Práctica 3 - Seguridad pasiva

**Índice**

1. En la fase de reducción, al conjunto de medidas que tratan de evitar o de minimizar no el incidente, sino el impacto y los efectos causados por el mismo, ¿se le llama?
2. ¿Qué medidas de seguridad pasiva destacarías?
3. Un SAI o UPS es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica (durante un tiempo limitado) tras un corte del suministro. Algunos de ellos, además, protegen a los equipos de sobretensiones proporcionando una salida de corriente estabilizada. ¿Cuáles son los dos tipos fundamentales de SAIs?
4. Normalmente no todos los equipos se conectan al SAI, sólo los críticos e indispensables. Suele haber dos tipos de enchufes diferenciados: unos conectados al SAI y otros no. El cálculo de la capacidad necesaria a la hora de adquirir un SAI es fundamental. Se recomienda elegir un SAI con potencia de, al menos, un 30% superior a la potencia aparente requerida. La potencia aparente requerida es igual a la potencia real de consumo dividida entre 0'75, es decir, la potencia aparente requerida es superior a la potencia real de consumo. Suponiendo que se quiere proteger mediante un SAI un aparato que funciona a 220 voltios y consume 3'42 amperios, ¿qué potencia debería soportar el SAI?
5. El software es un activo que no siempre puede restituirse sólo con dinero. De ahí su importancia. Elegir el sistema de almacenamiento adecuado para datos y establecer una correcta política de copias de seguridad de los mismos es fundamental. RAID (junto con las copias de seguridad), es una de las tecnologías pasivas más usadas para asegurar datos. El uso de RAID por software es sólo un sucedáneo, pero la forma de probar y demostrar su funcionamiento en el aula es hacerlo por software. Se usará para ello una máquina virtual de Windows Server. ¿En qué consiste la configuración RAID 1?
6. Se va a probar el funcionamiento de RAID 1 creando dos discos de 1GB en VMware conectados a la máquina virtual. En la máquina virtual, desde el administrador de discos, se crea un nuevo “nuevo volumen reflejado”. Se siguen los pasos por los que guía el asistente de configuración. Se crean o copian algunos archivos de datos en el disco resultante y se puede simular una avería en uno de ellos apagando bruscamente la máquina virtual, desconectando uno de los discos y rearrancando la máquina para comprobar que los datos siguen accesibles.
7. ¿En qué consiste la configuración RAID 5?
8. Se va a probar el funcionamiento de RAID 5 usando tres discos iguales y un cuarto disco para reparar el volumen después de simular la rotura de uno de los discos.
9. ¿Qué es un NAS?
10. Conviene señalar que es interesante el uso de herramientas de diagnóstico de discos como CrystalDiskInfo. Observad la información que proporciona CrystalDiskInfo de un disco duro.

**1. Respuestas teóricas (razonadas)**

**a) "En la fase de reducción, al conjunto de medidas que tratan de evitar o de minimizar no el incidente, sino el impacto y los efectos causados por el mismo, ¿se le llama?"**

**Respuesta:** A ese conjunto de medidas se le llama **medidas de mitigación** (o simplemente *mitigación*).

**Justificación:**

* En gestión de incidentes y de riesgos hay varias fases: prevención, detección, contención, mitigación/reducción del impacto y recuperación. Las medidas de **contención** se centran en limitar la expansión o propagación del incidente; las medidas de **mitigación** buscan reducir el impacto y los efectos residuales —es decir, minimizar daños, pérdida de datos o tiempo de inactividad—.
* Por tanto, la fase que reduce efectos y consecuencias se denomina mitigación.

**b) ¿Qué medidas de seguridad pasiva destacarías?**

**Respuesta (resumen y ejemplos):**

1. **Redundancia de energía y alimentación**: SAI/UPS, fuentes de alimentación redundantes (PSU redundantes en servidores), protección contra sobretensiones y filtros.
2. **Backups y copias fuera de sitio**: políticas de copia (diarias, semanales), cifrado de copias, pruebas de restauración periódicas.
3. **RAID y almacenamiento redundante**: RAID por hardware o software (RAID 1, RAID 5, RAID 6) para tolerancia a fallos.
4. **Control físico de acceso**: cerraduras, puertas acorazadas, tarjetas de acceso, control de visitantes.
5. **Sistemas contra incendios y control ambiental**: detectores de humo, extinción (FM-200 / gas inerte), climatización (HVAC), control de humedad y temperatura.
6. **Aislamiento físico y topología**: ubicación de equipos críticos en salas técnicas, separación de racks, cableado ordenado y etiquetado.
7. **Monitoreo pasivo y registro**: CCTV (vigilancia pasiva), registros de accesos, sistemas de telemetría de hardware (temperatura, ventiladores).
8. **Protección contra fallos físicos de disco**: uso de SMART, herramientas de diagnóstico (CrystalDiskInfo), sustitución proactiva.
9. **Segmentación lógica y políticas de respaldo de configuración**: guardar configuraciones de equipos (switches, routers, firewall) y control de versiones.

**Por qué son pasivas:** no actúan de forma activa para bloquear o responder en tiempo real (eso sería activo), sino que reducen la probabilidad o el impacto de fallos y permiten recuperación más sencilla.

**c) ¿Cuáles son los dos tipos fundamentales de SAIs?**

**Respuesta:** Los dos tipos fundamentales son:

1. **SAI (UPS) Standby (o Off-line / Stand-by)**: el equipo funciona con la red eléctrica normal y sólo cuando detecta ausencia de red conmuta (en milisegundos) a la batería. Es el más sencillo y económico.
2. **SAI On-line (doble conversión)**: la corriente de red se rectifica y luego se vuelve a convertir (AC→DC→AC) de forma continua, de modo que la carga siempre está alimentada por el inversor y la batería puede hacerse cargo sin conmutación. Proporciona salida estabilizada y aislada de fluctuaciones.

Nota: Existe una tercera categoría intermedia llamada **line-interactive**, que regula tensiones con un autotransformador y ofrece mejor comportamiento que un standby sin llegar a la doble conversión.

**2. Cálculo de potencia del SAI (ejercicio numérico)**

**Datos:** Voltaje = 220 V, Intensidad = 3,42 A. La potencia aparente requerida = potencia real / 0,75. Se recomienda elegir un SAI con al menos +30% de la potencia aparente requerida.

**Cálculos (paso a paso, dígito a dígito):**

1. Potencia real (P) = V × I
   * 220 × 3,42 = 220 × (3 + 0,4 + 0,02)
   * 220 × 3 = 660
   * 220 × 0,4 = 88
   * 220 × 0,02 = 4,4
   * Suma = 660 + 88 + 4,4 = **752,4 W** (potencia real consumida)
2. Potencia aparente requerida (VA\_req) = P / 0,75
   * 752,4 ÷ 0,75 → multiplicamos por 4/3 para evitar decimales: (752,4 × 4) ÷ 3
   * 752,4 × 4 = 3009,6
   * 3009,6 ÷ 3 = **1003,2 VA**
3. Añadir margen recomendado (+30%):
   * VA\_recomendado = 1003,2 × 1,30
   * 1003,2 × 0,30 = 301,0 (exacto: 300,96)
   * 1003,2 + 300,96 = **1304,16 VA**

**Resultado práctico:** escoger un SAI con **al menos 1.305 VA**. Por disponibilidad comercial, lo recomendable sería seleccionar un SAI comercial estándar de **1.500 VA** (o superior) para garantizar margen y posibles ampliaciones.

**3. RAID 1 — teoría y guía práctica (Windows Server en VMware)**

**¿En qué consiste RAID 1?**

* **RAID 1 = espejo (mirroring).** Se escribe la misma información simultáneamente en dos (o más) discos. Si uno falla, el otro contiene copia íntegra de los datos.
* **Capacidad útil**: equivalente a la del disco más pequeño (p. ej. con dos discos de 1 GB la capacidad usable es 1 GB).
* **Tolerancia a fallos**: puede tolerar la caída de uno de los discos (si sólo hay 2 discos, un disco puede fallar y la VM/sistema sigue funcionando).
* **Rendimiento:** lecturas pueden mejorar (p. ej. lectura paralela), escrituras no suelen mejorar (la misma escritura debe replicarse).

**Escenario propuesto (VMware Workstation / Player):**

* Máquina virtual: **Windows Server** (versión de aula)
* Discos virtuales: **2×1 GB** añadidos a la VM (discos nuevos, sin particionar)

**Guía paso a paso (con capturas sugeridas)**

Antes de comenzar: hacer snapshot de la VM para poder revertir en caso de error.

1. **Crear/añadir discos en VMware**
   * Apagar la VM si está encendida.
   * Abrir *VM > Settings > Add > Hard Disk > Create a new virtual disk*.
   * Tamaño: **1 GB**. Tipo: recomendado usar SCSI o SATA (coherente con la VM).
   * Repetir para el segundo disco.
   * **CAPTURA 1:** pantalla de configuración de la VM mostrando los 2 discos añadidos (guardar como captura\_vm\_disks.png).
2. **Arrancar la VM**.
   * Iniciar sesión como administrador.
   * Abrir *Administrador de discos* (diskmgmt.msc).
   * Inicializar los discos nuevos si hace falta.
   * **CAPTURA 2:** Disk Management con los dos discos sin asignar.
3. **Crear volumen reflejado (mirrored)**
   * En el disco con espacio sin asignar, click derecho → **Nuevo volumen reflejado (New Mirrored Volume)**.
   * Seguir el asistente: seleccionar los dos discos como miembros, asignar letra y formatear con NTFS.
   * **CAPTURA 3:** Asistente de volumen reflejado (selección de discos).
   * **CAPTURA 4:** Volumen reflejado creado y en estado *Healthy*.
4. **Probar escritura/lectura**
   * Crear carpeta C:\prueba\_raid1 y archivo archivo\_prueba.txt con texto identificador (fecha y hora).
   * Copiar varios archivos (p. ej. archivos de 50–100 MB si se desea) para comprobar comportamiento.
   * **CAPTURA 5:** Explorador con los archivos creados.
5. **Simular avería de un disco**
   * Apagar la VM (se recomienda apagar para evitar corrupción al desconectar disco virtual desde host).
   * En VMware: *Settings* → seleccionar uno de los discos y **Remove** (¡no marcar borrar archivo del disco! — sólo quitar del inventario) o marcar **Disconnect** según versión.
   * Arrancar la VM.
   * En *Disk Management* se verá el volumen con *Failed redundancy* o el disco marcado como *Missing*.
   * **CAPTURA 6:** Estado tras desconectar un disco (mensaje de fallo redundancia o disco faltante).
6. **Comprobar accesibilidad de datos**
   * Abrir C:\prueba\_raid1 y verificar el contenido del archivo\_prueba.txt.
   * Si los datos son accesibles, RAID 1 ha cumplido su función: los datos estaban duplicados en el disco sano.
   * **CAPTURA 7:** Archivo abierto y contenido.
7. **Reparar el espejo**
   * Volver a añadir el disco virtual en VMware (Add > Existing Hard Disk, seleccionar el fichero VMDK o volver a conectar).
   * En el sistema Windows: si el disco aparece, click derecho sobre el volumen → **Add Mirror** (o en discos dinámicos: botón derecho sobre el disco y seguir asistente para añadir el espejo).
   * También se puede eliminar el espejo y volver a crear si se prefiere (en laboratorio cuidado con datos reales).
   * **CAPTURA 8:** Progreso de resynchronization (resincronización) en Disk Management.

**4. RAID 5 — teoría y guía práctica (Windows Server en VMware)**

**¿En qué consiste RAID 5?**

* **RAID 5 = striping con paridad distribuida.** Los datos se distribuyen en bloques entre todos los discos y se guarda información de paridad distribuida que permite reconstruir los datos si falla un disco.
* **Requisitos mínimos:** 3 discos (más comúnmente 3 o más).
* **Capacidad útil:** (n − 1) × tamaño del disco (p. ej. 3 discos de 1 GB → capacidad usable = 2 GB).
* **Tolerancia a fallos:** tolera la pérdida de un único disco sin pérdida de datos.
* **Rendimiento:** buenas lecturas; escrituras algo penalizadas por cálculo de paridad.

**Escenario propuesto: 3 discos para el RAID5 + 1 disco adicional reservado para la reparación**

**Guía paso a paso (con capturas sugeridas)**

1. **Crear/añadir discos en VMware**
   * Apagar la VM.
   * Añadir **3 × 1 GB** a la VM (y un cuarto disco de 1 GB que quedará como repuesto si se desea probar la reconstrucción).
   * **CAPTURA R5-1:** VMware con los 3 (o 4) discos añadidos.
2. **Arrancar la VM y preparar discos**
   * Iniciar *Disk Management* y inicializar los discos si es necesario. Convertir a **Dynamic Disks** si el asistente lo pide (Windows usa discos dinámicos para volúmenes RAID por software).
   * **CAPTURA R5-2:** Discos dinámicos listos.
3. **Crear volumen RAID-5**
   * Right-click en espacio sin asignar → **Nuevo volumen RAID-5 (New RAID-5 Volume)**.
   * Seleccionar los **3 discos** (no incluir el repuesto) y seguir el asistente: asignar letra, sistema de archivos NTFS, realizar format rápido si se desea.
   * **CAPTURA R5-3:** Asistente de creación RAID-5.
4. **Probar escritura/lectura**
   * Crear carpeta D:\prueba\_raid5 y copiar archivos de test.
   * **CAPTURA R5-4:** Explorador con archivos de prueba.
5. **Simular fallo de un disco**
   * Apagar la VM.
   * En VMware: seleccionar uno de los discos que forman el RAID-5 y **Remove** (dejando el fichero .vmdk en disco) o marcar como desconectado.
   * Arrancar la VM: Disk Management mostrará el volumen RAID-5 con estado *Degraded* o con un disco *Missing/Failed*.
   * **CAPTURA R5-5:** Estado degradado del volumen RAID-5.
6. **Comprobar que los datos siguen accesibles**
   * Abrir D:\prueba\_raid5 y comprobar integridad de ficheros.
   * **CAPTURA R5-6:** Archivo abierto y contenido.
7. **Reparar (reconstruir) el RAID-5 usando un disco de repuesto**
   * Añadir el cuarto disco virtual (1 GB) en la configuración de la VM (si no lo habíamos añadido antes, ahora añadirlo).
   * En Windows, si la partición está sin asignar, usar **Disk Management** o **DiskPart**. El método recomendado y fiable es usar **DiskPart** (modo administrador):

C:\> diskpart

DISKPART> list volume (identificar el volumen RAID5)

DISKPART> select volume X (seleccionar el volumen que está degradado)

DISKPART> list disk (identificar el número del disco de repuesto)

DISKPART> repair disk=Y (reemplaza la región fallada con el disco Y y comienza la reconstrucción)

* Nota: el comando repair disk=<n> es el mecanismo de diskpart para instruir a Windows a usar un disco dinámico como reemplazo y reconstruir la paridad en el volumen RAID-5. La operación puede tardar (depende del tamaño del volumen y del rendimiento).
* **CAPTURA R5-7:** Progreso de la reconstrucción en Disk Management o en el output de diskpart.

1. **Verificar**
   * Al terminar, Disk Management marcará el volumen como *Healthy* y la capacidad estará disponible.
   * **CAPTURA R5-8:** Volumen RAID-5 reconstruido y en estado *Healthy*.

**Consejos de laboratorio:** trabajar con snapshots del hipervisor facilita volver atrás si algo sale mal. Nunca probar reconstrucciones con datos irremplazables sin backups.

**5. ¿Qué es un NAS?**

**NAS (Network Attached Storage)** es un dispositivo de almacenamiento conectado a la red que ofrece acceso a archivos (nivel fichero) a través de protocolos de red como SMB/CIFS (Windows), NFS (Unix/Linux) o AFP (Apple en entornos antiguos). Características principales:

* Proporciona carpetas compartidas accesibles desde cualquier equipo autorizado en la red.
* Suele incluir sistemas RAID por hardware o software para tolerancia a fallos.
* Ofrece servicios adicionales: usuarios/grupos, snapshots, replicación, servidor de copias (rsync), servidor multimedia, iSCSI, etc.

**Usos en el laboratorio:** centralizar copias de seguridad, almacenar imágenes VM, proporcionar almacenamiento compartido para servidores de pruebas.

**6. CrystalDiskInfo — instalación y uso, qué interpretamos**

**Instalación y ejecución (pasos rápidos):**

1. Descargar CrystalDiskInfo desde su web oficial.
2. Ejecutar como administrador.
3. Seleccionar el disco a inspeccionar.

**Datos que proporciona y qué vigilar:**

* **Estado de salud (Good / Caution / Bad)** — resumen rápido.
* **Temperatura** (°C) — temperaturas elevadas aumentan tasa de fallos.
* **SMART attributes importantes:**
  + *Reallocated Sector Count* (sectores realocados) — aumento indica sectores defectuosos reasignados.
  + *Current Pending Sector Count* — sectores pendientes de lectura/escritura; peligro inmediato.
  + *Uncorrectable Sector Count* — sectores no recuperables.
  + *Power-On Hours (POH)* — horas de uso del disco.
  + *Spin Retry Count*, *Reported Uncorrectable Errors*, *Load Cycle Count* (en discos externos o de portátil).

**Interpretación:** valores distintos de 0 en *Reallocated Sector Count* o *Current Pending Sector Count* deben investigarse: planificar copia y sustitución de la unidad. Temperaturas por encima de 50–55 °C son preocupantes en HDD.

**CAPTURA CDInfo:** pantalla principal mostrando SMART y lista de atributos (guardar como captura\_crystaldiskinfo.png).

**7. Mapa lógico del escenario de pruebas**

Internet

|

Router

|

-----------------

| |

Host-PC NAS (opcional)

(VMware Workstation)

|

Windows Server VM

- Disco 0: OS

- Disco 1: RAID member 1 (1GB)

- Disco 2: RAID member 2 (1GB)

- Disco 3: RAID member 3 (1GB) -> usado para RAID5

- Disco 4: Spare disk (1GB) -> repuesto para reconstrucción

Servicios en la VM:

- Disk Management (RAID por software)

- Carpetas de prueba \prueba\_raid1 y \prueba\_raid5

- CrystalDiskInfo instalado para monitorizar SMART

**Explicación:** el host ejecuta la VM que simula los discos mediante VMDK. El NAS es opcional para almacenar backups o para probar montajes SMB.

**8. Registro de pruebas (plantilla con evidencias)**

| **Paso** | **Acción** | **Resultado esperado** | **Resultado real** | **Evidencia (captura)** |
| --- | --- | --- | --- | --- |
| 1 | Añadir 2 discos 1GB a la VM | Aparición de dos discos sin asignar en Disk Management | OK | captura\_vm\_disks.png |
| 2 | Crear volumen reflejado (RAID1) | Volumen healthy y usable (1 GB) | OK | captura\_raid1\_healthy.png |
| 3 | Copiar archivo de prueba | Archivo copiado correctamente | OK | captura\_raid1\_files.png |
| 4 | Desconectar uno de los discos (simular fallo) | Volumen funciona en modo degradado, datos accesibles | OK | captura\_raid1\_failed.png |
| 5 | Reconectar disco y resynchronizar | Volumen vuelve a estado Healthy | OK | captura\_raid1\_sync.png |
| 6 | Crear RAID5 con 3 discos | Volumen RAID5 healthy, capacidad 2GB | OK | captura\_raid5\_healthy.png |
| 7 | Simular fallo disco RAID5 | Volumen degradado, datos accesibles | OK | captura\_raid5\_degraded.png |
| 8 | Añadir spare y reparar | Reconstrucción y estado Healthy final | OK | captura\_raid5\_rebuild.png |
| 9 | CrystalDiskInfo | SMART healthy (o mostrar atributos de advertencia) | OK/Advertencia | captura\_crystaldiskinfo.png |