**Seguridad: Tema 3**

1. Principios de la seguridad física

La seguridad física consiste en aplicar barreras físicas y control de acceso. Así como la prevención y contramedidas ante amenazas que pongan en peligro los recursos que gestionan la información confidencial ya sean provocadas por el hombre o la naturaleza. Las principales amenazas son:

* Ocasionadas por el hombre (robos, destrucción de información o equipos) asociadas con la acción de una persona que busca dañar el sistema
* Desastres naturales, cortes del suministro eléctrico o incendios accidentales.
* Disturbios, sabotajes internos y externos deliberados. Asociados a ataques en grupo

**Control de acceso**

* Identificar a los usuarios y permitir o denegar el acceso a recursos o áreas según su identidad
* El servicio de vigilancia es el encargado de controlar el acceso al edificio
* Usar credenciales de identificación para controlar la entrada y salida por los sectores de la empresa
* Disponer de un rack bajo llave
  + Un rack es un armario destinado a alojar equipos informáticos
  + Medidas estandarizadas (ancho de 19 pulgadas, alto y fondo variables)
  + Útiles cuando el espacio es escaso y hay que alojar muchos dispositivos

**Sistemas biométricos**

La biometría es la tecnología que mide de forma electrónica los rasgos físicos de una persona para su identificación. Para ello se comparan estos rasgos con los almacenados en una base de datos. Sus beneficios son

* Elimina la necesidad de tarjetas o contraseñas.
* Los costes a largo plazo son inferiores ya que solo hay que mantener el sistema por lo que se reduce el coste de administración.
* Las características biométricas son intransferibles

**Protección electrónica**

La protección electrónica permite detectar robos, intrusos o incendios mediante sensores conectados a centrales de alarmas. Pueden ser:

* Barreras infrarrojas y de microondas.
* Detector ultrasónico
* Circuitos cerrados de televisión (CCTV). Cámaras de seguridad

**Condiciones ambientales**

Ciertos lugares tienen peligro de desastres naturales y la probabilidad que ocurran está documentada. Estos factores se deben tener en cuenta al construir un edificio:

* Terremotos
* Inundaciones
* Incendios
* Sistemas de aire acondicionado

1. Centro de procesado de datos (CPD)

El data center (o CPD) es la ubicación donde se encuentran los dispositivos informáticos que procesan información. También se puede considerar si existen folios, carpetas con información.

Centralizando se consigue:

* Ahorrar en costes de protección y mantenimiento (no se duplica la vigilancia, refrigeración, etc…)
* Optimizar las comunicaciones entre servidores (al estar cerca no hacen falta cables largos, ni dispositivos intermediarios)
* Aprovechar mejor los recursos humanos del departamento de informática (no se tiene que desplazar de sala en sala)

**Requisitos de un CPD**

Los CPDs se crean para garantizar la continuidad y disponibilidad del servicio. Los requisitos generales son:

* Disponibilidad y monitorización 24/7
* Fiabilidad infalible (5 nueves): 99,999% de disponibilidad. Puede fallar una hora al año.
* Seguridad, redundancia y diversificación.
* Control ambiental/prevención de incendios.
* Acceso a Internet y conectividad a redes de área extensa (WAN) para conectividad a Internet.

**Plan de recuperación y equipamiento del CPD**

Es importante elaborar un plan de recuperación en caso de caída en los servicios del CPD. Este plan debe ser actualizado cuando se realizan cambios en el CPD. El plan debe incluir

* Hardware: modelos de los dispositivos instalados y de los que podemos utilizar como reemplazo y como se configuran
* Software: SO y aplicaciones instaladas con su respectiva versión y opciones de configuración
* Datos: Los sistemas de almacenamiento que utiliza y como se respaldan los datos (copias de seguridad)

**Ubicación y protección del CPD**

* Elegir una zona con baja probabilidad de accidente natural
* Evitar proximidad a ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.…
* Evitar edificios vecinos con actividades peligrosas: gases inflamables, explosivos, etc.…
* Situarse en las primeras plantas de un edificio
  + Planta baja expuesta a sabotajes externos
  + Plantas subterráneas pueden estar afectadas por inundaciones
  + Las plantas superiores tienen riesgo de accidente aéreo o incendio en plantas inferiores.
* Se recomienda que el edificio tenga dos accesos por calles diferentes
* Evitar señalizar la ubicación del CPD
* Los pasillos que llevan al CPD deben ser anchos
* El acceso a la sala debe estar muy controlado
* Utilizar pintura plástica ya que es más fácil de limpiar y evita el polvo
* Utilizar falso suelo y falso techo para favorecer el cableado y ventilación
* Altura elevada para que permita el falso techo y el falso suelo y poder acumular equipos de manera vertical
* Recubrir la sala con hormigón para evitar intrusos
* Detección de humo y sistema automático de extinción
* Mobiliario hecho con materiales ignífugos.

**Aislamiento del CPD**

Las máquinas del CPD utilizan circuitos electrónicos por lo que hay que protegerlas de:

* Temperatura: los equipos generan mucho calor el cual hay que controlar
* Humedad: un porcentaje de humedad alto puede dañar los equipos. Utilizar deshumidificadores.
* Interferencias electromagnéticas: Alejar el CPD de generadores de electricidad
* Ruido: Los ventiladores generan mucho ruido por lo que hay que aislar acústicamente el CPD

**Ventilación**

* Los CPD no tienen ventanas. La ventilación que se consigue no compensa el riesgo de intrusiones o la propia lluvia
* La temperatura ideal es de 22 grados. Hay que usar equipos de climatización
* Utilizar pasillos calientes y pasillos fríos colocando de forma estratégica los equipos. Hacer que todo el calor salga por el mismo sitio para que sea extraído por un ventilador y el aire frío se introduce por el falso suelo.
* Todo el cableado debe ir por los pasillos fríos.

**Suministro eléctrico y comunicaciones**

* El CPD no está aislado, necesita servicios del exterior como suministro eléctrico y comunicaciones
* Contratar dos líneas de suministro con empresas distintas por si falla una
* Separar el suministro eléctrico del CPD del resto de la empresa.
* Para sistemas críticos, utilizar un generador eléctrico alimentado por combustible
* Para las comunicaciones utilizar dos suministros que utilicen tecnologías diferentes

**Control de acceso**

* El acceso al CPD debe estar muy restringido.
* No se pueden tolerar los robos o intrusiones.
* Utilizar sistemas de identificación como contraseñas, tarjetas o biometría. Incluso un equipo de vigilancia o cámaras y sensores

1. Centro de respaldo

El centro de respaldo es un segundo CPD que ofrece los mismos servicios que un CPD en caso de fallo. Si el coste es muy elevado se puede limitar a los servicios principales. Deben estar lo más alejados posible el uno del otro.

Normalmente el CR está en stand-by, funcionará en caso de que se detenga el CPD, cuando este cambio suceda los usuarios no deberán notar el cambio. La configuración de los servicios y la información deberá ser la misma en ambos.

El proceso de conmutación (cambio) entre CPD y CR debe estar documentado detalladamente y es recomendable probar este cambio una vez al año a través de simulacros.

Los equipos del CPD y CR forman el centro de producción de la empresa, aunque pueden existir más servidores por la empresa.

Antes de introducir un cambio en el CPD o CR debe ser probado con antelación, se prueba en un entorno llamado maqueta de preproducción.

1. SAI/UPS

El SAI (sistema de alimentación ininterrumpida) es un dispositivo físico que proporciona energía eléctrica tras un corte en el suministro gracias a unas baterías. Además, puede filtrar y estabilizar la corriente

50% de los problemas están relacionados con un fallo eléctrico y un 40% de estos fallos supone la pérdida de información. 90% de las averías de HW son producidos por un corte de más de 4 milisegundos.

Lo más importante es saber cuántos vatios consumen los equipos y cuánto tiempo necesitan de protección.

La corriente original se llama tensión sucia y cuando sale del SAI es tensión limpia

Los problemas más comunes que resuelve el SAI son: Corte del suministro, bajada de tensión puntual, picos de tensión, bajada de tensión sostenida, subida de tensión sostenida, ruido eléctrico, variación de frecuencia, transitorios, micropicos, distorsión armónica

Un SAI puede tener tres niveles de protección

* Básica (nivel 3): para cortes de suministro puntuales
* Media (nivel 5): para alteraciones en el suministro, destinado a oficinas
* Alta (nivel 9): protección máxima

La autonomía es el tiempo medio (en minutos) que el SAI puede alimentar la carga

**Unidades de medida del SAI**

* Se utilizan los Voltiamperio (voltaje x amperio)
* W = VA \* 0,75
* VApc = VA \* 1,6

**Tipos de SAI**

* SAI offline o stand-by: Solo suministra energía cuando se produce una anomalía en el suministro, apropiados para pequeñas cargas (uso doméstico). El tiempo de conmutación (transferencia) debe ser menor a 4ms.
* SAI online: actúan constantemente, además estabilizan la corriente.

**Monitorización**

Los SAI suelen tener un panel luminoso en el frontal que indican su estado actual. Es recomendable conectarlo al ordenador para disponer de un Software con toda la información del uso del SAI. Se muestra:

* Tipo de evento
* Fecha y hora
* Descripción del evento

**Triggers**

El SW también permite configurar comandos para responder a un corte del suministro, usualmente para parar de forma controlada los equipos. Las opciones principales son:

* Cuando hacerlo: en un momento concreto o cuando la batería esta baja
* Qué hacer: suspender o apagar el sistema:
* Qué comando ejecutar antes de apagarlo: para apagar otras máquinas conectadas al SAI

Además, se pueden configurar avisos a los administradores

**Mantenimiento**

Los SAI utilizan una configuración modular (muchas baterías pequeñas en lugar de una grande. De este modo se pueden reemplazar las baterías de manera sencilla y se consigue la escalabilidad (comprar un bastidor con gran capacidad y se va llenando según su necesidad)

Las baterías se desgastan con el tiempo, pero el SW nos puede ayudar a través de:

* Test que comprueban su degradación para saber cuándo hay que cambiarlas
* Operaciones automáticas de descarga que alargan la vida de las baterías.

Se puede cambiar las baterías en un SAI stand-by en cualquier momento, pero en un SAI online hay que desconectar los equipos.

1. Estrategias de almacenamiento

Lo más importante para una empresa son sus datos. El HW, SW y recursos humanos son reemplazables, pero los datos son únicos e irremplazables. Es importante garantiza su integridad y disponibilidad

**RAID**

El sistema RAID consiste en crear un único volumen a través de varios discos con el fin de conseguir redundancia (tolerancia a fallos) o una mayor velocidad. El SO interpreta el sistema RAID como un único disco lógico.

Para poder hacer uso del sistema RAID es necesario un controlador, la mayoría de placas bases lo integran a través de un Software, y para empresas existen tarjetas de expansión RAID

Existen varios tipos de RAID

* Raid 0 (streaming): La información se distribuye en varios discos, incrementando la velocidad de transferencia. El volumen de espacio es igual a la suma de ambos discos. Sin embargo, si falla un disco se pierde toda la información
* Raid 1 (espejo): la información se escribe en ambos discos por igual. La capacidad de los discos se reduce a la mitad. Pensado para la seguridad, si falla uno de los discos el ordenador seguirá funcionando con el otro disco.
* Raid 5: La información se distribuye a través de los discos y uno va guardando la información necesaria para recuperar las otras partes en caso de fallo (se va alternando). Requiere un mínimo de tres discos. Garantiza la seguridad, pero se pierde parte del espacio de almacenamiento.

**Seguridad en medios de almacenamiento on-line**

El modelo arquitectónico indica la forma en la que los discos se conectan a los servidores (o a la red). Existen tres modelos arquitectónicos básicos.

* DAS (Direct Attached Storage): Los discos se conectan directamente con el servidor. Es el método más barato, el cuello de botella que se pueda producir dependerá del servidor. Su mayor inconveniente es que si el servidor se cae no se podrá acceder a la información.
* NAS (Network Attached Storage): los discos se comparten directamente con la red. La tecnología NAS es barata. EL problema es que la comunicación se realiza a través de la red por lo que se puede colapsar.
* SAN (Storage Area Network): Los discos son accedidos por los servidores a través de otra red, por lo que, si el servidor se cae, se pueden seguir accediendo. En el modelo SAN existen dos redes, la LAN habitual de los clientes y una de acceso al almacenamiento, la cual debe ser de alta velocidad. De este modo se evita el congestionamiento de la red

El sistema SAN funciona por bloques de información, tiene que existir un cliente que interprete dicha información

**Copias de seguridad**

El backup es una copia de los datos originales que se realiza en caso de recuperación ante una pérdida, permite guardar la información y configuración de los equipos. A cada backup se le asocian unos parámetros:

* Ficheros, directorios o discos de origen que se pretende proteger
* Lugar de destino
* Tipo de backup (completo, diferencial, incremental)
* Programación automática del backup

Desventajas de un backup

* Si el backup tiene virus, la restauración también los tendrá
* Si el backup ya tiene los datos perdidos, la restauración no solucionará el problema

Según el lugar de destino, el backup puede ser:

* Local: El origen y el destino del backup están en el mismo ordenador. Son sensibles a amenazas físicas
* Remota: El destino es un lugar distinto al equipo de origen. Es importante asegurar el acceso a la información en el equipo de destino.

Información del backup

* Copias de seguridad de ficheros
* Copias imagen o de volúmenes
* Copias de equipos completos

El formato en el que se envía la copia de seguridad puede ser:

* Reproduciendo la estructura original del sistema de ficheros
* En un solo paquete, fichero único. El cual contiene metadatos para reproducir la estructura original.

**Tipos de copia de seguridad**

* Normal: copia todos los ficheros seleccionados
* Incremental: copia todos los archivos modificados con respecto a la última copia. Es necesario realizar una copia de seguridad normal como base, donde luego se aplicarán todos los cambios
* Diferencial: copia todos los archivos que se han modificado con respecto a la copia normal. Es necesario realizar una copia normal donde se van aplicando las copias diferenciales.