Implantación de SO

UT3:

Administración y acceso a dominios

F.M.G

OBJETIVO

- En esta unidad de trabajo veremos todos los conceptos que debemos manejar para instalar el Servicio de Directorio Activo en Windows Server 2008 o superior, centrándonos en W2K19S.

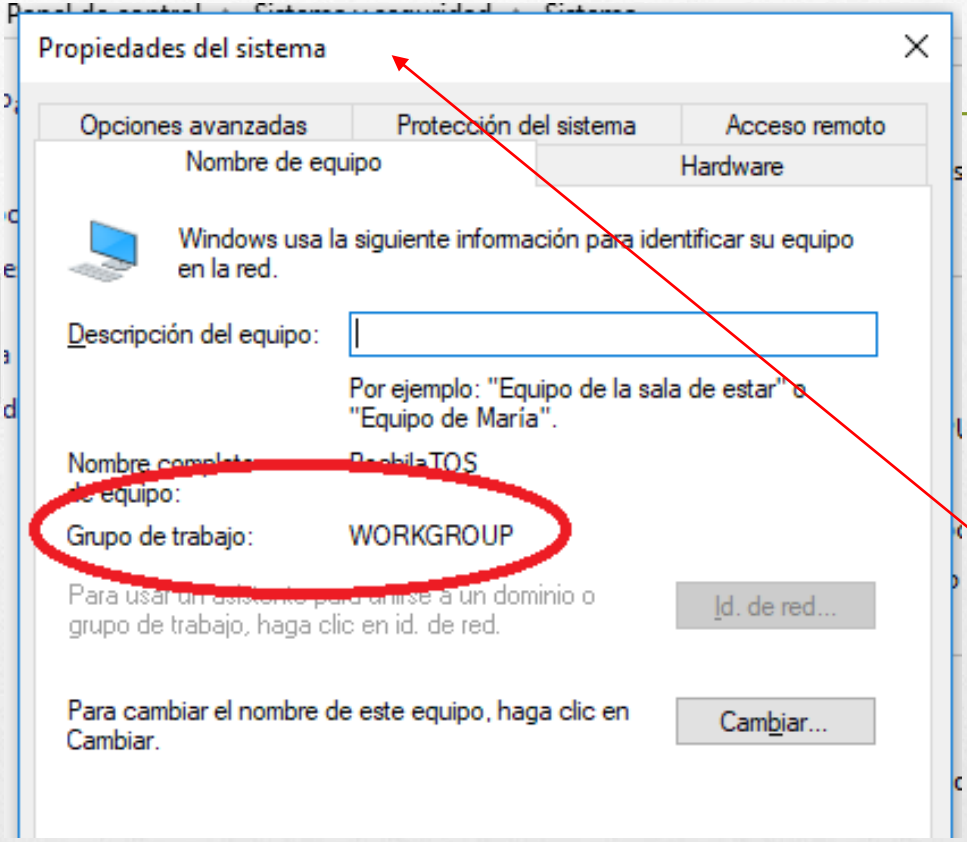
Índice

- Distinguir entre la estructura **grupo de trabajo** y la estructura **cliente-servidor**.
- Conocer en una estructura cliente-servidor los **Roles que puede tomar el servidor**
- Conceptos varios sobre **Active Directory**
- **Estructura lógica** de Active Directory
- **Estructura física** de Active Directory

Conceptos previos

- **Estructuras de configuración de la red**
  - Estructura de grupo de trabajo
  - Estructura cliente / Servidor

Conceptos Grupo de trabajo I



¿Dónde vemos que se trata de un Grupo de trabajo ?

Ir a la ventana de la izquierda.

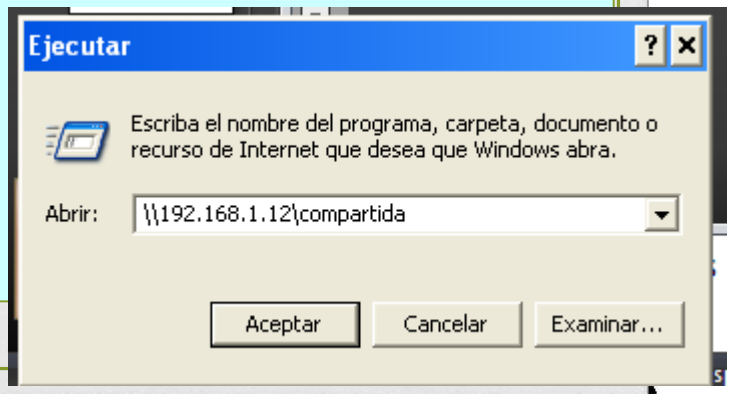
Propiedades del sistema

Conceptos Grupo de trabajo II

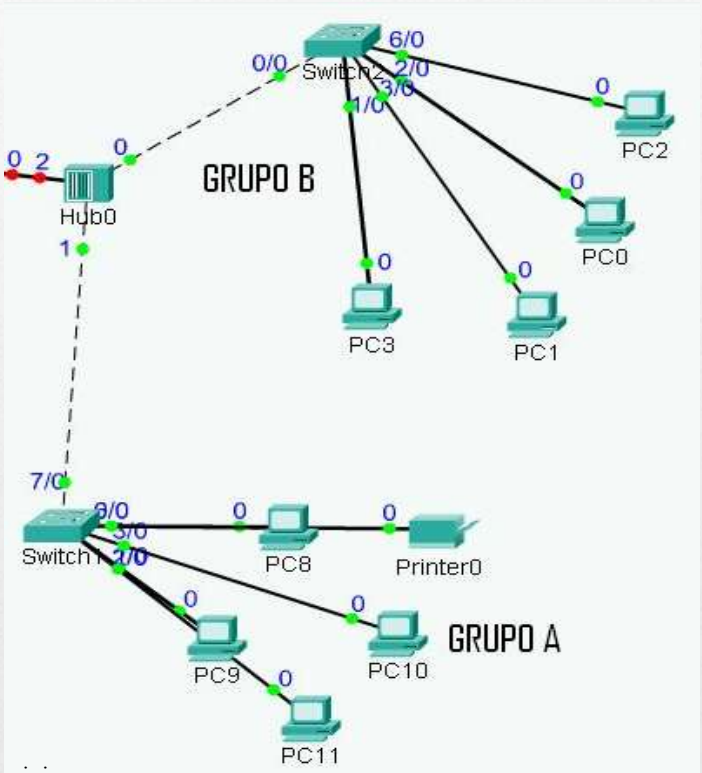
- **Estructura (I)**
  - Es la unión de los diferentes recursos de todos los ordenadores de los usuarios con el resto de los usuarios.
  - A través de una conexión de red se conectan entre sí todos los ordenadores para compartir recursos, y de esta manera cada usuario comparte sus recursos:
    - Impresoras
    - Modem
    - Archivos, Unidad de CD-ROM …

Conceptos Grupo de trabajo III

- **Estructura (II):**
  - Es sencillo ver y compartir recursos
  - La seguridad se establece sólo por contraseñas
  - Para localizar recursos compartidos se utilizan servicios de exploración.
  - Utilidades para explorar la red e identificar recursos a los que conectarse (depende de la versión de Windows):
    - Entorno de red
    - Mis sitios de red
    - Red



Conceptos Grupo de trabajo IV



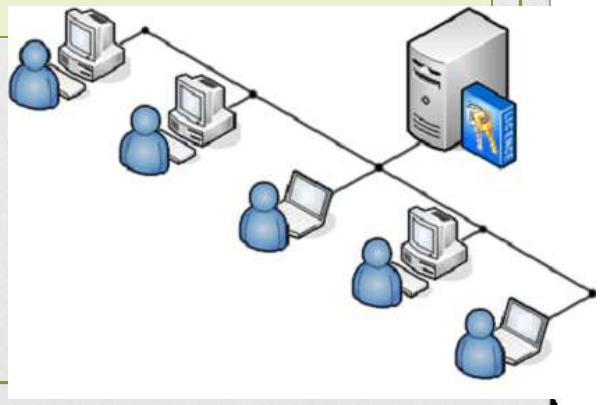
Estructura grupo de trabajo

Conceptos Grupo de trabajo V

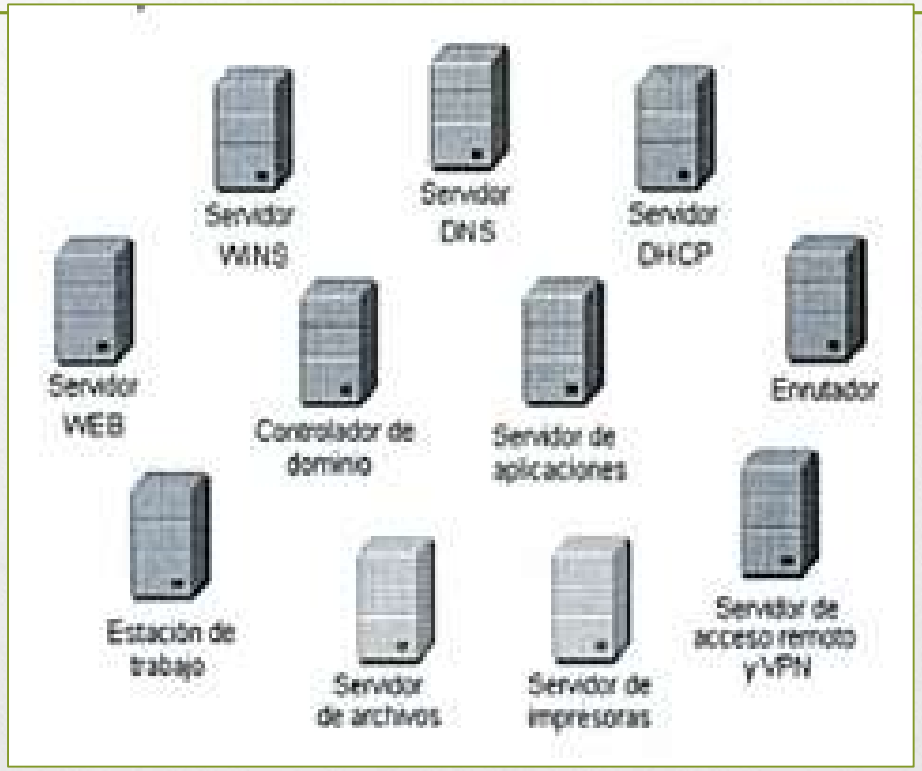
- **Inconvenientes:**
  - Algunos recursos compartidos son difíciles de localizar para los usuarios
  - Los recursos se comparten con un grupo limitado de colaboradores.
  - El usuario debe tener permiso en el ordenador donde esta el recurso.

Conceptos Cliente/Servidor I

- **Estructura cliente servidor**
  - **Servidor** es un PC que comparte todos los recursos, con el resto de PC, conectados a él.
  - **Clientes** son los diferentes PC que se conectan para utilizar los recursos.



Roles que puede tomar el Servidor



Conceptos cliente/servidor II

- **Roles del Servidor**
  - **Servidor de archivos:**
    - Mantiene los archivos en subdirectorios privados y compartidos para los usuarios de la red.
    - Pueden ser:
      - **Dedicados:**
        - Si se dedican sólo a la gestión de la red
      - **No dedicados (autónomo):**
        - Si se dedican a la gestión de la red y además es estación de trabajo

Roles del Servidor

- **Servidor de comunicaciones;**
  - Permite enlazar diferentes redes locales o una red local con grandes ordenadores o miniordenadores
- **Servidor de correo electrónico:**
  - Proporciona servicios de correo electrónico para la red.

Roles del Servidor

- **Servidor Web:**
  - Proporciona un lugar para guardar y administrar los documentos HTML a los que acceden los usuarios a través de navegadores
- **Servidor FTP:**
  - Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red

Roles del Servidor

- **Servidor Aplicaciones:**
  - Es el servidor en el que están las aplicaciones a las que se conectan los clientes para poder trabajar.
- **Servidor de impresión:**
  - Tiene conectadas una o más impresoras que comparten con los demás usuarios.

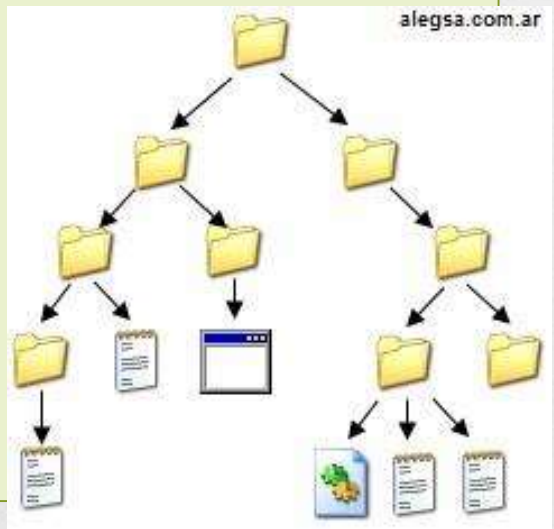
Roles del Servidor

- **Servidor proxy**
  - Se utiliza para monitorizar y controlar el acceso entre las redes.
  - Su función es:
    - Cambiar la dirección IP de los paquetes enviados por los usuarios con el objetivo de ocultar de la red interna a Internet
    - Cuando reciben contestación externa, la devuelve al usuario que lo ha solicitado.
    - Así se evita que los piratas accedan a la información interna de los PCs de la red.

Conceptos I

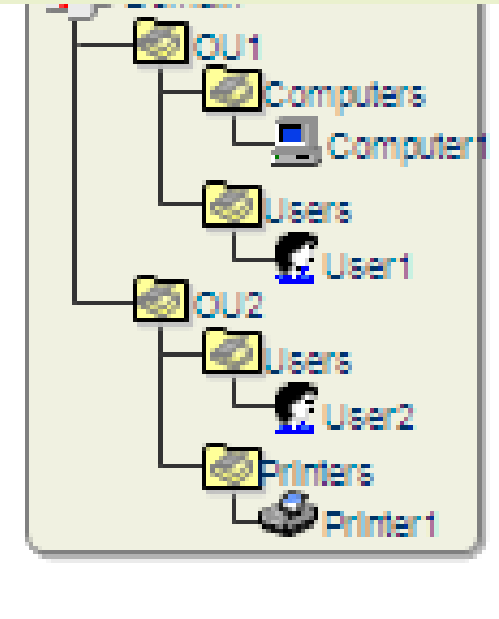
- **DIRECTORIO:**

  Es una estructura jerárquica que almacena información acerca de los objetos existentes de la red.



Conceptos II

- **OBJETO:**
  - Es cualquier cosa que tenga entidad en el directorio, o sea es la forma de representa un recurso de la red
  - Puede ser;
    - un programa,
    - un usuario,
    - un ordenador,
    - una impresora,
    - un router, un proxy, etc ...
  - Se guarda en **NTDS.dit**

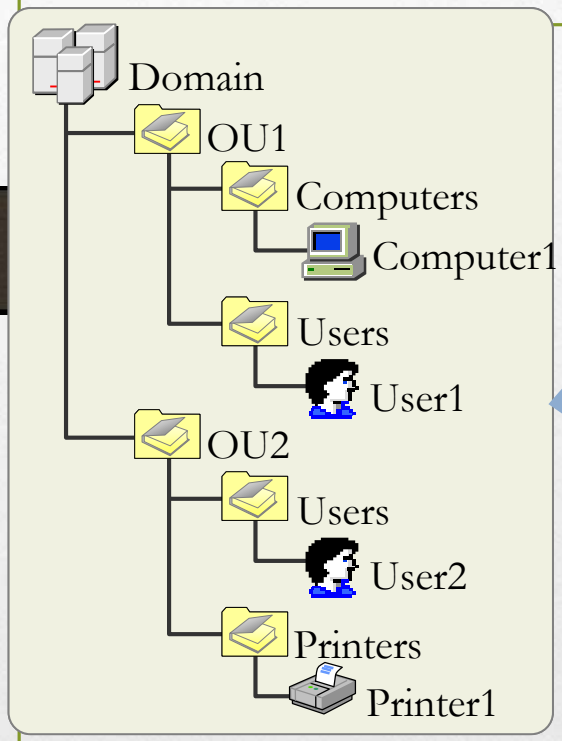


Conceptos III

- **SERVICIO DE DIRECTORIO:**
  - Proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores y los usuarios de la red.
  - Permitiendo que un usuario encuentre cualquier objeto con sólo conocer uno de sus atributos.

Concepto IV

- **ATRIBUTO**

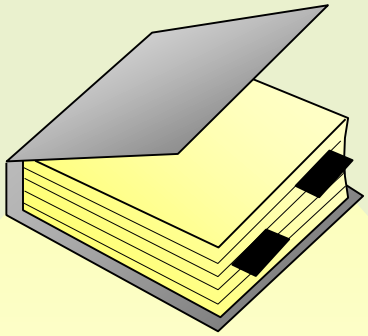


KimYoshida	
Atributos	Valores
Nombre	**Kim Yoshida**
Edificio	**117**
Planta	**1**

Conceptos V

- **DIRECTORIO ACTIVO:**
  - Es un servicio de directorio, utilizado por Windows Server.
  - Permite:
    - Agilizan las búsquedas de recursos,
    - Se asegura de la autentificación de usuarios y máquinas,
    - Se comparten mejor los recursos de la red.
    - Se abandona **Netbios** como protocolo para compartir recursos y se resuelven mediante **DNS** y el **catálogo global**
    - Nos dice la dirección IP de la maquina cliente para que encaminemos a ella.
    - Nos indica que máquina nos proporciona cada servicio.

Conceptos V



¿Qué es Directorio Activo?

La funcionalidad del servicio de directorio

- Organizar
- Administrar
- Controlar

Recursos

Administración centralizada

- Punto de administración único
- Acceso completo del usuario a los recursos de directorios al iniciar sesión una vez

Conceptos VI

- **Conceptos que aparecen en DA**
  - **FQDN:**
    - es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.
    - son dos partículas separadas por un pto.
    - Ejemplo: google.com o serv1.bar.com donde serv1 es nombre del equipo.
    - Admite hasta 256 caracteres y entre punto y punto 63 caracteres, y no distingue entre mayúscula y minúscula.
  - **NETBIOS:**
    - Admite 15 caracteres como máximo para cada máquina conectada a la red.
    - Usado por ordenadores NT

Conceptos VI

- El directorio activo hace uso de
  - Protocolo LDAP
  - DNS,
  - DHCP,
  - Kerberos
  - ...

Conceptos VII

- **Protocolo LDAP**
  - Lightwight Directory Access Protocol , o sea, Protocolo ligero de acceso a directorio.
  - Protocolo a nivel de aplicación que accede a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.
  - Es considerada una "BBDD" en la que se pueden realizar consultas.

LDAP basado en X.500.

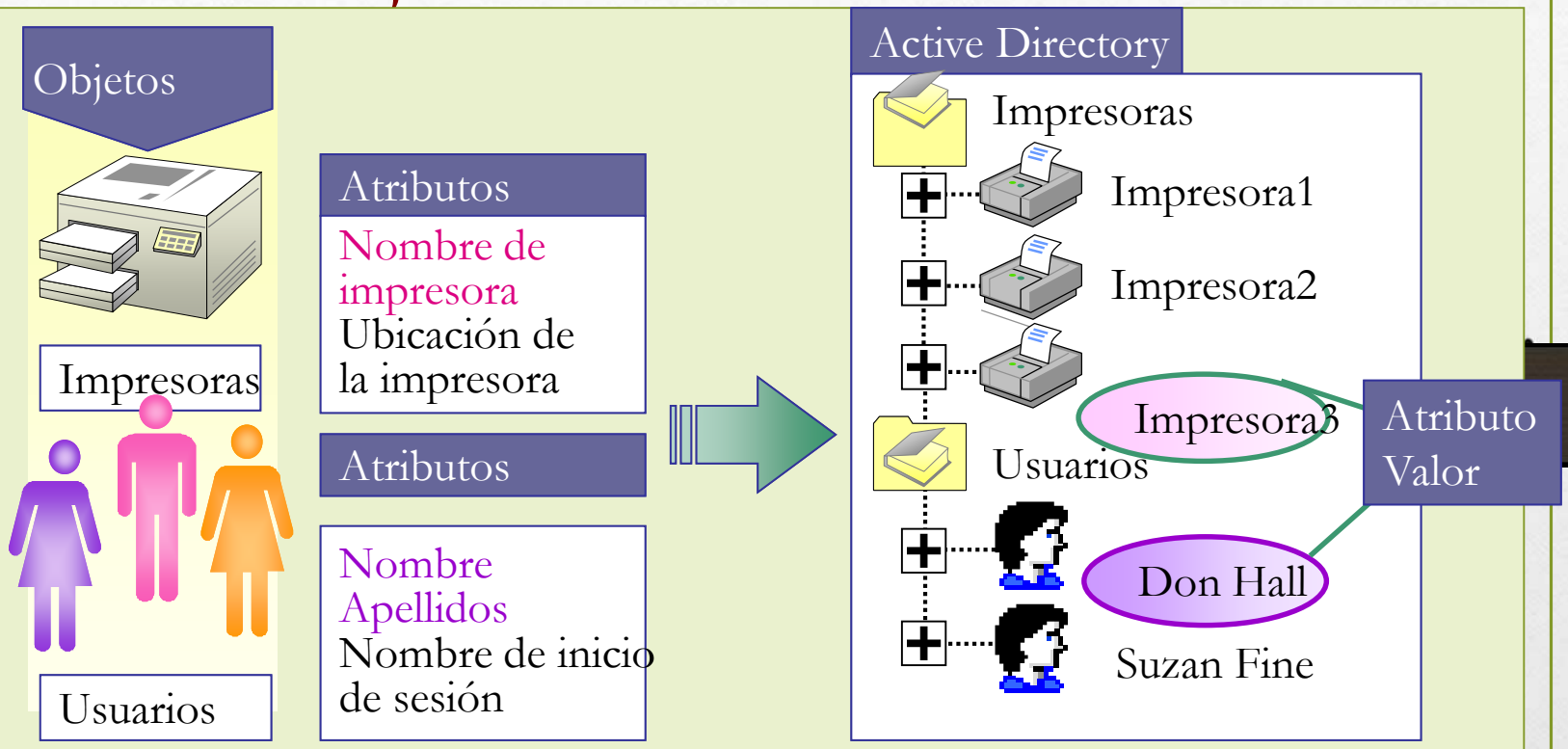
Conceptos VII

- LDAP proporciona una manera de comunicar con Active Directory especificando las rutas de nomenclatura únicas de cada objeto del directorio
- Las rutas de nomenclatura de LDAP incluyen:
  - Nombre completo

CN= Suzan Fine,OU=Sales,DC=contoso,DC=msft

  - Nombre completo relativo

Conceptos VIII:
Objetos Directorio Activo



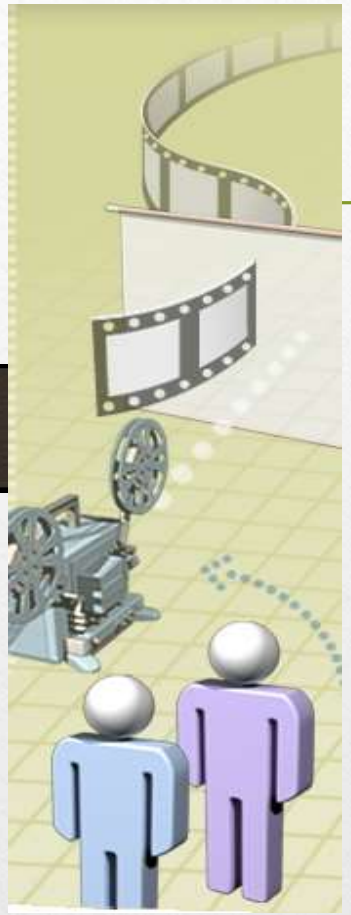
- Los objetos representan los recursos de red
- Los atributos definen la información relativa a un objeto

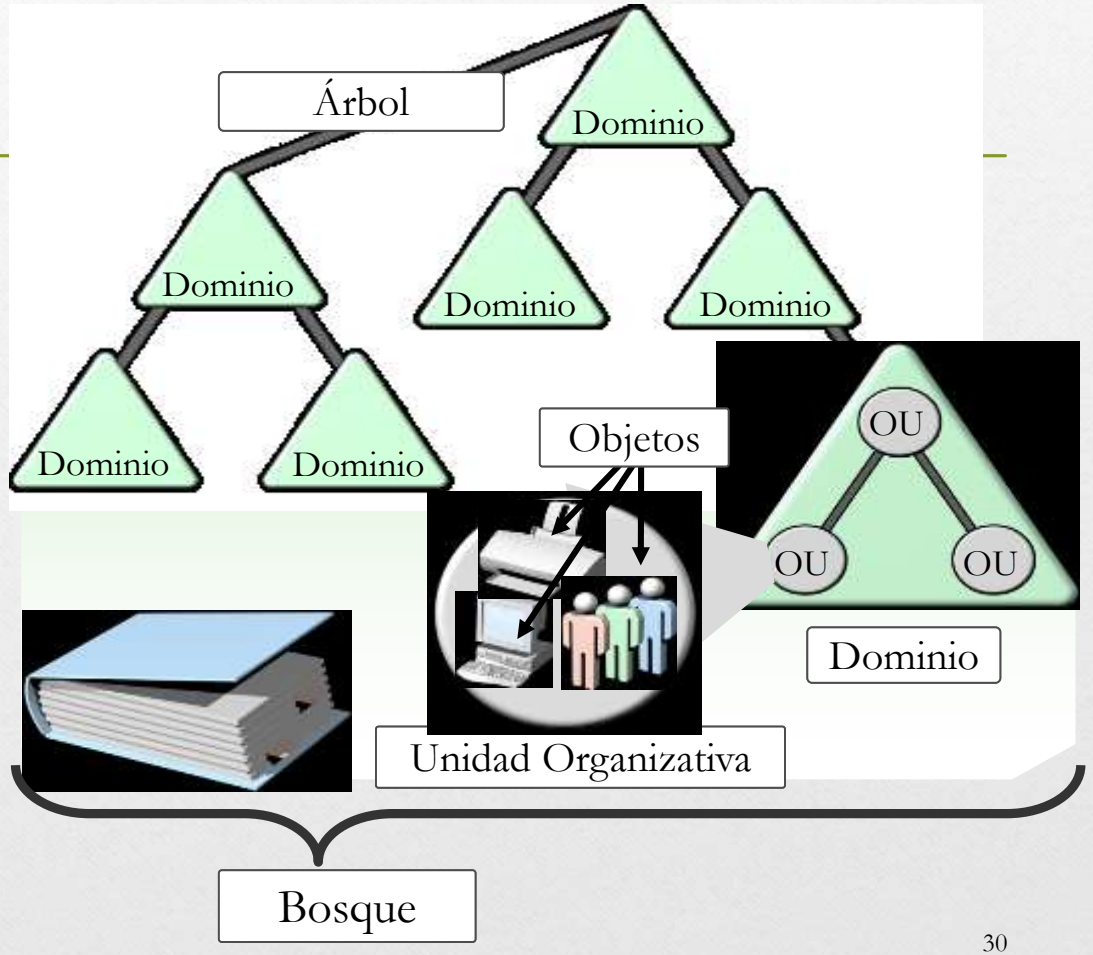
Debemos conocer:

Estructura lógica DA

Estructura física DA

Estructura Lógica DA

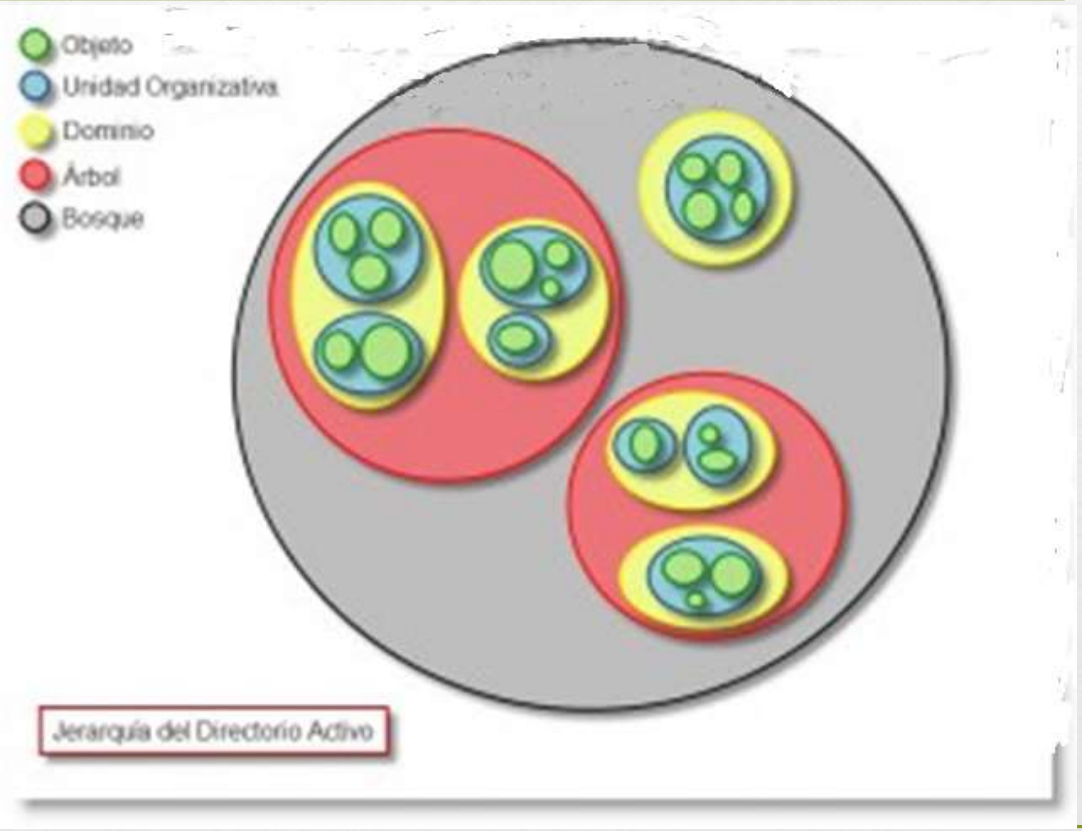




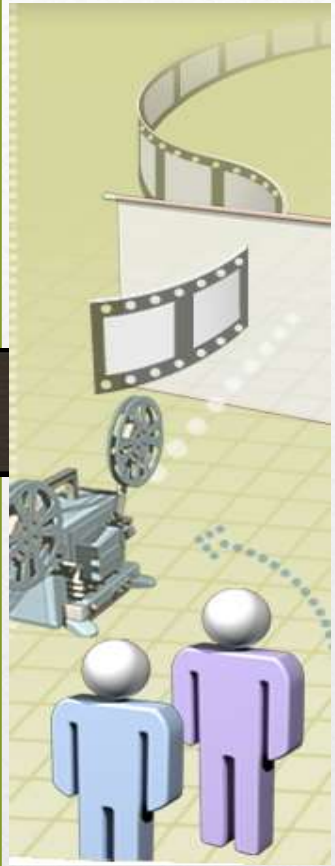
Jerarquía lógica del DA.

- **se basa en:**
  - Bosque
  - Árbol
  - Dominios
  - Unidades organizativas
  - Grupos
  - Objetos
    - usuarios, equipos,
    - impresoras, carpetas
    - …

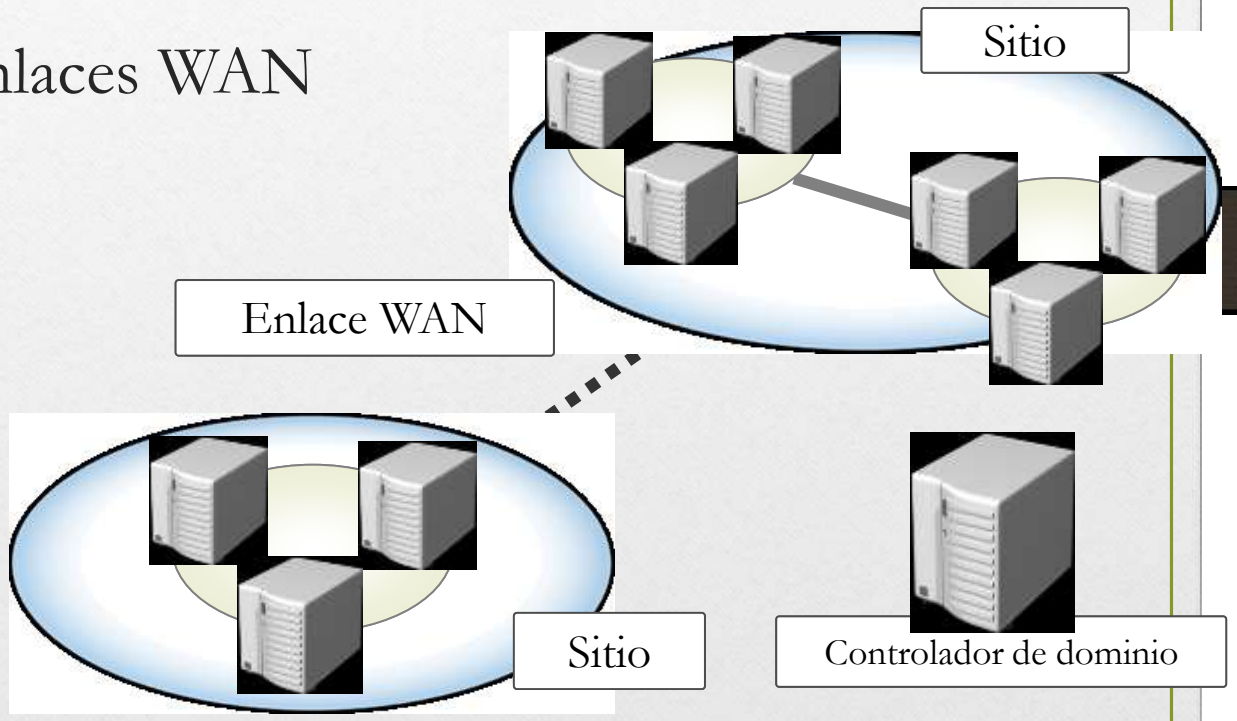
Jerarquía del directorio activo
Visión gráfica



Estructura física DA



- Sitios
- Controladores de dominio
- Enlaces WAN



Nos centraremos en los elementos de estas estructuras

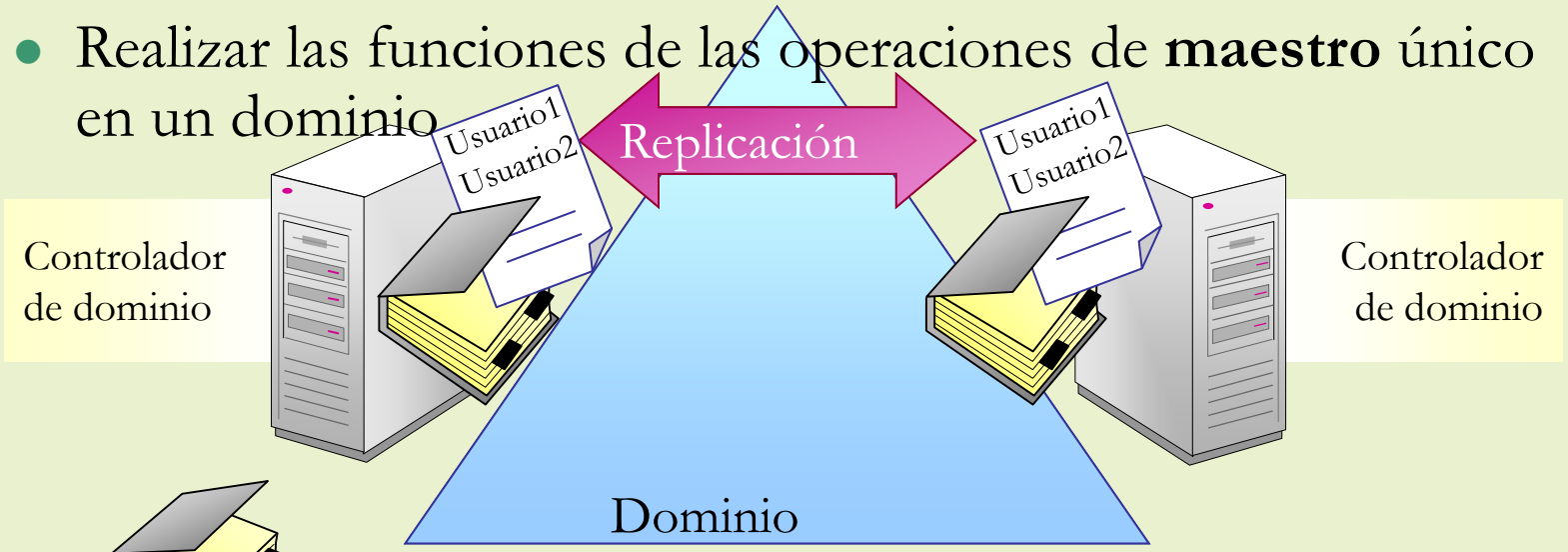
Directorio Activo (**Estructura física)**

Conceptos previos

- Controlador de dominio
- Sitio
- Enlace WAN

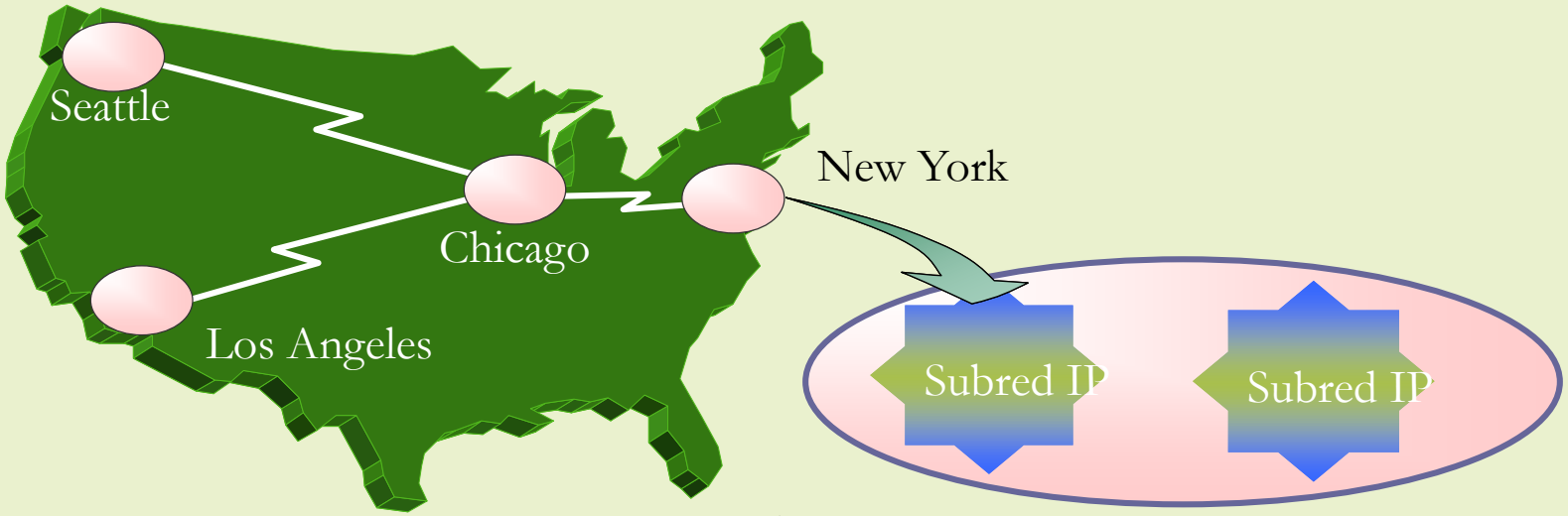
1. Controladores de dominio

- Es el policía que nos dice si pasamos o no a través de la BBDD que es AD.
- Alojar la carpeta **SYSVOL** (BBDD)
- Participar en la replicación de Active Directory
- Realizar las funciones de las operaciones de **maestro** único en un dominio



= Una copia escribible de la base de datos de Active Directory

2. Sitios



- Es la representación lógica de como se encuentran distribuidos los equipos físicamente

- Optimiza el tráfico de replicación.
- Permite que los usuarios inicien sesión en un controlador de dominio con una conexión de red confiable y bien conectada.

3.Enlace WAN

- Permite comunicar redes de computadoras entre distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

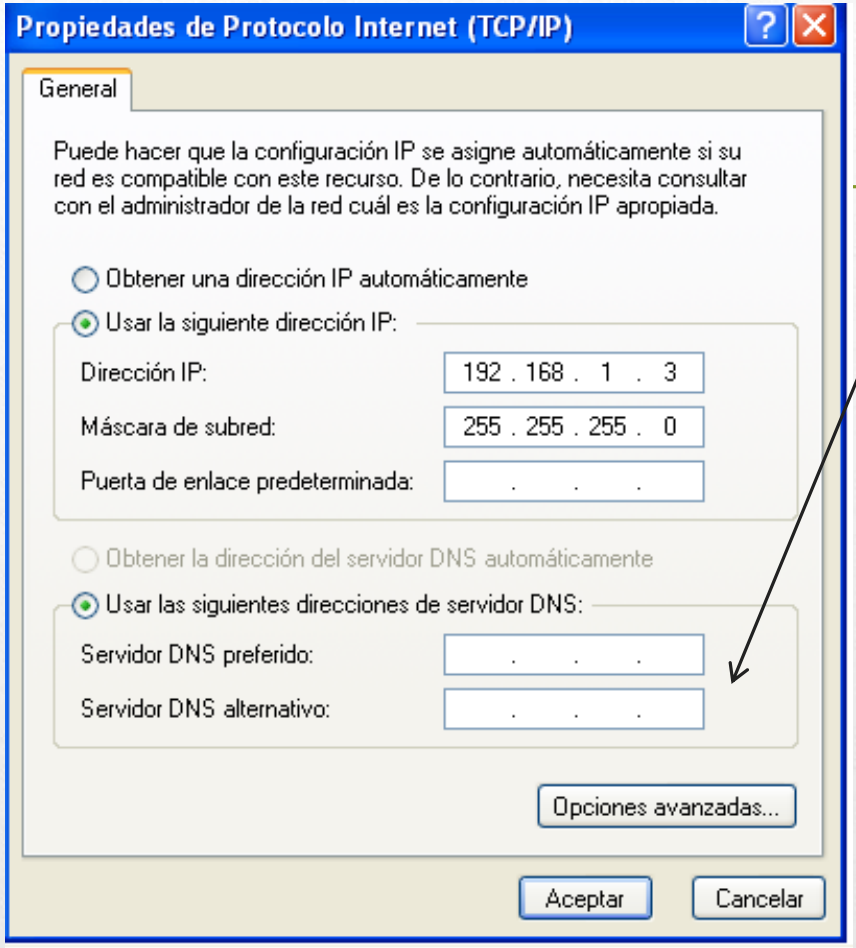
Active Directory y DNS

- Resolución de nombres.
- Definición de espacios de nombre.
- Localización de los componentes físicos de Active Directory.

Ósea

DNS sirven para identificar a los dominios y subdominios por sus respectivos namespaces

¿Cómo configurar el DNS?

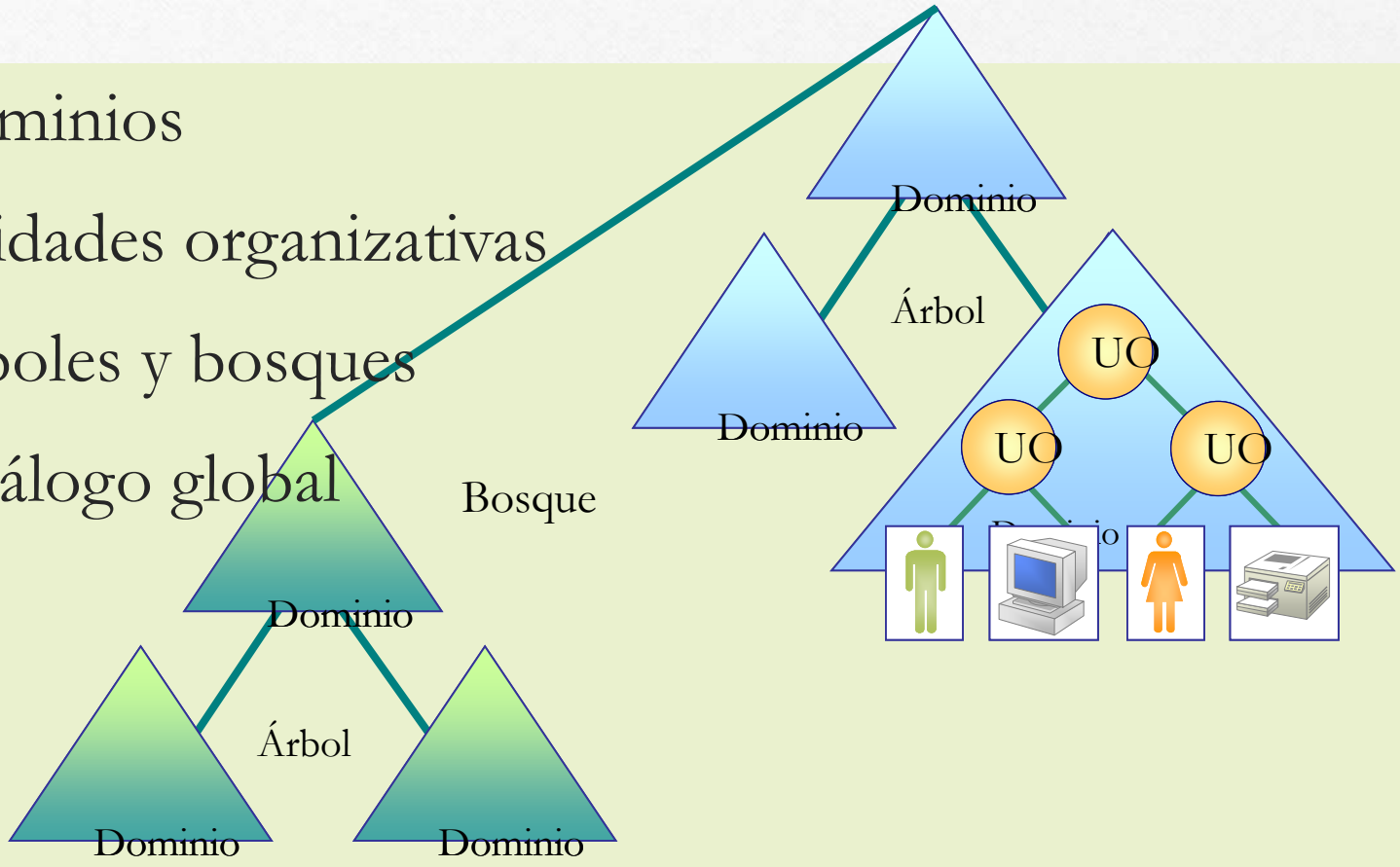


Recordemos que:

- **Servidor DNS:**
  - Siempre acompaña a un controlador de dominio.
  - En la primera máquina es obligatorio en las sucesivas es recomendable.
  - Sirven para identificar a los dominios y subdominios por sus respectivos nombres.

Estructura lógica del DA

- Dominios
- Unidades organizativas
- Árboles y bosques
- Catálogo global



Directorio Activo (**Estructura lógica)**

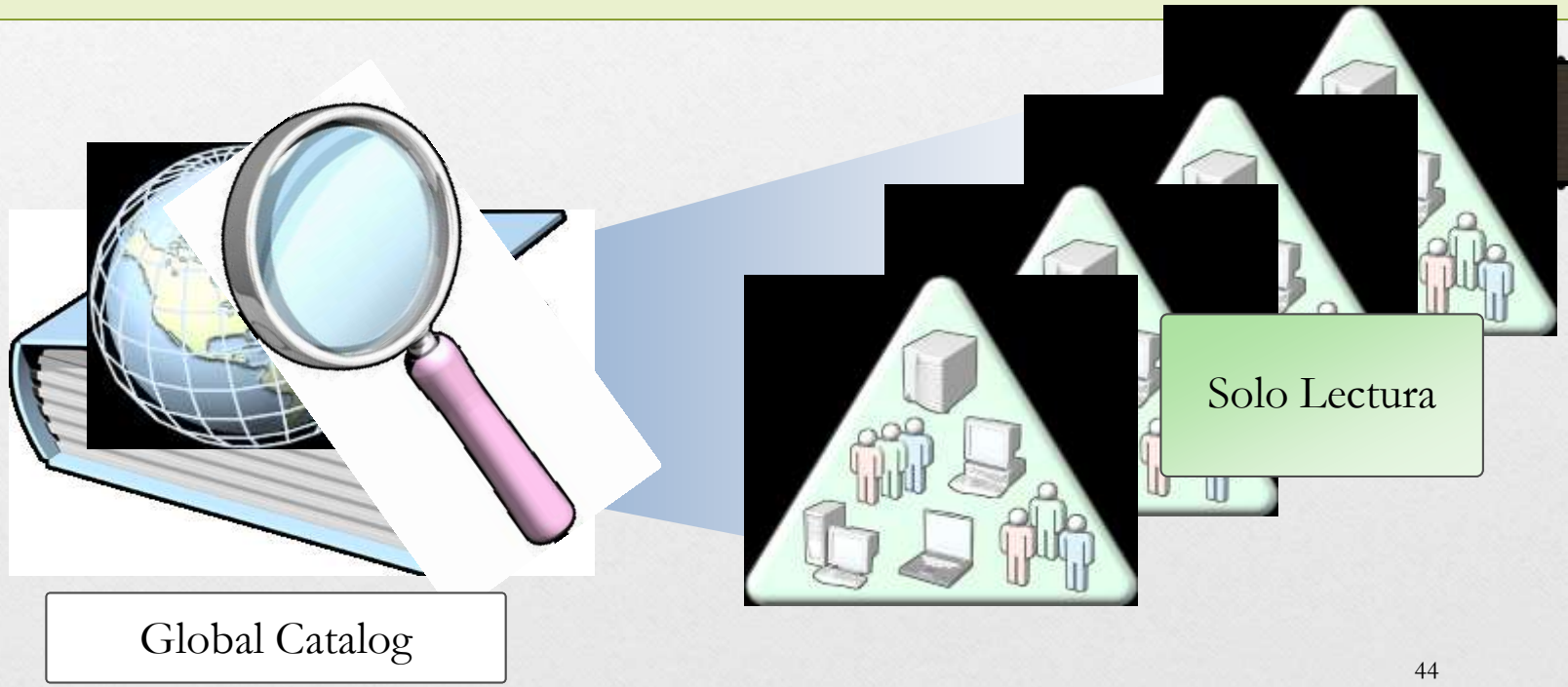
Conceptos previos

- Catálogo global
- Esquema

- Clase
- Atributo

- Dominio
  - UO
  - Usuarios
  - Grupos
- Árbol
- Bosque

Repositorio que contiene información acerca de cada uno de los objetos del directorio activo de un árbol o de un bosque



1. Catalogo Global del DA (I)

- El AD genera los contenidos del catalogo con los contenidos de los distintos Controlador de dominio (DC) mediante replicación.
- Es un servicio y un almacén.
- Al instalar un DC se instala un AD y se crea **un Catálogo global** y ese servidor se convierte en un Servidor de catálogo global
  - Posteriormente los DC se pueden convertir en Servidores de catálogo global
  - Cuantos más servidores de catalogo, más tráfico de replicación y respuestas más rápidas a los usuarios

1. Catalogo Global del DA (II)

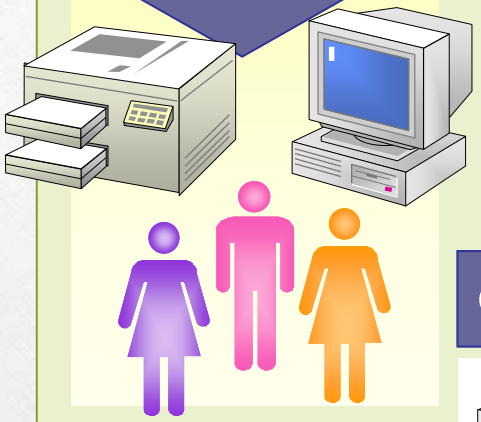
- Tiene una **copia completa,** del directorio de su dominio, con todos los objetos (todos sus atributos)
- Tiene una **copia parcial,** de los directorios de los otros dominios del bosque, de todos los objetos
  - La copia parcial almacena los atributos usados con más frecuencia en las operaciones de búsqueda.
- Luego es un almacén central de información de todos los objetos del directorio de los dominios del bosque
- Permite a los usuarios y administradores encontrar información independientemente del dominio de directorio que realmente los contiene.

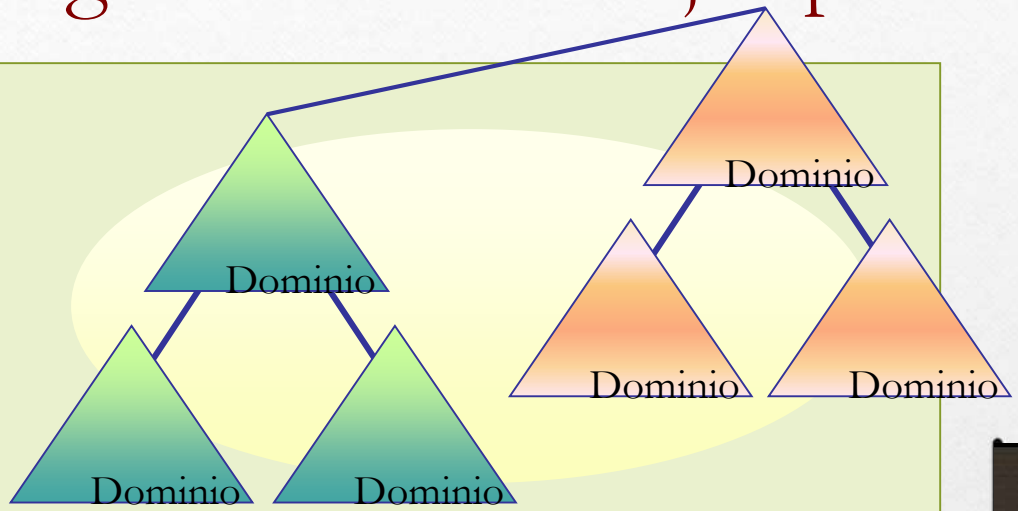
1. Catálogo global del DA (III)

- Es conocido como **servidor de catálogo global,** el primer controlador de dominio creado al instalar AD, que de forma predeterminada se convierte en catálogo global.
- Mediante el **proceso de replica,** la información que almacena es generada automáticamente en cada dominio.
- Se pueden definir varios controladores de dominio en un dominio, pero esto incrementará el tráfico de red para hacer las réplicas (para actualizar los distintos catálogos)

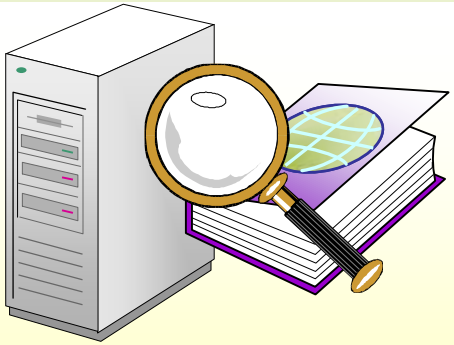
1. Catálogo global del DA. Ejemplo 1

Subconjunto de atributos de todos los objetos





Catálogo global

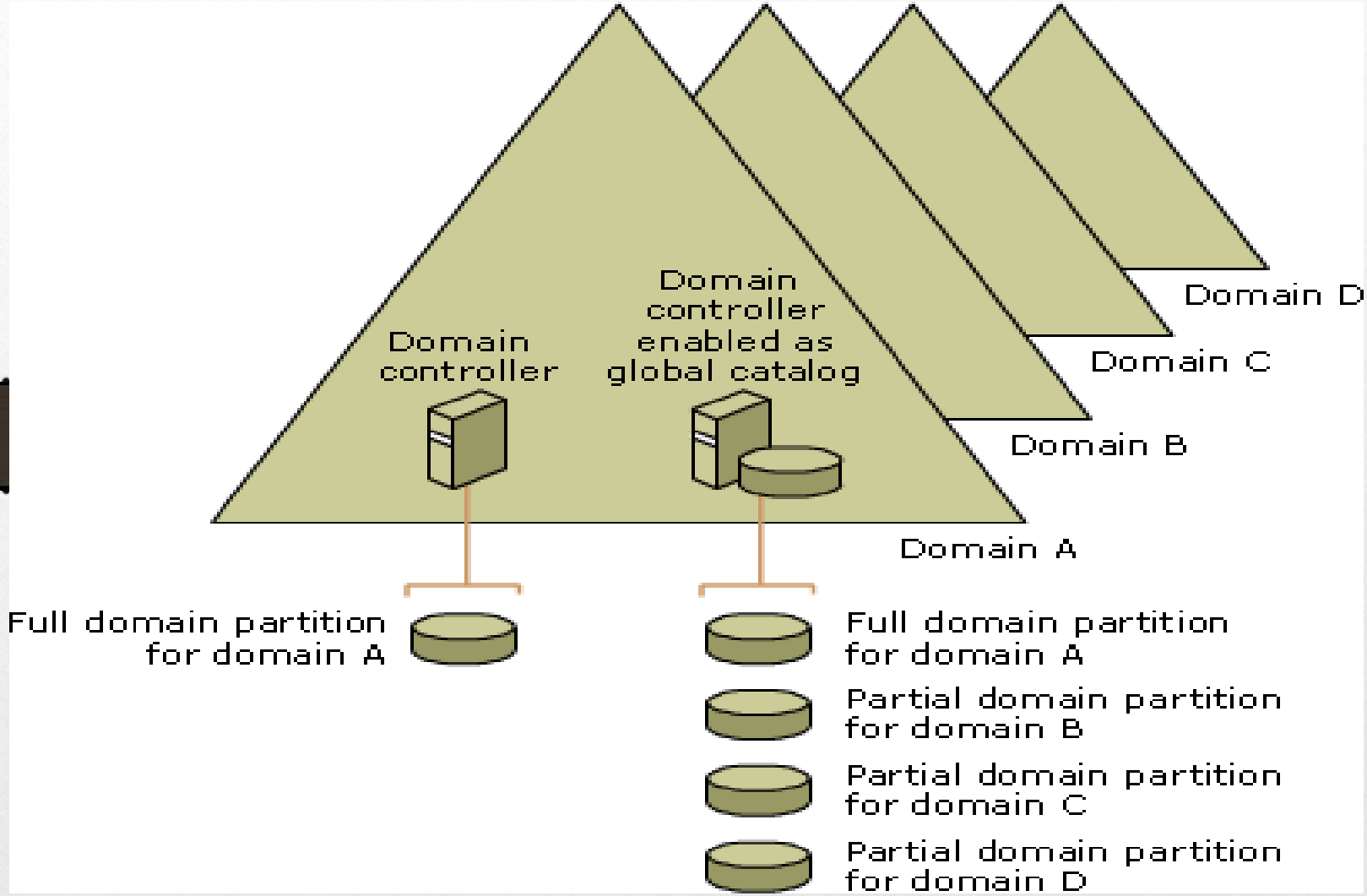


Servidor de catálogo global

Consultas

Pertenencia a grupos cuando el usuario inicia sesión

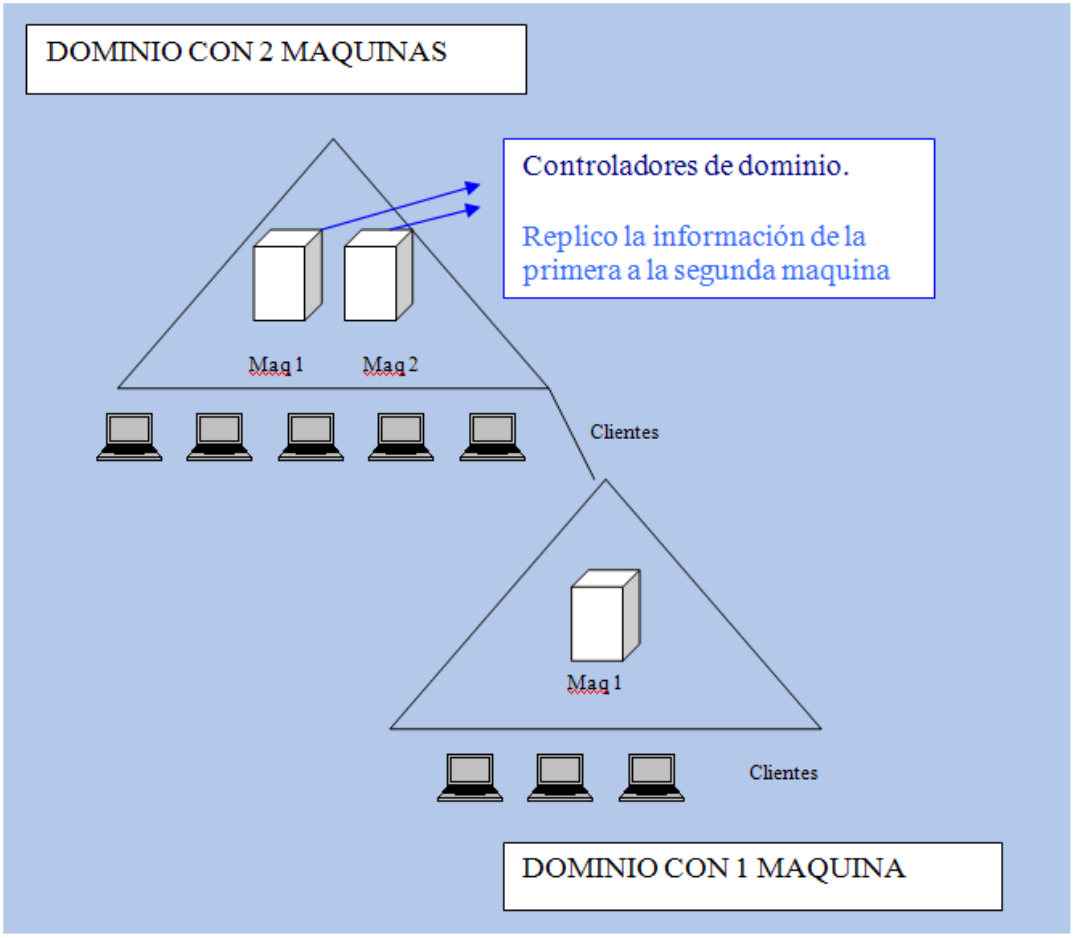
1. CATALOGO GLOBAL DA. Ejemplo 2



Por alusión: ¿Qué es una replica?

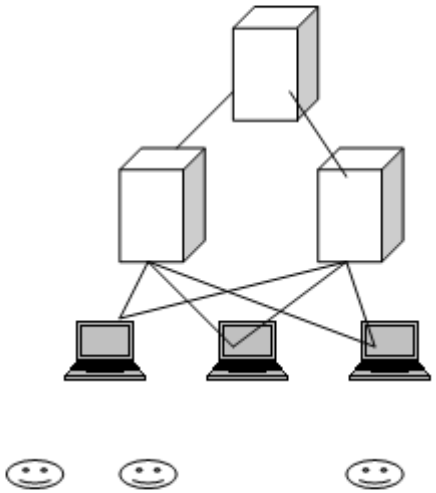
- Es una copia completa de los objetos que se encuentran en el servidor.

Ejemplo replicas



Antiguamente en NT

En NT tenemos PDC



Solo lectura

Maquinas

Usuarios

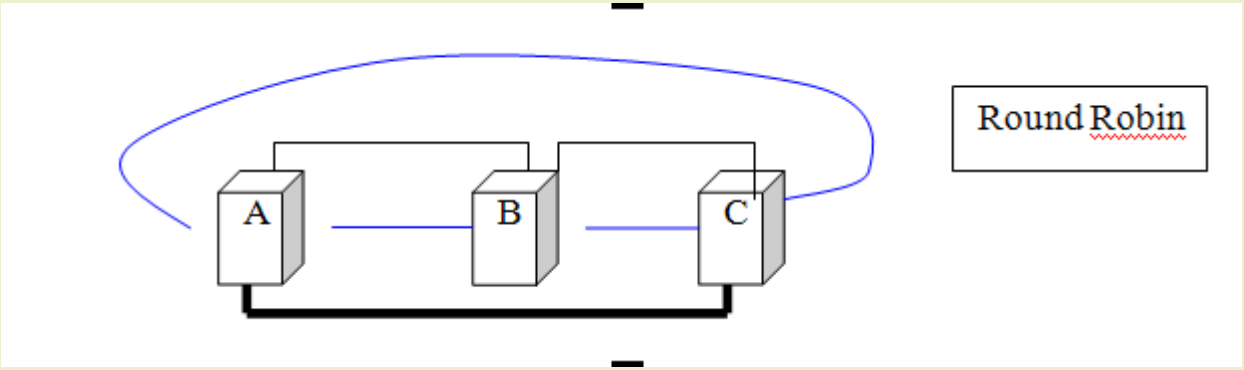
Si falla PDC (controlador de dominio primary) me quedo colgada por eso me crea BDC (controlador de dominio de backup) de solo lectura.

Replicas y validaciones entre servidores

- **En NT:**
  - Las validaciones se crean en el sistema y los que nuevos usuarios que quieren entrar al sistema ya no entran.
  - Esto también funciona en jerarquía pero en el caso que falle tengo que intercambiar PDC a BDC y eso supone un tiempo de lactancia.
- **En el Active Directory**
  - No existe Primary ni Backup de Primary. Todas las maquinas funcionan de lectura y escritura. Se replican constantemente y cualquiera de ellos me da la información.

Replicas y validaciones entre servidores

- ¿Quién me da esa información de cuantas maquinas me dan la información?
  - EL DNS
  - DNS le instalo en todas las maquinas, aunque solo sea obligatorio en la primera

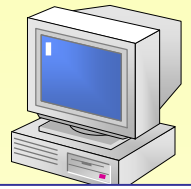


2. Esquema de Active Directory

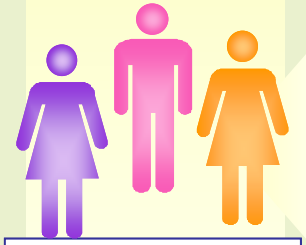
Objeto
Ejemplos de clase

Definidas en el contexto de nombres de esquema de Active Directory

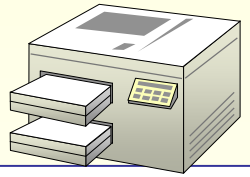
Almacenadas en el contexto de nombres de dominio de Active Directory



Equipos



Usuarios



Impresoras

Ejemplo
Atributos

Atributos de usuarios:

caducaCuenta
departamento
nombreCompleto
nombre

Ejemplo
Propiedades

Propiedades

10/02/03
Ventas
CN=Wendy Kahn,
OU=Beth

2. Esquema de Active Directory I

- Definición formal de todos los objetos Directorio Activo y sus atributos
- Cada tipo de objeto (clase) deriva de una clase principal TOP
  - Las clases heredan de otras clases su definición y comportamiento
- Cada objeto dispone de atributos obligatorios y atributos opcionales

2. Esquema de Active Directory II

- Símil con una tabla de BBDD Relacional
  - Clase => Definición en una fila de un objeto
  - Atributos => Columnas que definen una clase
- Cada **atributo** a su vez puede verse como una colección de posibles valores
- El **Esquema** se puede ver en la consola de Active Directory Schema
  - Se pueden ver/añadir/modificar clases y atributos por separado

2. Esquema de Active Directory III

Ejemplos de atributos
accountExpires department distinguishedName directReports dNSHostName operatingSystem repsFrom repsTo firstName lastName

3. Clases y atributos

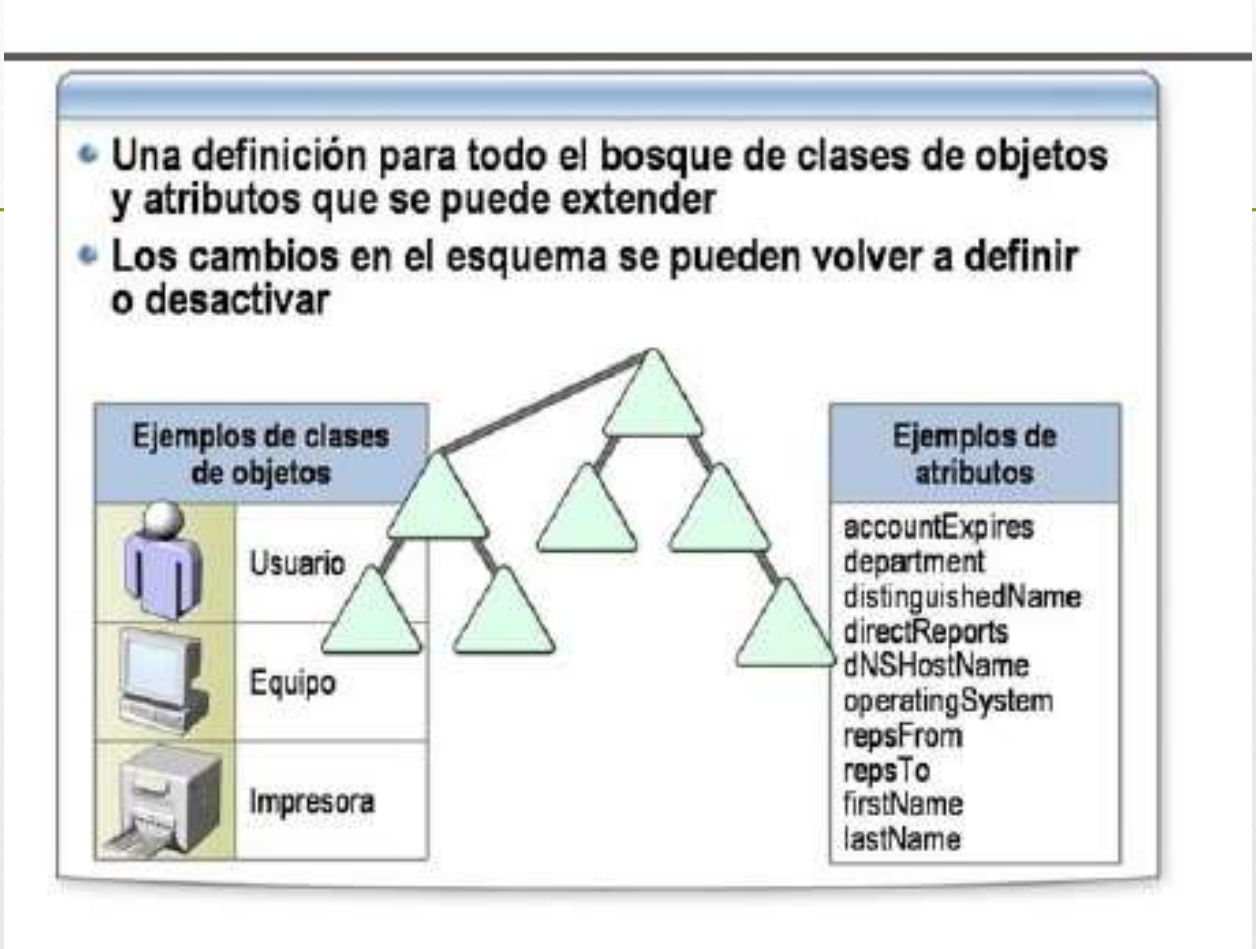
- **Clases** son los posibles objetos del directorio (usuarios, equipos …)

  Cada clase de objeto es un conjunto de atributos.

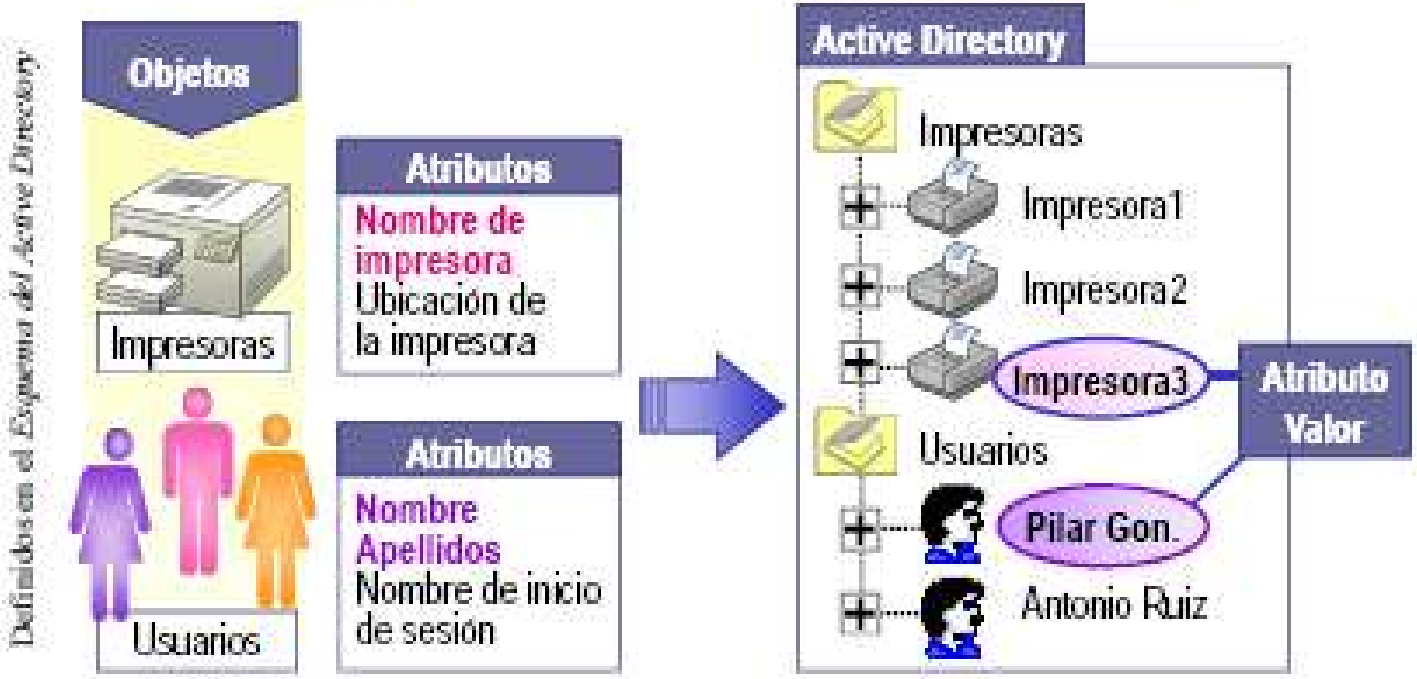
- **Atributos** nos define las diferentes cualidades de un objeto.

  Se definen una vez en el esquema y lo utilizan varios clases en el esquema,

EJEMPLO GRÁFICO

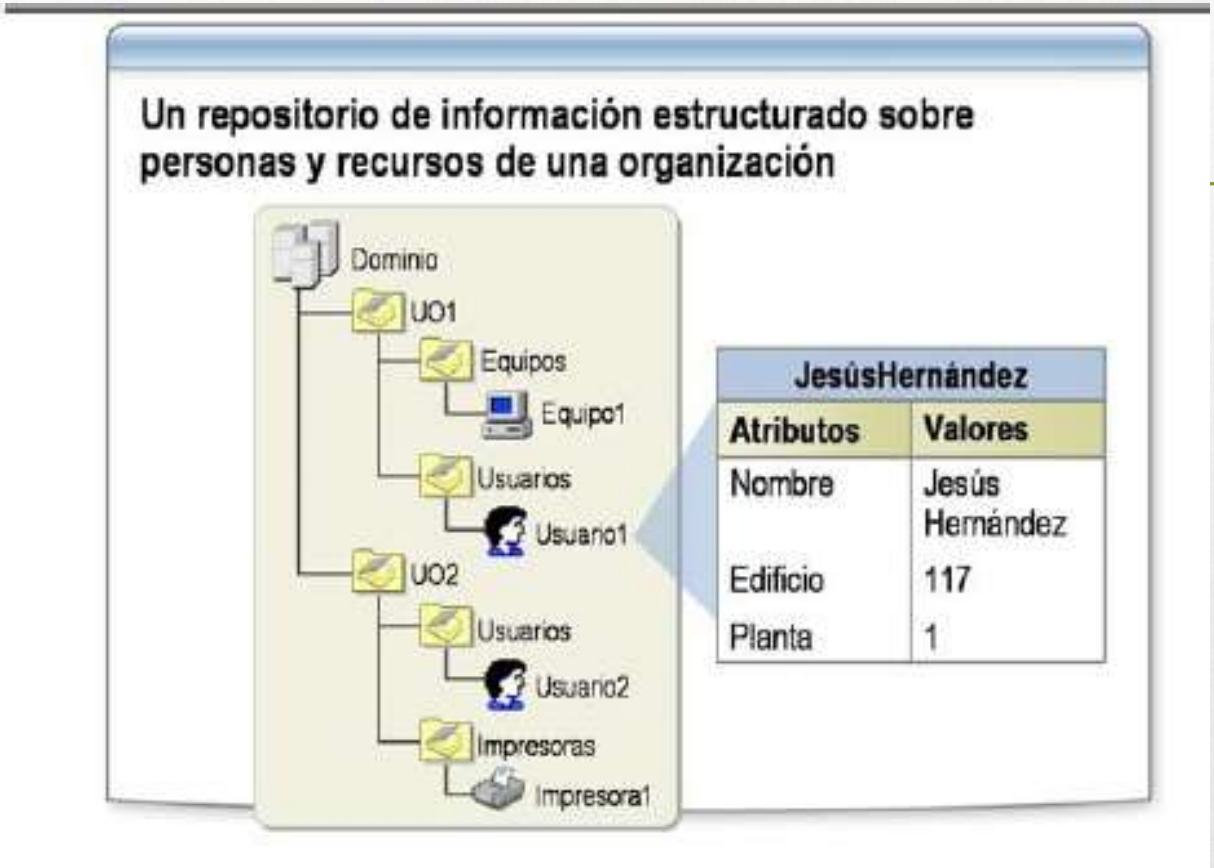


EJEMPLO GRÁFICO



- Los *objetos* representan los recursos de red
- Los *atributos* definen la información relativa a un objeto

COMPONENTES DEL DIRECTORIO ACTIVO

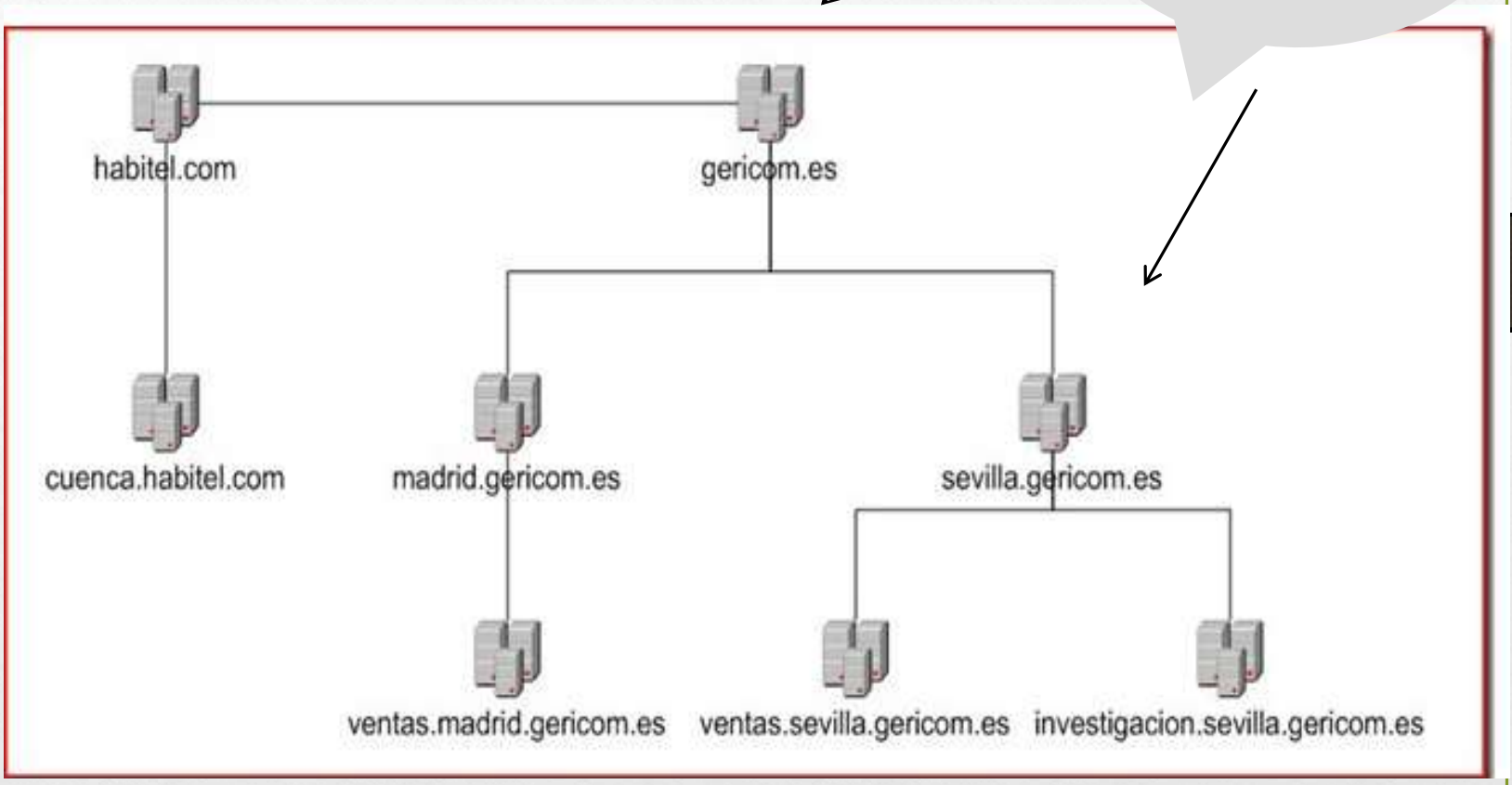


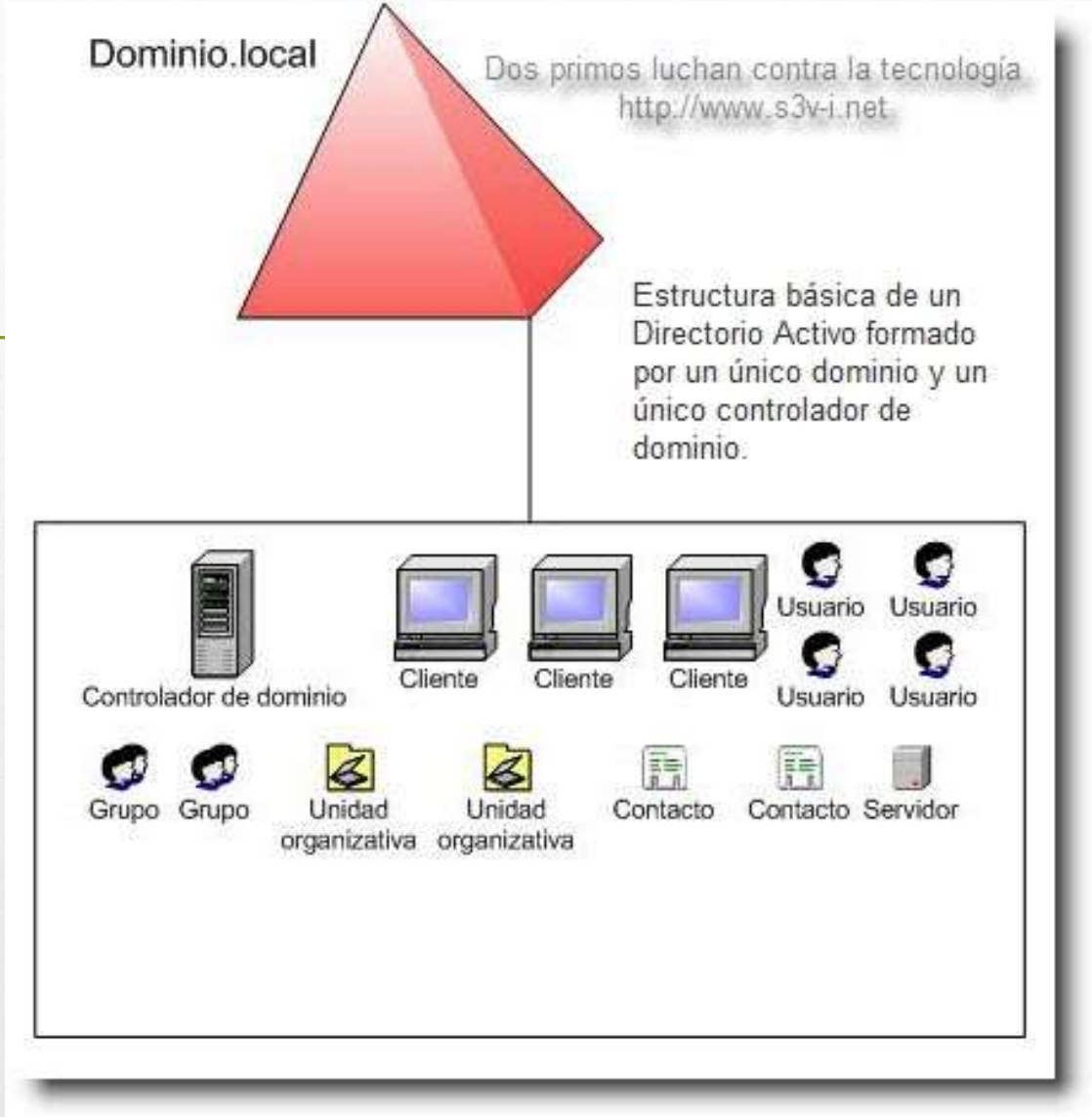
4. Dominio

- **Dominio**
  - Es la estructura fundamental de un Sistema operativo en red.
  - Permite agrupar y administrar todos los objetos que se administrarán de forma estructurada y jerárquica.
  - Cuenta con una BBDD de seguridad común.
  - Es más seguro que un grupo de trabajo.
  - Posibilita dividir redes extensas en redes parcialmente reducidas que simplifican el trabajo del administrador.

4. Dominio

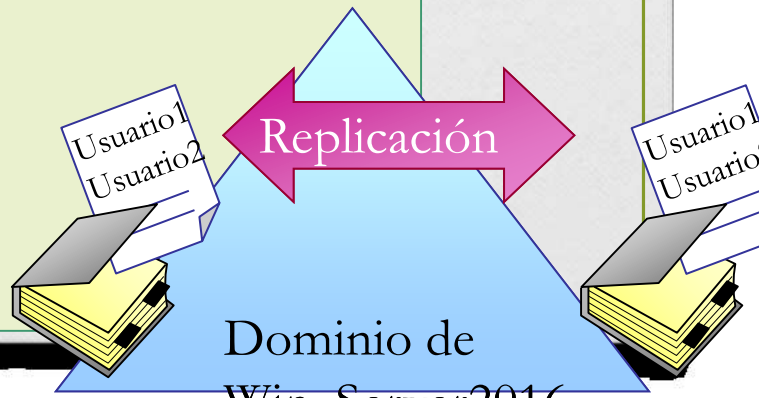
Cada uno de los nodos es un dominio




Dominio.local
Dos primos luchan contra la tecnología
http://www.s3v-i.net
Estructura básica de un Directorio Activo formado por un único dominio y un único controlador de dominio.
Controlador de dominio
Cliente
Cliente
Cliente
Usuario
Usuario
Usuario
Usuario
Grupo
Grupo
Unidad organizativa
Unidad organizativa
Contacto
Contacto
Servidor

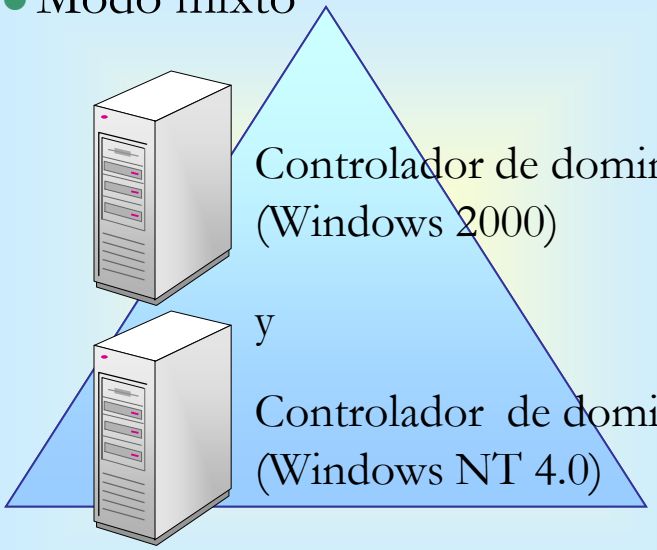
4. Dominios

- Un dominio es un **límite de seguridad**
- Un administrador de dominio sólo puede administrar dentro del dominio, a menos que se le concedan explícitamente derechos de administración en otros dominios
- Un dominio es una **unidad de replicación**
- Los controladores de un dominio participan en la replicación y contienen una copia completa de toda la información de directorio de su dominio



- Active Directory se instala en modo mixto para la compatibilidad con los controladores de dominio existentes
- El anidamiento de grupo y los grupos de seguridad universales requieren que un dominio esté en modo nativo

- Modo mixto

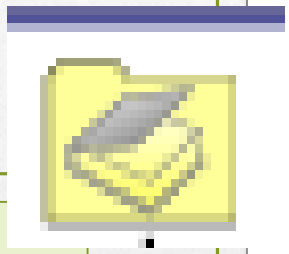


- Modo nativo

Por alusión:

- Unidad organizativa
- Usuarios
- Grupos

5. Unidad organizativa I



- Es el siguiente nivel de la jerarquía después del dominio.
- Son contendedores del DA, en que se puede colocar grupos, usuarios, equipos y otras unidades organizativas.
- Es la unidad más pequeña a la que se puede asignar derechos o a la que se puede delegar el control administrativo.

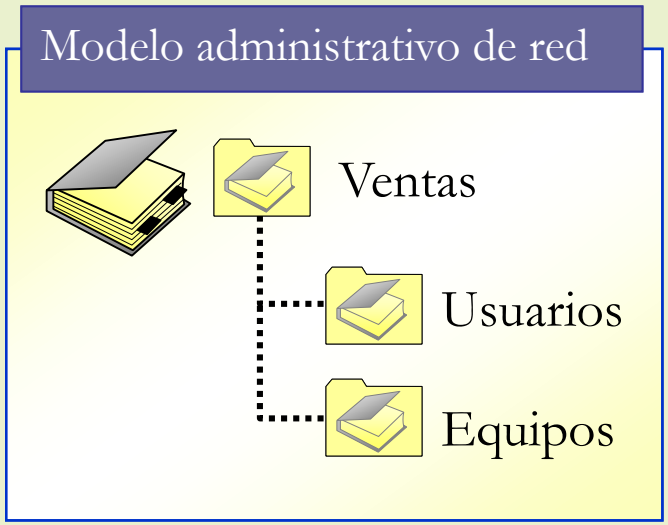
5. Unidad organizativa II

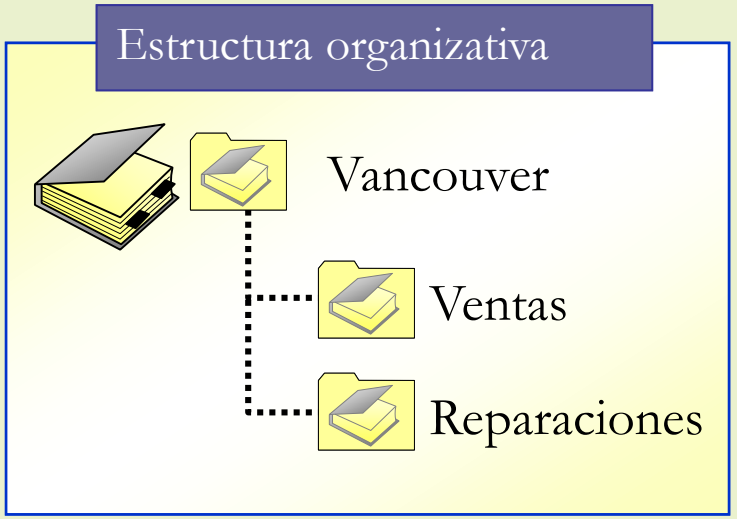
- Permite:
  - Organizar objetos en el dominio
  - Asignar estructuras jerárquicas distintas a distintos dominios
  - Delegar funciones administrativas
  - Aplicar directivas de grupos a ciertos usuarios y/o equipos del dominio

5. Unidades organizativas III

- Jerarquía de las OU
  - Según la función
  - Según la organización
  - Según la ubicación
  - Hibrida

5. Unidades organizativas





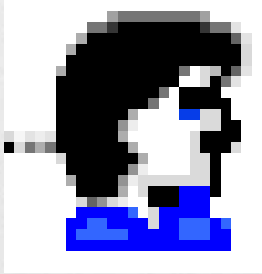
- Utilizar las unidades organizativas para agrupar objetos en la jerarquía lógica que mejor se adapte a las necesidades de su organización
- Delegar el control administrativo sobre los objetos que están dentro de una unidad organizativa asignando permisos específicos a usuarios y grupos

6. Grupos

- Conjunto de objetos del mismo tipo.
- Se utiliza principalmente para la asignación de derechos de acceso a los recursos.

7. Usuarios

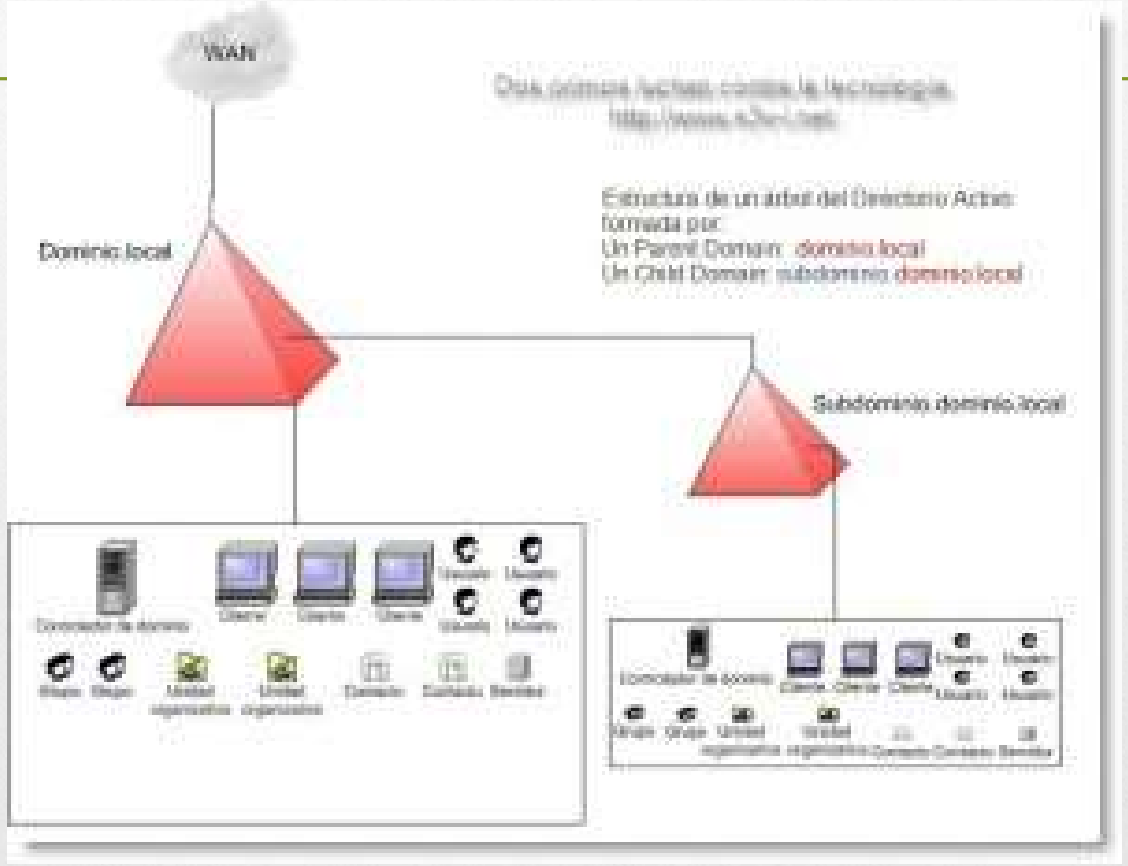
- Representación de los recursos de la red.
- Representa a las personas que usan la red



8. Árbol

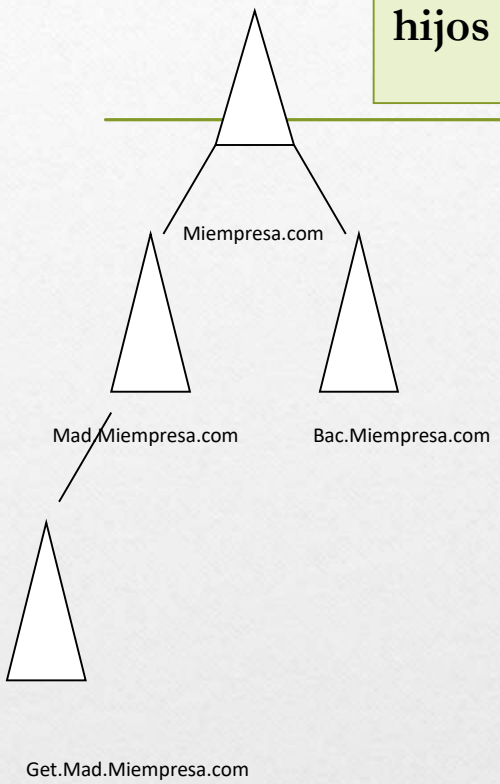
- Estructura jerárquica de dominios que comparten un espacio de nomenclatura continuo, un esquema común y catalogo global.
- Ejemplo:
  - Gericom.es
  - Madrid.gericom.es
  - Ventas.madrid.gericon.es

8. Árbol



8. Árbol

Creación de dominios hijos



- **Árbol:**
  - Es todo lo que cuelga de la misma raíz,
  - Es un conjunto de dominios con relaciones de confianza entre sí
  - Comparten recursos, clientes y *un sistema de resolución de nombres*.

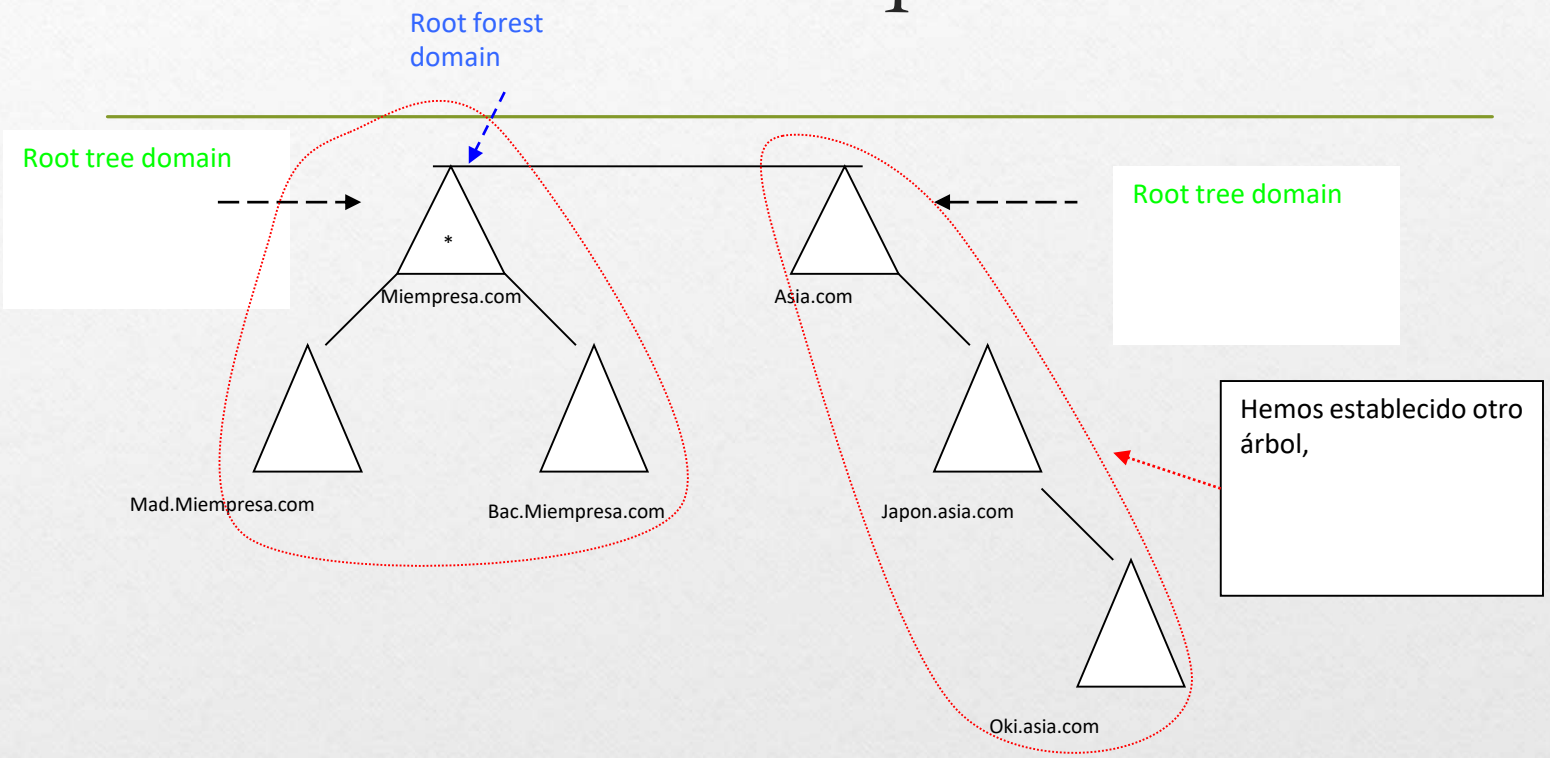
9. Bosque

- Es una colección de árboles de directorio que, que aunque *no comparten un espacio de nomenclatura contiguo, si un esquema común y un catalogo global.*
- Ejemplo:
  - Gericom.es
  - Habititi.es

9. Bosque

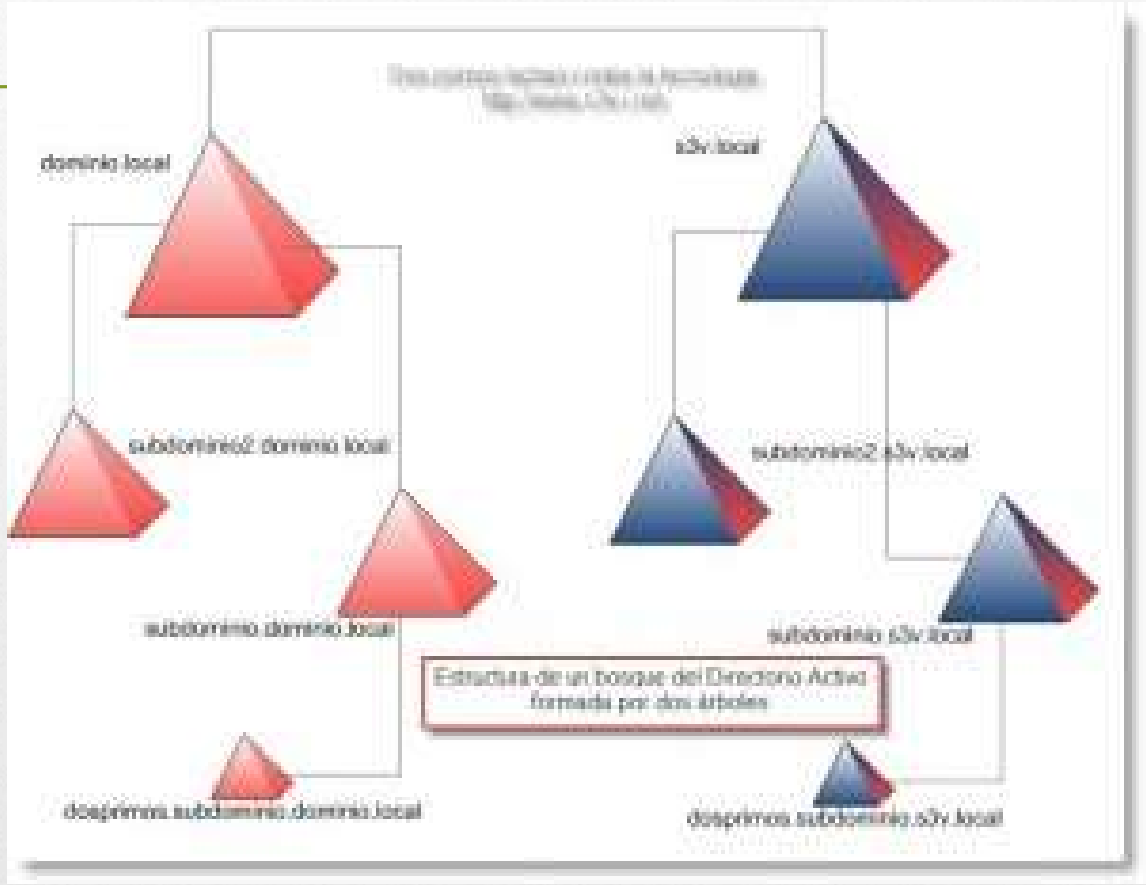
- Es un conjunto de árboles de dominio con relaciones de confianza entre sí.
  - Por ejemplo:
    - "*Miempresa.com*" es el dominio
    - "*Espania.Miempresa.com*" es el subdominio,
    - Podemos encontrar muchos subdominios dentro de un dominio, a eso se llama Árboles de Dominios.

9. Bosque



Al primer dominio montado dentro del bosque se conoce como "**ROOT FOREST DOMAIN",** es decir raíz del bosque

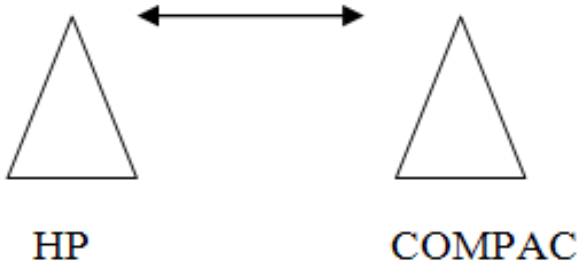
9. Bosque


dominio.local
s3v.local
subdominio2.dominio.local
subdominio2.s3v.local
subdominio.dominio.local
subdominio.s3v.local
Estructura de un bosque del Directorio Activo formada por dos árboles
dosprimos.subdominio.dominio.local
dosprimos.subdominio.s3v.local

9. Bosque

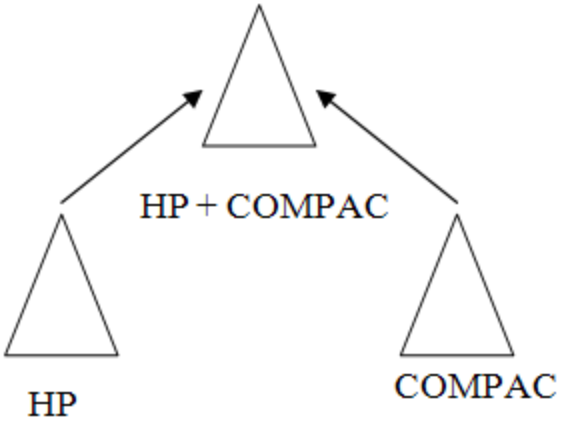
- Root Forest Domain (Raiz del bosque)
  - Es el dominio más importante
  - Tiene estas características:
    - Grupos que van a poder gestionar cualquier recurso que este en mi dominio, en mi forest (bosque).
      - El administrador de la empresa (Enterprise Administrador) llamado "admin."
      - El administrador del esquema (Schema Administrador)
      - El resto de administradores solamente cada nodo del dominio (cada triangulito)

9. Bosque. Ejemplo I



Es una función no real con 2 administradores

Para que sea real debemos migrar a un tercer nodo.



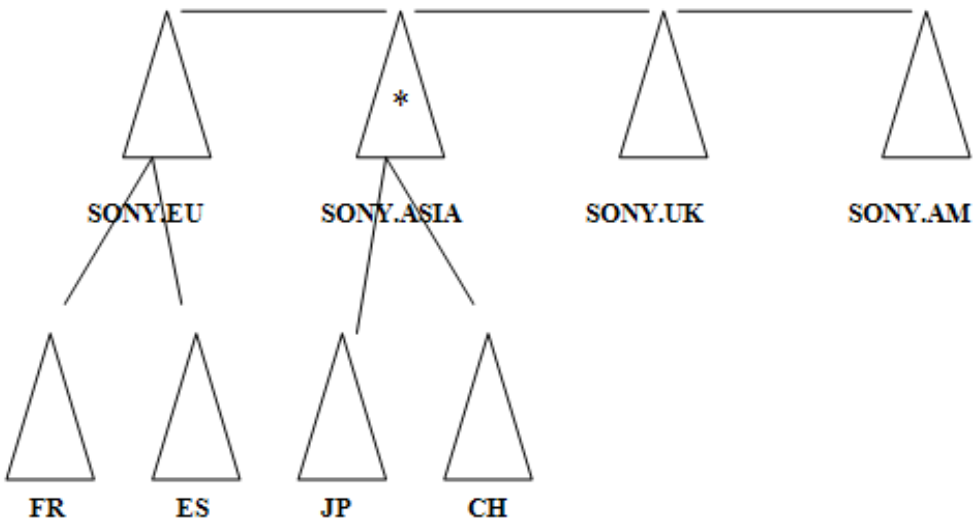
Sino migramos sólo será relaciones de confianza como en NT

9. Bosque. Ejemplo 2

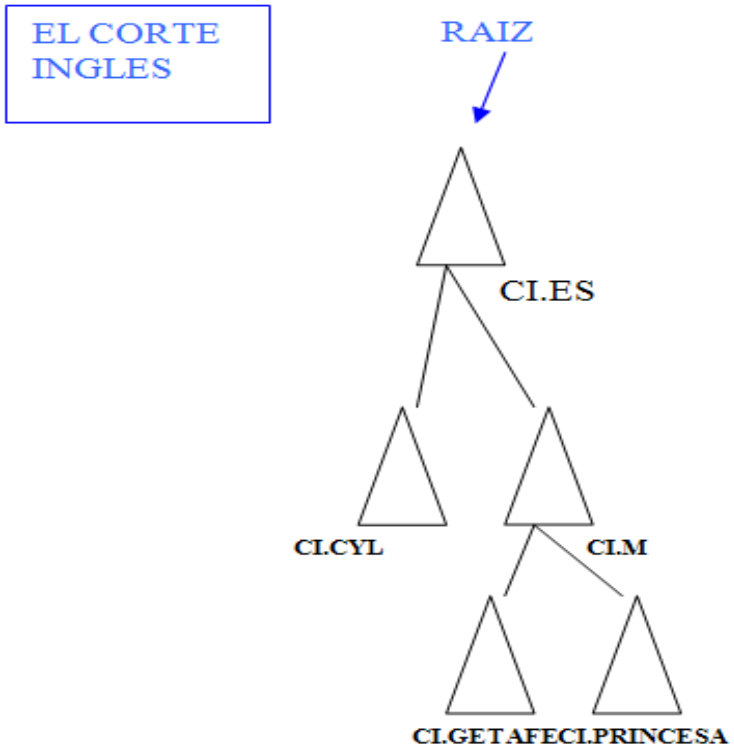
CASOS REALES

SONY

Primer dominio que se monto
ROOT TREE DOMAIN "admin."



Bosque. Ejemplo 3



Recomendaciones para dividir en dominios o en UO (I)

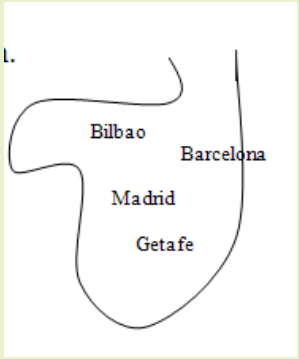
- Organización descentralizada (varios administradores administran distintos usuarios y recursos)
- Si dos partes de la red están separadas por un vinculo lento (replica completa es complicada llevarla a cabo)

Recomendaciones para dividir en dominios o en UO (II)

- Si es necesario reflejar en el dominio la estructura de la organización (OU)
- Delegar el control de los administrativos en pequeños conjuntos de usuarios, grupos, recursos (OU)
- Si la estructura puede sufrir modificaciones en el futuro (OU)

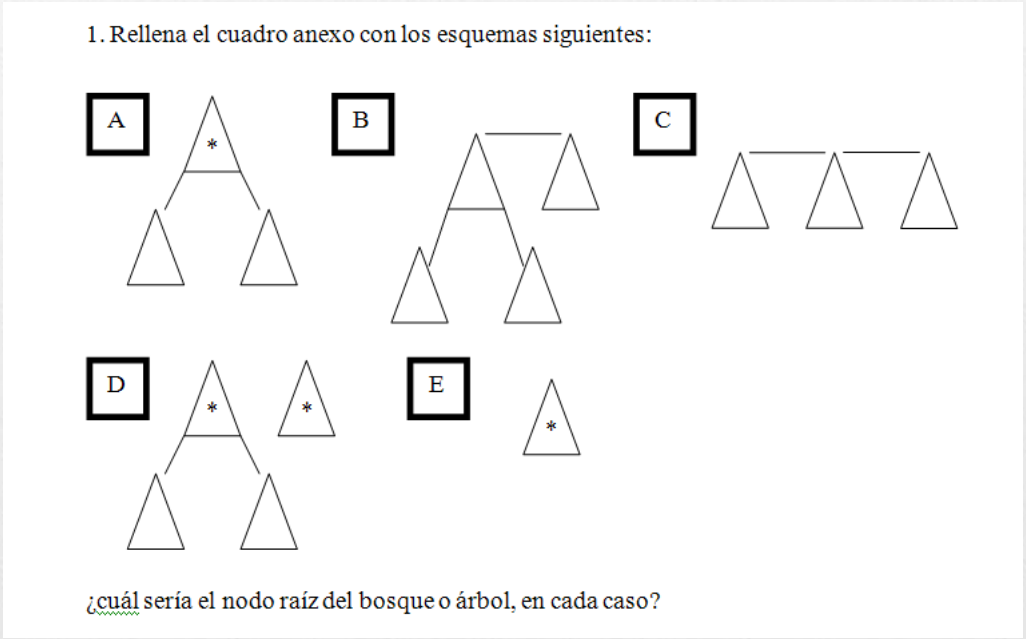
¿Cuántos Controladores de dominio instalo en mi empresa?

- Difícil respuesta
- Depende principalmente del ancho de banda y del numero de clientes de cada localidad física.
  - Ejemplo:
    - Tengo en Bilbao 10 personas, en Barcelona 500 personas, en Madrid 500 personas y en Getafe 500 personas.
    - Sabemos que cuanto mas DC mas trafico tengo en replicación.
      - Barcelona
      - Bilbao
- ¿Dónde los creo?
  - No hay respuesta.
    - - Si considero clientes en Barcelona, Madrid y Getafe, Madrid
    - - Por importancia Bilbao



Ejercicio

- Realiza las actividades del libro desde la página 292 a la página 299 y añádelas a tu blog.



Solución 1

Casos A) y E) admin.
Casos B) y C) Primero creado
Caso D) admin1 y admin2

	DOMINIOS	ARBOLES	BOSQUES
A)	3	1	1
B)	4	2	1
C)	3	3	1
D)	4	2	2
E)	1	1	1

La tendencia actual es llevarlo hacia el caso E), por ser lo más sencillo. Por ejemplo "El corte ingles".

Un dominio puede tener x maquinas a una sola pero es importante que cada dominio tiene un único controlador de dominio.
1 maquina implica 1 dominio y 1 dominio implica varias maquinas.

Relaciones de confianza

- Unidireccional
- Bidireccional
- Transitiva
- Intrasitiva

Concepto: Unidireccional (Diagrama)

Concepto: Unidireccional I

- Si existe una confianza unidireccional creada entre dos dominios A y B, los usuarios del dominio A pueden tener acceso a los recursos de B pero los usuarios del dominio B no pueden tener acceso a los recursos del dominio A.
- Estas pueden ser transitivas o intransitivas

Concepto: Unidireccional II

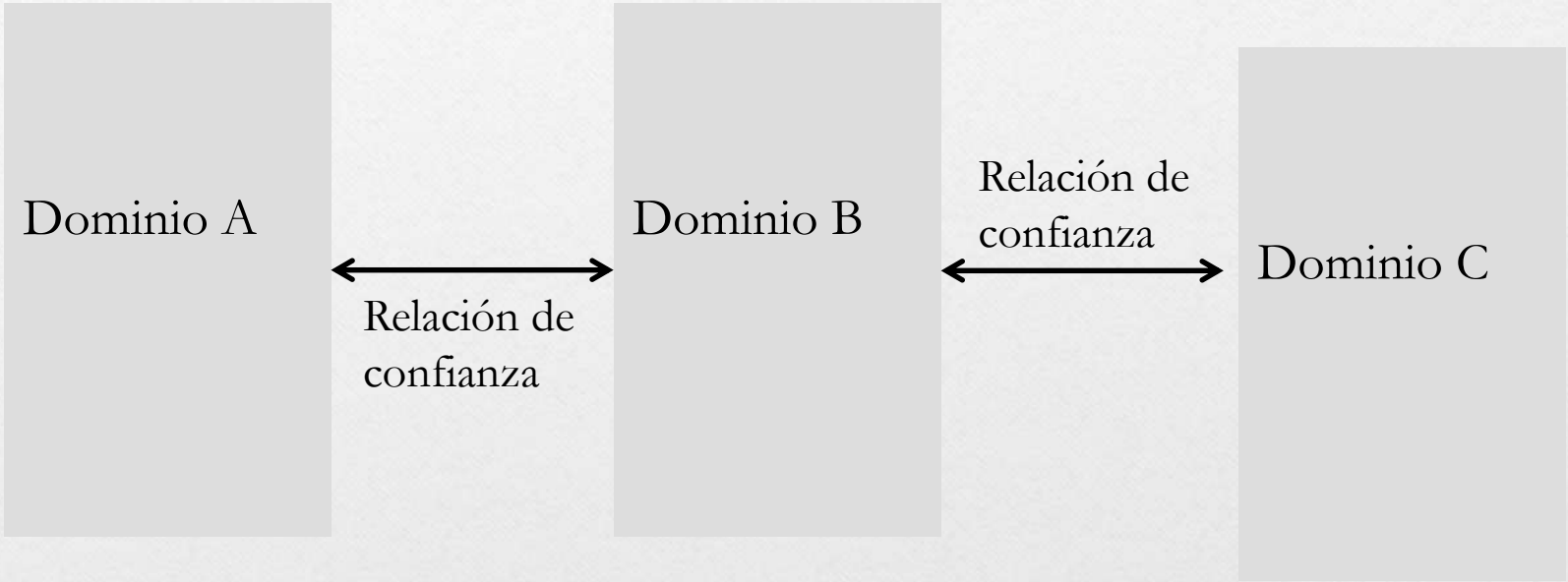
- Se da confianza unidireccional:
  - Entre bosques diferentes
  - Con dominios de Windows NT4.0
  - Territorios Kerberos v5

Concepto: Bidireccional (Diagrama)

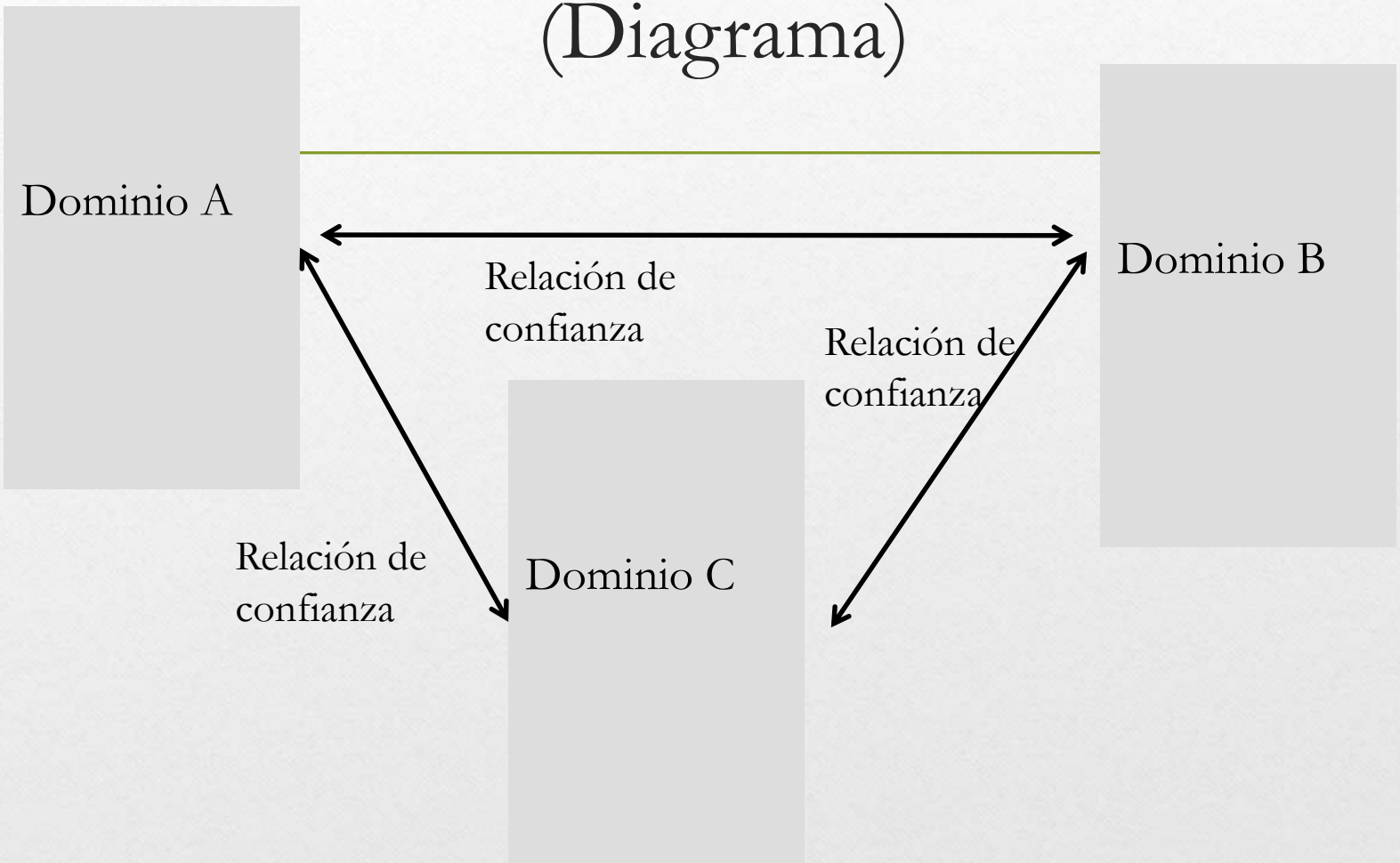
Concepto: Bidireccional

- Si existe una confianza bidireccional creada entre dos dominios A y B, los usuarios del dominio A pueden tener acceso a los recursos de B y los usuarios del dominio B a los recursos del dominio A

Concepto: No transitiva (Diagrama)



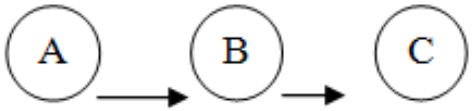
Concepto: Transitiva (Diagrama)



Concepto: Transitiva

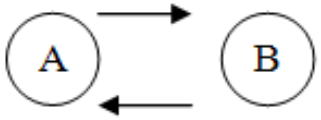
- Si un dominio A tiene una confianza transitiva con el dominio B y este la tiene con el C, el dominio A tiene una relación de confianza con el dominio C
- La confianza se transmite de abajo arriba hacia la raíz.
- Y de una raíz de un árbol a otro dentro del mismo bosque.

Un dominio no ve a otro pero puede darle permisos para hacer ciertas cosas.



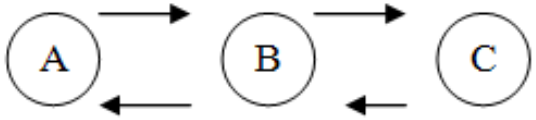
Los usuarios del dominio B pueden trabajar en A.

Ejemplo lenguaje común: Un vecino se va de vacaciones y le da las llaves al otro. Luego el vecino que me da las llaves confía en mi. B confía en A



Confianza mutua
y sentido bidireccional

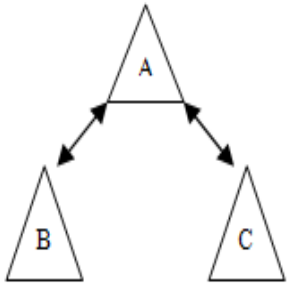
Ejemplo:



NO es transitiva
La confianza se la doy a B pero no a C

Relaciones de confianza

- **Directorio activo existe una jerarquía**



Son bidireccional y transitivas

Y no se pueden cambiar

Esta forma de relación, me permite conocer al vecino, aunque otra cosa es que tenga credenciales para entrar en la casa del vecino.

Características principales (I) **(Dominios)**

- Al crear un dominio nuevo en un árbol que ya existe, las relaciones de confianza que se establecen de forma automática son transitivas y bidireccionales con los demás dominios
- Por defecto, los dominios de un mismo bosque están vinculados con relaciones de confianza transitivas y bidireccionales.

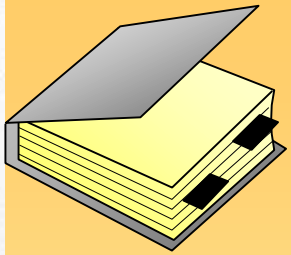
Características principales (II)

- Entre bosques distintos las relaciones de confianza son establecidas de forma manual, y suelen ser unidireccional e intransitiva

Características principales (III)

- Una modificación que se realice en el directorio de cualquier servidor se replica automáticamente a los restantes servidores del dominio
- Cualquier cambio en los derechos de acceso se propaga automáticamente a todos los niveles inferiores.
- La administración de privilegios es flexible, porque permite dar derechos de administración sobre un conjunto determinado de objetos en lugar de sobre la totalidad.

Bosque, arboles (confianzas transitivas bidireccionales)
Ejemplo gráfico



Relación de confianza transitiva bidireccional

(raíz)

contoso.msft

Bosque

Árbol

asia.
contoso.msft

au.
contoso.msft

nwtraders.msft

Árbol

asia.
nwtraders.msft

au.
nwtraders.msft

Relaciones de confianza transitivas bidireccionales

Definición: Confianzas explicitas entre dominios

- Son relaciones de confianza que crean los propios usuarios en lugar de crearse automáticamente durante la instalación de un controlador de dominio.
- Para crear una confianza de este tipo, se debe conocer:
  - Los nombre de los dominios
  - Una cuenta de usuario con permisos para crear confianzas en cada dominio.
  - La contraseña debes ser conocida por el administrador de ambos dominios de la relación

Clases de confianza explicitas (I)

- **Confianza externa:**

  Permite acceder a recursos ubicados:

  - En un dominio de Windows NT
  - En un dominio ubicado en un bosque separado y no unido por una relación de confianza de bosque.

- **Confianza de territorio Kerberos**:

  Permite establecer relaciones de confianza en territorios Kerberos que no es de Windows.

  (Entornos o seguros)

Clases de confianza explicitas (II)

- **Confianza bosque**

  Permite compartir recursos entre distintos bosques

- **Confianza de acceso directo o abreviada:**

  Permite acorta la ruta de una confianza en un bosque complejo

Establecer relaciones confianza con W2K16 (II)

- *Inicio* + *Administración del servidor* + Herramientas + *Dominios y confianza de AD*

- *Más información: https://www.youtube.com/watch?v=RTL7ESp0Bpo*

  (video basado en Windows 2008)

NOTA: Se verá un ejemplo a final de curso si da tiempo, de momento sólo me interesa el concepto para que tengáis una visión general.

Se verá en 2 ASIR