SAD - U1.2 Seguridad Física

Descargar estos apuntes

Índice

1. Importancia de la seguridad física

Desgraciadamente todos los días nos llegan noticias sobre sustracción de bienes materiales: dinero, joyas, etc. Una vez producido el delito, se puede intentar detener al culpable y recuperar los bienes robados; pero es mucho más útil e importante tomar medidas para que estos hechos no se produzcan instalando sistemas de seguridad preventivos: alarmas, rejas en ventanas, puertas de seguridad, etc. Del mismo modo, habitualmente se producen situaciones catastróficas ocasionadas por causas naturales como inundaciones, incendios, etc. Estas situaciones no pueden evitarse, pero sí disminuir sus consecuencias para las personas o bienes, mediante la adopción de medidas preventivas.

Si todas estas situaciones son desagradables en un entorno personal, en el ámbito de la empresa revisten especial gravedad, puesto que afectan a su patrimonio, necesario para llevar a cabo su actividad. En primer término se puede pensar que este patrimonio está integrado por los bienes tangibles de la empresa (mobiliario, ordenadores, etc.), pero aún más importantes que estos son los bienes intangibles (los datos). En efecto, una pérdida de un equipo físico puede ser reemplazada fácilmente; en cambio, es muy posible que la pérdida de los datos de la empresa sea irreemplazable. Además, hay que tener en cuenta que esos datos pueden ser utilizados por otras personas con fines ilícitos (para estafar a la empresa, para averiguar sus secretos industriales, etc.).

Es por ello que la seguridad física adquiere una importancia vital a la hora de preservar tanto los datos que poseen las empresas, como los equipos y dispositivos encargados de su tratamiento y almacenamiento. Podemos, por tanto, definir la seguridad física como:

> El conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos.

Los riesgos externos a los que están sujetos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes:

- Fenómenos naturales, como inundaciones, tormentas, terremotos, etc.
  Se pueden adoptar medidas preventivas como la instalación de los equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección (ubicaciones seguras, pararrayos, etc.).
- Riesgos humanos, como actos involuntarios, actos vandálicos y sabotajes.
  Entre las medidas preventivas estarían: control de acceso a recintos, elaboración de perfiles psicológicos de empleados con acceso a datos confidenciales, formación a usuarios en materia de seguridad, etc.

Riesgos

Actividad U1.1: Indica varios ejemplos de fenómenos naturales y de riesgos humanos que pueden poner en peligro la seguridad física de los equipos informáticos de tu aula.
Indica, respecto a cada uno, si puede evitarse o no y, en su caso, cómo podría evitarse.

2. Protección física de los equipos

En este epígrafe nos ocuparemos de las medidas de protección para los sistemas informáticos, centrándonos en los equipos de usuario. Dejaremos el estudio de la protección de los servidores para el siguiente apartado, ya que suelen estar situados en salas especiales y cuentan con medidas de protección especiales.

2.1. Entorno físico del equipo

Uno de los elementos más importantes a la hora de fijar las medidas preventivas para la seguridad física de los equipos informáticos es el lugar donde estos están situados. Las condiciones físicas de esta ubicación determinan los riesgos a que están sujetos los equipos. Así:

Factor de riesgo	Medidas preventivas
Espacio	Los ordenadores deben tener una buena ventilación; por ello, se debe procurar que exista espacio suficiente alrededor de la carcasa para permitir la correcta circulación del aire caliente proveniente de su interior. Igualmente, se debe evitar colocar objetos sobre la carcasa para no obstruir las salidas de ventilación.
Humedad	La humedad relativa aconsejable es del 50% aproximadamente: una humedad excesiva provoca corrosión en los componentes. Una humedad muy escasa (por debajo del 30%) favorece la existencia de electricidad estática. Por ello, hay que tener cuidado con la calefacción y con el aire acondicionado, pues secan mucho el ambiente.
Luz solar	La luz solar directa debe ser evitada pues puede producir un sobrecalentamiento del equipo. Para evitar la incidencia de los rayos solares sobre el equipo, pueden instalarse persianas y cortinas o cambiar la ubicación del mismo.

Factor de riesgo	Medidas preventivas
Temperatura ambiente	Los ordenadores están formados por componentes electrónicos y magnéticos sensibles a la temperatura. La temperatura ideal para los equipos informáticos se sitúa entre 15 y 25 ºC. Si la temperatura ambiente no está dentro del rango óptimo, es aconsejable la instalación de un aparato de refrigeración o climatización.
Partículas de polvo	El polvo y la suciedad afectan al buen funcionamiento del equipo informático. Por ejemplo, pueden disminuir la refrigeración de los componentes debido a la obstrucción de los ventiladores, etc. Por ello, los equipos deben situarse en zonas de mínimo impacto de partículas adversas y, periódicamente, se debe llevar a cabo una limpieza general del equipo.
Campos magnéticos	Los imanes y electroimanes alteran los campos magnéticos y pueden provocar la pérdida de datos en dispositivos de almacenamiento como el disco duro. Algunos de los dispositivos susceptibles de causar averías de este tipo son: destornilladores imantados, altavoces, motores eléctricos, etc.
Vibraciones y golpes	Pueden provocar averías en el equipo informático, sobre todo en los discos duros. Por ello, se debe colocar el equipo lejos de aparatos que produzcan vibraciones y en lugares resguardados que no sean de paso, fijar bien los componentes y utilizar carcasas de alta calidad.
Suelos	Determinados tipos de suelo (como los laminados), debido a su mala conductividad eléctrica, acumulan electricidad estática. Por ello, se debe poner especial cuidado respecto a la superficie donde se ubica el ordenador. Si se usan alfombras, debe cuidarse de que sean antiestáticas.

2.2. Instalaciones

Además de las condiciones ambientales, hay otras circunstancias derivadas de la ubicación de los equipos y de su propio funcionamiento que pueden ocasionar riesgos para los mismos:

- **Instalación eléctrica adecuada**: los equipos informáticos funcionan gracias a la energía eléctrica que les llega a través de sus conexiones. Una instalación eléctrica defectuosa es susceptible de causar graves daños. Se pueden adoptar las siguientes medidas preventivas:
  - *Protecciones eléctricas adecuadas*. Los enchufes deben contar con tomas de tierra y la corriente suministrada debe ser lo más estable posible para evitar picos de tensión.
  - *Mantenimiento del suministro eléctrico*. La corriente eléctrica está sometida a anomalías, como apagones, caídas de tensión, etc. Hay que tomar las medidas necesarias para minimizar el riesgo de estas anomalías, así como para disminuir sus consecuencias negativas. Para prevenir las averías que estas anomalías pudieran producir a los equipos
    informáticos se desarrollaron los sistemas de alimentación ininterrumpida (SAI). Un SAI es un dispositivo que tiene por finalidad proporcionar alimentación a los equipos conectados a él cuando se produce un corte en la corriente eléctrica, dando tiempo a que los equipos se apaguen de forma adecuada y no se produzca ninguna pérdida de información.
- **Instalación de red adecuada**. Los equipos estarán conectados a una red de datos y esta a su vez a una red general. En primer término, hay que proteger esta red de accesos físicos no deseados. Además, normalmente la red está configurada por cable, por lo que habrá que vigilar que el tipo de cable es el correcto, así como que su estado de conservación es el adecuado al entorno (los cables pueden estar expuestos a la humedad, afectados por radiaciones electromagnéticas, etc.).
- **Control de acceso**. Tanto si el ordenador está en una oficina, como si está en una sala especialmente destinada a su uso, habrá que controlar el acceso a ese lugar. Además, deberá asegurarse la entrada en el equipo en sí mediante el establecimiento de claves.

- **Protección frente a incendios**. Se deben utilizar tanto sistemas de prevención como sistemas de protección:
  - *Sistemas de prevención*: son los más eficaces, pues van encaminados a que no se produzca el incendio. Por ejemplo, instalación de detectores de humo y alarmas, mantenimiento del orden y la limpieza para evitar la acumulación de materiales combustibles, etc.
  - *Sistemas de protección*: son los que se ponen en marcha en caso de que se haya producido un incendio. Los más comunes son la colocación de barreras para aislar el incendio, la delimitación clara de las vías de evacuación y salidas de emergencia y la instalación de sistemas de extinción. En el caso de los incendios que se pueden producir en una oficina con equipos informáticos, los extintores apropiados son los de clase C (o ABC), de polvo seco polivalente o CO2. Nunca se debe intentar apagar uno de estos incendios con agua a chorro debido al riesgo de sufrir una descarga eléctrica.

Agua nebulizada como agente extintor

Si bien en los incendios de líquidos inflamables, equipos eléctricos y electrónicos el uso del agua a chorro está totalmente contraindicado, en los últimos tiempos se está extendiendo el empleo del agua nebulizada como agente extintor válido para este tipo de incendios.

Como veremos en el epígrafe dedicado a los CPD, en caso de incendio de componentes electrónicos, este sistema es muy recomendable, pues no solo extingue el fuego, sino que combate uno de los mayores enemigos de los sistemas electrónicos, como es el humo.

2.3. Sistemas de alimentación ininterrumpida

Como hemos visto en el apartado anterior, una de las principales fuentes de riesgo para los sistemas informáticos es la corriente eléctrica. Esta corriente no es perfecta, sino que está sometida a anomalías (apagones, caídas y picos de tensión, sobrevoltajes, ruido eléctrico, etc.) que hacen que el funcionamiento de los equipos no sea el idóneo y que, en los casos más graves, pueden ocasionar importantes daños a los mismos.

Para prevenir estos riesgos se han desarrollado los **sistemas de alimentación ininterrumpida (SAI)**, conocidos también por su nombre en inglés, *Uninterrupted Power Supply (UPS)*.

> Un SAI es un dispositivo cuya finalidad es proporcionar suministro eléctrico a los equipos conectados a él cuando se produce un corte en la corriente eléctrica.

Los SAI no tienen capacidad para suministrar corriente durante mucho tiempo, por ello, no están pensados para que los equipos conectados a ellos sigan funcionando a pleno rendimiento, sino que su función es ganar tiempo para realizar un apagado ordenado de los equipos. Además de esta función principal, sirven como estabilizadores de la tensión eléctrica, filtrándola y reduciendo el efecto nocivo que producen los picos de tensión y el ruido eléctrico.

El uso de estos dispositivos es beneficioso para todo tipo de equipos, aunque, debido a su elevado coste, tradicionalmente solo se instalaban en sistemas críticos como servidores, grandes bases de datos, hospitales, etc., donde su uso no solo era beneficioso sino imprescindible. Actualmente su precio ha bajado bastante y existen modelos asequibles para ser instalados en cualquier ordenador.

Tipos de SAI

Dependiendo de su modo de funcionamiento, podemos distinguir varios tipos de SAI:

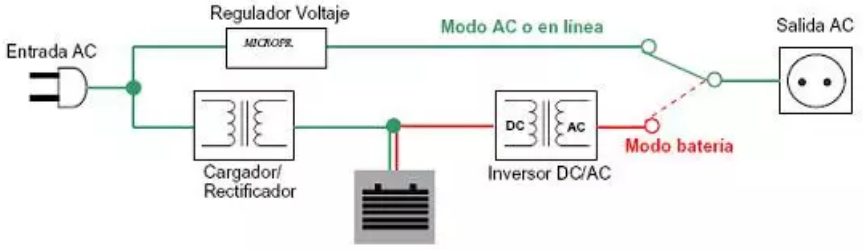
- **Offline pasivos**. Se ponen en funcionamiento cuando falla la alimentación eléctrica. Entre el fallo y su activación se produce un corte de energía muy pequeño que no es detectado por la mayoría de los equipos conectados a él. Son los

más habituales para proteger ordenadores domésticos, televisores, etc.

- **Offline interactivos In-Line**. Están conectados con la corriente eléctrica y siempre se encuentran activos. Además de su función principal, disponen de filtros activos que estabilizan la señal. Son de mejor calidad que los anteriores y se suelen utilizar para proteger equipos de pequeñas empresas (ordenadores, pequeños servidores, etc.).
- **Online**. Se colocan entre el suministro normal de corriente y los equipos a proteger, cumpliendo también con la función de estabilización y filtrado de la señal. Las baterías se van cargando mientras se suministra energía a los equipos, por lo que, en caso de apagón, en ningún momento deja de suministrarse energía. Esto tiene como consecuencia el progresivo deterioro de las baterías y la necesidad de su sustitución. Son los más caros y de mayor calidad.

Un SAI está compuesto por las siguientes partes o bloques funcionales:

- **Batería y cargador**: son los elementos que almacenan la carga eléctrica que se usará en caso de necesidad.
- **Filtro**: elemento destinado a limpiar la señal.
- **Conversor**: es un transformador que convierte la tensión de 12 v de su batería en corriente continua.
- **Inversor**: convierte la corriente continua en corriente alterna a 220 v.
- **Conmutador**: elemento que permite cambiar entre el suministro proporcionado por la red eléctrica y el generado por la batería del SAI.



Características de los SAI

Los SAI tienen dos características que permiten diferenciarlos:

- Autonomía: es el tiempo que el SAI puede seguir alimentando a un equipo en caso de fallo eléctrico. Se mide en minutos.
- Potencia: mide el consumo de energía de un SAI y se expresa en dos unidades distintas:
  - *Vatios (**W**)*: es la potencia real consumida por el dispositivo.
  - *Voltiamperios (**VA**)*: es la potencia aparente, que se halla multiplicando la tensión de la corriente en voltios por la intensidad en amperios. Normalmente, en las especificaciones técnicas de los SAI, la potencia va expresada en esta unidad.

> La relación entre VA y W se denomina *factor de potencia* y su valor está siempre entre 0 y 1 (normalmente alrededor de 0,6), ya que la potencia real siempre es mayor que la aparente.

Sistemas de alimentación ininterrumpida

Actividad U2.1: Busca en Internet un SAI y responde a las siguientes preguntas:

- a. ¿Qué tipo de SAI es?
- b. ¿Cuál es su autonomía?
- c. ¿Cuál es su potencia en VA y en W?
- d. ¿Cuál es su precio?

Actividad U2.2: Cálculo de la potencia de un SAI
Un equipo informático doméstico está compuesto por un ordenador (200 W de consumo), un monitor (50 W), un router (10 W) y una impresora (10 W).
Queremos instalar un SAI que proteja toda esa instalación y vamos a una tienda donde nos enseñan un modelo de 300 VA por 78 € y otro de 500 VA por 118 €. Ambos tienen un factor de potencia del 60%.

¿Cuál deberíamos elegir?

Actividad U2.3: Buscador de SAI
Dos de las marcas más conocidas de SAI son APC y Salicru. Ambas ofrecen calculadoras o recomendadores de SAIs en función de las características de consumo que necesitemos.

Busca un SAI de cada marca adecuado para el caso anterior y compara sus características.
¿Cuál elegirías y por qué?

Actividad U2.4: Dispones de un SAI de 300 VA con el que quieres proteger un ordenador que tiene instalada una fuente de alimentación de 250 W. ¿Sería suficiente?

Actividad U2.5: En una instalación local en la que tenemos dos ordenadores, dos monitores, dos teclados inalámbricos y un router ADSL, pretendemos añadir un SAI. ¿Qué dispositivos deberíamos conectar al SAI? Justifica tu respuesta.

Instalación y gestión de un SAI

Independientemente del tipo de SAI que estemos utilizando, la instalación y gestión de todos ellos se lleva a cabo siguiendo un procedimiento similar.

1. En primer lugar, hay que buscar aquella ubicación para el dispositivo que permita un funcionamiento óptimo. Una base estable y una ventilación adecuada, sin objetos encima o alrededor, harán que el SAI rinda mucho mejor.
2. El siguiente paso es la **conexión del SAI**. Estos equipos requieren dos tipos de conexión:
   - **Conexión eléctrica**: para cumplir su función, estos dispositivos tienen que ir conectados por un lado a la red eléctrica y por otro al equipo informático al que van a proteger.
   - **Conexión de datos**: conectar el cable de datos al sistema informático para poder gestionar el SAI, bien por el ordenador local o a través de una red (conexión de comunicaciones). Esta última conexión se suele realizar por alguno de los puertos serie o la interfaz de red. Los SAI permiten varios esquemas de conexión de datos:
     - *Conexión monopuesto local*: un único SAI va conectado a un único equipo local. En estos casos la conexión entre el ordenador y el SAI se realiza a través de los puertos serie: USB o RS-232C.
     - *Conexión de la batería del SAI a una LAN*: la batería del SAI se conecta, a través de un switch, a la red por TCP/IP y se gestiona mediante un servidor de la red o bien de equipos remotos de Internet.

Para mejorar su uso lo mejor es utilizar los drivers del fabricante. Los SAI disponen de diversos avisos sonoros y/o luminosos para llamar la atención acerca de las incidencias que pueden suceder al encenderlos (aviso de batería baja, sobrecarga, etc.).

Además, suelen disponer de un software de gestión que permite monitorizar el estado del SAI y de los equipos conectados, así como configurar las opciones de funcionamiento del SAI, programar las labores de encendido y apagado de los equipos conectados a la red para una mejor eficiencia y ahorro energéticos y el envío de mensajes de alerta e informes al administrador de la red a través de SMS, email, etc.

2.4. Controles de presencia y acceso

El primer punto débil de un sistema informático, hablando en términos de seguridad física, es la puerta de entrada al recinto o edificio. Debemos evitar que personal no autorizado tenga acceso físico a la sala donde se encuentran los ordenadores.

Un intruso podría robar los equipos o los soportes de almacenamiento internos (discos duros, tarjetas de memoria...) o externos (cintas, DVD, unidades de disco externas, etc.). Asimismo podría sabotear los equipos físicos o, lo que puede ser más grave para una empresa, acceder a la información contenida en los equipos.

Control de acceso en los entornos físicos

Medidas de seguridad	Funcionamiento
Sistemas de vigilancia	Personal de vigilancia que se encarga de evitar accesos no autorizados y alarmas y sistemas de detección de intrusos (cámaras, sensores de temperatura o movimiento, etc.) que complementan su trabajo.
Código de seguridad	Los usuarios deben recordar un código numérico o contraseña de seguridad para acceder al recinto o al sistema. La contraseña puede ser individual o común a un grupo de usuarios. Sus inconvenientes son la necesidad de recordar el código y la posibilidad de que un intruso acceda a las contraseñas de acceso.
Acceso mediante dispositivos	El acceso al área restringida o a los sistemas se realiza utilizando un instrumento de seguridad (llave, tarjeta, etc.). El inconveniente de estos sistemas es que el dispositivo de acceso debe custodiarse adecuadamente.
Sistemas biométricos	Estos sistemas se basan en la identificación de ciertos rasgos físicos únicos del sujeto para identificarlo (huella dactilar, reconocimiento facial, escáner del iris, reconocimiento facial, etc.). Sus ventajas son que no es necesario conservar ni recordar nada. Tampoco es necesario cargar con ningún dispositivo. Su principal inconveniente viene de que hay un incremento del coste, tanto económico como computacional, conforme aumenta su sofisticación.

Métodos de control de acceso físico

Los sistemas de control de acceso basan su funcionamiento en tres posibles métodos:

- Algo que sé (una clave).
- Algo que tengo (una tarjeta o dispositivo de acceso).
- Algo que soy (características biométricas).

Los sistemas más seguros emplean combinaciones de estos tres tipos.

Sistemas de control de presencia y acceso

Actividad U2.6 Averigua qué sistemas de control de presencia y de acceso se utilizan en los equipos informáticos de los siguientes centros de trabajo: un banco, un ayuntamiento, un hospital, un supermercado.
Responde a las siguientes cuestiones para cada uno de ellos

- a. ¿Qué tipo de sistema es?

- b. ¿Qué ventajas e inconvenientes tiene?
- c. ¿Cuál es su precio?

Actividad U2.7: Imagina que tienes que instalar un sistema de control de acceso en un centro educativo. ¿Qué tipo de sistema instalarías y por qué?

3. Centros de proceso de datos (CPD)

Las empresas de tamaño mediano o grande cuentan con gran cantidad de equipos informáticos y necesitan servidores y otros dispositivos que realicen el control de todo el parque informático y de comunicaciones.

Los servidores son los equipos informáticos que se encargan de gestionar los recursos de una red. Son los encargados de almacenar y gestionar los datos, de controlar el acceso a la red, de gestionar los recursos compartidos, etc. Por ello, su seguridad física es vital para el buen funcionamiento de la red.

Estos sistemas, que centralizan bases de datos, servicios de correo electrónico, gestión de usuarios, etc., precisan de unas instalaciones físicas y de unos requerimientos de hardware peculiares y reciben, en su conjunto, el nombre de **centro de proceso de datos (CPD)** o su denominación inglesa, `data center`.

Los sistemas informáticos a esta escala requieren servidores con varios procesadores y unidades de disco, sistemas de comunicaciones avanzados (con varios routers, switches, etc.), equipos de alimentación redundantes, dispositivos para copias de seguridad, etc.

Estos equipos deben trabajar a una temperatura ambiente baja (unos 17-19 ºC) y generan mucho ruido, por lo que deben ser confinados en un espacio físico diferenciado del trabajo con unas condiciones ambientales y de aislamiento acústico y térmico especiales. Además, esta situación de confinamiento permite adoptar respecto de estos equipos unas medidas de seguridad especiales.

Dado su cometido, los CPD deben estar operativos, ininterrumpidamente, las 24 h de todos los días del año, si bien no requieren la presencia de operadores en su interior. Dentro únicamente hay máquinas `– servidores, equipos de comunicaciones, dispositivos de almacenamiento, equipos de climatización, sensores, etc.–` que son controladas desde fuera de la sala, desde dentro del mismo edificio a través de la red local o bien remotamente a través de Internet.

CPD externo

Las pequeñas empresas, que no dispongan de medios económicos ni espacio para tener un CPD propio, pueden utilizar uno ya existente de otra empresa o bien crear uno nuevo entre varias pequeñas empresas y compartirlo. Con ello se consigue tener un CPD a menor precio con prácticamente la misma funcionalidad.

3.1. Características constructivas y de disposición

De todo lo expuesto se deduce que los centros de proceso de datos necesitan cumplir ciertos requisitos constructivos y de disposición de sus distintos elementos (cableado, instalación, aislamientos, etc.) que les permitan llevar a cabo su función con eficacia y seguridad.

A la hora de configurar un CPD habrá que tener en cuenta el tipo de datos que van a manejarse, el número de equipos que va a contener y su tipología. Por ello, cada empresa, en función de su volumen y su actividad, dimensionará el CPD de acuerdo a sus necesidades.

Por tanto, hay que diferenciar los supuestos de que el CPD ocupe un edificio específico del supuesto en que ocupe una parte del edificio en el que se ubican las oficinas de la empresa.

- **Edificio dedicado**: debe encontrarse en una zona lo más segura posible frente a catástrofes naturales (incendios, inundaciones, terremotos, etc.). La zona debe presentar escasa o nula actividad sísmica o, de lo contrario, debe contar con características técnicas preparadas para este tipo de sucesos. Todo el centro de proceso de datos suele rodearse de un encofrado que lo aísla de fenómenos ambientales externos y asegura sus propiedades ignífugas.
- **Ubicación del CPD en una sala dentro de un edificio**: los requerimientos de esta ubicación son los siguientes:
  - Como los CPD se suelen rodear de un encofrado de hormigón, metal o ambos, requieren un reforzamiento importante de la estructura arquitectónica del edificio. La zona donde se ubique el centro debe soportar el peso de este y por eso **no se suelen ubicar en los pisos superiores**. Sin embargo, la ubicación en sótanos debe realizarse teniendo en cuenta el mayor riesgo de humedades e inundaciones para proveer las medidas necesarias para evitarlos.
  - El cofre, por dentro, presenta generalmente falso suelo para el cableado y el sistema de refrigeración, así como falso techo para albergar los sistemas de detección y extinción de incendios y conducciones extra del sistema de refrigeración.
  - Deben tenerse en cuenta los accesos exteriores, salidas de emergencia, cercanía de material inflamable o peligroso, etc.
  - Habrá que asegurarse de que las dimensiones de la sala son las adecuadas, así como de la distribución de la sala en sí, con la presencia de columnas u otros factores que limiten el espacio.
  - Debe estar en una zona libre de inundaciones. En caso de que hubiera cierta probabilidad de humedad dentro de la sala, es necesaria la instalación de equipos especiales para la extracción de la misma.
  - La sala debe contar con sistemas de control de acceso y presencia que garanticen la seguridad de la información y equipos.

3.2. Sistemas de seguridad del CPD

Además de contar con unas características constructivas y de ubicación especiales, la sala o edificio dedicado a CPD debe contar con medidas de seguridad adecuadas frente a cualquier tipo de riesgos.

Sistemas contra incendios

El CPD debe disponer de medidas para su protección frente a incendios (detectores, extintores, mangueras, etc.). En salas informáticas y CPD el material debe ser ignífugo en la medida de lo posible.

El material de extinción de incendios debe ser adecuado a los equipos existentes; se estima que los sistemas más adecuados son los que **utilizan el agua como agente extintor y el nitrógeno como agente impulsor (sistemas de agua nebulizada)**, frente a los agentes extintores gaseosos.

> Además de ser más respetuosos con el medio ambiente, la extinción de incendios mediante agua nebulizada es inocua para los equipos protegidos y únicamente elimina el oxígeno en la zona de contacto directo con la llama, por lo que no supone un riesgo para el personal que se encuentre en la sala.

Sistemas eléctricos

En primer lugar, las instalaciones eléctricas deben ser adecuadas a la carga estimada que van a soportar, teniendo en cuenta cierta previsión de futuro para posibles nuevas exigencias.

Pero una instalación muy completa genera mucho cableado; por ello, el diseño de las **canalizaciones** es vital para, por un lado, aislar adecuadamente los cables y, por otro, que estos no ocasionen un problema en sí mismos al estar visibles y poder ocasionar caídas u otro accidente.

La **canalización, tanto vertical como horizontal**, debe realizarse a través de falsos techos y falsos suelos, que no hagan visibles los cables.

Además, los servidores van provistos de fuentes de alimentación redundadas para evitar que un fallo en una fuente de alimentación deje al servicio sin energía. Por ello, es básico que los CPD cuenten con dos acometidas de potencia diferentes en cada rack.

3.3. Climatización

Dadas las especiales características de los equipos existentes en un CPD y su sensibilidad a las condiciones climáticas (temperatura y humedad), estos centros deben contar con unos sistemas de climatización que garanticen que dichas condiciones sean las óptimas.

La climatización de un CPD no consiste en la mera instalación de equipos de aire acondicionado. Dado que se trata de una sala cerrada y llena de ordenadores y equipos que producen calor, hay que pensar en algún sistema que elimine todo este calor, inyecte aire libre de partículas y mantenga también unas condiciones óptimas de temperatura (17-19 ºC) y humedad, recomendándose una humedad relativa del 45% (±5%). Para ello, hay que cuantificar y estimar la carga térmica de la sala con el fin de dimensionar bien el sistema de refrigeración.

Existen varias formas de inyectar aire dentro de la sala formando lo que se llaman `pasillos fríos`. De la misma forma, las salidas de aire caliente de los equipos se deben disponer de forma que se puedan direccionar hacia un mismo sitio con el fin de ser recogido por extractores de aire para su enfriamiento y filtrado. La zona donde se mueve todo este aire cálido se denomina `pasillos calientes`.

> **Gasto energético de la climatización**
>
> Más de la mitad del consumo de energía de un CPD procede de los sistemas de refrigeración, la iluminación y otros equipos auxiliares, por lo que la elección del sistema de climatización es algo muy importante, así como la óptima configuración del mismo (una excesiva refrigeración supondría un gasto innecesario y además perjudicaría a los equipos).

3.4. Datos

Un centro de proceso de datos debe contar con redes y equipos robustos, los cuales deben poder soportar sistemas de comunicación de alta velocidad y altas prestaciones capaces de atender al tráfico de **redes SAN** (`Storage Area Networks`), **NAS** (`Network Attached Storage`), granjas de distintos tipos de servidores, **servidores blade** y otros dispositivos diversos.

Los cables de datos serán tanto de tipo Ethernet como de fibra óptica y la primera medida de aislamiento es mantenerlos convenientemente separados de los cables eléctricos para evitar interferencias electromagnéticas que afecten a su eficacia.

En segundo término, al igual que los cables eléctricos, los cables de datos deben quedar ocultos por falsos techos y suelos, pero a la vez deben ser fácilmente accesibles para los técnicos y dejar espacio suficiente para su manipulación y sustitución. Las canalizaciones deben estar diseñadas de forma que los técnicos no tengan opciones a la hora de llevar el cableado de un punto a otro, sino que el camino esté claramente definido.

3.5. Centros de respaldo

Por muchas medidas que se adopten, siempre puede ocurrir algún suceso imprevisto y desastroso que lo destruya absolutamente todo (terremoto, ataque terrorista, etc.). Esto hace, que, de forma adicional a todas las medidas expuestas, muchas empresas mantengan o contraten centros o salas de respaldo (en inglés **DRS**, `Disaster Recovery Sites`), que son

réplicas, más o menos exactas, del CPD principal, diseñadas para que, en caso de fallo de este, puedan tomar el control del sistema, evitando la pérdida de datos.

La primera medida a la hora de diseñar uno de estos centros es la separación
física. Se estima que la distancia óptima se encuentra en torno a 20-40 km, ya que tiene en cuenta los condicionantes de seguridad y las limitaciones impuestas por las líneas de comunicación existentes entre ambas.

En cuanto al diseño del centro de respaldo y a los equipos con que debe contar, hay que tener en cuenta que los costes son un factor fundamental en la seguridad. Así, a la hora de plantear un centro de respaldo hay que tener siempre en mente durante cuánto tiempo es asumible que los sistemas de la organización estén parados en caso de desastre y cuántos recursos estamos dispuestos a invertir para minimizar ese tiempo de parada.

Cold site o sala fría	CPD **externo a la organización** con toda la infraestructura necesaria en cuanto a climatización, potencia eléctrica, etc., para poner en marcha un CPD semejante al nuestro. En caso de contingencia, habría que trasladar allí los servidores y reinstalar todo el sistema a partir de copias de seguridad, por lo que la **puesta en funcionamiento es de más de una semana**, si bien es la solución más barata.
Hot site o sala caliente	CPD con comunicaciones, sistemas y software **análogo al principal** (aunque puede estar dimensionado a la mitad de capacidad de cálculo y memoria para ahorrar). En caso de contingencia, solo hay que restaurar los datos al último momento disponible en los backups, por lo que la **puesta en funcionamiento es inferior a un día**, pero su coste de mantenimiento es mayor, puesto que cualquier modificación que se haga en el principal debe realizarse también en el centro de respaldo.
Mutual backup	Se llega a un acuerdo con otra organización para ejercer de centro de backup mutuo entre sí. En este sentido, cada organización reserva un espacio de su CPD para los servidores de respaldo de la otra organización. Estos pueden estar apagados (con lo que **la solución se aproxima a la de la sala fría**) o bien estar encendidos funcionando al modo de una sala caliente.
Mirror site o centro espejo	Evolución de la sala caliente en la que los **datos son replicados en tiempo real** de un CPD a otro, por lo que el paso de un CPD a otro es bastante rápido al no tener que realizarse restauración de datos.
Configuraciones activo-activo	Las configuraciones anteriores son de tipo **activo-pasivo**. Para organizaciones que **no pueden permitirse un solo momento de parada se utilizan configuraciones de tipo activo-activo** entre CPD en las que los sistemas están configurados en clústeres geográficos repartidos en ambos CPD. Los usuarios trabajan indistintamente y de forma transparente con los sistemas de uno u otro en todo momento y, en caso de caída total de un CPD, el servicio no se ve afectado debido a que el otro puede funcionar de forma autónoma.

3.6. Clasificación de los CPD por su disponibilidad

Podemos clasificar los data center, gracias a los estándares TIA-942 que incluyen información sobre los grados de disponibilidad (TIER).

Los Tiers se basan en información desarrollada por el Uptime Institute, un consorcio dedicado a promover las mejores prácticas para la planificación y gestión de centros de datos.

Para cada uno de los Tiers que existen se detallan las recomendaciones para la infraestructura de seguridad, eléctrica y mecánica y telecomunicaciones. Cuando mayor Tier disponemos, mayor grado de disponibilidad.

Tier	% disponibilidad	% de indisponibilidad	Tiempo de indisponibilidad al año
Tier I	99.671 %	0.329 %	28.82 horas
Tier II	99.741 %	0.251 %	22.68 horas
Tier III	99.982 %	0.018 %	1.57 horas
Tier IV	99.995 %	0.005 %	26.28 minutos

Sistemas de control de presencia y acceso

Actividad U2.8 Relaciona cada elemento con el tipo de seguridad con el que está relacionado

Elemento	Seguridad Física / Lógica (F / L)	Seguridad Activa / Pasiva (A/P)
Cámaras de vigilancia		
Control de acceso biométrico		
Detectores de incendio		
Contraseña de acceso		
SAI		
Firewall en Ubuntu		
Sistema de detección de intrusos		
Sistema de extinción de incendios		
Ventiladores de un equipo		

Actividad U2.9: Busca información sobre las configuraciones de los TIER de los CPD e indica, de las siguientes configuraciones, cuáles están en un CPD según su clasificación por TIERs.

Configuraciones	TIER I	TIER II	TIER III	TIER IV
Suelo técnico				
Componentes redundantes				
Tiempo de implementación				
Múltiples líneas de corriente				

Google Data Centers

En el sitio web Google Centros de Datos puedes encontrar información y material gráfico sobre los data centers de Google.

- Google Data Center Security
- Google Data Center 360° Tour
- Google Data Center Security

Y como añadido os dejo un artículo y un vídeo del CPD mas grande de España, el de Interxion en Madrid.

- Así es un CPD por dentro y por fuera

Resumen del U1.2 Seguridad Física