TEMA 2

Seguridad Física

1.- INTRODUCCIÓN

Un experto es aquel que sabe cada vez más sobre menos cosas, hasta que sabe absolutamente todo sobre nada.. es la persona que evita los errores pequeños mientras sigue su avance inexorable hacia la gran falacia" Definición de Webwer - Corolario de Weinberger (Leyes de Murphy)

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. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Chema Alonso, es un experto en seguridad y uno de los fundadores de Informática64, una empresa afincada en Móstoles en el año 2000 cuya especialidad es la seguridad informática, ya sean auditorías, formación o consultoría. Suele decir, Chema Alonso, que "La seguridad de una empresa es tan fuerte como el punto donde menos está segura. SPOF, Single Point of Failure, en español se podría traducir como único punto de fallo.", Con esto, quiere decir que hay que tener asegurados en la empresa todos los elementos de la misma.

Si se trata de asegurar físicamente los ordenadores, servidores o armarios de comunicaciones, tendremos que tener en cuenta dónde están y quién tiene acceso a ellos. Además de analizar cuán importante es alguno, (o todos), de nuestros equipos o servidores, y tener previsto cualquier fallo que pudiera afectarle. Desde que se va la luz, hasta un terremoto, pasando por un incendio, inundación, robo… Todos estos SPOF es lo que llamamos entorno físico.

1.- INTRODUCCIÓN

DEFINICIÓN 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"(1). Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

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

1. Desastres naturales: incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre: Disturbios, sabotajes internos y externos deliberados o no.

Es muy importante recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

1. Robo
2. Fraude.
3. Sabotaje Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

2.2.- EQUIPOS

2.2.1.- ENTORNO FÍSICO

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.
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 °C. 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.

2.2.2.- INSTALACIONES

A) ELECTRICA

Elementos de la red eléctrica	Ejemplos de medidas de seguridad
Red eléctrica externa.	Inaccesibilidad al cableado externo. Protección y cubrimiento del cableado.
Red eléctrica interna.	Cumple la UNE –EN. **Potencia suficiente.**
Personas.	Tomas de tierra.

Seguridad de materiales eléctricos	
Recursos frente a fallos en el suministro de energía eléctrica	**Solución de seguridad**
Grupo electrógeno.	Genera corriente eléctrica independientemente de la corriente eléctrica.
Sistemas de alimentación ininterrumpida (SAI).	Protección frente a variaciones puntuales en el suministro de energía, como picos de intensidad que podrían dañar el sistema y proporciona corriente durante un espacio corto de tiempo a los equipos.
Luces de emergencia.	Iluminan el edificio para poder abandonar el edificio y/o acceder a servidores para apagarlos con normalidad y/o solucionar el problema que causó la avería.

P = I x V

Potencia: Consumo (W)
Voltaje: 230v
Intensidad: Consumo (máx)por unidad de tiempo (A) Amperios

Consumos eléctricos habituales

PC (reposo-pleno rendimiento)

- CPU 3w-65w
- grafica 5w-100 a 250
- ram 5w
- hd 10
- fuente 10w

Media
250 w

Monitor 0,5w-20w

Portátil: 4w-180-365W

Media 200w

Monofásica: 1 corriente
Trifásica: 3 corrientes (empresas)

Tabla de Potencias normalizadas en función de la instalación eléctrica

Instalación Monofásica	Instalación Trifásica
1.15 kW	3.464 kW
2.3 kW	6.928 kW
3.45 kW	10.392 kW
4.6 kW	13.856 kW
5.75 kW	17.321 kW
6.9 kW	20.785 kW
8.05 kW	24.249 kW
9.2 kW	27.713 kW
10.35 kW	31.177 kW
11.5 kW	34.641 kW
14.49 kW	43.648 kW

EJERCICIO

Teniendo en cuenta que en los aparatos se expresa su consumo en kw/h.

Hallar la potencia a contratar y el consumo anual en una pequeña empresa que cuenta con:

- 2 Despachos con
  - 1 Luz (60 w)
  - 2 ordenadores (250 w)
  - 1 estufa (800 w)

- 1 Sala de reuniones
  - 1 Luz (100 w)
  - 1 ordenadores (300 w)
  - 1 A/A (1800 w)
  - 1 Proyector (w)

- 1 Aseo
  - 1 Luz (40w)

- 1 Recepción
  - 1 Luz (60 w)
  - 1 ordenadores (250 w)
  - 1 estufa (800 w)
  - 1 router (10w)

UTILIZAR EL RAZONAMIENTO Y LOS DATOS REALES (SI LOS TENGO PARA LOS CÁLCULOS)

SIEMPRE SE AÑADE ENTRE 5%-20% POR SEGURIDAD

EJERCICIO RESUELTO

Iván ha comprobado la instalación eléctrica en las inmediaciones del lugar donde se va a instalar la **"TSCI"** (Tele Sala de Consulta en Internet)". Tienen un contrato de 25 Amperios. Quiere calcular cuántos amperios más van a suponer los cinco equipos añadidos en la "TSCI" (Tele Sala de Consulta en Internet).

Si son cinco equipos y cada uno de ellos, estando a máximo rendimiento, necesita 200 Vatios para la CPU y 20 Vatios para la pantalla. (Pleno rendimiento quiere decir, encendidos, grabando un disco en la grabadora y con la pantalla encendida.)

¿Cuál es la intensidad que consumen los cinco equipos funcionando a la vez?

Si Potencia = Voltaje*Intensidad y el voltaje de acometida de baja tensión es de 230 Voltios.

Si P=V*I, entonces I=P/V, luego para calcular la intensidad, divido la potencia de cada uno de los equipos entre el voltaje, 230 Voltios, y multiplico por cinco equipos.

Con lo que obtengo el resultado de los amperios que consumirían los equipos a pleno rendimiento.

Intensidad = Potencia / Voltaje = (200 + 20) Vatios * 5 equipos / 230 Voltios
= 4,78 Amperios.

B) RED

- Acceso físico protegido
- Cables correctos y bien conservados.
- Tener cuenta facilidad mantenimiento

C) INCENDIOS

- Prevención: Detectores, orden y limpieza.
- Protección: salidas emergencias, extintores(tipos)..

- EJERCICIO: Buscar los sistemas antiincendios mas usados y porque

D) CONTROL DE ACCESOS

Métodos de control de acceso físico

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

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

Los sistemas más seguros emplean combinaciones de estos tres tipos.

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.

2.3.- El CPD

Las empresas colocan los equipos de usuario cerca del usuario (un ordenador sobre su mesa, un portátil que se lleva a casa); pero los servidores están todos juntos en una misma sala. Esa sala tiene varios nombres: CPD (centro de proceso de datos), centro de cálculo, DataCenter, sala fría, «pecera», etc.

Centralizando se consigue: ahorrar en costes de protección y mantenimiento, optimizar las comunicaciones entre servidores y aprovechar mejor los recursos humanos del departamento de informática.

Todas las empresas deben tener documentado **un plan de recuperación ante desastres,** donde se describa con el máximo detalle qué hacer ante una caída de cualquiera de los servicios que presta el CPD. El plan debe incluir:

•**Hardware.** Qué modelos de máquinas tenemos instalados, qué modelos alternativos podemos utilizar y cómo se instalarán.

•**Software.** Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración.

•**Datos.** Qué sistemas de almacenamiento utilizamos, con qué configuración y cómo se hace el respaldo de datos.

2.3.1.- Factores para elegir la ubicación

- Edificio: espacios, accesos de equipos y personal, conductos eléctricos, suelos, columnas, techos,...
- Trat. acústico ruidos y vibraciones
- Seg. Física: contraincendios, inundaciones
- Suministro Eléctrico: doble, generador,..servidores doble fuente alim
- Ambientales y de servicios: lugar

Construcción antisísmica.	Probabilidad de terremoto.	Por ejemplo si se trata de una zona con alto riesgo de terremotos, la construcción tendrá que ser sobre pilares o antisísmica.
Aislamiento térmico.	Altas y/o bajas temperaturas.	Los muros y las ventanas exteriores estarán aislados térmicamente del exterior, así las condiciones de temperatura exterior no afectarán al interior del edificio, o al menos mitigarán su efecto.
Paredes.	Polvo y fuego.	En el interior las paredes tendrán tratamiento ignífugo y anti polvo.
Suelos.	Peso de los equipos de comunicación. Inundaciones.	El suelo tendrá una alta capacidad de carga, lo que quiere decir que podrá soportar el peso de los armarios de comunicación que se almacenen en el CPD. Y además si instalamos dobles suelos añadiremos protección frente a inundaciones y electrocuciones.

HACER EJEMPLO

Donde Ubicar

- Elegiremos un edificio en una zona con baja probabilidad de accidentes naturales.
- Evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a actividades potencialmente peligrosas: gases inflamables, explosivos, etc.
- Preferentemente seleccionaremos las primeras plantas del edificio. Se recomienda que el edificio tenga dos accesos y por calles diferentes.
- Es recomendable evitar señalizar la ubicación del CPD para dificultar su localización a posibles atacantes.
- Los pasillos que llevan hasta el CPD deben ser anchos porque algunos equipos son bastante voluminosos.
- El acceso a la sala debe estar muy controlado. Los servidores solo interesan al personal del CPD.
- En las paredes se deberá utilizar pintura plástica.
- En la sala se utilizará falso suelo y falso techo porque facilita la distribución del cableado y la ventilación.
- La altura de la sala será elevada tanto para permitir el despliegue de falso suelo y falso techo como para acumular muchos equipos en vertical.
- En empresas de alta seguridad, la sala del CPD se recubre con un cofre de hormigón para protegerla de intrusiones desde el exterior.
- Instalaremos equipos de detección de humos y sistemas automáticos de extinción de incendios.
- El mobiliario de la sala debe utilizar materiales ignífugos.

2.3.2 .- Control de acceso al CPD

El acceso a esta sala de máquinas debe estar especialmente controlado. No podemos consentir que alguien se lleve ninguna máquina o algún componente de ella (discos duros, cintas de backup) ni dejarle dentro intentando tener acceso desde las consolas de los servidores.

Las identificaciones habituales (contraseñas, tarjetas de acceso) se complementan con medidas más seguras, como la biometría. En instalaciones importantes, el CPD puede tener su propio **equipo de vigilantes** de seguridad. En la sala se suele instalar también una **red de sensores de presencia y cámaras de vídeo** para detectar visitas inesperadas.

DISPOSITIVOS DE AUTENTICACIÓN

- **(TENGO) Tarjetas: Es el sistema más extendido en Data Center.**
  - **Tarjetas de contacto**
  - **Las tarjetas de proximidad** **ROBO, PERDIDA,…**

- **(SE) Teclados: Pin** **OLVIDO,CONFUSIÓN, ANOTADO Y VISTO…**

- **(SOY) Sistemas biométricos e identificación personal.**

  Rasgos fisiológicos: huellas dactilares, geometría de la mano/dedo, iris, ADN, etc.
  Rasgos del comportamiento: voz, firma, modo de teclear, modo de andar, etc.

EJERCICIOS:

Bajar la aplicación BIOPASSWORD y comprobar su utilidad
Buscar Ibutton, Touch memories,..

2.3.3.- CLIMATIZACIÓN

NORMATIVAS: potencias, garaje 7 veces hora

Aislamiento

Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:

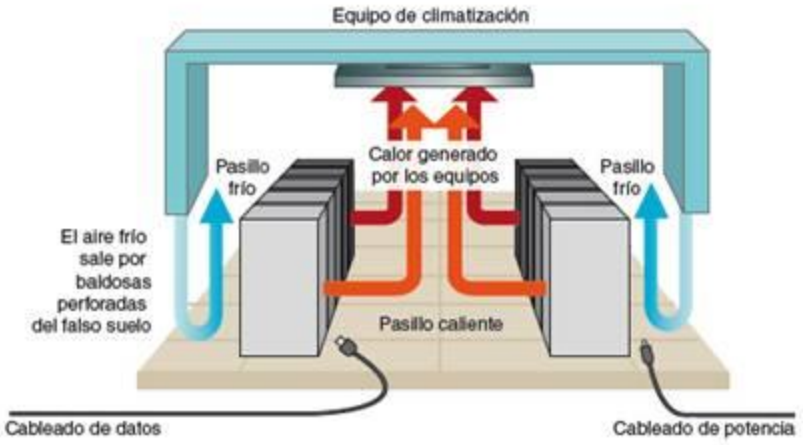
- **Temperatura.** Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.
- **Humedad.** Para evitarlo utilizaremos deshumidificadores.
- **Interferencias electromagnéticas.** El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad.
- **Ruido.** Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico.

Ventilación

Los CPD no suelen tener ventanas. La ventilación que conseguiríamos con ellas sería mínima y el riesgo de intrusiones desde el exterior (o simplemente la lluvia) no es admisible en una instalación de tanta importancia.

La temperatura recomendable estaría alrededor de los 22 grados. Para conseguirlo instalaremos equipos de climatización. Se suelen instalar por duplicado, para estar cubiertos ante el fallo de uno de los equipos.

En los CPD grandes se adopta la configuración de **pasillos fríos y calientes.**



2.3.4.- Redundancia.

Siguiendo con el refranero español: **dos mejor que una**. Si se trata de servidores en los cuales la información es crítica, qué mejor que tener la información duplicada por si uno de los equipos se estropea, poder tener otro que entre en servicio inmediatamente. Los elementos redundantes que tenemos deben de existir de forma ideal son:

•**Un CPD de respaldo**, es un edificio que contenga exactamente lo mismo que el CPD original, es decir, yo tengo dos CPD´s igualitos y, además situados en diferentes localización, como dicen los ingleses "just in case", es decir, si se diera el caso de que uno de ellos no pudiera dar servicio, el otro, que es una réplica de éste, entraría en funcionamiento tan solo en unas horas
•**Diferentes proveedores de internet**, ya que si en alguno de ellos se produce una avería, se podría utilizar el otro.
•**El control de la temperatura, la humedad y el filtrado del aire**, también tiene que tener salvaguarda, para que en caso de fallar el sistema principal, entre en funcionamiento el sistema secundario.
•.**En cuanto a la acometida eléctrica**, también conviene tener más de una compañía proveedora. Si una de ellas falla o se produce un apagón, disponemos de la otra compañía. En algunos lugares, si no existen dos compañías, deben tener un generador independiente que suministre electricidad al CPD.

2.3.5.- Centro de respaldo

A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible (inundación, terremoto, sabotaje). La continuidad de la empresa no puede depender de un punto único de fallo; si disponemos de presupuesto suficiente, debemos instalar un segundo CPD.

Este segundo CPD, también llamado **centro de respaldo (CR),** ofrece los mismos servicios del **centro principal (CP).** Aunque, si la inversión en hardware resulta demasiado elevada, puede limitarse a los servicios principales, o a los mismos servicios pero con menos prestaciones. Por supuesto, debe estar físicamente alejado del CP; cuantos más kilómetros entre ambos, mejor.

En condiciones normales, el CR está parado esperando que la empresa pueda necesitar detener el CP y activar el CR como nuevo CP. Para ello, la información del CP también está en el CR. Esto incluye la configuración de los servicios; pero, sobre todo, los datos que han sido modificados antes de la conmutación de centros.

No es suficiente con recuperar la última copia de seguridad del CP: debemos habilitar mecanismos especiales de réplica, en especial para las bases de datos. Pero esto necesita de muy buenas comunicaciones entre el CP y el CR.

Todo el procedimiento de conmutación debe estar documentado con el máximo detalle, así como la posterior recuperación del CP, asumiendo los cambios ocurridos mientras estaba inactivo.
Conviene probarlo una vez al año para confirmar que los pasos están bien descritos y el personal está capacitado para ejecutarlos bien.

2.3.5.- Centro de respaldo

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero bajo algunas consideraciones más.

En primer lugar, 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 mínimo 20 y 40 kilómetros del CPD principal.

En segundo lugar, el **equipamiento** electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser *exactamente* igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente.

En tercer lugar, el equipamiento **software debe ser idéntico** al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

Por último, pero no menos importante, 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, que se detalla a continuación.

- Copia síncrona de datos:
- Copia asíncrona de datos

TIPOS:

COLD SITE, HOT SITE, MUTUAL BACKUP, MIRROR,..

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad.

Cuando algo sucede, nos lamentamos de no haber invertido más...

Más vale dedicar recursos a la seguridad que convertirse en una triste estadística".

2.3.6.- SAI/UPS

Un **SAI es un Sistema de Alimentación Ininterrumpida**, son dispositivos que se utilizan para proporcionar protección contra problemas eléctricos y cortes de corriente también son conocidos por sus siglas en Ingles **UPS** (Uninterruptible Power Supply).

El **AVR** (Automatic Voltage Regulator) es un equipo electrónico que se utiliza para regular el voltaje, el funcionamiento básicamente consiste en regular el flujo eléctrico, controlando las subidas y bajadas de tensión (picos) que se dan en la red eléctrica proporcionando una tensión constante en la salida (230V) de esta forma protegemos los equipos conectados al **regulador de voltaje (AVR)**

LA CORRIENTE ALTERNA PUEDE TENER PICOS DE TENSIÓN

Partes de un SAI

- Baterías
- Filtro AVR(Limpiar señal)
- Conversor (alterna a continua 12v)
- Inversor (continua a alterna)
- conmutador (pasar de uno a otro)

2.3.6.- SAI/UPS

La corriente eléctrica es vital en cualquier ordenador. Como no podemos confiar en que nunca va a fallar la empresa con la que hemos contratado el suministro eléctrico, tenemos que pensar en alternativas. En esta misma unidad hemos sugerido contratar un **segundo suministrador** o disponer de un **generador propio** (grupo electrógeno).

Sin abandonar estas soluciones, en un CPD nunca debe faltar un SAI (**sistema de alimentación ininterrumpida**), en inglés UPS (Uninterruptible Power Supply). Un **SAI** es un conjunto de baterías que alimentan una instalación eléctrica (en nuestro caso, equipos informáticos).

FUNCIONAMIENTO

Cuando ocurre un corte de luz, el SAI procede de esta manera:

- Espera **unos minutos** por si el corte ha sido puntual y el suministro se recupera inmediatamente por sí solo.
- Si no es así, ejecuta una **parada ordenada** de los equipos conectados al SAI. Siempre es mejor solicitar una parada al sistema operativo y las aplicaciones que ejecuta que perder la corriente y confiar en que no se genere ninguna inconsistencia

2.3.6.- SAI/UPS

Características SAI

Potencia (real y aparente): equipos expresa watios y SAIS en voltiamperios. si no está expresado en ambos en los equipos

¿Qué capacidad de SAI necesito?

La unidad de "potencia aparente" que encontramos en los Sais es el Voltiamperio (Va) ya sea expresado en unidades (1000 Va) o en unidades de millar, el KiloVoltioampério (KVa), también llamado Kavea (1 KVa = 1000 Va) que es usado para Sais de potencia/capacidad medios-altos. Sin embargo, la mayoría de los aparatos que conectemos al Sai tendrán expresado su consumo en vatios (w), por lo que para poder realizar una estimación correcta del Sai que necesitamos, se incluye en las fichas de cada SAI una equivalencia de los Voltiamperios (Va) en vatios (W).

SI NO NOS PROPORCIONAN LA POTENCIA EN WATIOS SE SEGUIRA LA REGLA DE MULTIPLICAR POR 0,6

Debido a posibles picos de consumo de los aparatos conectados al Sai, se recomienda siempre elegir un SAI con una capacidad de suministro un 20% mayor que el consumo que vamos a proteger. Tan solo necesitamos conocer la suma de los consumos en vatios de cada uno de los aparatos que necesitemos proteger y sumar a ese total un 20%, esa cantidad serán los vatios que nuestro Sai deberá ser capaz de suministrar

2.3.6.- SAI/UPS

EJERCICIO

Un equipo informático domestico está compuesto por un ordenador (230w), un monitor (50w), un router (10w) y una impresora (10w).

Queremos instalar un SAI para proteger la instalación y el software y datos. En la tienda nos ofrecen un modelo de 310 VA por 78€ y otro de 550 VA por 118€.

¿Cuál deberiamos elegir?

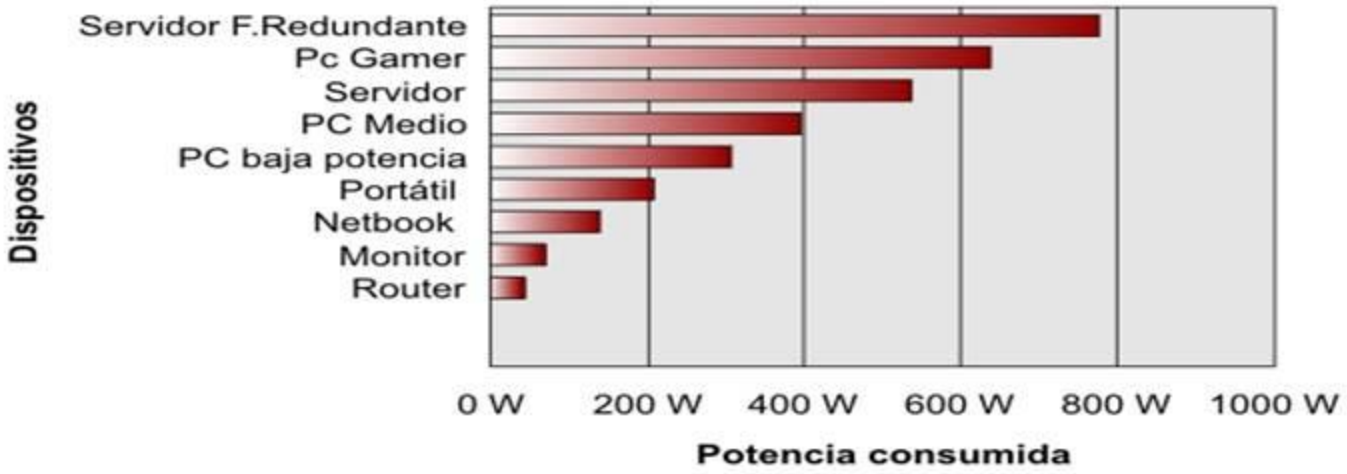
Consumo total sería: 240+50+10+10=300watios

A) SAI 1: 310 x 0,6=186 w NO SERIA SUFICIENTE
B) SAI 2: 550 x 0,6=330 w PODRÍA VALER.....

HAY QUE TENER EN CUENTA QUE LA IMPRESORA NO DEBERIAMOS CONECTARLA. LUEGO SON 290W PODRÍA VALER

HAY QUE TENER EN CUENTA QUE SE DEBE INCLUIR UN 20% MAS POR SEGURIDAD 290W x 1,1= 319w SEGUIRÍA VALIENDO EL DE 550VA

* Consumos aproximados de equipamiento más frecuente



Importante: Podemos observar que no existen impresoras en este cuadro, aún siendo dispositivos muy comunes. La razón es que las impresoras no deben ser nunca conectadas a un SAI, ya que al encenderse o durante su funcionamiento pueden emitir grandes picos de corriente que podrían dañar al SAI.

¿Cuánto tiempo puedo mantener mis equipos encendidos con un SAI?

A este lapso de tiempo es lo que denominamos **"Tiempo de autonomía de un SAI"** y es variable dependiendo del modelo, capacidad de suministro, carga conectada, etc... Encontrarás una estimación de la autonomía de cada modelo en su ficha de producto. En este punto queremos indicarte que una buena práctica cuando existe un apagón eléctrico es aprovechar el tiempo que nos brindan los SAIS para grabar, ordenar y apagar adecuadamente los dispositivos conectados, intenta no "exprimir" al máximo el tiempo de autonomía de tu SAI, ya que si terminas por agotar la energía de las baterías podrías acabar sufriendo también un apagón del SAI.

Tipos

- **SAI en estado de espera (stand-by).** Los equipos informáticos toman corriente del suministro principal, mientras el SAI se limita a vigilar que ese suministro fluya. Cuando ocurre un corte, el SAI activa inmediatamente sus baterías para que los equipos no se vean afectados. A partir de ese momento, el SAI aplica los tiempos de espera señalados en el punto anterior. Cuando vuelve la corriente, desactiva la generación de corriente propia y empieza a cargar las baterías. **(Buenas zonas, instalaciones pequeñas)**
- **SAI en línea (on-line).** Los equipos siempre están tomando corriente de las baterías del SAI. Cuando ocurre un corte, el SAI se limita a aplicar los tiempos de espera. Cuando vuelve la corriente, empieza a cargar las baterías. **(Servidores,…)**

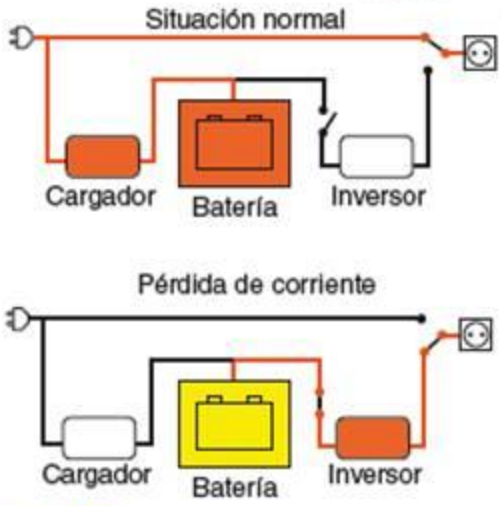


Fig. 3.12. *Esquema de un SAI en stand-by.*

Monitorización (PRÁCTICA)

Pero conviene revisar regularmente el estado del SAI. Estos equipos suelen incorporar unos indicadores luminosos en el frontal: si está cargando o descargando las baterías, porcentaje de batería restante, etc. Sin embargo, es una información puntual y solo disponible si se está delante del equipo. Para mejorar su gestión, los SAI suelen incorporar un **puerto de conexión con un ordenador.** En ese ordenador instalaremos el software adecuado para comunicarse con el SAI y conocer no solo el estado actual, sino todas las veces que ha actuado en el pasado reciente. Por supuesto, ese ordenador debe estar protegido, sea por este SAI o por cualquier otro.

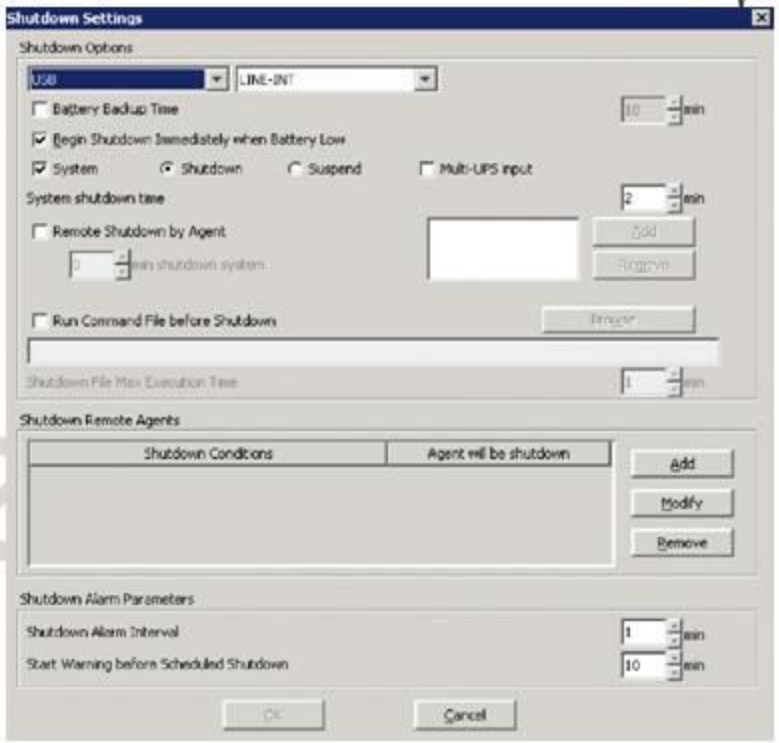
Triggers

El software del SAI, además de la monitorización, incluye la configuración de los **comandos para responder ante un corte de corriente.** En general, la respuesta consistirá en realizar la parada ordenada de los equipos protegidos. En la Figura 3.15 vemos un ejemplo de la interfaz asociada.

Las opciones principales son:

- **Cuándo hacerlo:** en un instante concreto (cuando se alcance Battery Backup Time) o cuando detecte que la carga de la batería está baja.
- **Qué hacer con el sistema:** suspenderlo o apagarlo.
- **Qué comando ejecutar antes de empezar el apagado** (Run Command File Before Shutdown).

Además de la parada, se puede configurar un **aviso por correo** a los administradores del sistema.



Mantenimiento

Las baterías se desgastan con el tiempo y ofrecen cada vez menos rendimiento. El software del SAI nos ayuda en este aspecto, pues permite lanzar test para **comprobar la degradación** de las baterías e incluye operaciones automáticas de **descarga controlada**, que alargan la vida de las baterías.

Los SAI empresariales suelen adoptar una **configuración modular:** no utilizan pocas baterías grandes, sino muchas baterías pequeñas. Con este diseño podemos reemplazar fácilmente una batería sin afectar demasiado a la carga total ofrecida por el equipo, y a la vez conseguimos escalabilidad.

3.8.- Políticas de seguridad.

Para implantar la política de seguridad se tuvo en cuenta los recursos, instalaciones y procesos a los que afectaba, marcando claramente los objetivos y prioridades.

Se identificaron todos los elementos que forman parte de la política, tanto elementos físicos como lógicos. Se analizó y gestionó los posibles riesgos, asignó responsabilidades, se definió qué se puede y qué no se puede hacer si eres un usuario del sistema....

Por otra parte, se identificaron las medidas, normas y procedimientos de seguridad a implantar, y cómo gestionar los incidentes. Para ello, se diseñaun plan de contingencia cumpliendo en todo momento la legislación vigente, y por último, definió las posibles violaciones y las consecuencias derivadas del incumplimiento de las políticas de seguridad.

Otro factor importante es determinar qué personas están implicadas en las Políticas de seguridad y no menos importantes son los documentos que hay que crear, en los cuales debe figurar información similar a la reflejada en este formulario:

En los procedimientos especificar además de lo arriba indicado, estos otros conceptos:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

3.8.- Políticas de seguridad. (EJEMPLO)

Política de seguridad		
Política	**Procedimiento**	**Plan**
Protección del servidor web del instituto contra accesos no autorizados.	Actualización del software del servidor Web.	Revisión diaria de los parches publicados por el fabricante del software. Seguimiento de las noticias sobre fallos de seguridad.
	Revisión de los registros de actividad en el servidor.	Revisión semanal de los "logs" del servidor para detectar situaciones anómalas. Configuración de alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión.

Y ahora vamos a crear una política de seguridad, la tarea se hace más sencilla si tenemos en mente un ejemplo. Imaginemos el servidor web de un instituto. En este servidor web se encuentran alojadas la página web del instituto, de la biblioteca y un gestor de contenidos o intranet

3.8.- Políticas de seguridad.

Primer paso: Lo más recomendable es crear unas guías de cómo realizar cada una de las tareas para aquellas personas que las llevan a cabo. Al mismo tiempo crear otras guías para usuarios con las directrices de lo que se considera un uso aceptable del sistema. Además, hay que instalar el hardware y software necesario para reforzarlas con otras que indiquen cuál es la forma que se espera que los usuarios. Por otra parte, habrán de instalarse y configurarse el hardware o software de seguridad necesario.

Segundo paso: Definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización.

Tercer paso: Debe cumplir con las exigencias del entorno legal.

Cuarto paso: Revisar de forma periódica (seis meses máximo) las políticas de seguridad para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal.

Quinto paso: Aplicación del principio de "Defensa en profundidad": definición e implantación de varios niveles o capas de seguridad.

3.8.- Políticas de seguridad.

Sexto paso: Asignación de los mínimos privilegios. Los servicios, las aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.

Séptimo paso: Configuración robusta ante fallos. Los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.

Octavo paso: Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros, sino que deberían estar adaptadas a las necesidades reales de cada organización. Es importante que se reflejen las características específicas de cada empresa o institución en las políticas, pues los entornos de una a otra pueden ser muy cambiantes.