

WUOLAH



IreneCR2

www.wuolah.com/student/ireneCR2



7798

Ejercicios PAS.pdf

EJERCICIOS RESUELTOS TEMAS PAS



2º Programación y Administración de Sistemas



Grado en Ingeniería Informática



**Escuela Politécnica Superior de Córdoba
UCO - Universidad de Córdoba**

 **escuela
de negocios**
CÁMARA DE SEVILLA

MÁSTER EN DIRECCIÓN Y GESTIÓN DE RECURSOS HUMANOS

www.mastersevilla.com

Inscríbete



BECAS

TEMA 1 – INTRODUCCIÓN A LA ADMINISTRACIÓN DE SISTEMAS:**1. Preguntas teóricas tipo test:****a) ¿Qué son las notificaciones CERT?**

- ☒ Notificaciones periódicas relativas a problemas de seguridad.
- ☐ Un tipo de ataque contra la seguridad del sistema.
- ☐ Petición de certificado digital que los usuarios del sistema realizan al administrador.

b) El soporte a usuarios es una tarea básica del Administrador de Sistemas:

- ☒ Verdadero
- ☐ Falso

c) ¿Qué aspectos cubre la seguridad informática en una organización?

- ☐ Protección física de las instalaciones que alojan el Sistema Informático.
- ☐ Protección *software* del Sistema Informático.
- ☒ Protección física de las instalaciones y protección *software* del Sistema Informático.

d) ¿Cuál es la labor del Responsable de Informática dentro del Departamento de Informática?

- ☒ Es el punto de unión que traduce las necesidades de la empresa a las posibles labores que se llevan a cabo en el Departamento de Informática.
- ☐ Es el que dirige todos los proyectos del Departamento de Informática.
- ☐ Es el responsable del equipo de desarrollo de *software* específico dentro de la empresa.

2. Obtenga información acerca de SNORT.

SNORT es un sistema de detección de intrusos en red, libre y gratuito. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

3. ¿A qué hace referencia “la catedral y el bazar”?

La catedral (estructura jerárquica) y el bazar (estructura de más libre albedrío (idea de software libre)) es un ensayo sobre el software de código abierto, escrito por el hacktivista Eric S. Raymond en 1997. Ha tenido dos secuelas tituladas “*Colonizando la noosfera*” y “*El caldero mágico*”.



Striking Vipers - black mirror



Toy Story 4



Segunda temporada de Dark

Próximos estrenos de series y películas.

Se acercan las vacaciones de verano y es el mejor momento de disfrutar de la televisión.

Las vacaciones ya están aquí. Si no has tenido mucho tiempo libre para ver cine y televisión ahora es tu momento. Muchos han sido los estrenos este 2019 que han movido las masas de fans. Sin embargo, las puertas al verano no van a dejar indiferente al espectador.

Si durante el curso no has visto nada desde el verano pasado, siempre puedes continuar todas la series acumuladas. Pero por si no estás al día, aquí os dejamos algunos estrenos próximos:

- **Aladdín.** Disney no nos dejará indiferente con la versión real de Aladdín. Esta historia de amor que todos conocemos ha saltado a la gran pantalla el 24 de mayo, y aún tienes tiempo para ir a verla. El dato más fascinante de este estreno es que el mago más pícaro de todo cuento está interpretado por Will Smith.

- **Black Mirror.** Desde el estreno de su película interactiva Bandersnatch en diciembre de 2018, Black Mirror se ha mantenido ausente hasta el estreno de la quinta temporada. La serie de antología que saca el lado más oscuro de la tecnología actual, ha dado paso con su última temporada a tres nuevos episodios el pasado 5 de junio.

Aladdín entre las películas de estreno más taquilleras.

- **El cuento de la criada.** Esta serie dramática basada en el premiado best-seller de Margaret Atwood, que muestra la lucha contra la antigua sociedad totalitaria de Estados Unidos, ha lanzado su tercera temporada también el 5 de junio.

- **X-Men: Dark Phoenix.** Basada en el personaje de Fénix Oscura, esta nueva entrega de los X-Men dió el salto a la gran pantalla el pasado viernes 7 de junio. Un dato relevante es que su protagonista está interpretada por Sophie Turner, que encarna el personaje de Sansa en Juego de Tronos.

- **Jessica Jones.** Volvemos con Marvel, esta vez en la televisión. La tercera y última temporada de la superheroína y detective Jessica Jones, ambientada en el Universo Cinematográfico de Marvel (UCM), se estrenará el próximo 14 de junio.

- **Toy Story 4.** Si eras un niño cuando se estrenó por primera vez Toy Story estamos seguros de que esta saga es especial para ti. La saga de animación sobre los juguetes más rebeldes no deja indiferente a ningún niño, joven o adulto. Por ello, Toy Story llega con más fuerza que nunca con su cuarta película, que tiene previsto su estreno el 21 de junio.

- **Stranger things.** La serie de ciencia ficción que ha dado vida al mitológico Demogorgon y protagonizada por Winona Ryder entre muchos otros actores, ha

La Casa de Papel, éxito mundial en numerosos países.

vuelto con su tercera temporada. Después de 2 temporadas de puro éxito, la serie vuelve a la pantalla el 4 de julio.

- **Spider-man: Far From Home.** Después del ansiado desenlace de Vengadores: Endgame llega Spider-man: Lejos de Casa. La segunda parte de Spider-man: Homecoming se estrenará el próximo 5 de julio. ¿Cómo se encuentra Peter Parker después de lo ocurrido? ¿A qué nuevos retos deberá enfrentarse?

- **La Casa de Papel.** Los delincuentes más gamberro ahora tienen competencia: la inspectora Sierra. La tercera temporada tiene previsto su estreno el próximo 19 de julio. ¿Quién ganará esta batalla? ¿la inspectora Alicia Sierra o la aclamada resistencia?

- **El Rey León.** Sin duda, el largometraje con el que Disney quiere despertar nuestro sentimiento más profundo es El Rey León. También próximamente estrenada el 19 de julio, esta película sobre el fantástico reino animal y la vida del León Simba nos dejará con la boca abierta. Una maravilla obligatoria.

- **Dark.** La segunda temporada de esta webserie de tipo drama sobrenatural se estrenará el 21 de junio. A tan sólo 1 semana y 3 días para conocer más sobre los oscuros secretos que guardan estas cuatro familias alemanas que ponen de manifiesto el pasado de una ciudad.

Wuolah Giveaway

Impresora y escáner Canon. Es momento de imprimir tus apuntes. Participa y llévate esta impresora con escáner.



Wuolah Giveaway

Altavoz inalámbrico ZoeeTree. Siente la música allá donde vayas con este altavoz Bluetooth inalámbrico.

El ensayo analiza dos modelos de producción de software bien diferenciados. Por un lado, la catedral, que representa el modelo de desarrollo más hermético y vertical característico del software propietario. Y por el otro, el bazar, con su dinámica horizontal y “bulliciosa”, que caracterizó al desarrollo del kernel Linux y otros proyectos de software libre que se potenciaron con el trabajo comunitario del código abierto a través de Internet.

El libro recopila una serie de lecciones aprendidas a partir de la experiencia que el autor comparte en el texto. En concreto:

- 1) Todo buen trabajo de software comienza a partir de las necesidades personales del programador.
- 2) Los buenos programadores saben qué escribir. Los mejores, qué reescribir (y reutilizar).
- 3) “Considere desecharlo; de todos modos, tendrá que hacerlo.” – Fred Brooks, *The Mythical Man-Month*.
- 4) Si tienes la actitud adecuada, encontrarás problemas interesantes.
- 5) Cuando pierdes el interés en un programa, debes darlo en herencia a un sucesor competente.
- 6) Tratar a los usuarios como colaboradores es la forma más apropiada de mejorar el código y la más efectiva de depurarlo.
- 7) Libere rápido y a menudo, y escuche a sus clientes.
- 8) Dad una base suficiente de desarrolladores asistentes y beta-testers, casi cualquier problema puede ser caracterizado rápidamente y su solución ser obvia, al menos para alguien. O, dicho de manera menos formal, “con muchas miradas, todos los errores saltarán a la vista”, A esto lo he bautizado como la Ley de Linus.
- 9) Las estructuras de datos inteligentes y el código burdo funcionan mucho mejor que el caso inverso.
- 10) Si usted trata a sus analistas (beta-testers) como si fueran su recurso más valioso, ellos le responderán convirtiéndose en su recurso más valioso.
- 11) Lo mejor, después de tener buenas ideas, es reconocer las buenas ideas de sus usuarios.
- 12) Con frecuencia, las soluciones más innovadoras y espectaculares provienen de comprender que la concepción del problema era errónea.
- 13) “La perfección (en diseño) se alcanza no cuando ya no hay nada que agregar, sino cuando ya no hay nada que quitar.
- 14) Toda herramienta es útil empleándose de la forma prevista, pero una gran herramienta es la que se presta a ser utilizada de la manera menos esperada.
- 15) Cuando se escribe software para una puerta de enlace de cualquier tipo, hay que tomar la precaución de alterar el flujo de datos lo menos posible y nunca eliminar información, a menos que los receptores obliguen a hacerlo.

- 16) Cuando su lenguaje está lejos de un Turing completo, entonces el azúcar sintáctico puede ser su amigo.
- 17) Un sistema de seguridad es tan seguro como secreto. Cuídese de los secretos a medias.
- 18) Para resolver un problema interesante, comience por encontrar un problema que le resulte interesante.
- 19) Si el coordinador de desarrollo tiene un medio al menos tan bueno como lo es Internet y sabe dirigir sin coerción, muchas cabezas serán, inevitablemente, mejor que una.

TEMA 2 – ORGANIZACIÓN DE UN SISTEMA OPERATIVO TIPO GNU/LINUX:

1. Crear un archivo con el contenido HOLA!, utilizando la orden echo, y asignarle permisos para que solo pueda ser consultado por su propietario y por los miembros del grupo.

- Archivo hola.sh:


```
#!/bin/bash
echo "HOLA!"
```
- Permisos -r--r-----:


```
chmod ug+r,ug-wx,o-rwx hola.sh
chmod 440 hola.sh
```

2. Marque todos los tipos de enlace que pueden establecerse en los siguientes casos (físico, simbólico o ambos):

- Enlace hacia un archivo en el mismo directorio: ambos
- Enlace hacia un archivo en otro sistema de archivos: simbólico
- Enlace hacia un directorio en el mismo sistema de archivos: simbólico
- Enlace hacia un directorio en otro sistema de archivos: simbólico

3. Transformar los siguientes permisos simbólicos en absolutos:

- `rw-r-xr-x` → 755
- `r-xr--r--` → 544
- `rw-r-----` → 640
- `r-x--x--x` → 511

4. Transformar los siguientes permisos absolutos en simbólicos:

- 644 → `rw-r--r--`



- 755 → `rwxr-xr-x`
- 610 → `rw---x---`
- 631 → `rw--wx--x`

5. Fijar, en modo simbólico, los permisos de arch1 en modo 754.

`754 → rwxr-xr--`

`chmod u+rw,x,g+rx,g-w,o+r,o-wx arch1`

6. Fijar, en modo absoluto, los permisos de arch1 en modo `rwxr-x--x`.

`chmod 751 arch1`

7. Fijar los permisos del directorio dir1 de modo que todos lo puedan leer y entrar, pero sólo el dueño pueda modificar sus archivos:

1) Modo simbólico:

`chmod a+rx,u+w,go-w dir1`

2) Modo absoluto:

`chmod 755 dir1`

8. Modificar para que el grupo también pueda modificar archivos:

`chmod g+w dir1`

`chmod 775 dir1`

9. Fijar en modo simbólico los permisos del archivo ejecutable `exec.tar` para que sea ejecutable por todos, legible por el dueño y el grupo, y modificable solo por el dueño. Repetir en modo absoluto.

`chmod a+x,ug+r,u+w,g-w,o-rw exec.tar`

`chmod 751 exec.tar`

10. Fijar en modo absoluto los permisos del directorio dir1 de modo que sólo el dueño y el grupo lo puedan recorrer y leer, y sólo el dueño pueda grabar y borrar en él. Repetir en modo simbólico.

`chmod 750 dir1`

`chmod ug+rx,u+w,g-w,o-rwx dir1`

11. Sea la siguiente salida del comando `ls -l`:

1	-rwSr-xr-x	1	pagutierrez	docentes	29024	ene	1	16:29	controlar
2	-rw-rw-r--	1	pagutierrez	docentes	2300	may	18	09:37	borrador.txt
3	-rw-r--r--	1	pagutierrez	docentes	5895	may	15	12:08	index.htm
4	-rwxr-xr-x	1	pagutierrez	docentes	29024	ene	1	16:29	revisar
5	-rwxr--r--	1	pagutierrez	docentes	29024	ene	1	16:29	mostrar
6	drwxrwxrwt	2	pagutierrez	tecnicos	1024	may	1	17:23	trabajos
7	drwxr-xr-x	2	pagutierrez	tecnicos	1024	oct	16	1998	netscape3
8	drwxrwx--x	2	pagutierrez	tecnicos	1024	may	11	7:29	finanzas
9	drwxrwxr-x	2	pagutierrez	tecnicos	1024	jul	7	6:54	redes
10	drwxr-xr-x	2	jsanchezm	docentes	1024	jun	17	19:35	corporacion

El usuario jsanchezm, del grupo docentes, tiene acceso al presente directorio. Indicar, si los hay:

1) Archivos de los que se puede mostrar contenido:

- controlar
- borrador.txt
- index.htm
- revisar
- mostrar

2) Archivos que puede ejecutar como programa:

- controlar
- revisar

3) Archivos en los que puede modificar contenido:

- borrador.txt

4) Subdirectorios en los que puede ingresar:

- trabajos
- netscape3
- redes
- corporacion

5) Subdirectorios en los que puede crear/eliminar ficheros propios:

- corporacion

6) Subdirectorios en los que puede borrar archivos de otros:

- trabajos

7) Subdirectorios en los que puede entrar y ejecutar programas contenidos en ellos, pero no ver nombres de archivos:

- finanzas

8) Archivos que puede ejecutar como programa con permisos del usuario pagutierrez:

- controlar

12. Sea la siguiente salida del comando `ls -l` (suponemos que pagutierrez pertenece a staff):

1	-rw-r--r--	1	root	root	33280	jun 12 19:40	Carta.doc
2	drwxrwxrwx	5	pagutierrez	staff	1024	dic 4 1999	step
3	drwxrwxr-x	22	pagutierrez	staff	1024	nov 20 1999	Office51
4	drwxr-x---	6	pagutierrez	staff	1024	may 7 16:43	argos
5	drwxrwxr--	21	pagutierrez	staff	1024	jul 11 18:22	bajados
6	-rw-rw----	3	root	root	542	jul 13 11:26	boor.exe
7	drwxrwxrwt	3	pagutierrez	staff	1024	may 25 10:02	borrador
8	-rwSrwsr-x	1	root	root	9218	jun 12 19:41	pph3
9	drwxrwx--x	2	pagutierrez	pagutierrez	1024	may 7 16:47	cdir
10	-rw-rw-r--	3	root	root	542	jul 13 11:26	mysql-doc
11	-rw-r-xr--	3	pagutierrez	staff	1084	ago 1 10:01	ver.exe
12	-rwxr-xr-x	3	pagutierrez	staff	1084	ago 1 10:01	ver
13	drwxr-xr-x	7	pagutierrez	pagutierrez	1024	jul 25 11:48	lit

Indicar, si los hay:

1) Directorios públicos (todo el mundo puede entrar. Listar y borrar archivos):

- step
- borrador

2) Archivos que tienen enlaces hard o físicos:

- boor.exe
- mysql-doc
- ver.exe
- ver

3) Archivos ejecutables por el usuario pagutierrez:

- pph3
- ver

4) Directorios navegables por todo el mundo:

- step
- Office51
- borrador
- cdir
- lit

5) Directorios donde miembros del grupo staff pueden borrar archivos:

- step
- Office51
- Bajados
- borrador

6) Archivos que son enlaces simbólicos: No hay

7) Archivos ejecutables que adquieren permisos de usuario root:

- pph3

TEMA 3 – ARRANQUE Y PARADA DEL SISTEMA:

1. Suponiendo la siguiente salida:

```
/etc/rc0.d/:
K74bluetooth README S20sendsigs S31umountnfs.sh
S35networking S60umountroot K80openvpn S10unattended-upgrades
S30urandom S32rpcbind S40umountfs S90halt

/etc/rc1.d/:
K15pulseaudio K20acpi-support K20kerneloops K20saned K74bluetooth
K80openvpn K81rpcbind README S30killprocs S70dns-clean S70pppd-dns
S90single

/etc/rc2.d/:
README S20kerneloops S20sysstat S24prueba
S50pulseaudio S50saned S70pppd-dns S90binfmt-support S99grub-common
S99rc.local S16openvpn S20speech-dispatcher S25bluetooth S50rsync
S70dns-clean S75sudo S99acpi-support S99ondemand S99rc.local

/etc/rc6.d/:
K74bluetooth README S20sendsigs S31umountnfs.sh
S35networking S60umountroot K80openvpn S10unattended-upgrades
S30urandom S32rpcbind S40umountfs S90reboot

/etc/rcS.d/:
README S13pcmciautils S25brltty S37apparmor S43rpcbind S55urandom
S70x11-common
```

Se pide:

- 1) Diferencias entre el apagado y el reinicio de la máquina. Comentar un ejemplo de un *script* que tuviese que ejecutarse al parar y no al reiniciar la máquina.

Cuando se apaga el equipo se desactivan todas las funciones y se borran los datos de la RAM. Sin embargo, al reiniciar la máquina se da una instrucción de apagado seguida de otra de encendido, lo cual permite no borrar los datos de la RAM.

Observando la salida y sabiendo que el apagado corresponde con el nivel 0 y el reinicio con el 6, un *script* que se ejecuta al parar y no al reiniciar la máquina es S90halt.

- 2) ¿Qué diferencias observas entre los niveles de tipo monousuario?



Atendiendo a los niveles de ejecución en GNU/Linux, sabemos que monousuario corresponde con el nivel 1 y S o s. Observamos en la salida que en el nivel 1 la mayoría de los *scripts* son para terminar procesos (K15pulseaudio, K20acpi-support, ...); sin embargo, en el nivel S los *scripts* son para comenzar procesos (S13pcmciautils, S25brltty, ...).

3) Indique qué se activa antes en el nivel 2: el soporte ACPI o el soporte para el bluetooth.

Los *scripts* se ordenan de la siguiente forma:

- Primero se activan los que empiezan por K y después los que empiezan por S.
- Dentro de cada grupo se ordenan numérica y alfabéticamente.

Por tanto, el soporte para el bluetooth (S25bluetooth) se activará antes que el soporte ACPI (S99acpi-support).

4) Si ejecutamos las siguientes órdenes como administrador:

```
echo "echo \"HOLA\$1\" > /tmp/p1" > /etc/rc2.d/S24prueba
mv /etc/rc2.d/S24prueba /etc/rc2.d/S71prueba
cp /etc/rc2.d/S71prueba /etc/rc4.d/K00prueba
chmod u+x /etc/rc2.d/S71prueba /etc/rc4.d/K00prueba
telinit 4
telinit 2
```

Indique el contenido del fichero /tmp/p1:

a) Después de ejecutar la orden telinit 4. Tras ejecutar la orden telinit 2.

HOLA stop

b) Antes de que se ejecute el script S70dns-clean.

HOLASTop

c) Antes de que se ejecute el script S75sudo.

HOLASTart

5) ¿Cómo eliminaría el servicio openvpn a todos los niveles?

Bastaría con introducir el siguiente comando:

```
rm /etc/rc*/openvpn
```

2. ¿Qué sucedería si el sector MBR de un disco duro queda dañado (por ejemplo, en una caída)? ¿Cómo podríamos repararlo?

Si se deteriora el programa cargador (MBR o GRUB), no hay forma de elegir sistema operativo al arrancar, por lo que el equipo quedaría congelado sin arrancar.

En Linux, una forma de repararlo sería reinstalando GRUB mediante el siguiente comando:

```
sudo grub-install /dev/sda
```

3. Comenta el significado de las siguientes líneas de un fichero de configuración:

```
menuentry 'Debian GNU/Linux, con Linux 3.16.0-4-amd64' --class debian
--class gnu-linux --class gnu --class os {
    insmod part_msdos
    insmod ext2
    set root='hd0,msdos1'
    search --no-floppy --fs-uuid --set=root bf8474c5-958e-4cca-a568-
4828b2310fda
    echo      'Cargando Linux 3.16.0-4-amd64...'
    linux     /boot/vmlinuz-3.16.0-4-amd64 root=UUID=bf8474c5-958e-4cca-
a568-4828b2310fda ro initrd=/install/gtk/initrd.gz quiet
    echo      'Cargando imagen de memoria inicial...'
    initrd    /boot/initrd.img-3.16.0-4-amd64
}
```

Por la línea echo 'Cargando Linux 3.16.0-4-amd64...' deducimos que se trata de un fragmento del fichero /boot/grub/grub.cfg. En la siguiente línea indica que tiene que cargar su kernel.

Se insertan módulos en las líneas insmod part_msdos y insmod ext2. Se carga la interfaz gráfica configurando la raíz como hd0,msdos1 y el superusuario al de UUID=bf8474c5-958e-4cca-a568-4828b2310fda.

¿Qué fichero modificaría para eliminar la opción quiet de todas las entradas linux?

Habría que modificar, en el fichero /etc/default/grub, la siguiente línea:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
```

Y convertirla en:

```
GRUB_CMDLINE_LINUX_DEFAULT=""
```

4. Interprete el siguiente código:

```
# tty1 - getty
#
# This service maintains a getty on tty1 from the point the system is
# started until it is shut down again.
start on stopped rc RUNLEVEL=[2345]
stop on runlevel [!2345]

respawn
exec /sbin/getty -8 38400 tty1
```

- Fichero de inicio upstart asociado a getty (terminal 1).

- rc arranca todos los procesos de inicio
- respawn vuelve a ejecutar el proceso en caso de error.

¿Qué sucedería si elimina el 2 en RUNLEVEL=[2345]?

El getty no se ejecutaría en nivel 2.

5. ¿Por qué no deberíamos apagar el sistema utilizando directamente el botón de POWER del ordenador? ¿Qué alternativas conoce?

Al pulsar el botón POWER no se cierran correctamente los procesos en ejecución ni se elimina la caché de manera ideal. Esto puede provocar daños en el sistema que, a la larga, puedan dejarlo no funcional.

Como alternativas, podríamos utilizar los comandos shutdown o telinit 0, pues son más adecuados para apagar el sistema desde la terminal.

6. Indique la secuencia de pasos necesaria para cambiar los parámetros de configuración de GRUB.

- 1.- Editar el fichero de configuración /etc/default/grub
- 2.- Actualizar el GRUB con el comando update-grub2
- 3.- (Opcional) Reinstalar GRUB con el comando grub-install /dev/sda

7. ¿Qué tendríamos que hacer si queremos que el script deliver_pizza.sh, que está en el HOME de root, se ejecute siempre en el nivel de ejecución 4?

Deberíamos crear un enlace simbólico a deliver_pizza.sh, de nombre S10deliver.sh (por ejemplo), y después mover ese enlace a la carpeta del nivel 4: /etc/rc4.d/S10deliver

```
ln -s /root/deliver_pizza.sh S10deliver.sh
mv S10deliver.sh /etc/rc4.d/S10deliver
```

TEMA 4 – GESTIÓN DE USUARIOS:

1. Comenta distintas formas de imposibilitar el acceso al sistema por parte de un usuario.

Tenemos varias opciones:

- En el fichero /etc/passwd: buscamos el usuario y en el argumento password (2º argumento), donde debería encontrarse su contraseña cifrada o una x indicando que ésta está en /etc/shadow, lo cambiamos por "*" o "!!".
- En el fichero /etc/passwd: buscamos el usuario y en el argumento shell (último argumento), le asignamos /bin/false o /sbin/nologin.

- En el fichero `/etc/passwd`: buscamos el usuario y en `shell` (último argumento), apuntamos a un ejecutable.
- En el fichero `/etc/shadow`: buscamos el usuario y en `expired:unused` (último argumento), donde se indica la fecha en que la cuenta expira y se deshabilita, cambiamos `unused` por una fecha expirada, de forma que la cuenta quede deshabilitada inmediatamente.

2. ¿Cómo se determina el grupo primario de un usuario? ¿Cómo lo cambiaría?

Hay varias opciones para determinar el grupo primario de un usuario:

- En el fichero `/etc/passwd`: buscamos el usuario y en `gid` (4º argumento) encontramos el identificador del grupo primario al que pertenece.
- Utilizar el comando `groups <usuario>`.
- Utilizar el comando `id <usuario>`.

Para cambiar el grupo primario de un usuario, podemos utilizar los siguientes comandos:

- `newgrp <nuevo_grupo>`
- `sudo usermod -g <nuevo_grupo> <usuario>`

3. Explica las diferencias que supondría utilizar las siguientes máscaras: 077, 027, 022 y 755. ¿Cómo modificarías los valores del `umask` por defecto de un usuario? ¿Y de todos los usuarios? ¿Habría alguna forma de forzarles a mantenerlos?

Los permisos base para los directorios son 777 y para ficheros, 666.

La máscara de bits indica con un 1 aquellos bits que deberán ser 0 en la cadena de permisos; es decir, indica qué permisos restringe la máscara.

Utilizando estas máscaras, sus permisos quedarían de la siguiente forma:

- `umask 077 = 000 111 111`
 - Directorio: $777 = 111\ 111\ 111 \rightarrow 111\ 000\ 000 = 700 = drwx-----$
 - Fichero: $666 = 110\ 110\ 110 \rightarrow 110\ 000\ 000 = 600 = -rw-----$
- `umask 027 = 000 010 111`
 - Directorio: $777 = 111\ 111\ 111 \rightarrow 111\ 101\ 000 = 750 = drwxr-x---$
 - Fichero: $666 = 110\ 110\ 110 \rightarrow 110\ 100\ 000 = 640 = -rw-r-----$
- `umask 022 = 000 010 010`
 - Directorio: $777 = 111\ 111\ 111 \rightarrow 111\ 101\ 101 = 755 = drwxr-xr-x$



- Fichero: 666 = 110 110 110 → 110 100 100 = 644 =
-rw-r--
- umask 755 = 111 101 101
 - Directorio: 777 = 111 111 111 → 000 010 010 = 022 =
d----w--w-
 - Fichero: 666 = 110 110 110 → 000 010 010 = 022 =
-----w--w-

Para modificar los valores de umask por defecto de un usuario debemos añadir su nuevo valor en el archivo oculto \$HOME/<usuario>/.bashrc.

Para modificar los valores de umask por defecto de todos los usuarios debemos añadir su nuevo valor en el archivo oculto /etc/profile.

Modificando estos ficheros, el valor de umask es permanente. Si se modifica en una terminal será temporal; es decir, solo se mantendrá en esa terminal y mientras esta esté abierta.

4. ¿Es cierto que el administrador del sistema puede modificar el *password* de un usuario? ¿Puede ejecutar algún programa que le permita leerla?

Sí, es cierto que el administrador de sistemas puede modificar el *password* de un usuario. Solo tiene que introducir el comando `passwd <usuario>`.

Sin embargo, no podrá leerla de ninguna manera.

5. Imagina la siguiente salida:

```
pagutierrez@pagutierrez--TOSHIBA:~/tmp$ ls -la
total 8
-rw-rw-r-- 1 root      profesores    0 2018-03-19 18:30 prueba
pagutierrez@pagutierrez--TOSHIBA:~/tmp$ newgrp profesores
Contraseña:
pagutierrez@pagutierrez--TOSHIBA:~/tmp$
```

El fichero prueba es propiedad del usuario root, que pertenece al grupo profesores.

El usuario pagutierrez cambia el grupo activo a profesores con el comando 'newgrp profesores'.

¿Qué salida producirían los siguientes comandos?

- 1) `chmod o+w prueba`

Aunque el usuario pagutierrez pertenezca al mismo grupo que root (grupo profesores), no puede cambiar los permisos de ficheros que son propiedad de root, por lo que este comando produce la siguiente salida:

chmod: cambiando los permisos de 'prueba': Operación no permitida

2) echo "HOLA" >> prueba

El usuario pagutierrez pertenece al grupo propietario del fichero prueba, y éste tiene permiso de escritura, por lo que es posible realizar esta acción: en el fichero prueba se escribirá 'HOLA'.

3) cat prueba

Se mostrará por pantalla el contenido del fichero prueba. Si no había nada escrito anteriormente, su contenido será 'HOLA'.

6. Comente el contenido del siguiente fichero:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:38:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
saned:x:112:121::/home/saned:/bin/false
pagutierrez:x:1000:1000:Pedro A. Gutiérrez,,,:/home/pagutierrez:/bin/bash
```

Por la estructura que muestra vemos que se trata del fichero /etc/passwd. Esta estructura es:

nombre:password:uid:gid:gecos:home:shell

Observamos que las shadows están activas pues en cada línea, relativa a cada uno de los usuarios, el segundo argumento (password) es una x, lo cual indica que la contraseña cifrada se encuentra en el fichero /etc/shadow.

¿Detecta alguna inconsistencia?

La inconsistencia existe en que los usuarios list e irc tienen el mismo uid (38), lo cual no puede ocurrir pues cada usuario debe tener un identificador único.

7. Explique por qué no produce ninguna salida el siguiente listado:

```
pedroa@pagutierrezLaptop:~$ ls /etc/skel/
pedroa@pagutierrezLaptop:~$
```

No produce ninguna salida porque los ficheros que contiene son ocultos.
Dependerán del intérprete de comandos, pero podrían ser:

- .bash_logout
- .bashrc
- .profile
- etc.

8. Prueba el siguiente comando:

```
echo "ibase=16;obase=2;$(echo "HOLA3" | sha1sum | tr -d ' -' |
tr '[a-z]' '[A-Z]')")" | bc
```

Explica qué es lo que está haciendo el comando.

Este comando utiliza la calculadora bc, un lenguaje de programación de cálculo numérico con precisión arbitraria. Con 'ibase=16' le indica que lo que le va a pasar está en base 16 (hexadecimal), y con 'obase=2' le indica que calcule eso que le ha pasado en base 2; es decir, que lo pase a binario.

Lo que le pasa a bc para traducir a binario es el resultado de `$(echo "HOLA3" | sha1sum | tr -d ' -' | tr '[a-z]' '[A-Z]')`, donde se realiza lo siguiente:

- 1) El algoritmo sha1sum cifra la cadena HOLA3, realizando la suma de sus bits:

```
irene@irenecasares:/$ echo "HOLA3" | sha1sum
c888118c94565b20ead38ac73407ecd14c5149c7 -
```

- 2) A continuación, el comando `tr -d ' -'` elimina de la cadena resultante lo indicado entre comillas simples:

```
irene@irenecasares:/$ echo "HOLA3" | sha1sum | tr -d ' -'
c888118c94565b20ead38ac73407ecd14c5149c7
```

- 3) El comando `tr '[a-z]' '[A-Z]'` cambia (traduce) a mayúsculas las letras que encuentra en la cadena:

```
irene@irenecasares:/$ echo "HOLA3" | sha1sum | tr -d ' -' | tr '[a-z]' '[A-Z]'
C888118C94565B20EAD38AC73407ECD14C5149C7
```

- 4) Finalmente, esta cadena es la que se le pasa a la calculadora bc para que traduzca a binario, indicándole que actualmente está en hexadecimal. El resultado final es:

```
irene@irenecasares:/$ echo "ibase=16;obase=2;$(echo "HOLA3" | sha1sum | tr -d ' -' | tr '[a-z]' '[A-Z]')")" | bc
11001000100010000001000110001100100100101000101011001011001000001110\
1010110100111000101011000111001101000000011111011001101000101001100\
010100010100100111000111
```

Otras formas de hacerlo serían:

- Abriendo la calculadora bc e insertando todo en una línea:

```
irene@irenecasares:/$ bc
bc 1.06.95
Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006 Free Software Foundatio
n, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
ibase=16;obase=2;C888118C94565B20EAD38AC73407ECD14C5149C7
11001000100010000001000110001100100101000101011001011011001000001110\
1010110100111000101011000111001101000000111111011001101000101001100\
010100010100100111000111
```

- Insertando cada indicación en una línea. Esto es posible gracias a que bc no es una calculadora cualquiera, sino un lenguaje:

```
irene@irenecasares:/$ bc
bc 1.06.95
Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006 Free Software Foundatio
n, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
ibase=16
obase=2
C888118C94565B20EAD38AC73407ECD14C5149C7
11001000100010000001000110001100100101000101011001011011001000001110\
1010110100111000101011000111001101000000111111011001101000101001100\
010100010100100111000111
```

Comprueba cómo cambiar un solo bit de la cadena hace que cambien más de la mitad de los bits del resumen.

En lugar de la cadena HOLA3, le pasaremos HOLA2. Vemos cómo han cambiado muchos bits:

```
irene@irenecasares:/$ echo "ibase=16;obase=2;$(echo "HOLA2" | sha1sum | t
r -d ' -' | tr '[a-z]' '[A-Z]')" | bc
10011000010010011011000101010010010100001110100000100110111000110010\
10111010100000111101110101110010011000101101001100001110011101000101\
00000001111010100111
```

TEMA 5 – GESTIÓN DE RECURSOS:

1. ¿Cómo podríamos listar el PID de todos los procesos en ejecución utilizando ls?

Cada proceso tiene una carpeta (cuyo nombre es el PID) que guarda información sobre el mismo, como por ejemplo la línea de comandos con que fue iniciado (cmdline). Estas carpetas se encuentran en el directorio /proc. Por tanto, podríamos listar el PID de todos los procesos en ejecución con el comando:

```
ls /proc/[[:digit:]]*/cmdline
```

Esto dará la siguiente salida:



```
irene@ireneacasares:~$ ls /proc/[[:digit:]]*/cmdline
/proc/1060/cmdline /proc/1339/cmdline /proc/1469/cmdline
/proc/10/cmdline /proc/1342/cmdline /proc/1472/cmdline
/proc/1124/cmdline /proc/1353/cmdline /proc/148/cmdline
/proc/1125/cmdline /proc/1364/cmdline /proc/14/cmdline
/proc/112/cmdline /proc/1369/cmdline /proc/1503/cmdline
/proc/1148/cmdline /proc/1374/cmdline /proc/1510/cmdline
/proc/1181/cmdline /proc/1378/cmdline /proc/152/cmdline
/proc/1182/cmdline /proc/1381/cmdline /proc/153/cmdline
/proc/1187/cmdline /proc/1394/cmdline /proc/154/cmdline
/proc/1189/cmdline /proc/1396/cmdline /proc/1554/cmdline
/proc/11/cmdline /proc/13/cmdline /proc/1557/cmdline
/proc/1256/cmdline /proc/1410/cmdline /proc/1558/cmdline
/proc/1267/cmdline /proc/1414/cmdline /proc/1562/cmdline
/proc/1279/cmdline /proc/1433/cmdline /proc/1569/cmdline
/proc/1296/cmdline /proc/1447/cmdline /proc/1571/cmdline
/proc/12/cmdline /proc/1450/cmdline /proc/1575/cmdline
/proc/1302/cmdline /proc/1454/cmdline /proc/1576/cmdline
/proc/1307/cmdline /proc/1455/cmdline /proc/1594/cmdline
/proc/1324/cmdline /proc/1457/cmdline /proc/15/cmdline
/proc/1333/cmdline /proc/1458/cmdline /proc/1603/cmdline
/proc/1334/cmdline /proc/1461/cmdline /proc/1610/cmdline
/proc/1337/cmdline /proc/1463/cmdline /proc/1615/cmdline
```

Si queremos una salida más limpia, con solo los PIDs, debemos utilizar el siguiente comando:

```
ls /proc/[[:digit:]]*/cmdline | sed -r -e 's/(.*)\\/(.*)\\/(.*)\\2/'
```

Dando la siguiente salida:

```
irene@ireneacasares:~$ ls /proc/[[:digit:]]*/cmdline | sed -r -e
's/(.*)\\/(.*)\\/(.*)\\2/'
1060
10
1124
1125
112
1148
1181
1182
1187
1189
11
1256
1267
1279
1296
12
1302
1307
```

2. Explicar cada una de las cifras que aparecen en la siguiente salida.


```
pagutierrez@TOSHIBA:~$ free
```

	total	used	free	shared	buffers	cached
Mem:	1012004	924100	87904	0	13292	142316
-/+ buffers/cache:		768492	243512			
Swap:	1000444	508868	491576			

Con el comando free podemos obtener información sobre el uso de la memoria. Su formato es:

- Mem -> muestra el estado actual de la memoria física.
- -/+ buffers/cache -> muestra la cantidad de memoria actualmente dedicada a las memorias del sistema (buffers y caché).
- Swap -> muestra el espacio swap (memoria de intercambio).

En las columnas nos encontramos lo siguiente:

- total -> memoria total disponible.
- used -> memoria consumida.
- free -> memoria libre.
- shared -> memoria compartida.
- buffers -> memoria usada en *buffers* (acceso a disco, red, temp, filesystems...).
- cached -> memoria caché.

3. ¿Qué diferencia existe entre hibernar un equipo y suspender un equipo? ¿En qué sentido influye en la memoria del sistema?

Al hibernar se guarda el contenido de la memoria dentro del espacio de intercambio *swap* (disco duro) y se indica al gestor de arranque que inicie directamente dentro del núcleo adecuado.

Por otro lado, al suspender se detiene el funcionamiento de todas las aplicaciones. El estado del sistema se guarda en la RAM y el equipo se pone en modo de bajo consumo, pero necesita energía para volver a funcionar correctamente.

Resumiendo, la hibernación guarda lo que se estaba realizando en el disco duro y, por tanto, no es necesaria alimentación de corriente; mientras que la suspensión guarda los procesos en la RAM, que necesita energía para no perder los datos.

4. ¿Para qué sirven los comandos vmstat e iostat? ¿Para qué tareas los utilizaría en su labor como administrador de sistemas?

El comando `vmstat` (Virtual Memory Status) da información sobre la memoria virtual y procesos desde el último reinicio. Es útil cuando se tienen problemas de ralentización de sistemas, de manera que se puede controlar qué memoria se está saturando para, a continuación, establecer los protocolos oportunos de diagnóstico y solución.

Por otro lado, el comando `iostat` (Input Output Status) presenta estadísticas sobre la CPU y los dispositivos y particiones de E/S. Es apropiado cuando se tienen conectados varios dispositivos de E/S y se están produciendo fallos y/o problemas en el sistema, pero no se sabe a priori qué dispositivo es el causante.

5. ¿Para qué sirven los comandos `df` y `du`? Ponga ejemplos de situaciones en que debería utilizar dichos comandos.

El comando `df` (Disk Free) muestra la capacidad, el espacio libre y el punto de montaje de cada sistema de ficheros del equipo. Sería apropiado a la hora de instalar una aplicación en una determinada partición, pues es necesario comprobar si el espacio libre es superior al que ocupará la aplicación.

Por otro lado, el comando `du` (Disk Used) muestra el espacio usado por cada subdirectorio del directorio actual. Es similar a `df` pues a la hora de copiar una determinada cantidad de datos de un sistema de ficheros a otro, debemos asegurarnos de que el tamaño de lo que queremos copiar no es superior al espacio libre disponible.

6. ¿Qué debería hacer si un proceso consume demasiada CPU del sistema que está administrando? ¿Qué comandos debería utilizar para pararlo temporalmente, reiniciarlo e investigar más sobre el mismo?

Si consume demasiada CPU, antes de matarlos, deberíamos saber que están haciendo, para lo que es útil el comando `strace -p <PID>`. Si parece legítimo, deberíamos suspenderlo con `SIGSTOP`, aplicarle `'renice'` y reanudarlo con `SIGCONT` tras hablar con el dueño del proceso.

El comando para pararlo utilizaría `SIGSTOP` (19) y sería `kill -s 19 <PID>`. Para reiniciarlo utilizamos `SIGCONT` (18) y sería `kill -s 18 <PID>`. Finalmente, para estudiarlo podemos utilizar los comandos `'strace'` o `'top'`.

7. Relacione el UID de un fichero con el UID real de un proceso y el UID efectivo de un proceso. Comente al menos dos motivos por los que el UID de un proceso es necesario en un sistema GNU/Linux.

En un fichero con permisos de ejecución, si `SUID=1`, entonces el UID efectivo es igual al UID propietario, y el UID real es igual al UID del que ejecuta. Sin

embargo, si SUID=0, entonces el UID efectivo es igual al UID real y al UID del que ejecuta.

8. Un *menor leak* es un consumo incremental sin fin de memoria por parte de un proceso. ¿Cómo encontraría este tipo de procesos en un sistema con GNU/Linux?

Podríamos hacerlo de varias formas. La más directa y óptima sería mediante `top`, que permite ver los recursos utilizados por los procesos en tiempo real, de manera que directamente se puede comprobar si hay algún proceso que no pare de crecer.

Otras formas menos intuitivas, pues no serían en tiempo real, podrían ser:

- `ps aux | sort -rk 4 ->` observar el PID que está provocando el problema, así como su consumo en cuestión de memoria y CPU.
- `vmstat ->` observar si la memoria virtual está siendo acaparada en incremento por algún proceso.

9. ¿Para qué sirve el comando `killall`? ¿Qué señal envían por defecto los comandos `kill` y `killall` (número y nemónico)?

El comando `killall` permite mandar una señal a todos los procesos. Esta señal es, por defecto, SIGTERM (15), al igual que en el comando `kill`.

10. Especifica el contenido de dos entradas para el fichero `crontab`:

En primer lugar, debemos dar permisos para poder crear los archivos en el directorio `/var/log`:

```
sudo chmod 777 /var/log
```

Si no tenemos ninguna tarea programada, escribimos `crontab`, pues aún no hay ningún fichero `crontab`. Si ya teníamos alguna, escribimos `crontab -e` para añadir más.

1) La primera debe imprimir el espacio libre en las particiones del sistema cada hora. La información se volcará al fichero `/var/log/reportEspacio.log`:

```
0 * * * * df -h | tr -s """:' | grp -e '/dev/' |
sed -rn 's/(.*):(.*):(.*):(.*):(.*):(.*):/En la
partición \1 hay libres \2/p' >>
/var/log/reportEspacio.log
```

2) La segunda debe imprimir el listado de todos los procesos, incluyendo el nombre de usuario, a las 9:00h, a las 12:00h y a las 15:00h, los viernes. La información se volcará al fichero `/var/log/reportProcesos.log`:



```
0 9,12,15 * * * ps aux | tr -s "": " | cut -d": " -
f1,2 | sed -rn 's/(.):(.)/:Nombre de usuario: \1;
\tPID --> \2/p' >> /var/log/reportProcesos.log
```

TEMA 6 – ORGANIZACIÓN DE SISTEMAS DE FICHEROS Y DISCOS:

1. ¿Qué son los superbloques y para que se utilizan? ¿Se establecen a nivel de partición o de disco?

Los superbloques de un sistema de archivos son bloques que contienen la información que describe a dicho sistema. Su función principal consiste en indicar al SF el tamaño de las distintas partes del propio sistema de archivos, así como su posición. Mantienen información común para todos los SFs y una entrada característica para cada tipo de SF. Al arrancar la máquina, los superbloques de todos los SFs que son cargados se mantienen en memoria.

Cada partición de disco contiene su sistema de ficheros, por lo que los superbloques del sistema de ficheros se establecen a nivel de partición.

2. Comente el sentido que tienen las políticas de actualización *write-through* para bloques de i-nodos y *delayed-write* para bloques de datos.

La política *write-through*, indicada para bloques especiales, mantiene el bloque siempre actualizado en tiempo real.

Por otro lado, la política *delayed-write*, indicada para bloques de datos, establece un tiempo periódico para realizar las actualizaciones, de forma que disminuye la carga de trabajo y la extensión de los posibles daños por caídas.

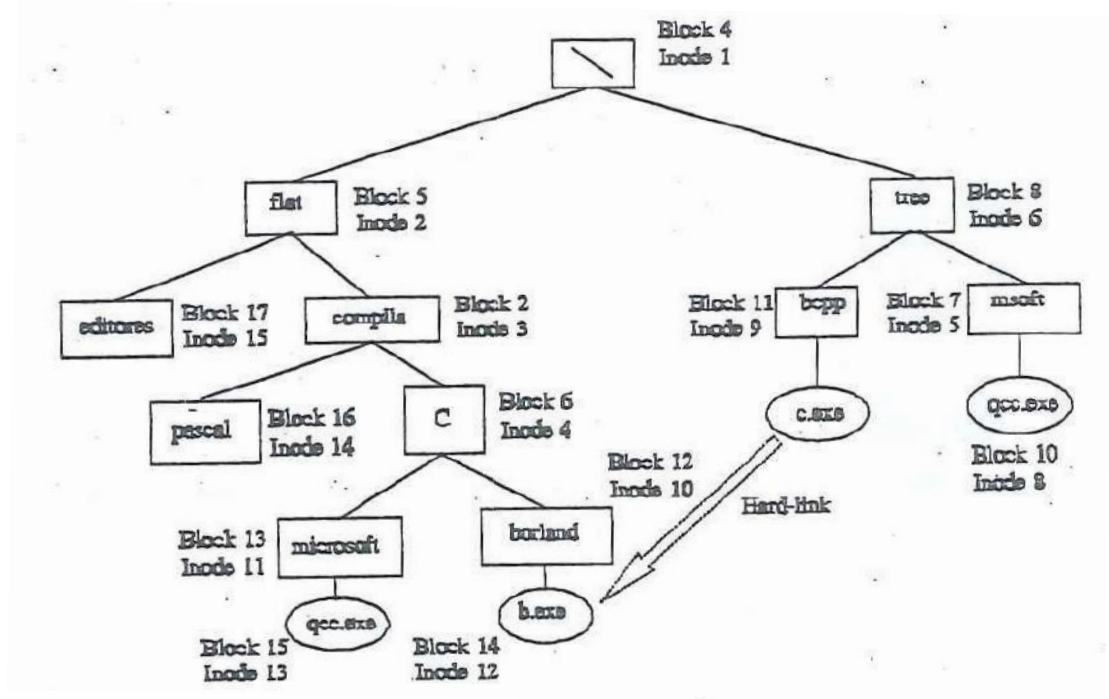
3. Explique los conceptos de bloque, i-nodo y v-nodo. ¿Cómo implementaría un enlace físico utilizando una tabla tipo FAT?

- Bloque: agrupación lógica de sectores físicos del disco, siendo la unidad de transferencia mínima que usa el SF.
- i-nodo: metadatos sobre un fichero que nos proporciona información sobre aspectos como su tamaño, sus permisos, la posición de sus sectores, número de enlaces... pero no su nombre.
- v-nodo: nodos virtuales usados en sistemas virtuales como NTFS.

4. (Problema 6) En la figura se muestra parte de la estructura de directorio de un sistema de ficheros, donde las elipses representan ficheros y los rectángulos directorios. Al lado de cada elemento se indica el número de

bloque que ocupa en el disco y el nodo-i asociado. El fichero *c.exe* es un *hard-link* del fichero *bc.exe*.

Indicar los contenidos de los bloques y nodos-i (solo los campos n° de link y uno de los punteros a bloque) que encontrará el sistema al hacer la búsqueda del fichero *c.exe*.



Bloque 4

1	*
1	**
2	flat
6	tree

Bloque 8

6	*
1	**
9	bcpp
5	msoft

Bloque 11

9	*
6	**
12	c.exe

Bloque 14

Datos

Nodo-1

4
B4

Nodo-6

4
B8

Nodo-9

2
B11

Nodo-12

2
B14

N° link

Puntero
a block

5. (Problema 9) En la figura 1 se muestra parte del árbol del directorio de un sistema operativo UNIX. Los directorios se representan mediante cuadrados y los ficheros mediante elipses. Al lado de cada elemento se indica el número(s) de bloque que ocupa en el disco y el nodo-i asociado.

En la figura 2 se representa el formato que tienen los bloques de disco. La figura 2.a se refiere a bloques que contendrán directorios y la 2.b a bloques que contienen datos.

La figura 3 representa un nodo-i. Las entradas que nos interesan son:

- Entrada 2: N° de enlaces (link)
- Entradas 9, 10, 11, 12: Punteros a bloques directos

En la zona de respuesta al ejercicio se representan los bloques y nodos-i usados por el árbol de directorios de la figura 1.

Se pide: rellenar los bloques y nodos-i en la zona de respuesta teniendo en cuenta que el fichero *dir* es un soft link hacia *ls* y el fichero *type* es un hard link hacia *cat*. Los bloques que pertenezcan a un directorio deben rellenarse de acuerdo al formato de la figura 2.a.

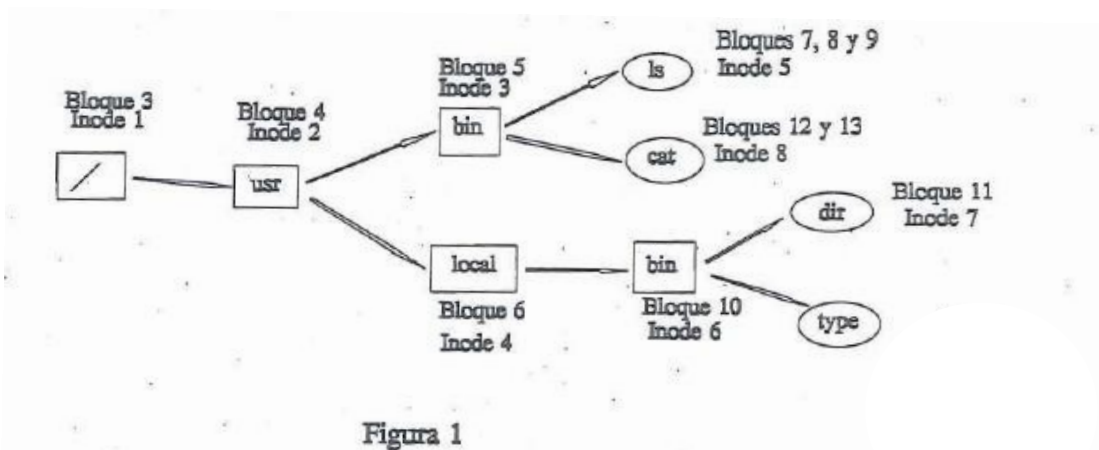


Figura 1

nº inode	nombre

Bloque de directorio

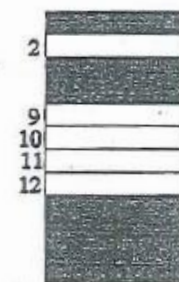
(a)



Bloque de datos

(b)

Figura 2



Inode

Figura 3

Nodo-1	Nodo-2	Nodo-3	Nodo-4	Nodo-5
3	4	2	3	1
B3	B4	B5	B6	B7
				B8
				B9

Nodo-6	Nodo-7	Nodo-8
2	1	2
B10	B11	B12
		B13

Bloque 1	Bloque 2	Bloque 3	Bloque 4	Bloque 5																						
Datos	Datos	<table><tr><td>1</td><td>*</td></tr><tr><td>1</td><td>**</td></tr><tr><td>2</td><td>usr</td></tr></table>	1	*	1	**	2	usr	<table><tr><td>2</td><td>*</td></tr><tr><td>1</td><td>**</td></tr><tr><td>3</td><td>bin</td></tr><tr><td>4</td><td>local</td></tr></table>	2	*	1	**	3	bin	4	local	<table><tr><td>3</td><td>*</td></tr><tr><td>2</td><td>**</td></tr><tr><td>5</td><td>ls</td></tr><tr><td>8</td><td>cat</td></tr></table>	3	*	2	**	5	ls	8	cat
1	*																									
1	**																									
2	usr																									
2	*																									
1	**																									
3	bin																									
4	local																									
3	*																									
2	**																									
5	ls																									
8	cat																									
Bloque 6	Bloque 7	Bloque 8	Bloque 9	Bloque 10																						
<table><tr><td>4</td><td>*</td></tr><tr><td>2</td><td>**</td></tr><tr><td>6</td><td>bin</td></tr></table>	4	*	2	**	6	bin	Datos	Datos	Datos	<table><tr><td>6</td><td>*</td></tr><tr><td>4</td><td>**</td></tr><tr><td>7</td><td>dir</td></tr><tr><td>8</td><td>type</td></tr></table>	6	*	4	**	7	dir	8	type								
4	*																									
2	**																									
6	bin																									
6	*																									
4	**																									
7	dir																									
8	type																									



Bloque 11	Bloque 12	Bloque 13	Bloque 14	Bloque 15
/usr/bin/l	Datos	Datos	Datos	Datos

6. (Problema 12) En las figuras 1 y 2 se representan los bloques y nodos-i (para éstos últimos se especifican únicamente las entradas correspondientes al número de enlaces y punteros directos a bloques, según refleja la figura 1) de un sistema de ficheros similar al de UNIX.

Se pide: dibujar la estructura en árbol, en la que se deben indicar los enlaces (si los hubiera) especificando su tipo, así como el nombre, número de nodo asignado y bloques que ocupa cada uno de los elementos (fichero o directorio).

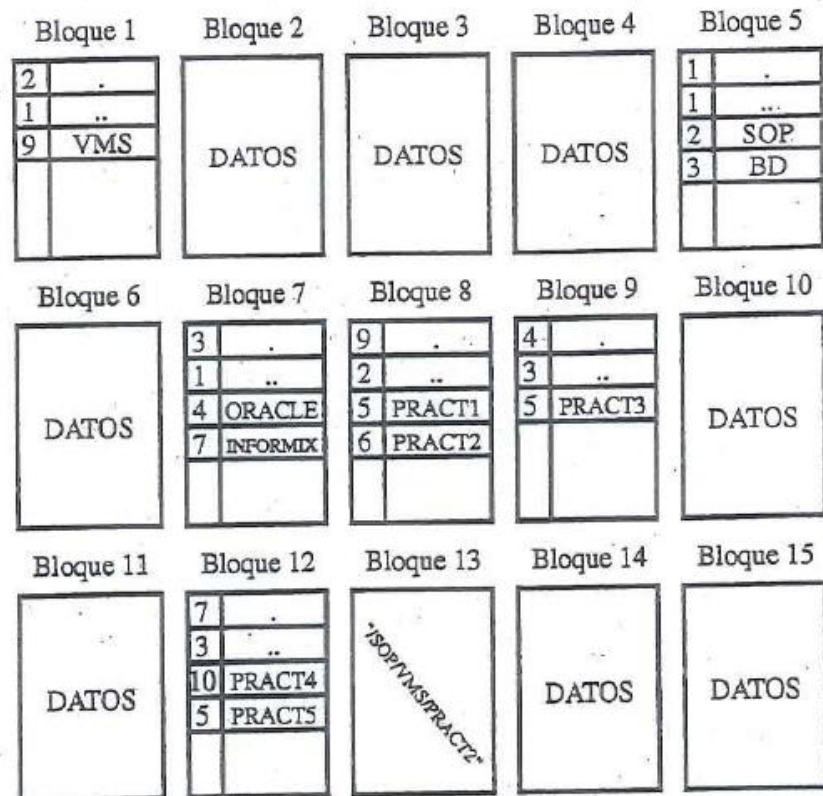


Figura 1 - BLOQUES DE DISCO

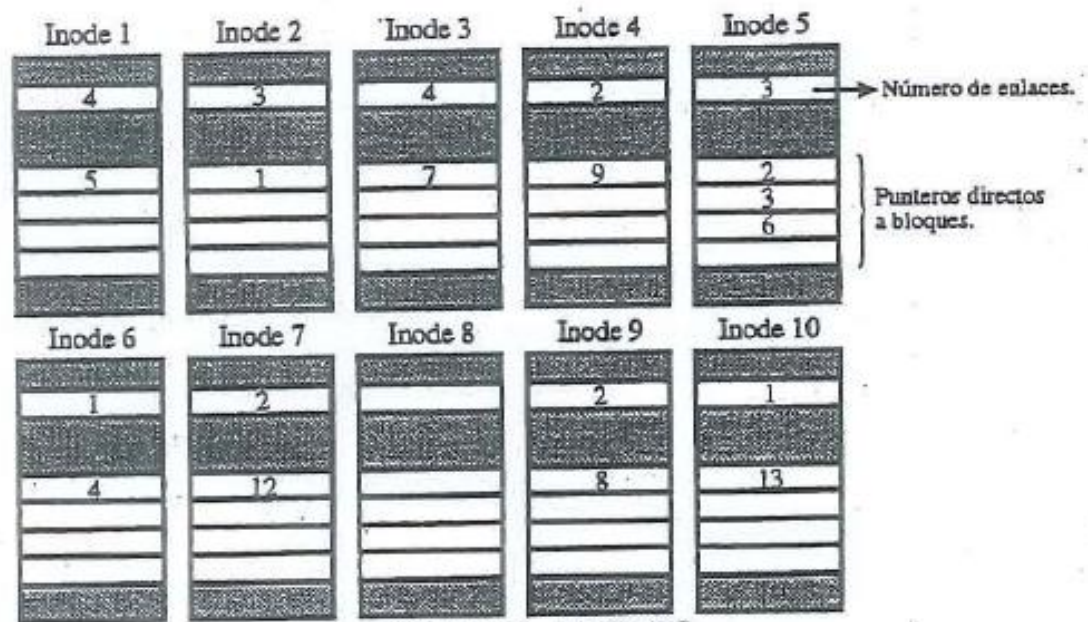
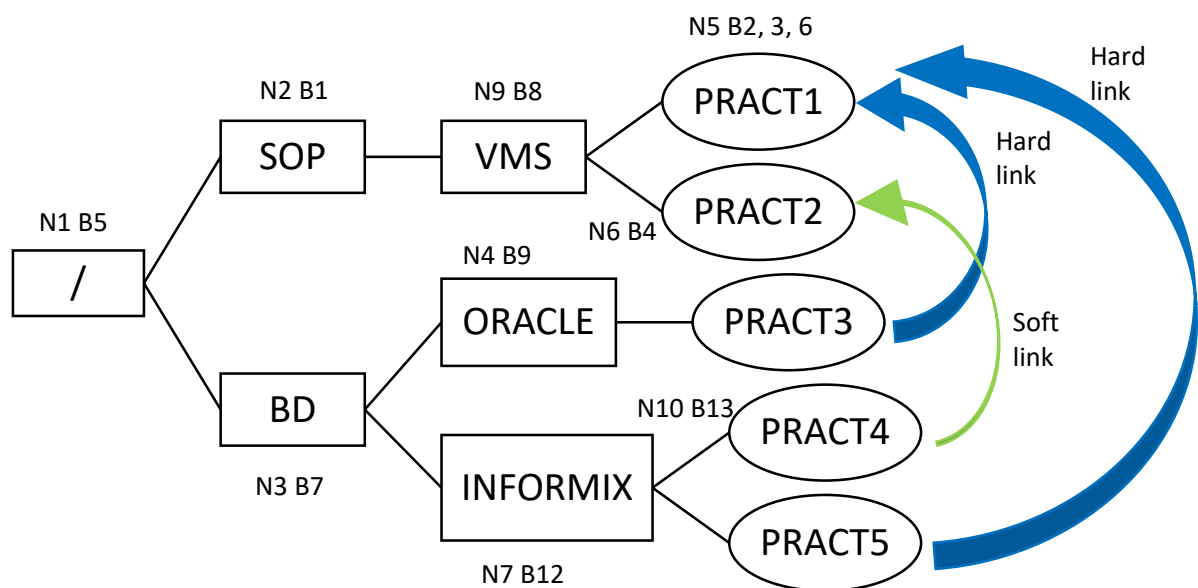


Figura 2 - INODES



TEMA 7 – ADMINISTRACIÓN DE SISTEMAS DE FICHEROS Y DISCO:

1. ¿Con qué se corresponde la siguiente salida? ¿Cómo puede obtenerse en un sistema GNU/Linux?

```
/dev/sda5 /      ext4 rw 0 0
/dev/sda6 /home ext4 rw 0 0
```

Se corresponde con el fichero /etc/fstab. En un sistema GNU/Linux se obtendría mediante el comando `cat /etc/fstab`.

¿Cómo podría indicar un dispositivo si solo conoce su UUID o su etiqueta?

El comando 'blkid' relaciona la etiqueta del dispositivo con su UUID, de manera que, sabiendo cualquiera de ambas, se pueden indicar o relacionar fácilmente.

2. Suponiendo el siguiente contenido para el fichero /etc/fstab:

LABEL= /	/	ext3	defaults,usrquota	0 1
/dev/sda3	/windows	vfat	defaults	0 0
/dev/dvd	/media/dvd	iso9660	noauto,owner,ro	0 0
/dev/fd0	/media/floppy	vfat	noauto,uid=500	0 0
/dev/sda4	/otrolinux	ext3	rw,auto	0 2
/dev/sda2	swap	swap	defaults	0 0

¿Qué puntos de montaje tendrían algún contenido tras iniciar el sistema?

Todos los que tengan la opción 'auto' o 'defaults', pues ya incluye auto. Por tanto, serían /windows, /otrolinux y swap.

3. Establezca que los permisos por defecto para archivos sean 601 para la partición /dev/sda4 del ejercicio anterior. Suponiendo que la partición ya esté montada, ¿cómo haría efectivos los permisos de manera inmediata?

Los archivos sda tienen los mismos permisos base que los directorios (777), por lo que, para establecer que los permisos por defecto para archivos creados en la partición /dev/sda4 sean 601, debemos añadir umask=176 a las opciones de la partición (cuarta columna).

Si la partición ya está montada, la forma más inmediata de cambiar los permisos sería mediante el comando `chmod -R 601 /dev/sda4` o `mount -a`.

4. ¿Cómo sabría el número de bloques libres de la partición /dev/sda3?

Mediante el comando `sudo tune2fs -l /dev/sda3 | grep 'Free blocks'`.

5. **¿Cuál es la diferencia entre formatear (a bajo nivel) y particionar un disco?**
¿Cuál es la diferencia entre formatear (a alto nivel) y particionar un disco?
¿Cuándo se crea el *journal*?

Para formatear a bajo nivel habría que recurrir a herramientas de fabricante; mientras que, para particionar un disco, simplemente hay que dividirlo de forma lógica.

Por otro lado, formatear a alto nivel aplica a sistemas de ficheros concretos, monta raíz, se dan extensiones, etc; mientras que particionar solo divide el disco de forma lógica.

Por último, el *journal* se crea para evitar la verificación completa de SFs de gran tamaño, que sería muy costosa, implementando un modelo de control transaccional basado en *logging*.

TEMA 8 – INSTALACIÓN DE IMPRESORAS:

1. **¿Cuál es el propósito de compartir una impresora Linux utilizando SAMBA?**

SAMBA es un sistema de compartición de archivos e impresoras en red cuyo propósito es permitir la interconexión de sistemas *heterogéneos* entre sí (GNU/Linux y Windows).

2. **Supón que tenemos la suerte de que el fabricante de una impresora nos haya proporcionado un fichero PPD denominado *newprinter.ppd*. ¿Para qué sirve ese fichero?**

El fichero PPD (PostScript Printer Description) es un archivo creado por el fabricante de la impresora para describir las características disponibles para sus impresoras PostScript. Este fichero ayuda a CUPS a saber cómo manejar la impresora mostrando las opciones soportadas por la impresora (formato de papel, dúplex, bandejas, contraseña...) en un lenguaje que entiende de forma nativa.

¿Qué labor administrativa está haciendo el siguiente comando?

```
lpadmin -p prueba -E -v parallel:/dev/lp0 -m newprinter.ppd
```

lpadmin es una orden para añadir y habilitar impresoras:

- -p prueba -> nombre de la impresora (*prueba*).
- -E -> habilita la impresora
- -v parallel:/dev/lp0 -> URI del dispositivo (*parallel:/dev/lp0*)
- -m newprinter.ppd -> fichero.ppd



3. ¿Qué comando utilizarías para imprimir un fichero a la impresora por defecto desde la línea de comandos? ¿Este comando es exclusivo de CUPS?

El comando sería `lp` fichero y sí es exclusivo de CUPS.

¿Cómo harías para saber las impresoras que hay instaladas en un sistema CUPS?

Existen dos formas posibles para saber qué impresoras hay instaladas:

- Mediante el comando `lpstat -v`
- Mediante el fichero `/etc/cups/printers.conf`

4. Explique los pasos necesarios para compartir una impresora en CUPS.

En primer lugar, editamos el fichero `/etc/cups/cupsd.conf` para que acepte trabajos desde la red:

```
<Location />
    Order Deny,Allow
    Deny From All
    Allow From 127.0.0.1
    Allow From IP
</Location>
```

Después, si así lo deseamos, podemos decir a CUPS que publique en broadcast las impresoras disponibles:

```
#Show shared printers on the local network
Browsing On
BrowseOrder allow,deny
BrowseAllow all
BrowseLocalProtocols CUPS dnssd
BrowseAddress 192.168.0.255:631
```

5. A partir de la siguiente salida, diagnostique la causa por la que no están imprimiéndose los trabajos en este equipo:

```
pagutierrez@PEDROLaptop:~$ ps ax | grep cupsd
4084 pts/0    S+        0:00 grep --color=auto cupsd
```

El estado del proceso, S+, indica que se trata de un proceso *foreground* (en primer plano) y que está durmiendo, esperando algún evento que lo active. Es por esto por lo que no se imprimen los trabajos.

¿Y si en el fichero `/etc/cups/cupsd.conf` encontramos lo siguiente?



Esto significa que está escuchando desde la IP de Google y podría aceptar trabajos enviados desde esa IP.

TEMA 9 – COPIAS DE SEGURIDAD Y RESTAURACIÓN:

1. ¿Cómo podrías utilizar el comando tar para crear una copia incremental de su directorio home con dos niveles (0 y 1)?

○ Nivel 0:

```
tar -czvf backup.0.tgz -g backup.snap /home
```

La opción -g o --listed-incremental permite generar un fichero de referencia a partir del cual hacer la copia incremental.

Este comando genera dos ficheros, el backup.0.tgz, que es un fichero con la copia de seguridad comprimida, y el fichero backup.snap, que es un fichero que lista los ficheros de los que se ha hecho copia hasta ahora, de manera que, conforme se vayan generando copias de nivel 1, se irá actualizando con el listado nuevo.

○ Nivel 1:

```
tar -czvf backup.1.tgz -g backup.snap /home
```

Para recuperar el respaldo bastaría con hacer:

```
tar -xzvf backup.0.tgz -g /dev/null -C/
tar -xzvf backup.1.tgz -g /dev/null -C/
```

2. Proporciona un comando que realice una copia de seguridad de su directorio home (nivel 0) en el primer dispositivo de cinta conectado al sistema. Elige el comportamiento más adecuado (*rewinding* o *non-rewinding*).

El comando sería el siguiente:

```
dump 0 -u /home
```

El comportamiento más adecuado debería ser *non-rewinding*, para poder seguir desde el punto de partida haciendo copias de seguridad.

3. Crea un fichero crontab que realice las siguientes copias de seguridad de /dev/sda1, regularmente, sobre el primer dispositivo de cinta:

- Una copia de nivel 0 una vez al mes.
`0 5 1 * * dump 0 -u /dev/sda1 #Día 1 del mes (5 a.m. por ej.)`
- Una copia de nivel 2 una vez a la semana.
 - `0 5 * * 1 dump 2 -u /dev/sda1 #Día 1 de la semana (Domingo) (5 a.m. por ej.)`
 - `0 5 */7 * * dump 2 -u /dev/sda1 #Cada 7 días (5 a.m. por ej)`
- Una copia de nivel 5 cada día que no se haya producido ni una de nivel 0 ni una de nivel 2.
`0 5 2-31 * 2-7 dump 5 -u /dev/sda1 #Del 2 al 31 del mes (el nivel 1 se hace el día 1) y de Lunes (2) a Sábado (7) (el nivel 2 se hace el Domingo (0 ó 1)).`

4. Realiza una copia de seguridad de tu directorio \$HOME en la carpeta /var/tmp utilizando el comando tar. Comprime el fichero con el algoritmo gzip. Haz un fichero que, al descomprimirlo, genere la misma estructura de directorios original. ¿Qué opción utilizarías para extraerlo preservando los permisos?

El comando necesario sería:

```
tar -zcvfPp /var/tmp/copiaSeguridad.tgz /home
```

- z: comprime en el algoritmo *gzip*.
- P: guarda los ficheros con su ruta absoluta.
- p: conserva los permisos de los ficheros.

Para extraerlo preservando los permisos, podemos utilizar:

```
tar -xzvfPp /var/tmp/copiaSeguridad.tgz
```

5. Comenta al menos tres directrices generales a tener en cuenta cuando se realizan copias de seguridad de los archivos.

- 1) Nivel de profundidad de la copia de seguridad.
- 2) Periodicidad.
- 3) Ruta para la copia de seguridad: el lugar “físico” de almacenaje debería ser distinto al original.

6. Supón que en una empresa la sensibilidad de los datos es muy alta y no hay restricciones de espacio en el dispositivo para hacer las copias. ¿Qué tipo de copia de seguridad crees que sería la más adecuada?

Se debería realizar una copia de seguridad completa.

¿Qué sistema instaurarías si el espacio fuese limitado?

Si el espacio fuese limitado, instauraría un sistema de copia de seguridad incremental, pues solo hace copia de aquellos ficheros que hayan cambiado desde la última copia.

Suponiendo que la mayoría de los cambios en el disco se producen de lunes a viernes y que el domingo el sistema está ocioso, ¿cómo organizarías las copias de seguridad en este segundo caso?

En primer lugar, podríamos realizar una copia de nivel 0 el domingo, siendo el día en que el sistema está ocioso y no hay usuarios trabajando en él, por lo que no hay problema en realizar una copia de todo el sistema.

Y, en segundo lugar, realizaríamos una copia de nivel 1 el sábado, donde solo se copiarían los archivos que se han modificado desde la última copia de nivel 0; es decir, los que se han modificado desde el domingo anterior.

TEMA 10 – GESTIÓN DE LAS COMUNICACIONES:**1. ¿Qué significa *stateless* para un sistema de ficheros distribuido y qué efectos tiene en el bloqueo de archivos, en los permisos de acceso y, en general, en la seguridad?**

Para un sistema de ficheros distribuido como NFS (*Network File System*), que sea un protocolo sin supervisión, *stateless*, significa que el servidor trabaja sin mantener información del *estado* de cada uno de los clientes (ficheros abiertos, último fichero o última posición escrita).

Necesita bloquear los archivos accedidos concurrentemente por varios clientes mediante demonios independientes, siendo estos clientes los responsables de mantener la coherencia.

2. Su jefe necesita que exporte las carpetas `/usr` y `/etc` utilizando NFS. Se le proporciona la siguiente información y peticiones:

- a) Debido a las políticas de la empresa, solo las personas de su Departamento (subred 192.168.123.0/24) deberían ser capaces de utilizar las carpetas exportadas (en modo lectura/escritura). ¿Qué líneas debería añadir a qué ficheros para hacer esto posible?

En el lado del servidor encontramos el fichero `/etc/exports`, en el que se indica qué SFs se exportan, bajo qué condiciones y a qué ordenadores. Es en este fichero en el que habría que añadir los siguiente:

```
/usr 192.168.123.0/24(rw)
/etc 192.168.123.0/24(rw)
```

Es muy importante que no haya ningún espacio entre la subred y los permisos pues, si lo hubiera, ya no permitiría acceder sólo a los usuarios



de la subred en modo lectura/escritura, sino que podrían montar el directorio sólo en modo lectura (predeterminado) y el resto de usuarios, no pertenecientes a la subred, podrían instalarlo como lectura/escritura.

Para que el montaje se pueda realizar en tiempo de arranque, se debe indicar en el fichero `/etc/fstab`, del lado del cliente, el listado de los sistemas de ficheros remotos a montar, el punto de montaje y las opciones:

```
192.168.123.0:/usr /usr/remoto nfs defaults, rw, bg,  
hard, intr 0 0
```

```
192.168.123.0:/etc /etc/remoto nfs defaults, rw, bg,  
hard, intr 0 0
```

- b) **¿Qué debería hacer para que los cambios sean efectivos y los demonios `mountd` y `nfsd` estuvieran al tanto de las nuevas carpetas sin tener que reiniciar el servidor?**

Habría que reiniciar los demonios `rpc.mountd` y `rpc.nfsd` con `/etc/init.d/nfs.kernel-server`.

- c) **¿Cómo podría hacer que, automáticamente, todas las máquinas tuvieran disponibles, al arrancar, estas dos carpetas en `/mnt/usr` y en `/mnt/etc` (suponga que el servidor tiene como IP `192.168.123.1`)?**

Al igual que en el apartado *a*, debemos modificar el fichero `/etc/fstab` del lado del cliente añadiendo lo siguiente:

```
192.168.123.1:/usr /mnt/usr nfs defaults, rw, bg, hard,  
intr 0 0
```

```
192.168.123.1:/etc /mnt/etc nfs defaults, rw, bg, hard,  
intr 0 0
```

3. **¿Cuál es la diferencia entre las utilidades `yppasswd` y `passwd`?**

Ambas utilidades sirven para cambiar la contraseña del usuario; sin embargo, mientras `yppasswd` se utiliza al trabajar sobre servidor NIS, `passwd` se utiliza cuando se trabaja en local, pues no tiene funcionalidad en el servidor NIS.

4. **¿Por qué el fichero `/etc/passwd` necesita dos mapas NIS distintos (`passwd.byname` y `passwd.byuid`)?**

El acceso a `password` por `name` y por `uid` son dos categorías distintas de un mismo rol de acceso, por lo que deben ir almacenadas en dos mapas diferentes.

5. **¿Para qué se utiliza el fichero `/etc/nsswitch.conf`?**

El fichero `/etc/nsswitch.conf` es el archivo de configuración del NSS (*Name Service Switch*) en el cual podemos indicar cómo se resolverá cierta información de configuración.

¿Qué implican las opciones `compat` y `nis`?

La opción `compat` es el modo de compatibilidad, permitiendo entradas especiales en `/etc/passwd`. Por otro lado, la opción `nis` es el mapa de `passwd` de NIS.

¿Existe alguna diferencia entre especificar “`passwd: compat nis`” y “`passwd: nis compat`”?

El orden correcto es el primero, que especifica una compatibilidad NIS.

6. Explique qué es el protocolo RPC y cuál es su relación con NFS y NIS.

El protocolo RPC (*Remote Call Procedure*) es el protocolo para encapsular llamadas al servidor cuando se piden archivos remotos. Facilita la conexión entre cliente y servidor, tanto NFS como NIS.