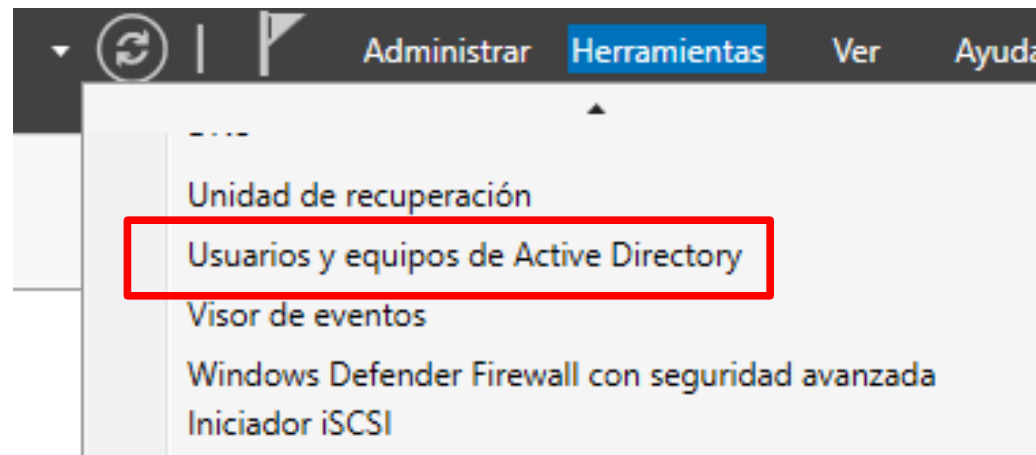


Usuarios, grupos y Unidades Organizativas en el Directorio Activo

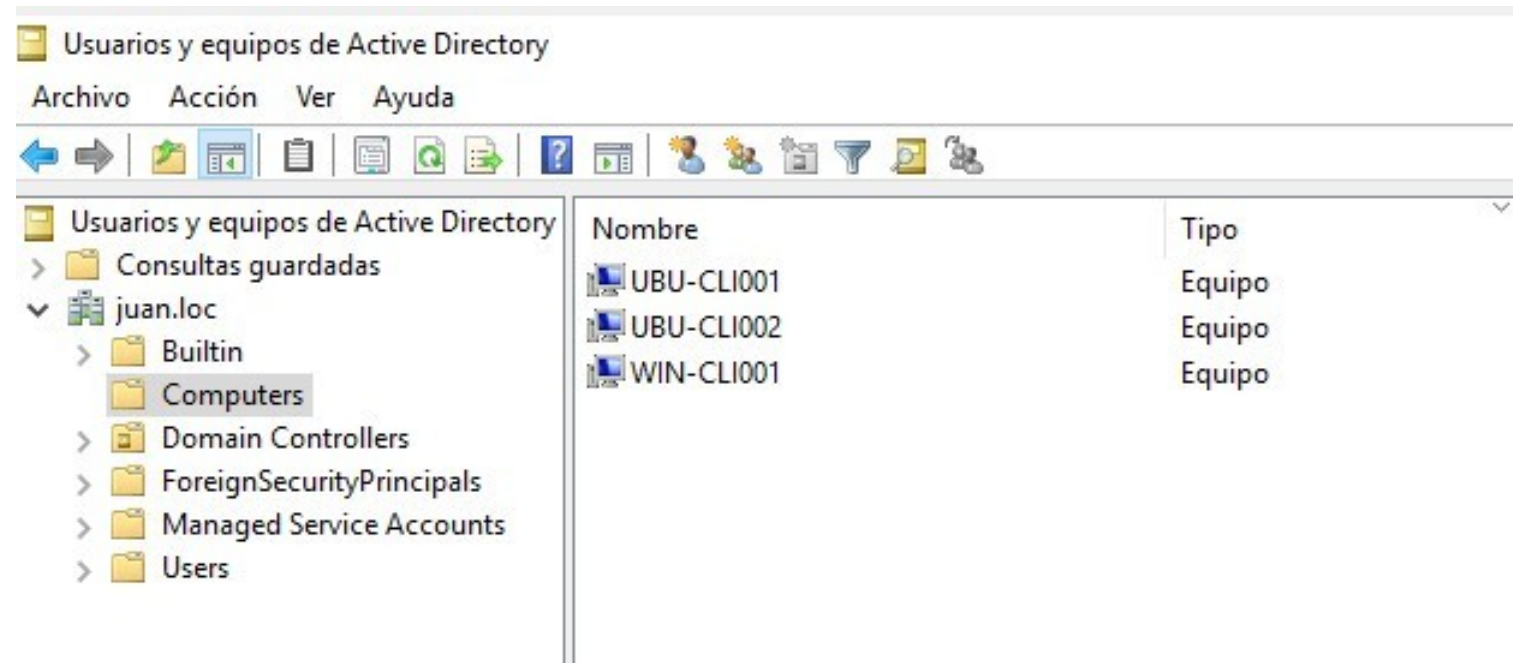
Usuarios y equipos de Active Directory

- La herramienta principal para gestionar usuarios, grupos y unidades organizativas es la consola de **Usuarios y equipos de Active Directory**.
- Se puede acceder a ella tanto desde el buscador como desde el Administrador.



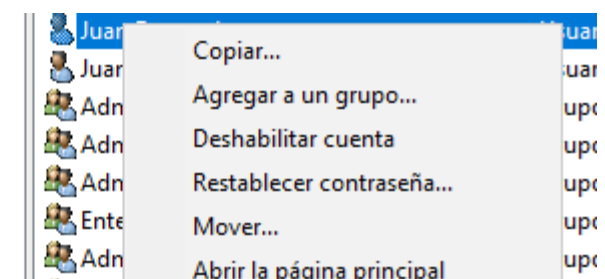
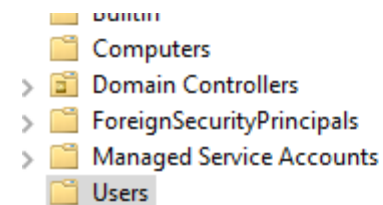
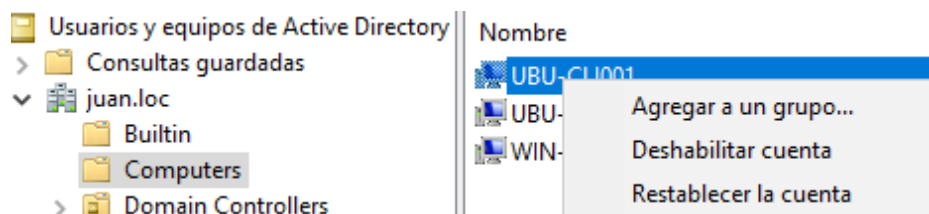
Usuarios y equipos de Active Directory (II)

- Por defecto, tras la instalación, existen un conjunto de contenedores y OUs creadas.
- A la izquierda vemos el árbol de navegación, y a la derecha los objetos dentro de cada elemento.



Usuarios y equipos de Active Directory (III)

- Se trata de la consola principal para la gestión de usuarios, grupos, equipos y unidades organizativas.
- Veremos cada elemento de forma detallada.
- Es posible realizar la administración de estos elementos mediante comandos del Símbolo de sistema o PowerShell.
- Cada tipo de objeto proporciona un menú contextual y unas propiedades diferentes.



Elementos por defecto del AD (I)

- En el árbol podemos distinguir:

→ **Contenedores** (símbolo de carpeta): almacenan objetos del sistema como grupos, equipos o usuarios y sirven de localización por defecto al crear grupos, usuarios o equipos.

Los objetos de un contenedor se pueden mover a una OU al implementar la estructura diseñada.

→ **Unidades Organizativas** (carpeta con icono en su interior): permiten distribuir los diferentes objetos del directorio de acuerdo a nuestro diseño.

Elementos por defecto del AD (II)

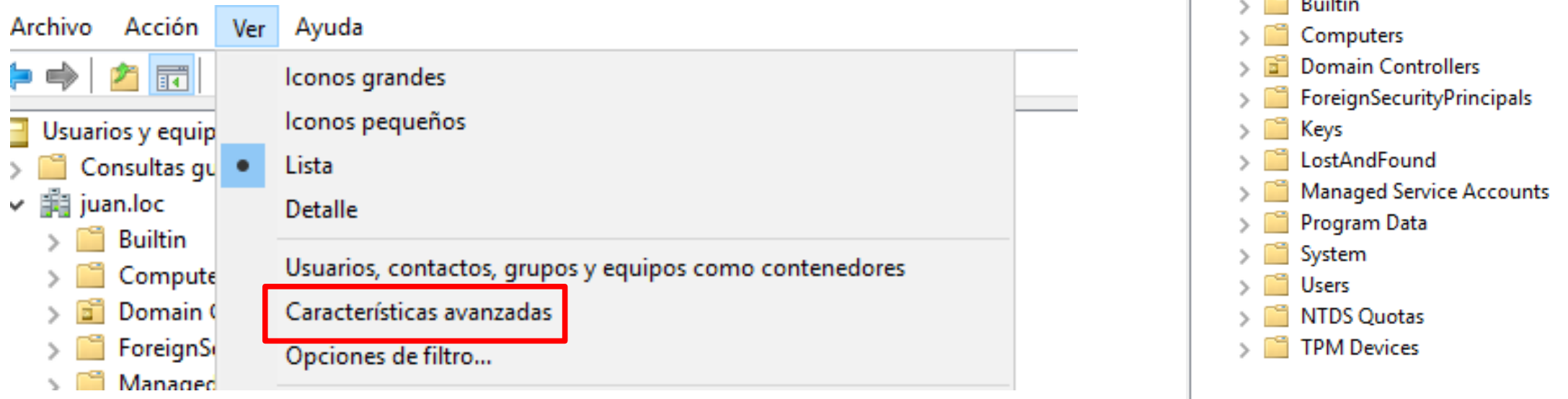
- Contenedor **Builtin**: Contiene grupos creados por defecto.
- Contenedor **Computers**: es la localización por defecto de nuevos equipos que incluyamos en el dominio si no los creamos antes.
- OU **Domain Controllers**: localización por defecto de las cuentas de los equipos DC. Es la única OU que se crea por defecto.

Elementos por defecto del AD (III)

- Contenedor **Foreign Security Principals**: localización por defecto de los objetos (SID) de otros bosques en los que se confía. Se crea, por ejemplo, cuando añadimos un objeto de otro bosque a un grupo de nuestro dominio.
Contiene también identidades especiales como el de los Usuarios Autenticados.
- Contenedor **Managed Service Accounts**: contiene cuentas que utilizan aplicaciones del dominio.
- Contenedor **Users**: localización por defecto de las cuentas de usuario y grupo.

Elementos por defecto del AD (IV)

- Existen un conjunto de contenedores y objetos que el sistema oculta por seguridad y por no ser habitual modificarlos.
- Para visualizarlos, se deben habilitar las Características avanzadas



Elementos por defecto del AD (V)

- **Keys:** empleado para el almacenamiento de claves en entornos distribuidos.
- **LostAndFound:** objetos recuperados “huérfanos”.
- **Program Data:** empleado por aplicaciones de Microsoft.
- **System:** configuraciones del sistema
- **NTDS Quotas:** datos del servicio de cuotas de AD.
- **TPM Devices:** desde W2012, información de recuperación de dispositivos TPM.

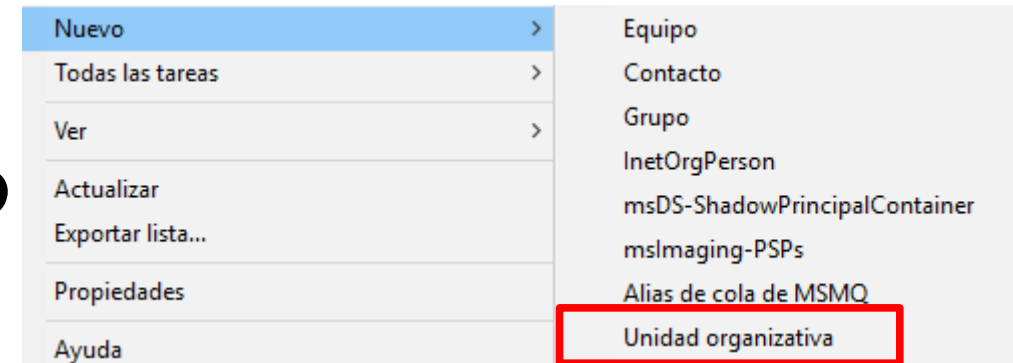
Las unidades organizativas

Unidades organizativas (I)

- Las unidades organizativas nos permiten organizar el directorio de forma que se cumplan las necesidades de cada organización.
- Sus funciones principales son dos:
 - 1) Permiten asociarles Directivas de Grupo diferentes (ya lo veremos). Esto implica que, dependiendo de la OU, los equipos y usuarios tendrán configuraciones diferentes.
 - 2) Permiten delegar la administración de los objetos de la OU en usuarios o grupos.

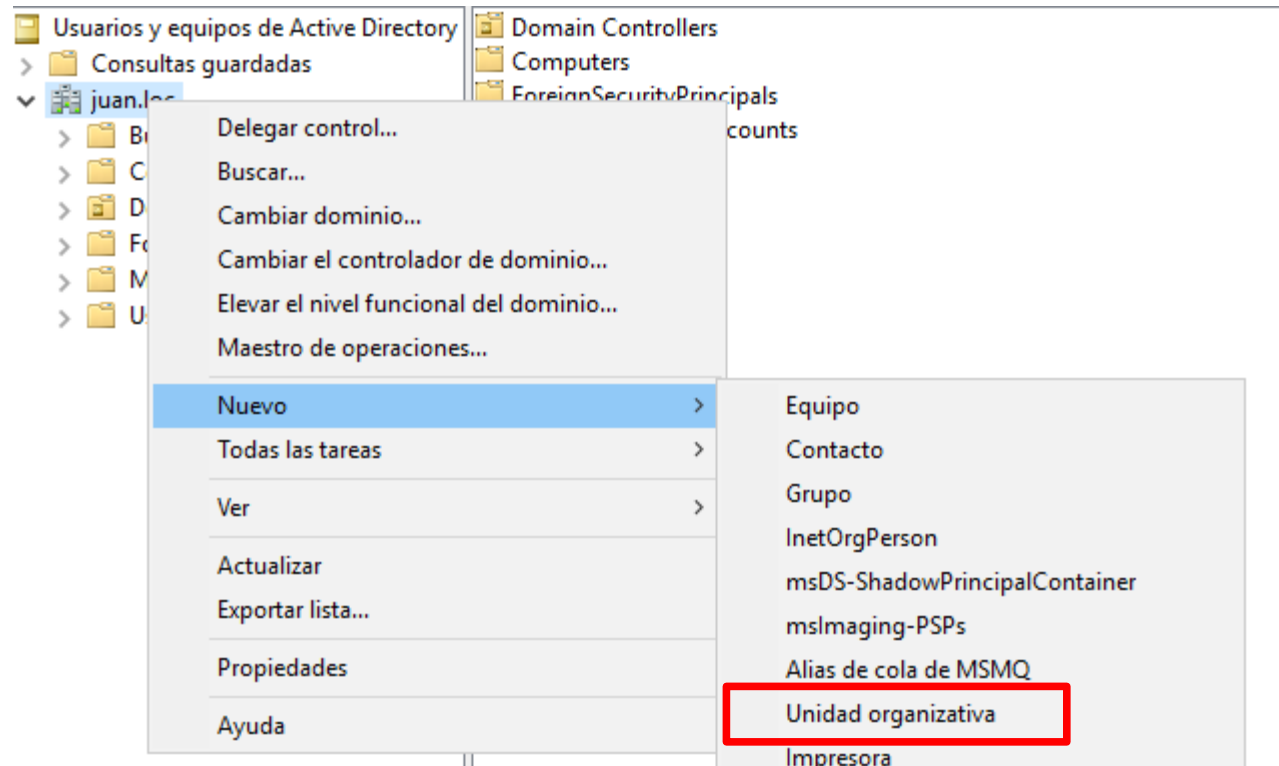
Unidades organizativas (II)

- Las OUs solo se pueden crear:
 - ✓ Directamente debajo del dominio
 - ✓ Dentro de otra OU
- No es posible crear una OU dentro de un Contendor.
- Si trabajamos con interfaz gráfica, los menús contextuales nos darán o no la opción de crear OU.
- Si trabajamos con comandos, nos darán error si intentamos una creación no permitida.



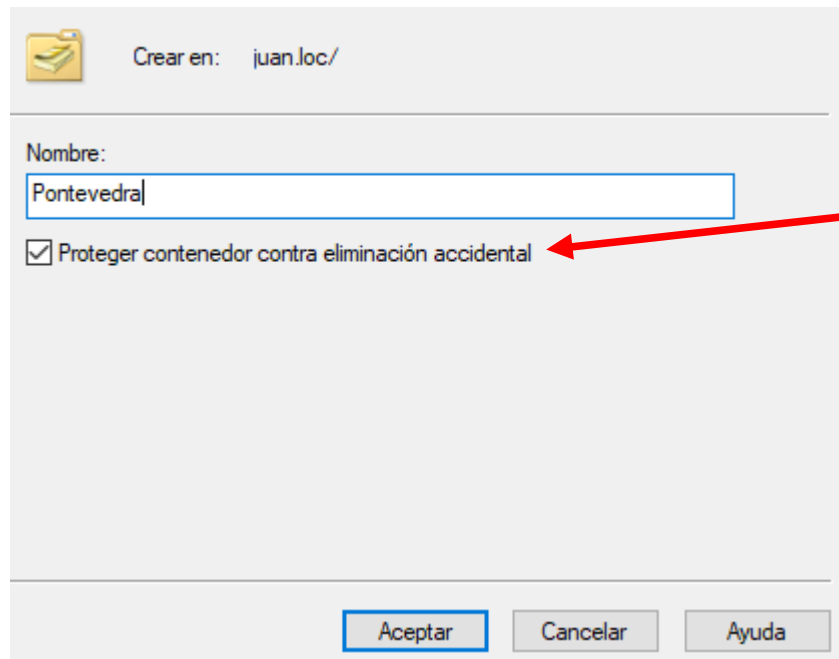
Unidades organizativas - Creación (I)

- Hacemos click con botón derecho del ratón en el elemento del directorio bajo el que queremos crear la OU



Unidades organizativas - Creación (II)

- Nos solicitará el nombre de la unidad.



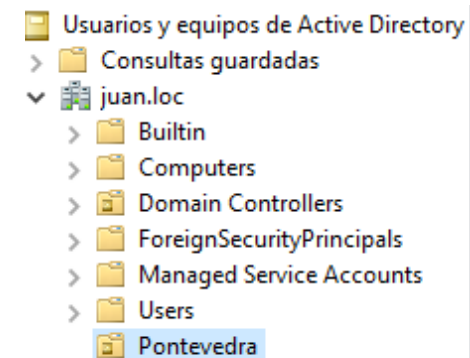
Crear en: juan.loc/

Nombre:
Pontevedra

☒ Proteger contenedor contra eliminación accidental

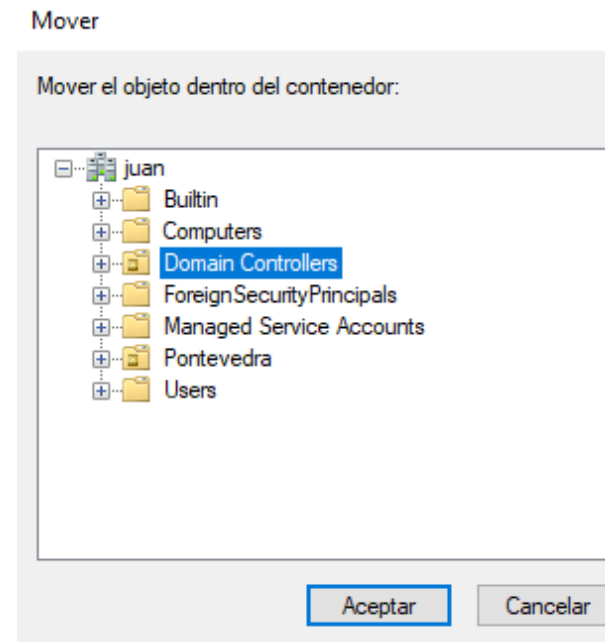
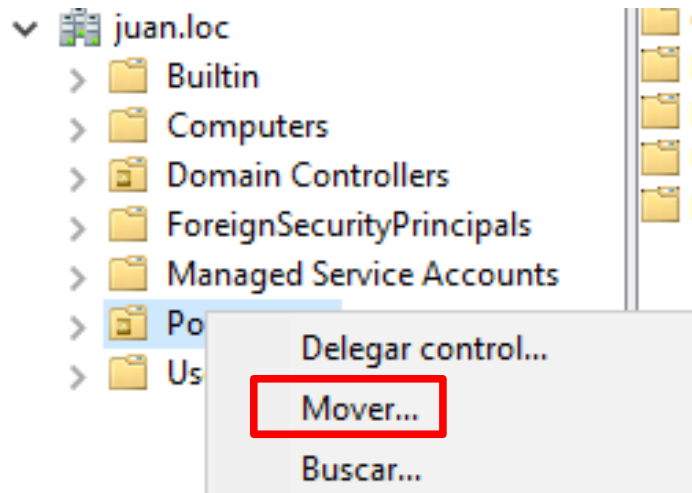
Aceptar Cancelar Ayuda

Por defecto está marcada estacasilla, que impide el borrado de



Unidades organizativas - Movimiento

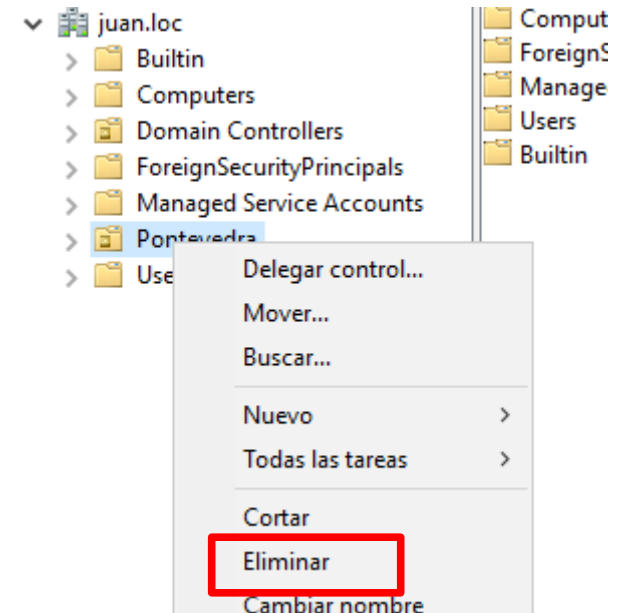
- Una OU se puede mover de un elemento a otro mediante el menú contextual que aparece si hacemos click con el botón derecho del ratón encima de ella.



Unidades organizativas - Borrado (I)

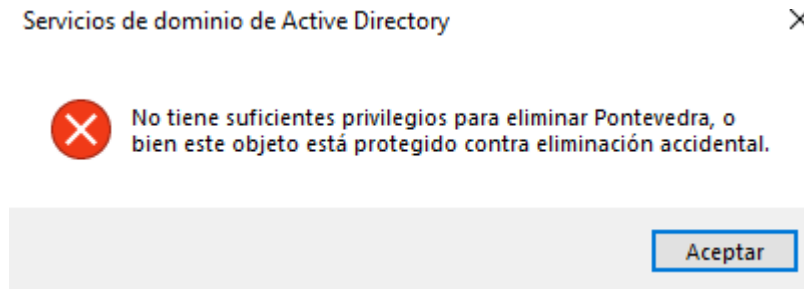
- Hacemos click con botón derecho del ratón en la OU a borrar (puede ser una estructura de Ous).
- Seleccionamos eliminar.

PRUEBA: EliminalaOUquehas creado previamente



Unidades organizativas - Borrado (II)

- Salvo que al crear la OU hayas indicado expresamente que no quieras que esté protegido contra borrado accidental, recibirás un error.



- Es necesario desmarcar la protección.
- Para ello, debes activar las **Características avanzadas**.

Unidades organizativas - Borrado (III)

- Una vez visibles las características avanzadas, selecciona las propiedades de la OU y navega a la pestaña **Objeto**

Propiedades: Pontevedra ? >

General Administrado por Objeto Seguridad COM+ Editor de atributos

Nombre canónico del objeto:

Clase de objeto: Unidad organizativa

Creado: 06/12/2021 11:34:37

Modificado: 06/12/2021 11:41:41

Números de secuencias actualizadas (USN):

Actual: 65653

Original: 65650

☒ Proteger objeto contra eliminación accidental

- Una vez desmarcado, ya te dejará eliminar el objeto.

Unidades organizativas- Estrategias de diseño (I)

- Antes de crear objetos en el AD debemos diseñar nuestra estructura.
- La estructura debe combinar:
 - **Simplicidad:** no introducir complejidad innecesaria. Si en nuestra organización solo hay un administrador y no distinguiremos distintas configuraciones, lo más recomendable es un diseño plano.
 - **Flexibilidad:** crear OUs en función de las necesidades de la organización (delegación de administración y directivas de grupo).


















Unidades organizativas- Estrategias de diseño (II)

- Existen multiples criterios. Entre los más habituales:
 - Por localización geográfica: empresas con oficinas en diferentes zonas.
 - Según la organización departamental.
 - Por el tipo de recurso que albergarán: equipos cliente, equipos servidor, usuarios, etc.
- Podemos usar uno de ellos o varios combinados.

Unidades organizativas - Crea tus Ous (I)

- Vamos a suponer que queremos organizar un centro de estudios que tiene 3 centros.
- Como cada centro será administrado por una persona diferente, crearemos 3 OUs bajo el dominio, una por centro.
- Dentro de cada OU definiremos dos OUs, una de equipos y otra de Usuarios.
- A su vez, para poder realizar una configuración distinta para usuarios Docentes y Alumnado, dentro de Usuarios crearemos dos OUs: Alumnado y Docentes.

Unidades organizativas - Crea tus Ous (II)

- ▼  **juan.loc**
 - >  Bultin
 - ▼  Centro A Coruña
 -  Equipos
 - ▼  Usuarios
 - >  Alumnado
 - >  Docentes
 - ▼  Centro Lugo
 -  Equipos
 - ▼  Usuarios
 - >  Alumnado
 - >  Docentes
 - ▼  Centro Vigo
 - >  Equipos
 - ▼  Usuarios
 - >  Alumnado
 - >  Docentes

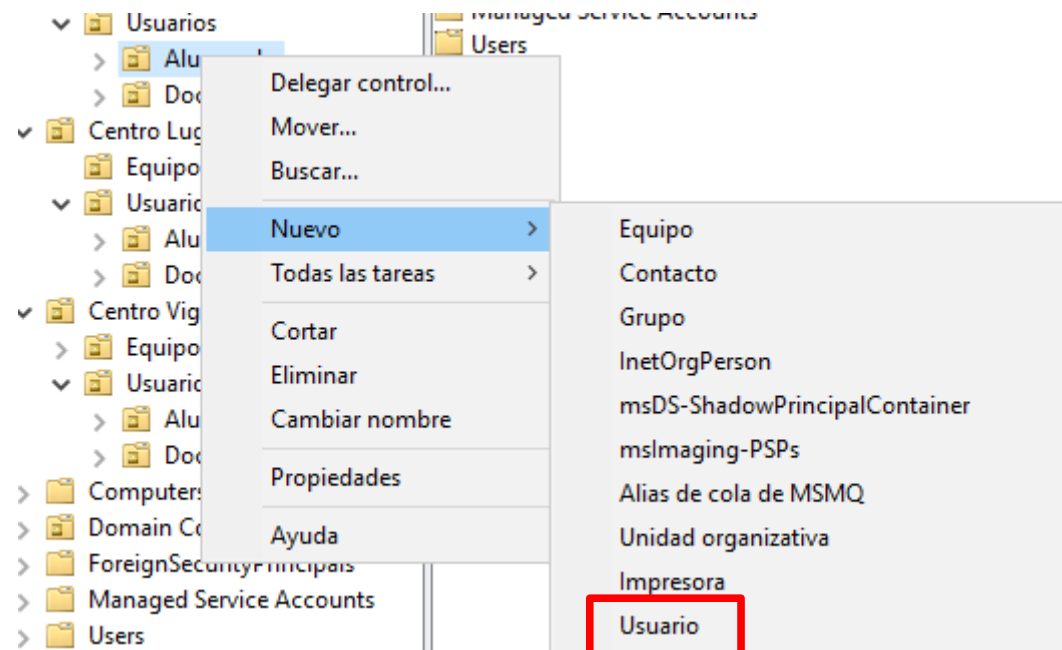
Usuarios

Usuarios

- Una cuenta de usuario en el dominio es global.
- No pueden existir dos cuentas con el mismo nombre.
- Se permiten nombre de cuenta de hasta 20 caracteres, en mayúsculas, minúsculas, números y caracteres especiales. Excepción:
/ | : ; = < > y *
- En el dominio están activas directivas de seguridad de cuenta, aunque se pueden modificar.
- Cada cuenta tiene asociado un SID (identificador de seguridad), único en la red.

Usuarios - Creación (I)


- Para crear usuarios, se selecciona la entidad de nivel superior (Contenedor u OU) y se hace click con el botón derecho



Usuarios - Creación (II)

- Comenzará el asistente de creación de usuarios

Nuevo objeto: Usuario


 Crear en: juan.loc/Centro A Coruña/Usuarios/Alumnado

Nombre de pila: Iniciales:

Apellidos:


Nombre completo:

Nombre de inicio de sesión de usuario:

@juan.loc 

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

Nuevo objeto: Usuario

 Crear en: juan.loc/Centro A Coruña/Usuarios/Alumnado

Contraseña:

Confirmar contraseña:

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

☐ El usuario no puede cambiar la contraseña

☐ La contraseña nunca expira

☐ La cuenta está deshabilitada

Usuarios - Creación (II)

En primer lugar, se proporciona el login y nombre

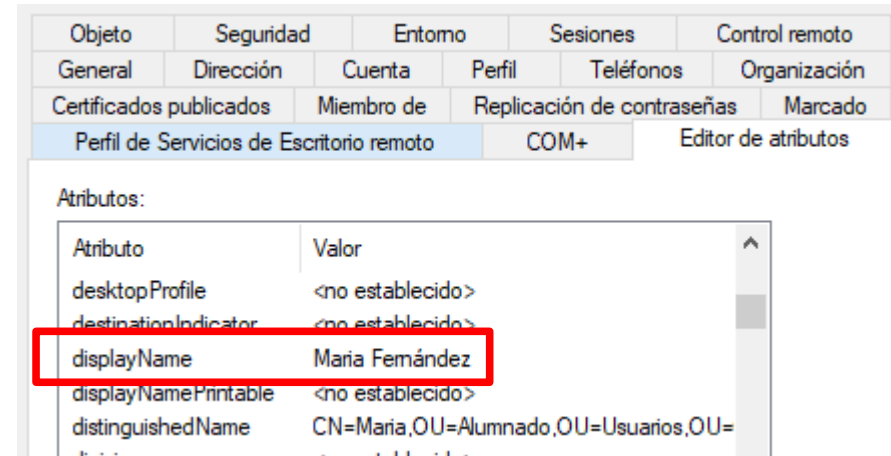
A continuación contraseña, con sus propiedades

Revisamos el resumen y finalizamos

The screenshot shows the 'Nuevo usuario' (New User) dialog box with the 'General' tab selected. The user's name is 'Maria'. The 'Nombre de pila' (First Name) field contains 'Maria' and 'Iniciales' (Initials) is empty. The 'Nombre para mostrar' (Display Name) field contains 'Maria Fernández'. The 'Apellido' (Surname) field is empty. The 'Descripción' (Description) and 'Oficina' (Office) fields are empty. The 'Número de teléfono' (Phone Number) field is empty, with an 'Otros...' (Other...) button next to it. The 'Correo electrónico' (Email) field is empty. The 'Página web' (Website) field is empty, with an 'Otros...' (Other...) button next to it. A red line is drawn under the 'Nombre de pila' field. The 'Cancelar' (Cancel) button is at the bottom right.

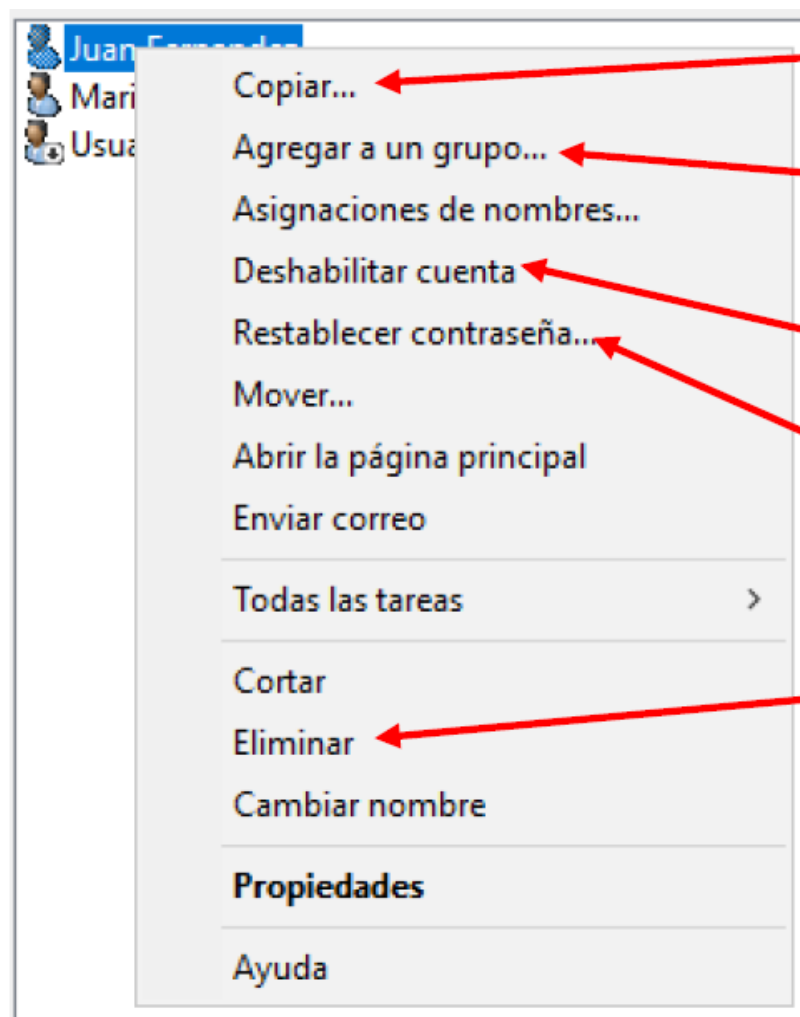
Usuarios - Creación (III)

- Una vez creado, si accedemos a las propiedades del usuario veremos atributos adicionales



Si activamos las características avanzadas, tendremos acceso al editor de atributos directamente. Algunos son los ya existentes en el resto de pestañas, otros solo se pueden modificar aquí

Usuarios - Operaciones frecuentes



Permite crear un usuario a partir de otro

Asignar un usuario a un grupo

El usuario no podrá acceder

Cambio de contraseña

Borrado de cuenta

Usuarios - Operaciones frecuentes

Usuarios - Creación (IV)

- Como has visto, un usuario puede tener multitud de atributos.
- Al crear nuevos usuarios es habitual emplear dos técnicas:
 - En entorno gráfico, definir un usuario “plantilla”
 - Crear un script en PowerShell

Usuarios - Creación (V)

- La opción de emplear una plantilla consiste en crear un usuario “abstracto”, que no es real.
- Debes dejar esa cuenta deshabilitada.
- Configuramos una única vez las propiedades genéricas de nuestros usuarios (grupos a los que pertenece, horas a las que pueden trabajar, etc.).
- Ojo, que no todas las propiedades se copian.
- Para crear nuevos usuarios utilizamos la opción gráfica de **Copiar...**

Grupos

Grupos

- El concepto de grupo es equivalente al que usábamos cuando trabajamos con usuarios locales.
- Permite agrupar usuarios, de forma que se facilite la administración, proporcionando permisos o privilegios a grupos.
- Un grupo es un conjunto de objetos del dominio que pueden administrarse como una unidad.
- En el caso del Directorio Activo, un grupo puede pertenecer a otro grupo.

Grupos- Tipos

- Existen dos tipos de grupos:
 - **Distribución:** se utilizan para crear listas de distribución de correo.
 - **Seguridad:** se utilizan para asignar permisos y privilegios. Son los que solemos emplear.

Grupos- Ámbito

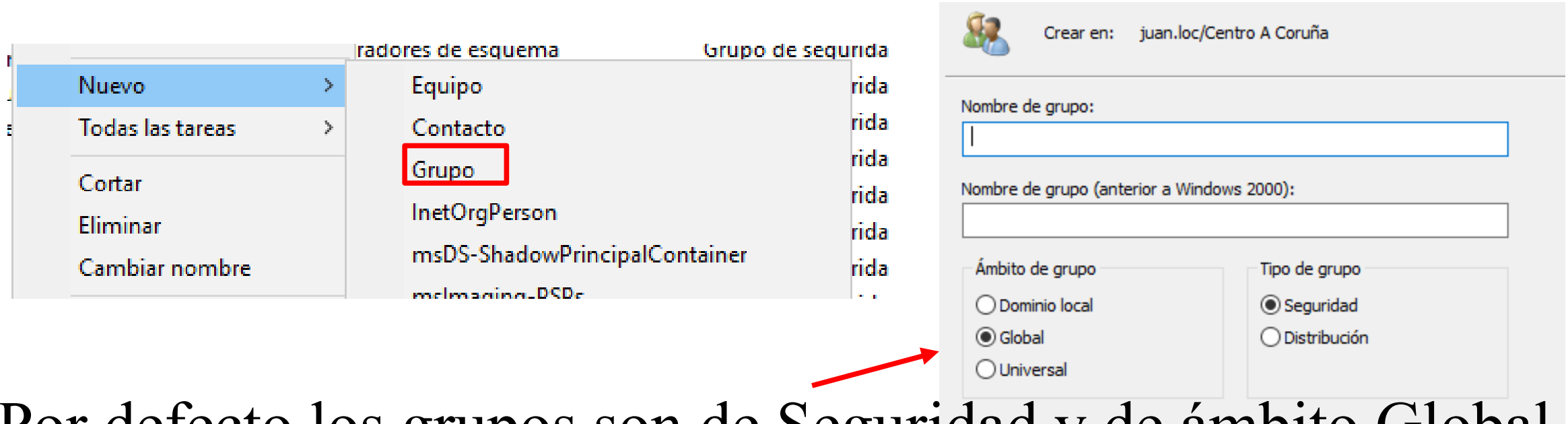
- Tres posibles ámbitos:
 - **Dominio local:** se utilizan para dar accesos dentro del dominio en el que se crean. Son los que se usan para dar acceso a carpetas compartidas o colas de impresión.
 - **Global:** usados para dar acceso a recursos de cualquiera de los dominios del bosque. Solo pueden incluir grupos y cuentas del dominio en el que se define el grupo.
 - **Universal:** misma función que los globales, pero pueden contener usuarios y grupos de cualquier dominio del bosque. Se almacenan en Catálogo Global.

Grupos- Ámbito

Ámbito	Permite asignar permisos en	Posibles miembros
Dominio local	Solo en dominio local	Cualquier objeto de cualquier dominio del bosque
Global	En cualquier dominio del bosque	Objetos del mismo dominio que el grupo
Universal	En cualquier dominio del bosque	Cualquier objeto de cualquier dominio del bosque

Grupos - Creación gráfica

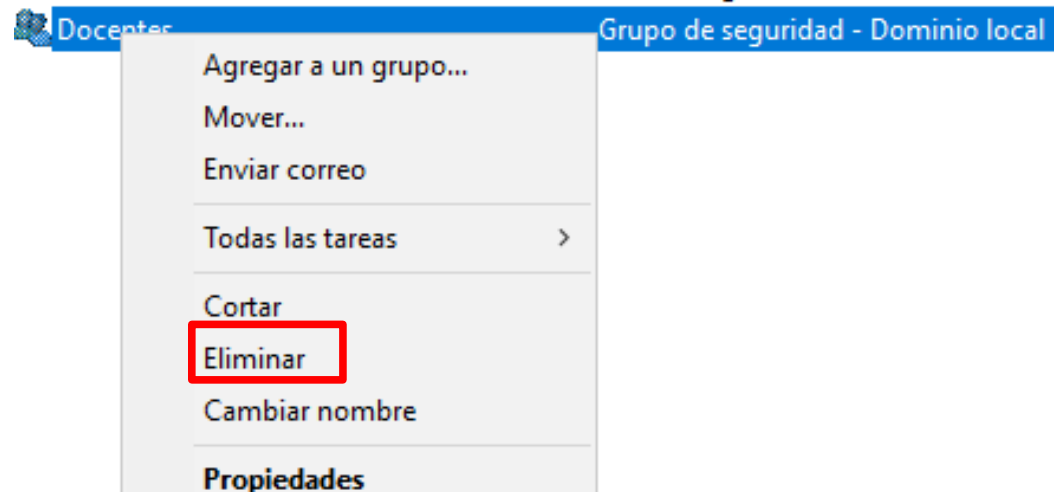
- Para crear usuarios, se selecciona la entidad de nivel superior (Contenedor u OU) y se hace click con el botón derecho



Por defecto los grupos son de Seguridad y de ámbito Global

Grupos - Eliminación gráfica

- Seleccionamos con el botón derecho del ratón sobre el grupo y escogemos **Eliminar**



Crea tus usuarios y grupos (I)

- Crea un grupo de **Profesorado**. A este grupo pertenecerán todos los docentes. Lo utilizaremos para dar accesos a carpetas de servidores dentro del dominio, y podrá contener usuarios de cualquier dominio del bosque.
- Crea otro grupo de **Alumnado**. OJO!!!, no lo confundas con las OUs. A este grupo pertenecerán los alumnos y alumnas. También lo utilizaremos para dar acceso a carpetas dentro del servidor, y podrá contener usuarios de cualquier dominio del bosque.

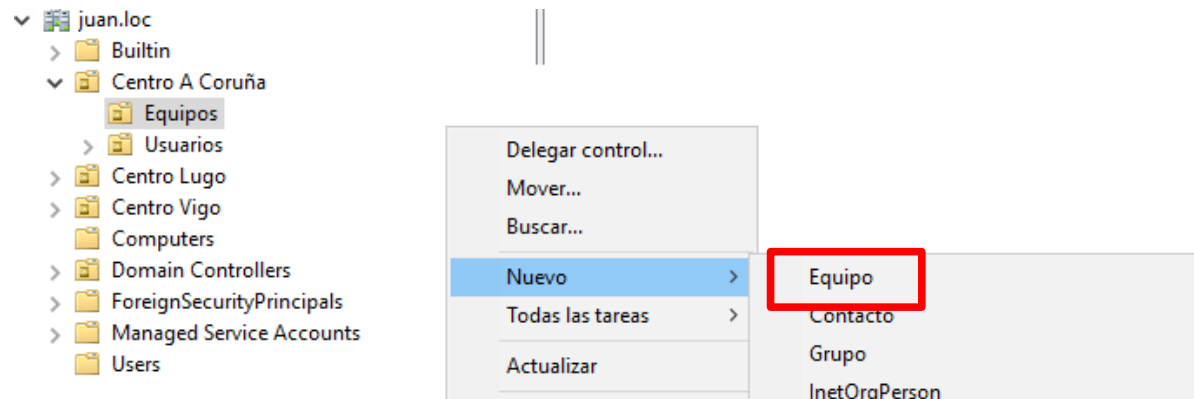
Crea tus usuarios y grupos (II)

- Crea varios usuarios:
 - Yolanda Ventura: será una alumna del centro de Vigo.
 - Gemma Prat: docente del centro de Vigo.
 - David Muñoz: alumno del centro de Lugo.
 - Constantino Fernández: docente del centro de Lugo.
 - Francisco Díaz: docente del centro de A Coruña.

Equipos

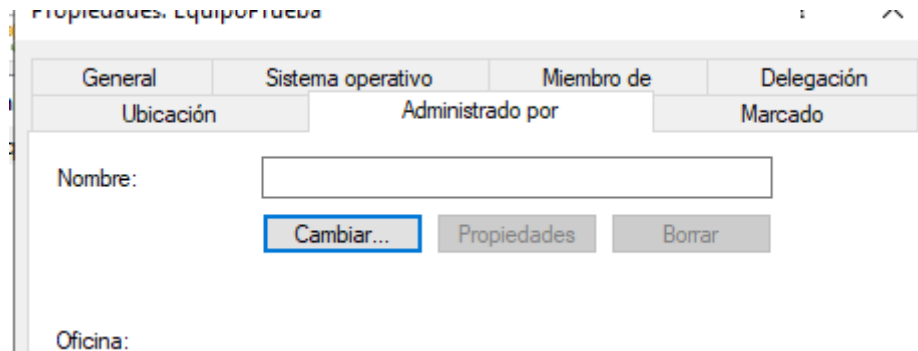
Equipos - Creación (I)

- Como vimos anteriormente, los equipos se pueden añadir al dominio de dos formas:
 - Automáticamente al unir un equipo al dominio
 - Manualmente. Permite asignar la cuenta de equipo a la OU deseada desde el primer momento.
- La creación de forma gráfica es como con el resto de elemento: click con el botón derecho encima del elemento superior y **Nuevo→Equipo**



Equipos - Creación (II)

- En el momento de la creación, podemos indicar el usuario/grupo que podrá añadir el equipo al dominio.



Propiedades: Equipo nuevo

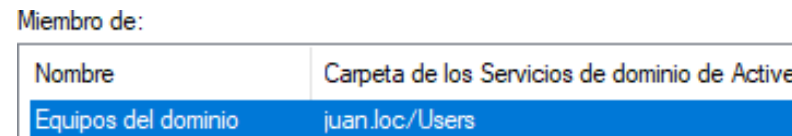
General Sistema operativo Miembro de Delegación

Ubicación Administrado por Marcado

Nombre:

Oficina:

- Al añadir un equipo de forma manual o automática, por defecto será miembro de un grupo local llamado **Equipos del dominio**.



Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active
Equipos del dominio	juan.loc/Users

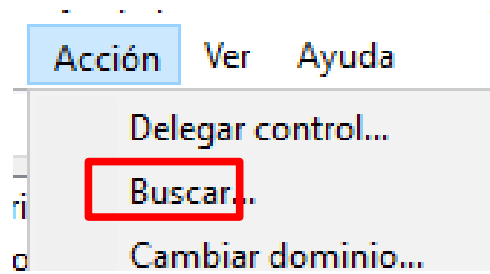
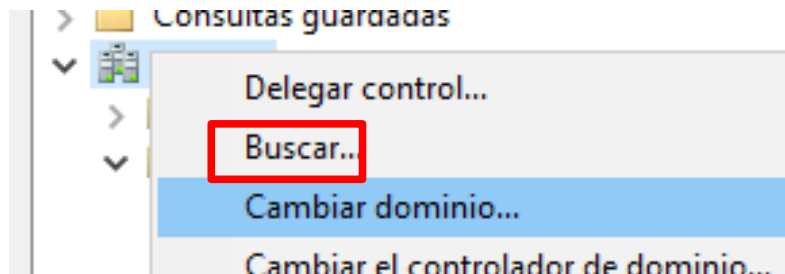
Búsqueda de objetos en AD

Búsquedas

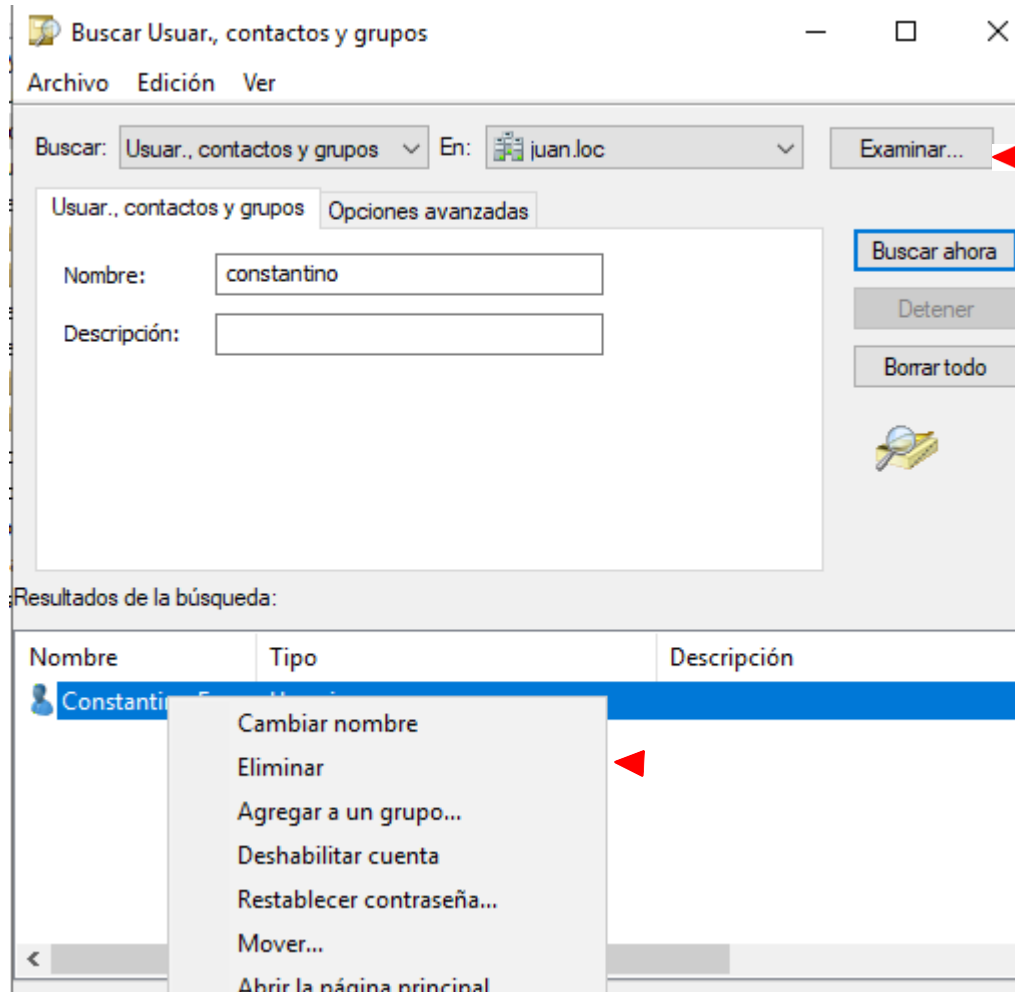
- El Directorio Activo permite hacer búsquedas de diferentes objetos, tanto de forma gráfica, como mediante comandos.
- Además, cuando trabajamos con las distintas aplicaciones, nos mostrarán objetos del dominio (usuarios/grupos).

Búsquedas gráficas (I)

- La consola de **Usuarios y equipos de Active Directory** permite realizar búsquedas, que además se pueden guardar para reutilizar en un futuro.



Búsquedas gráficas (II)



Es posible buscar en todo el bosque, un dominio o una OU concreta

Podemos buscar usuarios/grupos y realizar acciones directamente desde los resultados

Búsquedas gráficas (III)

Búsquedas gráficas (III)

Buscar: Usuar., contactos y grupos En: juan.loc Examinar...



Usuar., contactos y grupos Opciones avanzadas

Campo Condición: Valor:

Lista de condiciones:

Código po... Empieza con 36201

Resultados de la búsqueda:

Nombre	Tipo	Descripción
 Juan Fernandez	Usuario	
 UsuarioPlantilla	Usuario	

Es posible también
realizar búsquedas
por atributos
concretos

Filtros en la consola (I)

- En la consola de **Usuarios y equipos de Active Directory** es posible establecer filtros para mostrar solo aquellos objetos que cumplen unas condiciones.



- Es muy útil cuando queremos hacer modificaciones masivas de un campo sobre un conjunto de objetos.

Filtros en la consola (II)

- Por ejemplo, imagínate que en una OU hay 100 usuarios, y quieres cambiar el Departamento de aquellos que tienen **Finanzas** por **Financiero**.

