Copias de seguridad y restauración de la información

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Copias de seguridad y restauración de la información

DOI

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

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

https://twitter.com/AlbertoTICote/status/1369573281989328897

Introducción

Introducción

GitHub Arctic Code Vault (¡Mi código también!)

Definiciones

Copias de seguridad (Backup): duplicar la información como medida preventiva para ante posibles pérdidas poder recuperarla lo antes posible

Para:

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

Normativa

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 en diferentes soportes, uno de ellos offline
- 1 copia en otro sitio

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

Dia-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

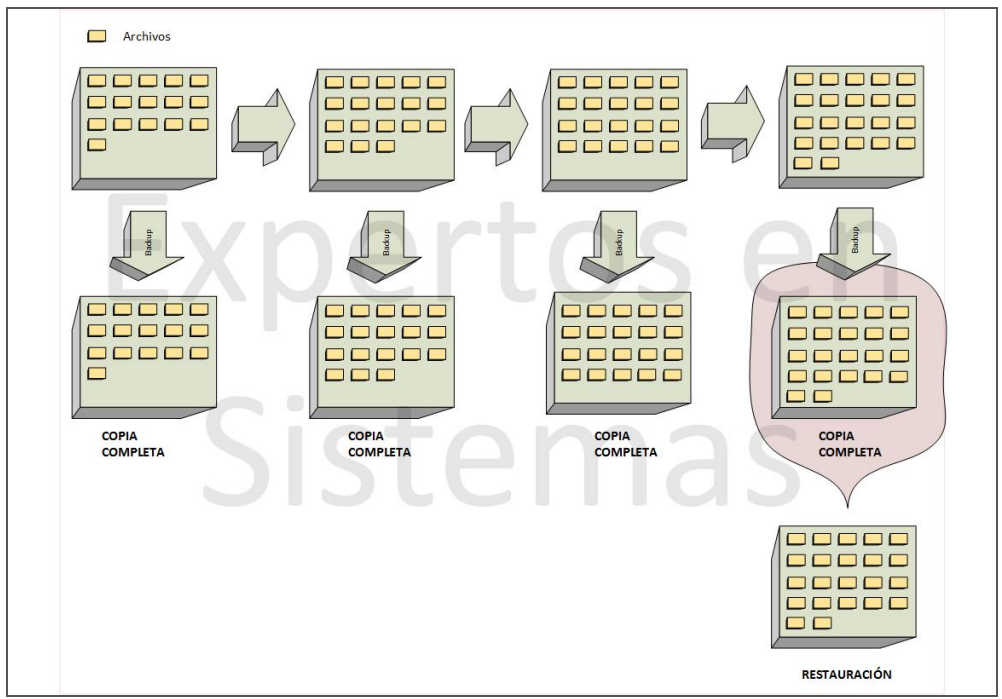
Diferencial:

- 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

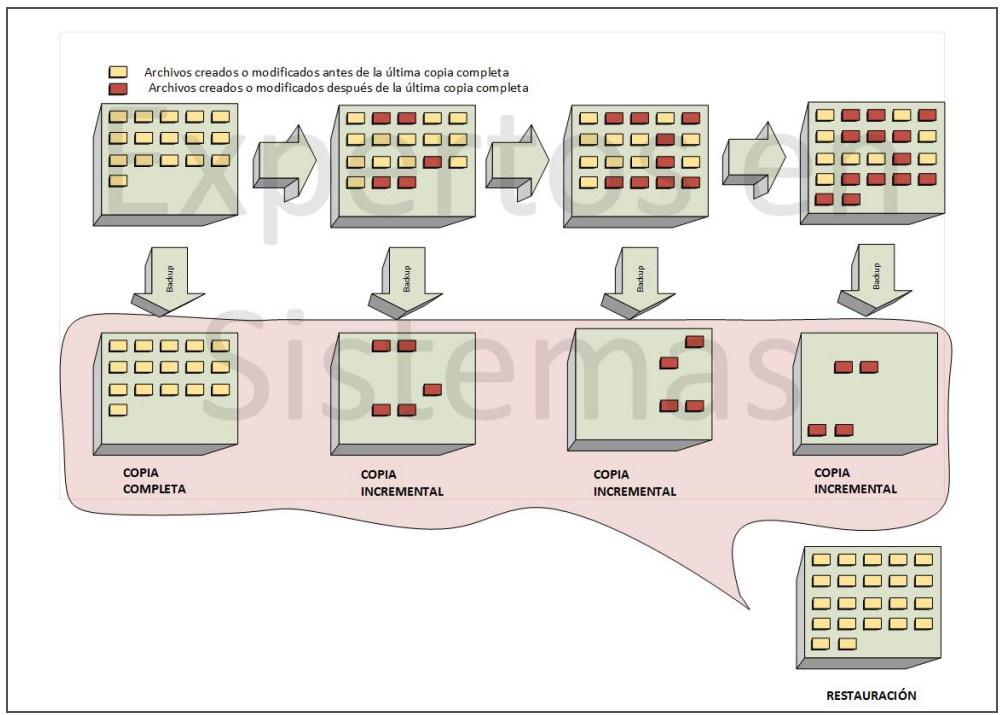
- Copia dia-cero: restaurar la copia
- Copia completa: restaurar la copia
- Copia incremental:
  - Restaurar la última copia completa
  - Restaurar una a una, siguiendo el orden todas las copias incrementales
- Copia diferencial:
  - Restaurar la última copia completa
  - Restaurar la última copia diferencial

Restauración de copias (Completa)



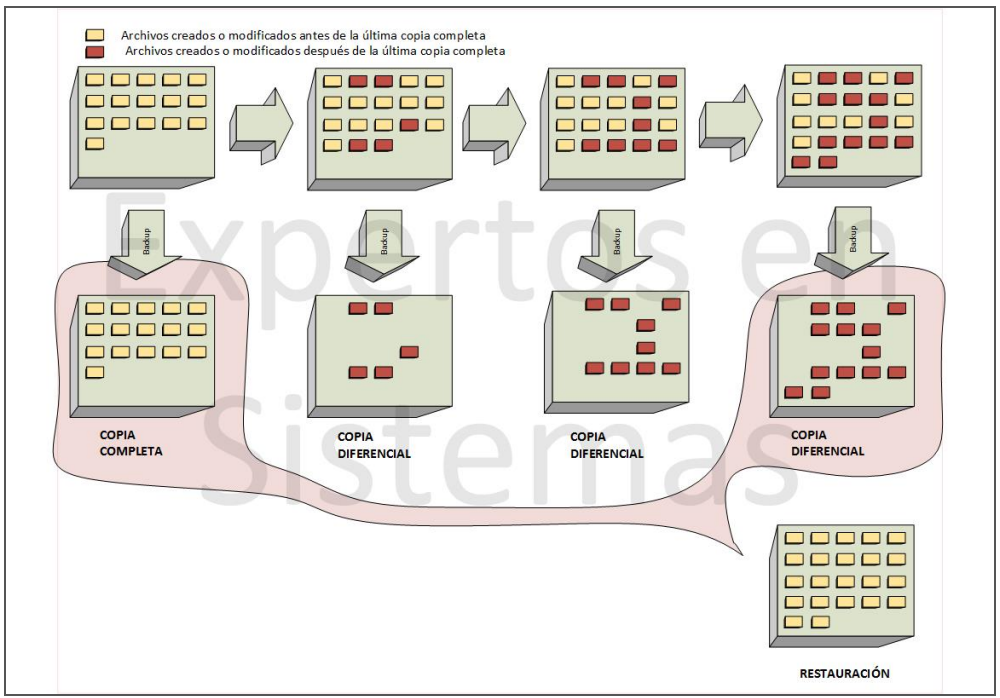
http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-iii/

Restauración de copias (Incremental)



http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-iii/

Restauración de copias (Diferencial)



http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-iii/

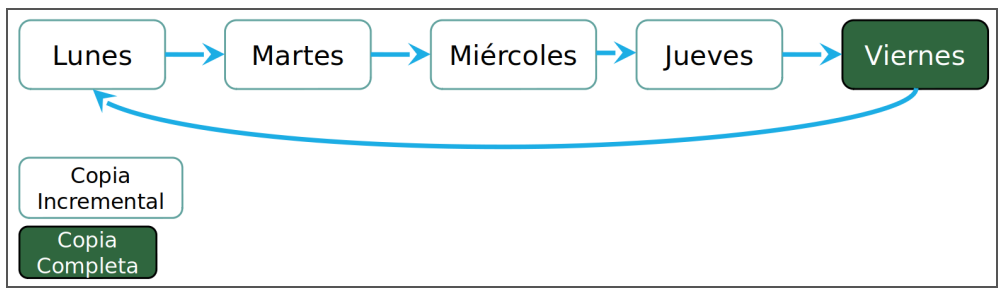
Frecuencia de copias

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:



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