

# *Implantación de Sistemas operativos*

---

## UT4

Administración y  
acceso a dominios  
Usuarios, Grupos y  
Permisos



# Usuario

---

- es un objeto, que consiste en toda la información que define al usuario en Windows Server.
- Consta de:
  - ▶ un nombre de cuenta (**username**)
  - ▶ de la contraseña (**password**) necesarios para iniciar sesión,
  - ▶ de los grupos a los que pertenece dicho usuario
  - ▶ de los derechos, privilegios y permisos que tiene para acceder al equipo, la red y los recursos.

# Usuarios

---

- Cuentas integradas, que se crean automáticamente al crear el dominio.
  - ▶ Administrador
  - ▶ Invitado (deshabilitada)



# Tipos de usuarios

---

- Usuario Local
- Usuario del Dominio.



# Tipos de usuarios I

## ● Usuario local

- ▶ Estas cuentas permiten a los usuarios iniciar una sesión y acceder a los recursos solamente en la computadora donde se crea la cuenta de usuario local



# Tipos de usuarios I

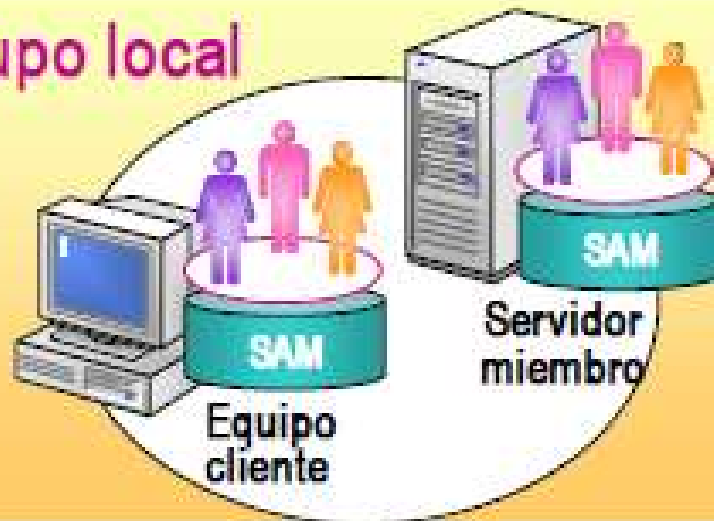
## ● Usuario dominio

- ▶ Estas cuentas permiten a los usuarios iniciar una sesión en el dominio y acceder a los recursos en cualquier parte de la red.
- ▶ El usuario proporciona su contraseña y nombre de usuario durante el proceso de inicio.
- ▶ AD una vez comprobado los datos ingresados se le concede el acceso a la red.



# RESUMEN GRAFICO

## Grupo local



- Creados en equipos que no son controladores de dominio
- Residen en SAM
- Se utilizan para controlar el acceso a recursos del equipo

## Dominio



- Creados en controladores de dominio
- Residen en Active Directory
- Se utilizan para controlar los recursos del dominio

# CUENTAS DE GRUPO

---


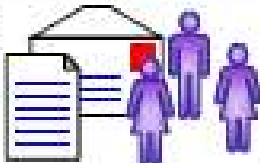
**Los grupos** son contenedores de usuarios que tienen los mismos derechos y permisos y nos facilitan la administración de los sistemas informáticos.



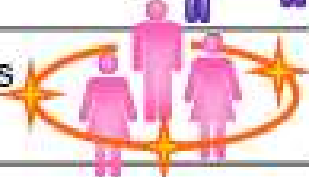
Normalmente es recomendable no asignar permisos a usuarios individuales, sino agregar estos usuarios como miembros de un grupo, y asignar permisos





# Tipos y ámbitos de los grupos de dominio

Tipos de grupo	
Grupos de seguridad	<p>Se usan para asignar permisos</p> <p>Se pueden usar como listas de distribución de correo electrónico</p> 
Grupos de distribución	<p>No se puede utilizar para asignar permisos</p> <p>Se pueden usar como listas de distribución de correo electrónico</p> 

Ámbitos de grupo de seguridad	
Grupo global	<p>Se utiliza para organizar usuarios con necesidades similares de acceso a la red</p> 
Grupo local de dominio	<p>Se usa para asignar permisos a recursos de dominios</p> 
Grupo universal	<p>Se utiliza para asignar permisos a recursos relacionados en varios dominios</p> 

# Tipos de Grupo:

---

1. Grupo de Distribución
2. Grupo de Seguridad



## ✓ Grupos de Distribución:

---

- Se utiliza sólo con aplicaciones de correo electrónico
- No está habilitado para seguridad



## ✓ Grupos de Seguridad:

---

- Se utiliza para asignar derechos y permisos a los grupos de usuarios y equipos
- Se utiliza de forma más eficaz cuando está anidado



# Ámbitos de Grupo:

---

1. Global
2. Local dominio
3. Universal



# Ámbito global

---



## ✓ Grupo de ámbito Global

---

- Es un grupo de seguridad o distribución que puede contener:
  - usuarios,
  - equipo y
  - grupos globales de su propio dominio.
  
- Puede conceder derechos y permisos a los grupos de seguridad global para los recursos de cualquier dominio del bosque.

# Ámbito dominio local

---





## ✓ Grupo de ámbito de Dominio Local

---

➤ Es un grupo de seguridad o distribución que puede contener\_

- grupos universales,
- grupos globales,
- otros grupos locales de dominio de su propio dominio y
- cuentas de cualquier dominio del bosque.

➤ En los grupos de seguridad local, solamente puede otorgar derechos y permisos sobre los recursos que residen en el dominio en el que está ubicado el grupo local de dominio.

---

# Ámbito universal

---



# ✓ Grupo de ámbito Universal

---

- Un grupo universal es un grupo de seguridad o distribución que puede contener:
  - usuarios,
  - equipos,
  - grupos universales y
  - grupos globales de cualquier dominio del bosque.
- Se pueden conceder derechos y permisos a los grupos de seguridad universales sobre los recursos de cualquier dominio del bosque

# INTEGRANTES DE LOS GRUPOS

---

Mientras que el ámbito de los grupos es independiente del nivel funcional de dominio (que establece la compatibilidad de Windows Server), la membresía de los grupos depende directamente de dicho nivel funcional.

Así, dependiendo del nivel funcional de nuestro dominio podremos o no introducir miembros determinados dentro de cada tipo de grupo.

---

**EN DETALLE:**



# Grupo Global



Pueden contener, además, otros grupos globales del mismo dominio. Son visibles en todos los dominios del bosque, y suelen utilizarse para clasificar a los usuarios en función de las labores que realizan.

## Reglas de grupos globales

### Miembros

Cuentas de usuarios, cuentas de equipos, grupos globales del mismo dominio.

### Pueden ser miembros de

Universal y grupos locales de dominio en todos los grupos de dominio y globales del mismo dominio.

### Permisos

Todos los dominios del bosque y dominios de confianza.



# Grupo Local Dominio



Pueden contener, además, grupos universales y otros grupos locales del dominio. Sólo son visibles en el dominio en que se crean, y suelen utilizarse para conceder permisos y derechos en cualquiera de los ordenadores del dominio.

## Reglas de grupos locales del dominio

### Miembros

Cuentas de usuarios, cuentas de equipos, grupos globales y grupos universales de cualquier dominio del bosque y grupos locales de dominio del mismo dominio.

### Pueden ser miembros de

Grupos locales de dominio del mismo dominio.

### Permisos

Dominio al que pertenece el grupo local de dominio.



# Grupo Universal



Pueden contener cuentas de usuario y grupos globales, así como otros grupos universales, de cualquier dominio del bosque. Son visibles en todo el bosque.

## Reglas de grupo universal

### Miembros

Cuentas de usuarios, cuentas de equipos, grupos globales y otros grupos universales de cualquier dominio del bosque.

### Pueden ser miembros de

Grupos locales de dominio y universales de cualquier dominio.

### Permisos

Todos los dominios de un bosque.



## Ejemplo:

### CUANDO UTILIZAR CADA TIPO DE GRUPO I

---

Los grupos con ámbito local de dominio nos ayudan a definir y administrar el acceso a los recursos en un solo dominio.

Por ejemplo,

Para conceder a 5 usuarios acceso a una impresora determinada, podemos agregar las cinco cuentas de usuario a la lista de permisos de la impresora.

Sin embargo, si más tarde deseamos dar a esos 5 usuarios acceso a una nueva impresora, debemos especificar nuevamente las 5 cuentas en la lista de permisos de la nueva impresora.

## CUANDO UTILIZAR CADA TIPO DE GRUPO II

---

Si planeamos antes **los grupos**, podemos simplificar esta tarea administrativa rutinaria.

Para hacerlo, deberemos crear **un grupo de seguridad con ámbito local de dominio** y asignarle los permisos necesarios para tener acceso a la impresora.

Ahora añadimos a los 5 usuarios como miembros del nuevo grupo con lo cual podrán acceder a la impresora.

## CUANDO UTILIZAR CADA TIPO DE GRUPO III

---

Si ahora deseamos dar a esos 5 usuarios acceso a una nueva impresora, basta con añadir a la lista de permisos de esa impresora el grupo local anteriormente creado **(1 operación)** y no añadir manualmente a los 5 usuarios **(5 operaciones)**.

## CUANDO UTILIZAR CADA TIPO DE GRUPO IV

---

Además, si queremos que un usuario deje de poder usar las impresoras, bastará con sacar a dicho usuario del grupo, con lo que habremos conseguido que no pueda usar dichos recursos. Si no usamos grupos, no nos quedaría más remedio que ir impresora por impresora e ir quitándole los permisos al usuario por cada una de ellas.

# CUANDO UTILIZAR CADA TIPO DE GRUPO V

---

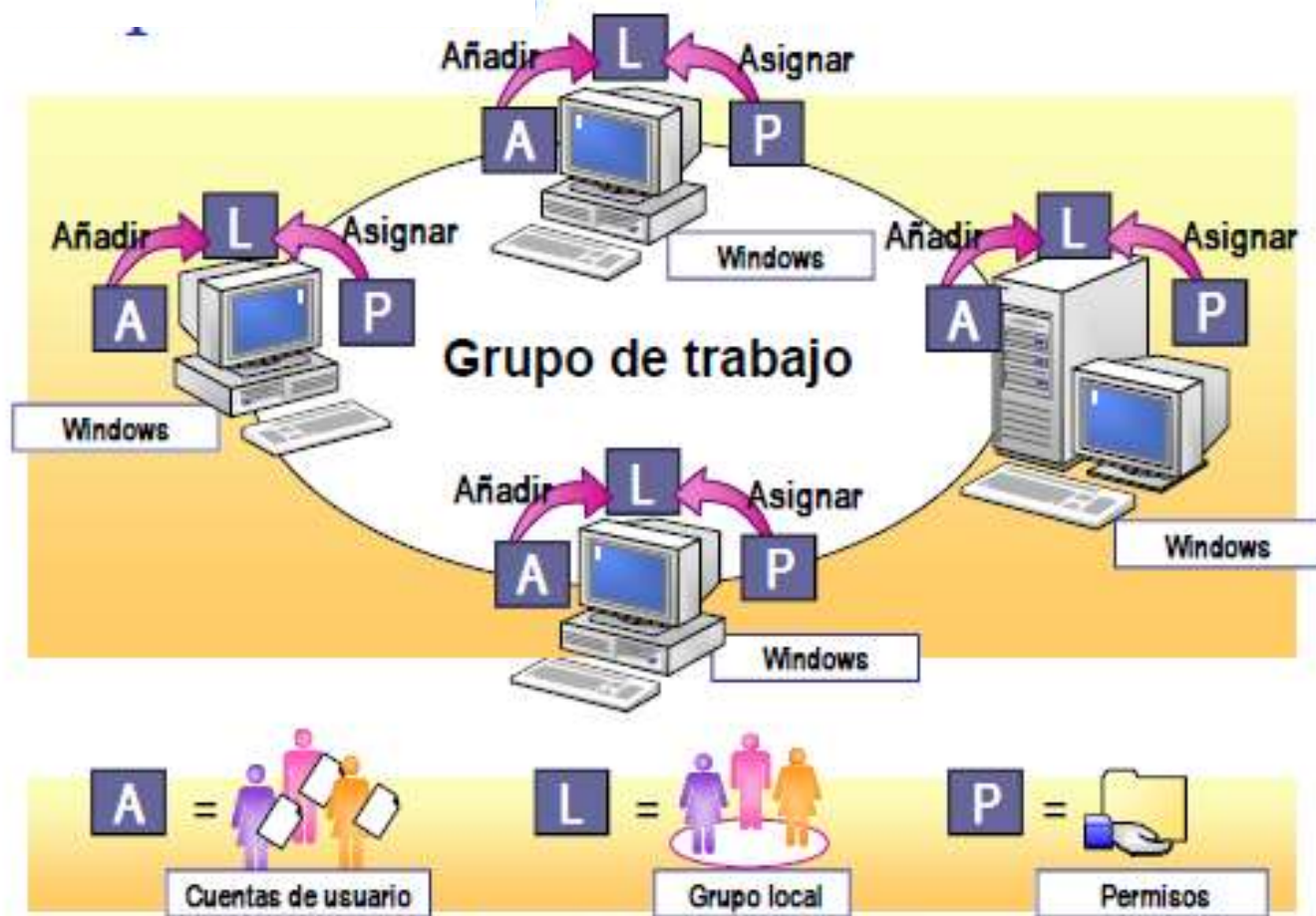
Pero, ¿y si de necesitamos que estos 5 usuarios impriman en una impresora situada en otro dominio del bosque?

Para ello, en lugar de añadir los usuarios a un grupo local de dominio, lo conveniente es colocar las cinco cuentas de usuario en un **grupo con ámbito global y agregar este grupo global como miembro del grupo local de dominio** que da permisos sobre las impresoras. De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque.

.

# Concesión de permisos

## Estrategias



Tema 14. Cuentas de grupo, equipo y usuario

23

# Estrategia 1: A DL P

---

- **Usuario-Grupo Local de Dominio-Permisos**

- ▶ Tenemos las cuentas de Usuario y las incluimos en Grupos Locales de dominio y a los Grupos locales les asignamos los permisos
- ▶ Esta estrategia es buena cuando la usemos en un bosque con un solo dominio y no se agregarán otros dominios al bosque, lo cual nos puede delimitar en un futuro si existen dominios de confianza u otros dominios dentro del bosque, **ya que no podremos asignar permisos a los grupos locales si los recursos están fuera del dominio** donde se encuentra el Grupo Local de Dominio.
- ▶ Problema: El administrador no puede administrar otros dominio

# Estrategia 2 : A G P

---

- **Usuario – Grupo local – Permisos**

- ▶ Tenemos las cuentas de Usuario y las incluimos en Grupos Globales, a los Grupos asignamos los permisos.
- ▶ Esta estrategia es buena cuando tenemos un bosque conformado tan sólo por un Dominio, ya que si se usan varios dominios tendremos complicaciones en la administración, si varios Grupos Globales necesitan los mismos permisos.
- ▶ Problema: La administración cuando entra más dominios es complicada, **porque todos los grupos requieren los mismos permisos y cada administrador debe asignar dichos permisos de forma individual**
- ▶ Recordemos que los grupos globales asignan derechos en todo el bosque y por tanto **pueden existir permisos contradictorios** si tenemos un bosque con más de un dominio



# Estrategia 3: A G DL P

---

- **Usuario-Grupo Global-Grupo Local de Dominio- Permisos**

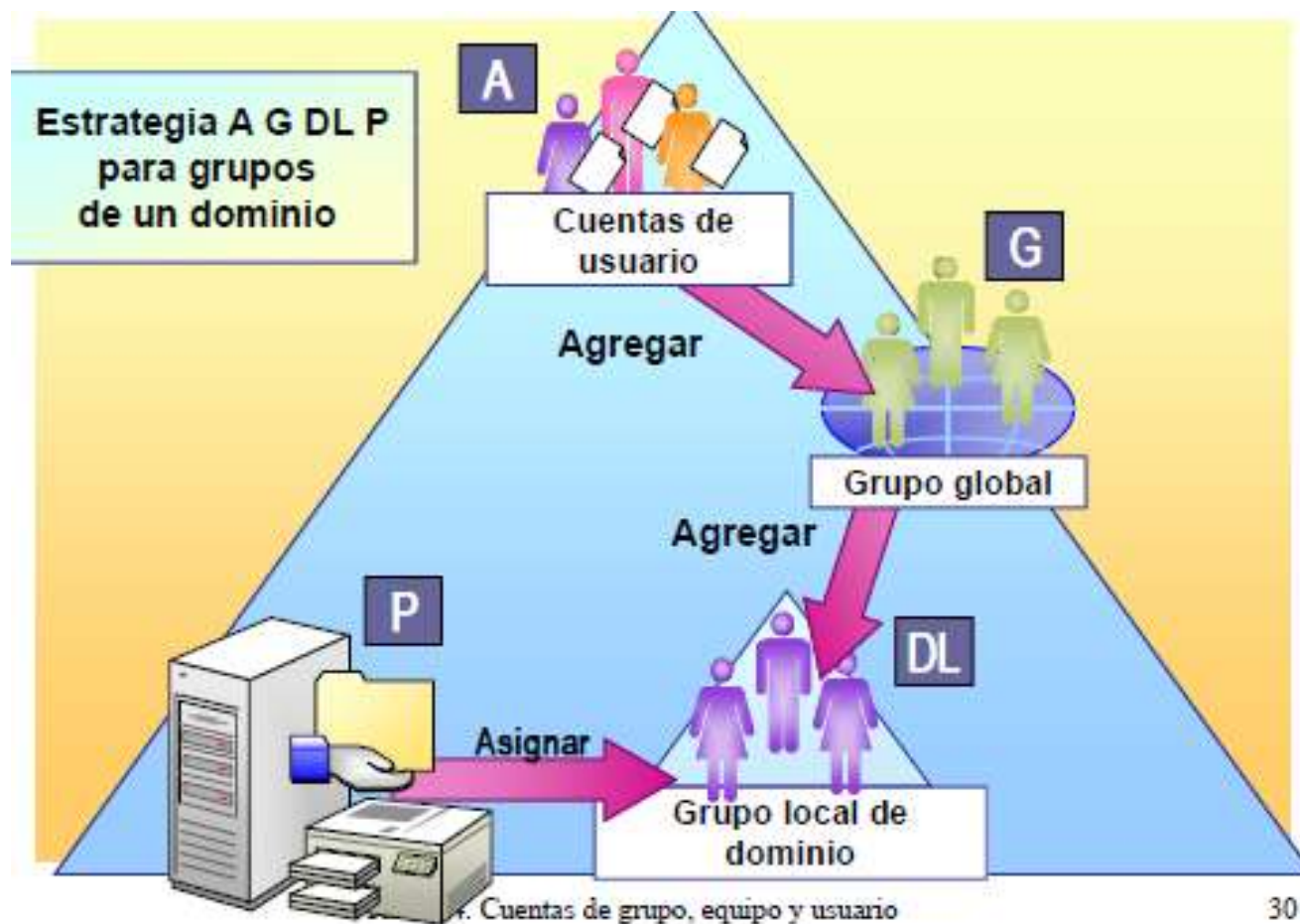
- ▶ Es la estrategia idónea.
- ▶ Creamos usuarios, que englobamos dentro de Grupos Globales y estos a su vez en Grupos Locales de Dominio y a estos últimos se les asignan los Permisos
- ▶ Esto implica sólo una vez dar los permisos y la administración es sencilla.

# Estrategia 3: A G D L P

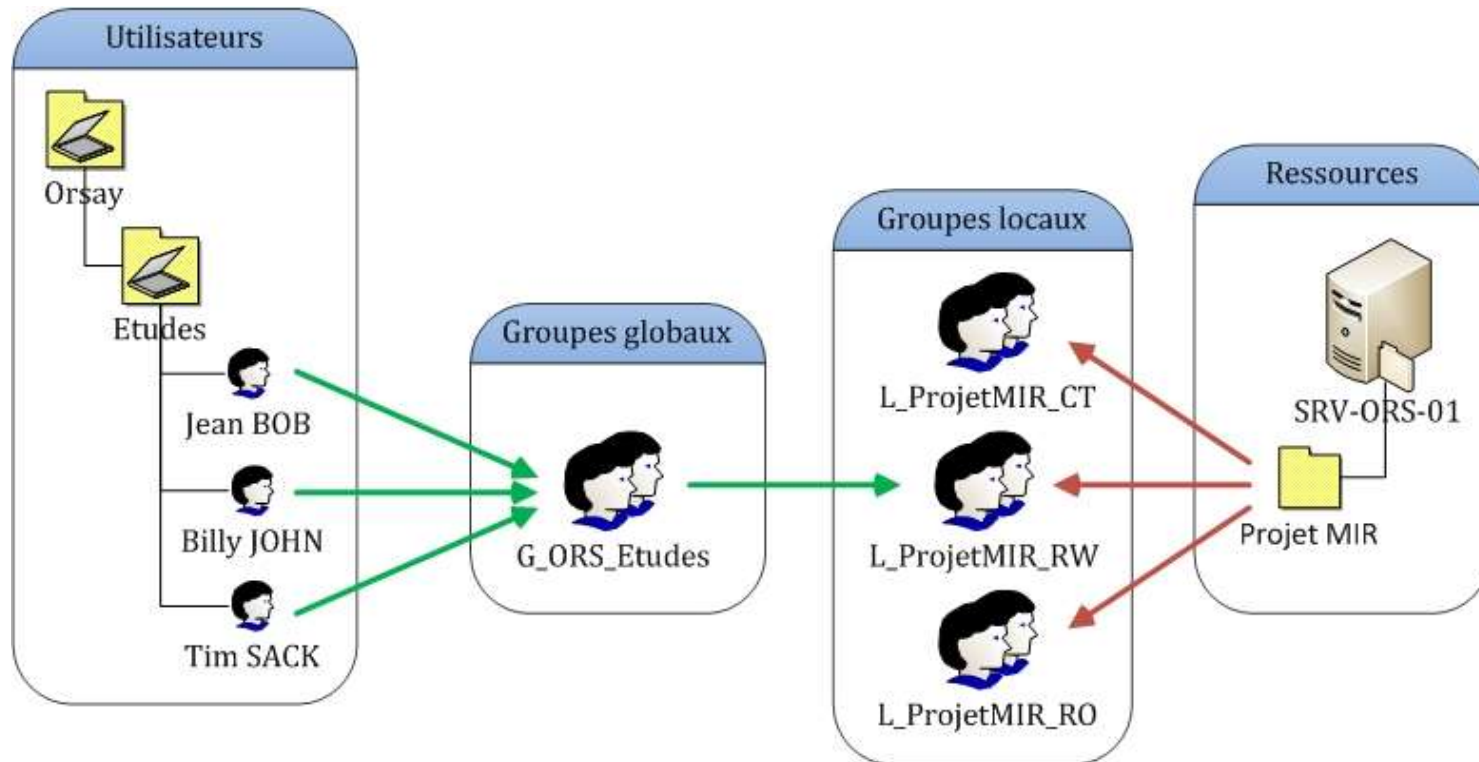
---

- ▶ Se hace uso de esta estrategia en bosques con un dominio o con varios, con lo cual ya es flexible.
- ▶ Podemos crear los Grupos Globales de Usuarios para cada dominio a modo de agrupación simple, y después delimitar los permisos a los recursos en Grupos Locales de Dominio, definiendo perfectamente cada permiso.

# Estrategia 3: A G DL P



# Visto de otra forma:



- La única **desventaja** es la complejidad de administración inicial al crear los Grupos, pero una vez realizado, es muy fácil de administrar y de mantener.

# Grupos especiales

- Son usuarios y grupos creados por defecto. Y Son:

- ▶ **Inicio de sesión anónimo**

No proporciona ni usuario ni contraseña.

- ▶ **Grupo creador**

Grupo que creo o tiene la propiedad del objeto

- ▶ **Propietario creador**

Usuario que creo o tiene la propiedad del objeto

- ▶ **Interactivo**

Usuario que acceden de forma local a través de una conexión de escritorio remoto.

- ▶ **Lotes**

Usuarios que han iniciado sesión en un recurso de cola de proceso por lotes o batch.

- ▶ **Todos**

Usuarios autenticados o no. Todos

- ▶ **Usuarios autenticados**

Usuarios y equipos autenticados por el sistema

Ver U.T. de  
derechos y  
permisos

Dependen su  
existencia,  
siempre de la  
versión de SO,

# Grupos locales I

Dependen su existencia, siempre de la versión de SO,

- **Administradores**

- ▶ Pueden hacer casi de todo

- **Operadores de copia**

- ▶ Hacer y recuperar backups

- **Operadores de configuración de red**

- ▶ Privilegios admirativos en torno a la red

- **Invitados**

- ▶ No pueden hacer casi de nada, excepto guardar archivos

Ver U.T. de derechos y permisos

# Grupos locales II

Ver U.T. de  
derechos y  
permisos

## ● Duplicadores

- ▶ Puede duplicar archivos y carpetas.
- ▶ Puede ejecutar programas y acceder a datos en un ordenador,

## ● Usuarios avanzados

- ▶ Pueden hacer casi de todo pero no ciertas labores administrativas.

## ● Todos

- ▶ Es un súper grupo que incluye a todos los demás grupos del sistema
  - ▶ Los grupos predeterminados
  - ▶ Los creados posteriormente
  - ▶ Al grupo Invitados

Dependen su  
existencia, siempre de  
la versión de SO,

# Herramienta a usar en AD

---

- ***Usuarios y equipos de Active Directory***

- ▶ Permite manejar todas las tareas relativas a cuentas de usuarios, grupos y equipos, además de administrar las unidades organizativas.

- ▶ *¿Cómo crear usuarios?*

- ▶ *Inicio / Programas / Administración del Servidor / Herramientas / **Usuarios y equipos del Active Directory***

- ▶ Por defecto se trabaja con el mismo dominio, aunque es posible trabajar con otros dominios



# Usuarios y equipos de AD

---

- Al acceder a un dominio con *Usuarios y equipos de AD*, existen por defecto una serie de unidades organizativas:
  - ▶ **Integrada (Builtin):**
    - ▶ Contiene los objetos que definen las cuentas integradas, (como los Administradores y Operadores de cuentas y grupos locales)
  - ▶ **Equipos (Computers):**
    - ▶ La unidad organizativa predeterminada para las cuentas de los equipos de los servidores miembro, y clientes
  - ▶ **Controladores de dominio (Domain Controllers):**
    - ▶ La unidad organizativa predeterminada para los equipos que son controladores de dominio
  - ▶ **Usuarios (Users):**
    - ▶ La unidad organizativa para los usuarios y grupos globales
  - ▶ **ForeignSecurityPrincipals:**
    - ▶ La unidad organizativa por defecto para los identificadores de seguridad (SIDs) asociados con los objetos de dominios externos en los que se confía.

# Usuarios y equipos AD

---

- También podemos ver otras carpetas
- ¿Cómo?
  - ▶ Activando la opción de **Opciones Avanzadas** (dentro del menú Ver, en la barra superior)
  - ▶ **LostAndFound:**
    - ▶ Contiene objetos cuyas UO se eliminaron al tiempo de crear el objeto.
    - ▶ Si un objeto se creó o se movió a una ubicación que ya no existe después de la replicación, el objeto perdido se agrega a este contenedor.
    - ▶ Son objetos que han quedado huérfanos, y se pueden eliminar o recuperar
  - ▶ **System:**
    - ▶ Contiene configuraciones integradas del sistema.

# Usuarios y equipos AD

---

- En estos contenedores los usuarios y grupos están mezclados
- Podemos crear **UNIDADES ORGANIZATIVAS** (UO) para agrupar los objetos del DA en estos nuevos contenedores, incluyendo en ellas lo que nos interesa.

# Gestión de grupos de usuarios en DA I

---

## □ ¿Qué puedo hacer?

- Crear UO
- Crear, modificar y eliminar cuentas de usuarios.
- Crear plantillas.
- Crear, modificar y eliminar de cuentas de grupos
- Añadir usuarios a un grupo

# Gestión de grupos de usuarios en DA IV

---

- Cambiar las contraseñas a los usuarios:

- ▶ Usuarios del dominio

- ▶ Situado sobre el usuario, visualizamos el menú contextual “Restablecer contraseña”

- ▶ Usuarios administradores

- ▶ A través de la combinación de teclas CTROL + ALT +SUPR

# Gestión de grupos de usuarios en DA V

The screenshot shows the 'dani gonzalez Properties' dialog box with the 'General' tab selected. The fields are as follows:

- First name: dani
- Last name: gonzalez
- Display name: dani gonzalez
- Description: (empty)
- Office: (empty)
- Telephone number: (empty)
- E-mail: (empty)
- Web page: (empty)

The website [www.aprendeinformaticaonmigo.com](http://www.aprendeinformaticaonmigo.com) is displayed at the bottom of the dialog box.

- Menú contextual
  - ▶ Propiedades de las cuentas de usuarios:

# Perfil de usuario. ¿Qué se entiende?

---

- Contiene todos los valores que puede **definir el usuario para su entorno de trabajo en un equipo**,
- Incluye:
  - ▶ la configuración del escritorio, la configuración del ratón, el menú de opciones, la configuración regional y de sonido, además de las conexiones de red y de las impresoras.
- Un perfil de usuario concede, por tanto, al usuario un conjunto predefinido de configuraciones del entorno del S.O.
- **Windows requiere un perfil de usuario para cada cuenta de usuario que tenga acceso al sistema**
  - ▶ Cada usuario tendrá su configuración específica.

# Perfil de usuario

---

- La primera vez que inicia la sesión un usuario se crea su perfil de usuario de la siguiente forma:
  - ▶ Se crea la carpeta para almacenar el perfil
  - ▶ A continuación, el contenido de la carpeta **Default (W08) Default User** (W. anteriores) se copia en la nueva carpeta de perfil de usuario
- El escritorio final del usuario (el que ve al conectarse) se crea usando el perfil creado para él y las configuraciones de los grupos de programas comunes de la carpeta **Acceso Público (W08) All Users (W. anteriores)**
- Cuando el usuario termina la sesión, todos los cambios realizados durante la sesión sobre la configuración predeterminada se guardan en su perfil de usuario. (El perfil por defecto no se modifica)
- **Perfil de usuario predeterminado (Default User):**
  - ▶ Sirve como base para todos los demás perfiles de usuario
  - ▶ Cada perfil comienza como una copia de perfil de usuario predeterminado



# Perfiles

---

- En Windows Server:



Local



De red



Temporal



Móvil



Obligatorio



SuperObligatorio

# Perfil local

---

- El perfil se crea cuando el usuario entra por primera vez (se loga)
- Se crean las siguientes carpetas, (depende de la versión de Windows)

▶ `%SystemDrive%\Users\%UserName%\ntuser.dat`

▶ *Ejemplo: c:\Users\pilar\ntuser.dat*

▶ `%SystemDrive%\Usuarios\%UserName%\ntuser.dat`

▶ `%SystemDrive%\Documents and Settings  
\\%UserName%\ntuser.dat`

# Perfil local

---

- Al cerrar la sesión, se actualiza el perfil con los cambios.
- Se mantienen en un directorio predeterminado o en una localización indicada en ***Ruta Perfil*** (*Ver Propiedades del usuario*)

# Estructura de la carpeta perfil (XP)
















Carpeta	Descripción
Configuración local	Datos de programa para las aplicaciones de Internet Coches de internet
Cookies	Cookies de internet
Datos de programa	Aquí ponen las aplicaciones de 32 bits su información de configuración y sus archivos temporales.
Entorno de red	Información de ordenadores próximos en la red
Enviar a	Lista de dispositivos a los que se pueden enviar archivos y directorios.
Escritorio	Iconos y accesos directos del escritorio
Favoritos	Lista de localizaciones preferidas en la red, utilizada principalmente por Internet Explorer
Impresoras	Guarda información sobre las impresoras de la red.
Menu inicio	Elementos que aparecen a través del menú de inicio.
Mis documentos	Punto de almacenaje para documentos e imágenes.
My documents	Análogo al anterior.
Plantillas	Localización de las plantillas de aplicación
Reciente	Los archivos utilizados por los documentos abiertos más recientemente.
Windows	Localización específica del usuario de archivos y configuraciones para aplicaciones que están instaladas en Windows.

**ntuser.dat** que contiene los parámetros del entorno.

# Estructura W10 22H2

---

Nombre

-  .afirma
-  .dotnet
-  Búsquedas
-  Contactos
-  Descargas
-  Documentos
-  Escritorio
-  Favoritos
-  Imágenes
-  Juegos guardados
-  Música
-  Objetos 3D
-  OneDrive
-  Vídeos
-  Vínculos

# Perfil temporal

---

- ▶ Es el perfil que se crea cuando se produce un error en la carga del perfil de red del usuario.
- ▶ Se elimina al cerrar la sesión

# Perfil móvil

---

- Se guardan el perfil de usuario en un servidor, para que el usuario tenga el mismo perfil en cualquier equipo.
- Perfil de usuario que se descarga desde el servidor de perfiles al equipo local cuando un usuario inicia una sesión.
- Se actualiza en el servidor cuando el usuario cierra la sesión
- Este perfil es fijado por el administrador y se almacena en el servidor. (Se crea la primera vez que un usuario inicia una sesión)
- Los usuarios accederán siempre al mismo perfil con independencia del equipo del dominio que estén utilizando
- Los cambios se guardan en el servidor al acabar la sesión
- Si por algún problema, el perfil móvil del usuario no está disponible, se crea y usa un perfil de usuario temporal en el equipo local
- Si no se asigna perfil móvil al usuario, el usuario tendrá un perfil temporal en cada equipo del dominio en el que trabaje

# Perfil obligatorio

---

- Es un perfil móvil que es “obligatorio” o está impuesto, de forma que no se guardarán los cambios que el usuario realice en el mismo
- Lo crea el administrador para especificar una configuración determinada a aplicar a un usuario concreto o a varios
- El usuario puede realizar cambios mientras tiene la sesión
- iniciada, pero dichos cambios se perderán al cerrar la sesión porque no se guardan
- Sólo los administradores de sistemas podrían realizar cambios sobre los mismos



# Perfil superobligatorio

---

- Es un perfil móvil que es “obligatorio, pero en el caso de no poderse cargar no se carga un perfil temporal, sino que no te deja iniciar sesión.
- Se implementa igual que el perfil obligatorio pero añadiendo la palabra **.man** al final si es windows NT y antes de V2 si es un Windows posterior a windows NT

# Resumiendo

---

## ● Perfil red

▶ Es el perfil que se crea al conectarse a un Servidor.

▶ Tipos:

### ▶ Móvil:

- Es asignado por los administradores y puede ser modificado por el usuario.

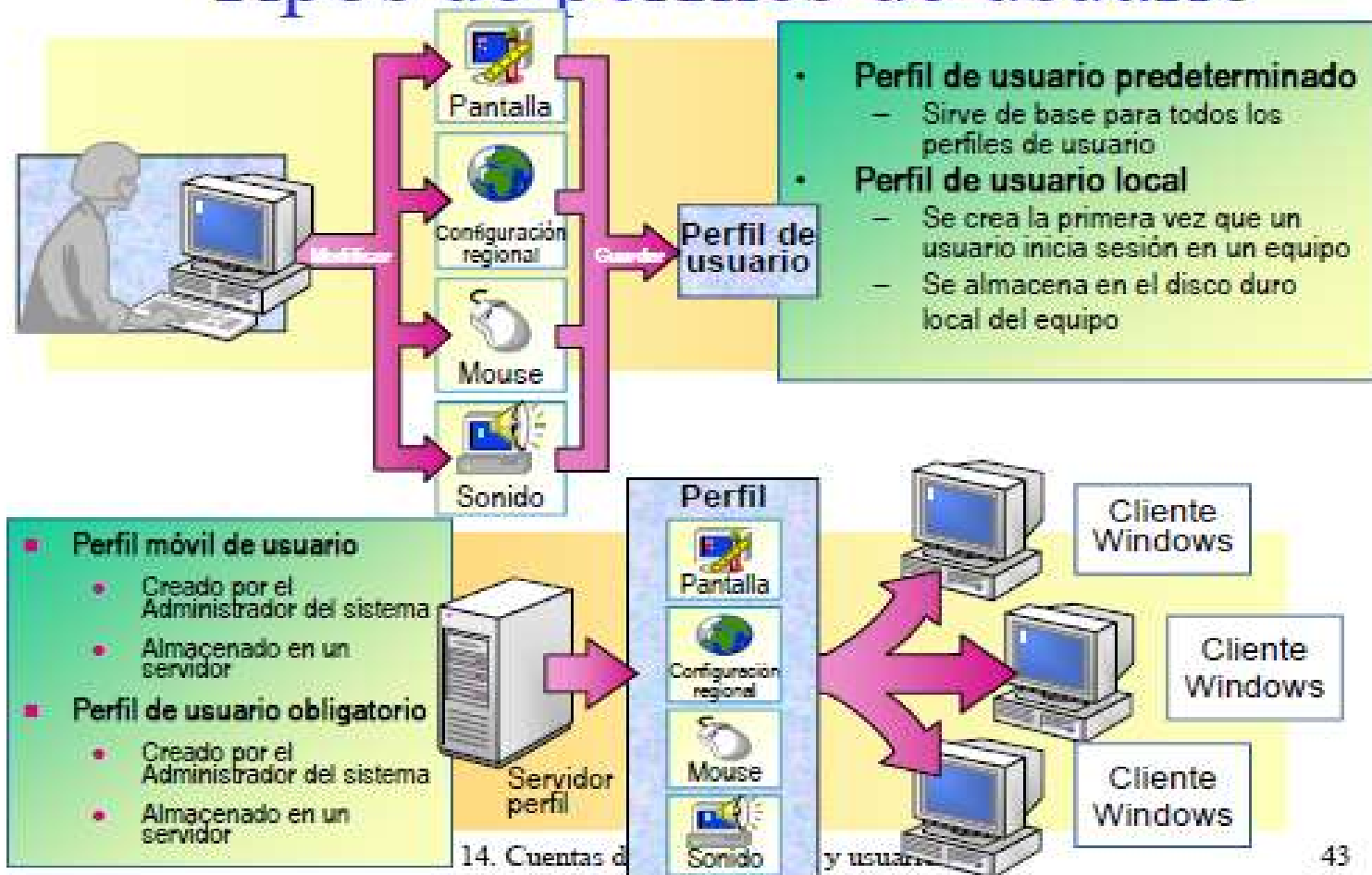
### ▶ Obligatorio:

- Es asignado por los administradores y aunque lo pueda modificar el usuario los cambios se pierden al finalizar la sesión.

### ▶ Super-obligatorio:

- Si el perfil no se carga al conectarse al servidor no se cargará el perfil temporal y no podrá conectarse.


# Tipos de perfiles de usuario



43

# ¿Cómo Administrar perfiles locales?

---

- Desde la utilidad **Sistema** *(en el Panel de control)*
- **Opción *Perfiles de usuario*** *(está en la ficha “Opciones Avanzadas”)*
  -  Podrá ver la información de los **perfiles guardados** en el sistema: nombre, tamaño, tipo (local o móvil) y última modificación
- Sólo es posible copiar el perfil “DEFAULT”.

# Cuentas de equipos

---

- Se almacenan en AD y representan un equipo concreto de la red
- Cada equipo del dominio, sea servidor miembro o controlador de dominio, tiene una cuenta de equipo
- Sirve para auditar las tareas que se realizan desde ese equipo, para otorgar permisos y restricciones o para controlar el acceso a la red y a los recursos
- Permiten realizar administración remota
- A los equipos con W95 y W98 no se les asignan cuentas de equipo porque no tienen las características de seguridad necesarias
- Se pueden agregar cuentas de equipo a cualquier unidad organizativa, pero las mejores son *Equipos* o *Controladores de dominio* o bien una unidad organizativa creada dentro de ellas

# Cuenta de equipos

---

- **Creación de cuentas de equipo**

- ▶ Automáticamente: al unirse un equipo a un dominio, se crea de forma automática la cuenta de equipo y se ubica en el contenedor **Computer** (si es un servidor miembro o cliente) o en **Controladores de dominio** (si es un controlador de dominio)

- Se pueden editar las “propiedades” de una cuenta de equipo, añadiendo información:

- ▶ sobre el SO, los grupos a los que pertenece, por quién está administrado, etc.

- Las cuentas de equipo pueden ser eliminadas, deshabilitadas y habilitadas, moverlas a una unidad organizativa distinta, etc.