Capítulo 2.
SEGURIDAD PASIVA

Autor: Jesús Costas Santos

SEGURIDAD PASIVA

Índice de contenidos

SEGURIDAD PASIVA

2.1 PRINCIPIOS DE LA SEGURIDAD PASIVA

- La **seguridad pasiva** minimizar el impacto y los efectos de accidentes: **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 hardware.*
  - *Falta de disponibilidad de servicios.*
  - *Pérdida de información.*

SEGURIDAD PASIVA

2.1 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 o UPS). - Generadores eléctricos autónomos. - Fuentes de alimentación redundantes.
Robos o sabotajes: acceso físico no autorizado al hardware, software 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.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- Medida transversal a los problemas de seguridad informática: Recuperación de Datos → Copia de seguridad.
- **Las copias de seguridad o *backup*, réplicas de datos que nos permiten recuperar la información original,** es uno o varios archivos digitales, **considerados lo suficientemente importantes para ser conservados**.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Soportes**: Disco duro, CD/DVD, memorias de estado sólido USB, cintas, etc.
- **Modelos de almacenamiento:**
  - DAS: Dispositivo conectado directamente al sistema. Ej: Disco duro o pendrive.
  - NAS: Almacenamiento en red. Ej: Carpetas compartidas mediante SMB, FTP o similar.
  - SAN: Red específica de almacenamiento. Ej: Sistemas, discos de almacenamiento y red específica, para el almacenamiento de una gran volumen de datos.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Tipos de copia:**
  - Desestructurada.
  - Completa o total: Todos los datos.
  - Incremental: solo se copia lo modificado desde la última copia de seguridad.
  - Diferencial: solo se copia lo modificado desde la última copia de seguridad total o completa.
  - Modelo óptimo: Planificación y Mixto:
    - Todos los días 1 mes, 23 h: copia de seguridad total.
    - Todos los viernes 23 h: copia diferencial desde copia día 1.
    - Todos los días 23 h: copia incremental desde copia día anterior.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Tipos de copia:**
  - Modelo óptimo:
    - Distribución geográfica: Copias custodiadas externas y copia en la nube u on-line.

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

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Prácticas y ejemplos**:
- Opciones a tener en cuenta en una herramienta de copia de seguridad:
  - Compresión / Duplicado / Tipo de copia / Cifrado / Nombre de archivo / Planificación o automatización de la tarea.
  - Copias de seguridad con herramientas del sistema:
    - Windows:
      - Herramienta preinstalada en el SO de Copias de seguridad.
      - Partición específica de datos. Mejora la recuperación.
      - Puntos de restauración.
    - GNU/Linux: Modo comando tar: empaquetar y comando cron: automatizar tarea.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Prácticas y ejemplos**:
- Opciones a tener en cuenta en una herramienta de copia de seguridad:
  - Compresión / Duplicado / Tipo de copia / Cifrado / Nombre de archivo / Planificación o automatización de la tarea.
  - Copias de seguridad con herramientas específica:
    - Windows:
      - Cobian Backup. Todas las opciones a tener en cuenta están incluidas.
    - GNU/Linux:
      - **Fwbackups**.

SEGURIDAD PASIVA

2.2 COPIAS DE SEGURIDAD

- **Recuperación de datos**: Cuando se borra un fichero de un medio de almacenamiento el sistema operativo 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.
  - Windows:
    - **Recuva.**
  - GNU/Linux:
    - **Testdisk, PhotoRec, Foremost, Scalpel.**

SEGURIDAD PASIVA

2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- **Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas**.
- Medidas costosas justificables en sistemas críticos: centros de procesamiento de datos o CPD: ubicación donde se concentran todos los recursos para procesamiento de la información de una organización.

SEGURIDAD PASIVA

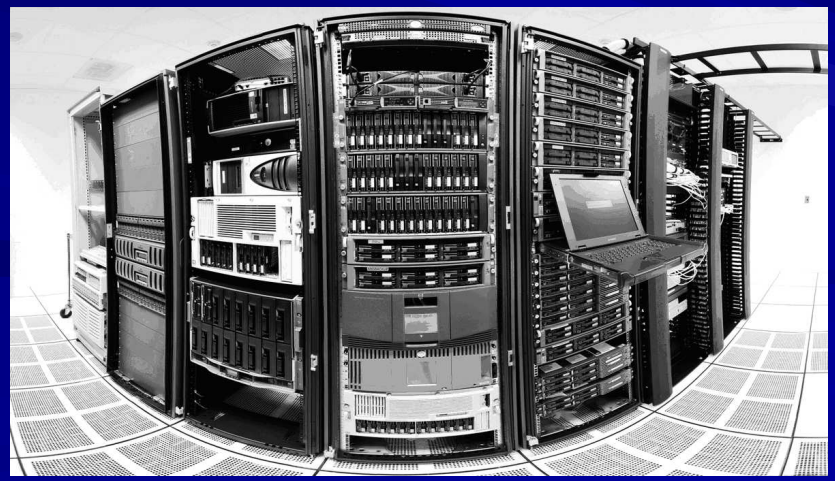
2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- **Grandes organizaciones:** Varios CPD interconectados e incluso duplicados: centros de respaldo con información sincronizada.
- Parámetro fundamental CPD: **garantizar la continuidad y alta disponibilidad**:
  - Alta Disponibilidad y Monitorización 99,999%. 24x7x365.
  - **Seguridad, redundancia y diversificación**: almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y servicios de telecomunicaciones con balanceo de carga, SAI o sistemas de alimentación ininterrumpida, control de acceso físico, etc.
  - **Control ambiental/prevención de incendios, inundaciones, etc.**

SEGURIDAD PASIVA

2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- Sala Fría, nevera o pecera:
  - Concentra grandes servidores, con un sistema específico de refrigeración (21 - 23ºC, óptimo 22,3ºC), y humedad relativa entre 40% y 60%.
  - Medidas estrictas de seguridad acceso físico,
  - Medidas de extinción de incendios: agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.



SEGURIDAD PASIVA

2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- Ubicación y acondicionamiento físico:
  - Minimizar probabilidad de ocurrencia o impacto:
    - Sistema antiincendios
    - Aire acondicionado: control temperatura y humedad.
    - Ubicaciones estancas contra inundaciones.
    - Control de probabilidad sísmica → construcciones antisísimicas.
    - Jaula de faraday → protección interferencias electromagnéticas y de rayos.

SEGURIDAD PASIVA

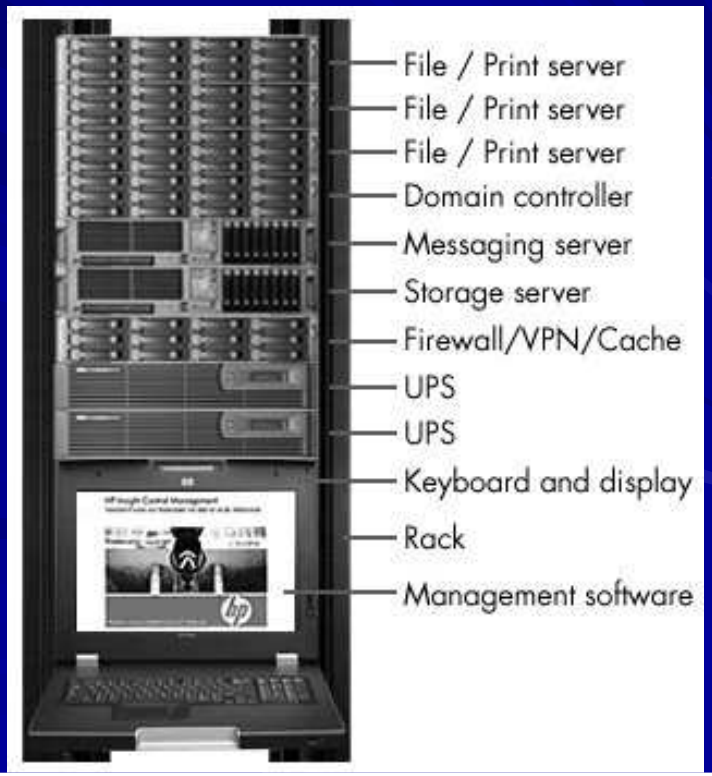
2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- Control de acceso físico:
  - Credenciales de identificación y acceso:
    - Posesión: Tarjeta inteligente.
    - Conocimiento: Clave o PIN.
    - Ser o Hacer: Biometría → huella o firma.
- Software específico con base de datos de usuarios autorizados y personal de vigilancia.
- Racks o Armarios Normalizados: Protección robo bajo llave.
  - Ancho: guías de 19”
  - Alto: guías para atornillar equipos 1U=1,75”.
  - Profundidad: No normalizada.
- CCTV: Cámaras de video vigilancia. Cámaras IP.

SEGURIDAD PASIVA

2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- Racks o Armarios Normalizados: Protección robo bajo llave.
  - Ancho: guías de 19”
  - Alto: guías para atornillar equipos 1U=1,75”.
  - Profundidad: No normalizada.



SEGURIDAD PASIVA

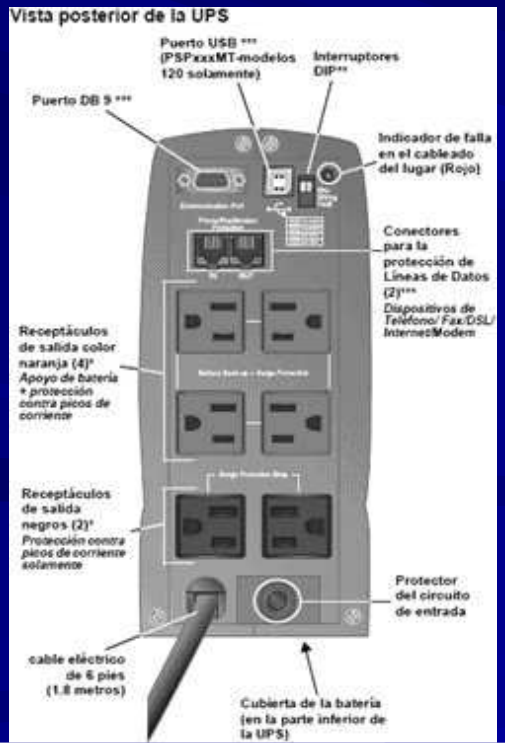
2.3 SEGURIDAD FÍSICA Y AMBIENTAL

- Biometría**: parte de la biología estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos**.
- Realiza mediciones electrónicas, guarda y compara características únicas para la identificación de personas.
  - Huella dactilar: Identificación de minucias. Más empleado. Mejor relación fiabilidad /coste.
  - Verificación ocular: Iris. Más fiable pero más intrusivo con capacidad de identificar enfermedades.
  - Verificación de voz. Muy variable.
  - Verificación de firma. VAF.

SEGURIDAD PASIVA

2.4 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

- Un SAI (Sistema de Alimentación Ininterrumpida), o UPS (*Uninterruptible Power Supply*, suministro de energía ininterrumpible), con baterías proporciona energía eléctrica tras un corte de suministro eléctrico.



SEGURIDAD PASIVA

2.4 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

- Otra función: mejorar la calidad de la energía eléctrica, filtrando subidas y bajadas de tensión y eliminando armónicos de la red eléctrica.
- Tipos de SAI:
  - Offline: sólo generan señal cuando existe corte eléctrico. Gama baja.
  - Inline o línea interactiva: con estabilizador continuo de salida o AVR. Gama media.
  - Online o doble conversión: generan señal nueva de forma continua. Gama alta.

SEGURIDAD PASIVA

2.4 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

- Potencia necesaria para una SAI:
  - Se mide en VA: potencia aparente.
  - Equipos de consumo conectados a carga:
    - Potencia real W → x 1,4 = VA necesarios.
- Métodos de cálculo:
  - Medida de potencia de consumo de equipos conectados con pinza amperimétrica (A) x 230V = W consumidos.
  - Consumo medio de equipos W, manuales de fabricante.
  - Consumo estimado W, con referencias de web Energy Star.
- Potencia de carga en SAI al 60-80% del total.

SEGURIDAD PASIVA

DIRECCIONES DE INTERÉS

- Sitio web sobre SAI.
  - http://www.newsai.es/
- Catálogo, manuales y documentación de SAI.
  - http://www.apc.com/es/
- Noticias y medidas de seguridad para CPD.
  - http://www.seguridadcpd.com/
- Seguridad física. Red – Iris.
  - http://www.rediris.es/cert/doc/unixsec/node7.html
- Soluciones técnicas para el control de acceso.
  - http://www.accesor.com/
- Soluciones técnicas de biometría.
  - http://www.biometriaaplicada.com/
- Sistema biométrico de reconocimiento de voz. Sistema BioCloser:
  - http://www.biometco.com/productos/control.acceso/biocloser.php
- Soluciones de seguridad para aulas de ordenadores
  - www.senfor.com

SEGURIDAD PASIVA

DIRECCIONES DE INTERÉS

- Soluciones de control de accesos a CPD
  - www.zksoftware.es
- Soluciones de almacenamiento para empresas HP:
  - http://welcome.hp.com/country/es/es/smb/storage.html
- Empresa dedicada a copias de seguridad remotas:
  - www.copiadeseguridad.com/
- Soluciones de almacenamiento y copia de seguridad Dell:
  - www.dell.es/
- Blog de seguridad informática. Copias de seguridad:
  - www.bloginformatico.com/etiqueta/copias-de-seguridad
- Copias de seguridad y recogida de dispositivos de almacenamiento extraíble:
  - www.copiasegura.com/rcs.htm.
- Recuperación de información y copia de seguridad:
  - www.copiadeseguridad.com
  - www.perfectbackup.es
- Soluciones técnicas para el control de acceso físico.
  - http://www.accesor.com/
- Soluciones técnicas de biometría.
  - http://www.biometriaaplicada.com/
- Energy-star: en la web podemos encontrar información y consejos sobre las ventajas que supone la compra del equipo ofimático más eficiente desde el punto de vista energético, qué configuración de ahorro de energía resulta más ventajosa y cómo sacarle el máximo rendimiento.
  - www.eu-energystar.org

SEGURIDAD PASIVA

SOFTWARE

- **FreeNAS**: Servidor NAS de distribución libre:
  - www.freenas.org
- Almacenamiento de datos en Internet **Idrive, Dropbox, Mozy**:
  - www.idrive.com
  - www.dropbox.com
  - www.mozy.com
- **Everest**: Software de testeo Hardware.
  - http://www.lavalys.com/support/downloads
- **Cobian Backup**: Software de copia de seguridad.
  - http://www.educ.umu.se/~cobian/cobianbackup.htm
- **Fwbackups**: Software de copia de seguridad, entornos GNU/Linux.
  - www.diffingo.com
- **Drivermax**: Actualizaciones y copia de seguridad de drivers.
  - http://www.drivermax.com

SEGURIDAD PASIVA

SOFTWARE

- **Recuva**: Recuperación de archivos
  - http://www.piriform.com/recuva
- **TestDisk**: recupera particiones perdidas y sectores de arranque en entornos GNU/Linux, y **PhotoRec**, que es una herramienta sencilla de usar para la recuperación de archivos.
  - www.cgsecurity.org/wiki/TestDisk
- **Foremost** recupera archivos en entornos GNU/Linux, basándose en una serie de estructuras internas además de otros datos.
  - http://foremost.sourceforge.net/
- **Scalpel:** recupera archivos en entornos GNU/Linux.
  - http://www.digitalforensicssolutions.com/Scalpel/
- **Biocloser:** sistema biométrico de reconocimiento de voz.
  - http://www.agedum.com/BioCloser/tabid/110/Default.aspx
- **Biopassword:** sistema biométrico de acceso lógico mediante reconocimiento biométrico de la pulsación de contraseña en teclado.
  - http://www.biopassword.com

SEGURIDAD PASIVA

NOTICIAS

- **Caída general de 13 horas durante la madrugada del 23 de septiembre de 2008**
  - Fuente: http://www.weblogssl.com/2008/09/23-caida-general-de-x-horas-durante-la-madrugada-del-23-de-septiembre-de-2008
- **Análisis de mejoras de un CPD en una solución real. Lee y analiza el siguiente caso real "Solución integral de CPD altamente seguro para Supermercados Condis".**
  - **Fuente** web: http://www.abast.es/cs_condis_cpd.shtml