UT5: Configuración de Sistemas Operativos

Gestión de Usuarios y Grupos

Sistemas Informáticos

Ciclo Formativo de Grado Superior en Desarrollo de Aplicaciones Web

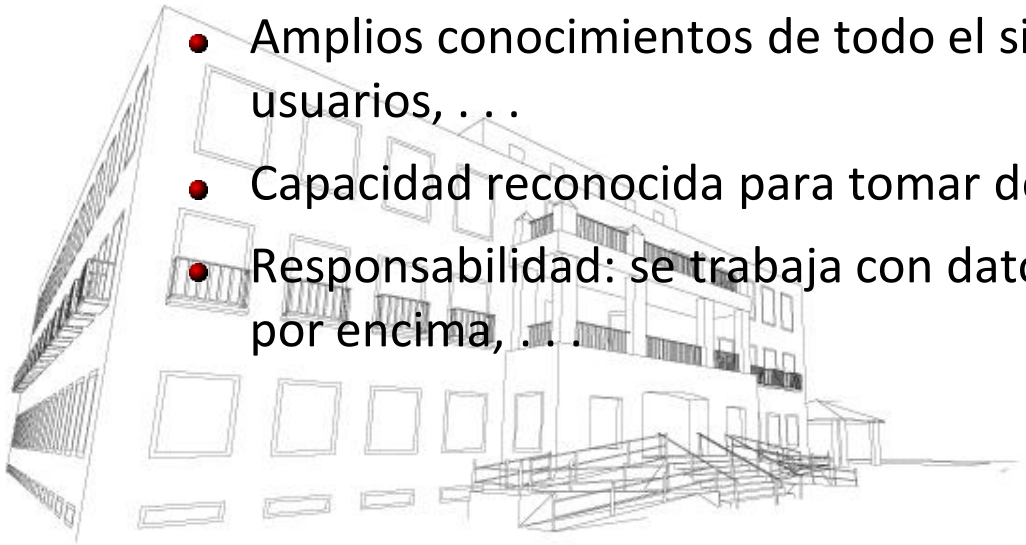
Universidad Católica San Antonio de Murcia - Tlf: (+34) 968 27 88 00
info@ucam.edu - www.ucam.edu

Índice

- Introducción
- Tareas esenciales del administrador de sistemas
- Super-usuario o administrador
- Gestión de Usuarios y Grupos en Linux
- Gestión de Usuarios y Grupos en Windows

Introducción (1/2)

- ¿Quién es el administrador?
  - Persona encargada de configurar y administrar el sistema
  - Ideal) una persona encargada sólo de la administración
  - En ocasiones) compagina su trabajo y el de administración
- ¿Qué se espera del administrador?
  - Amplios conocimientos de todo el sistema: hardware, software, datos, usuarios, . . .
  - Capacidad reconocida para tomar decisiones
  - Responsabilidad: se trabaja con datos muy importantes, hay un jefe por encima, . . .

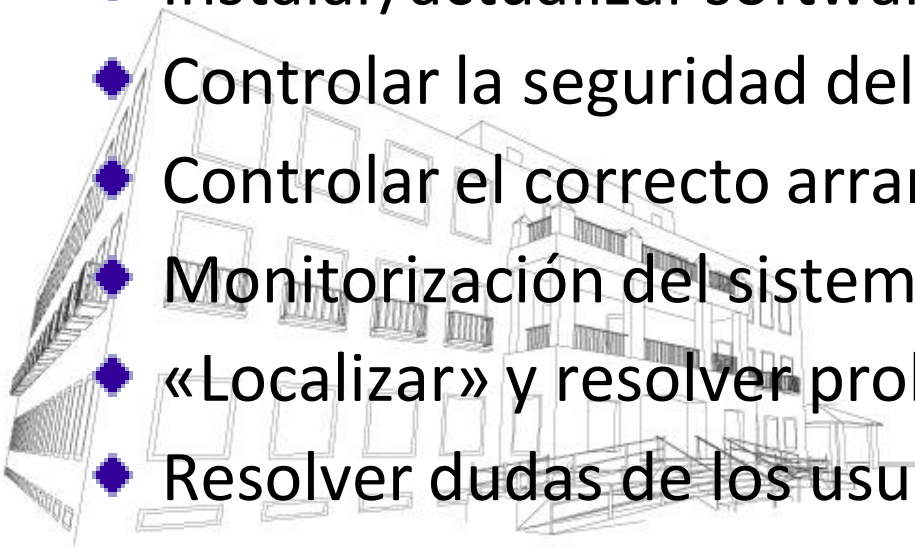


Introducción (2/2)

- Estrategias del administrador:
  - Planearlo antes de hacer los cambios
  - Hacer los cambios reversibles
  - Realizar los cambios incrementalmente
  - Probarlo, probarlo, probarlo antes de hacerlo público
  - Conocer cómo realmente trabajan las cosas
- Al realizar una modicación:
  - Precaución antes de . . .
  - Testear después de . . .
- Es recomendable tener un cuaderno de bitácora para registrar todos los cambios (p.e. /etc/INFORMACION)
- El administrador tiene que tener por un lado autoridad y responsabilidad, por otro servicio y cooperación

Tareas Esenciales del Administrador

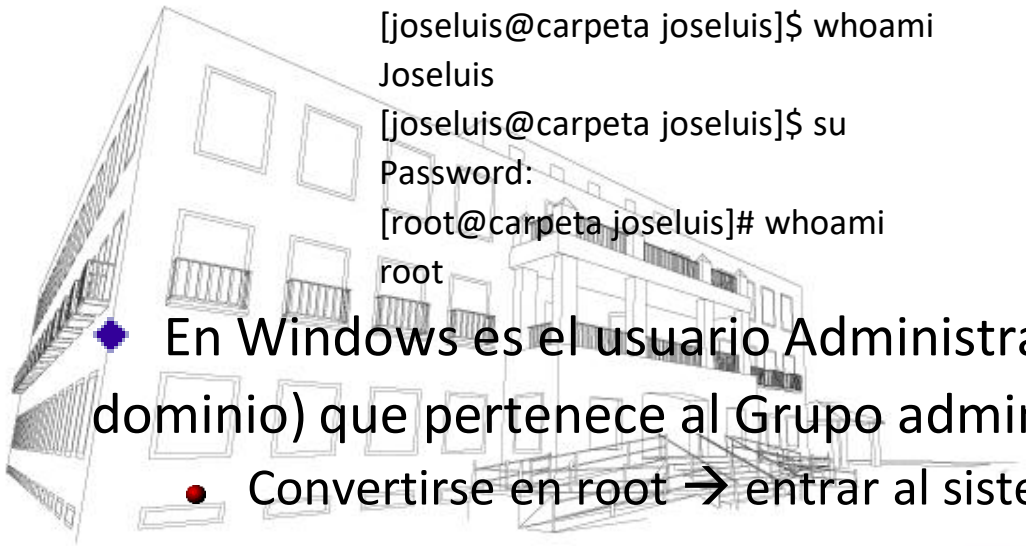
- Añadir nuevos usuarios
- Controlar el rendimiento del sistema
- Realizar las copias de seguridad (y restaurarlas. . .)
- Añadir/eliminar elementos hardware
- Instalar/actualizar software (o desinstalar. . .)
- Controlar la seguridad del sistema
- Controlar el correcto arranque del sistema
- Monitorización del sistema
- «Localizar» y resolver problemas del sistema
- Resolver dudas de los usuarios



Superusuario o Administrador

- El administrador siempre tiene todos los privilegios sobre todos los ficheros, instrucciones y órdenes del sistema
- En Linux es el usuario root que pertenece al grupo root
  - HOME: /root (antiguamente /)
  - Convertirse en root:
    - Entrar al sistema como usuario root
    - Ejecutar orden su → pide la contraseña del root, y lanza un shell como root

```
[joseluis@carpeta joseluis]$ whoami
Joseluis
[joseluis@carpeta joseluis]$ su
Password:
[root@carpeta joseluis]# whoami
root
```

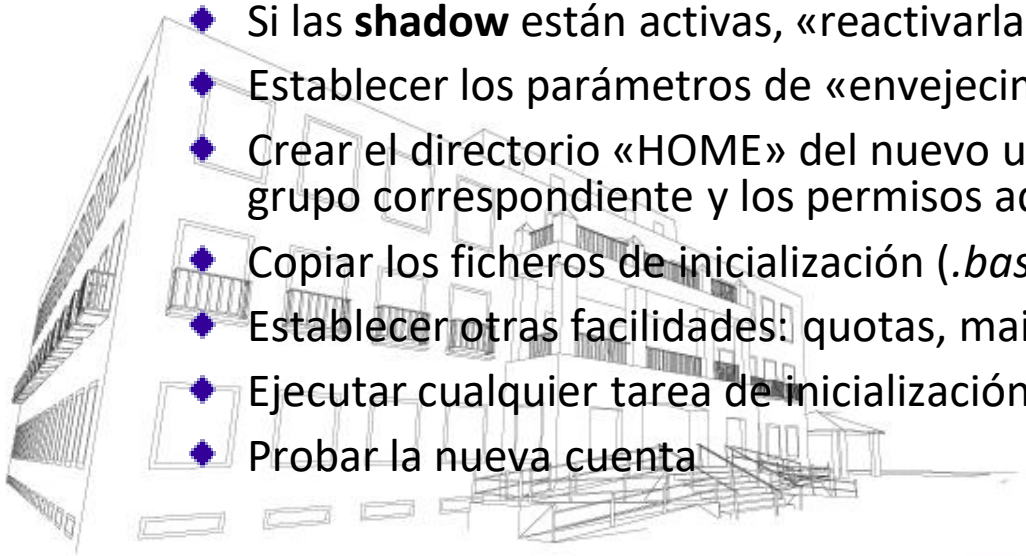


- En Windows es el usuario Administrador (o Administrador de dominio) que pertenece al Grupo administrador
  - Convertirse en root → entrar al sistema como administrador

Usuarios en Linux

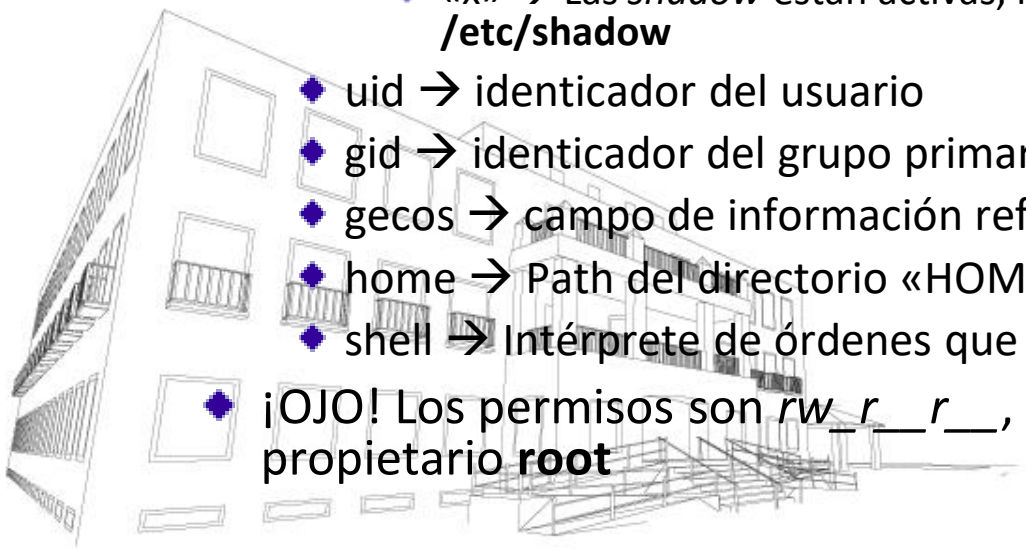
Añadir un nuevo usuario al sistema

- Pasos a realizar (hay herramientas específicas):
  - Decidir el nombre de usuario, el UID, y los grupos a los que va a pertenecer (grupo primario y secundarios)
  - Introducir los datos en los ficheros **/etc/passwd** y **/etc/group** (bloqueando la cuenta para que no pueda ser usada)
  - Asignar un password a la nueva cuenta
  - Si las **shadow** están activas, «reactivarlas»
  - Establecer los parámetros de «envejecimiento» de la cuenta
  - Crear el directorio «HOME» del nuevo usuario, establecer el propietario y grupo correspondiente y los permisos adecuados
  - Copiar los ficheros de inicialización (*.bash_prole*, *.bashrc*, etc.)
  - Establecer otras facilidades: quotas, mail, permisos para imprimir, etc.
  - Ejecutar cualquier tarea de inicialización propia del sistema
  - Probar la nueva cuenta



Usuarios en Linux (II)

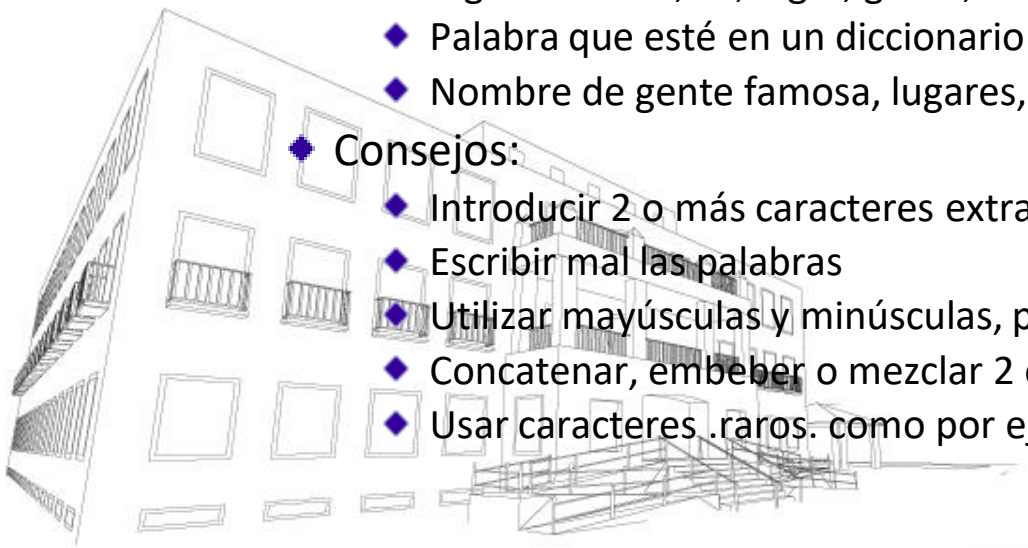
- Fichero/etc/passwd
  - Contiene la lista de usuarios denidos en el sistema
  - Formato:*nombre:password:uid:gid:gecos:home:shell*
    - nombre → Nombre del usuario, **logname** o **username**
    - password → contraseña cifrada o :
      - «*» o «!!» → la cuenta está desactivada
      - «x» → Las *shadow* están activas, la contraseña cifrada se guarda en **/etc/shadow**
    - uid → identicador del usuario
    - gid → identicador del grupo primario al que pertenece
    - gecos → campo de información referente al usuario
    - home → Path del directorio «HOME» del usuario
    - shell → Intérprete de órdenes que se ejecutará al entrar al sistema
  - ¡OJO! Los permisos son *rw_r__r__*, el usuario es el **root** y el grupo propietario **root**



Usuarios en Linux (iii)

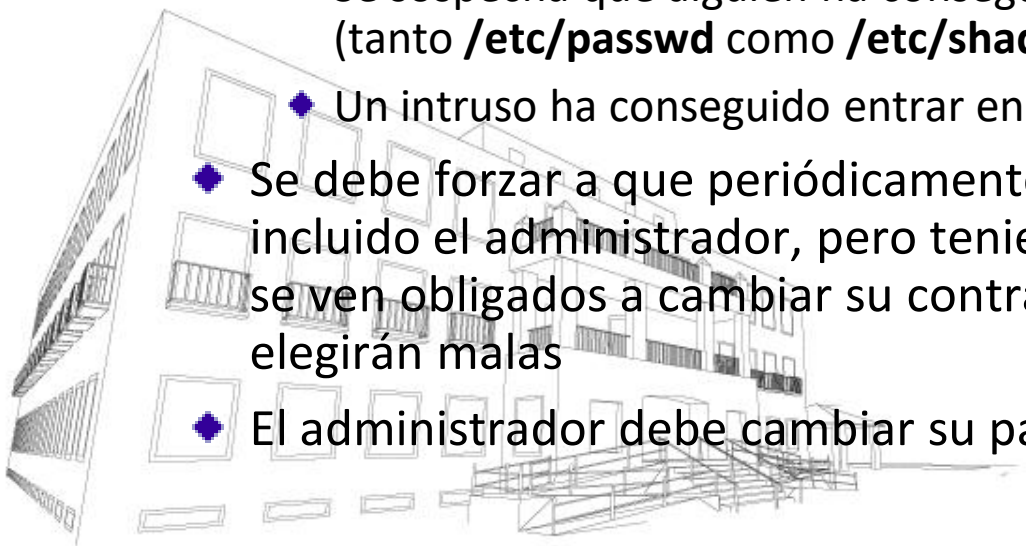
Contraseñas

- **passwd** nombre_usuario) asignar contraseña a un usuario
- A la hora de elegir una buena contraseña:
  - No utilizar como password:
    - Tu nombre o parte de él, de alguien cercano a ti.
    - Nº's significativos para ti o alguien cercano a ti.
    - Algún nombre, nº, lugar, gente, etc., asociado a tu trabajo.
    - Palabra que esté en un diccionario (español, inglés, etc.)
    - Nombre de gente famosa, lugares, películas, relacionadas con publicidad, etc.
  - Consejos:
    - Introducir 2 o más caracteres extras, símbolos especiales o de control
    - Escribir mal las palabras
    - Utilizar mayúsculas y minúsculas, pero no de forma evidente
    - Concatenar, embeber o mezclar 2 o más palabras, o partes de palabras
    - Usar caracteres .raros. como por ejemplo $, &, # , ^



Contraseñas

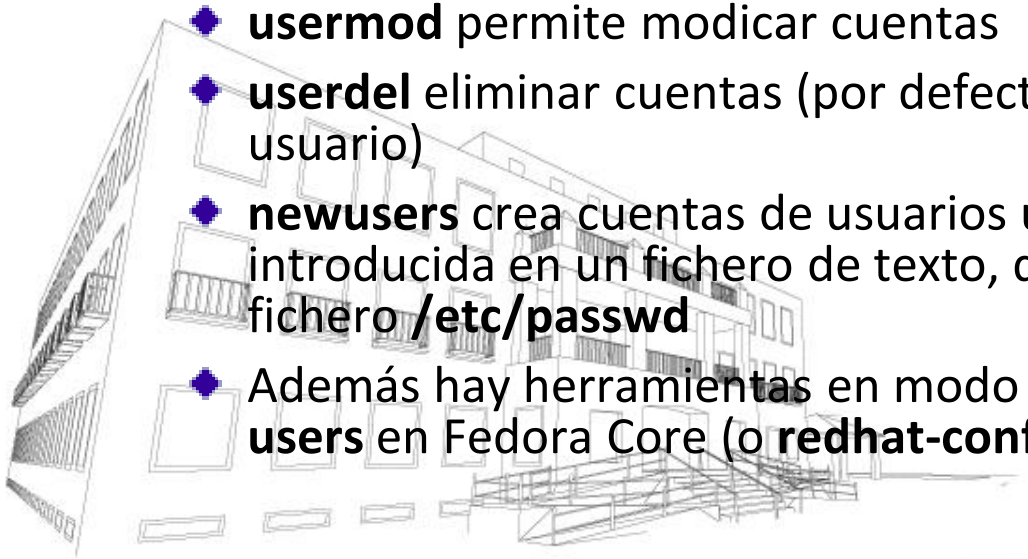
- La contraseña se debe cambiar cuando:
  - Se sospecha que alguien la ha podido conocer o averiguar
  - Un usuario se marcha del trabajo, se deben cambiar todas las que conozca
  - Un administrador del sistema se va: TODAS
  - Se despide a un usuario o a un administrador
  - Se sospecha que alguien ha conseguido el chero con las contraseñas (tanto **/etc/passwd** como **/etc/shadow**)
  - Un intruso ha conseguido entrar en el sistema
- Se debe forzar a que periódicamente se cambien las contraseñas, incluido el administrador, pero teniendo en cuenta, que si los usuarios se ven obligados a cambiar su contraseña con mucha frecuencia, elegirán malas
- El administrador debe cambiar su password de forma periódica



Usuarios en Linux (IV)

Herramientas para crear/modicar cuentas de usuario

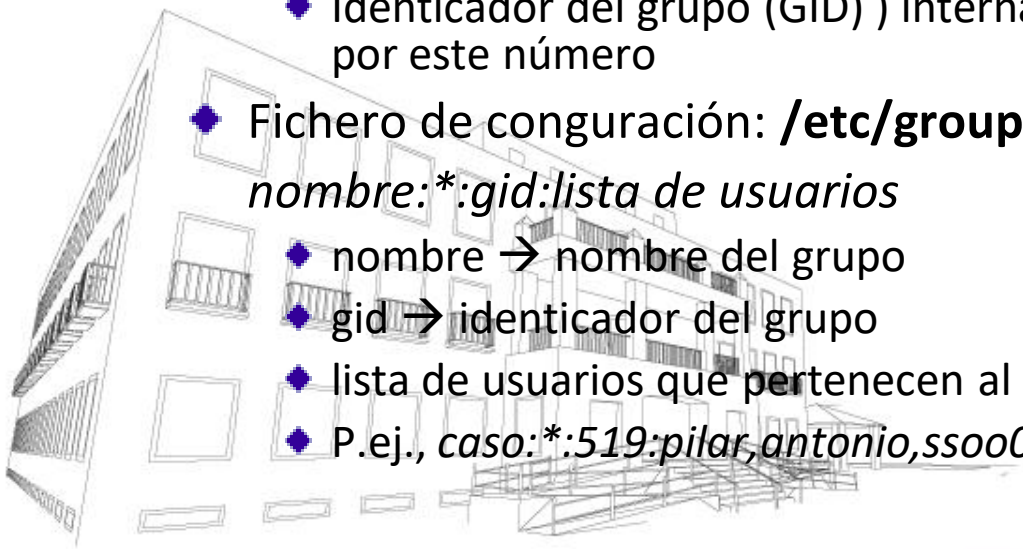
- Las herramientas automáticas para la creación de cuentas de usuario suelen realizar todas las tareas básicas del proceso, a excepción de las especícas (quotas o impresión, etc.)
- La orden **adduser** o **useradd** permite crear cuentas de usuario, o modicar cuentas ya existentes. Toma los valores por defecto de **/etc/default/useradd** y de **/etc/login.defs**
- **usermod** permite modicar cuentas
- **userdel** eliminar cuentas (por defecto no borra el directorio home del usuario)
- **newusers** crea cuentas de usuarios utilizando la información introducida en un fichero de texto, que ha de tener el formato del fichero **/etc/passwd**
- Además hay herramientas en modo gráfico, como **system-config-users** en Fedora Core (o **redhat-config-users** de RedHat)



Grupos en Linux

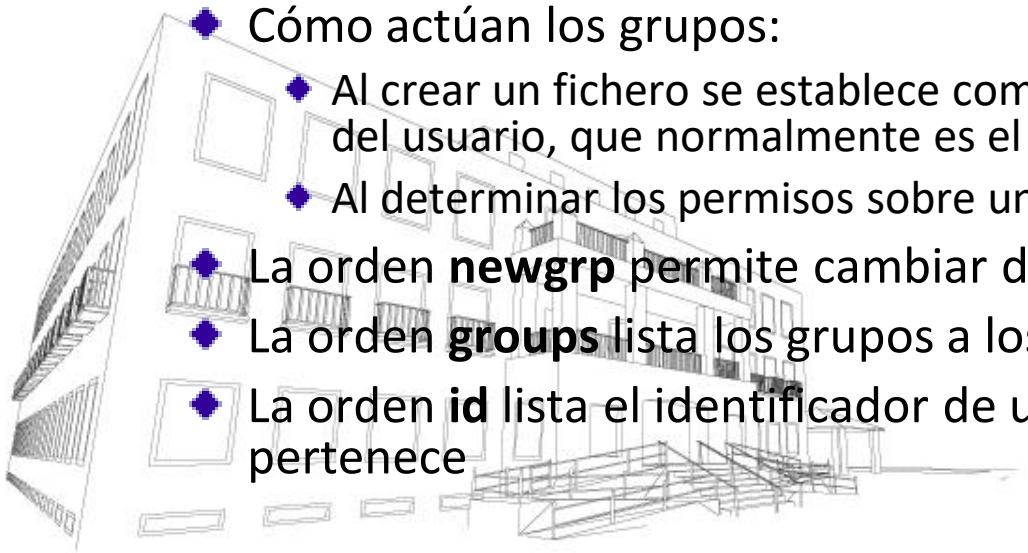
- Los grupos son «colecciones» de usuarios que comparten recursos o ficheros del sistema
- Con los grupos se pueden garantizar permisos concretos para un conjunto de usuarios, sin tener que repetirlos cada vez que se desee aplicarlos
- Características de un grupo
  - Nombre del grupo, o *groupnam*
  - Identicador del grupo (GID)) internamente el sistema identica al grupo por este número
- Fichero de conguración: **/etc/group**, con el formato:

  nombre::gid:lista de usuarios*
  - nombre → nombre del grupo
  - gid → identicador del grupo
  - lista de usuarios que pertenecen al grupo, separados por «,»
  - P.ej., *caso:*:519:pilar,antonio,ssoo001,aso01,aso02,aso03*



Grupos en Linux (II)

- Definición:
  - Implícita: nuevo GID en el 4º campo de **/etc/passwd**
  - Explícita: nueva entrada en **/etc/group**
- Tipos de grupos:
  - **Primario** → el grupo especificado en el fichero **/etc/passwd**
  - **Secundarios** → el resto de grupos al que pertenece el usuario, indicados en **/etc/group**
- Cómo actúan los grupos:
  - Al crear un fichero se establece como grupo propietario el grupo activo del usuario, que normalmente es el primario
  - Al determinar los permisos sobre un fichero se usan todos sus grupos
- La orden **newgrp** permite cambiar de grupo activo
- La orden **groups** lista los grupos a los que pertenece un usuario
- La orden **id** lista el identificador de usuario junto a los grupos a los que pertenece



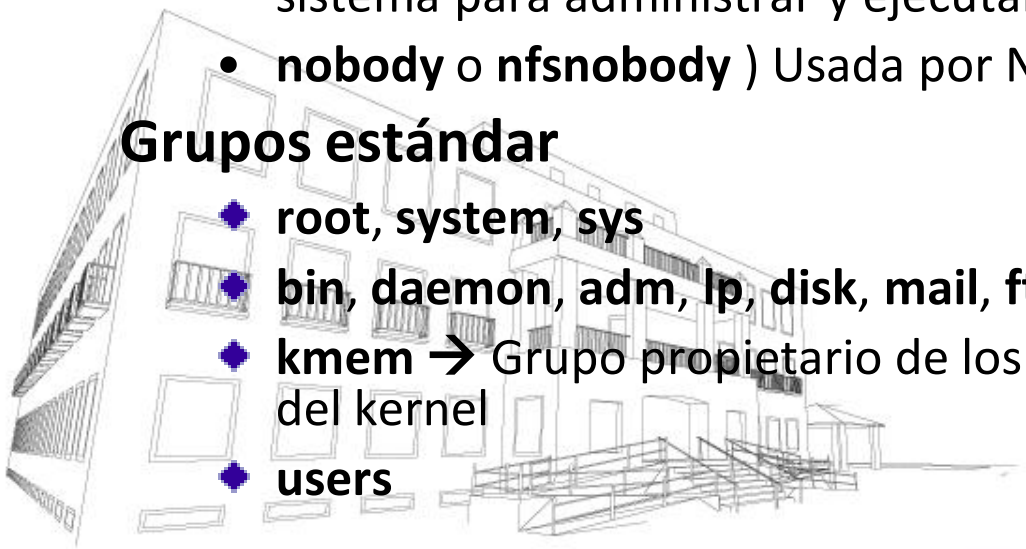
Usuarios y Grupos en Linux

Usuarios estándar

- **root** → Cuenta del administrador
- **bin**, **daemon**, **lp**, **sync**, **shutdown**, etc. → Tradicionalmente usados para poseer ficheros o ejecutar servicios
- **mail**, **news**, **ftp** → Asociados con herramientas o facilidades
- **postgres**, **mysql**, **xfs** → Creadas por herramientas instaladas en el sistema para administrar y ejecutar sus servicios
- **nobody** o **nfsnobody**) Usada por NFS y otras utilidades

Grupos estándar

- **root**, **system**, **sys**
- **bin**, **daemon**, **adm**, **lp**, **disk**, **mail**, **ftp**, **nobody**, etc.
- **kmem** → Grupo propietario de los programas para leer la memoria del kernel
- **users**



La Configuración del SO en Windows

LOS PERFILES DE USUARIO

Un **perfil de usuario** es una de las herramientas más potentes de Windows para configurar el entorno de trabajo de los usuarios de red.

Se puede especificar el aspecto del Escritorio, la barra de tareas, el contenido del menú Inicio, etc., incluidos programas o aplicaciones.

Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo, y aquellos usuarios que acceden a varias estaciones pueden tener un perfil en cada una de ellas. Este perfil se denomina **perfil local** porque solo es accesible desde la estación en que está creado.

Además, existe un **perfil temporal** que se crea cuando se produce un error en la carga del perfil del usuario. Éste se elimina al final de la sesión y no se almacenan los cambios realizados por el usuario en la configuración del *Escritorio* y los archivos.

La Configuración del SO en Windows

LOS PERFILES DE USUARIO

Los usuarios que se conectan a un servidor Windows pueden tener también perfiles en dicho servidor. De esta manera, se puede acceder al perfil independientemente de la estación en que se esté conectado. Este perfil se denomina **perfil de red** y hay varios tipos :

- **Perfil móvil**: este tipo de perfil es asignado a cada usuario por los administradores pero puede ser modificado por el usuario y los cambios permanecerán después de finalizar la conexión.
- **Perfil obligatorio**: este tipo de perfil es igual que el perfil móvil pero asegura que los usuarios trabajen en un entorno común. Por tanto, puede ser modificado por el usuario pero los cambios realizados se pierden al finalizar la conexión. Solo pueden ser modificados y guardados sus cambios por los administradores**.**
- **Perfil superobligatorio**: este tipo de perfil que únicamente está disponible en Windows Server 2008, es igual que el obligatorio pero con un nivel superior de seguridad. Cuando el usuario se conecta al servidor, si no se puede cargar este perfil, no se le permitirá conectarse, es decir, no se le cargará el perfil temporal.

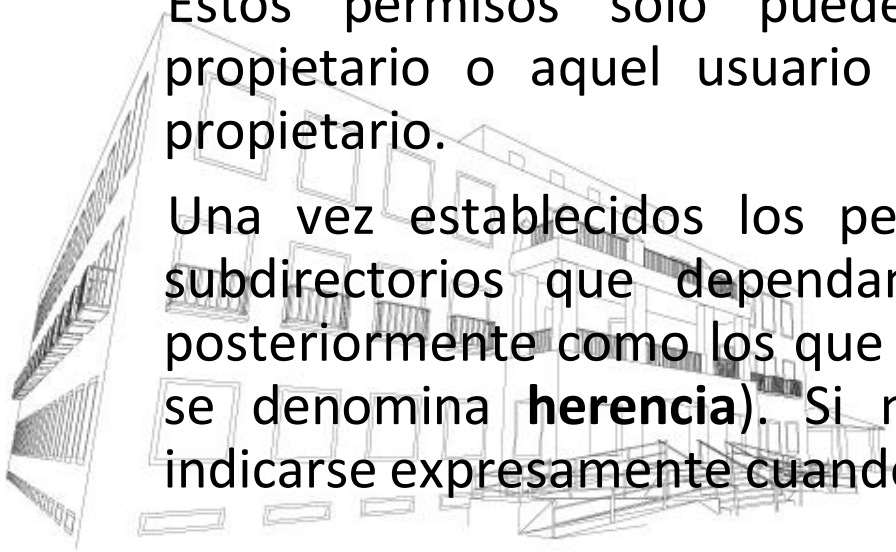
La Configuración del SO en Windows

LOS PERMISOS DE DIRECTORIOS

Cuando se establecen los permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos.

Estos permisos solo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él, tanto los que se creen posteriormente como los que ya existían previamente (este hecho se denomina **herencia**). Si no desea que se hereden, deberá indicarse expresamente cuando se indiquen los permisos.



La Configuración del SO en Windows

LOS PERMISOS DE DIRECTORIOS

Solo es posible establecer permisos para directorios de unidades formateadas con el sistema NTFS.

Los permisos estándar para directorios que se pueden conceder o denegar son:

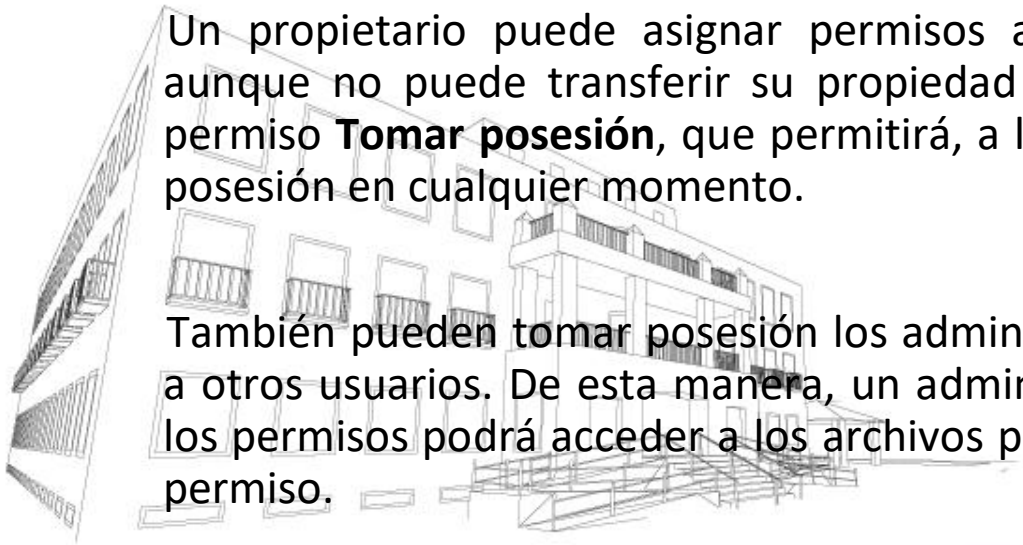
- **Control total**: es el máximo nivel y comprende poder realizar todas las acciones tanto a nivel de archivos como de directorios.
- **Modificar**: comprende todos los permisos menos eliminar archivos y subdirectorios, cambiar permisos y tomar posesión.
- **Lectura y ejecución**: comprende ver los nombres de los archivos y subdirectorios, ver los datos de los archivos, ver los atributos y permisos y ejecutar programas.
- **Mostrar el contenido de la carpeta**: comprende los mismos permisos que **lectura y ejecución** pero aplicables solo a las carpetas.
- **Leer**: comprende ver los nombres de los archivos y directorios, ver los datos de los archivos, así como ver los atributos y permisos.
- **Escribir**: comprende crear archivos y subdirectorios, añadir datos a los archivos, modificar los atributos y leer los permisos.
- **Permisos especiales**: se activa cuando se indican permisos más concretos.

Estos permisos son acumulables pero denegar el permiso **Control total** elimina todos los demás.

La Configuración del SO en Windows

EL PROPIETARIO DE UN DIRECTORIO

Cuando un usuario crea un directorio, un archivo o cualquier objeto, se convierte automáticamente en su propietario (también durante el proceso de instalación se adjudicaron propietarios a todos los directorios y archivos que se crearon).



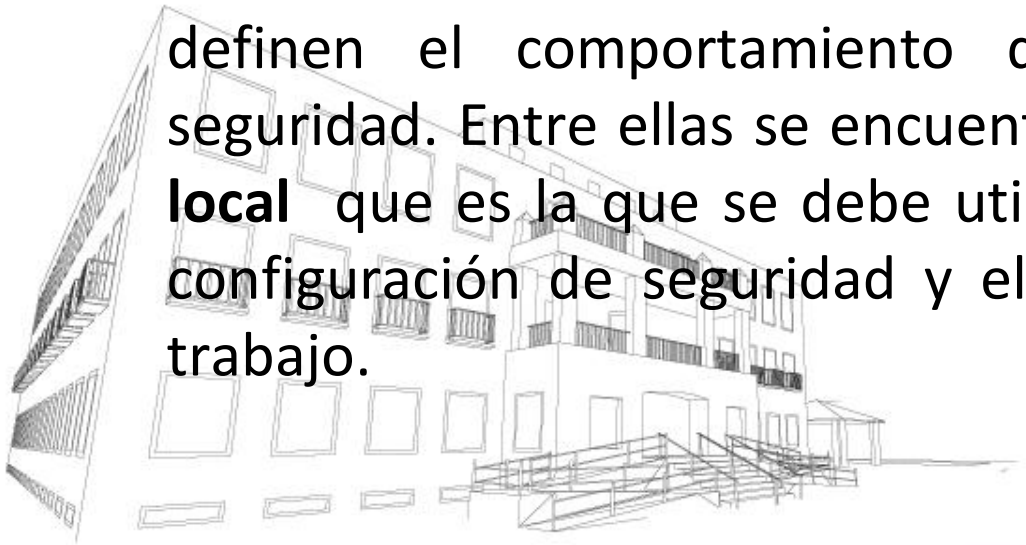
Un propietario puede asignar permisos a sus directorios, archivos u objetos aunque no puede transferir su propiedad a otros usuarios. Puede conceder el permiso **Tomar posesión**, que permitirá, a los usuarios que se les conceda, tomar posesión en cualquier momento.

También pueden tomar posesión los administradores pero no pueden transferirla a otros usuarios. De esta manera, un administrador que tome posesión y cambie los permisos podrá acceder a los archivos para los que no tiene concedido ningún permiso.

La Configuración del SO en Windows

LAS DIRECTIVAS LOCALES

En Windows, los derechos se han agrupado en un conjunto de reglas de seguridad y se han incorporado en unas consolas de administración denominadas **directivas de seguridad** que definen el comportamiento del sistema en temas de seguridad. Entre ellas se encuentra la **Directiva de seguridad local** que es la que se debe utilizar si se desea modificar la configuración de seguridad y el equipo es una estación de trabajo.

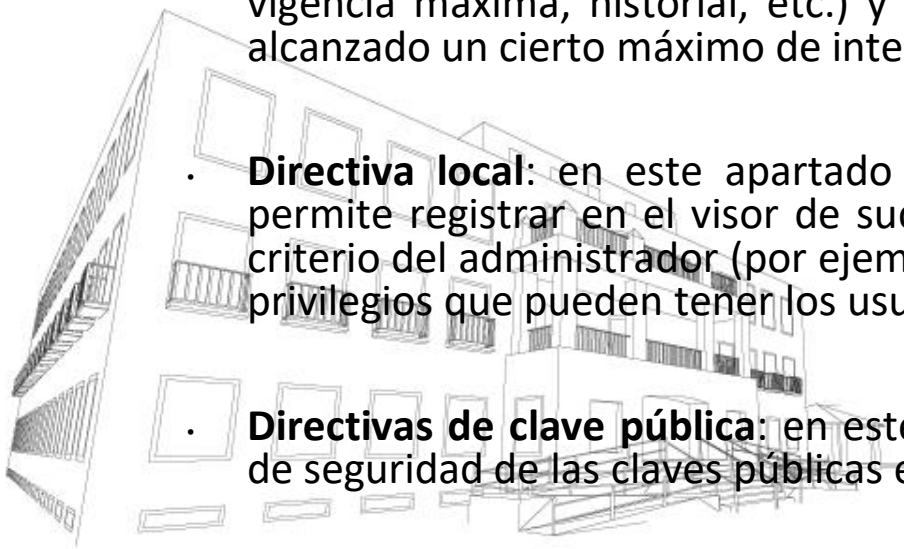


La Configuración del SO en Windows

LAS DIRECTIVAS LOCALES

Desde ellas se pueden establecer, entre otras, las siguientes directivas:

- **Directivas de cuentas**: en este apartado se puede establecer cuál es la política de cuentas o de contraseñas que se seguirá. Dentro de este apartado se pueden distinguir reglas en dos grupos: **Contraseñas** y **Bloqueo**. Entre ellas, hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión.



- **Directiva local**: en este apartado se encuentran: la **Auditoría** del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, los inicios de sesión local), y los derechos y privilegios que pueden tener los usuarios en el equipo.

- **Directivas de clave pública**: en este apartado se pueden administrar las opciones de seguridad de las claves públicas emitidas por el equipo.