



**ULPGC**  
Universidad de  
Las Palmas de  
Gran Canaria

**eii**

ESCUELA DE  
INGENIERÍA INFORMÁTICA

Administración de Sistemas Operativos

# Tema 4.2. Seguridad física y copias de seguridad

© 2020 José Miguel Santos

# Resumen

- Integridad física
- Integridad de la información
- Copias de seguridad: cuestiones básicas
- Copias completas, copias incrementales
- Plan de copias de seguridad

# Objetivo: integridad física

- Prevenir vandalismo y robo.
- Asegurar que el acceso a los dispositivos críticos está controlado.
- Controlar los riesgos ambientales:
  - Higiene: desinfección y limpieza periódicas
  - Mantener niveles bajos de humedad y temperatura
  - Estabilizar la corriente eléctrica (evitar picos dañinos)
  - Fuentes de alimentación de respaldo
  - Medidas contra incendio, inundación o seísmo

# Objetivo: integridad de la información

- Riesgos de pérdida de información:
  - Errores y negligencias del usuario
  - Errores de las aplicaciones software
  - Acciones maliciosas: del usuario o del software
  - Fallos del hardware
- Medidas:
  - **Copias de seguridad (*backups*)**
  - Redundancia de información (ej. RAID)
  - Monitorización de los registros del sistema

# Copia de seguridad (*backup*)

- Duplicado de datos originales que se realiza con el fin de recuperarlos en caso de pérdida.
- Cuestiones claves:
  - *QUÉ* ¿qué datos copiamos?
  - *DÓNDE* ¿dónde almacenamos la copia?
  - *CUÁNDO* ¿con qué frecuencia realizamos la copia?
  - *CÓMO* ¿qué herramientas utilizamos?
  - *QUIÉN* ¿quién es el responsable de las copias?
  - *¡SOCORRO!* ¿cómo se recuperan los datos?

# ¿Qué datos copiamos?

- *No tienen por qué ser todos. Ej. ¿merece la pena copiar los ejecutables de las aplicaciones?*
- Modalidades de copia:
  - Bajo nivel: imagen completa de un sistema de ficheros, directamente copiando bloques del disco. Muy rápido.
  - Alto nivel: copiar archivos y directorios. Más lento, pero facilita la recuperación (no dependes de un SO).

# Almacén de la copia

- El volumen de información puede ser muy alto  
→ cuidado con el coste
- Debe residir en un lugar diferente al sistema copiado
- El tiempo de recuperación incluye localizar e instalar el soporte de la copia (salvo que sea un sistema robotizado)

# Dispositivo de almacenamiento

- cintas magnéticas, discos ópticos, discos extraíbles, sistemas robotizados, servicio en la nube...





# ¿Con qué frecuencia?

- Caso extremo: copiar cada vez que se modifica un archivo  
→ muy costoso
- Habrá que definir un periodo razonable, que dependerá de la importancia de los datos y de las costumbres de la organización
  - *En una empresa típica, como mínimo habría que hacer una copia diaria*
- Aprovechar momentos de baja actividad
  - *Ej. fines de semana, madrugadas...*
- Podemos establecer frecuencias distintas según qué datos:
  - *Ej. diaria para los archivos de usuario, semanal para los archivos de registro (logs), mensual para los ejecutables del sistema...*

# Catálogo de copias

- Debe existir un catálogo o inventario de las copias realizadas, para facilitar las futuras recuperaciones.
- Por cada elemento del catálogo:
  - Fecha de la copia
  - Nombres de los archivos/directorios copiados
  - Ubicación de la copia (si están en distintas localizaciones físicas)
  - Etc.

# Copia completa (*full backup*)

- Cada vez que copiamos, lo hacemos de todos los archivos
- *Ineficiente* → habrá archivos que no han cambiado desde la última vez que se hizo copia... ¿merece la pena perder tiempo en copiarlos?
  - Se desperdicia espacio en la copia
  - Se desperdicia tiempo de CPU y de acceso a E/S

# Copias incrementales/diferenciales

- **Copia diferencial.** Sólo copiamos los archivos que han cambiado desde la última copia de seguridad completa.
- **Copia incremental.** Sólo copiamos los archivos que han cambiado desde la última copia (ya sea completa u otra incremental).
- El UNIX clásico implementa sistemas de copia *incremental*.

# Ejemplo de plan de copia incremental

- Ciclo semanal
  - lunes: copia completa
  - miércoles, viernes: copia incremental
- Si hoy es sábado y quisiera restaurar todos los datos, tengo que:
  1. Recuperar la copia completa del lunes
  2. Recuperar la copia del miércoles (sobrescribir)
  3. Recuperar la copia del viernes (sobrescribir)

# Copia incremental con niveles (Unix)

- Se definen *niveles* de copia, ej. Nivel 0, Nivel 1, Nivel 2
- Nivel 0 = copia completa
- La copia incremental de **nivel N** se hace con respecto a la última copia de **nivel N-1** (los archivos que cambiaron desde esa copia)

# Ejemplo con niveles

Día	nivel	Qué copia
domingo	0	Copia completa
lunes	1	Copia lo que cambió desde el domingo
martes	2	Copia lo que cambió desde el lunes
miércoles	3	Copia lo que cambió desde el martes
jueves	1	Copia lo que cambió desde el domingo
viernes	2	Copia lo que cambió desde el jueves
sábado	3	Copia lo que cambió desde el viernes

# Recuperación de datos

- Queremos restaurar un archivo tal y como estaba en una determinada fecha.
  - **Con sistema de copias completas:** restaurar la copia que tenga la fecha más cercana al dato que se desea recuperar.
  - **Con sistema de copia diferencial:** restaurar la copia completa más cercana y luego superponer la copia diferencial posterior más cercana.
  - **Con sistema de copia incremental:** restaurar la copia completa con fecha más cercana, y después ir restaurando las copias incrementales posteriores, en el mismo orden en que se realizaron, hasta la fecha deseada.



# Herramientas de software

- Órdenes básicas del SO (Unix):
  - **tar, cpio, dd** → empaquetan archivos
  - **dump/restore** → utilidades antiguas de cp.seg.
  - **rsync, rsnapshot** → utilidades más avanzadas
  - **crontab** → para planificar las copias
- Utilidades del SO de escritorio:
  - Déjà Dup (Ubuntu)
  - File History (Windows 10)
  - Time Machine (Mac OS X)
- Herramientas comerciales avanzadas

# Precauciones durante la copia

- ¡modificación concurrente de los datos mientras se copian!
- Medidas:
  - Copiar “en frío” → ejecutar la copia en modo monousuario
  - Montar el s.fich. como sólo lectura (no siempre es posible)
  - Realizar *snapshots* de los archivos, si el sistema de ficheros lo permite, ej. EXT4, ZFS, NTFS (VSS)





**ULPGC**  
Universidad de  
Las Palmas de  
Gran Canaria

**eii**

ESCUELA DE  
INGENIERÍA INFORMÁTICA

Administración de Sistemas Operativos

# Tema 4.2. Seguridad física y copias de seguridad

© 2020 José Miguel Santos