

Máster Universitario en Ingeniería Informática



CyberSeguridad
Tema 6: Backups
José Ismael Ripoll Ripoll



- § Términos
- § ¿Qué información guardar?
- § ¿Dónde almacenar las copias?
 - ◆ Lugar geográfico.
 - ◆ Soporte físico.
- § ¿Cómo realizar la copias?
 - ◆ Checksums
- § ¿Cuándo realizar las copias?
- § Aplicaciones de backup



- § Es evidente que no se puede tener una única copia de la información importante.
- § Las copias de respaldo sirven para:
 - ◆ Recuperarse ante fallos físicos.
 - ◆ Perdidas causadas por borrados accidentales.
 - ◆ Ataques de borrado o modificación de la información.
- § Por desgracia, solo se aprende el valor de las copias de respaldo cuando se pierde la información.



1. Información de operación:

- ◆ Aquellos ficheros que hemos creado y que no podamos recuperar por otros medios.

2. Soporte de ejecución:



- ◆ Configuración del sistema.
- ◆ El sistema completo: si el tiempo de recuperación es importante.



§ Seguir la regla: “**3-2-1 rule**”:

- ◆ **[3]** copias de seguridad: una primaria y dos secundarias.
 - No te esperes a que también falle la segunda copia.
- ◆ **[2]** tipos diferentes de soportes de almacenamiento.
 - El soporte o el lector del soporte pueden fallar.
- ◆ **[1]** de las copias debe estar fuera de la zona de trabajo.
 - Si se incendia la oficina...



- § Tener los datos en una ubicación remota es conveniente en caso de desastres totales (terremotos,...). 
- § Podemos acceder rápidamente a la información, si no es muy voluminosa.
- § La conexión a la red puede ser lenta, para grandes volúmenes 
- § No conocemos en qué país pueden estar nuestros datos y la normativa que se les aplica.
- § Sistema propietario y podemos quedar atrapados.

*Cifra tus datos
antes de subirlos!!*



§ Mantener una copia primaria en un disco conectado es muy sencillo y rápido.





§ Un fallo o un ataque en el equipo se puede propagar rápidamente a la copia de seguridad.



§ Puesto que el disco de respaldo está conectado, el tiempo de vida será similar al sistema de trabajo.

§ Si se roba el equipo... también desaparece la copia.



- § HD, SSD, DVD, cinta, etc. que conecta solo para realizar la copia, tras lo cual se guarda en un lugar seguro.
- § Es la forma más conveniente de realizar copias de seguridad. 
- § Pero se pueden perder o ser robados. 



Son los componentes de estado sólido eternos



*¡Aún estando apagados,
los discos **NO** son eternos!*



§ Disco duro externo:

- ◆ Se puede desmagnetizar (**perder** la información).
- ◆ Lugar seguro (temperatura controlada) de almacenamiento.

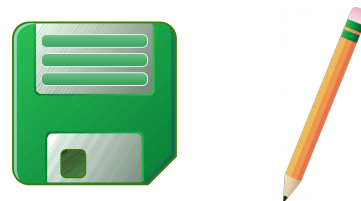
§ Almacenamiento en estado solido:

- ◆ SSD, USB, SD, tarjetas flash, etc.
- ◆ Pierden la información con el **tiempo**.
- ◆ Son dispositivos activos → problemas de seguridad.

*¿Cuánto es
"Mucho tiempo" ?*

§ Almacenamiento óptico:

- ◆ DVD, Bluray.
- ◆ Poca capacidad.



§ Cintas.... ¿Quién utiliza cintas hoy?

¿Qué sabemos del
inicio de la escritura?



§ Hacer un “backup”:

- ◆ No es otra cosa que **copiar** la información a otro lugar.
- ◆ No es nada mágico ni “especial”.

§ Restaurar un backup

- ◆ No es otra cosa que **copiar** la información sobre los directorios de trabajo diario.

§ Es MUY importante conocer BIEN los mecanismos de copia y restauración.

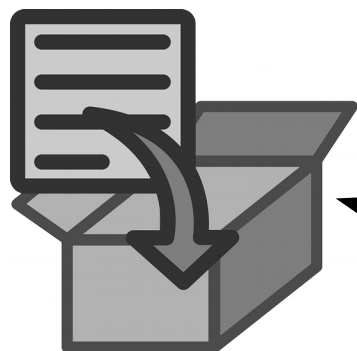
- ◆ Vaya, eso del “cp” o el arrastrar y soltar de toda la vida!



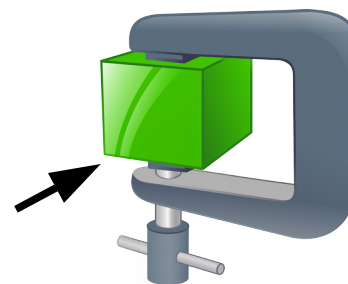
Los nervios y las prisas...
¡Nooo, yuyu, sooo!



- § O bien te dedicas a realizar copias (backup-man), o bien usas **utilidades convencionales** del día a día.
- § No es aconsejable empezar a “jugar” con herramientas que pueden sobre escribir los datos de forma masiva, cuando hay prisas.
- § Es preferible utilizar herramientas que se CONOZCAN
- § Oblígate a utilizar las herramientas de backup cada semana!



No es lo mismo
Empaquetar que **Comprimir**



§ dd: Disk Dump

- ◆ Copia **un (y solo uno)** fichero, desde donde sea.
- ◆ Puede copiar un disco entero (incluida tabla de particiones), en un fichero regular.
- ◆ Puede copiar de disco y pasarlo por la “salida estándar”.
- ◆ No interpreta los datos → hace copias EXACTAS de la información origen.
- ◆ No puede recorrer árboles de directorios!
- ◆ Pero es como el nc (netcat) de los ficheros: por sí solo hace poco, pero **no se puede entender la vida sin el “dd”**.



- § tar: Tape ARchive.
- § Es como el winzip o lo que que ahora se lleve en las ventanas. Pero sin pasar de moda.
- § Súper versátil
- § Universal.
- § Simple.
- § Potente.
- § Solo empaqueta.
- § Pero se puede jugar al LEGO(r) con ella!
 - ◆ Tarpipe, tar+dd, tar+xz, tar+ssh



- § Cuando las copias se realizan entre máquinas, la forma de mover la información debe ser cifrada.
- § SSH es la forma de hacerlo por excelencia.
- § También se puede utilizar NC, pero solo si confiamos en la red.
- § Rsync es útil para mantener dos copias iguales de un directorio de trabajo, optimizando la velocidad de sincronización



- § Dropbox está operado por un tercero.
- § Nuestros datos deben estar cifrados cuando salen de nuestros sistemas.
- § Dropbox es muy práctico para datos no sensibles.
- § Pero es un **gran problema para cumplir la LOPD**.
 - ◆ ¿Dónde están nuestros datos?
 - ◆ ¿Cuándo se realizan las copias?
 - ◆ ¿Quién puede acceder a ellos?



- § También podemos utilizar el soporte de los gestores de repositorios como herramienta de backup.
- § Un repositorio es un “**sistema de gestión de versiones**”.
- § Existen varios: SVN, GIT, Mercurial, etc.
- § El más potente es GIT:
 - ◆ “the stupid content tracker” (manpage).
- § No es trivial aprender git (o un DCVS)
 - ◆ pero vale la pena!



*Hay dos tipos de personas:
Lo que saben **GIT** y los que no*



§ Utiliza una herramienta como

- ◆ Amanda
- ◆ Bacula
- ◆ Etc.

§ Prográmate la tuya propia!

- ◆ Seguramente te costará menos que aprender alguna ya existente.

§ Considera hacer copias “incrementales”

- ◆ Solo los ficheros modificados cada día.
- ◆ Y una completa completa cada semana (cada mes, año).

§ ¿¿**Es bueno hacer copias ciegas** (automáticas)??



- § Si nunca has restaurado un copia de seguridad...
 - ◆ Es probable que otro las restaure por ti (pierdes el trabajo).
- § Vaya, SIEMPRE tienes que comprobar que lo que guardas es CORRECTO y que eres capaz de RECUPERARLO cuando hace falta.
- § **No puedes dudar** a la hora de formatear un disco o reinstalar un sistema.
- § Si falla todo el sistema, entonces tienes que reinstalar un sistema nuevo y ponerle los datos de backup.
 - ◆ Puesto que vas a “mover” muchos datos
 - ◆ **Una orden incorrecta puede retrasar** la recuperación horas!!!



§ https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

§

