

# Tema 14.

## Configuración de cuentas de grupo, equipo y usuario

Administración de Sistemas Operativos



M<sup>a</sup> Pilar González Férez

# Índice

1. Herramienta *Usuarios y equipos de Active Directory*
2. Cuentas de usuario
3. Los grupos y su configuración
4. Cuentas predeterminadas de usuarios y grupos
5. Perfiles de usuario
6. Administración de perfiles de usuario
7. Configuración y administración de cuentas de equipos

# Herramienta *Usuarios y equipos* de Active Directory

- *Usuarios y equipos del Active Directory* es la herramienta de administración más importante de Active Directory
- Permite manejar todas las tareas relativas a cuentas de usuarios, grupos y equipos, además de administrar las unidades organizativas
- *Inicio / Programas / Herramientas administrativas/ Usuarios y equipos del Active Directory*
- Por defecto se trabaja con el dominio al que esté conectado el equipo, accediendo a la información del *Active Directory* y a los objetos de usuario que estén definidos en el mismo
- También es posible conectarnos a otro controlador de dominio de ese dominio, o de otro dominio

# Herramienta *Usuarios y equipos de AD* (ii)

- 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)
  - ***Equipos (Computers)***: La unidad organizativa predeterminada para las cuentas de los equipos de los servidores miembro
  - ***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
  - ***ForeignSecurityPrincipals***: La unidad organizativa por defecto para los identificadores de seguridad (SIDs) asociados con los objetos de dominios externos en los que se confía

# Herramienta *Usuarios y equipos de AD* (iii)

- También podemos ver otras carpetas activando la opción de *Opciones Avanzadas* (dentro del menú *Ver*)
  - ***LostAndFound***: contiene objetos cuyas unidades organizativas 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

# Cuentas de usuario

- W2008 ofrece **cuatro** tipos de cuentas de usuario:
  - **Cuentas de usuarios locales**
    - Cuentas de usuario definidas en el equipo local, con acceso solamente al equipo local y, por tanto, a los recursos del mismo
    - Los usuarios pueden tener acceso a los recursos de otro equipo de la red si disponen de una cuenta en dicho equipo
    - Para poder acceder a los recursos que un equipo comparte, es necesario autenticarse en él
    - Estas cuentas de usuario residen en el administrador de cuentas de seguridad (*Security Account Manager, SAM*) del equipo, que es la BD de cuentas de seguridad local
    - Se pueden crear en estaciones de trabajo o en servidores miembros pero NO en *controladores de dominio*
    - Al usar cuentas locales de un servidor miembro, el usuario no podrán usar los recursos del dominio (al no estar autenticadas en él)

# Cuentas de usuario (ii)

- W2008 ofrece 4 tipos de cuentas de usuario: (continúa...)
  - **Cuentas de usuario de dominio**
    - Permiten a un usuario iniciar sesión en el dominio para obtener acceso a los recursos de la red
    - El usuario tendrá acceso en cualquier equipo de la red con una única cuenta y contraseña
    - Estas cuentas de usuario residen en el servicio de directorio AD y se crean definiéndolas en un *controlador de dominio*
    - En los controladores de dominio sólo puede haber cuentas de este tipo, no se pueden definir cuentas de usuario local
    - Un usuario puede acceder a los recursos del dominio utilizando un inicio de sesión único

# Cuentas de usuario (iii)

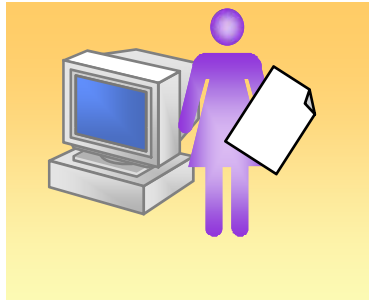
- W2008 ofrece 4 tipos de cuentas de usuario: (continúa...)
  - **Cuentas de usuario integradas**
    - Permite a un usuario realizar tareas administrativas u obtener acceso temporalmente a los recursos de red
    - Existen dos cuentas de usuario integradas que no pueden eliminarse: *Administrador* e *Invitado*
    - Las cuentas de usuario locales *Administrador* e *Invitado* residen en SAM
    - Las cuentas de usuario integradas de dominio residen en AD
    - Estas cuentas se crean automáticamente durante la instalación de Windows o la de un dominio del Active Directory
    - Son cuentas instaladas con el sistema operativo y las aplicaciones o servicios



# Cuentas de usuario (iv)

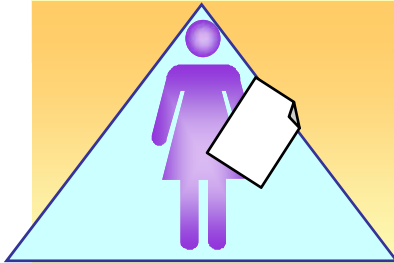
- W2008 ofrece 4 tipos de cuentas de usuario: (continúa...)
  - **Cuentas de usuario implícitas**
    - Creadas de forma implícita por el sistema operativo o aplicaciones, se usan para asignar permisos en ciertas situaciones
    - **SistemaLocal (Localsystem)**: permite ejecutar procesos del sistema y administrar las tareas relativas al sistema. No se puede iniciar una sesión con esta cuenta, pero algunos procesos se ejecutan con ella:
      - Por ejemplo, esta cuenta es la que se usa para ejecutar muchos de los servicios del sistema (los demonios)
    - **LocalService**: acceso al sistema local
    - **NetworService**: acceso al sistema local y en la red
    - Otras cuentas son, por ejemplo, las de **Internet Information Services** o los servicios de terminales

# Cuentas de usuario (v)



## Cuentas de usuario locales

- Permiten a los usuarios iniciar sesión y acceder a recursos en un equipo específico
- Residen en SAM



## Cuentas de usuario de dominio

- Permiten a los usuarios iniciar sesión en el dominio para tener acceso a los recursos de red
- Residen en Active Directory



## Cuentas de usuario integradas

- Permiten a los usuarios realizar tareas administrativas o tener acceso temporal a recursos de red
- Residen en SAM (cuentas de usuario integradas locales)
- Residen en Active Directory (cuentas de usuario integradas del dominio)

# Cuentas de usuario (vi)

- **Nombres de inicio de sesión:** Todas las cuentas de usuario se identifican con este nombre que tiene 2 partes:
  - **Nombre de usuario**
  - **Nombre del dominio o grupo de trabajo** al que pertenece la cuenta
  - P.e., para el usuario *pilar*, cuya cuenta está definida en el dominio *aso.es*, tendríamos: pilar@aso.es
- **Nombre completo de dominio del usuario:** *nombre del dominio + unidad organizativa + nombre usuario:*
  - aso.es\Users\pilar
  - aso.es\Users\Profesores\AdministracionSO\pilar

# Cuentas de usuario (vii)

- **Identificador de seguridad, SID ó Id. de Seguridad**
  - Cada cuenta (de usuario, grupo o equipo) tiene asociado un número único, el *identificador de seguridad*, que la identifica de forma única y que es generado al crear la cuenta
  - Los procesos internos de Windows hacen referencia al SID de las cuentas y no a los nombres de las cuentas
  - Cada cuenta tiene un SID diferente
  - Un SID nunca se reutiliza
    - Si se elimina una cuenta, y después se crea una nueva cuenta usando el nombre de cuenta anterior, a la nueva se le asigna un SID distinto. La nueva cuenta NO tendrá los derechos o permisos de la anterior
  - El SID de una cuenta de dominio está formado por dos partes:
    - Prefijo, que actúa como Id. de seguridad del dominio
    - Id. relativo único, que alberga el maestro de Id. Relativo
  - Se utiliza, por ejemplo, para el cifrado de archivos. Si el usuario es borrado, sus ficheros no se pueden descifrar

# Cuentas de usuario (viii)

- Creación de cuentas de dominio de usuario:
  - Herramienta *Usuarios y equipos del AD*, clic con el botón derecho del ratón en la unidad organizativa donde se quiera añadir la nueva cuenta, seleccionando el menú *Nuevo* y la opción *Usuario*
  - Configurar los nombres:
    - *Nombre y apellidos*, que se usan para crear el **nombre completo**
    - *Nombre completo* que es el nombre para mostrar el usuario (no se distingue entre mayúsculas y minúsculas y puede tener 64 caracteres como máximo)
    - *Nombre de inicio de sesión* (no distingue entre mayúsculas y minúsculas y puede tener 20 caracteres como máximo)
    - Seleccionar el *dominio* con el que va a estar asociada la cuenta
  - Configurar la contraseña y algunas restricciones
    - El usuario debe cambiar la contraseña en el siguiente inicio de sesión
    - El usuario no puede cambiar la contraseña
    - La contraseña nunca caduca
    - Cuenta deshabilitada

# Cuentas de usuario (ix)

- Creación de cuentas locales de usuario:
  - Herramienta *Administración de equipos*, expandir el nodo *Herramientas de sistema* y abrir *Usuarios y grupos locales*. Hacer clic con el botón derecho del ratón en *Usuarios* y seleccionar *Nuevo usuario*
  - Configurar los nombres:
    - *Nombre de usuario*
    - *Nombre completo* del usuario
    - *Descripción*
  - Configurar la contraseña y algunas restricciones
    - El usuario debe cambiar la contraseña en el siguiente inicio de sesión
    - El usuario no puede cambiar la contraseña
    - La contraseña nunca caduca
    - Cuenta deshabilitada

# Cuentas de usuario (x)

- Configuración de cuentas de usuario: en *Propiedades*
  - **Información de contacto del usuario:** nombre, iniciales, apellidos, nombre para mostrar, descripción, oficina, n° de tlf, e-mail y página Web
  - **Parámetros del entorno del usuario**
    - *Ruta de acceso al perfil* (determinar la configuración del escritorio y del panel de control, la disponibilidad del menú y las aplicaciones)
    - *Archivo de comando de inicio de sesión* (archivo por lotes que se ejecutará siempre que el usuario inicie una sesión)
    - *Ruta de acceso local* (directorio a usar para guardar ficheros)
      - En un dominio, haciendo que el directorio de trabajo esté compartido en la red, podemos conseguir que el usuario siempre trabaje en el mismo directorio de trabajo
  - **Grupos** a los que pertenece
  - Aspectos de configuración del *Terminal Server*

# Cuentas de usuario (xi)

- Configuración de cuentas de usuario:
  - **Opciones de cuenta y restricciones**
    - **Horas de inicio de sesión:** Permiten controlar las horas durante las cuales el usuario puede iniciar la sesión localmente o en el dominio, trabajar normalmente, acceder a sus recursos. Si un usuario mantiene la sesión cuando su hora de inicio de sesión termina, se pueden forzar dos comportamientos:
      - **Desconexión forzada:** se desconecta al usuario cuando caduca su hora de inicio de sesión (mediante la *Configuración de seguridad* de las **Directivas locales**, activando *Cerrar automáticamente la sesión de los usuarios cuando termine su tiempo de sesión*)
      - **Sin desconexión:** no desconecta las conexiones ya establecidas cuando entran en una franja de horario restringido, sencillamente no se permite que realicen nuevas conexiones de red
    - **Iniciar sesión en:** Para cuentas de dominio, equipos del dominio en los que puede iniciar una sesión para trabajar en ellos



# Cuentas de usuario (xii)

- Operaciones con cuentas de usuario:
  - Las principales operaciones que se pueden realizar son:
    - Deshabilitar/habilitar una cuenta
    - Desbloquear una cuenta
    - Prohibir que se cambie la contraseña de la cuenta
    - Eliminar una cuenta
    - Mover una cuenta
    - Renombrarla
    - Cambiar la contraseña
  - Todas estas operaciones se realizarán desde la herramienta *Usuarios y Equipos del AD* o desde *Usuarios y grupos locales*

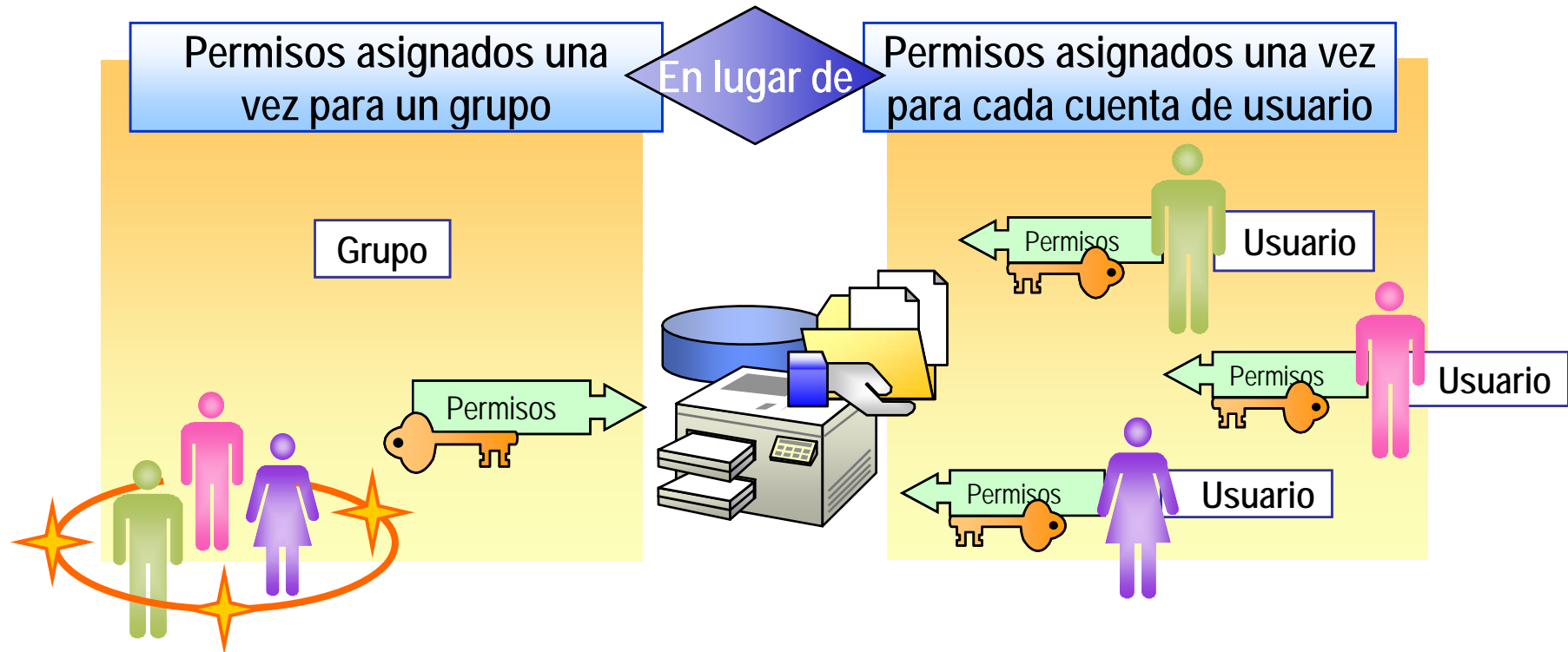
# Cuentas de usuario (xiii)

- Derechos de los usuarios comunes
  - Los derechos autorizan a un usuario que ha iniciado sesión en un equipo o en una red a realizar ciertas acciones sobre el sistema (Si no posee los derechos apropiados para realizar una acción se bloquean los intentos de llevarla a cabo)
  - Los derechos de una cuenta de usuario local incluyen:
    - Iniciar sesión localmente y acceder a los recursos del equipo según los permisos asignados a los mismos
    - Cerrar el sistema
    - Acceder a ese equipo desde la red
  - Los derechos de una cuenta de usuario de dominio:
    - Iniciar sesión en el dominio y acceder a cualquier objeto del mismo según los permisos asignados

# Grupos

- Un **grupo** es una colección de usuarios, equipos u otros grupos
- Los grupos se usan para simplificar la administración del acceso de usuarios y equipos a los recursos (directorios, ficheros, impresoras, etc.)
- Permiten conceder permisos de acceso a varios usuarios al mismo tiempo, en lugar de concederlos usuario a usuario

# Grupos (ii)



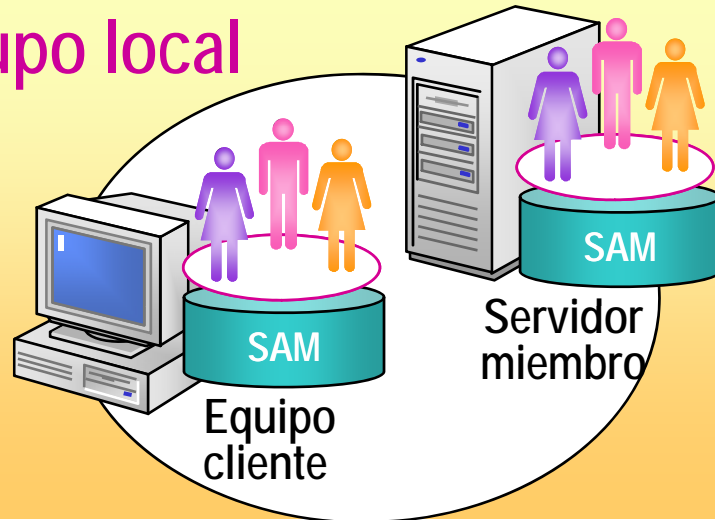
- Los miembros de un grupo tienen los mismos derechos y permisos concedidos al grupo
- Los usuarios pueden pertenecer a varios grupos
- Los grupos y las cuentas de equipos también pueden pertenecer a un grupo

# Grupos (iii)

- Los grupos funcionan de forma diferente en un equipo local que en un dominio
- **Grupos en un equipo local**, llamados *grupos locales*
  - Se crean en equipos que son estaciones de trabajo independientes o servidores miembro, pero NO en controladores de dominio
  - Residen en SAM (*Security Accounts Manager*)
  - Se usan para otorgar permisos a recursos y otorgar derechos para las tareas del sistema en el equipo local
- **Grupos en un dominio:**
  - Se crean únicamente en *controladores de dominio*
  - Residen en el servicio de directorio Active Directory
  - Se usan para otorgar permisos a recursos y otorgar derechos para tareas del sistema en cualquier equipo del dominio

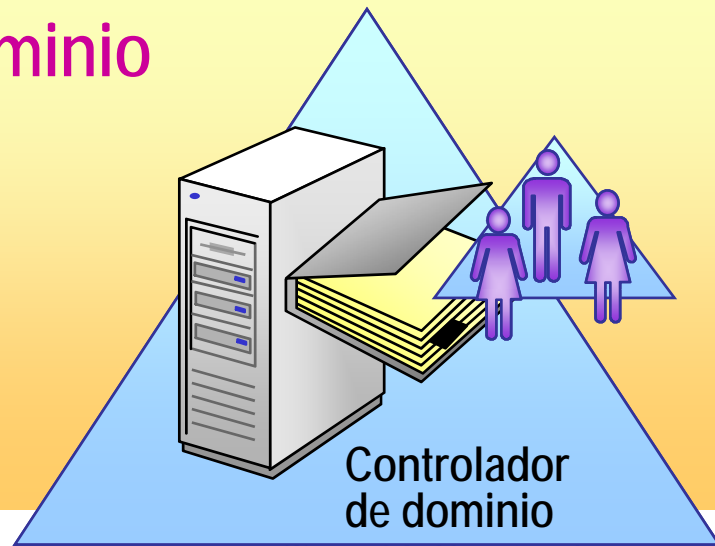
# Grupos(iv)

## Grupo local



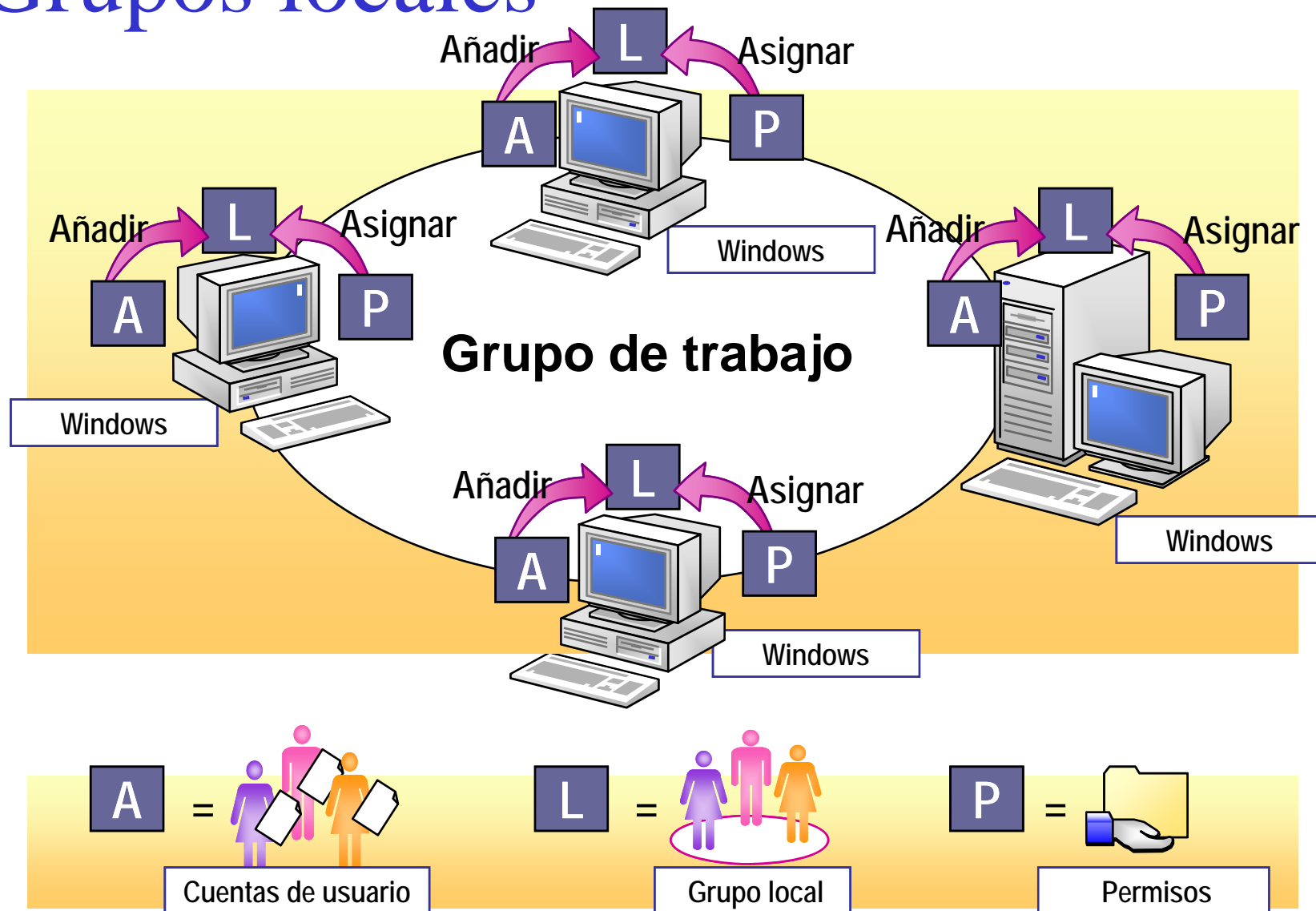
- Creados en equipos que no son controladores de dominio
- Residen en SAM
- Se utilizan para controlar el acceso a recursos del equipo

## Dominio



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

# Grupos locales



# Grupos (v)

- **Tipos de grupos de dominio**
  - **Grupos de seguridad:**
    - Pueden tener descriptores de seguridad asociados
    - Permiten asignar permisos para el acceso a los recursos compartidos en el dominio
      - Su finalidad es controlar quién puede usar qué recursos
    - También pueden ser usados para enviar mensajes de correo
  - **Grupos de distribución:**
    - Se usan para listas de distribución de correo electrónico
    - A estos grupos no se les puede asignar permisos para el acceso a los recursos



# Grupos (vi)

- **Ámbito de grupos de seguridad de dominio**
  - El **ámbito de un grupo** determina dónde se usará ese grupo, y afecta a la pertenencia del grupo y al anidamiento de grupos (agrupar grupos como miembros de otros grupos)
  - **Grupos de ámbito local de dominio** (grupos locales de dominio): se usan para garantizar permisos a recursos de dominio situados en el mismo dominio
    - Están pensados para ayudar a administrar el acceso a los recursos, tales como impresoras y carpetas compartidas
    - El recurso no tiene por qué residir en un controlador de dominio, puede estar en un servidor miembro
    - Sólo se les pueden asignar permisos en el mismo dominio
    - Pueden tener como miembros cuentas de usuario, grupos globales y universales de cualquier dominio y grupos locales de su mismo dominio
    - Se pueden agregar a otros grupos locales de dominio

# Grupos (vii)

- **Ámbito de grupos de dominio:** (continúa...)
  - **Grupos de ámbito global** (grupos globales): se usan para otorgar permisos a objetos del dominio
    - Están pensados para administrar cuentas de usuario y grupo en el dominio particular
    - Se incluyen en un grupo de dominio local para acceder a sus recursos
    - Tienen una pertenencia limitada, sólo pueden tener como miembros cuentas y grupos globales del mismo dominio
    - Pueden anidarse dentro de otros grupos, e.d., pueden ser miembro de otro grupo global del mismo dominio, a grupos locales de dominio y a grupos universales del mismo y otro dominio

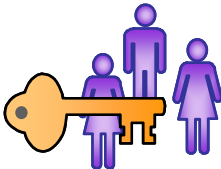
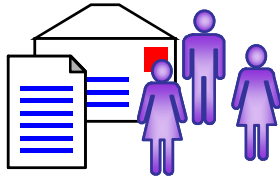
# Grupos (viii)

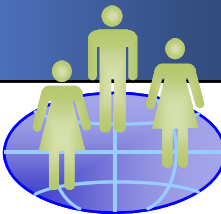
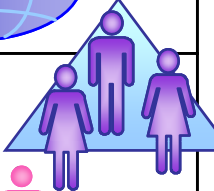
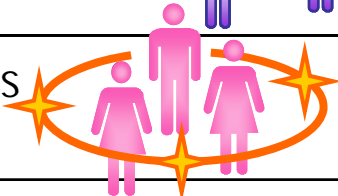
- **Ámbito de grupos de dominio:** (continúa...)
  - **Grupos de ámbito universal** (grupos universales): se usan para otorgar permisos a gran escala en el árbol de dominio o en el bosque
    - Usados para conceder permisos de acceso a recursos situados en cualquier dominio
    - Pensados para consolidar grupos que abarcan varios dominios. Normalmente se agregan grupos globales como miembros
    - Tienen pertenencia abierta, pueden tener como miembros cualquier cuenta de usuario del dominio, grupos globales y universales de cualquier dominio
    - Pueden ser miembro de cualquier grupo de dominio local o universal en cualquier dominio
    - No están disponibles cuando el dominio funciona en modo mixto (compatibilidad con WNT)

# Grupos (ix)

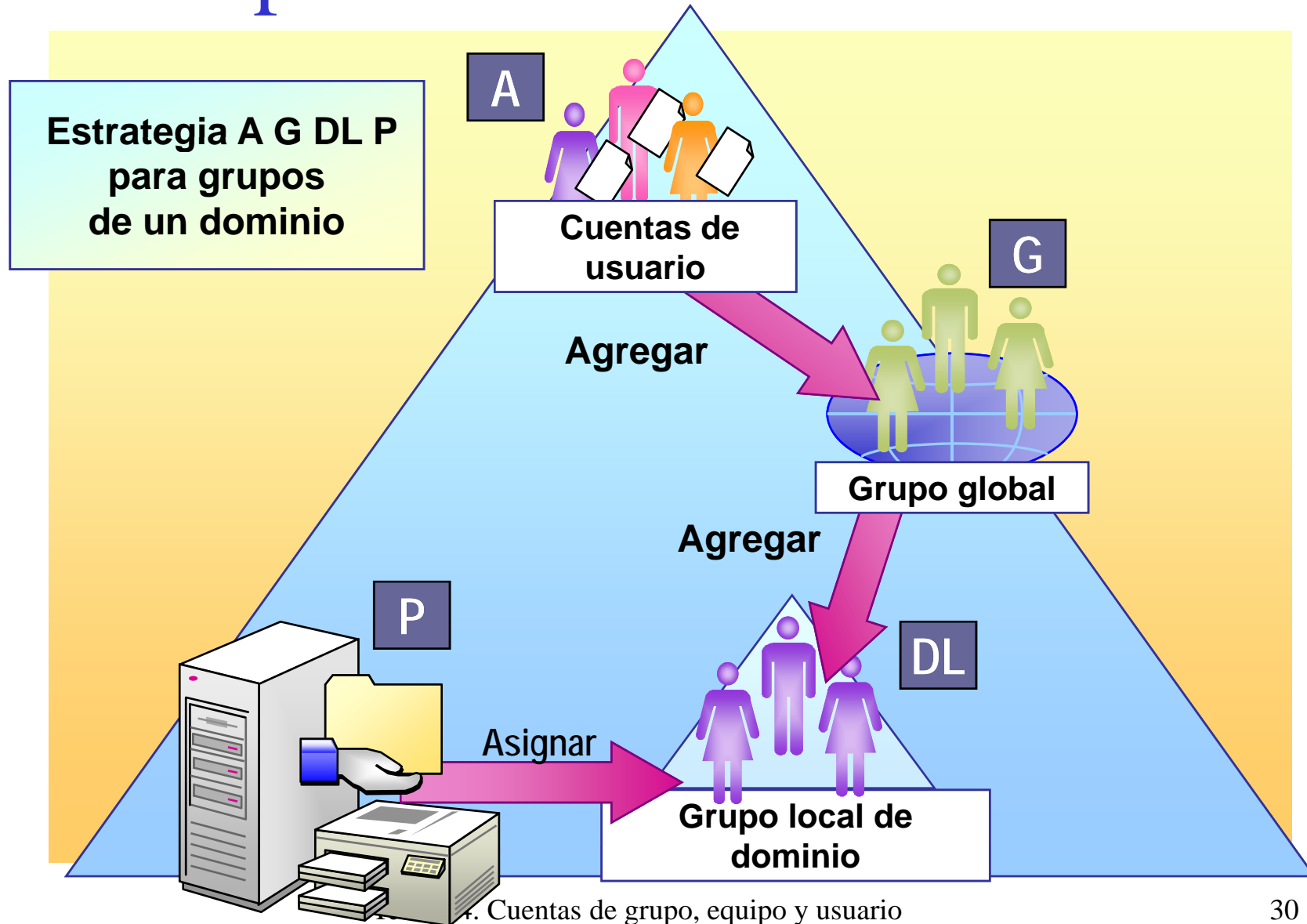
- Ejemplo de ámbito de grupos de dominio:
  - Grupo local de dominio **impresora\_color** que tiene permisos para imprimir en la impresora LaserColor
  - Grupo global de dominio **profesoresASO**
    - A ese grupo pertenecen los usuarios que son profesores de la asignatura ASO: Pilar, Eduardo, Juanjo (pero no el resto de profesores)
    - Ese grupo de usuarios puede imprimir en la impresora LaserColor
    - El grupo **profesoresASO** se hace miembro de **impresora\_color** para darle permisos sobre la impresora, y que puedan imprimir
  - Grupo universal **Todosusuimpresora**
    - Se hacen miembros los grupos globales **aso.es\alumnos** y **etc.es\alumnos** (*aso.es* y *etc.es* son dos dominios del mismo bosque)
    - El grupo **Todosusuimpresora** se hace miembro del grupo local **impresora\_color**
    - Al asignar permisos al grupo universal se dan a todos sus miembros

# 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	Se utiliza para organizar usuarios con necesidades similares de acceso a la red	
Grupo local de dominio	Se usa para asignar permisos a recursos de dominios	
Grupo universal	Se utiliza para asignar permisos a recursos relacionados en varios dominios	

# Grupos en un único dominio



# Grupos (x)

- **Creación de un grupo de dominio**
  - Herramienta *Usuarios y equipos del AD*, en la Unidad organizativa, seleccionar *Nuevo* y después ***Grupo***
  - Es necesario seleccionar
    - *Nombre del grupo* (no se distingue entre mayúsculas y minúsculas)
    - *Ámbito de grupo*: Dominio Local, Global o Universal
    - *Tipo de grupo*: Seguridad o Distribución
- **Creación de un grupo local**
  - Herramienta *Usuarios y grupos locales*: en *Grupos* y seleccione ***Nuevo grupo***
  - Nombre del grupo y una descripción del mismo

# Grupos (xi)

- **Pertenencia a un grupo por defecto**
  - Por defecto hay establecidas una serie de pertenencias
  - En un dominio
    - Todos los usuarios de dominio son miembros del grupo **Usuarios de dominio** y ese es su grupo principal
    - Todos los equipos (servidores miembro) del dominio son miembros de **Equipos de dominio** y ese es su grupo principal
    - Todos los controladores de dominio son miembros de **Controladores de dominio** y ese es su grupo principal
  - Para sistemas con grupos locales
    - Todos los usuarios son miembros del grupo **Usuarios**



# Grupos (xii)

- **Pertenencia a un grupo**
  - Pertenencia individual:
    - En el usuario, grupo o equipo (sólo para AD) que quiere modificar y en *Propiedades* seleccione la ficha ***Miembro de***
    - Seleccione *Agregar* para abrir el cuadro de diálogo *Seleccionar grupos*, escoja en él los nuevos grupos
    - También puede eliminar la cuenta de un grupo con *Quitar*
  - Administración de varias pertenencias:
    - En el *Propiedades del grupo*, seleccione la ficha ***Miembros***
    - Seleccione *Agregar* y escoja usuarios, equipos y grupos que serán miembros del grupo
    - También puede eliminar la cuenta de un grupo con *Quitar*

# Cuentas de grupo predeterminadas

- Existen dos tipos de cuentas de predeterminadas:
  - **Integradas:** cuentas de grupos que se instalan con el SO, aplicaciones y servicios
  - **Implícitas:** grupos especiales creados implícitamente que se usan para asignar permisos en ciertas situaciones; también son llamadas *identidades especiales*
- A los grupos predeterminados se les asigna automáticamente un conjunto de derechos que autoriza a los miembros del grupo a realizar acciones específicas, p.e., realizar una copia de seguridad, añadir/administrar impresoras, etc.

# Cuentas predeterminadas (ii)

- Grupos de dominio integrados
  - **Usuarios de dominio:** Se agrega automáticamente al grupo local de dominio **Usuarios**. Todos los usuarios son miembros del mismo
  - **Administradores de dominio:** Se agrega automáticamente al grupo local de dominio **Administradores**. Permite a los miembros del grupo realizar tareas administrativas
  - **Invitados de dominio:** Se agrega automáticamente al grupo local de dominio **Invitados**
  - **Administración de empresas:** Diseñado para usuarios que necesitan tener control administrativo sobre el dominio. Se agrega automáticamente al grupo local de dominio **Administradores**

# Cuentas predeterminadas (iii)

- Grupos locales integrados
  - **Usuarios:** Pueden realizar tareas para las que hayamos concedido derechos. No pueden modificar la configuración del sistema operativo ni los datos de otros usuarios
  - **Usuarios avanzados** Los miembros de este grupo pueden realizar tareas administrativas, excepto algunas reservadas al grupo *Administradores*. Pueden, iniciar/detener servicios, instalar programas, administrar las cuentas, o personalizar los recursos del sistema (impresoras, fecha, ...)
  - **Administradores:** Realizar todas las tareas administrativas en el equipo
  - **Operadores de copias de seguridad:** Pueden realizar copias de seguridad y restaurar todos los controladores de dominio usando la herramienta *Copias de seguridad de Windows*
  - **Operadores de impresión:** Pueden configurar y administrar impresoras de red que existen en los controladores de dominio

# Cuentas predeterminadas (iv)

- **Cuentas implícitas**

- Identidad **Todos**: Todos los usuarios interactivos, de red, de acceso telefónico y autenticados son miembros del grupo **Todos**. Este grupo se usa para dar un acceso amplio a los recursos del sistema
- Identidad **Usuarios autenticados**: Todos los usuarios que están autenticados (no pertenecen ni usuarios ni invitados anónimos)
- Identidad **Propietario creador**: La persona que creó el archivo o directorio es miembro de este grupo. Se usa para garantizar automáticamente los permisos de acceso al creador del mismo
- Identidad **Interactiva**: Cualquier usuario que haya iniciado la sesión en el equipo local
- Identidad de **Red**: Se concede a cualquier usuario que accede al sistema a través de la red
- Identidad **Sistema**: El propio SO Windows tiene esta identidad que se utiliza cuando necesita realizar funciones a nivel de sistema

# Perfiles

- El *perfil de usuario* contiene todos los valores que puede definir el usuario para su entorno de trabajo en un equipo, incluyendo la configuración del escritorio, el 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 S.O.
- Windows requiere un perfil de usuario para cada cuenta de usuario que tenga acceso al sistema
  - Cada usuario tendrá su configuración específica
- Los perfiles de usuario crean y mantienen automáticamente la configuración de escritorio del entorno de trabajo de cada usuario

# Perfiles (ii)

- 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 (iii)

- Hay tres tipos de perfiles
  - **Perfil de usuario local:**
    - La primera vez que un usuario inicia sesión en un equipo se crea un perfil para él y se guarda en el disco duro del equipo
    - Los cambios realizados en este perfil son específicos del equipo en el que se hicieron esos cambios
    - Es referente al equipo local y no es compartido por los equipos de la red (el usuario tendrá un perfil local en cada equipo en el que trabaje)
    - 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 (Propiedades del usuario)*
    - Directorios:
      - `%SystemDrive%\Users\%UserName%\ntuser.dat`  
*c:\Users\ pilar\ntuser.dat*
      - `%SystemDrive%\Usuarios\%UserName%\ntuser.dat`
      - `%SystemDrive%\Documents and Settings \%UserName%\ntuser.dat`



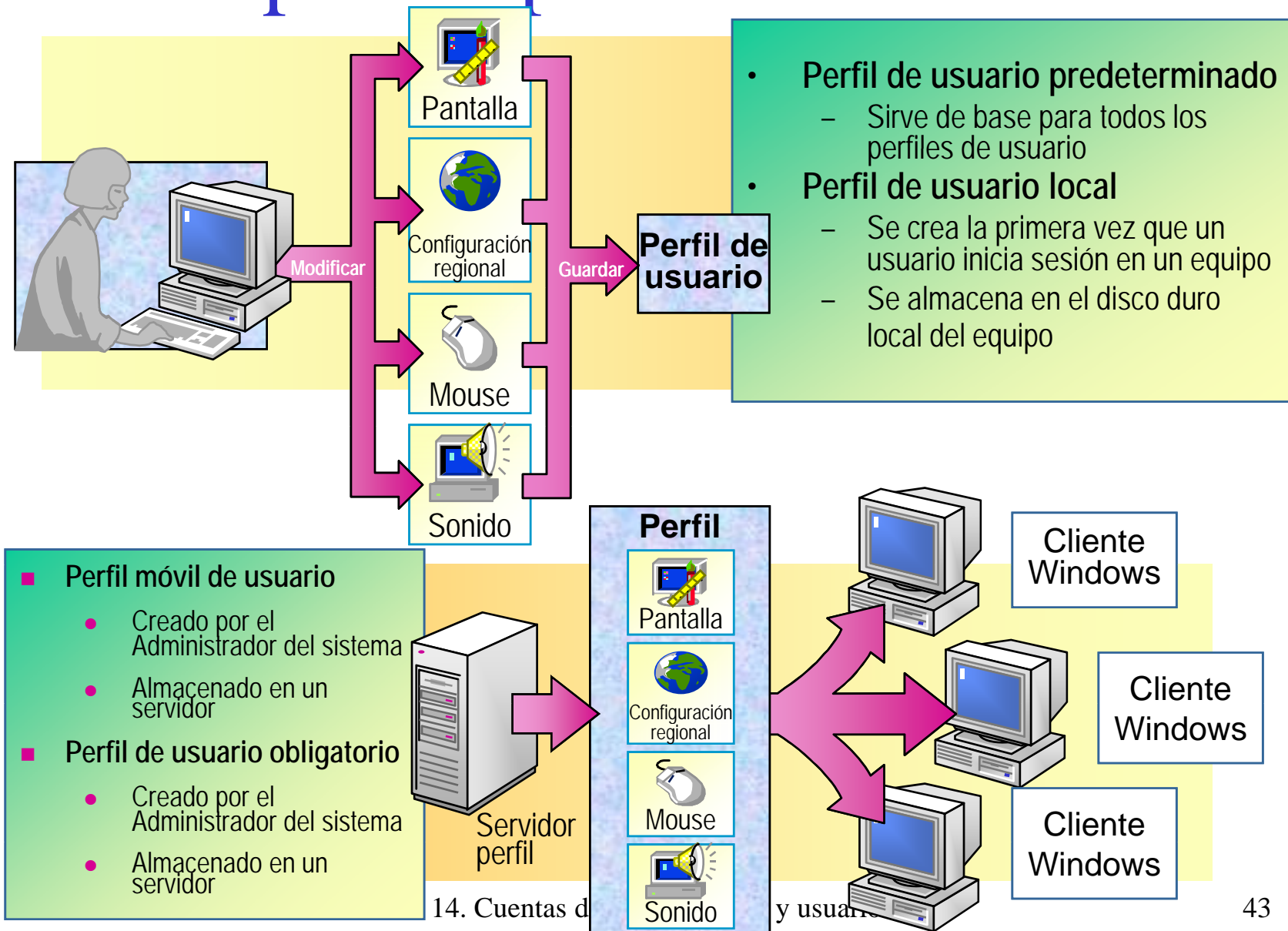
# Perfiles (iv)

- Hay tres tipos de perfiles
  - **Perfil de usuario móvil:**
    - En un dominio, se puede guardar el perfil de usuario en un servidor, *perfil móvil*, 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 en el equipo local
    - Si no se asigna perfil móvil al usuario, el usuario tendrá un perfil en cada equipo del dominio en el que trabaje

# Perfiles (v)

- Hay tres tipos de perfiles (continúa ...)
  - **Perfil de usuario 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

# Tipos de perfiles de usuario



# Administración de perfiles

- Creación de **perfiles móviles**:
  - Compartir el directorio donde van a residir los perfiles de usuario, asegurándose que el grupo **Todos** tiene acceso al mismo
    - P.e., en el servidor de perfiles compartir *c:\perfiles\*
  - Crear el directorio vacío en el que se guardará el perfil del usuario. El usuario ha de tener el permiso *Control total* sobre el directorio
    - P.e., en el servidor de perfiles crear *c:\perfiles\Pilar*
  - Desde *Usuarios y equipos del AD*, para el usuario, en su cuadro de *Propiedades* en la ficha *Perfil* indique la ***ruta de acceso al perfil***, con el servidor y el directorio compartido:
    - P.e., *\\servidor\_de\_perfiles\perfiles\Pilar*
  - El perfil móvil se almacenará en el fichero ***ntuser.dat***
  - La próxima vez que el usuario inicie una sesión se creará el perfil del usuario y se guardará al cerrar la sesión en ese directorio

# Administración de perfiles (ii)

- Creación de **perfiles obligatorios**:
  - Hay que crear un perfil móvil (como se ha indicado anteriormente)
  - A continuación, el perfil obligatorio se crea cambiando de nombre el fichero *ntuser.dat* a *ntuser.man*
- Administrar perfiles locales
  - Desde la utilidad *Sistema* (en el *Panel de control*) en la 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
  - Se pueden copiar, cambiar el tipo (si fuese posible) o eliminar

# Cuentas de equipos

- Las **cuentas de equipo** se almacenan en Active Directory 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

# Cuentas de equipos (ii)

- **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 *Equipos* (si es un servidor miembro) 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.