

Administración del Directorio Activo.

Objetos del directorio.
Usuarios.

Administración del Directorio Activo: Objetos.

- ▶ Usuarios.
 - Definición:
- ▶ Trabajando desde el entorno gráfico.
- ▶ Trabajando desde el Core (Powershell)

Usuarios.

► Los Usuarios:

- Son objetos dentro de un dominio que representan entidades físicas (personas).
- También pueden ser cuentas de servicios.

► Se denominan Entidades de seguridad y al crearlas se les asigna un identificador único de seguridad (SID).

Usuarios.

- ▶ Las cuentas de usuario permiten:
 - **Comprobar la identidad de un usuario para entrar al sistema:**

Permite al usuario iniciar sesión en equipos y dominios con una identidad que el dominio pueda autenticar. Un usuario que inicia sesión en la red debe tener una cuenta de usuario y una contraseña propias y únicas.

- **Autoriza o denegar el acceso a los recursos del dominio.**

Después de que un usuario se autentica, se le concede o se le deniega el acceso a los recursos del dominio en función de los permisos explícitos que se le hayan asignado en el recurso. Recuerda: Permisos de compartición y NFTS.

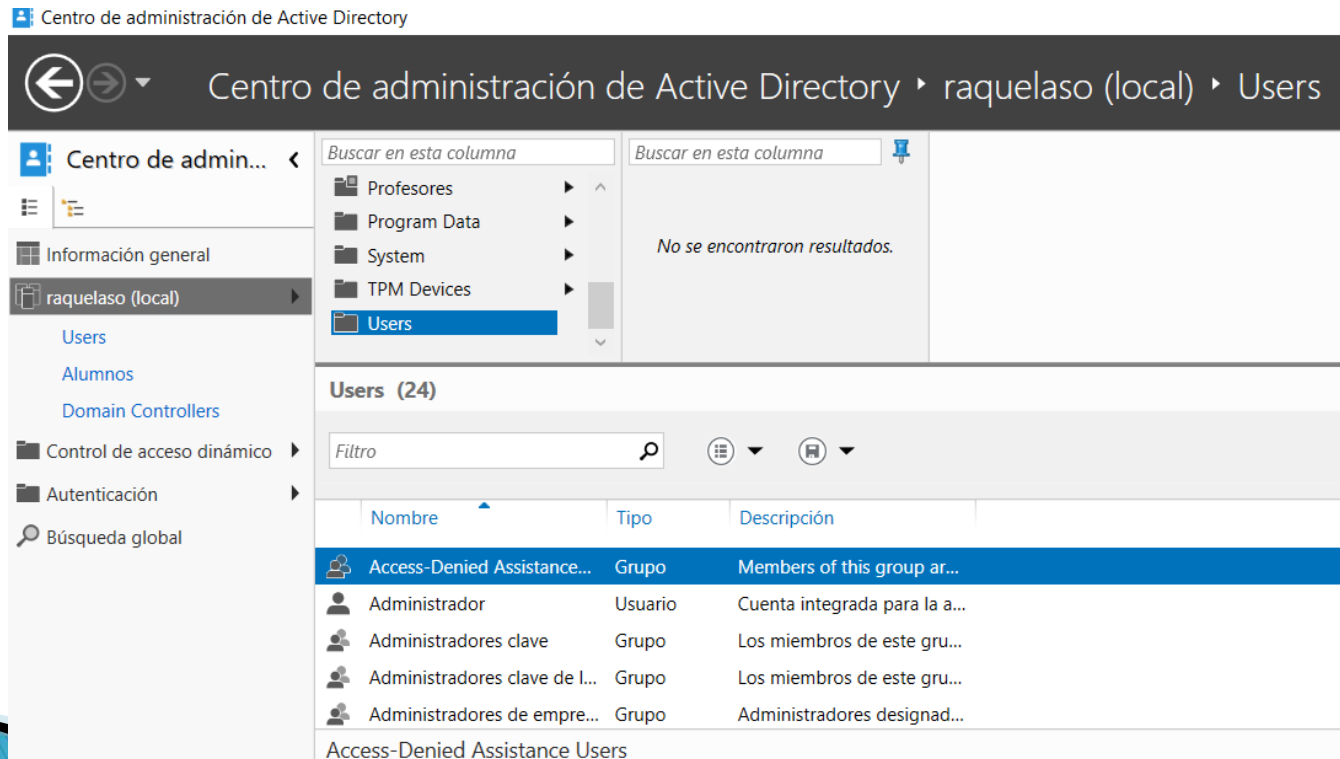
Usuarios.

Tipos de usuarios:

- **Los usuarios locales**: Son cuentas se almacenan en el local Administrador de cuentas de seguridad (SAM) Base de datos en el equipo donde residen. Sólo tienen acceso a recursos locales.
- Recuerda que puedes iniciar sesión con ellos utilizando:
Nombreequipo\usuario o .\usuario
- **Usuarios del dominio**: Puede acceder a estas cuentas de AD DS o recursos basados en red, como impresoras y carpetas compartidas.
 - La información de cuenta para estos usuarios se almacena en la base de datos de AD DS y se replican a todos los controladores de dominio dentro del mismo dominio.
 - **Dominio\usuario**

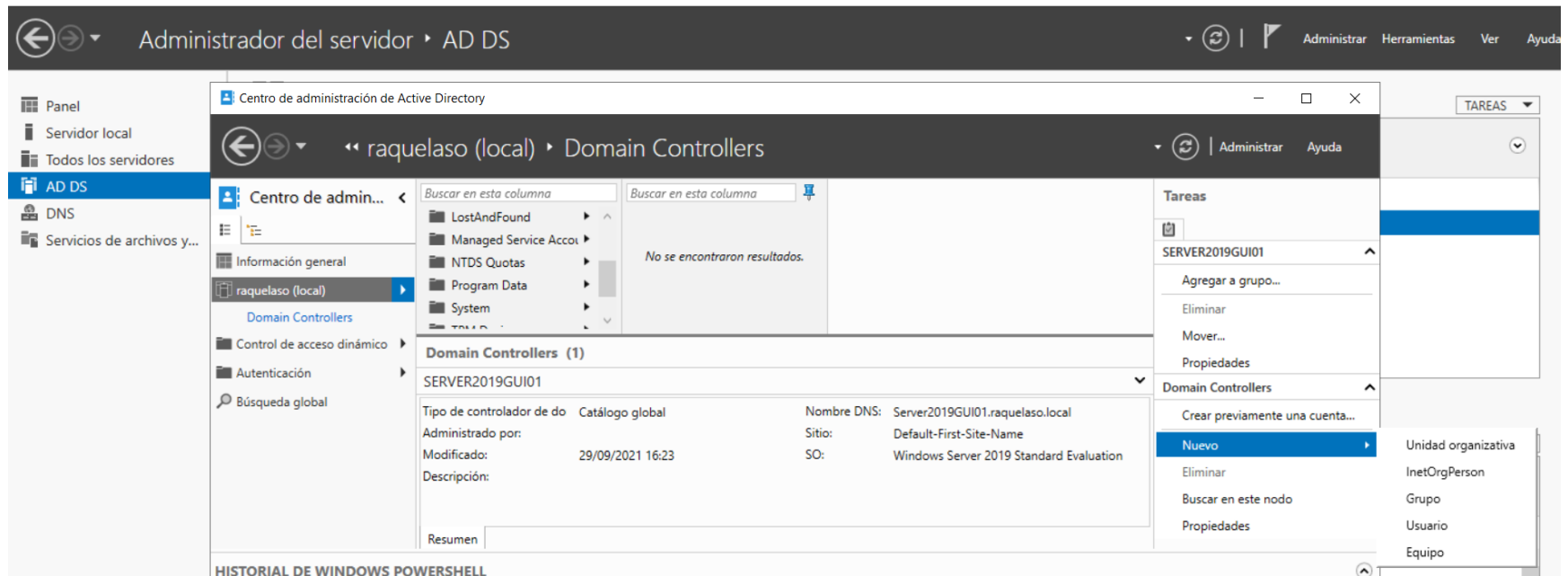
Usuarios.

- Podemos ver que al crear el directorio activo se crea un contenedor Users para almacenar los usuarios y grupos de dominio por defecto:



Usuarios.

Desde el centro de administración del DA:



Usuarios.

- Rellenaremos los campos y en especial los marcados como obligatorios:

Crear Usuario:

TAREAS SECCIONES

* Cuenta

Organización

Miembro de

Configuración de contraseña

Perfil

Directiva

Silo

Cuenta

Nombre:

Iniciales del segundo nom...

Apellidos:

Nombre compl. *

Inicio de sesión UPN de us...

Inicio de sesión SamAccou... raquelaso *

Contraseña:

Confirmar contraseña:

Crear en: OU=Alumnos,DC=raquelaso,DC=local Cambiar...

☐ Proteger contra eliminación accidental

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

La cuenta expira:

☒ Nunca

☐ Fin de

Opciones de contraseña:

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ Otras opciones de contraseña

☐ Microsoft Passport o la tarjeta inteligente son necesarios para realizar u...

☐ La contraseña nunca expira

☐ El usuario no puede cambiar la contraseña

Opciones de cifrado:

Otras opciones:

Organización

Nb para mostrar:

Oficina:

Correo electr.:

Página web:

Puesto:

Departamento:

Compañía:

Administrador:

Supervisa a:

Editar... Borrar

Otras páginas web...

Más información

Resultados de BPA

Resultados de BPA

Resultados de BPA

Resultados de BPA

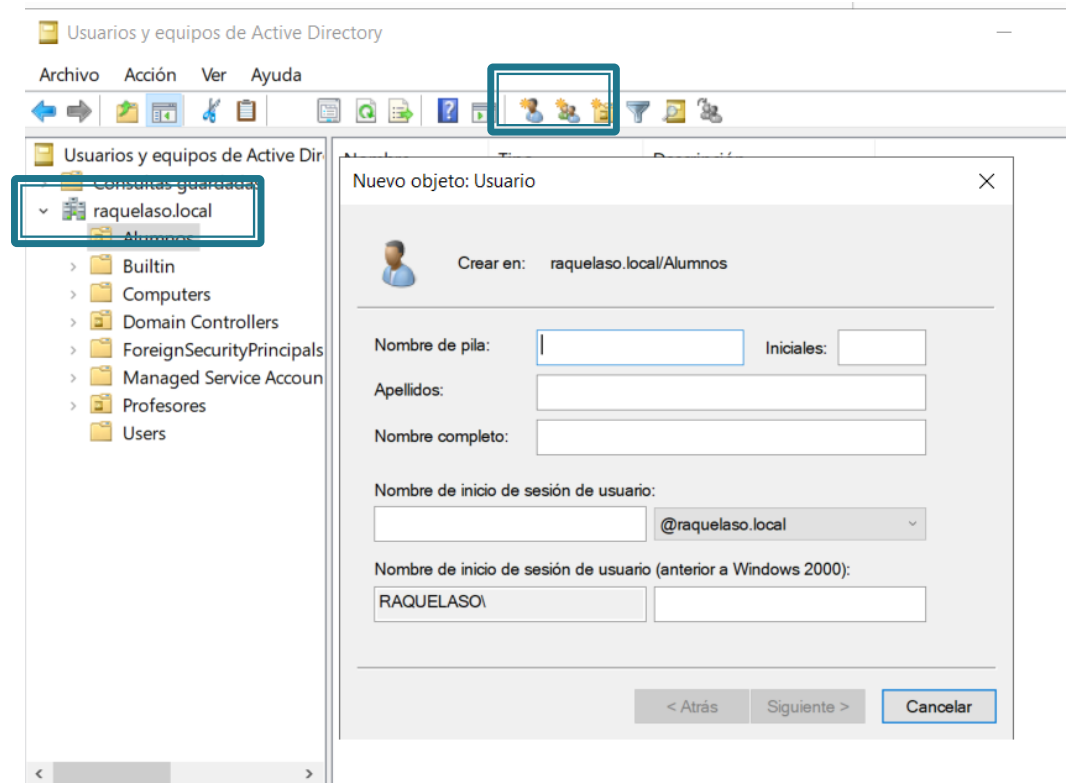
Aceptar Cancelar

Usuarios.

- ▶ Entre los datos obligatorios están:

Usuarios.

- También podemos trabajar con Usuarios y Equipos de AD:



Usuarios.

- Una vez creados podemos volver a modificar sus propiedades:

The image displays two screenshots of Windows user management interfaces. The left screenshot shows the 'Alumno1' user properties in the Windows Control Panel, with tabs for Cuenta, Organización, and Extensión. The right screenshot shows the 'Propiedades: Alumno1' dialog box, with tabs for General, Dirección, Cuenta, Perfil, Teléfonos, Organización, and Miembro de.

Left Screenshot: Windows Control Panel - Alumno1

- Cuenta**
 - Nombre: Alumno1
 - Apellidos: [Empty]
 - Nombre compl.: * Alumno1
 - Inicio de sesión UPN de us...: alumno1 @ raquelaso.local
 - Inicio de sesión SamAccou...: raquelaso * alumno1
 - ☐ Proteger contra eliminación accidental
- Organización**
 - Nb para mostrar: Alumno1
 - Oficina: [Empty]
 - Correo electr.: [Empty]
 - Página web: [Empty]
 - Números de teléfono: [Empty]

Right Screenshot: Propiedades: Alumno1

- General**
 - Nombre de pila: Alumno1
 - Apellidos: [Empty]
 - Nombre para: Alumno1
 - Descripción: [Empty]
 - Oficina: [Empty]
 - Número de teléfono: [Empty]
 - Correo electrónico: [Empty]
 - Página web: [Empty]

Usuarios

Server Core.

Usuarios.

- ▶ Veamos los comandos para trabajar con Usuarios:

```
PS C:\Users\Administrador> Get-Command -Module ActiveDirectory -name *ADUser*
```

CommandType	Name	Version	Source
Cmdlet	Get-ADUser	1.0.1.0	ActiveDirectory
Cmdlet	Get-ADUserResultantPasswordPolicy	1.0.1.0	ActiveDirectory
Cmdlet	New-ADUser	1.0.1.0	ActiveDirectory
Cmdlet	Remove-ADUser	1.0.1.0	ActiveDirectory
Cmdlet	Set-ADUser	1.0.1.0	ActiveDirectory

- Con Get-ADUserResultantPasswordPolicy podemos ver las políticas que se aplican a un usuario en concreto. La sintaxis es:

```
PS C:\Users\Administrador> Get-ADUserResultantPasswordPolicy -Identity Administrator
```

Usuarios.

- ▶ Para **crear** Usuarios desde Powershell ejecutamos el comando:
 - **New-ADUser**

```
New-ADUser -Name raquel -Path "OU=UOCore,dc=sub,dc=raquelaso,dc=local"
```

- ▶ Comprobamos que se creó:

```
PS C:\Users\Administrador> Get-ADUser -filter 'name -like "r*"'  
  
-----  
DistinguishedName : CN=raquel,OU=UOCore,DC=sub,DC=raquelaso,DC=local  
Enabled           : False  
GivenName         :  
Name              : raquel  
ObjectClass       : user  
ObjectGUID        : 7e252f45-a94f-462c-b519-ef9dcc507509  
SamAccountName     : raquel  
SID               : S-1-5-21-3131810216-48221901-3194634025-1104  
Surname           :  
UserPrincipalName :
```

Usuarios.

- ▶ Sin embargo, si lo creamos así, se creará sin los valores suficientes para poder usarla.
- ▶ Si miramos las opciones a utilizar son muchas:



```
Administrator: Windows PowerShell

NAME
New-ADUser

SYNTAX
New-ADUser [-Name] <string> [-WhatIf] [-Confirm] [-AccountExpirationDate <datetime>] [-AccountNotDelegated <bool>]
[-AccountPassword <securestring>] [-AllowReversiblePasswordEncryption <bool>] [-AuthType <ADAuthType> {Negotiate |
Basic}] [-CannotChangePassword <bool>] [-Certificates <X509Certificate[]>] [-ChangePasswordAtLogon <bool>] [-City
<string>] [-Company <string>] [-CompoundIdentitySupported <bool>] [-Country <string>] [-Credential <pscredential>]
[-Department <string>] [-Description <string>] [-DisplayName <string>] [-Division <string>] [-EmailAddress
<string>] [-EmployeeID <string>] [-EmployeeNumber <string>] [-Enabled <bool>] [-Fax <string>] [-GivenName
<string>] [-HomeDirectory <string>] [-HomeDrive <string>] [-HomePage <string>] [-HomePhone <string>] [-Initials
<string>] [-Instance <ADUser>] [-KerberosEncryptionType <ADKerberosEncryptionType> {None | DES | RC4 | AES128 |
AES256}] [-LogonWorkstations <string>] [-Manager <ADUser>] [-MobilePhone <string>] [-Office <string>]
[-OfficePhone <string>] [-Organization <string>] [-OtherAttributes <hashtable>] [-OtherName <string>] [-PassThru]
[-PasswordNeverExpires <bool>] [-PasswordNotRequired <bool>] [-Path <string>] [-POBox <string>] [-PostalCode
<string>] [-PrincipalsAllowedToDelegateToAccount <ADPrincipal[]>] [-ProfilePath <string>] [-SamAccountName
<string>] [-ScriptPath <string>] [-Server <string>] [-ServicePrincipalNames <string[]>] [-SmartcardLogonRequired
<bool>] [-State <string>] [-StreetAddress <string>] [-Surname <string>] [-Title <string>] [-TrustedForDelegation
<bool>] [-Type <string>] [-UserPrincipalName <string>] [<CommonParameters>]
```

<https://docs.microsoft.com/en-us/powershell/module/activedirectory/new-aduser?view=windowsserver2019-ps>

Usuarios.

- ▶ Veamos las opciones que rellenamos en el entorno gráfico:

The screenshot shows the Windows 7 User Account Control window for the user 'raquele'. The window is divided into two main sections: 'Cuenta' (Account) and 'Organización' (Organization). The 'Cuenta' section contains fields for Name (Prosor), Initials (Rojo), Surname (Raquela), Username (raquela), and Password (Raquela). It also includes options for account expiration (Nunca or Fin de) and password options (El usuario debe cambiar la contraseña en el si... or Otras opciones de contraseña). The 'Organización' section contains fields for Nb para mostrar, Oficina, Correo electr., Página web, Puesto, Departamento, Compañía, Administrador, and Supervisa a. The window has a sidebar on the left with links to Cuentas, Organización, Miembro de, Configuración de contraseña, Perfil, Directiva, Silo, and Extensiones. The bottom of the window has buttons for 'Aceptar' and 'Cancelar'.

raquele

TAREAS ▼ SECCIONES ▼

Cuenta

Nombre: Prosor

Iniciales del segu... Rojo

Apellidos: Raquela

Nombre compl.* raquela

Inicio de sesión U... raquela @ raquelaso.l

Inicio de sesión S... raquelaso * Raquela

☐ Proteger contra eliminación accidental

La cuenta expira: ☒ Nunca ☐ Fin de

Opciones de contraseña:

☐ El usuario debe cambiar la contraseña en el si...

☐ Otras opciones de contraseña

☐ Microsoft Passport o la tarjeta inteligente...

☐ La contraseña nunca expira

☐ El usuario no puede cambiar la contras...

Opciones de cifrado:

Otras opciones:

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

Organización

Nb para mostrar:

Oficina:

Correo electr.:

Página web:

Puesto:

Departamento:

Compañía:

Administrador: Editar... Borrar

Otras páginas web...

Números de telef...

Supervisa a: Agregar...

Más información

Aceptar Cancelar

Usuarios.

- ▶ En el comando **New-ADUser** serían:
 - Name, surname, GivenName.
 - Path o ruta de creación, indicando unidades organizativas y dominio (OU y DC).
 - "Ou= ,dc= , dc="
 - UserPrincipalName: nombreInicio@dominio.local
 - AccountPassword: leyendo del teclado:
 - Habilitar la cuenta.

```
Escriba Contraseña: *****> New-ADUser -name "raquele" -Surname "Rojo" -givenname "Prosor" -Path "ou=profesores,dc=raquelaso,dc=local"
-Enabled $true -SamAccountName "Raquele" -AccountPassword (Read-Host -AsSecureString "Escriba Contraseña") -UserPrincipalName "raque
le@raquelaso.local"
Escriba Contraseña: *****
```

Usuarios.

- ▶ Para poder modificar los usuarios que hemos creados disponemos del comando:
 - **Set-ADUser**
- ▶ Tenemos que indicar el usuario al que queremos modificar y la propiedad.
- ▶ Por ejemplo:

```
PS C:\Users\Administrador> Set-ADUser invitado -Enabled $true
PS C:\Users\Administrador> Get-ADUser -Identity invitado

DistinguishedName : CN=Invitado,CN=Users,DC=dominio1raquel,DC=local
Enabled           : True
GivenName        :
Name             : Invitado
ObjectClass      : user
ObjectGUID       : 18072e18-c17e-4417-a6f1-b515ea4e3f46
SamAccountName    : Invitado
SID              : S-1-5-21-970135835-9769154-2383746456-501
Surname          :
UserPrincipalName :
```

Usuarios.

- ▶ Para eliminar la Unidad organizativa utilizaremos el comando:

Remove-ADUser -Identity ...

```
PS C:\Users\Administrador> Remove-ADUser -Identity "raquale"

Confirmar
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "Remove" en el destino "CN=raquale,OU=Profesores,DC=raquelaso,DC=local".
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "S"): s
PS C:\Users\Administrador>
```

Usuarios.

- Para ver los usuarios del sistema:

```
PS C:\Users\Administrador> Get-ADUser

cmdlet Get-ADUser en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
(Escriba !? para obtener Ayuda).
Filter: *

DistinguishedName : CN=Administrador,CN=Users,DC=raquelaso,DC=local
Enabled           : True
GivenName        :
Name             : Administrador
ObjectClass       : user
ObjectGUID        : bbb691f7-ef34-4657-875b-8f610fb80a07
SamAccountName    : Administrador
SID              : S-1-5-21-2850116191-298867576-450433861-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=Invitado,CN=Users,DC=raquelaso,DC=local
Enabled           : False
GivenName        :
Name             : Invitado
ObjectClass       : user
ObjectGUID        : 2867ee28-feb7-45d7-ba3d-5a20334c59e3
SamAccountName    : Invitado
SID              : S-1-5-21-2850116191-298867576-450433861-501
Surname          :
UserPrincipalName :
```

Usuarios.

- ▶ Para ver los usuarios del sistema filtrados:
 - `-filter -searchBase`

```
PS C:\Users\Administrador> Get-ADUser -filter * -SearchBase "ou=profesores,dc=raquelaso,dc=local"
```

```
DistinguishedName : CN=raquel,OU=Profesores,DC=raquelaso,DC=local
Enabled           : True
GivenName        : raquel
Name             : raquel
ObjectClass      : user
ObjectGUID       : 443391c2-4309-42cc-9249-8fb35afae3bb
SamAccountName   : raquelprofe
SID              : S-1-5-21-2850116191-298867576-450433861-1109
Surname          :
UserPrincipalName : raquelprofe@raquelaso.local
```

```
PS C:\Users\Administrador> Get-ADUser -filter 'name -like "r*"' -SearchBase "ou=profesores,dc=raquelaso,dc=local"
```

```
DistinguishedName : CN=raquel,OU=Profesores,DC=raquelaso,DC=local
Enabled           : True
GivenName        : raquel
Name             : raquel
ObjectClass      : user
ObjectGUID       : 443391c2-4309-42cc-9249-8fb35afae3bb
SamAccountName   : raquelprofe
SID              : S-1-5-21-2850116191-298867576-450433861-1109
Surname          :
UserPrincipalName : raquelprofe@raquelaso.local
```

Prácticas.

- ▶ Crea dentro de las unidades organizativas los siguientes usuarios desde la herramienta gráfica:
 - UOGruposGUI:
 - UOG1
 - usu1
 - usu2
 - usu3
 - UOG2
 - Usu4
 - Usu5
 - usu6
 - UOG3
 - Usu7
 - Usu8
 - usu9

Prácticas

- ▶ Crea dentro de las unidades organizativas los siguientes usuarios desde Powershell:
 - UOGruposCore:
 - UOG1
 - usu1
 - usu2
 - usu3
 - UOG2
 - Usu4
 - Usu5
 - usu6
 - UOG3
 - Usu7
 - Usu8
 - usu9

Prácticas.

- ▶ Pruebas con los **usuarios** creados:
 - Intenta iniciar sesión con el usuario usu1. ¿Te deja? ¿Por qué?
 - Realiza las modificaciones necesarias para que pueda iniciar sesión en el controlador de dominio.
 - Deshabilita la cuenta de usu1 tanto en el GUI como en el Core.
 - Crea los usuarios ProfesorG, ProfesorG2 y ProfesorG3 en el dominio y después muévelos a cada uno de sus UO.

Practicar.

- ▶ Crea dos scripts para crear usuarios y para eliminarlos en la raíz del dominio, uno de tipo menú y otro con valores en la llamada.
- ▶ Añade a los scripts anteriores la opción de borrar usuarios.