbol de la izquierda, pulsamos en "**Usuarios locales y grupos**" y vemos la lista de "**Usuarios**". Verás, como en el ejemplo, que hay varias cuentas de usuarios, algunas de ellas deshabilitadas (icono). Para crear una cuenta pulsaremos con el botón derecho y seleccionamos "**Usuario nuevo**". Crear uno llamado **usuLocal**:



Donde tenemos las opciones de esta cuenta. Por supuesto, no aparece nada del dominio porque no se crea en él. Inicia ahora sesión en este equipo con el usuario local creado.



Debemos evitar la creación de estas cuentas porque no están centralizadas en nuestro dominio y no las podemos controlar tanto.

Iniciaremos ahora sesión en el equipo **CLIENTEWIN7**, con el usuario José Rodríguez (volveremos a poner que este cliente puede entrar a cualquier hora).

Hay unos datos de equipo que son vitales para conocer bien el funcionamiento de nuestro equipo y dominio. Estos datos los recibe el equipo al iniciar la sesión y los almacena en forma de "**variables de entorno**" que se actualizan en cada inicio de sesión.

Para verlas iremos al menú Inicio y pulsaremos en ejecutar para escribir el comando "**cmd**", que abrirá una consola de comandos. Ejecutamos el comando "**set**" y pulsamos "**Intro**".

Nos va a aparecer una serie de valores interesantes.

```
ps: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. Reservados todos los derechos.

E:\ Usuarios\jrodriguez>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=E:\ Usuarios\jrodriguez\AppData\Roaming
COMMONPROGRAMFILES=C:\Program Files\Common Files
COMPUTERNAME=CLIENTEWIN7
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.UVE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 42 Stepping 7, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=2a07
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$PSG
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=E:\ Usuarios\JRODRIGUEZ\Temp
TMP=%TEMP%
USERDNSDOMAIN=DOMINIO01.EDU
USERDOMAIN=DOMINIO01
USERNAME=jrodriguez
USERPROFILE=E:\ Usuarios\jrodriguez
windir=C:\Windows
```

y entre ellos tenemos:

- "**COMPUTERNAME**" que indica el nombre del equipo.
- "**LOGONSERVER**", indica el servidor en el que ha iniciado la sesión. En nuestro caso sólo tenemos un controlador de dominio pero en una red con varios de ellos esta variable indicará en cuál de ellos está "logeado".
- "**USERDNSDOMAIN**" y "**USERDOMAIN**" indica el dominio en el que está trabajando, como ves tiene los dos nombres el estándar del DNS y el del NETBIOS.
- "**USERNAME**", indica el usuario que ha iniciado la sesión en el equipo.

Muchos programas comerciales simplemente leen estas variables de sistema y así saben el nombre del equipo, usuario,... incluso dónde deben instalar los programas gracias a "*ProgramFiles*" que apunta a la carpeta estándar donde se instalar los programas: "C:\Archivos de Programa".

2.4. Creación de un directorio particular para usuarios de dominio

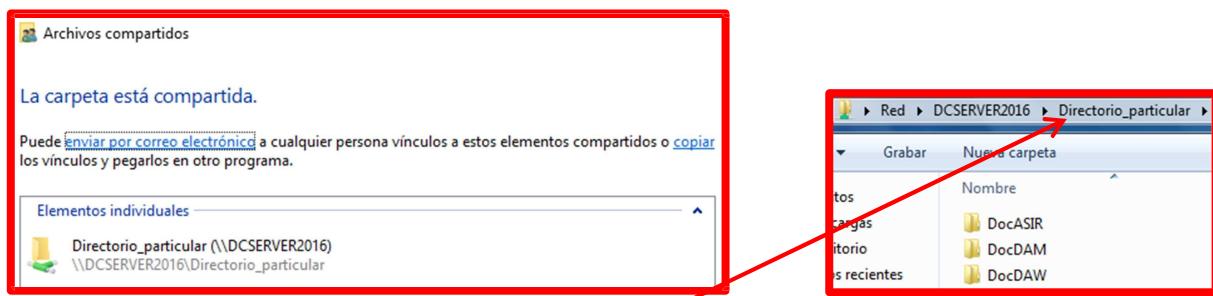
Los **directorios particulares** son almacenes incluidos en un servidor de red para los documentos de los usuarios. Situar los directorios particulares en un servidor de archivos de la red tiene varias ventajas:

1. La copia de seguridad de los documentos de usuario está centralizada.
2. Los usuarios pueden acceder a sus directorios particulares desde cualquier equipo cliente.

Los contenidos de los directorios particulares no son parte de los perfiles de usuario, por lo que no afectan al tráfico de la red durante el inicio de sesión. Se deben almacenar en una partición con formato NTFS.

Para **crear un directorio particular** en un Controlador de Dominio haz lo siguiente:

1. Crea una carpeta, **Directorio_particular**, para los directorios compartidos.
2. Para compartirlo: pulsar con el botón derecho del ratón en la nueva carpeta y escoger **Propiedades**, elige la pestaña **Compartir** y pulsa en **Compartir**.
3. Dar el **permiso de lectura** al **grupo Usuarios del Dominio**, lo que evitará que nadie excepto las cuentas de usuario del dominio puedan acceder a la carpeta.



Inicia sesión en **CLIENTEWIN7** y comprueba que **jrodriguez** puede leer la carpeta.

Para **proporcionar un directorio particular a un usuario en concreto** (José Rodriguez), se debe añadir la ruta de acceso de la carpeta a las propiedades de la cuenta de usuario. Hay que seguir estos pasos para otorgar a un usuario acceso a un directorio particular:

1. Abre **Usuarios y equipos** de Active Directory.
2. Pulsa la **Unidad Organizativa** que contiene la cuenta de usuario. Pulsa con el botón derecho del ratón en el **nombre del usuario** y escoge **Propiedades** en el menú contextual.
3. Pulsa en la pestaña **Perfil**.
4. En el área **Carpeta particular** hay que pulsar la opción **Conectar** y especificar una letra de unidad (I:) a utilizar para conectarse al servidor de archivos.

En el cuadro a: se especifica el nombre UNC de la conexión; por ejemplo,

[\\nombre_del_servidor\carpeta_compartida\nombre_de_inicio_de_sesion_del_usuario.](#)

Si se utiliza la variable **%username%**, se le dará al directorio particular el nombre de inicio de sesión del usuario y se le asignarán permisos de acceso exclusivos para el usuario.

Ejercicio: Hazlo para José Rodriguez sobre la carpeta DocDAM. Se creará dentro de ella, automáticamente, la carpeta jrodriguez.

2.5. Secuencias de comandos de inicio de sesión a perfiles de usuario

En la pestaña **perfil de un usuario** se especifica el nombre de la secuencia de comandos de inicio de sesión que va a utilizar una **cuenta de usuario**. Se pueden asignar secuencias de comandos de inicio de sesión por medio del perfil o a través de Directiva de grupo.

Windows Server 2016 siempre busca las secuencias de comandos de inicio de sesión en el mismo lugar: en el controlador de dominio de autenticación en la ruta de acceso,

C:\Windows\SYSVOL\sysvol\nombre_delDominio\SCRIPTS (*ver Herramientas > Administración de equipos > carpetas compartidas> recursos compartidos, ruta de NETLOGON*).

Las secuencias de comandos de esta carpeta se pueden introducir en la ruta de acceso **Script de inicio de sesión** sólo con el nombre. Si se utilizan carpetas dentro de la carpeta Scripts, se debe mostrar la parte de la ruta de acceso en la ruta de acceso Script de inicio de sesión.

El script con extensión **.bat**, puede contener, por ejemplo, líneas como la siguiente:

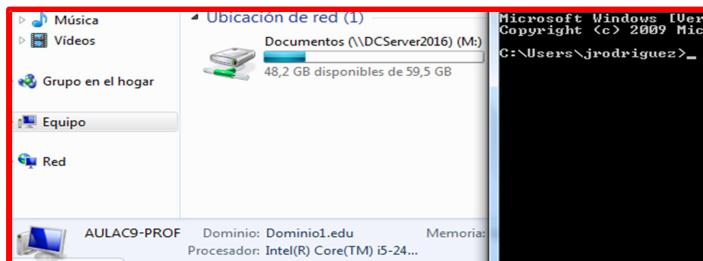
```
net use M: \\servidor\Documentos
```

siendo **Documentos** una **carpeta compartida** en el equipo **DCSERVER2016**.

Ejercicio: Vamos a crear una secuencia de comando de inicio de sesión para el usuario **jrodriguez**. Para ello crearemos una carpeta compartida **Documentos**, con permiso de lectura para Todos. Desmarcamos la opción a la carpeta particular anterior.

A continuación creamos el script **prueba.bat** (con el Bloc de notas) cuyo contenido será: **net use M: \\DCServer2016\Documentos** y lo guardamos en la ruta del recurso compartido NETLOGON.

Ahora asignaremos una secuencia de comandos al perfil (usuario *jrodriguez*). Para ello pulsamos sobre la Unidad Organizativa *Informatica* que contiene la cuenta de usuario. En sus *Propiedades* elegimos la pestaña *Perfil* e introducimos el nombre de la secuencia de comandos de inicio de sesión (*prueba.bat*) en el cuadro *Script de inicio de sesión*. Actualizamos y ahora iniciamos sesión con este usuario desde el CLIENTEWIN7. Si esta iniciada la sesión con él, la cerramos. Vemos que aparece la unidad de red que hemos escrito en el script:



Iniciamos ahora sesión, en este equipo, con el usuario **usuPers** (quitamos la restricción que tenía de sólo poder iniciar sesión desde CLIENTEW10) y vemos que para él no aparece la unidad M: con el recurso compartido Documentos.

2.6. Perfiles de usuario

Un perfil es un entorno personalizado específicamente para un usuario. El perfil contiene la configuración de escritorio y de los programas del usuario.

Cada usuario tiene un perfil, tanto si el administrador lo configura como si no, porque se crea un perfil automáticamente para cada usuario cuando inicia sesión en un equipo.

Los perfiles ofrecen numerosas ventajas:

1. Múltiples usuarios pueden utilizar el mismo equipo, con la configuración de cada uno recuperada al iniciar la sesión al mismo estado en que estaba cuando cerró la sesión.
2. Los cambios hechos por un usuario en el escritorio no afectan a otros usuarios.
3. Los perfiles de usuario se almacenan en el servidor y así se pueden seguir a los usuarios a cualquier equipo de la red.

Desde el punto de vista de un administrador, la información del perfil puede ser una valiosa herramienta para configurar perfiles de usuario predeterminados (perfiles obligatorios) para todos los usuarios de la red o para personalizar los perfiles predeterminados para diferentes departamentos.

Estos perfiles obligatorios permiten a un usuario hacer cambios en el escritorio mientras está conectado, pero no guardar ninguno de los cambios.

Un perfil obligatorio siempre se muestra exactamente igual cada vez que un usuario inicia sesión. Tenemos los siguientes tipos de perfiles:

1. **Perfiles locales:** perfiles creados en un equipo cuando un usuario inicia sesión. El perfil es específico de un usuario, local al equipo y se almacena en el disco duro del equipo local.
2. **Perfiles móviles:** perfiles creados por un administrador y almacenados en un servidor. Siguen al usuario a cualquier máquina Windows de la red.
3. **Perfiles obligatorios:** perfiles móviles que sólo pueden ser modificados por un administrador.

Todos los perfiles comienzan como una copia del perfil **Default User** (nombre del usuario).

La información del registro para **Default User** se encuentra en el archivo **Ntuser.dat** incluido en el perfil **Default User**. Dentro de cada perfil se encuentran las siguientes carpetas:

- **Configuración local:** Datos de programa, Historial y Archivos temporales.
- **Cookies:** Mensajes enviados a un navegador web por un servidor web y almacenados localmente para registrar información y preferencias del usuario.
- **Datos de programa:** configuraciones específicas de programa determinadas por el fabricante del programa además de la configuración de seguridad específica del usuario.
- **Entorno de red:** Accesos directos a Mis sitios de red.
- **Escritorio:** Archivos, carpetas, accesos directos del escritorio y su apariencia.
- **Favoritos:** Accesos directos a ubicaciones favoritos y sitios web.
- **Impresoras:** Accesos directos a elementos de la carpeta Impresoras.
- **Menú Inicio:** Elementos del menú Inicio del usuario.
- **Mis documentos:** Documentos del usuario y Mis imágenes, que contiene los archivos gráficos del usuario.
- **Plantillas:** Plantillas de programas.
- **Reciente:** Accesos directos a las carpetas y archivos más recientemente utilizados.
- **SendTo:** Elementos del menú Enviar a.

De forma predeterminada, sólo Cookies, Escritorio, Favoritos, Menú Inicio y Mis documentos son visibles en el Explorador de Windows. Las otras carpetas están ocultas; para verlas es necesario seleccionar Opciones de carpeta, pulsar en la pestaña Ver y seleccionar Mostrar archivos, carpetas y unidades ocultos.

Perfiles locales

Como ya sabemos los perfiles locales se crean en los equipos cuando los usuarios individuales inician sesión. En un equipo con una nueva instalación de Windows Server 2016, el perfil del usuario está en la carpeta *Usuarios*.

La primera vez que un usuario inicia sesión en un equipo, se genera una carpeta de perfil para el usuario, y los contenidos de la carpeta **Default User** se copian en ella. Cualquier cambio realizado por el usuario al escritorio se almacena en ese perfil de usuario cuando cierra la sesión.

Si un usuario tiene una cuenta local en el equipo además de una cuenta de dominio e inicia sesión varias veces utilizando ambas cuentas, el usuario tendrá dos carpetas de perfil en el equipo local: una para cuando el usuario inicie sesión en el dominio utilizando la cuenta de usuario del dominio y otra para cuando el usuario inicie sesión localmente en el equipo. El perfil local se mostrará con el nombre de inicio de sesión. El perfil de dominio también se mostrará con el nombre de inicio de sesión, pero llevará añadido el nombre del dominio.

Perfiles móviles

Los perfiles móviles son una gran ventaja para los usuarios que utilizan frecuentemente más de un equipo. Un perfil móvil se almacena en un servidor y, después de que el inicio de sesión del usuario sea autenticado en el servicio de directorio, se copia al equipo local. Esto permite al usuario tener el mismo escritorio, la configuración de las aplicaciones y la configuración local en cualquier máquina Windows.

El funcionamiento es el siguiente: se asigna una ubicación de un servidor para perfiles de usuario y se crea una carpeta compartida con los usuarios que tengan perfiles móviles. Se introduce una ruta de acceso a esa carpeta en la ventana propiedades de los usuarios. La siguiente vez que el usuario inicie sesión en un equipo, el perfil del servidor se descarga al equipo local. Cuando el usuario cierra la sesión, el perfil se almacena tanto localmente como en la ubicación de la ruta de acceso al perfil del usuario. La especificación de la ruta de acceso al perfil del usuario es todo lo que hace falta para convertir un perfil local en un perfil móvil, disponible en todo el dominio.

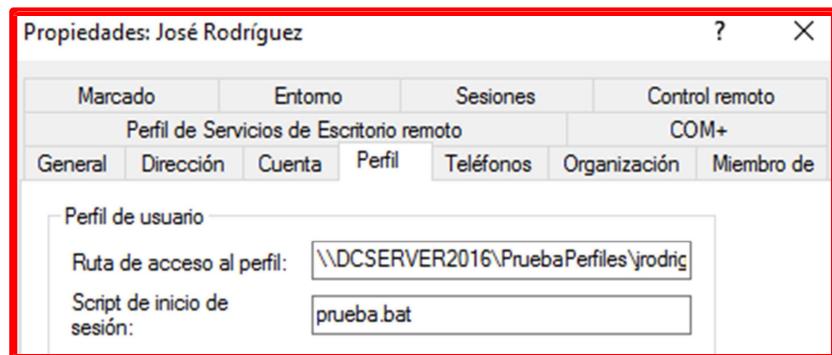
Cuando el usuario inicia sesión de nuevo, el perfil del servidor se compara con la copia en el equipo local y se carga para el usuario la más reciente. Si el servidor no está disponible, se utiliza la copia local. Si el servidor no está disponible y es la primera vez que el usuario ha iniciado sesión en el equipo, se crea un perfil de usuario localmente utilizando el perfil Default User. Cuando el perfil no es descargado a un equipo local a causa de problemas con el servidor, el perfil móvil no se actualiza cuando el usuario cierra la sesión.

Configuración de los perfiles móviles

Para configurar un perfil móvil simplemente hay que asignar una ubicación en un servidor y completar los siguientes pasos:

1. Crear una carpeta compartida (**PruebaPerfiles**) en el servidor para los perfiles, con permisos de **lectura** y **escritura** para el grupo **Todos** por ejemplo.
2. En la pestaña **Perfil** de la cuenta de usuario (jrodriguez) hay que dar la ruta de acceso a la carpeta compartida (Ruta de acceso al perfil), como **\nombre_del_servidor\carpeta_de_perfiles_compartida%\username%**

Actualizamos. Una vez que se ha creado una carpeta de perfiles compartida en un servidor y se ha suministrado una ruta de acceso al perfil en la cuenta del usuario, se ha habilitado un perfil móvil. La configuración del usuario de su escritorio se copia y almacena en el servidor y estará disponible para el usuario desde cualquier equipo.



Inicia sesión en **CLIENTEWIN7** (y en **CLIENTEW10** después), con **jrodriguez**, haz cambios en el fondo de escritorio y crea una carpeta en él. Cierra la sesión.

Vuelve a iniciarla y comprueba que los cambios se mantienen.

Comprueba también que el usuario **jrodriguez** tiene perfil móvil y que se ha creado la carpeta del perfil del usuario.



Perfiles obligatorios

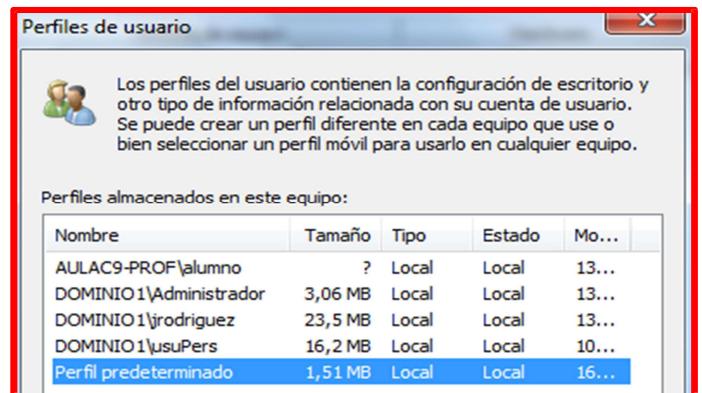
Podemos configurar el perfil de usuario local predeterminado para convertirlo en un perfil obligatorio. Mediante esta acción, permitiremos que todos los usuarios utilicen un perfil central. Para ello, debemos preparar la ubicación del perfil obligatorio, copiar el perfil de usuario local predeterminado en la ubicación del perfil obligatorio y, a continuación, configurar una ubicación para el perfil de un usuario que se establezca como perfil obligatorio.

1. Paso 1: Preparar la ubicación del perfil obligatorio:

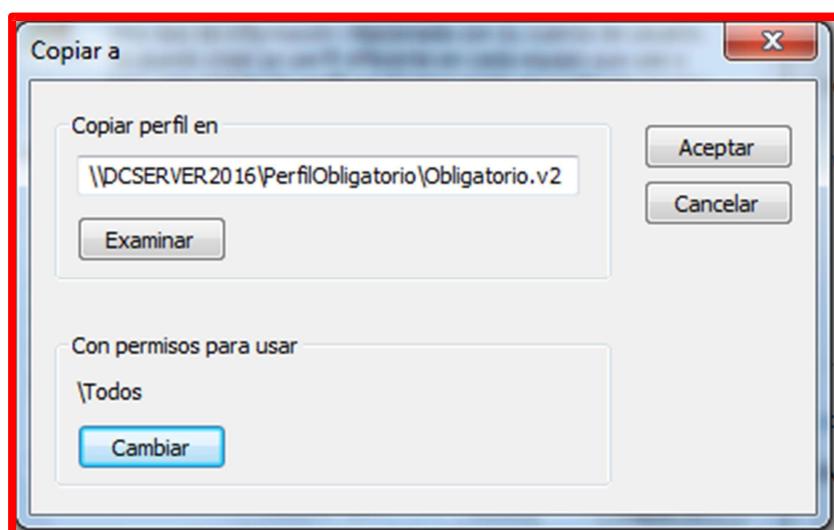
1. En nuestro controlador de dominio, crearemos una nueva carpeta, llamada **PerfilObligatorio** y dentro de ella otra llamada, por ejemplo, **Obligatorio.v2** (debe terminar en v2).
2. Compartimos **PerfilObligatorio** con permiso de **lectura** para el grupo **Usuarios del dominio** (el grupo **Administradores** debe tener permisos de **lectura** y **escritura**).

2. Paso 2: Copiar el perfil de usuario predeterminado en la ubicación del perfil obligatorio

1. Inicia sesión en el cliente windows7, con el **Administrador local**.
2. Entramos en **Equipo > Propiedades > Cambiar configuración > Opciones avanzadas**.
3. En **Perfiles de usuario**, pulsamos el botón **Configuración**. El cuadro de diálogo **Perfiles de usuario** mostrará una lista de perfiles que se encuentran almacenados en el equipo.
4. Selecciona **Perfil predeterminado** y, a continuación, pulsamos en **Copiar a...**



- En el cuadro de texto **Copiar perfil en**, escribimos la ruta de acceso de red de la carpeta del perfil de usuario predeterminado de Windows que creamos en la sección anterior, aunque también podemos pulsar en **Examinar** y buscar la carpeta en la Red: **\nombre_del_Servidor\PerfilObligatorio\Obligatorio.v2**.
- En el botón **Cambiar**, de la sección **Con permisos para usar**, escribimos **Todos** (nos pedirá las **credenciales del Administrador del dominio**) y, a continuación, pulsamos en **Aceptar** para iniciar la copia del perfil.

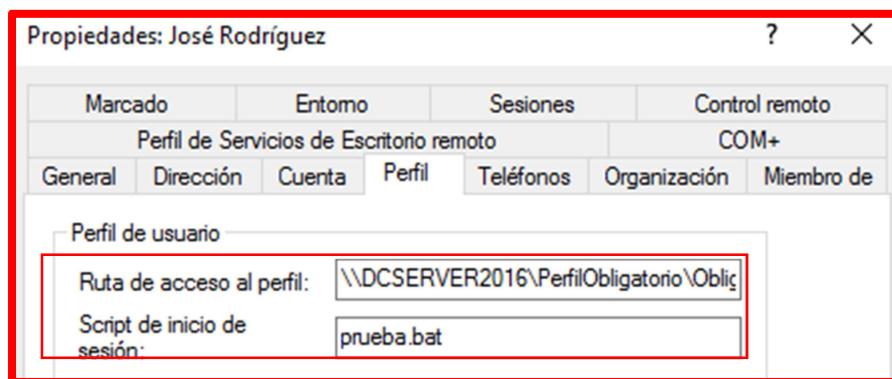


- Una vez **finalizado el proceso de copia, cierra la sesión** en el equipo cliente.
- En el servidor**, buscamos la carpeta creada **PerfilObligatorio\Obligatorio.v2**.
- Desplegamos el menú **Organizar** y, a continuación, elegimos **Opciones de carpeta y búsqueda** y pulsamos en la pestaña **Ver**, activamos la casilla de verificación **Mostrar archivos, carpetas y unidades ocultos**, y **desactivamos las casillas de verificación Ocultar las extensiones de archivo** para tipos de **archivo conocidos** y Ocultar archivos protegidos del sistema operativo, hacemos clic en **Sí** para descartar la advertencia y, a continuación, hacemos clic en **Aceptar** para aplicar los cambios y cerrar el cuadro de diálogo.
- Hacemos clic en el archivo **ntuser.dat**, y lo renombramos como **ntuser.man**.

3. Paso 3: Preparar una cuenta de usuario

- Como **administrador de dominio**, abrimos la consola de administración de **Usuarios y equipos de Active Directory**.
- Hacemos clic con el **botón secundario en la cuenta de usuario** que deseamos aplicar a perfil de usuario obligatorio, por ejemplo, **jrodriguez** y, a continuación, elegimos sus **Propiedades**.
- Elegimos la ficha **Perfil**, escribimos la ruta de acceso de red creada, **\nombre_del_Servidor\PerfilObligatorio\Obligatorio** en el cuadro de texto de la ruta de acceso del perfil. En

este caso, **no** agregamos .v2 al final.



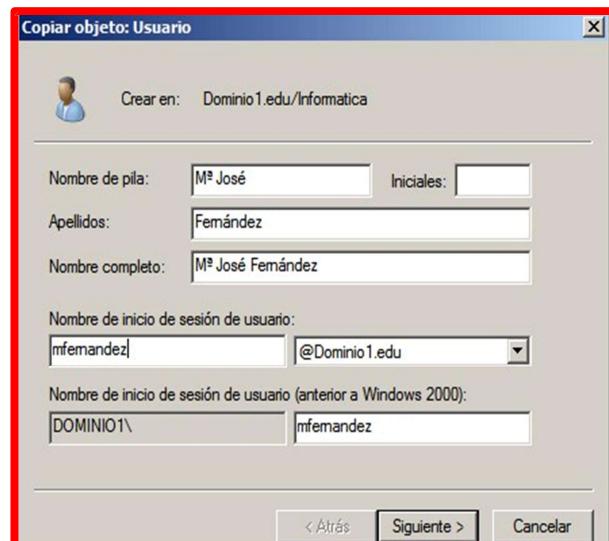
4. Aceptamos, actualizamos y cerramos la consola de administración de **Usuarios y equipos de Active Directory**. Ahora el usuario *jrodriguez* utilizará el perfil de usuario obligatorio.

Ejercicio: Para comprobarlo inicia sesión con él en el cliente windows7, cambia el fondo de escritorio y crea alguna carpeta en él. Cierra la sesión y vuelve a iniciarla. Como puedes comprobar se carga el perfil predeterminado de windows7 y ninguno de los cambios realizados en el perfil de *jrodriguez* permanecen. Configura ahora un perfil móvil para este usuario y haz los cambios anteriores, ahora verás que al cerrar e iniciar sesión sí se conservan los cambios realizados en su perfil.

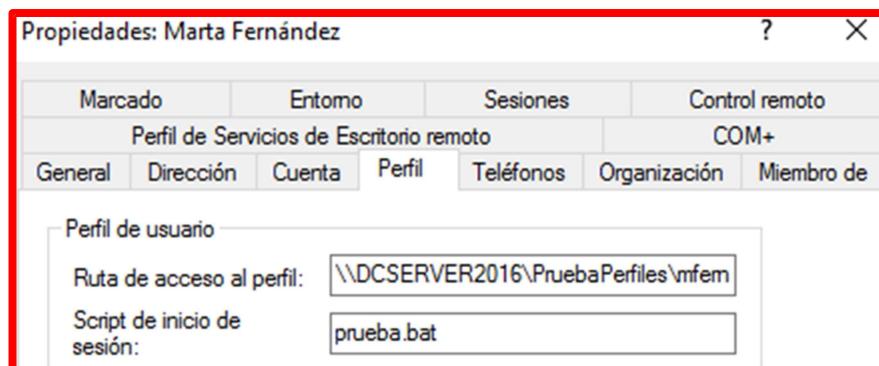
2.7. Plantillas de cuentas

Podemos crear cuentas de usuarios a partir de plantillas. Por ejemplo, tenemos que dar de alta 15 usuarios del departamento de *Compras*. Para crear la plantilla primero crearemos un usuario y completaremos todos los datos de su ficha: datos personales, del departamento, ... y esta cuenta será nuestra base para crear las otras.

El proceso es el siguiente: pulsamos con el **botón derecho en la cuenta del usuario** que queremos duplicar (en nuestro caso José Rodríguez) y seleccionamos "**Copiar ...**" para que aparezca esta pantalla:



Nos pide los datos básicos del usuario, los completamos y pulsamos en siguiente para establecer la contraseña y si todo va bien nos habrá creado la cuenta, pero con la considerable ventaja de que todos los campos de configuración e identificación completados ya que ha copiado los de la cuenta que utilizó de "*plantilla*". Por ejemplo se puede usar para crear scripts de inicio de varios usuarios.



2.8. Habilitar y desbloquear cuentas de usuarios

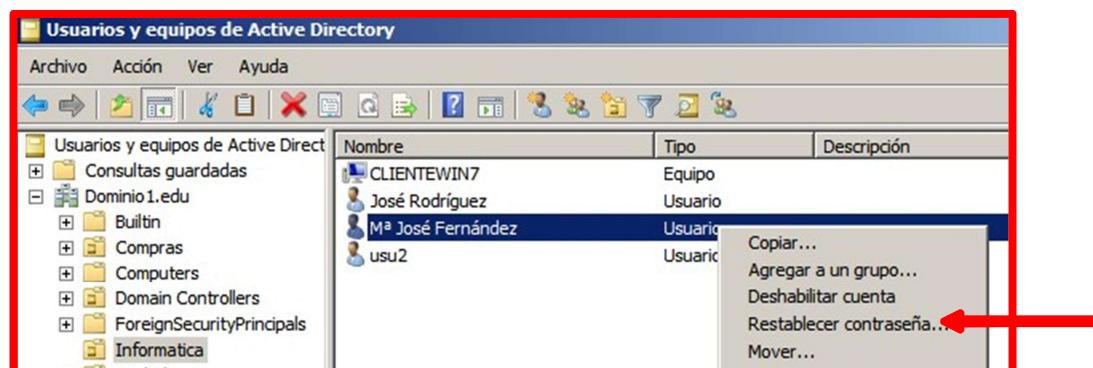
Esta parte va a ser una de las más importantes en nuestra administración ya que vamos a gestionar los usuarios que pueden acceder a los recursos. Se incluye la posibilidad de bloquear/desbloquear las cuentas y su deshabilitación.

Después de crear las cuentas de usuario, se suelen realizar tareas administrativas para garantizar que la red sigue cumpliendo los requisitos de la empresa. Estas tareas incluyen como hemos dicho las opciones de habilitar y deshabilitar cuentas de usuario y de equipo. Al habilitar o deshabilitar una cuenta, concede o restringe el acceso a la misma.

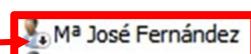
Para que un entorno sea seguro, el administrador de sistemas debe deshabilitar las cuentas de los usuarios cuando éstos no vayan a utilizarlas durante un periodo de tiempo largo, aunque las necesiten más adelante. Por ejemplo, en estos casos será necesario habilitar o deshabilitar una cuenta:

- Si el usuario va a permanecer ausente dos meses, habrá que deshabilitar la cuenta cuando el usuario deje el trabajo y habilitarla cuando vuelva.
- Cuando se agregan a la red cuentas que se van a utilizar en el futuro o por razones de seguridad, habrá que deshabilitar las cuentas hasta que sean necesarias.
- Cuando no deseé que se autentique a los usuarios desde un equipo compartido, tendrá que deshabilitar la cuenta.

Para habilitar o deshabilitar una cuenta pulsaremos con el botón derecho sobre ella:



En la pantalla aparece la opción "**Deshabilitar cuenta**" porque la cuenta está correctamente habilitada y así poder cambiar su estado desde aquí. Las cuentas deshabilitadas aparecen con una flecha hacia abajo.



Intenta iniciar sesión desde *CLIENTEWIN7* con este usuario. En el caso contrario, si la cuenta está deshabilitada podemos habilitarla, de forma análoga: Habilita la cuenta de Mª José Fernández e inicia sesión desde *CLIENTEWIN7* con ella.

Una cuenta de usuario se bloquea cuando ha sobrepasado el umbral de bloqueo de la cuenta para un dominio. Esto ocurre porque el usuario ha intentado muchas veces obtener acceso a la cuenta con una contraseña incorrecta o porque un pirata informático ha intentado descubrir las contraseñas de usuario y ha activado la directiva de bloqueo de la cuenta.

Los usuarios autorizados pueden bloquear una cuenta al escribir mal la contraseña, al olvidarla o al haber intentado cambiarla en un equipo después de iniciar la sesión en otro. El equipo en el que se escribe una contraseña incorrecta intenta continuamente autenticar al usuario. Y puesto que la contraseña que se está utilizando es incorrecta, la cuenta finalmente se bloquea.

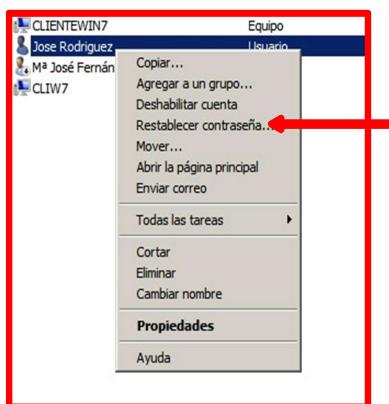
La **configuración de seguridad del directorio activo determina el número de intentos fallidos** de inicio de sesión que provoca el bloqueo de una cuenta. El usuario no podrá utilizar la cuenta bloqueada hasta que el administrador la restablezca o hasta que el tiempo de bloqueo finalice. Cuando una cuenta de usuario se bloquea, aparece un mensaje de error y no se permite al usuario que realice más intentos de inicio de sesión.

Un usuario puede bloquear una cuenta si intenta iniciar la sesión muchas veces con una contraseña incorrecta. Los intentos con contraseña incorrecta se producen cuando:

- El usuario inicia la sesión en la pantalla correspondiente, pero proporciona una contraseña incorrecta.
- El usuario inicia la sesión con una cuenta local y proporciona una cuenta de usuario de dominio y una contraseña incorrecta cuando intenta obtener acceso a los recursos de la red.
- El usuario inicia la sesión con una cuenta local y proporciona una cuenta de usuario de dominio y una contraseña incorrecta cuando intenta obtener acceso a los recursos de la red con el comando "runas".

De forma predeterminada, los intentos de inicio fallidos de la cuenta de dominio no quedan almacenados cuando se desbloquea la estación de trabajo (usando un protector de pantalla protegido con contraseña). Para cambiar este comportamiento, cambiaremos la **configuración de la directiva de grupo *Inicio de sesión interactivo***: **requerir la autenticación del controlador de dominio para desbloquear el equipo**. Esto lo veremos en el tema de las políticas.

Para desbloquear una cuenta utilizaremos la opción de desbloqueo de la pestaña de la cuenta del usuario. También podemos restablecer la contraseña del usuario con el botón derecho del ratón encima de la cuenta de usuario:



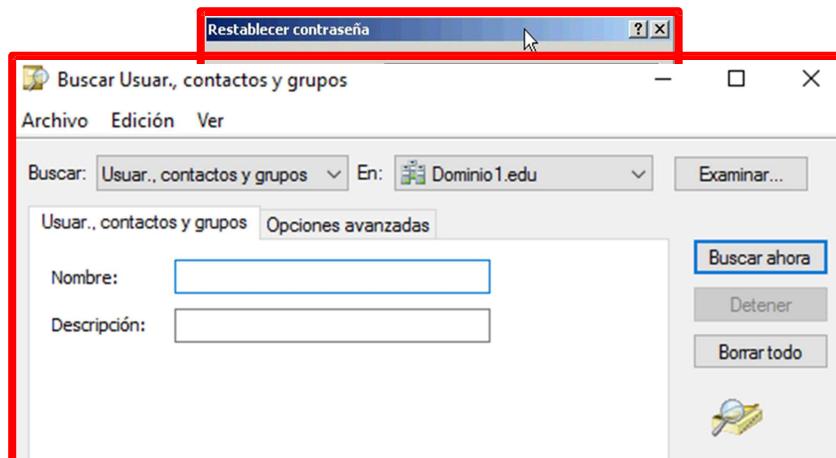
Al restablecer la cuenta nos pedirá que introduzcamos una nueva contraseña:

Con lo que le hemos "resetead" la cuenta cambiando la contraseña y dejando marcada la casilla de verificación, que el usuario vuelve a escribir una nueva. Este sería el mejor sistema para actuar cuando un usuario nos avise de que ha bloqueado la cuenta. Podemos desbloquearla desde la ficha del usuario o restablecerla desde aquí.

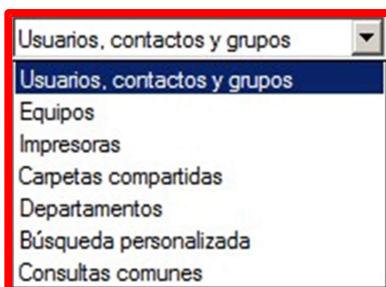
3. Buscar equipos y usuarios

Una vez que tengamos nuestro Directorio Activo configurado con todos los equipos, usuarios, grupos y otros objetos, habrá que hacer el mantenimiento de todos ellos. Para localizar cada uno de estos objetos utilizaremos una pantalla de consulta de objetos que nos proporciona la consola administrativa.

Para acceder a la pantalla de consulta podemos hacerlo, por ejemplo, desde la opción "**Buscar**" que sale al pulsar con el botón derecho del ratón en el nombre de nuestro dominio "**Dominio1.edu**" en la consola administrativa:



En el desplegable "**Buscar**" podemos seleccionar un montón de tipos de objetos. Por defecto aparece el más utilizado que es el de los **Usuarios, contactos y grupos**.



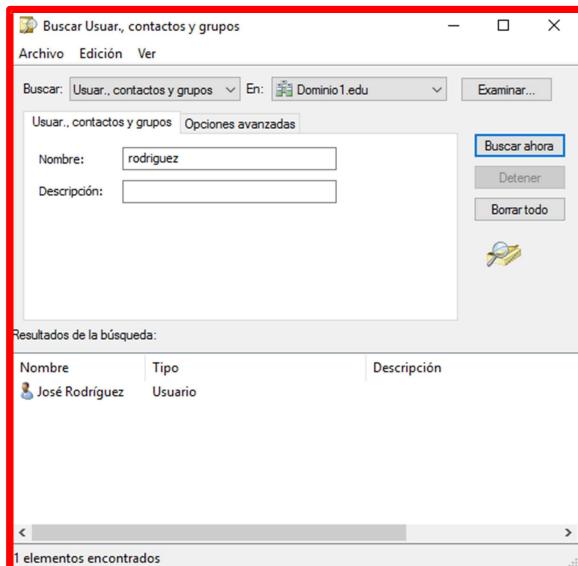
Puesto que todas las cuentas de usuario se encuentran en el Directorio Activo, los administradores pueden buscar las que quieren administrar.

Esta era una de las opciones que no hemos activado, pero en todos los objetos de cuentas de usuarios y equipos teníamos una opción de "**Administrado por**". Esto es interesante para cuando los dominios son muy grandes y hay varios administradores de red. En ese caso pueden dividirse por ejemplo las unidades organizativas para administrarlas por separado.

Con la **búsqueda de cuentas** no es necesario que examinemos cientos o miles de cuentas en **Usuarios y equipos del directorio**. Además, como hemos visto en el cuadro desplegable podemos buscar también otros objetos como equipos, impresoras y carpetas compartidas. Una vez haya encontrado estos objetos, podremos administrarlos desde el cuadro **Resultado de la búsqueda**.

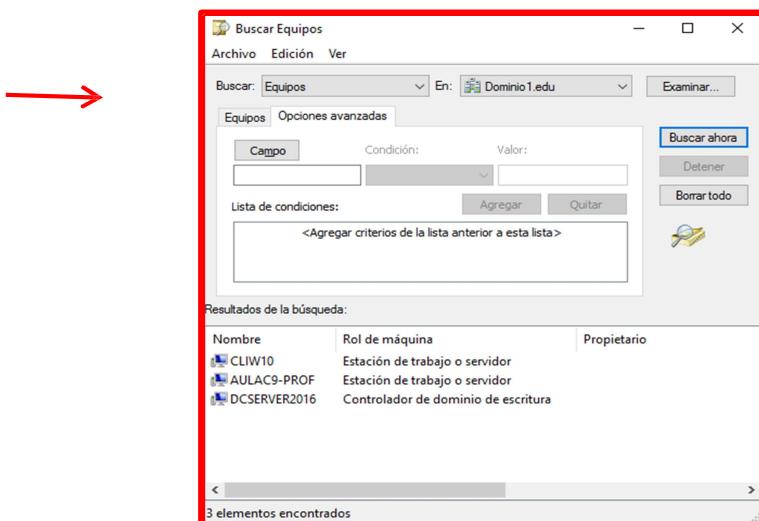
Una vez finalizada la búsqueda, se muestran los resultados y podremos realizar tareas de administración de los objetos encontrados. Las funciones administrativas disponibles dependen del tipo de objeto encontrado. Por ejemplo, si estamos buscando cuentas de usuario, podremos cambiarles el nombre, eliminarlas, deshabilitarlas, restablecer la contraseña, moverlas a otra unidad organizativa o modificar sus propiedades.

Vamos a ver esto con un ejemplo, pon para buscar todo o parte de un nombre, vamos a poner "rodriguez" y veamos qué encuentra:



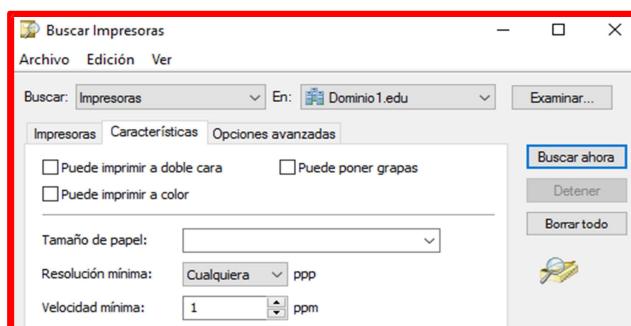
Como lo que nos ha encontrado es una cuenta de usuario, si pulsamos con el botón derecho sobre ella tendremos las mismas opciones que si estuviéramos en su unidad organizativa. Y con doble clic en ella accederemos a su pantalla de configuración.

Si pulsamos en la segunda pestaña de "**Opciones avanzadas**" podremos además ponerles campos especiales como la del administrador de la cuenta:



Cuando una impresora compartida está publicada en el Active Directory, podemos buscar impresoras: utilizar "**Buscar**" y luego "**Impresoras**" para buscarla mediante criterios como el número de activo, el lenguaje que utiliza la impresora o si admite impresión a doble cara.

Una vez encontrada la impresora podemos conectar con ella haciendo clic con el botón derecho del ratón en la impresora en el cuadro **Resultado de la búsqueda** y, luego, hace clic en **Conectar** o doble clic en la impresora:



En definitiva, es una potente herramienta para localizar cualquier tipo de objeto en nuestro directorio activo.

4. Grupos

Los grupos son uno de los temas más importantes a la hora de organizar nuestro Directorio Activo. Nos servirán para gestionar los permisos de los recursos. Si este proceso lo diseñamos bien podemos administrar los recursos de una forma muy sencilla. En cualquier caso esto lo veremos en los siguientes temas, cuando veamos los recursos...

Decimos entonces que un grupo es un conjunto de cuentas de usuario. Utilizaremos los grupos para administrar de forma eficaz el acceso a los recursos de un dominio y simplificar, de este modo, la administración y mantenimiento de la red. También los utilizaremos de forma independiente o incluiremos un grupo dentro de otro para simplificar aún la administración (no se puede hacer esto en Windows 7).

Antes de poder utilizar grupos de forma eficaz, debemos conocer la función de los grupos y los tipos de grupo que se pueden crear. El servicio de directorio admite diferentes tipos de grupos y ofrece también opciones para determinar el ámbito del grupo, es decir, cómo puede utilizarse el grupo en varios dominios.

Tipos de grupos:

Solapa	Descripción
Seguridad	Se utilizan para asignar derechos y permisos de usuario.
Distribución	Se utilizan únicamente en aplicaciones de correo electrónico. No se pueden utilizar para asignar permisos.

Aquí veremos solo el primer tipo porque el segundo se utiliza únicamente para sistemas de correo electrónico.

4.1. Administrar grupos

Los **grupos** son un **conjunto de cuentas** de **equipo** y de **usuario** que se pueden **administrar como una sola unidad**.

Los grupos:

- Simplifican la administración al facilitar la concesión de permisos para recursos a todo un grupo en lugar de a cada una de las cuentas de usuario individualmente.
- Pueden estar basados en el Directorio Activo o ser locales (de un equipo).
- Se distinguen por su ámbito y tipo.
- Pueden anidarse, es decir, se puede agregar un grupo a otro.

El **ámbito** de un grupo determina si el **grupo comprende varios dominios o se limita a uno solo**. Los ámbitos de grupo permiten utilizar grupos para la concesión de permisos. El ámbito de grupo determina:

- Los dominios desde los que puede agregar miembros al grupo.
- Los dominios en los que puede utilizar el grupo para conceder permisos.
- Los dominios en los que puede anidar el grupo en otros grupos.

El **ámbito** de un grupo determina **cuáles son los miembros del grupo**. Las reglas de pertenencia controlan los miembros que pueden contener un grupo y los grupos de los que puede ser miembro. Los miembros de un grupo están formados por **cuentas de usuario, cuentas de equipo y otros grupos**.

Para asignar los miembros correctos a los grupos y para anidar un grupo, es importante conocer las características del ámbito de grupo. Existen los siguientes ámbitos de grupo:

- Global
- Universal
- Local de dominio
- Local

Hay dos tipos de grupos en el Directorio Activo:

- **Grupos de seguridad**. Utilizaremos estos grupos para asignar derechos y permisos de usuario a grupos de usuarios y equipos. Los derechos especifican las acciones que pueden realizar los miembros de un grupo de seguridad en un dominio o bosque, y los permisos especifican los recursos a los que puede obtener acceso un miembro de un grupo en la red.

- **Grupos de distribución.** Son un tipo especial que se utiliza sólo para crear grupos de distribución para el correo electrónico. Con Exchange de Microsoft, con estos grupos podríamos crear listas de distribución o grupos de usuarios por departamento, ...

Crearemos siempre "*grupos de seguridad*" En esta tabla vemos los ámbitos de los grupos:

	Windows 2000 mixto (predeterminado)	Windows 2000 nativo	Windows 2003-2016 Server
Controladores de dominio admitidos	Windows NT 4.0, Windows 2000 y 2003	Windows 2000 y 2003	Windows 2003-2016
Ámbitos de grupo admitidos	Global y local de dominio	Global, local de dominio y universal	Global, local de dominio y universal

Las características de los grupos dependen del nivel funcional de dominio. Recuerda que en la instalación nos pedía el tipo de instalación ya que podía ser mixta (si había equipos anteriores a Windows 2000) o nativa (todos los clientes son W2000 y XP). La funcionalidad de dominio activa funciones que afectan a todo un dominio y sólo a ese dominio. Hay tres niveles funcionales de dominio disponibles: Microsoft Windows 2000 mixto, Windows 2000 nativo y Microsoft Windows Server 2003/2016. Los dominios funcionan de forma predeterminada en el nivel funcional Windows 2000 mixto. Luego pondremos el nivel funcional de dominio a Windows 2000 nativo, Windows Server 2003 o Windows Server 2016.

Ahora vamos a aclarar el tema de los ámbitos de los dominios, es decir qué alcance tienen. Recuerda que había estos ámbitos: global, local de dominio, universal y local.

Grupos globales

Un grupo global es un grupo de distribución o de seguridad que puede contener usuarios, grupos y equipos procedentes del mismo dominio que el grupo global. Utilizaremos grupos de seguridad globales para asignar derechos y permisos de usuario a los recursos de cualquier dominio del bosque. Veamos sus propiedades:

	Reglas de los grupos globales
Miembros	<ul style="list-style-type: none"> • Modo mixto: cuentas de usuario del mismo dominio • Modo nativo: cuentas de usuario, cuentas de equipo y grupos globales del mismo dominio
Puede ser miembro de	<ul style="list-style-type: none"> • Modo mixto: grupos locales de dominio • Modo nativo: Universal y grupos locales de dominio en todos los grupos de dominio y globales del mismo dominio
Ámbito	Todos los dominios del bosque y dominios de confianza
Permisos	Todos los dominios del bosque y dominios de confianza

Debido a que los grupos globales son visibles en todo el bosque, no debemos crearlos para obtener acceso a recursos específicos del dominio. Utilizaremos estos grupos para organizar a los usuarios que comparten las mismas tareas de trabajo y necesitan requisitos de acceso a la red similares. Para controlar el acceso a los recursos de un dominio, sería conveniente utilizar otro tipo de grupo (los *universales*).

Grupos universales

Un grupo universal es un grupo de distribución o de seguridad que contiene usuarios, grupos y equipos de cualquier dominio del bosque. Utilizaremos grupos de seguridad universales para asignar derechos y permisos de usuario a los recursos de cualquier dominio del bosque. Resumiendo, sus propiedades:

	Reglas de los grupos universales
Miembros	<ul style="list-style-type: none"> • Modo mixto: no se puede aplicar • Modo nativo: cuentas de usuario, cuentas de equipo, grupos globales y otros grupos universales de cualquier dominio del bosque
Puede ser miembro de	<ul style="list-style-type: none"> • Modo mixto: no se puede aplicar • Modo nativo: Grupos locales de dominio y universales de cualquier dominio
Ámbito	Todos los dominios del bosque
Permisos	Todos los dominios del bosque

Utilizaremos grupos universales para anidar grupos globales y poder asignar permisos a recursos relacionados de varios dominios. Un dominio de Windows Server 2016 debe estar en el modo Windows 2000 nativo o superior para poder utilizar grupos universales.

Parecen iguales, pero éstos sólo se pueden crear, como hemos dicho, en dominios de Directorio Activo "nativos" es decir, sin la compatibilidad de equipos anteriores a W2000. Además, estos grupos pueden contener grupos globales, lo que le da un alcance mayor que el anterior.

Grupos locales del dominio

Aunque sólo estamos viendo un bosque con un sólo dominio, podríamos tener una estructura más compleja y englobar dentro de un mismo bosque distintos dominios. Un grupo local de dominio es un grupo de distribución o de seguridad que puede contener grupos universales, grupos globales, otros grupos locales de dominio de su propio dominio y cuentas de cualquier dominio del bosque. Utilizaremos grupos de seguridad locales de dominio para asignar derechos y permisos de usuario sólo a recursos del mismo dominio en el que se encuentra ubicado el grupo local de dominio.

	Reglas de los grupos globales
Miembros	<ul style="list-style-type: none"> Modo mixto: cuenta de usuario, cuentas de equipo y grupos globales de cualquier dominio Modo nativo: cuentas de usuario, cuentas de equipo, grupos globales y otros grupos universales de cualquier dominio del bosque y grupos locales de dominio del mismo dominio
Puede ser miembro de	<ul style="list-style-type: none"> Modo mixto: ninguno Modo nativo: Grupos locales de dominio del mismo dominio
Ámbito	Visible sólo en su propio dominio
Permisos	Dominio al que pertenece el grupo local del dominio

4.2. Dónde crear los grupos y nomenclatura

Los grupos se crean en los dominios y para crearlos utilizaremos nuestra consola administrativa de [Usuarios y equipos de Active Directory](#).

Si tenemos los permisos adecuados podremos crear también grupos en otro dominio del bosque o en una unidad organizativa.

Además de por el dominio en el que se ha creado, un grupo también se caracteriza por su ámbito. El ámbito de un grupo determina:

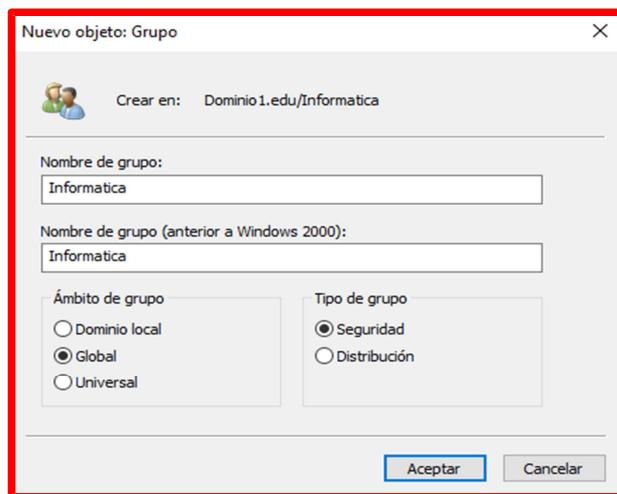
- El dominio desde el que se pueden agregar miembros.
- El dominio en el que son válidos los derechos y permisos de usuario asignados al grupo.

Por ejemplo, si nuestra estructura tiene varias unidades organizativas, cada una de ellas con un administrador diferente, es posible que queramos crear grupos globales en esas unidades organizativas para que los administradores puedan administrar la pertenencia al grupo de los usuarios incluidos en sus respectivas unidades organizativas.

Si es necesario que los grupos controlen el acceso fuera de la unidad organizativa, podemos anidar los grupos de la unidad organizativa en grupos universales (o en otros grupos con ámbito global) que puedan utilizarse en cualquier otra ubicación del bosque.

4.3. Crear grupos

Vamos a crear un grupo en la unidad organizativa *Informatica* para luego meter en él los dos usuarios que tenemos creados. Pulsamos con el **botón derecho en la unidad organizativa** y decimos que "**Nuevo**" y "**Grupo**":



Escribiremos el nombre de "*Informatica*", sin acento.

En los nombres de cualquier objeto del directorio activo debemos evitar la utilización de caracteres extendidos (acentos, eñes, etc.) no va a pasar nada, pero en ocasiones nos encontraremos con servidores en inglés que no tienen el idioma español instalado y podríamos tener problemas. Si hablamos de un sólo dominio sencillo en instalaciones básicas pase.

Como vemos tenemos debajo del nombre como se llamará en equipos anteriores a W2000 que en principio es el mismo nombre, y así debemos intentar que se quede, lo mismo que con las cuentas de usuarios.

Debajo a la izquierda tenemos el ámbito que por defecto es **Global**, es decir, visible en todos los dominios del bosque. Si tuviéramos más bosques conectados tendríamos la opción de hacerlo "**Universal**". Y finalmente, en la parte derecha el tipo de grupo que será de **Seguridad** ya que el otro es sólo para el correo electrónico.

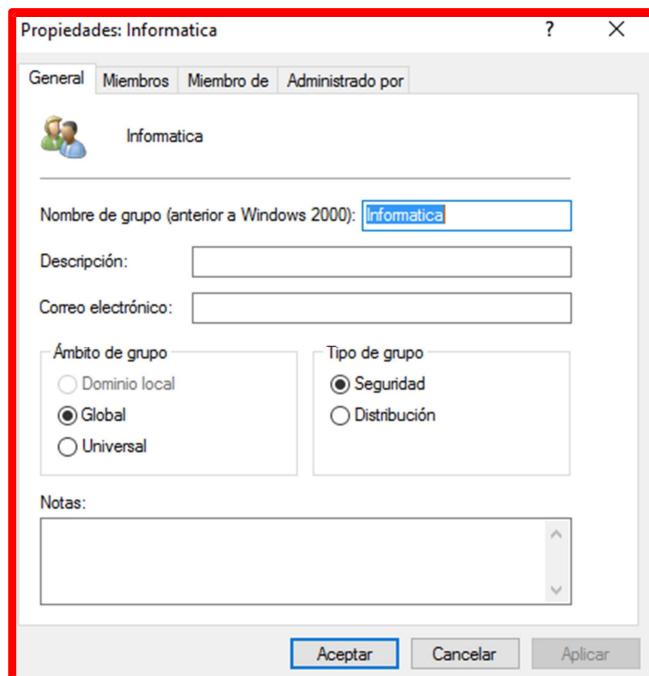
Nombre	Tipo
AULAC9-PROF	Equipo
Informatica	Grupo de seguridad - Global
José Rodríguez	Usuario
Mª José Fernández	Usuario

Al crearlo, vemos que aparece en nuestra unidad organizativa y con el icono que indica que es un grupo.

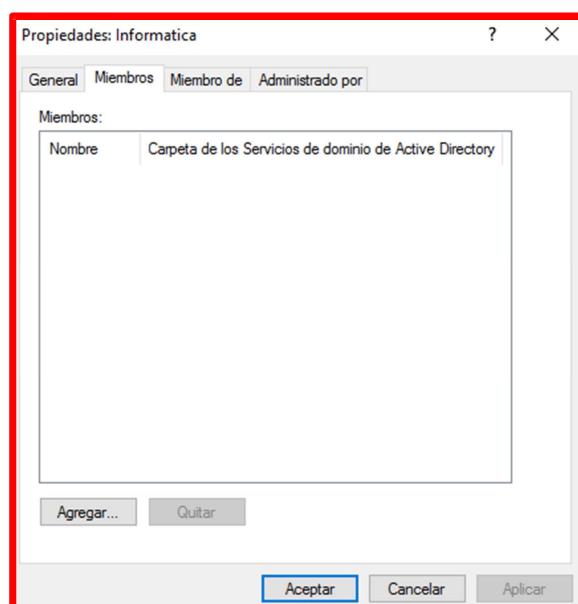
Una de las organizaciones de Directorio Activo que se utiliza mucho es crear unidades organizativas dentro de esta de "*Informatica*" para incluir los tipos de objetos: usuarios, equipos, grupos, etc.

De esta forma si le dejamos a alguien la delegación de la unidad organizativa de los equipos dentro de "*Informatica*" sólo tendrá acceso a estos objetos y no a los usuarios.

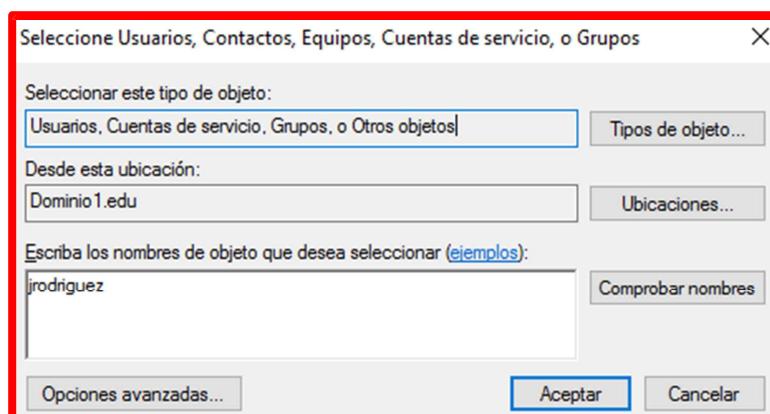
Veamos ahora los detalles de este grupo, haz doble clic sobre él:



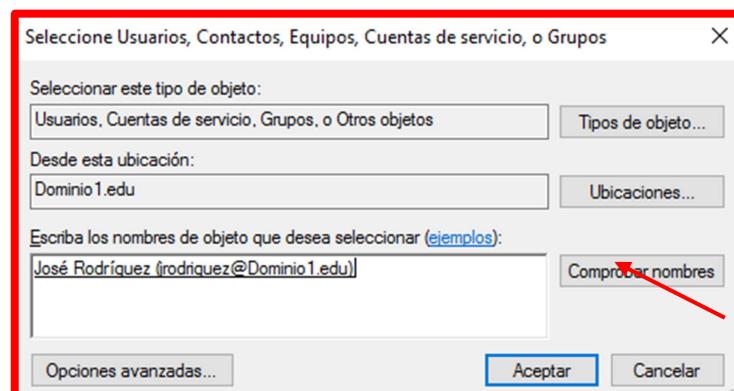
Vemos los datos generales que se introdujeron antes. Ahora debemos añadir los miembros de este grupo, así que seleccionamos la segunda pestaña.



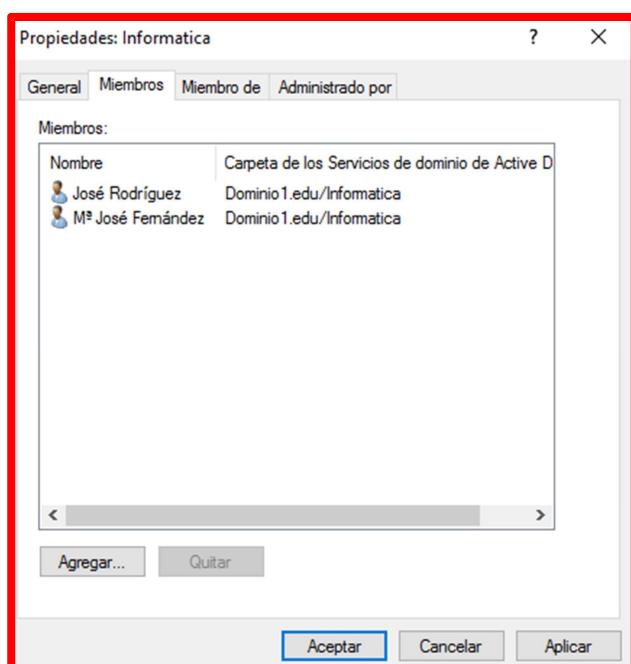
De momento no hay ningún usuario así que pulsamos en "**Agregar**" para añadir los que queramos...



Podemos escribir los usuarios en el cuadro de abajo, si sabemos el nombre de usuario lo mejor es escribirlo y darle al botón "**Comprobar nombres**":

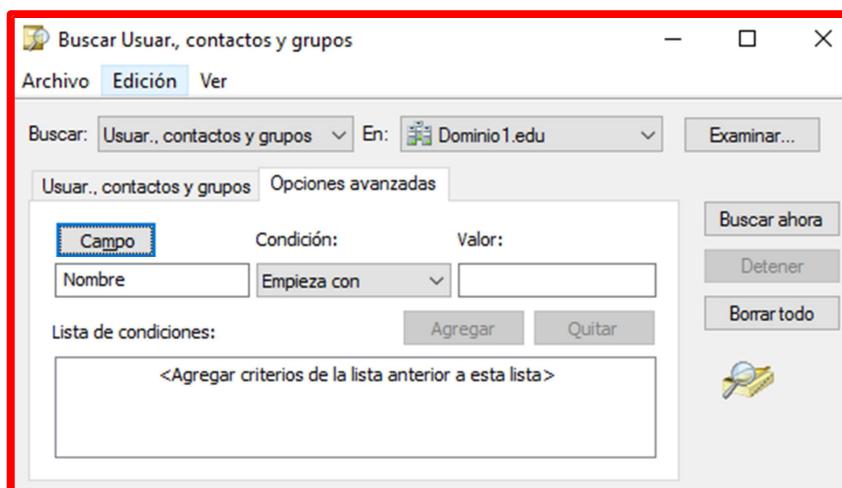


Si como ves en la pantalla te cambia el nombre de usuario por su nombre completo estará bien seleccionado, pulsamos entonces en "**Aceptar**":



Para terminar añadimos el otro usuario Mª José Fernández.

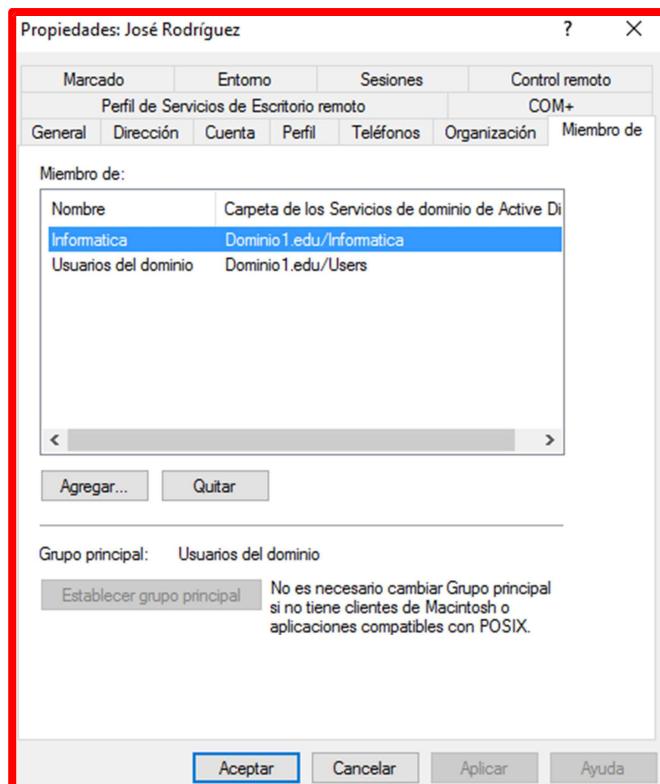
Solo un detalle si en la pantalla de búsqueda pulsamos en el botón de "**Avanzadas**" podemos realizar una búsqueda más completa:



Tenemos muchas más opciones para buscar ya que no siempre conoceremos los nombres de cuenta de los usuarios. En este caso buscaremos en la ubicación "**Dominio1.edu**", es decir, en nuestro dominio, los nombres que "**Empieza con**". Si no escribimos nada y pulsamos en "**Buscar ahora**" nos muestra todos los usuarios y grupos, algunos de ellos, deshabilitados. Como normalmente tendremos muchos usuarios, seguramente será mejor si ponemos las iniciales de su nombre para filtrar mejor la consulta.

Comprobación de los grupos

En la pestaña **Miembro** de en la cuenta de usuario teníamos:



Que es la lista de grupos de los que es miembro. Como ves, hay uno predeterminado que es "**Usuarios del dominio**" y otro "**Informatica**" que es en el que le acabamos de añadir.

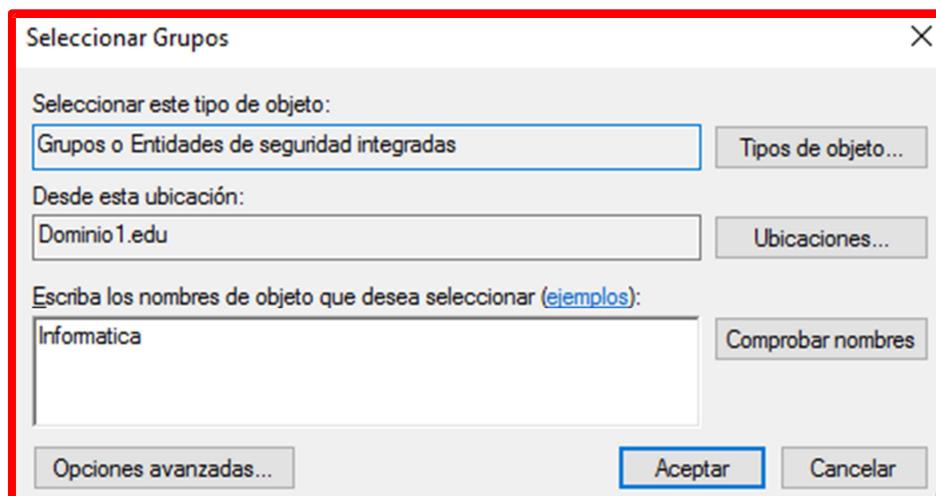
Método rápido

El sistema más rápido para introducir usuarios al dominio es marcando todos los que queremos insertar:

The screenshot shows the 'Usuarios y equipos de Active Directory' (Active Directory Users and Computers) snap-in. The left pane shows the navigation tree with 'Dominio1.edu' expanded, showing 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Users', and 'Informatica'. The right pane displays a list of users with their names and types. The user 'José Rodríguez' is selected. The list includes:

Nombre	Tipo
AULAC9-PROF	Equipo
Informatica	Grupo de seguridad - Global
José Rodríguez	Usuario
Mº José Fernández	Usuario
usu2	Usuario

Y pulsando con el botón derecho tendremos la opción de "**Agregar a un grupo**" que mostrará esta pantalla:



que es la típica de consulta, pero personalizada ya para buscar grupos, como ves en los “*tipos de objetos*” que va a buscar en la primera casilla. Escribimos el nombre del grupo y listo. Como ves es mucho más rápido que el sistema manual y es la mejor forma de hacer los grupos inicialmente. Luego cuando ya existen será desde la ficha del usuario donde le incorporaremos a los grupos.