TEMA 2. SEGURIDADE PASIVA

La seguridad pasiva intenta minimizar el impacto y los efectos causados por accidentes, es decir, se consideran medidas o acciones posteriores a un ataque o incidente

1. Introducción

La seguridad pasiva intenta minimizar el impacto y los efectos causados por accidentes, es decir, se consideran medidas o acciones **posteriores a un ataque o incidente**. A continuación se presenta una tabla que relaciona los posibles problemas con soluciones propuestas:

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.

Las consecuencias o efectos producidos por las distintas amenazas previstas son:

- **Pérdida y/o mal funcionamiento** del hardware.
- **Falta de disponibilidad** de servicios.
- **Pérdida de información**.

Como hemos visto en el tema anterior la pérdida de información es el aspecto fundamental en torno a la que gira gran parte de la seguridad informática, por lo que, como medida transversal y siempre recomendada en primer lugar abordaremos la planificación y realización de copias de seguridad, que permitan recuperar los datos.

2. Copias de seguridad

Por acción de algún tipo de malware, acceso no autorizado a nuestro sistema, por fallos en el hardware o, simplemente, por accidente o descuido, la información contenida en nuestro equipo puede resultar dañada o incluso desaparecer. Las copias de seguridad o backup, son réplicas de datos que nos permiten recuperar la información original en caso de ser necesario, es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.

Uno de los principios de segundad: "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".

Corresponde a cada usuario determinar los datos, que por su importancia, serán almacenados en la copia de seguridad. Estas copias, se pueden almacenar en soportes extraíbles (CD/DVD, pendrive, cintas de backup, etc.), en otros directorios o particiones de datos de nuestra propia máquina, en unidades compartidas de otros equipos o en discos de red, en servidores remotos, etc. Es aconsejable que dichas copias de seguridad se encuentren cifradas y comprimidas en un solo archivo facilitando su confidencialidad, mantenimiento y distribución.

Teniendo en cuenta los **modelos de almacenamiento masivo** de los sistemas hoy en día encontramos:

- **Direct Attached Storage (DAS):** es el método tradicional de almacenamiento y el más sencillo. El dispositivo de almacenamiento se encuentra directamente conectado físicamente al sistema que hace uso de él. Es el caso convencional disponer un disco duro conectado directamente al sistema informático. Los discos duros extraíbles, y las particiones de datos, son una solución sencilla y económica para realizar copias de seguridad locales.

- **Network-Attached Storage (NAS):** almacenamiento conectado en red. Las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos de red, como **NFS**, **FTP**, **CIFS** o **SMB**. Las carpetas compartidas en red y servidores específicos NAS son una buena solución para una LAN de tamaño pequeño o medio.
- **Storage Área Network (SAN):** red de área de almacenamiento. Los dispositivos de almacenamiento se encuentran conectados a una red de alta velocidad directamente y resuelven las peticiones que se le realizan. La infraestructura necesaria hace que solo sea posible en grandes organizaciones.

A modo de ejemplo veremos cómo implementar un servidor **NAS** como servidor de archivos para distintos usuarios en una red corporativa en el tema 8.

Modelo de almacén de datos

Los datos de la copia deben ser almacenados de alguna manera y probablemente deban ser organizados con algún criterio. Para ello se puede usar desde una hoja de papel con una lista de las cintas de la copia de seguridad y las fechas en que fueron hechas, hasta un sofisticado programa con una base de datos.

Un almacén **desestructurado** o conjunto de disquetes, CD/DVD, memorias USB, discos duros externos o cintas de backup, con una mínima información sobre qué ha sido copiado y cuándo. Esta es la forma más fácil de implementar pero ofrece pocas garantías de recuperación de datos. Lo

habitual es trabajar con almacenes estructurados, en función de la cantidad de archivos que se salvaguardan a la hora de realizar la copia de seguridad, podemos distinguir tres tipos de copia:

- **Completa, total o íntegra**: es una copia de seguridad total de todos los archivos y directorios seleccionados.
- **Incremental:** se hace una copia de seguridad solo de los archivos que han cambiado desde la última copia de seguridad realizada, sea del tipo que sea. Tiene en cuenta los bits de archivo modificado.
- **Diferencial:** es similar a la incremental pero realiza una copia de todos los archivos que han cambiado desde la última copia de seguridad total que hayamos hecho.

Si hacemos una copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día, por tanto el volumen de información de cada backup incremental será menor que el de la total. Si tenemos que realizar la restauración de archivos **ante un desastre, debemos disponer de la copia total y de todas las copias increméntales que hayamos realizado desde la copia total**.

Si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad diferencial el resto de los días, cada copia diferencial guardará los archivos que se hayan modificado desde el día 1. La ventaja es que se requiere menos espacio que la copia total y que **en el proceso de restauración únicamente necesitaremos la última copia total y la última copia diferencial**. Una copia diferencial anula a la copia diferencial anterior. Por el contrario, se consume más tiempo en realizar la copia y también más espacio que en el caso de copia incremental.

Recomendación sobre el tipo de copia a efectuar

Si el volumen de datos de nuestra copia de seguridad **no es muy elevado** (menos de 4 GB), lo más práctico es realizar **siempre copias totales** ya que en caso de desastre, tan solo debemos recuperar la última copia.

Si el volumen de datos de nuestra copia de seguridad es **muy elevado** (mayor de 50 GB) pero el volumen de datos que se modifican no es elevado (sobre 4 GB), lo más práctico es realizar una primera copia total y, posteriormente, realizar **siempre copias diferenciales**. Así, en caso de desastre, tan solo debemos recuperar la copia total y la última diferencial. Periódicamente debemos realizar una copia total y así empezar de nuevo.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparán mucho espacio, por lo tanto en este caso lo más práctico será realizar una primera copia total y posteriormente realizar **siempre copias incrementales**, ya que son las que menos espacio ocupan. El problema es que en caso de desastre debemos recuperar la última copia total y todas las increméntales realizadas desde que se hizo la última copia total. En estos casos, conviene hacer copias totales más a menudo para no tener que mantener un número muy elevado de copias increméntales.

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

En grandes compañías donde la realización de copias de seguridad está perfectamente **planificada**, se suelen utilizar **sistemas mixtos**. Por ejemplo en un caso típico se realizarían las siguientes tareas:

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total.
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia de día 1.
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

Con esta planificación nos aseguramos disponer de copia de seguridad diaria. En caso de desastre deberíamos recuperar la copia total, la última diferencial y todas las increméntales desde la última diferencial.

Para garantizar la disponibilidad de los datos, en caso de desastre en la ubicación principal, es recomendable distribuir en distintas ubicaciones las copias de seguridad. Para ello se puede utilizar una empresa especializada que **transporte y custodie duplicados** de las copias, así como emplear **alojamiento remoto**, o **backup online** o en la nube.

Práctica 2.1 Copias de seguridad con herramientas del sistema. En esta práctica realizaremos simulacros de copias de seguridad, y de recuperación de las mismas, mediante herramientas de los propios sistemas operativos.

Práctica 2.2 Copias de seguridad con aplicaciones específicas. Esta práctica está enfocada a conocer y a practicar con las distintas herramientas específicas de copias de seguridad.

Recuperación de datos

¿Podemos recuperar archivos borrados definitivamente de nuestro sistema? En el caso de haber sido víctima de un ataque o haber sufrido un accidente como corte de suministro eléctrico o fallo de hardware, la recuperación de archivos en disco lo intenta. Cuanto menor tiempo y modificaciones de disco transcurran entre el borrado o accidente y nuestro intento de recuperación, mejor será nuestro resultado. Por ejemplo, cuando en un sistema de ficheros de un sistema operativo se borra un fichero de un medio de almacenamiento (disco duro, pendrive USB, cinta, etc.), marca aquellas posiciones que ocupaba dicho fichero en el dispositivo como libres, para poder almacenar nueva información, pero no las borra. Los datos permanecerán en esas posiciones

hasta que se sobrescriban con nueva información. Por lo que es posible recuperarlo mediante alguna herramienta software.

Práctica 2.3 Comparativa de software de recuperación de fichero. En esta ocasión conoceremos y compararemos tres importantes programas de recuperación de datos.

Práctica 2.4 Actualización segura de sistemas, virtualización discos fijos, borrado seguro. Con esta práctica aprenderemos a virtualizar máquinas reales, así como borrar de forma segura la información sensible.

3. Seguridad física y ambiental

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc., la seguridad de la misma será nula si no se ha previsto cómo combatir un robo o un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa, que intenta a acceder físicamente a una sala de operaciones de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr acceder y robar una cinta o DVD de backup, que intentar acceder de forma remota o lógica a los datos que contienen los sistemas.

Así, la seguridad física consiste en **la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial**.

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 al mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

En este tema se abarcarán medidas aplicables tanto a equipos de hogar y pequeñas oficinas como a servidores y centros de procesamiento de datos (CPD), que por su gran valor en la empresa requieren de medidas de seguridad específicas.

Centros de procesado de datos (CPD)

Se denomina procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como **centro de cómputo** (Iberoamérica) o **centro de cálculo** (España), o centro de datos por su equivalente en inglés **data center**. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones.

Un CPD, por tanto, es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y en general electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las

compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios interconectados, en distintas ubicaciones geográficas, con distintos **centros de respaldo**.

Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia o fallo. Debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.

El equipamiento hardware no tiene por qué ser igual al del CPD, aunque el software y los datos si, por lo que es necesario contar con una **réplica de los mismos datos** con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo, por lo que existen políticas de gestión de copias síncronas o asíncronas de datos.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el **garantizar la continuidad y alta disponibilidad** del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica. Requisitos generales:

- **Disponibilidad y monitorización "24x 7x 365":** proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.
- **Fiabilidad infalible (5 nueves):** un 99,999% de disponibilidad, lo que se traduce en una única hora de no disponibilidad al año.
- **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:** el control del ambiente trata de la calidad del aire, temperatura, humedad, inundación, electricidad, control de fuego, etc.

Generalmente, en un CPD todos los grandes servidores se suelen concentrar en una sala denominada sala fría, nevera o **pecera**. Esta sala requiere un sistema específico de refrigeración para mantener una temperatura baja (entre 21 y 23 grados centígrados), necesaria para evitar averías a causa del sobrecalentamiento. Según las normas internacionales, la temperatura exacta debe ser **22,3 grados centígrados**, recomendada entre 15° y 23°, y humedad relativa entre 40% y 60%.

La pecera suele contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.

Un CPD y sus centros de respaldo por sí solo no bastan para hacer frente a una contingencia grave. Es necesario disponer de un **Plan de Contingencias** corporativo, con las **actuaciones en caso** de incidente.

Veremos algunas de las configuraciones avanzadas empleadas en alta disponibilidad en CPD y centros de respaldo en el tema 8.

Ubicación y acondicionamiento físico

Aunque son difíciles de predecir con exactitud, las condiciones atmosféricas adversas severas se localizan espacial y temporalmente en ciertas partes del mundo y la **probabilidad de que ocurran está documentada**.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la ubicación y posterior construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de condiciones atmosféricas adversas, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, construcciones antisísmicas, la provisión de calor, iluminación o combustible para la emergencia. Algunos de los aspectos a tener en cuenta son:

- **Incendios:** son causados por el uso inadecuado de combustibles, fallo de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. Algunas precauciones: ubicación en área no combustible o inflamable, tener extintores manuales (portátiles) y/o automáticos (rociadores).
- **Sistema de aire acondicionado:** control de temperatura y humedad relativa según recomendaciones, entre 15° - 23° C, y 40 - 60 %, respectivamente.
- **Inundaciones:** ubicación estanca de agua, con especial precaución en puertas y ventanas.
- **Terremotos:** los fenómenos sísmicos pueden ser tan intensos que causen la destrucción de edificios. Es recomendable conocer la actividad sísmica de la localización de nuestro centro de datos para disponer de las técnicas de seguridad constructivas requeridas.
- **Rayos e interferencias electromagnéticas:** para evitar posibles desastres provocados por derivaciones de carga por rayos, y minimizar el efecto no deseado de interferencias en las comunicaciones, las salas de sistemas se protegen mediante jaula de Faraday, convirtiéndose en un bunker con respecto a radiaciones externas.

Control de acceso físico

Los ordenadores, servidores, así como las copias de seguridad con datos importantes y el software, son elementos valiosos para las empresas y están expuestas a posibles robos y actos delictivos como sabotajes o destrozos, por parte de personal ajeno o propio de la empresa. El software es una propiedad muy fácilmente sustraíble y las unidades de almacenamiento como memorias USB, cintas y discos son fácilmente copiados sin dejar ningún rastro.

El uso de **credenciales de identificaciones** uno de los puntos más importantes del sistema de seguridad físico, a fin de poder efectuar un control eficaz del ingreso y salida del personal a los distintos sectores de la empresa. El control de acceso físico no solo requiere la capacidad de identificación, sino también **asociarla a la apertura o cerramiento de puertas**, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. A las personas se les puede identificar por:

- **Algo que se posee**, por ejemplo una llave, una tarjeta de identificación o tarjeta inteligente (SmartCard).
- **Algo que se sabe**, por ejemplo un número de identificación único (PIN - Personal Identification Number) o una password, que se solicitará a su ingreso.
- **Algo que se es** (señas de identidad: manos, ojos, huellas digitales y voz) o sabe hacer (firma escrita) es un principio que emplea la biometría. Es el método más seguro, ya que es muy difícil de falsificar.

Cada una de estos identificadores asociados a cada persona o usuario se almacenan en una base de datos que debe controlar un **servicio de vigilancia** para su posterior seguimiento, si fuera necesario. La principal precaución con el personal de vigilancia es que éste puede llegar a ser sobornado. Las tarjetas pueden ser copiadas, robadas, etc., y los números secretos pueden llegar a

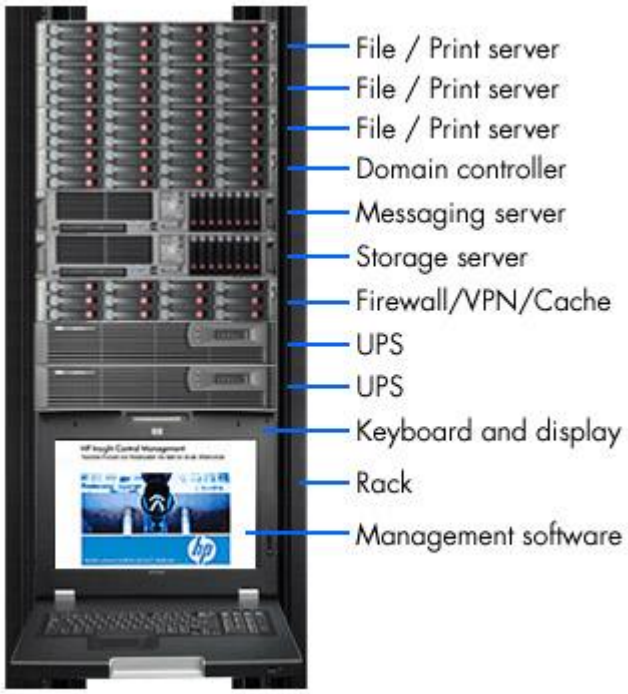
usuarios no autorizados, permitiendo entrar a cualquier persona que la posea. La biometría ayuda a mejorar el nivel de seguridad.

Otra solución muy empleada para la seguridad de los sistemas informáticos en las salas de equipamiento informático, es disponer los mismos en un **armario o rack** bajo llave.

Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante. Constan de un armazón metálico con un ancho normalizado de **19 pulgadas**, con 2 guías verticales que poseen agujeros a intervalos regulares llamados unidades de Rack (U) agrupados de tres en tres. Verticalmente, los racks se dividen en regiones de **1,75** pulgadas de altura **= 1 U**, con tres agujeros en cada guía.

El alto (4 - 46U) y la profundidad del bastidor (600, 800,1000 mm) no está normalizada, ya que así se otorga cierta flexibilidad al equipamiento.

El armazón suele contar con bandejas horizontales donde puede apoyarse el equipamiento no normalizado como un monitor, PC de sobremesa y un teclado o un ratón.



Los dispositivos que se suelen alojar son: servidores, paneles de parcheo (que centralizan todo el cableado del armario) sistemas de audio y vídeo, sistemas de alimentación ininterrumpida (UPS o SAI), switches, routers, cortafuegos, periféricos que permitan configuración como monitores, ratón, teclad o, etc.

Sistemas biométricos

Definimos la biometría como **la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos**. Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos, de esta forma permitirá el control de

acceso físico, incluso es aplicable como método de identificación y acceso a sistemas operativos y aplicaciones. Las características biométricas de una persona son **intransferibles** a otra, por lo que hace a estos sistemas **muy seguros**.

Veamos a continuación algunas de las formas de identificación biométricas más comunes:

- **Huella digital:** se basa en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados **minucias**) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que cada persona posee más de 30 minucias, y que dos personas no tienen más de ocho minucias iguales, lo que hace al método sumamente confiable, y uno de los más empleados por su baja relación calidad/precio.

- **Verificación de voz**: la dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.), este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc., por lo que no es un mecanismo muy adoptado.
- **Verificación de patrones oculares**: basado en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). La principal desventaja es que es un método intrusivo. Las personas son reacias a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

- **Verificación Automática de Firmas** (VAF): es extremadamente difícil reproducir las dinámicas del trazo de realización de las firmas, aunque el efecto visual final parezca similar. La VAF, usa emisiones acústicas, toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo.

Existen algunas otras soluciones a la biometría más complejas y menos usadas en acceso a organizaciones o a un sistema informático concreto, como son la geometría de la mano, el reconocimiento facial o patrones térmicos.

Lo que sigue a continuación es una tabla en la que se recogen las diferentes características de los 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

Circuito cerrado de televisión (CCTV)

Se llama **protección electrónic**a a la detección de robo, intrusión, asalto e incendios mediante la utilización de **sensores conectados a centrales de alarmas**. Estas centrales tienen conectados los elementos de señalización, que son los encargados de hacer saber al personal de una situación de emergencia. Uno de los métodos más empleados en las empresas son los circuitos con cámaras de grabación de vídeo o **circuitos cerrados de televisión (CCTV).**

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizadas como medida disuasiva, incluso en ocasiones se instalan falsificaciones o cámaras que no graban) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

En la actualidad unas de las cámaras más empleadas, por bajo coste y buenas prestaciones son las cámaras IP. Son dispositivos autónomos que cuentan con un servidor web de vídeo incorporado, lo que les permite transmitir su imagen a través de redes IP como redes **LAN**, **WAN**, o incluso **WLAN** o inalámbrica. Las cámaras IP permiten al usuario tener la cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de Internet o una red local.

En este punto os aconsejo desconectar un poco y revisar el punto de jugando con cámaras cctv que hay en el aula virtual.

4. Sistemas de alimentación ininterrumpida (SAI)

Un **SAI** (Sistema de Alimentación Ininterrumpida), también conocido por sus siglas en inglés **UPS** (Uninterruptible Power Supply, suministro de energía ininterrumpible), es un dispositivo que gracias a sus **baterías** puede proporcionar energía eléctrica tras un corte de suministro eléctrico a todos los dispositivos que tenga conectados, durante un tiempo limitado, permitiendo de este modo poder apagar los equipos sin que sufran cortes sus fuentes de alimentación.

Los distintos dispositivos hardware no irán enchufados a las tomas de corriente directamente, se enchufarán a la SAI que será la que estará conectada a las tomas de corriente, haciendo de este modo de intermediario entre la red eléctrica y los dispositivos hardware.

Existen distintos modelos de SAI ajustándose a las necesidades energéticas de los equipos conectados a las mismas.

Características	Descripción

Tipo y número de conectores	Los conectares de alimentación de la carga se diferencian entre tipo IEC y Schucko.  Existen tomas que solo filtran variaciones de la señal eléctrica de entrada (impresora, fax, escáner), de aquellas que filtran y tienen alimentación de la batería en caso de corte de suministro (equipos, monitores, dispositivos de comunicaciones) denominadas de backup.
Otras conexiones	Conectores para la protección de Líneas de Datos RJ11-RJ45 para dispositivos de Teléfono/Fax/DSL/Internet/MODEM. Conexiones seriales COM o USB para monitorización y consulta de estado remoto, mediante software específico.
Tiempo de funcionamiento solo con batería.	Según el modelo y la carga conectada, la batería suele estar diseñada para suministrar alimentación desde varios minutos hasta varias de horas y, de esa forma, apagar los sistemas conectados correctamente.
Regulador de voltaje	Integrado para evitar picos (subidas y bajadas) de tensión que se producen en la línea de suministro de entrada y que si no se filtran pueden afectar a las fuentes de alimentación de los equipos.

Otra de las funciones de los SAI es la de **mejorar la calidad de la energía eléctrica que llega a los aparatos**, **filtrando subidas y bajadas de tensión y eliminando armónicos de la red eléctrica**. Los SAI dan energía eléctrica a equipos llamados cargas o equipos críticos, como pueden ser aparatos médicos, industriales o informáticos que, como se ha dicho antes, requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Tipos de SAI

Habitualmente, los fabricantes de SAI clasifican los equipos en función de la tecnología y calidad de la señal eléctrica generada a su salida:

- **SAI OFFLINE**: los más económicos, recomendados para equipos en el hogar. No estabilizan la corriente y solo generan la tensión de salida cuando se produce un corte de suministro eléctrico.
- **SAI INLINE** o **LINE INTERACTIVE**: equipos de gama media-alta que estabilizan la corriente incorporando un estabilizador de salida (AVE). Solo general la tensión de salida cuando se produce un corte de suministro eléctrico. Son adecuados para ordenadores, centralitas telefónicas y equipos servidores de pequeñas y medianas empresas (Pymes).
- **SAI ONLINE** o de **DOBLE CONVERSIÓN**: equipos de gama alta, pensados para proteger sistemas críticos.

Estos equipos generan siempre la tensión de salida nueva, independientemente de la entrada.

Potencia necesaria

Para ajustar las dimensiones y capacidad eléctrica de la batería de la SAI a la que enchufar nuestros equipos, también denominados carga, es necesario realizar un cálculo de la potencia que consumimos y por tanto que necesitamos suministrar por las conexiones de batería de la SAI.

La **potencia eléctrica** se define como la cantidad de energía eléctrica o trabajo que se transporta o que se consume en una determinada unidad de tiempo.

Cuando se trata de corriente continua (CC) la potencia eléctrica (P) desarrollada en un cierto instante por un dispositivo de dos terminales, es el producto de la diferencia de potencial entre dichos terminales (V) y la intensidad de corriente (I) que pasa a través del dispositivo. Esto es, **P = V x I.** Si I se expresa en amperios y V en voltios, P estará expresada en vatios.

En circuitos eléctricos de corriente alterna (CA), como son las tomas de corriente (enchufes), se emplean medidas de potencia eficaz o aparente y potencia real. La unidad de potencia que suministran comercialmente los SAI es el **voltiamperio** (VA), que es potencia **aparente**, también denominada potencia **efectiva** o **eficaz**, **consumida por el sistema**.

Si tenemos la potencia en vatios (W) **potencia real**, de forma aproximada se multiplica por 1,4 para tener en cuenta el pico máximo de potencia que puede alcanzar su equipo y de esta forma obtener la potencia aparente en VA.

Por ejemplo: 200 W x 1,4 = 280 VA. En ocasiones el factor 1,4, puede ser 1,33 ó 1,6 o factor divisor 0,7 ó 0,75, depende de la eficiencia energética del dispositivo electrónico.

Algunos métodos para calcular el consumo en W de nuestros equipos y de esta forma estimar.

- Mediante un **medidor de potencia** o mediante una pinza **amperimétrica** que mida la corriente suministrada para los equipos conectados, de esta forma multiplicando por la tensión nominal (en España 230 V), podremos obtener el consumo medio aproximado.
- Conociendo el **consumo medio (W) suministrado en las características del fabricante.**
- Mediante un modelo aproximado de estimación de consumos, tomando como referencia estimaciones previas. Por ejemplo podemos ver estimaciones de consumos en la **web de etiquetado de eficiencia energética Energy Star**.

La carga total enchufada a la batería de la SAI, se recomienda que **no sobrepase el 70%** del total de la potencia suministrada por la misma.

Por ejemplo: en caso de querer enchufar a 4 tomas de una SAI, 2 PC y 2 monitores que consumen en total 200 W, nuestra SAI deberá de suministrar 200 x 1,4 = 280 VA. Por tanto, nuestra SAI deberá de tener al menos una potencia máxima suministrada de 280 x 100/70 = 400 VA.

Práctica 2.5 Monitorización de la SAI. Probaremos a monitorizar una de las SAI del departamento, investigando sobre sus características.

Práctica 2.6 Cálculo energético de la SAI. Estudiaremos el consumo de los elementos conectados a las SAI del departamento, pudiendo hacer un informe en cuanto a la adecuación del uso del mismo.

0. Índice

2. Copias de seguridad 2
Modelo de almacén de datos 2
Recomendación sobre el tipo de copia a efectuar 3
Recuperación de datos 4
3. Seguridad física y ambiental 5
Centros de procesado de datos (CPD) 5
Ubicación y acondicionamiento físico 6
Control de acceso físico 7
Sistemas biométricos 8
Circuito cerrado de televisión (CCTV) 9
4. Sistemas de alimentación ininterrumpida (SAI) 10
Tipos de SAI 11
Potencia necesaria 11
0. Índice 13