0.

Objetivos del aprendizaje

- Justificar la necesidad de establecer planes de prevención de catástrofes en la administración de cualquier sistema informático.
- Identificar distintos escenarios en los que pueda perderse información y establecer medidas de prevención: errores humanos, virus y *software* destructivo, personas malintencionadas y fallos del *hardware*.
- Proporcionar una serie de consejos generales a la hora de planear las copias de seguridad de un sistema.
- Establecer los factores que determinan la forma en que se realizan las copias de seguridad.
- Diferenciar los tres tipos de estrategias a seguir a la hora de realizar copias de seguridad: completa, parcial e incremental.
- Identificar diferentes soportes *hardware* en los que realizar las copias de seguridad.
- Utilizar la herramienta `tar` para realizar copias de seguridad en un sistema GNU/Linux.
- Utilizar la herramienta `cpio` para realizar copias de seguridad en un sistema GNU/-Linux.
- Utilizar la herramienta `dump` para realizar copias de seguridad en un sistema GNU/-Linux y `restore` para restaurarlas.

Contenidos

9.1. Planes de prevención de catástrofes.

- 9.1.1. Escenarios de pérdida de información.
  - 9.1.1.1. Errores humanos.
  - 9.1.1.2. Virus y *software* destructivo.
  - 9.1.1.3. Personas malintencionadas.
  - 9.1.1.4. Fallos del *hardware*.
- 9.1.2. Consejos generales.
- 9.1.3. Factores.
- 9.1.4. Estrategias.
  - 9.1.4.1. Copias de seguridad completas.
  - 9.1.4.2. Copias de seguridad parciales.
  - 9.1.4.3. Copias de seguridad incrementales.

9.2. Soportes de seguridad.

9.3. Copias de seguridad y restauración.

9.3.1. Comando `tar`.

9.3.2. Comando `cpio`.

9.3.3. Comando `dump`.

9.3.4. Comando `restore`.

9.4. Pasos para la restauración de un sistema completo.

Evaluación

- Cuestionarios objetivos.
- Pruebas de respuesta libre.
- Tareas de administración.

1. Planes de prevención de catástrofes

Planes de prevención de catástrofes

- En cualquier momento, algunos archivos serán totalmente ilegibles por algún motivo:
  - Se exige capacidad de recuperación.
- Las copias de seguridad dependen de la situación y es necesario determinar:
  - De qué archivos hacer la copia, dónde, cómo y cuándo...
- El administrador del sistema debe:
  - Planear e implementar un sistema de copias de seguridad.
  - Periódicamente, hacer copias de seguridad de los ficheros.
  - Guardar las copias de seguridad en un lugar seguro.

Planes de prevención de catástrofes

- La estrategia de copias de seguridad tiene que ser efectiva, para conseguir *seguridad*:
  - El tiempo empleado es un esfuerzo que prevé futuras pérdidas.
  - El dinero gastado se compensa al evitar el desastre que supone una pérdida de datos (que conlleva enormes pérdidas de trabajo y, por tanto, dinero).

- Tener en cuenta:
  - Capacidad restaurar el sistema entero o parte del mismo, en un tiempo aceptable.
  - Tiempo que tarda en hacerse la copia de seguridad.
  - Facilidad de recuperar algún fichero de forma independiente.

1.1. Escenarios de pérdida de información

Escenarios de pérdida de información

- Causas:
  - Errores de usuario.
  - Virus y software destructivo.
  - Personas malintencionadas.
  - Fallos mecánicos.
  - Fuerzas mayores: desastres naturales, electricidad estática, ...
- Si valoramos los costes, merece la pena incluir mecanismos/dispositivos específicos para esta labor.

Escenarios de pérdida de información: errores humanos

- Comandos mal escritos:

```
1 $ rm foo *
```

- Errores durante el redireccionamiento y uso de tuberías:

```
1 $ cat fstab | sed 's/ext2/ext3' > fstab
```

- Usuarios con acceso de `root`:
  - Los errores anteriores serían catastróficos si ocurrieran sobre directorios o archivos de sistema.

Escenarios de pérdida de información: prevención de errores humanos

- Medidas de prevención sencillas:
  - Utilizar alias:

```
1 Alias rm='rm -i' # El -i fuerza confirmacion
```

  - Utilizar sistema de control de versiones (SVN, GIT...):
    - Conservan el archivo original y llevan un histórico de los cambios realizados sobre éste.
  - Crear copias de seguridad personales.
  - Utilizar `sudo` para limitar el acceso de los usuarios con privilegios de `root`:
    - Se limitará el acceso únicamente a los comandos necesarios para que el usuario pueda llevar a cabo su tarea.

Virus y software destructivo

- *Virus*: programa que se adhiere a un ejecutable y se propaga a otros al mismo tiempo que realiza otra acción (desde escribir un mensaje hasta mezclar las tablas de particiones).
  - Caballos de Troya: Programas que se hacen pasar por otros, funcionando como éstos, pero además realizando otras operaciones como obtener y enviar contraseñas. El grado de destrucción depende de quien los ejecuta.
  - Gusanos: Programas que se aprovechan de las debilidades de un sistema para propagarse a otros.
  - Software destructivo: Aplicaciones no mal intencionadas pero con errores de programación que pueden ser muy dañinos.
- Linux dispone de mecanismos de seguridad que dificultan su propagación (los usuarios no tienen control total del sistema).

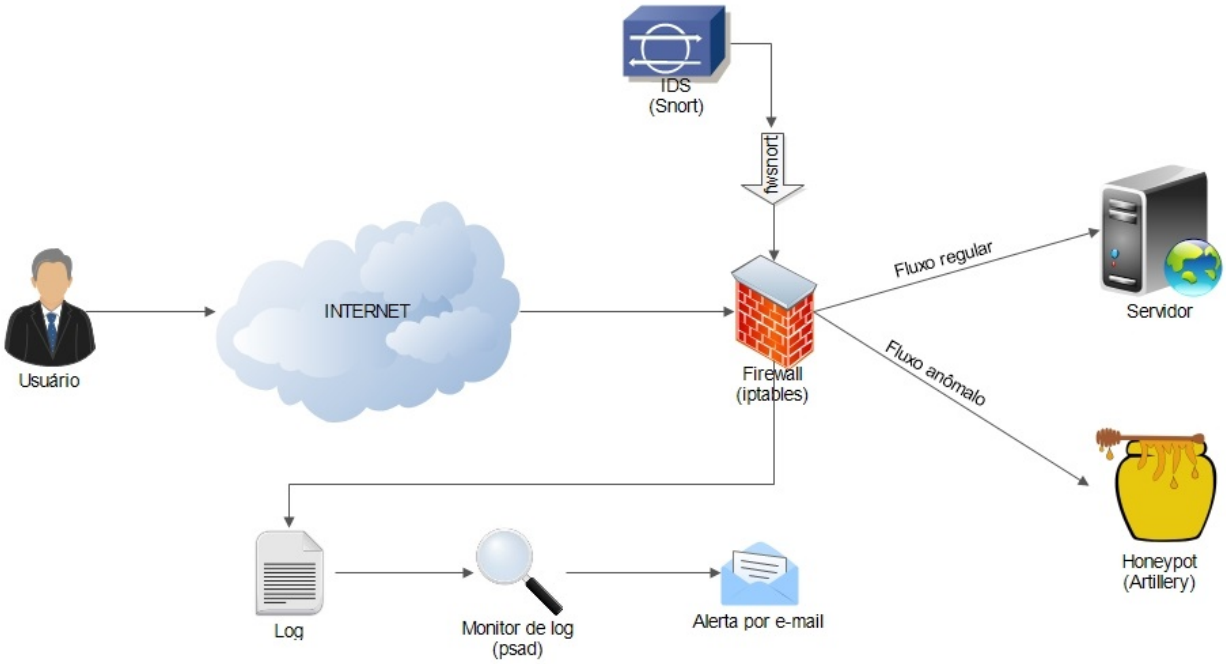
Virus y software destructivo: prevención

- Medidas de prevención sencillas:
  - Software específico de búsqueda y destrucción de virus.
  - Configuración del entorno: p.ej. la variable PATH no incluye la carpeta actual:

```
1 $ echo $PATH
2 /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

  - *Host* víctimas:
    - Se usan ciertos equipos para probar *software* nuevo, asumiendo que puede resultar dañado (*honeypots*).
    - Se suelen basar en un sistema de detección de intrusos (IDS) que genera reglas para el *firewall* separando el tráfico normal del anómalo.

Virus y software destructivo: prevención (*honey pots*)

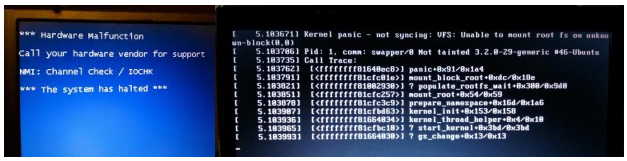


Personas malintencionadas

- *Crackers* ($\neq$ *Hackers*):
  - Personas que entran en los sistemas de forma, a veces, ilegal con fines malintencionados.
- Usuarios descontentos:
  - Usuario con acceso al sistema y recelo.
- Medidas preventivas:
  - Cortafuegos y Seguridad Física para los *crackers*.
  - Seguimiento de personas sospechosas de ser "usuarios descontentos" controlando sus accesos y sus privilegios.

Fallos de *hardware*

- Fallo en la unidad de disco duro:
  - El kernel suele avisar antes de un fallo completo.
- Fallo de la memoria:
  - Pérdida de información por la caída del sistema o información corrupta en memoria es copiada a disco.
- Prevención y recuperación:
  - Redundancia de la información: utilizar RAID.
  - Supervisión de registros del sistema (orden `dmesg`, datos SMART).
  - Recuperación desde copias de seguridad.
  - Intentar leer bloques para construir una imagen con '`dd`'.
  - Recuperación en entorno estéril: empresa dedicada.



1.2. Consejos generales

Consejos generales

- Prevención: Ante cualquiera de los escenarios de pérdida de información debemos tener la capacidad de recuperarnos inmediatamente o en un corto lapso de tiempo.
- Una opción es utilizar copias de seguridad.

Consejos generales

Consejos generales:

- Etiquetar siempre las copias realizadas.
- Elegir correctamente la frecuencia de copias.
- Usar particiones distintas para el sistema de ficheros.

- Hacer que el *backup* diario quepa en la unidad.
- Llevarse la copia a otro lugar y proteger ese lugar.
- Limitar la carga computacional durante el proceso de *backup*.
- No esperar a que ocurra un problema para verificar las copias.
- Tener en cuenta el tiempo de vida de los dispositivos.
- *Prepararse para lo peor*.

1.3. Factores

Factores

Factores a considerar en una estrategia de copias de seguridad:

- ¿Qué ficheros se deben copiar y dónde están esos ficheros?.
- Conocer qué es lo más importante del sistema.
- ¿Quién hará la copia?
  - ¿el *administrador* o el propietario de los ficheros?.
- ¿Dónde, cuándo y bajo qué condiciones se deben hacer?
  - Mejor hacer las copias cuando no haya usuarios trabajando (por la noche, a la hora de comer...).
- Frecuencia de cambios en los ficheros $\Leftrightarrow$ Frecuencia de las copias.

Factores a considerar en una estrategia de copias de seguridad:

- ¿Cada cuánto tiempo habrá que recuperar ficheros dañados o perdidos? (muy difícil saberlo).
- ¿Dónde se restaurarán los datos?.
- Rutinas de restauración sencillas.
- Proteger las copias de seguridad contra escritura.
- Seguridad de las copias:
  - Lugar donde se almacenan, condiciones ambientales, propiedades de los medios empleados...

1.4. Estrategias

Estrategias de copias de seguridad

Copia de seguridad completa

- Se guardan todos los archivos asociados a un ordenador.
- La restauración necesita un solo fichero pero *mucho tiempo*.
- Puede ser difícil recuperar un archivo suelto.
- Si los ficheros no cambian muy a menudo: no hay justificación.
- Si cambian mucho y son vitales para el trabajo de mucha gente: están justificadas incluso a diario.
- Hacerla ante grandes cambios: nuevo *software*, nuevo SO, . . .

Copia de seguridad parcial

- Se copia sólo algunos archivos específicos (por ejemplo, la carpeta `/etc`).
- Proceso de restauración sencillo, ya que hay menos archivos implicados.
- Problema: nos dejamos archivos sin copiar.

Copia de seguridad incremental

- Solo aquellos ficheros que hayan cambiado desde la última copia.
- Se deben realizar casi a diario.
- Se mantiene una copia completa del sistema, y se incorporan cambios muy pequeños, de los que se irán haciendo copias incrementales.

- Copias incrementales organizadas por niveles.
  - Nivel 0 → *Backup* completo.
  - Nivel 1 → Todos los ficheros que han cambiado desde el último *backup* de nivel 0.
  - Nivel 2 → Todos los ficheros que han cambiado desde el último *backup* de nivel 1.
  - ...
- Posibilidades de estrategias:
  - Lunes: nivel 0. Resto de días: nivel 1.
  - Lunes: nivel 0. Martes: nivel 1. Miércoles: nivel 2. Jueves: nivel 1. Viernes: nivel 2.
- También hay que asociar una estrategia de restauración.

2. Soportes de seguridad

Soportes para realizar las copias

- Guardar la copia de seguridad en el mismo disco (o en otro disco conectado a la máquina) *no es seguro*.
- Multitud de dispositivos:
  - Cintas magnéticas (`/dev/st0`, normal, o `/dev/nst0`, *non-rewinding*, para unidades de cinta SCSI):

  - Discos extraíbles (disco duro que puedes extraer sin apagar la máquina).

  - CD-Roms o DVD's regrablables.

  - Disquetes.
  - Librería de cintas o *jukeboxes*, *stackloaders* y similares...

  - etc.

Criterios para elegir el soporte

- Coste: no solo del dispositivo sino también del soporte físico de almacenamiento.
- Soporte del *kernel* para el dispositivo.
- Capacidad de almacenamiento de datos de los soportes físicos.
- Tasa de transferencia de datos para realizar copias de seguridad.
- Mecanismo de cargador automático.
  - Cuando se llena una cinta se inserta otra automáticamente.
  - Permite las copias no supervisadas de grandes volúmenes.

3. Copias de seguridad y restauración

3.1. tar

Comando tar (Tape ARchiver)

- Realiza copias de seguridad de ficheros o "dispositivos".
- Algunas opciones son:
  - `c` → Crea un fichero contenedor.
  - `x` → Extrae ficheros de un fichero contenedor.
  - `v` → Modo *verbose* (mayor cantidad de mensajes).
  - `f` → Permite especificar el nombre del fichero contenedor.
  - `z` → Comprime o descomprime mediante `gzip`.
  - `j` → Comprime o descomprime mediante `bz2`.
  - `p` → Conserva los permisos de los ficheros.
  - `P` → Guarda los ficheros con su ruta absoluta.
  - `N` → Considera *solo* archivos cuya fecha sea superior al argumento.

Comando tar (Tape ARchiver)

- `tar cPf /dev/nst0 /home` ⇒ copia todos los ficheros del directorio `/home` en la unidad de cinta.
- `tar czvf /dev/sda1 /home` ⇒ ¿qué sucede con la partición `/dev/sda1`?
- `tar czvf /dev/nst0 /dev/sda1`
- `tar czvf practicas.tgz prac_pas`
- `tar tzvf practicas.tgz` ⇒ listar el contenido de la copia de seguridad realizada en el fichero.
- `tar xzvf practicas.tgz` ⇒ descomprimir.
- `tar xzvf practicas.tgz prac_aso/boletin1.pdf` ⇒ recuperar el fichero `boletin1.pdf` (observa que hay que indicar la ruta con la que `tar` lo almacenó).

3.2. cpio

Comando cpio

- Copias de seguridad de conjuntos de ficheros seleccionados arbitrariamente.
  - Empaqueta los datos en una cinta más eficientemente que `tar` (al restaurar es capaz de saltar trozos de la cinta defectuosos).
  - Lee de la entrada estándar el nombre de los ficheros a guardar, para usarlo enlazado con otras órdenes con tuberías.

- Algunas opciones:
  - `o` → Copiar "fuera" (*out*) (crear la copia).
  - `i` → Copiar "dentro" (*in*) (descomprimir).
  - `m` → Conserva fecha y hora de los ficheros.
  - `t` → Muestra la tabla de contenidos, es decir, muestra el contenido de la copia.
  - `A` → Añade ficheros a un contenedor existente.
  - `d` → Crear directorios al descomprimir.
  - `v` → Modo *verbose*.
  - `F` → Crear la copia en un fichero.

Comando cpio

- `find /home | cpio -o > /dev/nst0` → se copia en la unidad de cinta.
- `find /home | cpio -o -F h.cpio` → la copia la realiza en un fichero.
- `cpio -i < h.cpio` → restaura la copia de seguridad de ese fichero.
- `cpio -i -F h.cpio fichero` → restaura sólo el fichero indicado.

3.3. dump

Comando dump

- Hace copias de seguridad de un sistema de ficheros `Ext2`, `Ext3` o `Ext4`, copiando la partición completa.
- Permite realizar copias de seguridad por niveles: desde el nivel 0, copia completa, al nivel 9 (que es el valor por defecto).
- Actúa solo a nivel de dispositivo.
- `/etc/dumpdates` → información sobre las copias de seguridad de cada SF y de qué nivel son: `/dev/sda1 0 Mon Feb 14 09:56:44 2017 +0100`
- Algunas opciones son:
  - `0-9` → Nivel de la copia de seguridad, no requiere argumento.
  - `-u` → Actualiza `/etc/dumpdates`, no requiere argumento.
  - `-f` → Indica fichero destino diferente al usado por defecto, sí requiere argumento. Por defecto, se usa la unidad de cinta.

3.4. restore

Comando restore

- Restaura copias de seguridad creadas con `dump`.
- Permite recuperar ficheros, directorios y SF enteros.
- Se ha de recuperar el más reciente de cada nivel empezando por el 0. ¡Mucho cuidado con las fechas!
- Para recuperar SF → crear y montar un SF limpio y vacío, entrar en el punto de montaje y deshacer el *backup*.
- Algunas opciones son:
  - `-r` → Restaura la copia completa, no requiere argumento.
  - `-f` → Indica el dispositivo o archivo donde está el *backup*, sí requiere argumento.
  - `-i` → Modo interactivo, no requiere argumento.
  - `-x` → Extrae los archivos y directorios desde el directorio actual.
  - `-t` → Imprime los nombres de los archivos de la copia, no requiere argumentos.

Ejemplos de dump y restore

- `dump 0 -u -f /dev/nst0 /dev/sda1` → Copia de nivel 0 de `/dev/sda1` en la unidad de cinta, actualizando `/etc/dumpdates`.
- `dump 1 -u -f /dev/nst0 /dev/sda1` → Copia de nivel 1 de `/dev/sda1` en la unidad de cinta, actualizando `/etc/dumpdates`.
- `dump 0 -f jj.dump /dev/sda1` → Copia de nivel 0 de `/dev/sda1` en el fichero jj.dump.
- `restore -t -f fichero_backup` → listado de la copia.
- `restore -x -f fichero_backup practicas/smallsh.c` → restaura sólo el fichero `practicas/smallsh.c`.
- `restore -r -f /dev/nst0` → restaura una copia completa.
- `restore -i -f /dev/nst0` → permite restaurar ficheros interactivamente (con ls, cd, pwd, add y extract).

4. Restauración de un sistema completo

Restauración del sistema

- Si se tiene una copia de todo el sistema:
  1. Arrancar desde un dispositivo distinto (p.e. un DVD).

2. Si es necesario, crear los ficheros especiales de dispositivos para los discos (`/dev/sda1`, etc.).
3. Preparar el disco duro, e.d., crear las particiones.
4. Crear el sistema de ficheros en la partición donde se restaurarán los datos y montarlo en un directorio.
5. Restaurar la copia de seguridad sobre ese sistema de ficheros.
   - Restaurar la copia más reciente de nivel 0.
   - Restaurar la copia más reciente del nivel más bajo después del último restaurado.
   - Si quedan más copias por restaurar, volver al paso anterior.
6. Desmontar el sistema de ficheros restaurado.
7. Volver al paso 2, para restaurar otros SF adicionales.

Restauración del sistema

- De las siguientes copias realizadas, ¿qué copias de seguridad se restaurarían?:
  - 0 0 0 0 0 0 0.
  - 0 5 5 5 5 5.
  - 0 3 2 5 4 5.
  - 0 9 9 5 9 9 3 9 9 5 9 9.
  - 0 3 5 9 3 5 9.

Restauración del sistema

- Solución (restauraciones en negrita):
  - 0 0 0 0 0 0 **0**.
  - **0** 5 5 5 5 **5**.
  - **0** 3 **2** 5 **4** **5**.
  - **0** 9 9 5 9 9 **3** 9 9 **5** 9 9 **9**.
  - **0** 3 5 9 **3** **5** **9**.

5. Referencias

Referencias

Referencias

[Nemeth et al., 2010] Evi Nemeth, Garth Snyder, Trent R. Hein y Ben Whaley Unix and Linux system administration handbook.
Capítulo 10. *Backups*, Capítulo 32. *Management, policy and politics* (sección *Disaster recovery*).
Prentice Hall. Cuarta edición. 2010.

[Frisch, 2002] Aeleen Frisch. Essential system administration.
Capítulo 11. *Backup and restore*. O'Reilly and Associates. Tercera edición. 2002.