Seguridad y Alta Disponibilidad

UNIDAD 2.
SEGURIDAD PASIVA

Contenidos

1. Principios de la Seguridad Pasiva
2. Copias de Seguridad
   - 2.1. Modelos de almacén de datos
   - 2.2. Recomendación sobre el tipo de copia a efectuar
   - 2.3. Recuperación de datos
3. Seguridad Física y Ambiental
   - 3.1. Centros de Procesado de Datos (CPD)
   - 3.2. Ubicación y acondicionamiento físico
   - 3.3. Control de acceso físico
   - 3.3. Sistemas Biométricos
   - 3.3. Circuito cerrado de televisión (CCTV)
4. Sistemas de Alimentación Ininterrumpida (SAI)
   - 4.1. Tipos de SAI
   - 4.2. Potencia necesaria

1

PRINCIPIOS DE LA SEGURIDAD PASIVA

Principios de la Seguridad Pasiva

- **Seguridad pasiva**:
  - Intenta minimizar el impacto y los efectos causados por accidentes.
  - Se consideran **medidas** o **acciones posteriores** a un ataque o incidente.
- Ataques o incidentes: **físicos o ambientales** (cortes de suministro, robos, incendios, desastres atmosféricos, etc…)
- Consecuencias:
  - ✓ Pérdida y/o mal funcionamiento del HW.
  - ✓ Falta de disponibilidad de servicios.
  - ✓ Pérdida de información.

Principios de la Seguridad Pasiva

Amenazas	Medidas paliativas
Suministro eléctrico Cortes, variaciones del nivel medio de tensión (subidas y bajadas), distorsión y ruido añadido.	▪ Sistema de alimentación ininterrumpida (SAI). ▪ Generadores eléctricos autónomos. ▪ Fuentes de alimentación redundantes.
Robos o sabotajes Acceso físico no autorizado al HW, SW y copias de seguridad	▪ Control de acceso físico: armarios, llaves, blindaje, biometría… ▪ Vigilancia mediante personal y circuitos cerrados de televisión (CCTV)
Condiciones atmosféricas y naturales adversas Temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos…	▪ Elegir la correcta ubicación de sistemas, teniendo en cuenta en la construcción la probabilidad de catástrofes naturales y ambientales. ▪ Centro de respaldo en ubicación diferente al centro de producción. ▪ Proporcionar mecanismos de control y regulación de temperatura, humedad, etc.

2

COPIAS DE SEGURIDAD

Copias de Seguridad *(Backups)*

- Réplicas de datos que nos permiten recuperar la información original en caso de ser necesario

- Un archivo, un conjunto de archivos o la totalidad de los datos

  ➡ corresponde al usuario determinar los datos que, por su importancia, serán almacenados en el *backup*.

Uno de los principios de seguridad: "Ordenar de mayor a menor prioridad qué archivos, datos y configuraciones son difíciles de volver a realizar o recuperar, y mantener de forma segura copias de seguridad de los mismos, distribuidas en espacio y tiempo".

Copias de Seguridad *(Backups)*

- ¿Dónde se guardan las *backups*?
  - ✓ Soportes extraíbles (CD/DVD, pendrive, cintas de backup…)
  - ✓ Directorios o particiones de la propia máquina.
  - ✓ Unidades compartidas de otros equipos, discos en red, servidores remotos…

- *Consejo*: cifrar y comprimir la copia de seguridad en un solo archivo, facilitando su confidencialidad, mantenimiento y distribución.

Copias de Seguridad *(Backups)*

- Modelos de almacenamiento masivo:
  - **DAS** *(Direct Attached Storage)*
    - Dispositivo de almacenamiento conectado directamente al sistema.
    - *Ej*: discos duros extraíbles, particiones de datos, pendrives…
  - **NAS** *(Network Attached Storage)*
    - Almacenamiento conectado en red.
    - *Ej*: servidores NAS, carpetas compartidas en red mediante NFS, FTP, SMB o CIFS…
  - **SAN** *(Storage Area Network)*
    - Dispositivos conectados directamente a una red de alta velocidad, para el almacenamiento de un gran volumen de datos.
    - Infraestructura necesaria posible sólo para grandes organizaciones.

Copias de Seguridad *(Backups)*

- Tipos de copia de seguridad:
  - **Completa** *(íntegra o total)*
    Copia de seguridad total de todos los archivos y directorios seleccionados.
  - **Incremental**
    Sólo se copia lo modificado desde la última copia de seguridad.
  - **Diferencial**
    Sólo se copia lo modificado desde la última copia de seguridad completa.

Copias de Seguridad *(Backups)*

- Recomendación sobre el tipo de copia:

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Copia recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + Incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + Diferencial	Intermedio	Lento	Sencilla	Datos cuya velocidad de cambio es moderada

Copias de Seguridad *(Backups)*

- Modelo óptimo: sistema mixto perfectamente planificado
  - ✓ Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total.
  - ✓ Todos los viernes, 23:00 horas: copia diferencial desde la copia de día 1.
  - ✓ Todos los días (salvo viernes y día 1), 23:00 horas: copia incremental desde la copia del día anterior.

- Garantizar la disponibilidad: distribuir las copias de seguridad en distintas ubicaciones.
  - ✓ Empresas especializadas en transporte y custodia
  - ✓ Alojamiento remoto, ***backup online*** o en la nube

Copias de Seguridad *(Backups)*

- EJEMPLOS y ENLACES
  - Servicio de alojamiento en la nube (*cloud computing*):
    - ✓ **Dropbox** (www.dropbox.com) 2 GB
    - ✓ **Idrive** (www.idrive.com/spanish/) 5 GB
    - ✓ **Mozy** (www.mozy.com)
  - Empresas especializadas en copia de seguridad remota (de pago):
    - ✓ www.perfectbackup.es
    - ✓ www.copiadeseguridad.com
    - ✓ www.copiasegura.com

PRÁCTICA 1. Copias de seguridad con herramientas del sistema

- **GNU/Linux**
  - **TAR** (Empaquetado/desempaquetado de archivos)

    Empaquetado: **tar –vcf** *nombre_archivo.tar* *nombre_archivos_a_empaquetar*

    Desempaquetado: **tar –vxf** *mi_archivo.tar*

    - **v** (verbose): descripción
    - **c** (create): crea un archivo *tar*
    - **x** (extract): extrae los archivos
    - **z** : compresión con gzip
    - **f** (file): indica que se dará un nombre
    - **t** : ver el contenido sin extraer

    -- **newer =** fecha: empaquetado incremental

  - **CRONTAB** (Automatización de tareas)

    crontab [-e | -l | -r] [usuario]

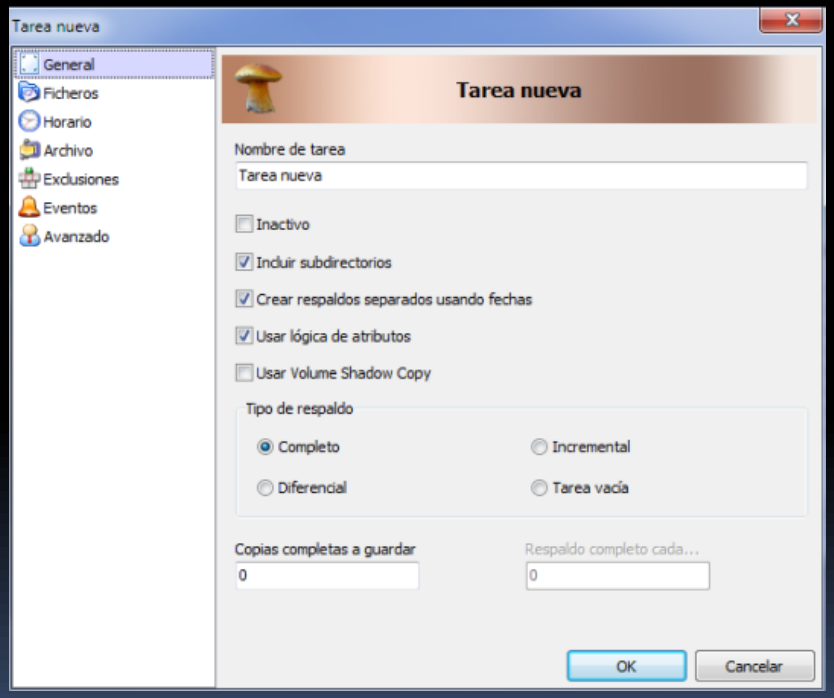
    - **e** : edición del *cron*
    - **l** : ver tareas programadas
    - **r** : borrar un archivo *cron*

PRÁCTICA 1. Copias de seguridad con herramientas del sistema

- **Windows**
  - Recomendaciones:
    - Dos particiones: 1) SO + aplicaciones
      2) Datos de usuario
    - No guardar información relevante en *Mis Documentos, Escritorio*…
      Podría perderse en caso de sobre-instalación
    - Una vez instalado y configurado todo, realizar puntos de restauración.
  - Herramientas: *Inicio/Todos los programas/Accesorios/Herramientas del Sistema*
    - **Copia de seguridad** *(→ archivo .bkf)*
    - **Restaurar Sistema**

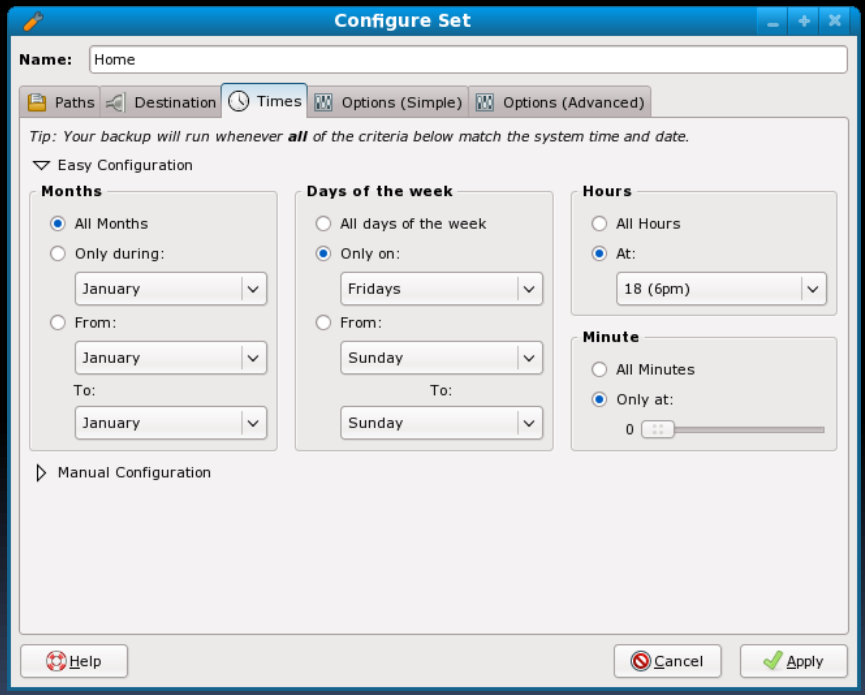
PRÁCTICA 2. Copias de seguridad con aplicaciones específicas

- **Windows:**



Cobian Backup

- **GNU/Linux:**



fwbackups

Copias de Seguridad *(Backups)*

RECUPERACIÓN DE DATOS

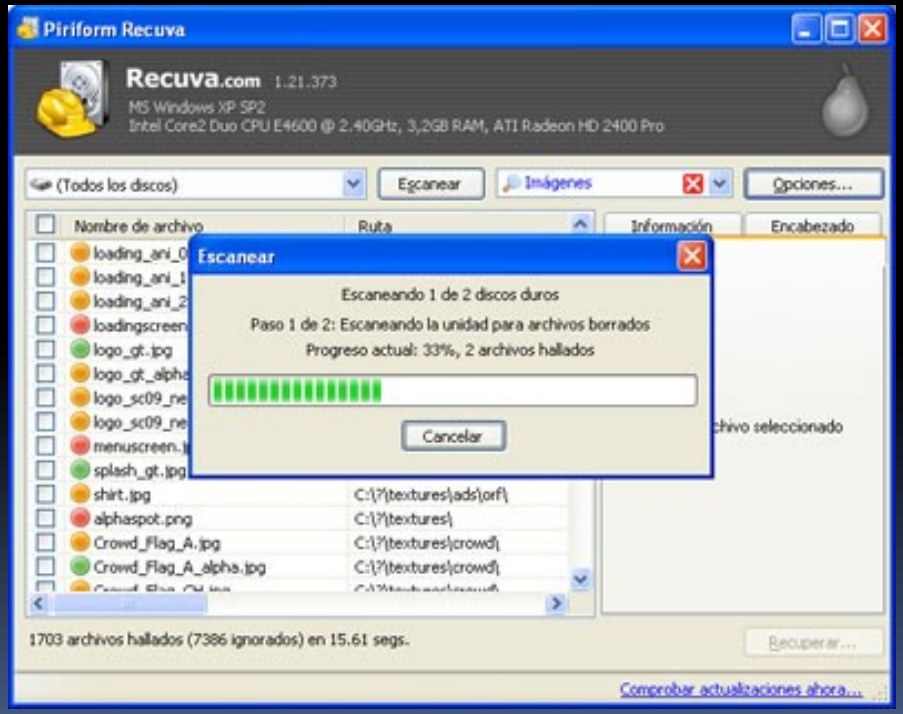
- Cuando se borra un fichero de un medio de almacenamiento, el S.O. marca aquellas posiciones que ocupaba dicho fichero en el dispositivo como libres, para almacenar nueva información, pero no las borra.

- Los datos permanecerán hasta que se sobrescriban con nueva información

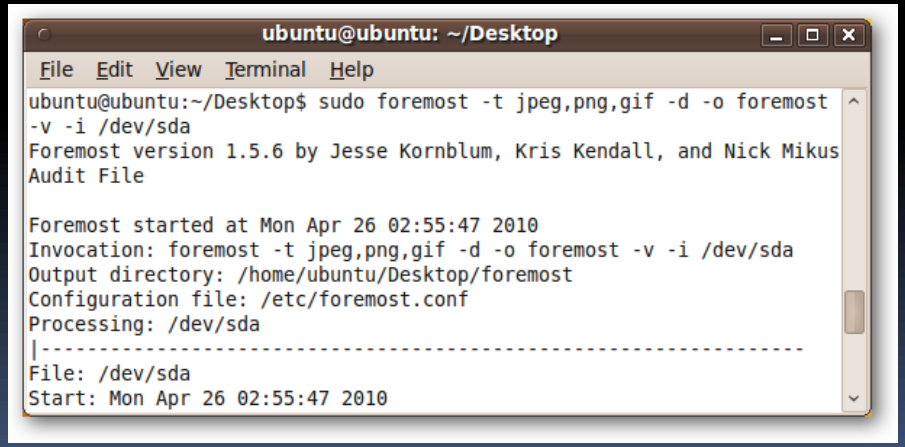
Es posible recuperar mediante software

PRÁCTICA 3. Recuperación de datos

- **Windows:**
  - ✓ Recuva



- **GNU/Linux:**
  - ✓ Foremost
  - ✓ Scalpel
  - ✓ TestDisk



3

SEGURIDAD FÍSICA Y AMBIENTAL

Seguridad Física y Ambiental

- Controles y medidas de seguridad, alrededor y dentro de la ubicación física de los sistemas informáticos, así como los medios de acceso al mismo, implementados para proteger el HW y medios de almacenamiento de datos.

- Medidas:
  - ✓ CPD y centros de respaldo
  - ✓ Ubicación y acondicionamiento físico
  - ✓ Control de acceso físico
  - ✓ Sistemas biométricos
  - ✓ Circuito cerrado de televisión (*CCTV*)

Centro de Procesamiento de Datos (**CPD**)

- Lugar donde se ubican los recursos necesarios para el procesamiento de la información de una organización.
- Puede ser una sala de gran tamaño o un incluso un edificio, que albergará gran cantidad de equipamiento informático y, en general, electrónico.

- Prácticamente todas las compañías medianas o grandes tienen algún tipo de CPD. Las más grandes llegan a tener varios interconectados, con distintos **centros de respaldo**.

Centro de Procesamiento de Datos (CPD)

Centro de respaldo

- CPD diseñado para tomar el control de otro CPD en caso de contingencia o fallo.
- Localización distinta al CPD principal.
- Equipamiento HW compatible con el CPD original (no necesariamente el mismo), SW idénticos y datos replicados.

El *centro de respaldo* debe contar con una réplica de los mismos datos con los que se trabaja en el CPD original

Ubicación y acondicionamiento físico

- Tener en cuenta las condiciones atmosféricas adversas al decidir la ubicación y posterior construcción de los *data centers*.

Aspectos a considerar	Precauciones y/o medidas
Incendios	✓ Ubicación en área no combustible o inflamable ✓ Disponer de un sistema antiincendios
Temperatura y humedad	✓ Sistema de aire acondicionado
Inundaciones	✓ Ubicación estanca de agua
Terremotos	✓ Conocer la actividad sísmica de la zona ✓ Construcciones antisísmicas
Rayos e interferencias electromagnéticas	✓ Salas protegidas mediante jaula de Faraday

Control de acceso físico

- Uso de **credenciales de identificación** y **acceso** para apertura/cierre de puertas, entrada/salida a los distintos sectores de una empresa.
  - A una persona se le puede identificar por:
    - **Algo que posee**: llave, tarjeta de identificación, tarjeta inteligente.
    - **Algo que sabe**: PIN *(Personal Identification Number)*, password.
    - **Algo que se es** (señas de identidad: manos, ojos, huellas digitales, voz) o **sabe hacer** (firma escrita). *Biometría*.
  - Los identificadores se almacenan en un **base de datos** que debe controlar un **servicio de vigilancia**.



Control de acceso físico

- Disponer de **armarios** o **racks bajo llave** en las salas de equipamiento informático
  - Dimensiones para racks normalizados:
    - Ancho: guías de 19 pulgadas (1'' = 2,54 cm)
    - Alto: guías de 1U (1U = 1,75'')
    - Profundidad (no normalizada)
  - Dispositivos que se suelen alojar: servidores, paneles de parcheo, sistemas de audio y video, switches, routes, SAI, periféricos para configuración…
  - Protección antirrobo bajo llave.

- Usar cámaras de videovigilancia o circuitos cerrados de televisión (**CCTV**)
  Cámaras más usadas (bajo coste y buenas prestaciones): ***cámaras IP***.

Sistemas biométricos

- **Biometría**: parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos, utilizando métodos estadísticos.
- La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una **BD**.
- Sistemas **muy seguros**: las características biométricas de una persona son **intransferibles** a otra.

Huella dactilar

Iris

Voz

Escritura / firma

Sistemas biométricos

	 Ojo (*iris*)	 Huellas dactilares	 Escritura y firma	 Voz
Fiabilidad	Muy alta	Muy alta	Media	Alta
Facilidad de uso	Media	Alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Media	Media
Aceptación	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Baja	Media

4

SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

Sistemas de Alimentación Ininterrumpida (**SAI**)

- Un **SAI**, o también **UPS** (*Uninterruptible Power Supply*, suministro de energía ininterrumpible), es un dispositivo que:
  - Proporciona energía eléctrica a los dispositivos que tenga conectados tras un corte de suministro eléctrico, durante un tiempo limitado, gracias a las **baterías** de las que dispone.
  - Mejora la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red eléctrica.

- A los **SAI** se conectan equipos llamados **cargas** o **equipos críticos** (aparatos médicos, industriales o informáticos) que requieren estar en todo momento operativos y sin fallos, por lo que deben tener siempre alimentación y que ésta sea de calidad.

Sistemas de Alimentación Ininterrumpida (**SAI**)

- Tipos de **SAI**:
  - **SAI OFFLINE**
    - ✓ Sólo generan señal cuando existe corte eléctrico. No estabilizan la corriente.
    - ✓ Gama baja. Recomendados para equipos en el hogar.
  - **SAI INLINE** o ***LINE INTERACTIVE***
    - ✓ Generan señal cuando existe corte eléctrico. Estabilizan la corriente incorporando un estabilizador continuo de salida o *AVR*.
    - ✓ Gama media. Recomendados para pymes.
  - **SAI ONLINE** o de ***DOBLE CONVERSIÓN***
    - ✓ Generan señal nueva de forma continua, independientemente de la entrada.
    - ✓ Gama alta, pensados para proteger sistemas críticos.

Sistemas de Alimentación Ininterrumpida (**SAI**)

- Potencia necesaria:
  - Unidades de potencia:
    - Voltiamperio (**VA**): potencia aparente, para configurar el SAI.
    - Vatio (**W**): potencia real, consumida por el sistema.
  - Para calcular cuánta energía requiere un SAI, se debe conocer el consumo del dispositivo.
    - Si se conoce la potencia real (en W), multiplicamos por 1,4 para obtener la potencia aparente (en VA).

      Ejemplo: 200 W x 1,4 = 280 VA.
    - Si lo que se encuentra es la tensión (en voltios) y la corriente (en amperios), la potencia aparente será el producto de ambas. **P =V x I**.

      Ejemplo: 3 amperios x 220 voltios = 660 W

Sistemas de Alimentación Ininterrumpida (**SAI**)

- Potencia necesaria:
  - La carga total enchufada a la batería del SAI se recomienda que **no sobrepase el 70%** del total de la potencia suministrada por la misma.
  - Ejemplo:
    - Se quieren enchufar 4 tomas de una SAI, 2 PC y 2 monitores que consumen un total de 200 W.
    - La SAI deberá suministrar: 200 W x 1,4 = 280 VA
    - La SAI deberá tener, al menos, una potencia máxima suministrada de 280 x 100/70 = 400 VA.

Enlaces de interés

- SAI:
  - ✓ www.newsai.es
- Biometría:
  - ✓ www.biometriaaplicada.com
- Soluciones de seguridad física:
  - ✓ www.accesor.com
  - ✓ www.apc.com/es
  - ✓ www.zksoftware.es