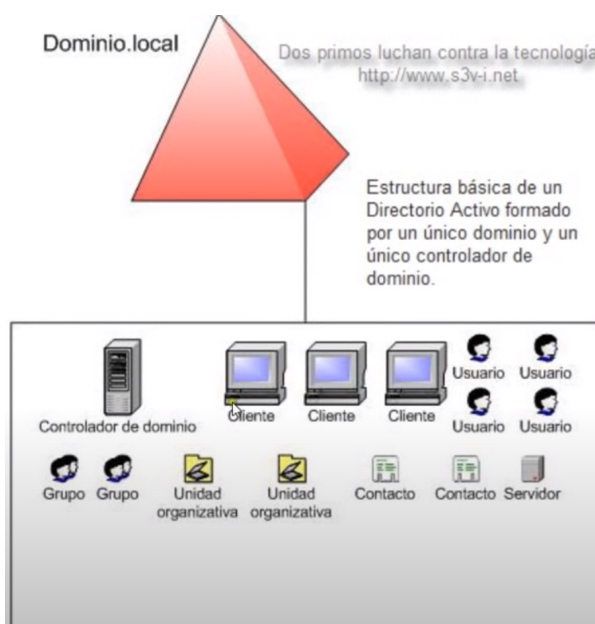
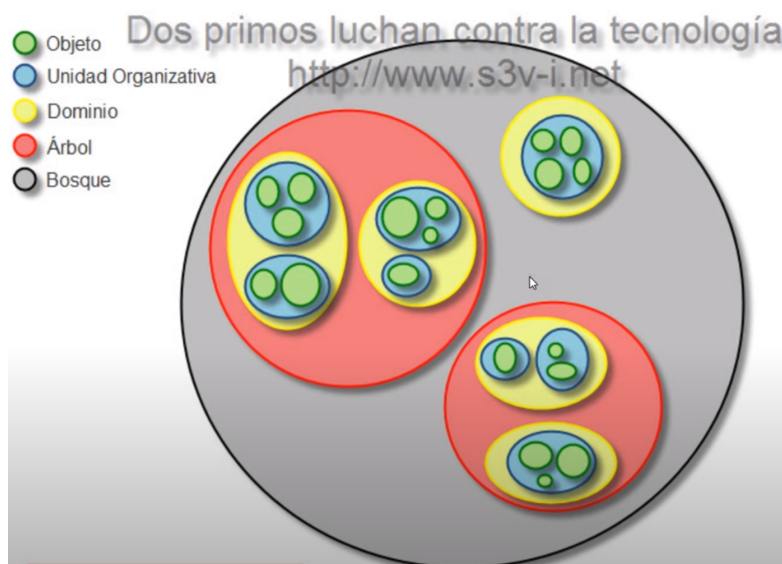


## Dominios, Unidades Organizacionales y Grupos

El dominio es el componente básico del sistema AD.



Dentro del dominio se guardan objetos, los cuales corresponden a controladores de dominio, clientes, usuarios, grupos, unidades organizacionales, entre otros.



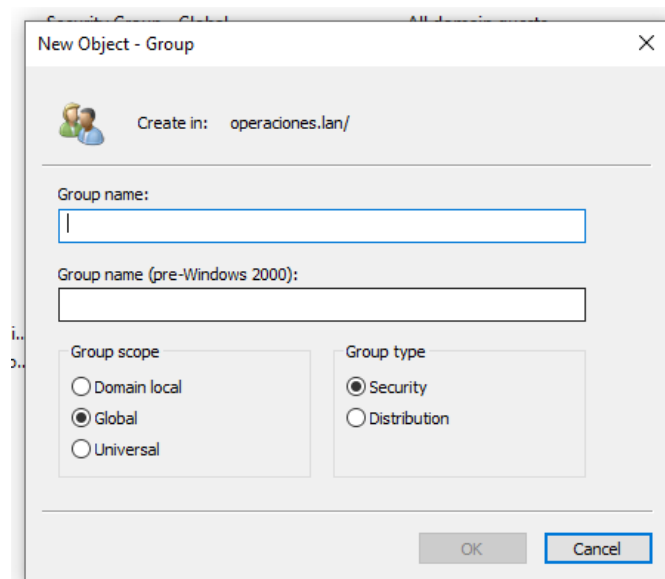
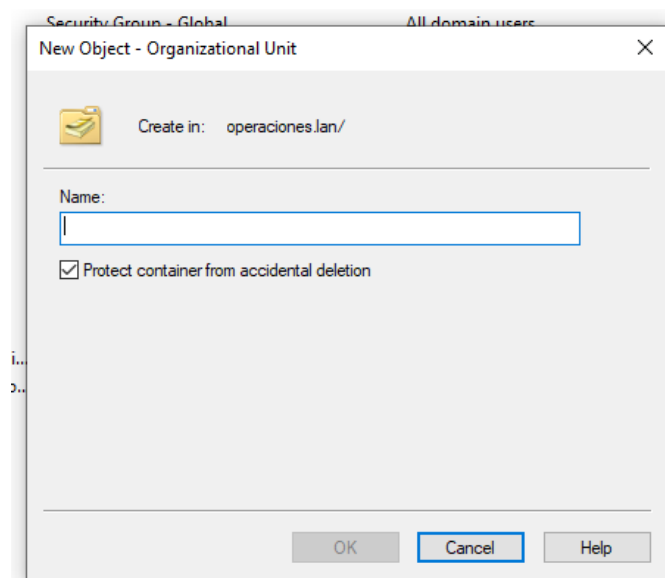
La jerarquía dentro de una estructura completa de AD es como se aprecia en la imagen, los **objetos** se pueden agrupar en **unidades organizativas**, las cuales pertenecen a un **dominio** o **subdominio**. Un dominio que contiene uno o más subdominios se considera un **árbol**, donde la posterior interacción entre dos o más **árboles** termina en el establecimiento de un **bosque**.

## Con respecto al uso de UO y Grupos

Las unidades organizacionales y los grupos tienen dos usos distintos dentro de Active Directory.




1. Unidades organizacionales: agrupan usuarios y grupos, se utilizan para aplicar políticas a los mencionados anteriormente.
2. Grupos: agrupan usuarios, se utilizan para la aplicación de seguridad y acceso a recursos en la red.

Utilizando **RSAT Active Directory Users and Computers** es posible crear usuarios, unidades organizacionales y grupos, además de administrar ciertos aspectos como delegación de control para unidades organizacionales o integrantes de grupos.





## Pruebas con SAMBA AD, RSAT y ldapsearch

Dentro de **RSAT Active Directory Users and Computers** se crearon tres unidades organizacionales:

- >  Académicos
- >  Administrativos
- >  Estudiantes

Dentro de la unidad organizacional **Administrativos** se crearon los dos siguientes objetos:

Name	Type
 Coordinacion TI	Security Group - Global
 Roberto Lillo	User

```
# Coordinacion TI, Administrativos, operaciones.lan
dn: CN=Coordinacion TI,OU=Administrativos,DC=operaciones,DC=lan
objectClass: top
objectClass: group
cn: Coordinacion TI
instanceType: 4
whenCreated: 20210508231044.0Z
whenChanged: 20210508231044.0Z
uSNCreated: 3821
uSNChanged: 3821
name: Coordinacion TI
objectGUID:: dFjsLOst3USrNcBG4HcVKA==
objectSid:: AQUAAAAAAAAUVAFAFZelTHONeKVLueJhVwQAAA==
sAMAccountName: Coordinacion TI
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=operaciones,DC=lan
distinguishedName: CN=Coordinacion TI,OU=Administrativos,DC=operaciones,DC=lan
```

```
# Roberto Lillo, Administrativos, operaciones.lan
dn: CN=Roberto Lillo,OU=Administrativos,DC=operaciones,DC=lan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Roberto Lillo
sn: Lillo
givenName: Roberto
instanceType: 4
whenCreated: 20210508231113.0Z
whenChanged: 20210508231113.0Z
displayName: Roberto Lillo
uSNCreated: 3822
name: Roberto Lillo
objectGUID:: vml0IzhZn0qN3yLWcQ+1mQ==
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAFAFZelTHONeKVLueJhWAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: roberto.lillo
sAMAccountType: 805306368
userPrincipalName: roberto.lillo@operaciones.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=operaciones,DC=lan
pwdLastSet: 1326498907300000000
userAccountControl: 66048
uSNChanged: 3825
distinguishedName: CN=Roberto Lillo,OU=Administrativos,DC=operaciones,DC=lan
```

## INFORMACIÓN IMPORTANTE SOBRE EL CORREO COMO ID

Cuando se crea un usuario utilizando **samba-tool** hay dos atributos a los que se les asigna el mismo valor, **cn** y **sAMAccountName** (esto siempre y cuando no se entreguen los valores correspondientes a la herramienta al momento de crear el usuario). **sAMAccountName** es el valor que Active Directory utiliza como ID del usuario y es el con mayor importancia de los dos.

Cuando se crea un usuario en **samba-tool** es posible utilizar de **sAMAccountName** un correo (como por ejemplo “*roberto.lillo@usach.cl*”), valor que posteriormente puede ser verificado mediante **ldapsearch** o con **RSAT Active Directory Users and Computers**.

```
sAMAccountName: roberto.lillo@usach.cl
```

*Versión ldapsearch*

Attribute	Value
sAMAccountName	roberto.lillo@usach.cl

*Versión RSAT Active Directory Users and Computers*

Pero surgen los dos siguientes problemas:

1. Cuando se intenta crear el usuario directamente desde **RSAT Active Directory Users and Computers**, la herramienta no permite el uso de caracteres especiales como el “@” y los reemplaza por un “\_”.

Esto es posible de solucionar habilitando **Advanced Features** en la pestaña **View**, lo que permite editar a un nivel más bajo los atributos del objeto directamente, de esta forma se puede modificar el valor guardado “*roberto.lillo\_usach*” por “[roberto.lillo@usach.cl](mailto:roberto.lillo@usach.cl)”

2. El segundo es un problema de mayor escala, que produce que la anterior solución no sea viable de todos modos.

Al momento de iniciar sesión en un dominio en Windows 10 se puede realizar de varias formas:

- Si el usuario anterior ya había iniciado sesión en el dominio, solo necesita ingresar su nombre de usuario y contraseña.
- En el caso contrario puede utilizar la dirección del dominio para ingresar, por ejemplo:
  - i. **OPERACIONES**\nombreDeUsuario
  - ii. **OPERACIONES.LAN**\nombreDeUsuario
  - iii. nombreDeUsuario@operaciones.lan

Es particularmente con el último que existe una contradicción con nuestra idea de utilizar el correo institucional como ID de un usuario del dominio, ya que si intento iniciar sesión con mi usuario "*roberto.lillo@usach.cl*" Windows lo interpreta como que quiero ingresar al dominio **USACH.CL** de Active Directory.

Al intentar ingresar utilizando **OPERACIONES.LAN***roberto.lillo@usach.cl* tampoco se obtiene el resultado esperado y no se puede iniciar sesión en Windows 10.

Debido a lo anterior considero que ya no es posible utilizar el correo como **sAMAccountName**, lo que hace imposible hacer login en Windows 10 con el correo usach.

Como solución está utilizar solo la parte del correo que no corresponde a dominio como ID (solo *roberto.lillo* en vez de *roberto.lillo@usach.cl*) y luego utilizar el atributo **mail** para guardar el valor del correo institucional completo.

De esta forma se seguiría usando el concepto del correo institucional como ID única, mientras que se podría usar el atributo **mail** para la búsqueda y mapping de usuarios en otros sistemas como Gluu o Auth2.