UT 3: Seguridad Física y Ambiental

2ºSMR – Seguridad Informática

Ubicación y Protección Física

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

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".

La seguridad física está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

- **Desastres naturales**, **incendios accidentales tormentas e inundaciones.**
- **Amenazas ocasionadas por el hombre.**
- **Disturbios, sabotajes internos y externos deliberados**.

Ubicación y Protección Física

Para establecer la seguridad de un servidor o equipo debemos definir donde se va a instalar.

Los **planes de seguridad física** se basan en proteger el hardware de los posibles desastres naturales como incendios, inundaciones, robos, sobrecarga eléctrica, etc.

Cada sistema informático es único, no es lo mismo un CPD de una organización grande que de una empresa pequeña.

El objetivo de la instalación de un CPD es:

- Ahorrar en costes de protección y mantenimiento. No necesita duplicar vigilancia, refrigeración, etc.
- Optimizar las comunicaciones entre servidores. Evitan utilizar cables largos….
- Aprovechar mejor los recursos humanos del departamento de informática. No hay q desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc

Ubicación y Protección Física

Factores para elegir la ubicación de un CPD

- **Edificio**: Se deben evaluar aspectos como:
  - ✓ Espacio del que se dispone
  - ✓ Acceso de equipos y de personal
  - ✓ Características de las instalaciones de suministro eléctrico
  - ✓ Acondicionamiento térmico
  - ✓ Altura y anchura de los espacios
  - ✓ Si tienen columnas
  - ✓ Como es el suelo
  - ✓ Como es la iluminación, etc.

- **Tratamiento acústico**
  - ✓ Equipos de aire acondicionado para refrigerar los servidores (bastante ruidoso)
  - ✓ Debemos tener en cuenta que el ruido y las vibraciones debe estar amortiguados.

Ubicación y Protección Física

Factores para elegir la ubicación de un CPD

- **Seguridad física del edificio**
  - ✓ Sistema contra incendios
  - ✓ Protección contra inundaciones
  - ✓ Y otros peligros naturales que afectan a la instalación.

- **Suministro eléctrico propio del CPD**
  - ✓ Debe tener unas condiciones especiales ya que no puede estar sujeto a fluctuaciones o picos de la red eléctrica.
  - ✓ **Conviene contrastar dos empresas distintas por si hay fallos**. El suministro eléctrico del CPD deberá estar separado del que alimenta al resto del edificio o empresa

- **Otros factores que influyen en la localización son:**
  - ✓ Condiciones ambientales que rodean al CPD como: frio, calor, inundaciones, incendios, terremotos
  - ✓ La zona donde debe situarse el CPD debe ser tranquila pero no un sitio desolado
  - ✓ Zona donde no exista mucho vandalismo, sabotaje o terrorismo.
  - ✓ Los servicios de energía eléctrica y comunicaciones (antenas, líneas telefónicas...) han de tenerse en cuenta al poner un CPD

Control de Acceso

Dependiendo del tipo de instalación y de la inversión económica que se realice se puede disponer de distintos sistemas de seguridad como:

- **Servicio de vigilancia**, donde el acceso será controlado por el personal de seguridad, por lo general suele utilizarse en el control de acceso al edificio.
- **Detectores de metales y escáneres**
- Utilización de **sistemas biométricos** basados en la identificación de características únicas de cada persona.(ver documento anexo)
- **Protección electrónica** basada en el uso de sensores conectados a centrales de alarma.

Control de Acceso

Servicio de vigilancia encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y salida del personal a los distintos sectores de la empresa.

Control de Acceso

Sistemas Biométricos 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.

- **Huella Digital** Basado en el principio de que no existen dos huellas dactilares iguales. Método sumamente confiable, y uno de los más empleados por la relación calidad/precio.
- **Biometría vascular** El formato de las venas es capturado a través del principio de la Transmitancia en la imagen, un proceso de diferencia de absorción de haces de luz del espectro infrarrojo

- **Verificación de Voz** La dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.). Sistema 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 aceptado.

Control de Acceso

- **Verificación de Patrones Oculares** Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos.

- **Verificación Automática de firmas (VAF)** Mientras es posible para un falsificador producir una buena copia visual, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo, la firma genuina con exactitud. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo.

Control de Acceso

Comparación 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

Protección Electrónica

Detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas.

Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

- **Barreras Infrarrojas y de Microondas** Transmiten y reciben haces de luces infrarrojas y de microondas respectivamente. Estas barreras están compuestas por un transmisor y un receptor, cuando el haz es interrumpido, se activa el sistema de alarma. Son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire …
- **Detector Ultrasónico U**tiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma.

Protección Electrónica

- **Detector de aberturas** Se trata de contactos magnéticos externos o embutidos que cuando se abren, activan la alarma.

- **Circuitos Cerrados de Televisión (CCTV)** Permiten el control de todo lo que sucede en planta/s según lo captado por las cámaras estratégicamente colocadas.

Condiciones Ambientales

Las condiciones ambientales deben ser tenidas en cuenta:

Incendios Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. Reducir el riesgo de incendio:

- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.
- Deben instalarse extintores manuales y/o automáticos.

Condiciones Ambientales

- **Se recomiendan sistemas contra incendios, y se debe utilizar**:
  - **Un sistema de detección precoz de incendios** que realice análisis continuos del aire observando cambios en la composición del aire para que detecte el incendio antes de que se produzca el fuego y activa un sistema de desplazamiento de oxígeno.
  - **El sistema de desplazamiento de oxígeno**, reduce la concentración de oxigeno extinguiendo el fuego de modo que no se utiliza agua. Existen otros sistemas más complejos como es el uso de pasillos fríos y calientes y refrigeración líquida utilizados en grandes CPDs

Condiciones Ambientales

Sistemas de Climatización CPD no suelen tener ventanas, los equipos del CPD desprenden mucho calor y hay que utilizar un sistema de refrigeración.

Es recomendable que el centro se encuentre a una temperatura de 22ºC.

Para mantener las condiciones adecuadas en el interior en cuanto a temperatura y humedad se debe situar los rack o servidores a una altura adecuada para una buena circulación del aire, por ello se recomienda la utilización de equipos de climatización.

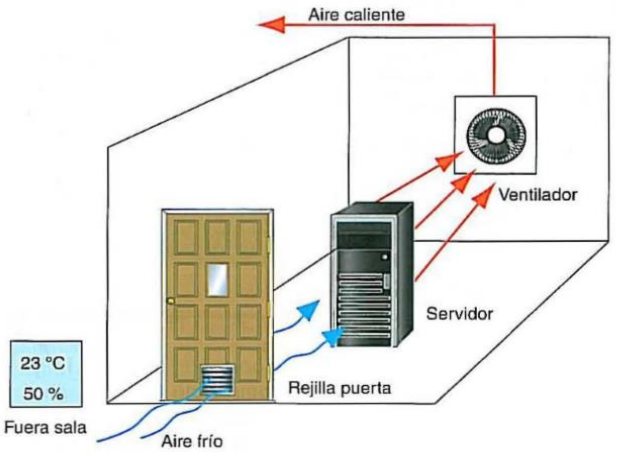


Fig. 2.5. *Sistema de climatización con ventilador.*

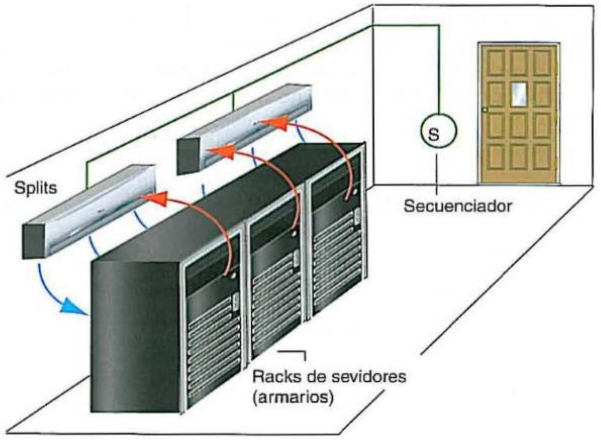


Fig. 2.6. *Sistema de climatización con Splits.*

Condiciones Ambientales

Inundaciones Invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en CPD.

Terremotos Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

Plan Recuperación Caso Desastre

A pesar de tanta protección se debe pensar en la posibilidad de que ocurra alguna catástrofe en un CPD y quede inservible.

Debería existir un segundo CPD se le llama centro de respaldo y ofrece el mismo servicio que el centro principal (CP), separado del centro principal.

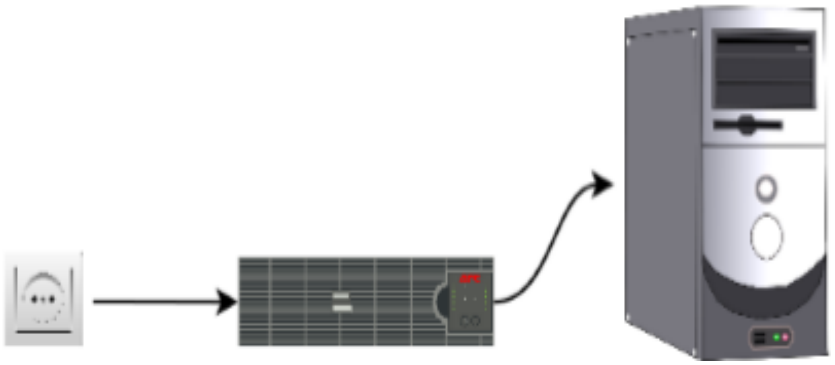
Dentro de los planes de contingencia debemos tener en cuenta la realización de sistemas redundantes como por ejemplo los RAID.

Sistemas Alimentación Ininterrumpida (SAI)

Nos permiten proteger los equipos frente a los picos o caídas de tensión, permite disponer de mayor estabilidad a los cambios de suministro eléctrico y de una fuente de alimentación auxiliar cuando se produce un corte de luz.

Funciones de un SAI:

- Alimentación de ordenadores: Se pueden conectar uno o varios equipos a un SAI
- Tiempo extra de trabajo: Permite seguir trabajando con el ordenador de 18 a 270 minutos cuando se produce un corte
- Alimentación de otros equipos
- Regulador de voltaje: Evita picos de tensión



Sistemas Alimentación Ininterrumpida (SAI)

Tipos de SAI:

- **Stand-by Power system**: Es un SAI en estado de espera y activa la alimentación baterías automáticamente cuando detecta un fallo de suministro eléctrico.

- **On-line**: Alimenta equipos de modo continuo aunque no exista problemas en el suministro eléctrico y al mismo tiempo recarga las baterías. Este sistema tiene la ventaja, que ofrece una tensión de alimentación constante ya que filtra los picos de la señal.

- **In-line**: Su uso más común es la protección de dispositivos en hogares con tensiones anómalas, pequeños comercios o empresas, en entornos de trabajo donde se requiera una protección silenciosa de calidad.