Seguridad Informática - 2º SMR
Tema 2: Seguridad pasiva. Hardware y almacenamiento

2.1. Ubicación y protección física

El primer paso para establecer la seguridad de un servidor o un equipo es decidir adecuadamente donde vamos a instalarlo. Esta decisión puede parecer superflua, pero nada más lejos de la realidad: resulta vital para el mantenimiento y protección de nuestros sistemas.

Los planes de seguridad física se basan en proteger el hardware de los posibles desastres naturales, de incendios, inundaciones, sobrecargas eléctricas, robos y otra serie de amenazas.

Se trata, por tanto, de aplicar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas para proteger los recursos y la información, tanto para mantener la seguridad dentro y alrededor del Centro de Cálculo como los medios de acceso remoto a él o desde él.

2.1.1 Factores para elegir la ubicación

Cuando hay que instalar un nuevo centro de cálculo es necesario fijarse en varios factores. En concreto, se elegirá la ubicación en función de la disponibilidad física y la facilidad para modificar aquellos aspectos que vayan a hacer que la instalación sea más segura. Existen una serie de factores que dependen de las instalaciones propiamente dichas, como son:

- **El edificio.** Debemos evaluar aspectos como el espacio del que se dispone, cómo es el acceso de equipos y personal, y qué características tienen las instalaciones de suministro eléctrico, acondicionamiento térmico, etc. Igualmente, hemos de atender a cuestiones de índole física como la altura y anchura de los espacios disponibles para la instalación, si tienen columnas, cómo es el suelo, la iluminación, etc. Además atenderemos a la seguridad física del edificio contra incendios, inundaciones y otros peligros naturales que puedan afectar a la instalación.

- **Tratamiento acústico.** En general, se ha de tener en cuenta que habrá equipos, como los de aire acondicionado, necesarios para refrigerar los servidores, que son bastante ruidosos. Deben instalarse en entornos donde el ruido y la vibración estén amortiguados.

- **Suministro eléctrico propio del CPD.** La alimentación de los equipos de un centro de procesamiento de datos tiene que tener unas condiciones especiales, ya que no puede estar sujeta a las fluctuaciones o picos de la red eléctrica que pueda sufrir el resto del edificio. No suele ser posible disponer de toda una red de suministro eléctrico propio, pero siempre es conveniente utilizar un sistema independiente del resto de la instalación y elementos de protección y seguridad específicos, como sistemas de alimentación ininterrumpida.

- **Condiciones ambientales** que rodean al local donde vayamos a instalar el CPD. Los principales son los factores naturales (frío, calor, inundaciones, incendios o terremotos); los servicios disponibles, especialmente de energía eléctrica y comunicaciones (antenas, líneas telefónicas, etc.), y otras instalaciones de la misma zona; y la seguridad del entorno, ya que la zona donde vaya a situarse el CPD

debe ser tranquila, pero no un sitio desolado. Otros factores que han de tenerse en consideración son el vandalismo, el sabotaje y el terrorismo.

2.1.2 ¿Donde se debe instalar el CPD?

Atendiendo solo a estos factores ya podemos obtener las primeras conclusiones para instalar el CPD en una ubicación de características idóneas. Así pues, siempre que podamos, tendremos en cuenta que:

- Deben evitarse áreas con fuentes de interferencia de radiofrecuencia, tales como transmisores de radio y estaciones de TV.
- El CPD no debe estar contiguo a maquinaria pesada o almacenes con gas inflamable o nocivo.
- El espacio deberá estar protegido ante entornos peligrosos, especialmente inundaciones. Se buscará descartar:
  - Zonas cercanas a paredes exteriores, planta baja o salas de espera, ya que son más propensas al vandalismo o los sabotajes.
  - Sótanos, que pueden dar problemas de inundaciones debido a cañerías principales, sumideros o depósitos de agua.
  - Última planta, evitando desastres aéreos, etc.
  - Encima de garajes de vehículos de motor, donde el fuego se puede originar y extender más fácilmente.

Según esto, la ubicación más conveniente se sitúa en las plantas intermedias de un edificio o en ubicaciones centrales en entornos empresariales.

> **Ejercicios propuestos**
>
> **2.1.1.** Estudia las instalaciones de tu centro. Dadas las características del mismo, ¿donde crees que podría instalarse un pequeño CPD?

2.1.3 Control de acceso

De modo complementario a la correcta elección de la ubicación del CPD es necesario un férreo control de acceso al mismo. Dependiendo del tipo de instalación y de la inversión económica que se realice se dispondrá de distintos sistemas de seguridad, como los siguientes:

- Servicio de vigilancia, donde el acceso es controlado por personal de seguridad que comprueba la identificación de todo aquel que quiera acceder a una ubicación. En general, suele utilizarse en el control de acceso al edificio o al emplazamiento y se complementa con otros sistemas en el acceso directo al CPD.

- Detectores de metales y escáneres de control de pertenencias, que permiten “revisar” a las personas, evitando su acceso a las instalaciones con instrumentos potencialmente peligrosos o armas.

- Utilización de sistemas biométricos, basados en identificar características únicas de las personas cuyo acceso esté autorizado, como sus huellas digitalizadas,su iris, la voz o la dinámica de firma manuscrita.

- Protección electrónica, basada en el uso de sensores conectados a centrales de alarma que reaccionan ante la emisión de distintas señales. Cuando un sensor detecta un riesgo, informa a la central que procesa

la información y responde según proceda, por ejemplo emitiendo señales sonoras que alerten de la situación.

Ejercicios propuestos

2.1.2. Busca información sobre distintos sistemas de protección electrónica, sus aplicaciones y costes de implantación.

2.1.3. Investiga acerca de los precios y características de periféricos como teclado, ratón con lector de huella, o lector de huella USB, así como el software compatible con ellos. Realiza una tabla resumen.

2.1.4 Sistemas de climatización

Además de instalar el CPD en la mejor localización posible, es imprescindible que se instalen en su interior sistemas de climatización, de protección contra incendios (PCI) y sistemas de alarma apropiados.

Los equipos de un CPD disipan mucha energía calorífica y hay que refrigerarlos adecuadamente para mantener las condiciones interiores de temperatura y humedad estables, ya que las altas temperaturas podrían dañar estos equipos

Podemos, por ejemplo, utilizar un ventilador que expulsa el aire caliente al exterior para refrigerar un servidor, pero debemos tener en cuenta que haya recirculación de aire y que éste atraviese el servidor *(figura 1)*.

Para un CPD con varios racks, podemos optar por el uso de equipos murales (splits) que darán directamente aire frío a los racks. *(figura 2)*.

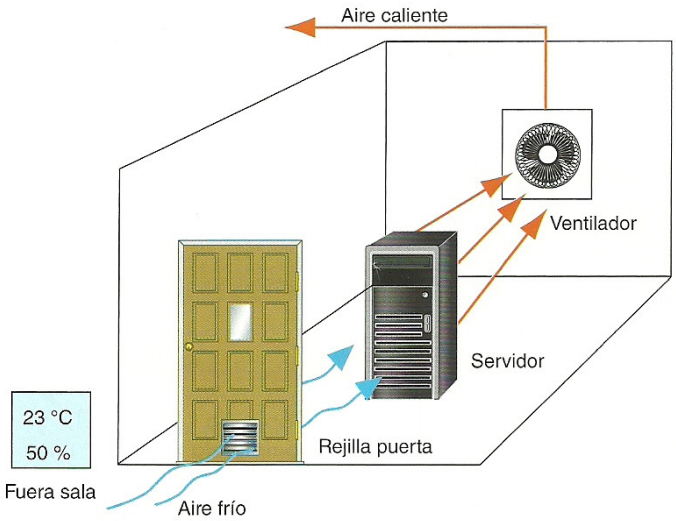


Figura 1

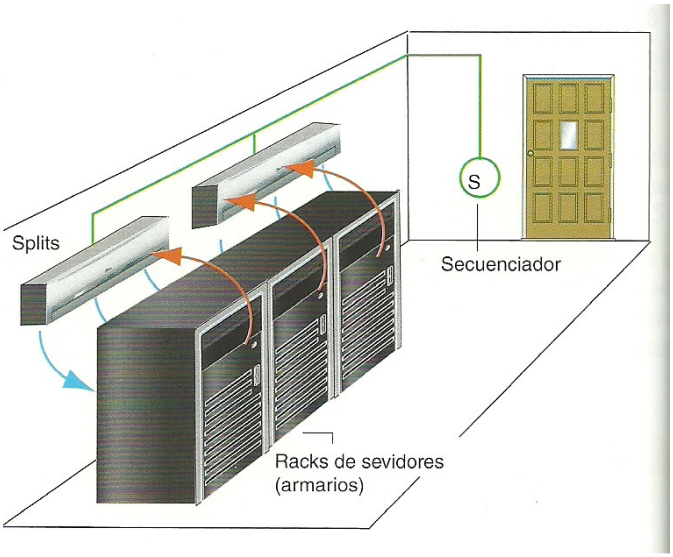


Figura 2

2.1.5 Sistemas contra incendios

Estos sistemas no son instalados por los responsables de seguridad informática, aunque sí es necesario conocer su funcionamiento:

- Sistema de detección: Por ejemplo el sistema de detección precoz, que realiza análisis continuos del aire, de modo que pueda observar un cambio de composición en el mismo, detectando un incendio incluso antes de que se produzca el fuego.
- Sistema de desplazamiento del oxígeno: Reduce la concentración de oxígeno, extinguiendo así el fuego sin necesidad de usar agua, que podría estropear los equipos. Para el uso de este sistema, es necesario que antes haya una evacuación de todo el personal, pues podría peligrar su integridad física.

2.1.6 Recuperación en caso de desastre

Una opción a tener en cuenta es la de tener un centro de backup independiente, de modo que aunque los equipos del CPD queden fuera de servicio, la organización podrá seguir realizando su actividad con cierta normalidad recuperando sus datos. También es conveniente la realización de sistemas redundantes, como sistemas RAID y copias de seguridad.

En caso de que se produzca un desastre, el comité de crisis decidirá poner en marcha el plan de contingencia, recuperando en primer lugar las bases de datos y ficheros esenciales, así como desviar las comunicaciones más críticas al centro alternativo.

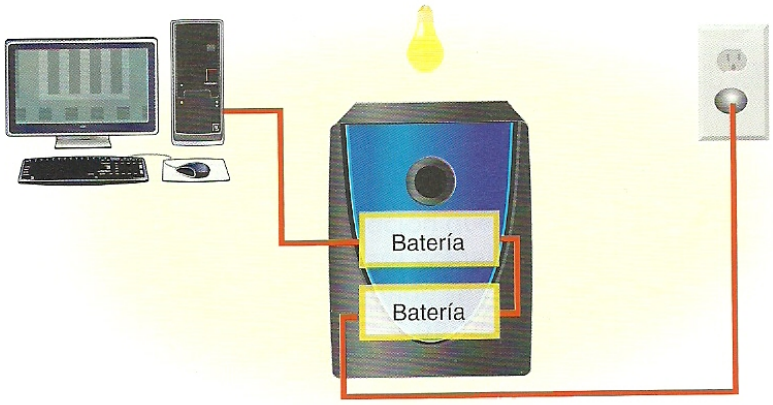
> **Ejercicios propuestos**
>
> **2.1.4.** Investiga sobre los distintos sistemas de climatización y contra incendios que podrían ser adecuados para el CPD de una pequeña empresa.

2.2 Sistemas de alimentación ininterrumpida (SAI)

Un SAI o sistema de alimentación ininterrumpida es un dispositivo electrónico que permite proteger a los equipos frente a los picos o caídas de tensión. De esta manera se dispone de una mayor estabilidad frente a los cambios del suministro eléctrico y de una fuente de alimentación auxiliar cuando se produce un corte de luz.

2.2.1 Tipos de SAI

- **Sistemas de alimentación en estado de espera o Stand-by Power Systems (SPS).** Este tipo de SAI activa la alimentación desde baterías automáticamente cuando detecta un fallo en el suministro eléctrico.
- **SAI en línea (on-line)**, que alimenta el ordenador de modo continuo, aunque no exista un problema en el suministro eléctrico, y al mismo tiempo recarga su batería. Este dispositivo tiene la ventaja de que ofrece una tensión de alimentación constante, ya que filtra los picos de la señal eléctrica que pudiesen dañar el ordenador, si bien el tiempo extra que ofrecen es menor que el de los SPS.



Ejercicios propuestos

2.2.1. Un SAI tiene un precio elevado lo cual no suele ser asequible para un usuario doméstico. En el mercado existen alternativas más económicas para proteger los equipos contra subidas y picos de tensión. Busca información sobre estos equipos y selecciona el que te parezca más adecuado para tu ordenador personal. Puedes consultar las páginas de fabricantes como Emerson, APC, Eaton o Socomec.

2.2.2. Realiza una tabla comparativa que analice diferentes tipos y modelos de SAIs existentes en el mercado teniendo en cuenta el tiempo extra que proporcionan, si protegen contra picos de tensión, el número de equipos que se pueden conectar y el precio. Teniendo en cuenta estos parámetros, decide el SAI a comprar para:

- Un ordenador personal para un casa.
- Un servidor de un centro pequeño como un instituto.
- Un CPD con 10 servidores.

Si para el ordenador personal consideras que los SAIS en línea serían demasiado caros, indica a su vez otros dispositivos que puedan proteger un equipo de subidas o bajadas de tensión.

2.3 Almacenamiento de la información

Otro de los factores claves de la seguridad es cómo y dónde se almacena la información. Los tres aspectos más importantes que debemos tener en cuenta cuando tratemos la seguridad física de la información son:

- **Rendimiento:** Capacidad de cálculo de información de un ordenador.
- **Disponibilidad:** Capacidad de los sistemas de estar siempre en funcionamiento. Un sistema de alta disponibilidad está compuesto por sistemas redundantes o que trabajan en paralelo y así cuando falla el sistema principal, se arranquen los sistemas secundarios automáticamente y el equipo no deje de funcionar en ningún momento.
- **Accesibilidad a la información:** disponer de nuestros datos relativamente cerca para que en caso de desastre no tardemos demasiado tiempo en recuperar el sistema.

Existen numerosas técnicas que nos pueden proporcionar estas características, como los sistemas RAID, los clusters de servidores y las arquitecturas SAN y NAS.

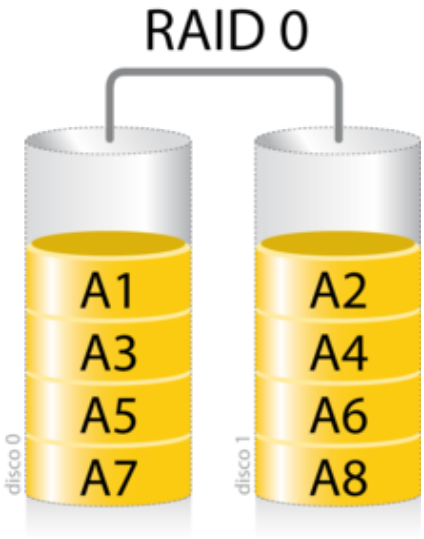
2.4 Almacenamiento redundante y distribuido (RAID)

RAID consiste en un conjunto de técnicas HW y SW que utilizando varios discos y distribuyendo o replicando la información entre ellos consigue alguna de las siguiente características:

- Mayor **capacidad**: Combinando varios discos más o menos económicos conseguimos una unidad de almacenamiento de una capacidad mucho mayor que la de los discos por separado.
- Mayor **tolerancia a fallos**: En caso de error, el sistema será capaz en algunos casos de recuperar la información perdida y seguir funcionando correctamente.
- Mayor **seguridad**: Al ser tolerante a fallos y mantener cierta duplicidad de la información, aumentaremos la disponibilidad y mejoraremos la integridad de los datos.
- Mayor **velocidad**: Cuando la información esté repetida y distribuida, se podrán realizar varias operaciones simultáneamente, lo que provocará mayor velocidad.

2.4.1 RAID 0

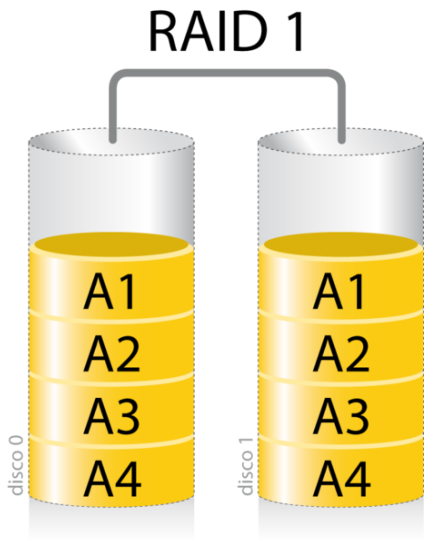
Los datos se distribuyen equilibradamente entre 2 o más discos, pero no hay redundancia de información.



Esta técnica favorece la velocidad cuando se lea o escriba un dato repartido en varios discos si éstos están gestionados por controladoras independientes. No es tolerante a fallos, ya que no hay información redundante.

2.4.2 RAID 1

También conocido como disco espejo, consiste en mantener una copia idéntica de un disco en otro, de forma que el usuario ve sólo una unidad pero físicamente está siendo almacenada en dos o más discos.

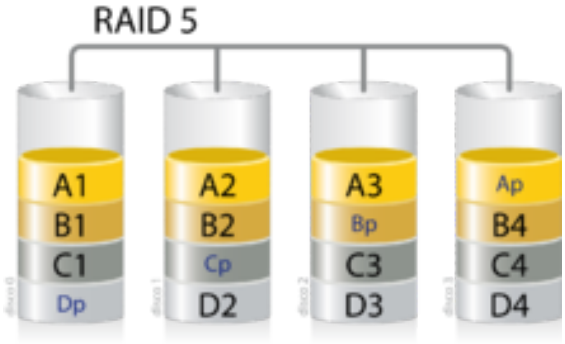


Tolerante a fallos, si falla un disco, sigue funcionando con los otros mientras cambiamos el disco estropeado y rehacemos el espejo.

El inconveniente es que si toda la información está duplicada, reducimos nuestro espacio de almacenamiento a la mitad.

2.4.3 RAID 5

Los bloques de datos que se almacenan en la unidad y la información redundante de dichos bloques (bloques de paridad) se distribuye cíclicamente entre todos los discos que forman el volumen (mínimo 3). Cada línea de datos se almacenará en bloques en los distintos discos dejando un disco para el bloque de paridad, que irá rotando para cada línea.

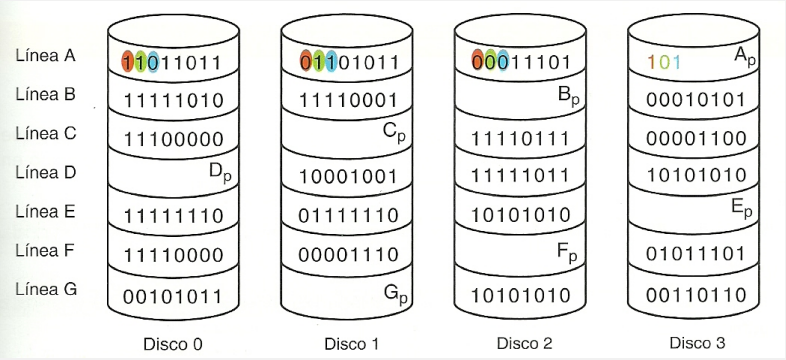


- De esta forma aumenta la velocidad ya que podemos acceder a varios discos a la vez (como en RAID 0) y el sistema es tolerante a fallos, ya que si se produce algún error en un disco, con el bloque de paridad se podría recuperar la información.
- El bloque de paridad se calcula a partir de los bloques de la misma línea, de forma que el primer bit será un 1 si hay un número impar de unos en el primer bit de los bloques de datos, y un 0 si hay un número par de unos.

Estos sistemas no son los únicos RAID. Existen más tipos, algunos de ellos que provienen de la combinación de dos tipos de sistema RAID, por ejemplo RAID 0+1 que combina RAID 0 con RAID 1, aprovechando la velocidad de uno con la tolerancia a fallos del otro.

Ejercicios propuestos

2.4.1. Dado el conjunto de 4 discos que muestra la figura, calcula los bloques de paridad y completa la figura.



- Imagina que se perdiera el disco 1. Llega una petición de lectura de la línea F, ¿podría realizarse? ¿cómo?
- Una vez que se ha conseguido un disco adecuado se decide sustituir el disco dañado y recuperar el funcionamiento normal usando los 4 discos. Recupera la información de dicho disco utilizando solo la información de los discos 0, 2 y 3.

2.5 Clusters de servidores

Es un conjunto de servidores que se construyen e instalan para trabajar como si fuesen uno solo. Se unen mediante una red de alta velocidad, de tal forma que el conjunto se ve como un único ordenador mucho más potente que los ordenadores comunes.

No es necesario que los equipos sean iguales a nivel de HW ni que tengan el mismo sistema operativo, lo que permite reciclar equipos en desuso.

Con estos sistemas se busca conseguir cuatro servicios principales:

- Alta disponibilidad.
- Alto rendimiento.
- Balanceo de carga.
- Escalabilidad.

2.5.1 Clasificación de los clusters

- **Clusters de alto rendimiento (HC o High Performance)**: Ejecutan tareas que requieren una gran capacidad de cálculo o el uso de grandes cantidades de memoria.
- **Clusters de alta disponibilidad (HA o High Availability)**: Se utiliza hardware duplicado, de modo que en caso de fallo se garantice la disponibilidad del sistema. También incorporan software de detección y recuperación ante fallos, con objeto de hacer más confiable el sistema.
- **Clusters de alta eficiencia (HT o High Throughput)**: El objetivo es que se puedan ejecutar el mayor número de tareas en el menor tiempo posible.

Según su ámbito de uso, hablaremos de dos tipos:

- **Clusters de infraestructuras**: conjugan alta disponibilidad con alta eficiencia.
- **Clusters científicos**: en general son sistemas de alto rendimiento.

2.5.2 Componentes de los clusters

- **Nodos**: Cualquier máquina que usemos para montar el cluster. Aunque no es necesario, es buena idea que los nodos tengan un cierto parecido en cuanto a capacidades para no sobrecargar en exceso a un equipo.
- **Sistema operativo**: Nos vale cualquiera que tenga dos características básicas: multiproceso y multiusuario.
- **Conexión de Red**: Para conectar los nodos del cluster usaremos una conexión Ethernet u otra de alta velocidad (Fast Ethernet, Gigabit Ethernet, Myrinet, Infiniband, SCI, etc).
- **Middleware**: Software que se encuentra entre el SO y las aplicaciones, cuyo objetivo es que el usuario del cluster tenga la sensación de estar frente a un único superordenador ya que provee de una interfaz única de acceso al sistema. Mediante este SW se consigue optimizar el sistema en cuanto al balanceo de carga, tolerancia a fallos y detectar nuevos nodos que vayamos añadiendo al cluster.
- **Sistema de almacenamiento**: Se puede usar el almacenamiento de los discos duros de los equipos que forman el cluster, o recurrir a sistemas más complejos que proporcionan mayor eficiencia y disponibilidad como son los dispositivos NAS o las redes SAN.

> **Ejercicios propuestos**
>
> **2.5.1.** Realiza un listado de sistemas operativos multiusuario y multiprocesador. Consulta en internet si pueden utilizarse para montar un cluster.
>
> **2.5.2.** Busca información sobre las conexiones de alta velocidad mencionadas antes. ¿Qué velocidades proporcionan? ¿Qué requisitos hardware necesitamos para utilizarlas?

2.6 Ejercicios de comprobación

2.6.1. ¿Qué características debe reunir un edificio donde queremos instalar un Centro de Proceso de Datos?

2.6.2. Una empresa de construcción ha decidido trasladar sus oficinas a un nuevo edificio. Estudia las distintas opciones y presenta un informe razonado sobre las ventajas e inconvenientes de los distintos edificios y cual sería el idóneo. Realiza una tabla comparativa con todos los factores.

1. Se trata de 3 edificios situados en diferentes zonas, todas ellas seguras, en la misma área geográfica y sin riesgo de inundaciones y todos tienen un buen sistema antiincencios.
2. El primero de ellos está en el centro de la ciudad junto a una serie de edificios de oficinas y algunas viviendas.
3. El segundo se encuentra en un gran parque empresarial con múltiples oficinas pero donde no hay fábricas.
4. El tercero está en un polígono industrial donde hay fábricas de metalurgia, factorías de vehículos y otras serie de fábricas de maquinaria pesada.
5. Todos los edificios tienen control de acceso mediante guardias y cámaras.
6. En el edificio céntrico disponemos de 7 plantas en un edificio compartido con otras empresa.
7. En el parque empresarial disponemos de un edificio de 6 plantas.
8. En el polígono industrial de un edificio de 2 plantas.
9. Las tres zonas están bien comunicadas y las instalaciones no presentan problemas eléctricos.
10. En el edificio del centro se tendrán que realizar reformas para amortiguar los sonidos.
11. La empresa ha decidido realizar la inversión necesaria para instalar sistemas de control de acceso biométrico al CPD y sistemas de alimentación necesarios.

2.6.3. ¿Qué diferencias hay entre sensores y detectores?

2.6.4. ¿Es posible que el hardware funcione sin corriente eléctrica? Razona tu respuesta.

2.6.5. Explica paso a paso como funciona un SAI antes, durante y después de una caída de la red eléctrica

2.6.6. Busca información sobre el funcionamiento de los sistemas de detección precoz de incendios e ilústralo con casos reales de uso.

2.6.7. Calcula el bloque de paridad de las siguientes líneas de datos en un sistema RAID 5:

DISCO 0	DISCO 1	DISCO 2	DISCO 3	DISCO 4
10001101	10010110	01101100.	10011000	p
00111011	00111111	10011101	p	11101010
00000111	01110101	p	00101101	10110110
11110010	p	10001010	10111011	11101001
p	10011001	01101101.	10101111	

2.6.8. Imaginemos la siguiente linea de datos en un sistema RAID 5 donde se acaba de estropear el disco 1. Recupera el bloque del disco que ha fallado para solucionar el problema.

DISCO 0	DISCO 1	DISCO 2	DISCO 3	DISCO 4
10001101	- - - - - - - -	P**10011101**	10011000	11001001

2.8 Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill