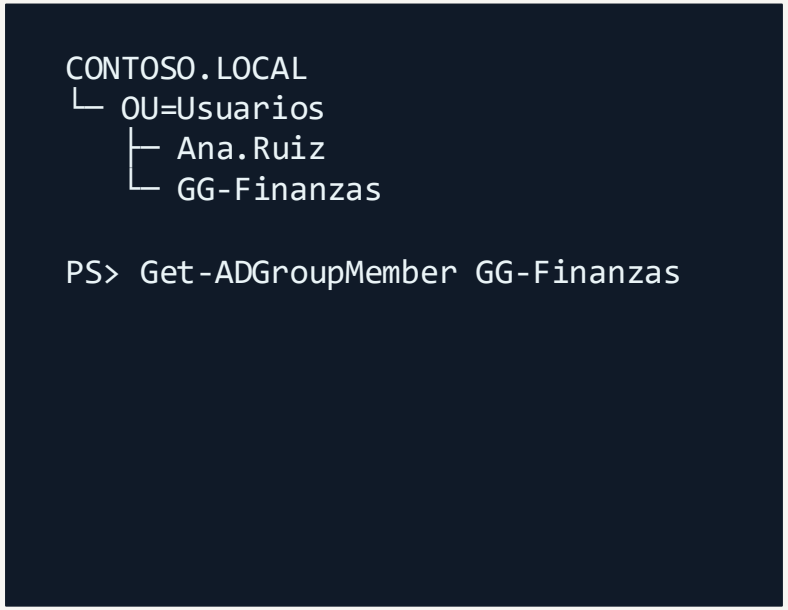
MANUAL PRÁCTICO

Administración de Usuarios y Grupos

Windows Server 2022 · local + Active Directory

20 diapositivas · 20 preguntas resueltas



La identidad correcta depende de dónde debe acceder

CUENTA LOCAL

`SERVIDOR\operador`

La autoridad es el propio equipo.
Permisos solo en ese servidor.
Se administra con lusrmgr.msc o PowerShell.

CUENTA DE DOMINIO

`CONTOSO\aruiz`

La autoridad es Active Directory.
Accede a recursos del dominio.
Se administra con ADUC o módulo AD.

Elige local para aislamiento; dominio para identidad centralizada.

Fuente: Microsoft Learn — Local accounts / AD user accounts

La cuenta local vive y se autoriza en un solo servidor

```
SAM local
C:\Windows\System32\config\SAM

Usuario: soporte_local
Grupo: Remote Desktop Users
SID: S-1-5-21-...
```

GUI

Computer Management → Local Users and Groups

01	CREAR	`New-LocalUser`
02	AGRUPAR	`Add-LocalGroupMember`
03	VERIFICAR	`Get-LocalUser`
04	PROBAR	`RunAs / RDP`
05	AUDITAR	`Event Viewer`

Fuente: Microsoft Learn — Local accounts

Crear, agrupar, probar y auditar evita accesos huérfanos

```
$pw = Read-Host -AsSecureString
New-LocalUser -Name 'soporte_local' `
  -Password $pw -FullName 'Soporte Local'
Add-LocalGroupMember `
  -Group 'Remote Desktop Users' `
  -Member 'soporte_local'
Get-LocalGroupMember 'Remote Desktop Users'
```

01 Nombre único y propósito

02 Contraseña inicial segura

03 Grupo mínimo necesario

04 Prueba de inicio de sesión

05 Registro de propietario y fecha

Evita añadir directamente al grupo Administrators salvo necesidad justificada.

Fuente: Microsoft Learn — Local accounts

El dominio centraliza; las OUs organizan y delegan

CONTOSO.LOCAL

OU=Usuarios

Cuentas de personas

Delegar alta/baja

OU=Equipos

Objetos de equipos

Aplicar GPO

OU=Servidores

Servidores miembro

Administración restringida

Diseña OUs para delegación y políticas; no para imitar el organigrama completo.

Fuente: Microsoft Learn — Creating an Organizational Unit Design

ADUC crea una identidad completa, no solo un nombre

NOMBRE	Ana Ruiz
INICIO DE SESIÓN	`aruiz`
UPN	`aruiz@contoso.local`
UBICACIÓN	`OU=Usuarios,DC=contoso,DC=local`
ESTADO	Habilitada tras asignar contraseña

ANTES DE FINALIZAR

- ✓ Nombre estándar
- ✓ OU correcta
- ✓ Contraseña temporal
- ✓ Cambio al iniciar
- ✓ Responsable registrado

No marques “Password never expires” sin una excepción documentada.

Fuente: Microsoft Learn — Manage user accounts in ADUC

PowerShell convierte el alta en una operación repetible

```
Import-Module ActiveDirectory
$pw = Read-Host -AsSecureString
New-ADUser -Name 'Ana Ruiz' `
 -GivenName 'Ana' -Surname 'Ruiz' `
 -SamAccountName 'aruiz' `
 -UserPrincipalName 'aruiz@contoso.local' `
 -Path 'OU=Usuarios,DC=contoso,DC=local' `
 -AccountPassword $pw `
 -Enabled $true -ChangePasswordAtLogon $true
```

CONSISTENCIA

Mismos campos y reglas

ESCALA

CSV + ForEach-Object

CONTROL

-WhatIf antes de ejecutar

EVIDENCIA

Transcript y registro de cambios

Fuente: Microsoft Learn — New-ADUser

Los grupos traducen funciones en permisos

A Cuentas ——— **G** Grupo global GG-Finanzas ——— **DL** Grupo local de dominio DL-Carpeta-Finanzas-RW

P Permiso sobre el recurso

```
New-ADGroup -Name 'GG-Finanzas' -GroupScope Global
Add-ADGroupMember -Identity 'GG-Finanzas' -Members 'aruiz'
Get-ADGroupMember 'GG-Finanzas'
```

Fuentes: Microsoft Learn — New-ADGroup / Add-ADGroupMember

La política debe corresponder al riesgo de la identidad

POLÍTICA DEL DOMINIO

Base común

Longitud mínima
Complejidad
Historial
Bloqueo

POLÍTICA GRANULAR (FGPP)

Mayor riesgo

Administradores
Cuentas de servicio especiales
Usuarios expuestos

VERIFICA

```
Get-
ADUserResultantPassword
Policy aruiz

Get-
ADDefaultDomainPassword
Policy
```

Las FGPP aplican a usuarios y grupos globales, no directamente a una OU.

Fuente: Microsoft Learn — Fine-grained password policies

El acceso termina antes de eliminar la cuenta

01	DESHABILITAR	`Disable-ADAccount`
02	CERRAR ACCESO	Revocar sesiones y VPN
03	TRANSFERIR	Correo, archivos y propiedad
04	RETIRAR GRUPOS	`Remove-ADGroupMember`
05	DOCUMENTAR	Motivo, fecha y aprobador
06	ELIMINAR	Tras retención definida

```
Get-ADUser aruiz -
Properties
Enabled,MemberOf,LastLogonD
ate
Get-WinEvent -
FilterHashtable
@{LogName='Security';
Id=4720,4722,4725,4726,4732
}
```

Audita altas, activaciones, bloqueos, eliminaciones y cambios de grupo.