

## 4.-Gestion-de-usuarios.pdf



user\_2269691



Programación y Administración de Sistemas



2º Grado en Ingeniería Informática



Escuela Politécnica Superior de Córdoba  
Universidad de Córdoba

WUOLAH + BBVA

Hazte **cliente de BBVA y...**  
**ahórrate 6 meses**  
**de suscripción**

BOOM

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

Ahora, si te abres una Cuenta Online en BBVA, te reembolsamos una de estas suscripciones durante 6 meses (hasta 9,99€/mes) al pagarla con tu tarjeta Aqua Débito

NETFLIX

Spotify

HBOmax

Disney+

PlayStation Plus

DAZN

Promoción solo para nuevos clientes de BBVA. Válida hasta el 30/06/2023. Estas empresas no colaboran en la promoción.

Abre tu cuenta



# Hazte cliente de BBVA y ... ahórrate 6 meses de suscripción

WUOLAH  
+ BBVA

NETFLIX

Spotify

HBOmax

Disney+

PlayStation.Plus

DAZN

Ahora, si te abres una Cuenta Online en BBVA, te reembolsamos una de estas suscripciones durante 6 meses (hasta 9,99€/mes) al pagarla con tu tarjeta Aqua Débito

Promoción solo para nuevos clientes de BBVA. Válida hasta el 30/06/2023. Estas empresas no colaboran en la promoción.

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

## Usuario:

- Persona que trabaja en el sistema, editando ficheros, ejecutando programas
- Pseudo-usuario: entidad que sin ser una persona puede ejecutar programas o poseer ficheros (usado para servicios o tareas automatizadas)

## Información mínima de un usuario

- Nombre de usuario (logname)
- Identificador de usuario (UID) (sist. trabaja con UID)
- Identificadores a los grupos que pertenece (GIDs)

## Ficheros básicos

- `/etc/passwd`: información de cuentas de usuario
- `/etc/shadow`: contraseñas cifradas con hash
- `/etc/group`: definición de los grupos y usuarios miembros
- `/etc/gshadow`: passwords de los grupos cifradas

## Usuarios

### Fichero `/etc/passwd`

- Contiene la lista de usuarios del sistema y sus contraseñas
- Formato: `nombre:password:uid:gid:gecos:home:shell`
  - `nombre`: nombre del usuario (username)
  - `password`: contraseña cifrada o:
    - `*` o `!!`: contraseña bloqueada
    - `x`: shadow está activa
  - `uid`: identificador del usuario
  - `gid`: identificador del grupo primario
  - `gecos`: campo de información del usuario (nombre, telefono, etc.)
  - `home`: path del directorio `$HOME`
  - `shell`: interprete de órdenes
- Propietario `root:root`
- Permisos son `rw-r--r--`
- `/usr/sbin/vipw`: modificar manualmente
- `pwck`: verificar integridad de `/etc/passwd` y `/etc/shadow`



Abre tu cuenta



WUOLAH  
+ BBVA

WUOLAH

- Se permite acceso al fichero `/etc/passwd` en modo lectura para leer info del usuario, pero no se debe permitir acceso al fichero con las passwords (aunque esten cifradas)

## Contraseñas

- `passwd <usuario>`: asignar contraseñas a un usuario
- Elección de una contraseña adecuada
- No utilizar:
  - Contraseñas más usadas
  - Tu nombre, parte de el o alguien cercano
  - Numeros significativos para ti o cercano a ti
  - Nombre, nº, lugar o persona relacionados con tu trabajo
  - Nombres de gente famosa, lugares, películas, publicidad
  - Palabras en el diccionario
- Consejos sin políticas absurdas
  - Introducir 2 o mas caracteres extra, simbolos especiales
  - Escribir mal las palabras
  - Utilizar mayúsculas y minúsculas, sin ser evidente
  - Concatenar o mezclar 2 o mas palabras
  - Caracteres poco comunes
- Contraseñas se deben de cambiar cuando:
  - Sospechas de acceso no autorizado
  - Sospecha que se ha accedido al fichero `/etc/passwd` o `/etc/shadow`
  - Usuario se marcha del trabajo
  - Administrador se va
  - Intrusión
- Periodicamente se debe de forzar a los usuarios que cambien las contraseñas
  - Mala cosa: con mucha frecuencia → llevar a contraseñas poco seguras

## Shadow passwords

- Permite que las contraseñas cifradas se guarden en un fichero más seguro
- `/etc/shadow` → `rw-----` → `root:root`
- Guarda para cada usuario del sistema la contraseña cifrada con su info de envejecimiento
- Para aquellos usuarios que tengan una `x` en `/etc/passwd`
- Activadas por defecto y se actualizan automáticamente



# Hazte cliente de BBVA y ... **ahórrate 6 meses** **de suscripción**

Ahora, si te abres una Cuenta Online en BBVA, te reembolsamos una de estas suscripciones durante 6 meses (hasta 9,99€/mes) al pagarla con tu tarjeta Aqua Débito

**NETFLIX****HBOmax** **Spotify** **PlayStation.Plus**[Abre tu cuenta](#)

- Estructura: `nom:pass:changed:minlife:maxlife:warn:inactive:expired:unused`
  - `nom`: nombre de usuario, loginname
  - `pass`: contraseña cifrada
- Comandos de actualización
  - `pwconv` → crear y actualizar shadow
  - `pwunconv` → desactivar shadow
- Cifrar shadow → algoritmos criptográficos de resumen
  - Mensaje secreto es la contraseña (`C`)
  - Salt (`S`) es una palabra aleatoria que se concatena a los bytes de la contraseña - > dificulta ataques a través de diccionarios
  - Concat (`C, S`), calcula el resumen `F = H(C, S)` y almacena `S` y `F`
  - Cuando usuario introduce contraseña (`C'`) se repite todo el proceso (`F'`)
  - Si `F == F'`, el usuario puede acceder al sistema
- Propiedades desables de función resumen
  - Con `C` sea facil calcular `H(C)` → coste computacional no sea alto
  - Con `H(C)` sea dificil calcular `C` → contraseñas originales no se pueden conocer sabiendo el resumen
  - Dado `C` sea dificil encontrar otro mensaje `C'` que `H(C) == H(C')` → dos usuarios no terminen con la misma contraseña
- Funciones de dispersión de un solo sentido
- Cifrados del shadow
  - `$1$` es MD5
  - `$2a$` es Blowfish
  - `$2y$` es Blowfish
  - `$5$` es SHA-256
  - `$6$` es SHA-512

## Algoritmos de hash

### MD5 (Message-Digest algorithm 5)

- Aplica funciones no lineales a los 17 segmentos de 32 bits de un bloque de 512 bits
- Resumen de 128 bits
- **SHA (Secure Hash Algorithm)**
- Estandar del NIST
- Genera resúmenes mas grandes que MD5, mas seguro contra ataques fuerza bruta
- Se pueden considerar 160, 224, 256, 384 o 512 bits para el resumen.

### Restricciones de tiempo



# Hazte cliente de BBVA y ... ahórrate 6 meses de suscripción

WUOLAH  
+ BBVA

NETFLIX

Spotify

HBOmax

Disney+

PlayStation.Plus

DAZN

Ahora, si te abres una Cuenta Online en BBVA, te reembolsamos una de estas suscripciones durante 6 meses (hasta 9,99€/mes) al pagarla con tu tarjeta Aqua Débito

Promoción solo para nuevos clientes de BBVA. Válida hasta el 30/06/2023. Estas empresas no colaboran en la promoción.

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

- Introducir restricciones de tiempo o envejecimiento para la validez de la cuenta o de la contraseña.
  - `changed` ⇒ fecha del último cambio de contraseña.
  - `minlife` ⇒ nº de días que han de pasar para poder cambiar la contraseña.
  - `maxlife` ⇒ nº de días máximo que puede estar con la misma contraseña sin cambiarla.
  - `warn` ⇒ cuántos días antes de que la contraseña expire (`maxlife`) el usuario será informado sobre ello, indicándole que tiene que cambiarla.
  - `inactive` ⇒ nº de días después de que la contraseña expire en que la cuenta se deshabilitará si no ha sido cambiada.
  - `expired` ⇒ fecha en la que la cuenta expira y se deshabilita de forma automática.
- Comando `chage` para modificar las restricciones de tiempo de un usuario

## Ficheros de inicialización y cierre

- `/etc/skel/` → ficheros que se copian automáticamente a cada `$HOME`
- Ficheros inicialización son scripts shell que realizan tareas como dar valores a variables, nombrar alias, realizar funciones específicas.
- Los ficheros dependen del intérprete de ordenes seleccionado: `sh`, `bash`, `csh`
- Incluyen en el PATH, variables de entorno, `umask`, funciones de inicialización, alias, var. shell...
- Normal es que lean parte de su contenido de algún fichero global
- `bash_profile` en bash, `.profile` en bash/sh, `.login` en csh
- `.bashrc`/`.cshrc` cada vez que se ejecuta un shell
- `.bash_logout` en bash, `.logout` en csh

## Selección intérprete de órdenes

- Último campo `/etc/passwd` se establece el intérprete
- Fichero `/etc/shells` define los permitidos
- Un usuario puede cambiar su shell con `chsh`
- Si un usuario no tiene un shell asignado, usará `/bin/sh`
- `/bin/false` y `/sbin/nologin` para evitar que un usuario no pueda iniciar sesión
- Fichero ejecutable como shell
  - Abre la aplicación cuando entra al sistema y al finalizar sale del sistema

## Cuentas

- `rbash` es un enlace simbólico a `bash -r`

WUOLAH  
+ BBVA

WUOLAH

- Interprete normal, pero no deja hacer determinadas tareas
  - Cambiar directorio
  - Establecer valores de `$PATH` o `$HOME`
  - Especificar nombres u órdenes que contengan `/`
  - Usar redirección
  - Utilizar la orden `exec` para reemplazar el shell por otro programa
- A esos usuarios hay que limitarles los ficheros que pueden ejecutar, copiandolos a un directorio y que su `$PATH` sea sólo ese directorio. Con un `$PATH` normal sería igual que no tener restricciones.

## Nuevos usuarios al sistema (pasos a realizar)

1. Decidir nombre de usuario, UID, y grupos a los que va a pertenecer
2. Introducir los datos en `/etc/passwd` y `/etc/group`, poniendo como contraseña `*`
3. Asignar contraseña a la cuenta nueva
4. Si los shadow están activados, escribir la contraseña
5. Establecer parámetros de envejecimiento de la cuenta
6. Crear directorio `$HOME`
7. Copiar ficheros necesarios por defecto  
Opcional:
8. Establecer otras facilidades: quota, mail, permisos
9. Ejecutar cualquier tarea de inicialización
10. Probar nueva cuenta

## Herramientas:

- `adduser` o `useradd`: crear usuarios
- `usermod`: modificar cuentas
- `deluser` o `userdel`: quitar cuentas
- `newusers`: batch import nuevos usuarios con un fichero de sintaxis similar a `/etc/passwd`
- `users-admin`: herramienta en modo grafico

## Grupos

- Tipos de grupos
  - Primarios: guardados en `/etc/passwd`
  - Secundarios: indicados en `/etc/group`
- Funcionamiento de los grupos

- Al crear un fichero, se establece como propietario el grupo activo del usuario en ese momento
- Grupo activo: grupo primario
- Al determinar los permisos sobre un fichero, se usan todos los grupos del usuario

## Contraseñas (opt.)

- Poco usada
- Grupos pueden tener contraseña `/etc/gshadow`
  - Si usuario conoce la contraseña del grupo puede usarlo sin unirse a el
  - Información en `/etc/gshadow`: grupo, contraseña, admin users (pueden cambiar contraseña y añadir usuarios) y miembros (idea parecia a `/etc/shadow`)

## Herramientas

- `addgroup`: añadir grupo
- `groupmod`: modificar grupo
- `delgroup`: quitar grupo
- `groups`: ver grupos de un usuario
- `id`: listar identificador de usuario y grupos a los que pertenece
- `grpck`: comprobar consistencia de fichero de grupos

## Usuarios y grupos estándar

### Rangos del UID

- 0-99: Usuarios pertenecientes al SO
- 100-499: Usuarios especiales que representan servicios/programas
- | = 1000: Usuarios normales

## Algunos usuarios y grupos estándar

- Usuarios estándar
  - `root` (0): cuenta del administrador
  - `bin` (1): utilidades comunes de usuarios
  - `daemon` (2): ejecución de demonios
  - `mail`, `news`, `ftp`: asociados a utilidades



Hazte cliente de BBVA y ...

**ahórrate 6 meses de suscripción**

**WUOLAH**  
+ BBVA

**NETFLIX**

**Spotify**

**HBOmax**

**Disney+**

**PlayStation.Plus**

**DAZN**

Ahora, si te abres una Cuenta Online en BBVA, te reembolsamos una de estas suscripciones durante 6 meses (hasta 9,99€/mes) al pagarla con tu tarjeta Aqua Débito

Promoción solo para nuevos clientes de BBVA. Válida hasta el 30/06/2023. Estas empresas no colaboran en la promoción.

**1/6**

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

- `postgres`, `mysql`, `xfp`: creados por herramientas instaladas para administrar y ejecutar sus servicios
- `nobody` o `nfsnobody`: usado por NFS y otras utilidades, usuario sin privilegios
- Grupos estándar
  - `root`, `sys`
  - `bin`, `daemon`, `lp`, `disk`, `mail`, `ftp`, `nobody`, etc
  - `kmem`: grupo propietario de los programas para leer la memoria del kernel
  - `user` o `users`: grupo de los usuarios normales (no siempre usado)



Abre tu cuenta



**WUOLAH**  
+ BBVA

**WUOLAH**