

Unidad 2: Seguridad Pasiva

Resultados de Aprendizaje a trabajar en esta Unidad:
RA1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
Contenidos a trabajar en esta Unidad:
- Principios de seguridad pasiva - Copias de seguridad - Modelos de almacén de datos - Recomendación sobre el tipo de copia a efectuar - Recuperación de datos - Seguridad física y ambiental. - Centros de proceso de datos (CPD) - Ubicación y acondicionamiento físico - Control de acceso físico - Sistemas biométricos - Circuito cerrado de televisión (CCTV) - Sistemas de alimentación ininterrumpida (SAI). Tipos y potencia necesaria

Contenidos de la Unidad

1. PRINCIPIOS DE LA SEGURIDAD PASIVA 2
2. COPIAS DE SEGURIDAD 2
3. RECUPERACIÓN DE DATOS 8
4. SEGURIDAD FÍSICA Y AMBIENTAL 8
5. SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA 11
6. BIBLIOGRAFÍA 13

1. PRINCIPIOS DE LA SEGURIDAD PASIVA

La seguridad pasiva intenta minimizar el impacto y los efectos causados tras un incidente o ataque de ciberseguridad. Son medidas o acciones posteriores a un ataque o incidente.

En la siguiente tabla se muestran posibles amenazas, y algunas medidas que se pueden implantar para minimizar los daños producidos:

Amenazas	Medidas de seguridad
Suministro eléctrico (cortes de corriente, variaciones de tensión, aumento de ruido...)	- Sistema de alimentación ininterrumpida - Generadores eléctricos autónomos - Fuentes de alimentación redundantes
Robos o sabotajes (acceso físico no autorizado al hardware, software, o datos)	- Control de acceso físico (armarios, llaves, medidas biométricas...) - Vigilancia mediante personal
Condiciones atmosféricas y naturales adversas (temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos...)	- Correcta ubicación de sistemas - Centro de respaldo en ubicación diferente al centro de producción - Regulación y control de temperatura y humedad

Como consecuencias por las distintas amenazas podemos tener:

- Pérdida y/o mal funcionamiento del hardware
- Falta de disponibilidad de servicios
- Pérdida de información
- Y de forma indirecta, pérdida de confianza de los usuarios

La pérdida de información es el aspecto fundamental en torno al que gira la seguridad informática por lo que, como medida genérica siempre recomendada, se abordará la planificación y realización de copias de seguridad que permitan recuperar la información.

2. COPIAS DE SEGURIDAD

Debido a diferentes causas, la información almacenada en los sistemas informáticos puede desaparecer o resultar dañada.

Las **copias de seguridad o backup** son réplicas de datos que permiten recuperar la información original. Una de seguridad es un archivo digital, o conjunto de archivos, que se consideran lo suficientemente importantes como para ser conservados. Corresponde a cada usuario, o administrador de sistema, determinar los datos que por su importancia serán almacenados en la copia de seguridad.

Las copias de seguridad se pueden almacenar en soportes extraíbles (CD/DVD, pen drive, discos duros externos, etc.), en otros directorios o particiones de la propia máquina, en unidades compartidas en otros equipos, discos en red, servidores remotos, etc. En cualquier caso, es aconsejable que las copias de seguridad se encuentren cifradas y comprimidas en un único archivo para facilitar su confidencialidad, mantenimiento y distribución.

Teniendo en cuenta los modelos de almacenamiento masivo de los sistemas, según la forma en que los sistemas acceden al almacenamiento, podemos distinguir tres modelos principales:

- **DAS (Direct Attached Storage):** método tradicional de almacenamiento, y el más sencillo. El dispositivo de almacenamiento se encuentra directamente conectado al sistema que lo utiliza. Por ejemplo: disco duro secundario, disco duro extraíble, segunda partición de datos…
- **NAS (Network Attached Storage):** almacenamiento conectado en red. Permite que diferentes equipos accedan a los datos a través de protocolos de red. Las carpetas compartidas en red y servidores específicos NAS son una buena solución para redes de área local de tamaño pequeño o mediano.
- **SAN (Storage Area Network):** red de área de almacenamiento. Los dispositivos de almacenamiento se encuentran conectados a una red de alta velocidad y resuelven las peticiones que se les realizan. Se usa en grandes organizaciones.

2.1. Modelos de almacén de datos

Los datos de las copias de seguridad deben ser almacenados y etiquetados según un criterio, ya sea un simple apunte en una libreta con las fechas y la identificación de las copias, o un complejo programa de clasificación.

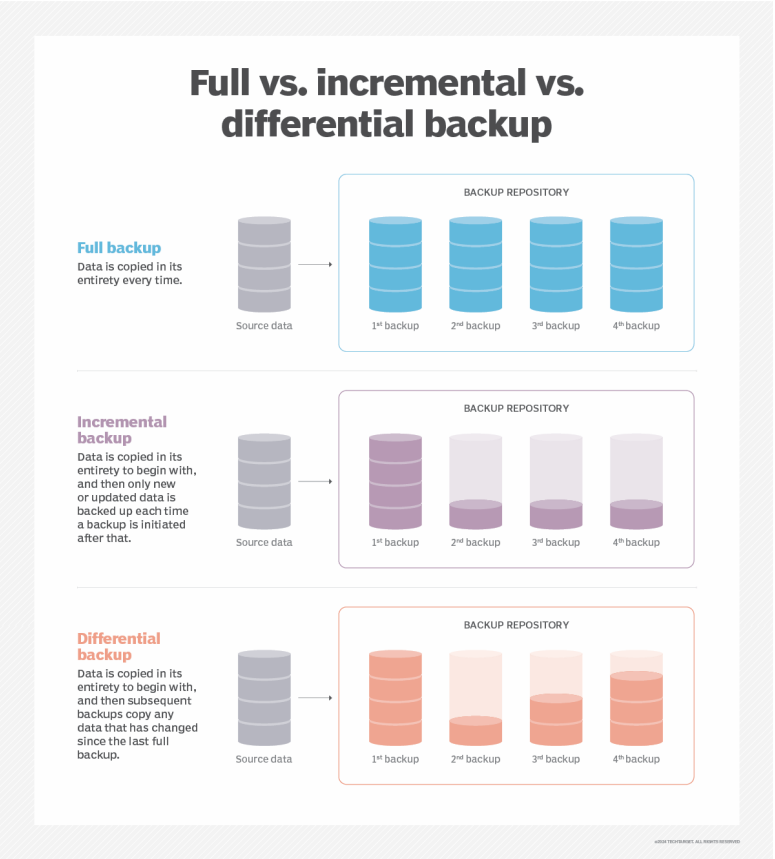
Un almacén es desestructurado cuando es una mera colección de dispositivos (CDs, USBs, discos duros externos…) con una mínima información sobre qué contienen y cuándo ha sido copiado.

En función de qué información contienen, podemos diferenciar **tres tipos de copias de seguridad:**

- **Completa, total o íntegra:** es una copia de seguridad total de los archivos y carpetas seleccionados.
- **Incremental**: es una copia de los archivos que han cambiado desde la última copia de seguridad realizada, ya sea completa o incremental.
- **Diferencial**: es una copia de los archivos que han cambiado desde la última copia de seguridad completa.

Ahora nos podemos preguntar, ¿cuál es el mejor tipo de copia de seguridad? Dependerá de la cantidad a información a almacenar:

- Si el volumen de datos no es muy elevado (menor de 5GB, por ejemplo) podemos realizar siempre copias totales.
- Si el volumen de la copia total es muy elevado (mayor a 50GB) pero el volumen de datos que se modifican es pequeño, se recomienda hacer una copia total y después, diferentes copias diferenciales.
- Si el volumen total y las modificaciones en los datos son elevados, se recomienda realizar una copia total y posteriores copias incrementales. Conviene hacer copias totales más a menudo para no tener demasiadas copias incrementales y que sea más fácil la recuperación de los datos.



Además, conviene tener en cuenta la información de la siguiente tabla:

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Cuándo usar
Completo	Máximo	Muy lento	Muy simple	Pocos datos
Completo + incremental	Mínimo	Rápido	Compleja	Muchos datos y variables
Completo + diferencial	Intermedio	Lento	Sencilla	Datos poco variables

En grandes compañías, donde las copias de seguridad suelen estar planificadas y automatizadas, se suelen usar sistemas mixtos. Por ejemplo: todos los días 1 de mes a las 23:00 una copia de seguridad total. Todos los viernes a las 23:00, una copia diferencial respecto a la copia del día 1. Todos los días (salvo viernes y día 1), copia de seguridad incremental desde el día anterior.

2.2. Nomenclatura de los archivos de copia de seguridad

El nombre del archivo de la copia de seguridad es el principal método de identificación de la copia. Se suele componer de:

- Un texto descriptivo de su contenido.
- Fecha de realización.
- Identificación del tipo de copia realizada (total, diferencial o incremental).
- En ocasiones se indica también las carpetas que contiene, u otro tipo de información que se considere relevante.

Por ejemplo:

"BD_ventas_total_01ENE2026.tar.gz"

"BD_compras_dif_01ENE_08ENE2026.tar.gz"

2.3. Herramientas para copias de seguridad

- **tar (unix/linux)**

Se usa en sistemas unix/Linux para realizar el archivado de ficheros (agrupación de ficheros bajo un único archivo). Es la orden estándar de archivado en sistemas unix/Linux. Su nombre proviene de tape archive (archivo en cinta).

Permite agrupar un conjunto de ficheros en un único archivo o el proceso contrario, extraer los ficheros del archivo. Se suele ejecutar en momentos prefijados marcados según el servicio cron (administrador de tareas de linux). Además, de forma opcional, permite su compresión.

La extensión de los archivos suele ser:

- .tar si son un conjunto de ficheros archivados sin compresión.
- .tar.gz si es un conjunto de archivos comprimidos

Para empaquetar ficheros:

```
tar cvf nombreArchivo.tar ficherosAArchivar
```

Donde:

- v indica que se muestre el proceso en pantalla
- c indica que se crea el archivo
- f indica que se asignará un nombre al archivo tar

Para extraer los contenidos:

```
tar xvf nombreArchivo.tar destinoArchivos
```

Donde:

- x indica que queremos hacer la extracción de los ficheros

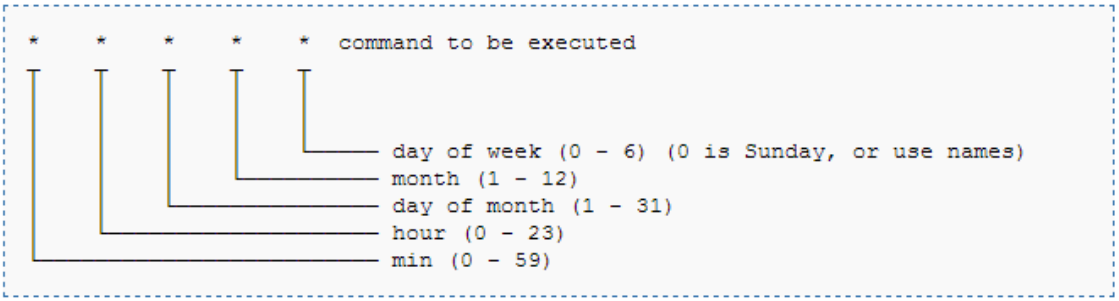
En el caso de archivos comprimidos, para ambos casos, se añade la opción z.

- **cron (linux)**

El servicio o demonio (daemon) cron es el sistema de planificación de tareas en sistemas Linux. Este proceso revisa los archivos crontab de los usuarios para comprobar las tareas que debe realizar en los momentos indicados en ese fichero de configuración.

Para editar el archivo crontab de usuario se utiliza el comando crontab -e.

El formato del archivo contrab es muy sencillo:



La primera columna indica el minuto, la segunda la hora, la tercera el día del mes, la cuarta el mes, la quinta el día de la semana, y finalmente el comando a ejecutar.

Ejemplos:

```
0 8 * * 0          /root/bin/backup_total
```

Realiza una copia de seguridad total todos los domingos a las 8:00.

```
0 8 * * 1,2,3,4,5       /root/bin/backup_incremental
```

Realiza una copia incremental de lunes a viernes a las 8:00.

```
0,15,30,45 * * * *       /usr/bin/who >> usuarios.txt
```

Cada 15 minutos añade al fichero los usuarios que se encuentran conectados al sistema.

- **Backup (Windows)**

En Windows existen diferentes herramientas que permiten realizar copias de seguridad y restaurar el sistema. Para facilitar estas tareas, pueden aplicarse algunas buenas prácticas como son:

- Separar, cuando sea posible, el sistema y los datos. Se puede utilizar una partición para el sistema operativo y otra para los datos de usuario: C: → Windows y programas y D: → Datos de usuario. Esta organización puede facilitar la reinstalación o restauración del sistema sin tener que modificar los datos almacenados en la partición de datos.
- Proteger los datos de usuario mediante copias de seguridad. Los documentos, fotografías, proyectos y demás información importante deben incluirse en las copias de seguridad, independientemente de que se encuentren en carpetas como Documentos, Escritorio, Imágenes, etc. Puede ser conveniente mantener los datos organizados en una ubicación específica, por ejemplo: D:\Datos y establecer una política de copias de seguridad sobre dicha ubicación.
- Crear un punto de restauración tras configurar el sistema. Una vez instalado Windows, los controladores, las actualizaciones y el software básico, puede ser conveniente crear un punto de restauración. De esta forma, si posteriormente una instalación o modificación provoca problemas en el sistema, se puede intentar volver a un estado anterior.

Windows 10 incluye un sistema de copia de seguridad integrada en el sistema denominada “historial de archivos”, aunque por defecto está desactivado.

- **Cobian backup (Windows)**

Es un software gratuito, multitarea, capaz de crear copias de seguridad en diferentes soportes locales y remotos.

Sus principales características son:

- Consume pocos recursos.
- Se ejecuta en segundo plano.
- Permite planificar las tareas de copia que pueden ser completas, diferenciales o incrementales.
- Soporta diferentes tipos de comprensión y permite cifrar la información.

- **Rsync y Grsync (Linux)**

Rsync es una herramienta para crear copias de seguridad en sistemas Linux. Admite copias de seguridad de carpetas locales, túneles SSH, sincronización, etc.

Grsync agrega una interfaz gráfica de usuario, eliminando la complejidad de la utilización de un conjunto de argumentos de línea de comandos.

3. RECUPERACIÓN DE DATOS

- **Recuva (Windows)**

Es una herramienta de recuperación de datos para sistemas Windows que permite recuperar archivos borrados, incluso desde dispositivos formateados o dañados.

No siempre se pueden recuperar los archivos al 100% ya que su espacio en disco puede haber sido ocupado por otros archivos, o bien el nombre del archivo recuperado por estas utilidades no coincide con el archivo original.

- **Testdisk (Linux)**

Software libre que permite recuperar particiones perdidas y sectores de arranque. Incluye PhotoRec, una herramienta sencilla para recuperación de archivos.

- **Foremost (Linux)**

Recupera archivos basándose en el tipo de archivo. Se puede instalar mediante línea de comandos:

```
sudo apt install foremost
```

- **Scalpel (Linux)**

Con iguales características que foremost. También se puede instalar mediante línea de comandos:

```
sudo apt install scalpel
```

4. SEGURIDAD FÍSICA Y AMBIENTAL

Aunque en una organización o empresa haya elevados estándares de seguridad lógica ante accesos indebidos a la información, aún serán vulnerables a catástrofes como incendios, inundaciones, terremotos, cortes eléctricos, etc.

La **seguridad física** consiste en la aplicación de barreras físicas, medidas de prevención y procedimientos de control ante amenazas a los recursos informáticos e información confidencial. Este tipo de seguridad se tiende a minusvalorar respecto a otro tipo de amenazas.

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor de la ubicación física de los sistemas informáticos, así como los medios de acceso a esos sistemas, implantados para proteger el hardware y soportes de almacenamiento de datos.

En este apartado veremos las medidas aplicables tanto a equipos de hogar, pequeñas oficinas, servidores, centros de proceso de datos (CPD), etc.

4.1. Centros de proceso de datos (CPD)

Se denomina **CPD** (también conocido como Data Center) a una ubicación en la que se concentran los recursos de procesamiento de la información de la organización.

Un CPD es un edificio o sala de gran tamaño usado para mantener en él una gran cantidad de equipamiento informático y/o electrónico. Dado lo costoso de su mantenimiento, sólo grandes organizaciones disponen de un CPD propio.

En ocasiones, por razones de seguridad, las grandes organizaciones deciden duplicar el CPD con otro CPD de respaldo. Un centro de respaldo está específicamente diseñado para asumir las funciones del CPD principal en caso de fallo. Debe ubicarse en una localización diferente al CPD principal para que no les afecten los mismos incidentes al mismo tiempo. El equipamiento del CPD de respaldo no tiene por qué ser idéntico al CPD principal, pero el software y los datos sí, siendo especialmente importante que disponga de una réplica exacta de los datos.

La motivación principal de las empresas para construir un CPD es garantizar la alta continuidad o disponibilidad del servicio.

Las **características generales** de un CPD son:

- **Disponibilidad y monitorización 24/7/365:** debe estar disponible el 100% del tiempo.
- **Fiabilidad**: debe tratar de tener el servicio disponible el 99’99% del tiempo.
- **Seguridad, redundancia y diversificación:** almacenaje de datos exterior, duplicidad de alimentación eléctrica, comunicaciones con balanceo de carga, controles de acceso, etc.
- **Control ambiental y prevención**: control de temperatura y humedad, prevención ante inundaciones, incendios, etc.

En un CPD los servidores se concentran en una ubicación llamada sala fría, nevera o pecera. Esta sala requiere un sistema de refrigeración para mantener la temperatura en los márgenes establecidos para evitar averías por calor.

La pecera suele contar con medidas estrictas de acceso y de extinción de incendios.

Además de un CPD y un CPD de respaldo, debe existir un plan de contingencias con el protocolo de actuación en caso de incidente.

4.2. Control de acceso físico

Los dispositivos informáticos son elementos valiosos que están expuestos a posibles actos delictivos como robos, sabotajes, etc.

El uso de credenciales es básico en el control de acceso físico a diferentes ubicaciones de la empresa. A las personas las podemos identificar por:

- Algo que posee: llaves, tarjetas de identificación…
- Algo que se sabe: PIN, contraseña…
- Algo que se es: huellas dactilares, firma escrita, voz…

Cada uno de estos identificadores se almacenan en una base de datos de apoyo al servicio de vigilancia.

Algunas posibles vulnerabilidades respecto a la seguridad física pueden ser:

- El personal de seguridad: sobornos, venganza…
- Las tarjetas pueden ser robadas o extraviadas.
- Los pines y contraseñas pueden ser revelados o descubiertos.

4.2.1. Sistemas biométricos

La **biometría** es la parte de la biología que estudia la variabilidad individual de los seres vivos utilizando métodos estadísticos.

La forma de identificación consiste en la comparación de características físicas de la persona con un patrón conocido y almacenado en una base de datos. De esta forma se verifica la identidad de la persona con el objetivo de tener un mejor control de acceso físico.

Algunas formas de identificación biométricas comunes son:

- **Huella digital**: se basa en el principio de que no existen dos personas con huellas dactilares iguales. Cada huella posee unas características particulares llamadas minucias cuya posición y forma es diferente de unos individuos a otros. Cada persona tiene más de 30 minucias, y no hay dos personas que tengan más de 8 minucias iguales.
- **Verificación de voz**: se compara la dicción de una frase con una grabación. Es un sistema muy sensible a factores externos, y no muy fiable.
- **Verificación de patrones oculares**: se basa en los patrones del iris o de la retina. La probabilidad de que dos personas tengan los mimos patrones es práctica nula. Sin embargo, es un método considerado intrusivo porque puede revelar enfermedades, que son datos privados de las personas.
- Otras: geometría de la mano, reconocimiento facial…

4.2.2. Circuito cerrado de televisión

Se puede utilizar protección electrónica para la detección de robo, intrusión, asalto e incendios mediante el uso de sensores conectados a sistemas de alarmas. En las centrales tienen conectados los elementos de señalización encargados de notificar situaciones de emergencia.

Uno de los métodos más empleados son los circuitos con **cámaras de grabación de video o circuitos cerrados de televisión (CCTV).**

Los CCTV permiten el control de lo que sucede en el área de cobertura captado por un conjunto de cámaras situadas estratégicamente. Las cámaras pueden estar a la vista, a forma de medida disuasiva, u ocultas.

En la actualidad, se utilizan las llamadas cámaras IP, que son dispositivos autónomos que cuentan con un servidor web de vídeo que les permite transmitir por la red, y almacenar las imágenes que están siendo grabadas.

5. SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Un **sistema de alimentación ininterrumpida (SAI),** también conocido por sus siglas en inglés como UPS, es un dispositivo que suministra energía desde sus baterías a los dispositivos informáticos cuando se produce un corte en el suministro eléctrico.

Un SAI ofrece alimentación eléctrica durante un tiempo limitado, lo que permite a los sistemas la posibilidad de apagarse de forma ordenada sin perder datos. Otra posibilidad es que los sistemas estén mantenidos por el SAI mientras se sustituye la fuente de alimentación original por otra de respaldo.

Los diferentes dispositivos de la organización no se conectan a las tomas de corriente directamente, sino que lo hacen al SAI, que es el dispositivo que está conectado a los enchufes. Es el intermediario entre la red eléctrica y los dispositivos informáticos.

Otra función de los SAI es el trabajo de estabilización del flujo eléctrico que llega a los dispositivos informáticos. El SAI filtra cambios de la corriente eléctrica.

Según las necesidades energéticas de los dispositivos conectados, existen diferentes tipos de SAI:

- **SAI offline**: son los más económicos, recomendados para equipos domésticos. No estabilizan la corriente. Sólo generan tensión de salida cuando se produce un corte.
- **SAI inline**: estabilizan la corriente incorporando un estabilizador de salida. Sólo generan tensión de salida cuando se produce un corte en el suministro. Adecuados para pequeños servidores.
- **SAI online o de doble conversión**: equipos de gama alta para proteger servicios críticos. Siempre generan tensión de salida, independientemente de la entrada.

5.1. Capacidad de un SAI

Para ajustar las dimensiones y capacidad de la batería de un SAI es necesario realizar un cálculo de la potencia que consumen los equipos que deseamos proteger.

La **potencia eléctrica** se define como la cantidad de energía eléctrica que se transporta o que se consume en un determinado tiempo.

En corriente continua:

$$Potencia = Voltaje\ x\ Intensidad$$

En este caso, mediremos la potencia en vatios (W).

En circuitos de corriente alterna, se usan medidas de **potencia aparente o eficaz (S)** y **potencia real (P)**. Ambas se relacionan mediante el **Factor de potencia (FA).**

La unidad de medida usada por los SAI es el voltiamperio (VA), que mide la potencia aparente consumida por el sistema.

Para entender un poco mejor estos conceptos, vamos a ver un ejemplo real.

Al mirar las características de un SAI encontraremos el valor de la tensión eléctrica (por ejemplo, 220 voltios) y de la intensidad (por ejemplo, 5 amperios).

Con estos datos, podemos calcular la potencia que genera el SAI:

$$P = 220\ x\ 5 = 1100\ Watios.$$

Sin embargo, esta no es la potencia real que podremos utilizar para alimentar a nuestros equipos en caso de apagón, sino que será menor puesto que hay ciertas "pérdidas" de potencia.

Para saber de cuánta potencia dispondremos realmente, deberemos tener en cuenta el factor de potencia (FA). Si nuestro FA es de 0,8, entonces nuestra potencia disponible será:

$$1100\ x\ 0{,}8 = 880\ Watios$$

Por tanto, manejamos los siguientes conceptos:

- **Potencia aparente (S)** que es la que se genera. Se da su medida en voltiamperios (VA) para diferenciarla de P.
- **Potencia real (P)** es la que realmente tenemos disponible y se da su medida en Watios (W).
- **Factor de potencia (FA)** es la relación entre ambas potencias.
- A la energía no utilizable, se le denomina **potencia reactiva (Q).**

Ejemplos:

1) Si en nuestro SAI vemos 900 VA 480 W, entonces:

$$S = 900\ VA;\ P = 480\ W;\ FA = 480/900 = 0{,}533$$

2) Si en nuestro SAI vemos 220 V 5 A 0,6 FA, entonces:

$$S = 220 * 5 = 1100\,VA;\ P = 1100 * 0{,}6 = 660\,W$$

3) Si en una oficina se dispone de un SAI con una capacidad de 1.500 VA, ¿Cuántos equipos podría alimentar en caso de corte del suministro eléctrico, si cada equipo consume 250 W en la torre y 90 W en el monitor? Suponemos un factor de potencia del SAI es FA = 0,6

Calculamos la potencia real del SAI:

$$P = 1500\,VA * 0{,}6 = 900\,W$$

Calculamos lo que consume cada equipo:

$$Pconsumo = 250\,W\ (torre) + 90\,W\ (monitor) = 340\,W$$

Con lo cual, dividiendo la potencia que ofrece el SAI entre el consumo de potencia de cada equipo, obtenemos cuantos equipos podrá alimentar el SAI en caso de corte de suministro eléctrico:

$$Nº\ equipos = 900\,W\ /\ 340\,W = 2{,}64\ equipos \rightarrow 2\ equipos$$

6. BIBLIOGRAFÍA

Seguridad Informática. Alfonso García-Cervigón, María del Pilar Alegre. Paraninfo.

Seguridad Informática. José Fabián Roa Buendía. McGraw Hill.

Seguridad y alta disponibilidad. Ignacio Triviño Mosquera. Síntesis.

Types of backup explained. TechTarget. Disponible en: https://www.techtarget.com/it-infrastructure/feature/Types-of-backup-explained-Incremental-vs-differential-vs-full-etc [Última consulta 1 octubre 2026].

Programa tareas en Linux como un experto: Cron y Crontab. RedesZone. Disponible en: https://www.redeszone.net/tutoriales/servidores/cron-crontab-linux-programar-tareas/ [Última consulta 1 octubre 2026].

Sitio web oficial de Cobian Backup. Disponible en: https://www.cobiansoft.com/

Sitio web oficial de rsync. Disponible en: https://rsync.samba.org/

Sitio web oficial de grsync. Disponible en: https://www.opbyte.it/grsync/

Sitio web oficial de Recuva. Disponible en: https://www.ccleaner.com/es-es/recuva