

Copias de seguridad

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Copias de seguridad

DOI [10.5281/zenodo.4700384](https://doi.org/10.5281/zenodo.4700384)

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



Copias de seguridad

- Introducción
- Planificación de las copias
- Tipos de copias
- Restauración de copias
- Frecuencia de copias
- Protección / Comprobación de copias
- Pixar / GitHub Arctic Code Vault

Introducción

Estudio [IBM Security 2018](#):

- Coste medio de una pérdida de datos: 148\$ por registro
- Tiempo medio en detectar una pérdida de datos: 196 días

Introducción

Estudio [Acronis](#):

- El 65% de los usuarios perdió datos el año 2018
- El 29% de las empresas tuvieron que parar su actividad temporalmente debido a una pérdida de datos en el 2018

Introducción

La información se puede perder por:

- Errores de usuarios o administradores del sistema
- Errores de software
- Errores de hardware
- Ataques o robo
- Desastres naturales

Introducción

Causas pérdida información:

- Negligencia (29%): borrado accidental de datos, modificaciones no deseadas, sobreescritura de archivos, etc.
- Fallo del Hardware (31%): fallo de dispositivos, drivers, corrupción de archivos, etc.
- Malware (29%): virus, troyanos, gusanos, etc.
- Otros: robo de los dispositivos de almacenamiento, desastres naturales, etc.

Introducción

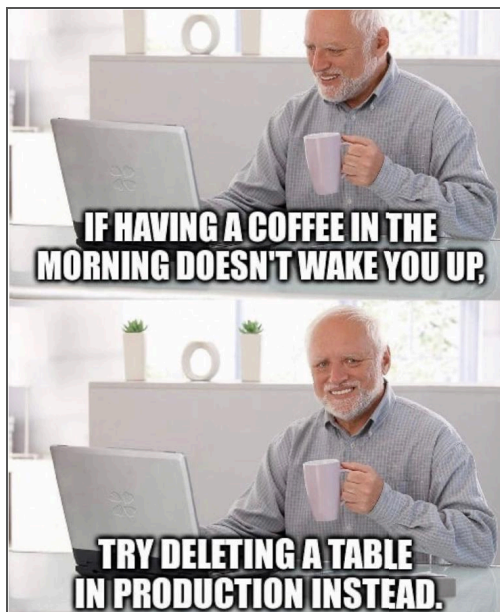
Hay dos tipos de ciclistas:

- Los que se han caído
- Los que se caerán

Hay dos tipos de informáticos:

- Los que hacen backups
- Los que harán backups

Introducción



Introducción



Pesadilla en la Web

@AlbertoTICote

...

¿A qué huele una nube quemada? OVH en estos momentos:



9:58 AM · Mar 10, 2021 · Twitter for Android

Introducción

Copias de seguridad (Backup): duplicar la información como medida preventiva para:

- Recuperar información perdida lo antes posible
- Tener un histórico de la evolución de la información
- Auditorías
- Informática forense

Introducción

ISO 27002:2013 estándar para seguridad de la información:

- Apartado 12.3: Information Backup
- Qué copiar
- Dónde copiarlo
- Cada cuánto copiarlo
- Mecanismos de recuperación
- Equivalente nacional: UNE 71501

Planificación de las copias

Regla 3-2-1:

- Por los menos 3 copias de un registro (2 copias + original)
- 2 copias en diferentes soportes, uno de ellos [offline](#)
- 1 copia en un lugar físico diferente al de las otras 2 (Fallas tectónicas)

Planificación de las copias

Versiones: simplemente sincronizar archivos no vale, ya que no impide la corrupción

De-duplicación: ahorrar espacio

Encriptar

"Append-only"

Planificación de las copias

Plan de Prevención:

- Decidir qué copiar
- Diseñar el plan de copias
- Implantarlo (Dispositivos, pruebas, ...)

Planificación de las copias

Plan de recuperación:

- Diseñar el proceso de recuperación
- Implantarlo

Planificación de las copias

¿Qué copiar?

- ¿Cómo de rápido debemos ser capaces de recuperar el sistema?
- ¿Existen distintas prioridades entre los datos?
- ¿Qué datos son los más valiosos?
- ¿De qué recursos disponemos?
- En general, aquello que es único / cambia rápidamente

Tipos de copias

Dia-cero

Completa

Incremental

Diferencial

Tipos de copias

Día-cero:

- Copiar todo antes de empezar a usar el sistema
- Para recuperar el sistema al punto de partida

Tipos de copias

Completa:

- Se realiza una copia de todos los datos
- Información duplicada
- Adecuada cuando hay muchas modificaciones
- Poco adecuada cuando la cantidad de información es muy grande

Tipos de copias

Incremental:

- Se realiza una copia de todos los datos modificados desde la última copia completa o incremental
- Puede ser muy rápida
- Optimiza el espacio

Tipos de copias

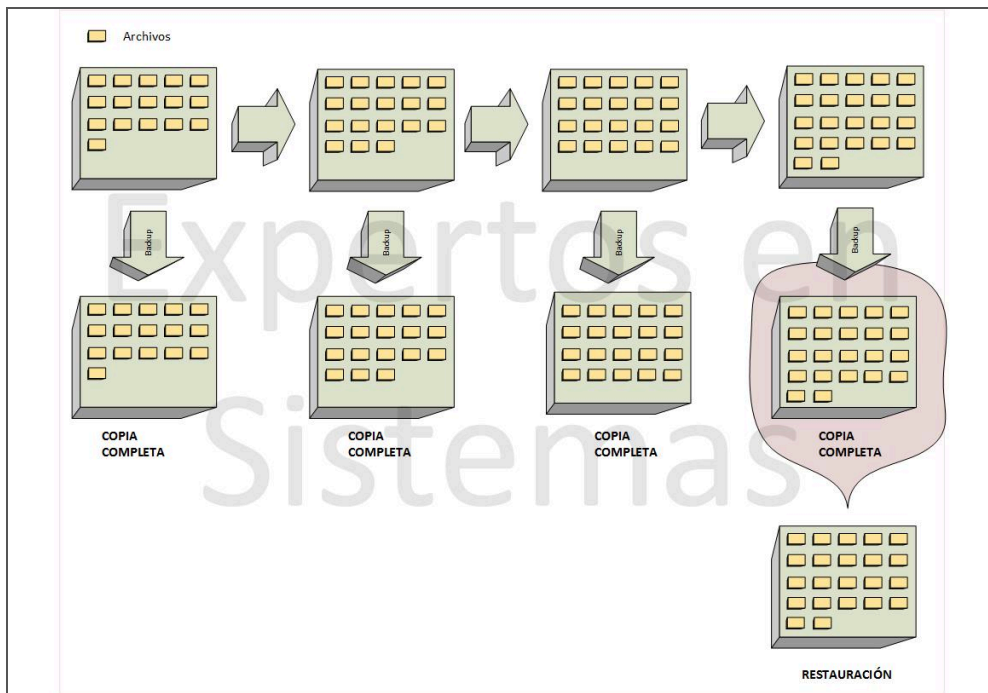
Diferencial:

- Se realiza una copia de todos los datos modificados desde la última copia completa
- Necesita menos espacio que una copia completa, pero más que una incremental

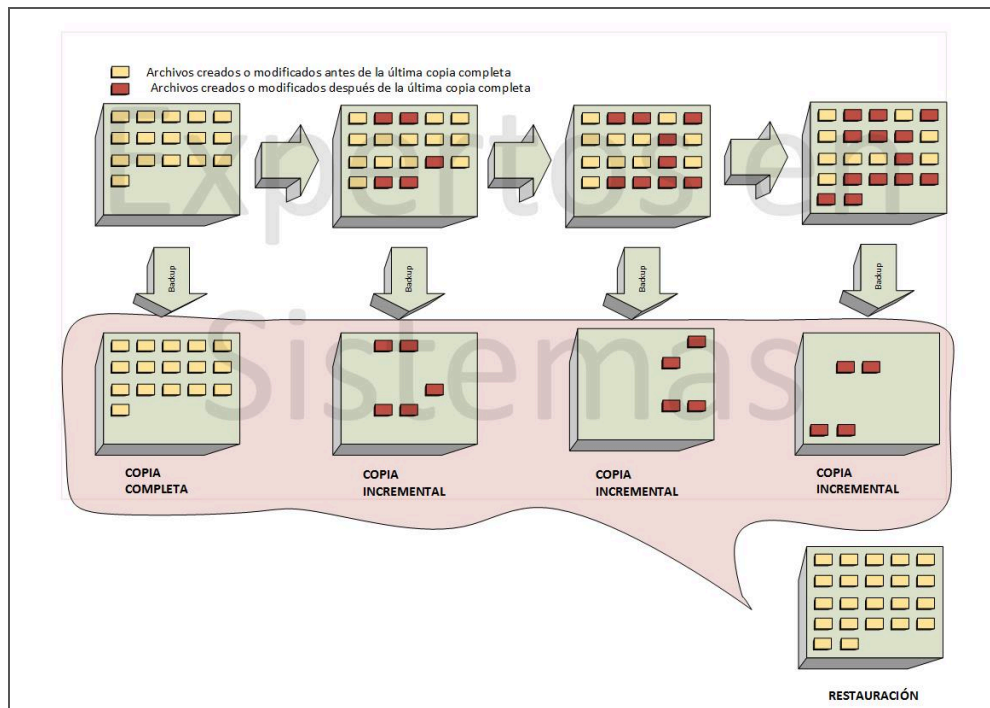
Restauración de copias

- Copia dia-cero: restaurar la copia
- Copia completa: restaurar la copia
- Copia incremental:
 - Restaurar la última copia completa
 - Restaurar una a una, siguiendo el orden todas las copias incrementales
- Copia diferencial:
 - Restaurar la última copia completa
 - Restaurar la última copia diferencial

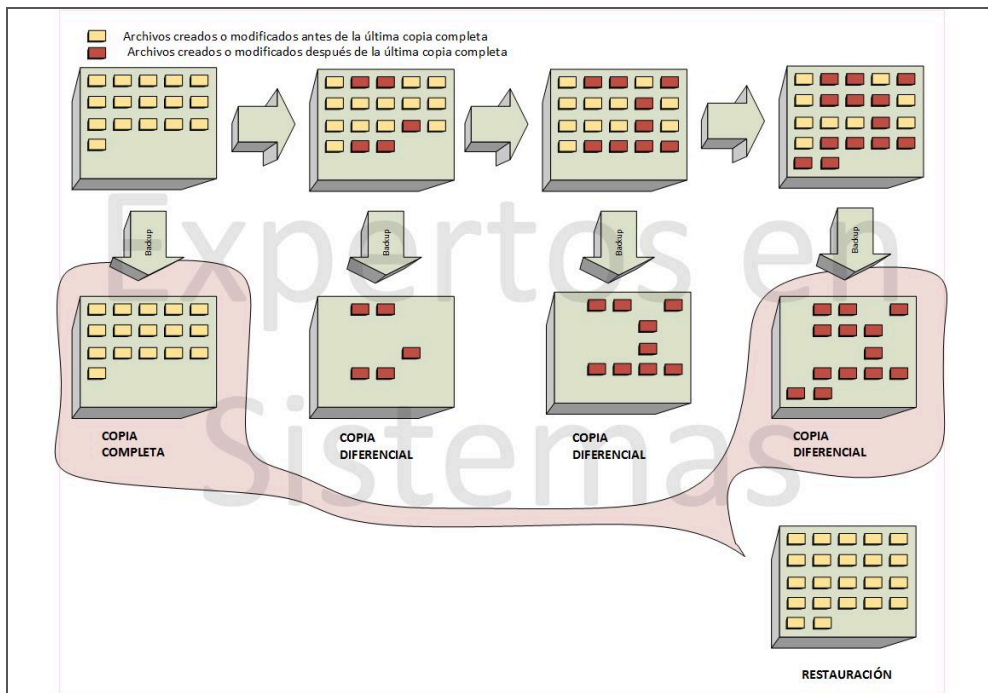
Restauración de copias (Completa)



Restauración de copias (Incremental)



Restauración de copias (Diferencial)



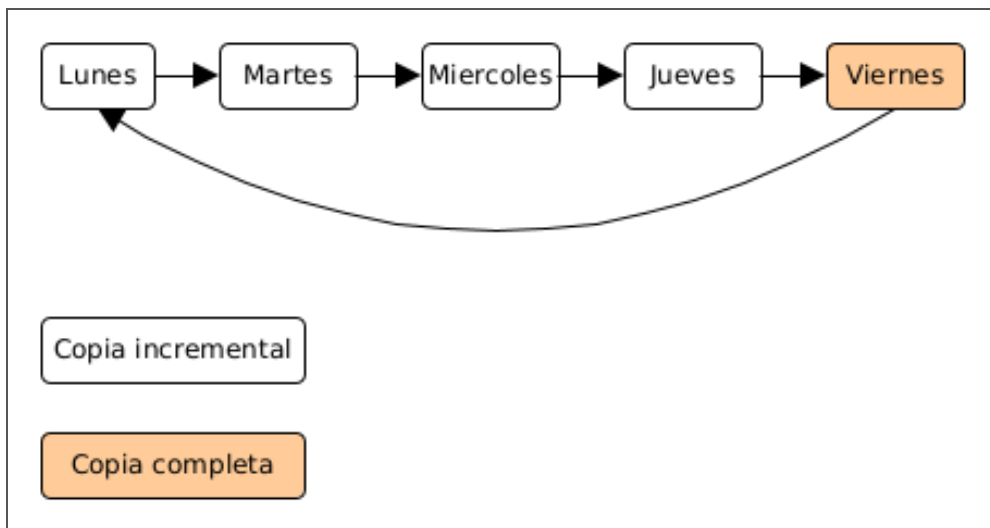
Frecuencia de copias

Teniendo en cuenta:

- Valor de la información
- Coste de no disponer de cierta información
- Cantidad de información
- Cantidad de cambios
- Coste de realizar las copias
- Para cada caso, se planifica un ciclo de copias

Frecuencia de copias (Ciclos)

Ejemplo ciclo semanal:



Frecuencia de copias (Cron)

Cron: servicio UNIX para ejecutar comandos de manera periódica:

- Crontab: archivo de configuración para definir los procesos a lanzar
- Daemon (crond): verifica periódicamente los archivos de configuración y lanza los procesos necesarios

Frecuencia de copias (Crontab)

```
* * * * * comando
| | | | |
| | | | +---- Día de la semana (0 - 7) (domingo es tanto 0 como 7)
| | | +----- Mes (1 - 12)
| | +----- Día del mes (1 - 31)
| +----- Hora (0 - 23)
+----- Minuto (0 - 59)
```

Protección de copias

Las copias también pueden sufrir ataques

Plan de protección:

- Acceso al soporte
- Disponibilidad
- Protección
- Tiempo de vida del soporte

Comprobación de copias

Hay que comprobar que las copias se realizan correctamente

De manera periódica hacer una prueba de restauración del sistema

Pixar

How Toy Story 2 Almost Got Deleted: Stories From Pixar An...



Pixar

Disney Just Laid Off The Pixar Employee Who 'Saved' *Toy Story 2*

Galyn Susman's backups famously saved the film when most of its files were accidentally deleted in 1998

By **Luke Plunkett** Published June 4, 2023



Screenshot: Toy Story 2

GitHub Arctic Code Vault

[GitHub Arctic Code Vault](#) ([¡Mi código también!](#))

GitHub Arctic Code Vault

