SEGURIDAD INFORMÁTICA

2º DE SISTEMAS MICROINFORMÁTICOS Y REDES

Noelia Huguet Chacón

TOBALCAIDE

TEMA 3: SEGURIDAD PASIVA

1. Principios de la Seguridad Física
2. Centro de Procesamiento de Datos
3. Centro de respaldo
4. SAI/UPS
5. Estrategias de almacenamiento

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

- La seguridad física consiste en la aplicación de barrera 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:
  - Amenazas ocasionadas por el hombre (robos, destrucción de información o equipos…)
  - Desastres naturales, alteraciones y cortes de suministro eléctrico, incendios accidentales, tormentas e inundaciones.
  - Disturbios, sabotajes internos y externos deliberados.

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

CONTROL DE ACCESO

- El **control de acceso** no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.
- El **Servicio de vigilancia** es el encargado del control de acceso de todas las personas al edificio.
- 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.
- Una solución muy empleada para la seguridad de los sistemas informáticos, es disponer los mismo en un **armario o rack bajo llave**.

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

CONTROL DE ACCESO

- Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante. (19 pulgadas de ancho, alto y fondo son variables)
- Los racks son muy útiles en un centro de procesos de daos, donde el espacio es escaso y necesita alojar un gran número de dispositivos.

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

SISTEMAS BIOMÉTRICOS

- La Biometría es una 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.
- Beneficios de una tecnología biométrica:
  - Pueden eliminar la necesidad de poseer una tarjeta para acceder, y de una contraseña difícil de recordar o que finalmente acaba siendo escrita en un papel visible por cualquier persona.
  - Utilizando un dispositivo biométrico los costes de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada.
  - Las características biométricas de una persona son intransferibles a otra.

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

PROTECCIÓN ELECTRÓNICA

- Se llama así a la detección de robo, intrusión, asalto o incendios mediante la utilización de sensores conectados a centrales de alarmas.
- Pueden ser:
  - Barreras infrarrojas y de microondas.
  - Detector ultrasónico.
  - Circuitos cerrados de televisión (CCTV)

3.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

CONDICIONES AMBIENTALES

- Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran esta documentada.
- La frecuencia y severidad de su ocurrencia deber ser tenidas en cuenta al decidir la construcción de un edificio.
  - Terremotos
  - Inundaciones
  - Incendios
  - Sistema de aire acondicionado

3.2 CENTRO DE PROCESADO DE DATOS (CPD)

- Se denomina procesamiento de datos o **CPD o data center** a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.
- **Centralizando se consigue:**
  - **Ahorrar en costes de protección y mantenimiento**. No necesitan duplicar la vigilancia, la refrigeración, etc.
  - **Optimizar las comunicaciones entre servidores.** Al estar unos cerca de otros no necesitan utilizar cables largos o demasiados elementos intermedios que reducen el rendimiento.
  - **Aprovechar mejor los recursos humanos del departamento de informática.** No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc.

3.2.1 EQUIPAMIENTO DE UN CPD

- Los CPDs se crean para garantizar la continuidad y disponibilidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras.
- Requisitos generales de un CPD:
  - Disponibilidad y monitorización "24x7x365".
  - Fiabilidad infalible (5 nueves): 99,999% de disponibilidad.
  - Seguridad, redundancia y diversificación.
  - Control ambiental/prevención de incendios.
  - Acceso a Internet y conectividad a redes de área extensa (WAN) para conectividad a Internet.

3.2.2 UBICACIÓN DEL CPD

- Tan importante como tomar medidas para proteger los equipos es tener en cuenta qué hacer cuando esas medidas fallan.
- 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.
- Este plan debe ser actualizado cuando se efectúe un cambio en el CPD.

3.2.2 UBICACIÓN DEL CPD

- El plan debe incluir:
  - **Hardware**. Qué modelos de máquinas tenemos instalados (tanto servidores como equipamiento de red), qué modelos alternativos podemos utilizar y cómo se instalarán (conexiones, configuración).
  - **Software**. Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc.).
  - **Datos**. Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y cómo se hace el respaldo de datos (copias de seguridad).

3.2.3 PROTECCIÓN

- La informática es vital para la empresa: si los servidores se paran, la empresa se para.
- El CPD debe estar protegido al máximo:
  - Elegiremos un edificio en una zona con baja probabilidad de accidentes naturales.
  - También 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.
    - La planta baja está expuesta a sabotajes desde el exterior (impacto de vehículos, asaltos, etc.).
    - Las plantas subterráneas serían las primeras afectadas por una inundación.
    - Las plantas superiores están expuestas a un accidente aéreo y, en caso de incendio iniciado en plantas inferiores, es seguro que nos afectará.

3.2.3 PROTECCIÓN

- Se recomienda que el edificio tenga dos accesos y por calles diferentes. Así siempre podremos entrar en caso de que una entrada quede inaccesible (obras, incidente, etc.).
- Es recomendable evitar señalizar la ubicación del CPD para dificultar su localización a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.
- Los pasillos que llevan hasta el CPD deben ser anchos porque algunos equipos son bastante voluminosos. Incluso conviene dotarlo de un muelle de descarga.
- El acceso a la sala debe estar muy controlado. Los servidores solo interesan al personal del CPD.
- En las paredes de la sala se deberá utilizar pintura plástica porque facilita su limpieza y se evita la generación de polvo.

3.2.3 PROTECCIÓN

- En la sala se utilizará falso suelo y falso techo porque facilita la distribución del cableado (para electricidad y comunicaciones) 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, porque el espacio de esta sala es muy valioso.
- 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, como los elementos del techo.
- El mobiliario de la sala debe utilizar materiales ignífugos.

3.2.4 AISLAMIENTO

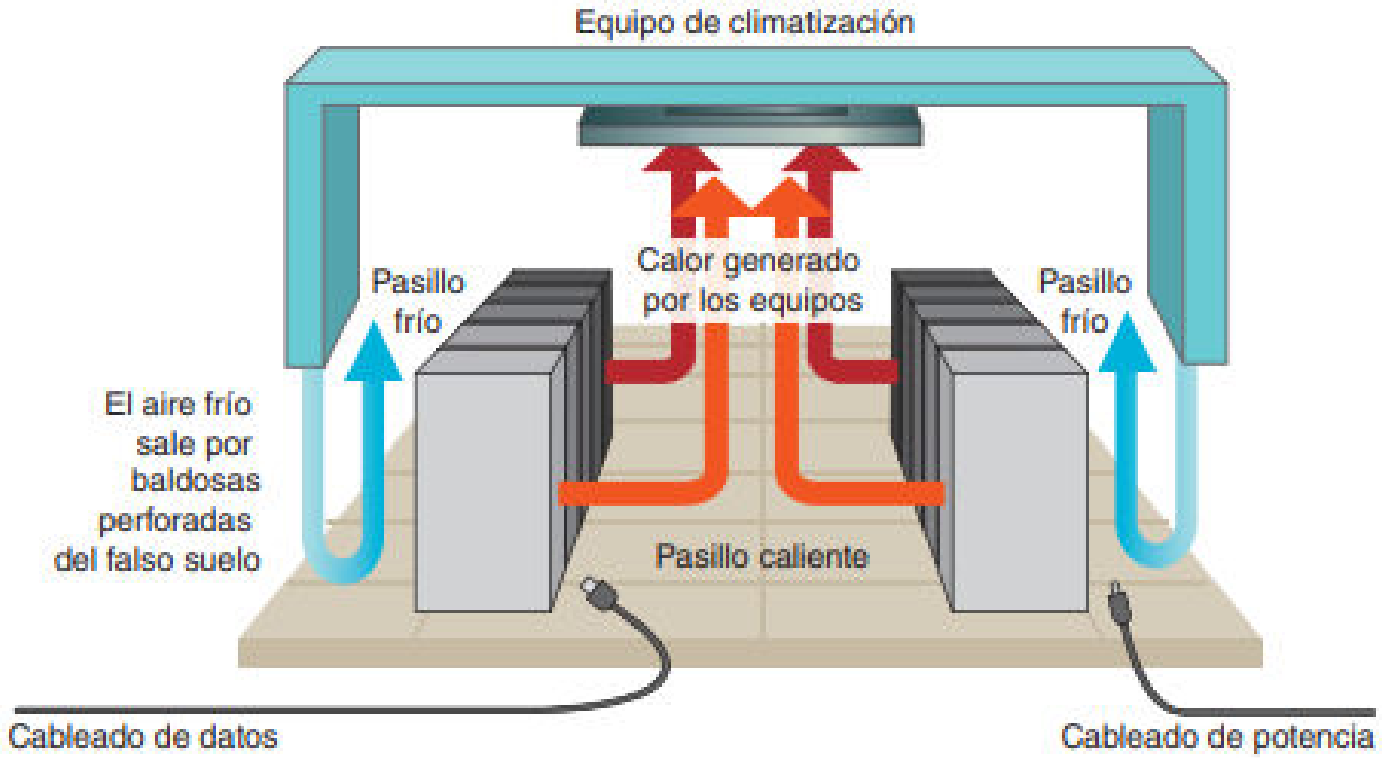
- Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:
  - **Temperatura**. Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.
  - **Humedad**. No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.
  - **Interferencias electromagnéticas**. El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.
  - **Ruido**. Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico para no afectar a los trabajadores de las salas adyacentes.

3.2.4 VENTILACIÓN

- Los CPD no suelen tener ventanas. La ventilación que conseguiríamos con ellas sería mínima para todo el calor que se genera, y el riesgo de intrusiones desde el exterior (o simplemente la lluvia) no es admisible en una instalación de tanta importancia.
- La temperatura recomendable en la sala estaría alrededor de los 22 grados. Las máquinas no lo necesitan, pero hay que pensar que ahí también van a trabajar personas. Para conseguirlo instalaremos equipos de climatización.
- En los CPD grandes se adopta la configuración de pasillos calientes y pasillos fríos. Las filas de equipos se colocan en bloques formando pasillos, de manera que todos los ventiladores que extraen el calor de la máquina (fuente de alimentación, caja de la CPU) apunten hacia el mismo pasillo. En este pasillo se colocan los extractores de calor del equipo de climatización.
- Ese mismo equipo introduce aire frío en los pasillos fríos, generalmente a través del falso suelo utilizando baldosas perforadas.
- Si es posible, todo el cableado de potencia irá en los pasillos fríos (es peligroso sobrecalentarlos) y el cableado de datos en los pasillos calientes.

3.2.4 VENTILACIÓN

- **PASILLOS CALIENTES Y FRÍOS**



3.2.5 SUMINISTRO ELÉCTRICO Y COMUNICACIONES

- Nuestro CPD no está aislado: necesita ciertos servicios del exterior.
- Los principales son la alimentación eléctrica y las comunicaciones.
- En ambos casos conviene contratar con dos empresas distintas, de manera que un fallo en una compañía suministradora no nos impida seguir trabajando.
- El suministro eléctrico del CPD debería estar separado del que alimenta al resto de la empresa para evitar que un problema en cualquier despacho de ese edificio afecte a los servidores, porque están siendo utilizados por empleados de otros edificios, incluso por clientes y proveedores.
- Para los sistemas críticos, en los que la empresa no puede permitirse ninguna interrupción del servicio, deberemos instalar generadores eléctricos alimentados por combustible.
- En cuanto a las comunicaciones, conviene que el segundo suministrador utilice una tecnología diferente al primero.

3.2.6 CONTROL DE ACCESO

- Las máquinas del CPD son vitales para la empresa y solo necesitan ser utilizadas por un reducido grupo de especialistas.
- 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.

3.3 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.

3.3 CENTRO DE RESPALDO

- En condiciones normales, el CR está parado (stand-by) esperando que, en cualquier momento, la empresa pueda necesitar detener el CP y activar el CR como nuevo CP.
- Los usuarios (empleados, clientes, proveedores) no deberían notar el cambio.
- 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 en el último instante, antes de la conmutación de centros.
- Por tanto, 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, que son más complejas que los sistemas de ficheros.
- Pero esto necesita de muy buenas comunicaciones entre el CP y el CR, con lo que la distancia que los separa puede ser un problema.

3.3 CENTRO DE RESPALDO

- Puede que las circunstancias que nos lleven a conmutar el CR al CP sean muy urgentes y no haya tiempo para descubrir cómo se hace: 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.
- Incluso conviene probarlo una vez al año para confirmar que los pasos están bien descritos y el personal está capacitado para ejecutarlos bien.
- Los equipos del CP y el CR constituyen los **centros de producción** de la empresa: están en funcionamiento para dar servicio a los empleados, clientes y proveedores de la misma.
- Pero no son las únicas salas con servidores y equipamiento de red.
- Cualquier cambio en las aplicaciones corporativas o la nueva web de la empresa no puede instalarse directamente en las máquinas de producción, porque un fallo no detectado puede bloquear algunas áreas de la empresa.
- Primero se prueba en un entorno controlado, llamado **maqueta de preproducción**, donde el personal de la empresa aplica el cambio. En esta fase hay un contacto directo con el suministrador del software para resolver inmediatamente cualquier contingencia.

3.4 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 un CPD nunca debe faltar un **SAI** (**sistema de alimentación ininterrumpida**), en inglés UPS (Uninterruptible Power Supply).
- Un **SAI** es un dispositivo físico que, gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

3.4 SAI/UPS

- Como valor añadido, un SAI puede proporcionar mejoras en el suministro eléctrico como filtrado y estabilización de corriente.
- Se estima que aproximadamente un 50% de los problemas ocasionados en los equipos informáticos tiene su causa en un fallo eléctrico y, de estos fallos, en el 40% de los casos se producen pérdidas de información.
- El 90% de los casos de avería en el hardware están producidos por cortes de suministro mayores de 4 milisegundos.
- En caso de corte de la corriente, los equipos conectados al SAI siguen funcionando porque consigue electricidad de las baterías.
- La capacidad de estas baterías es reducida depende del SAI elegido y del consumo de los equipos, aunque el mínimo garantizado suele ser diez minutos.

3.4 SAI/UPS

- Este es el **factor más importante** a la hora de adquirir un SAI: cuántos vatios consumen los equipos que debe proteger y cuánto tiempo necesitamos que los proteja.
- Al igual que ocurría con los equipos de climatización, si el presupuesto lo permite, conviene aplicar redundancia e instalar un doble juego de equipos SAI, para estar cubiertos en caso de que uno fallara.
- Esto es posible porque la mayoría de los servidores vienen con doble fuente de alimentación y conectaríamos una fuente a cada grupo de SAI.
- Además de pérdida de información también se pueden producir daños en la infraestructura, disminución de la productividad laboral y, en general, pérdidas económicas.
- Todo esto debe llevar a estimar convenientemente la instalación de un SAI en el despliegue de un sistema informático.
- La corriente eléctrica original, expuesta a todo tipo de problemas, antes de llegar al SAI se denomina "tensión sucia", frente al suministro de salida del SAI que se denomina "tensión estabilizada".

3.4 SAI/UPS

- Algunos de los problemas más comunes que el SAI vienen a corregir:
  - Corte de energía, apagón o *blackout*
  - Bajada de tensión momentánea, microcortes o *sag*
  - Picos de tensión, alto voltaje momentáneo o *surge*
  - Bajada de tensión sostenida o *undervoltage*
  - Subidas de tensión sostenida o *overvoltage*
  - Ruido eléctrico o *line noise*
  - Variación de frecuencia o *frecuency variation*
  - Transitorios, micropicos o switc*hing transient*
  - Distorsión armónica o *harmonic distortion*

3.4 SAI/UPS

- Los fabricantes suelen definir en sus especificaciones tres grados de protección asociados a tres niveles:
  - **Básica (nivel 3):** si se necesita solucionar un problema de cortes de suministro puntuales en un entorno de oficina.
  - **Media (nivel 5):** en un entorno de oficinas si el problema fuera de alteraciones en el suministro (ya que se requiere algo más que una batería de apoyo).
  - **Alta (nivel 9):** si se necesita protección máxima porque el suministro es muy irregular.

3.4 SAI/UPS

- La **autonomía del un SAI** es el tiempo (medido en minutos) durante el cual el SAI puede alimentar a las cargas que se le conectan a su salida en ausencia de suministro externo.
- Este parámetro depende de la carga: a mayor carga menor será el tiempo que durará el suministro desde las baterías.
- Esta es la razón por la que suele estandarizarse la autonomía como la medida de este tiempo de suministro eléctrico desde la batería a media carga, es decir, cuando el SAI tiene conectada el 50% de la potencia máxima que aguanta.
- Es un parámetro que proporciona el fabricante.

3.4 SAI/UPS

- UNIDADES DE MEDIDA EN EL SAI
  - Los fabricantes suelen utilizar el concepto de potencia aparente, que se miden en VA (voltiamperio), que es el producto de la tensión nominal por la intensidad nominal máximas.
  - Por ejemplo, si un SAI suministra 200 V y 10 A, entonces su potencia aparente será de 2.000 VA o 2 KVA.
  - El vatio (W), es la unidad de potencia eficaz, la realmente consumida. Suele tomarse que la potencia eficaz (W) es la potencia aparente (VA) multiplicada por 0,75.
  - Algunos fabricantes utilizan una unidad superior para incorporar un margen de seguridad adicional que es el VAi (VA informático) o también denominado VApc.
  - La equivalencia es VApc = VA x 1,6.

VA (voltiamperios)= V (voltios) * A (amperios)

W (vatios) = VA (voltiamperios) * 0,75

VApc (VA informático)= VA (voltiamperios) * 1,6

3.4 SAI/UPS

- EJEMPLO:
  - Si un circuito eléctrico consume 1 A de intensidad eléctrica cuando es alimentado con 220 V de tensión, entonces tiene una potencia aparente de 1 x 220 = 220VA.
  - Lo que equivale a 220 * 0,75 = 165 W de potencia eficaz.
  - Si se necesita conectar este circuito a un SAI, tendríamos que elegir este para que suministrara un potencia eficaz igual o superior a 165W.
  - VApc = 165 VA x 1,6 = 264 VApc.
  - Elegiríamos un SAI de 300 VApc o 165 VA o 220 W.

3.4.1 TIPOS

- TIPOS DE SAI
  - SAI offline o standby.
  - SAI online.

3.4.1 TIPOS

- TIPOS DE SAI
  - **SAI offline o standby**
    - El SAI suministra energía procedente de las baterías solo cuando se produce una anomalía en el suministro, por ejemplo, un corte.
    - Aunque habitualmente no acondicionan la señal, hay modelos que llevan incorporados estabilizadores.
    - Son apropiados para pequeñas cargas y entornos de baja exigencia.
    - Su tiempo de conmutación (también llamado tiempo de transferencia) esté por debajo de los 4 milisegundos porque por encima de este valor puede ser peligroso para algunas cargas.

3.4.1 TIPOS

- TIPOS DE SAI
  - **SAI online**
    - Actúan constantemente, no solo cuando hay cortes.
    - Por tanto, las baterías actúan de continuo y cuando se produce un corte se dejan de cargar, pero el suministro de salida no se interrumpe.
    - Estos SAI estabilizan la corriente ya que la energía de salida procede siempre de las baterías y no de la entrada directamente, por lo que solucionan la mayor parte de los problemas.

3.4.2 MONITORIZACIÓN

- Cuando tenemos un SAI confiamos en que está bien y que responderá cuando sea necesaria su intervención.
- 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 (puerto serie o/y un USB).
- 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.

3.4.2 MONITORIZACIÓN

- En la ventana del log de un SAI. Muestra una lista de los eventos que ha registrado:
  - La primera columna señala el **tipo de evento**. Puede ser informativo o una alerta.
  - Las dos siguientes indican la **fecha y hora** en que ocurrió el evento. Es importante para asociarlo a otros sucesos ocurridos: caída de alguna máquina, corte de líneas de comunicaciones, etc.
  - La cuarta es la **descripción del evento**. Hay algunos sencillos, como Agent Start, que indican que ha arrancado el agente (el software que corre en el ordenador). Vemos que minutos antes ha ocurrido un USB Communication with device lost, lo que significa que el ordenador se ha reiniciado.
- Los más graves son los eventos AC power failure, que es un corte de luz. Después ocurre un AC power restored, que indica que se ha recuperado el suministro.
- Observar el tiempo transcurrido entre ambos eventos nos servirá para ajustar la espera del SAI antes de lanzar la parada de equipos (y para reclamar a la compañía eléctrica, por supuesto).

3.4.3 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.
- 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). En este apartado aprovecharemos para apagar las otras máquinas conectadas a este SAI.
- Además de la parada, se puede configurar un aviso por correo a los administradores del sistema.

3.4.4 MANTENIMIENTO

- 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**: el cliente compra un bastidor con capacidad de alojar muchas baterías, y lo va rellenando según aumenta el número de equipos protegidos.

3.4.4 MANTENIMIENTO

- Las baterías se desgastan con el tiempo y ofrecen cada vez menos rendimiento. El software del SAI nos ayuda en este aspecto:
  - Permite lanzar determinados test para comprobar la degradación actual de las baterías. Si no es suficiente para garantizar la parada ordenada de los equipos protegidos, debemos cambiarlas. Para cambiar las baterías acudiremos al personal especializado, porque las baterías utilizan componentes químicos muy peligrosos.
  - Incluye operaciones automáticas de descarga controlada, que alargan la vida de las baterías.
- La operación de cambiar las baterías será relativamente sencilla en un SAI de tipo stand-by porque mientras tanto los equipos seguirán alimentados.
- Pero en un SAI on-line perderemos la alimentación, por lo que es necesario detener los equipos. Este aspecto puede ser crítico en una empresa que no pueda permitirse ninguna parada.

3.5 ESTRATEGIAS DE ALMACENAMIENTO

- Para una empresa, la parte más importante de la informática son los datos: sus **datos**. Porque:
  - El hardware es caro, pero se puede volver a comprar.
  - Un informático muy bueno puede despedirse, pero es posible contratar otro.
  - Si una máquina no arranca porque se ha corrompido el sistema de ficheros, puedes instalar de nuevo el sistema operativo y las aplicaciones desde los CD o DVD originales.
- En todos los casos anteriores se recupera la normalidad en un plazo de tiempo razonable. Sin embargo, los **datos de esa empresa son únicos**: no se pueden comprar, no se pueden contratar, no hay originales. Si se pierden, no los podemos recuperar (por lo menos, ni fácil ni rápidamente).
- Ya que los datos son tan importantes, hay que esforzarse especialmente en mejorar su **integridad y disponibilidad:**
  - Podemos comprar los mejores discos del mercado en calidad y velocidad; aunque nunca debemos olvidar que son máquinas y pueden fallar.
  - Podemos concentrar los discos en unos servidores especializados en almacenamiento.
  - Podemos replicar la información varias veces y repartirla por ciudades distintas.
  - Podemos contratar el servicio de respaldo de datos a otra empresa, conectados por Internet, para no depender de nuestros equipos y personal.

3.5.1 RAID

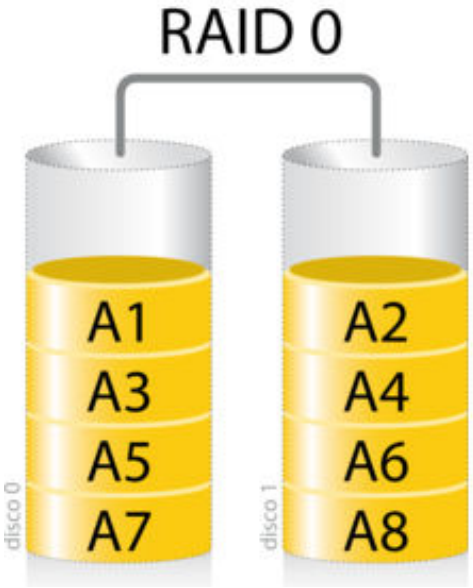
- Los ordenadores pueden conectar varios discos internos porque las placas base suelen traer integrada una controladora de discos para dos o tres conexiones.
- Podemos aprovechar varios discos de un ordenador para:
  - **Crear unidades más grandes.** Dos discos de 500 GB juntos nos pueden dar una unidad de 1 TB. Con tres discos tenemos 1,5 TB, etc. Por ejemplo, si queremos ripear un Blu-ray de 25 GB y solo tenemos discos de 20 GB, necesitamos juntar dos en una unidad de 40 GB. O, si queremos darle al /home 2 TB y solo tenemos discos de 640 GB, podemos juntar tres.
  - **Crear unidades más rápidas**. Si tenemos dos discos de 500 GB y configuramos el sistema para que, en cada fichero, los bloques pares se escriban en un disco y los impares en otro, después podremos hacer lecturas y escrituras en paralelo (en el mejor caso, ahorramos la mitad de tiempo). Con un único disco de 1 TB tenemos la misma capacidad, pero cada lectura o escritura debe esperar que termine la operación anterior. La diferencia es más notable si ponemos tres discos, cuatro, etc.
  - **Crear unidades más fiables.** Si configuramos los dos discos anteriores para que, en cada fichero, los bloques se escriban a la vez en ambos discos, podemos estar tranquilos porque, si falla un disco, los datos estarán a salvo en el otro.

3.5.1 RAID

- RAID (Redundant Array of Independent Disks), **consiste en crear un único volumen con varios discos duros funcionando en conjunto**, y con este conjunto se puede conseguir **redundancia** (tolerancia a fallos) o **mayor velocidad**, haciendo que ese conjunto sea en realidad un tándem.
- Un sistema RAID funciona emplazando los datos en varios discos duros, y permitiendo que las operaciones de entrada y salida (I/O) funcionen de manera balanceada, mejorando el rendimiento.
- O bien los datos se escriben en ambos discos al mismo tiempo, o bien se escribe un dato en uno, y otro dato en otro para repartir el trabajo.
- Los sistemas RAID se presentan en el SO como si fueran un único disco lógico, dado que consisten en un solo volumen.
- Para que un sistema RAID funcione es necesaria la presencia de una controladora RAID, y puede ser o bien por hardware o bien por software.
- A día de hoy, la gran mayoría de PCs de usuario ya cuentan con una controladora RAID por software integrada en la BIOS de la placa base, y de hecho las **controladoras por hardware** tan solo se usan en entornos empresariales a día de hoy.

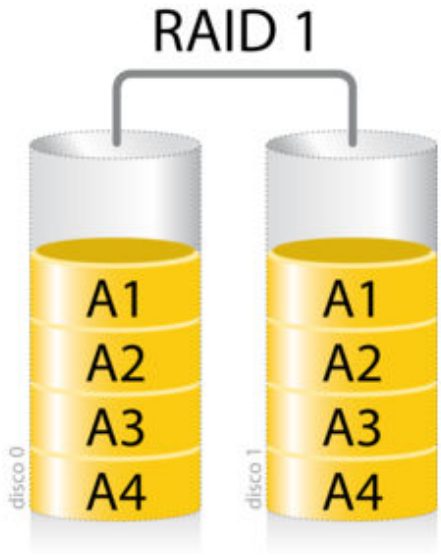
3.5.1 RAID

- **RAID 0** o data striping: conjunto dividido, distribuye los datos equitativamente entre dos o mas discos sin información de paridad que proporcione redundancia, incrementa el rendimiento pero si falla un disco se pierden los datos.
  - El RAID reparte los datos en varios discos duros.
  - No hay redundancia de datos.
  - Se aumenta el rendimiento.
  - Se puede leer o escribir a la vez en varios discos.
  - Se necesita al menos dos discos.
  - Las capacidades de los discos duros se suman y los veremos como si tuviéramos una sola unidad.
  - Pueden tener distintas capacidades, pero se reduce al del menor.
  - Lo ideal es que los dos discos duros sean iguales.



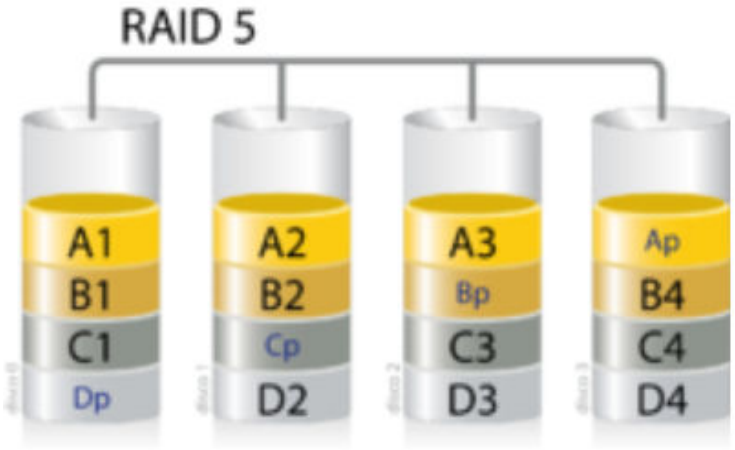
3.5.1 RAID

- **RAID 1** o data mirroring: conjunto espejo, crea una copia exacta de los datos en dos o mas discos, si falla uno de los discos la información no se pierde al estar replicada en otro disco.
  - Se necesita al menos dos discos.
  - Hay redundancia total de datos.
  - Se aumenta la fiabilidad.
  - Las lecturas son en paralelo, las escrituras NO.
  - Los discos empleados pueden ser de distinta capacidad, pero la capacida d total será la capacidad del menor.
- **¿Qué ocurrirá si hay un error en uno de los discos?**
  - El sistema sigue en marcha empleando los otros discos.
  - La recuperación de un disco es transparente al usuario.



3.5.1 RAID

- **RAID 5:** conjunto dividido con paridad distribuida, requiere un mínimo de tres discos, consiste en una división a nivel de bloques distribuyendo la información de paridad entre los discos miembros del conjunto, gracias a la información de paridad si falla un disco la información no se pierde.
  - La información del usuario se graba por bloques y de forma alternativa en todos los discos.
  - Gracias a la información de paridad se puede restablecer la información pérdida. Está distribuida y se almacena en un disco distinto a los que almacenan cada serie de datos.
  - Se aumenta la fiabilidad.
  - Se necesita al menos tres discos.
- **¿Qué ocurrirá si hay un error en uno de los discos?**
  - Se puede recuperar la información en tiempo real, sobre la marcha, sin que el servidor deje de funcionar.



3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

- Un modelo arquitectónico de almacenamiento indica la forma en que los discos que contiene los datos se conectan a los servidores o, con mayor generalidad, a la red para ser servidores a los clientes de la red.
- Básicamente hay tres **modelos arquitectónicos** básicos:
  - **DAS**
  - **NAS**
  - **SAN**

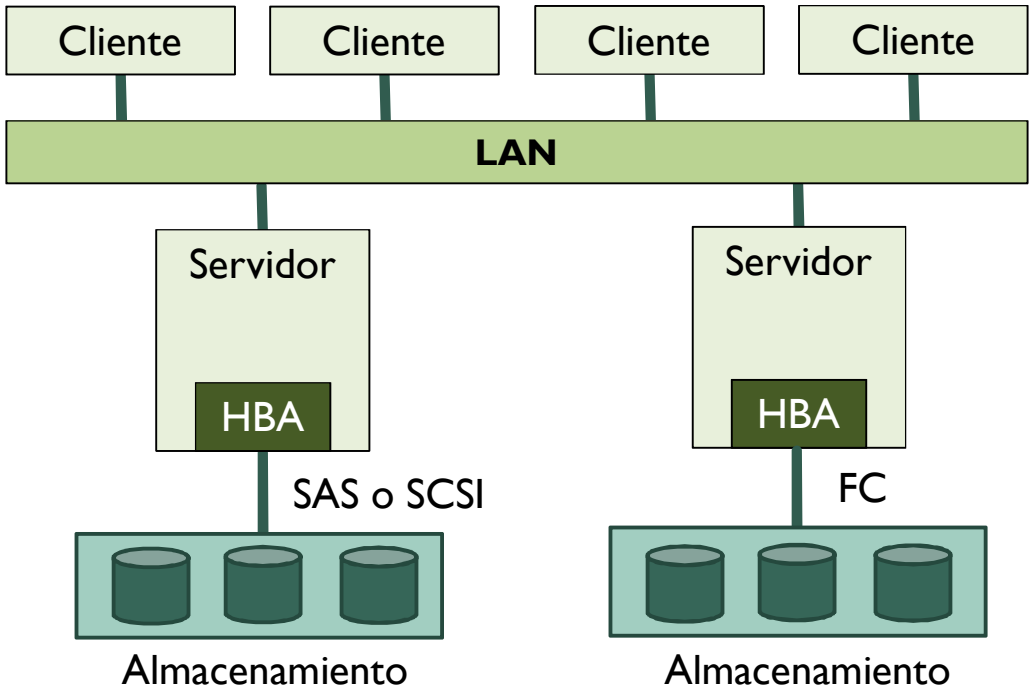
3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

DAS (Direct Attached Storage)

- Es la arquitectura tradicional de conexión de discos en servidores en la que los medios de almacenamiento (discos) se conectan directamente al servidor cuyas aplicaciones y usuarios consumen los datos que residen en estos discos, por tanto la relación entre los discos y el servidor es física.
- Dispositivo conectado directamente al sistema.
- Ejemplo: Disco duro del PC.
- La ventaja del modelos DAS es que es el más barato y el posible cuello de botella de acceso a los discos debe ser controlado por el servidor al que se conectan ya que las peticiones de cualquier cliente se hacen a través de este servidor y nunca directamente a los discos.
- Por el contrario, adolece de un gran inconveniente: si el servidor deja de estar operativo, los datos contenidos en los discos dejan de estar disponibles.

3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

DAS (Direct Attached Storage)



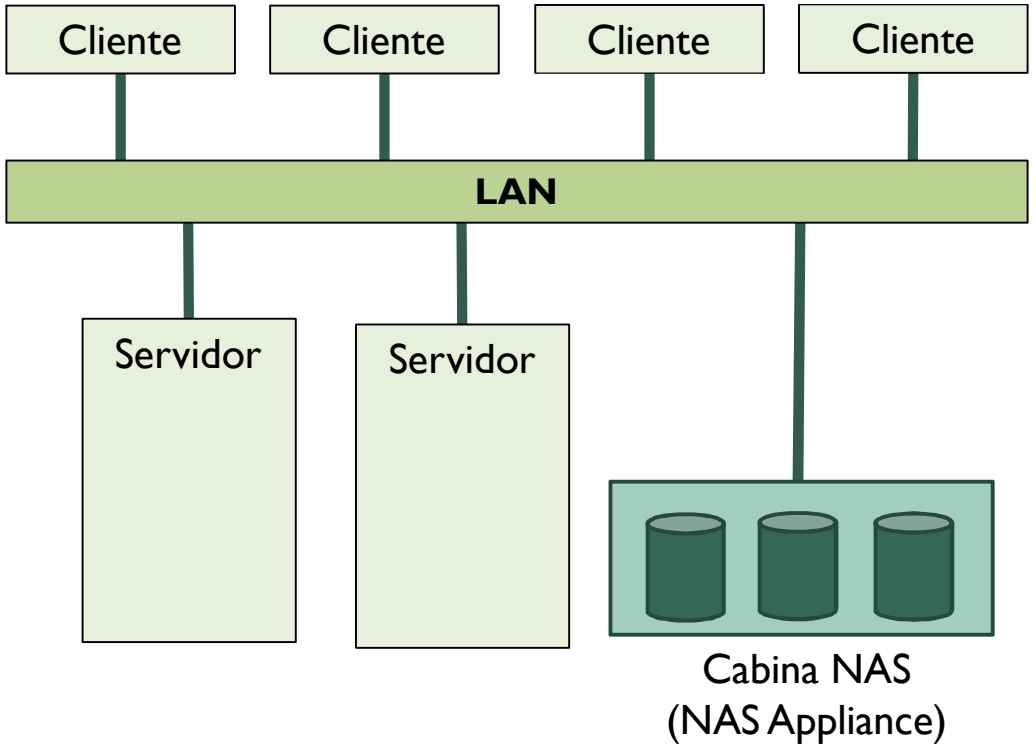
3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

NAS (Network Attached Storage)

- En este modelo, los discos conectados a un servidor son compartidos a la red para que otros clientes de red consuman estos servicios de disco.
- Los discos y los clientes residen en distintos sistemas y se comunican a través de la LAN.
- Ejemplo: carpetas compartidas mediante SMB , FTP o similar.
- La tecnología NAS es barata puesto que los sistemas que alojan los discos no requieren una capacidad de cálculo elevada, basta con que puedan ejecutar ágilmente los servicios de red y los accesos a los discos.
- Muchos de estos sistemas (NAS box) se construyen en torno a un SO del tip GNU/Linux lo que abarata todavía más el coste del producto al ser de libre coste.
- Sin embargo, NAS tiene un inconveniente: como las comunicaciones de los clientes con los discos se hacen a través de una LAN, típicamente Ethernet, se pueden producir situaciones de colapso en la red y, además, este flujo de datos interfiere con el tráfico habitual de los usuarios de la LAN, que pueden notar la congestión si hay un consumo elevado de acceso a disco.

3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

NAS (Network Attached Storage)



3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

SAN (Storage Area Network)

- La configuración de este modelo hace que los discos sean servidos por servidores que alcanzan los discos a través de una red, es decir, los discos no están alojados dentro de ellos por lo que si ellos se paran, los discos pueden seguir estando disponibles.
- La red de acceso a los discos no es la misma LAN que la que utilizan los usuarios de la red por lo que se atenúan los problemas de congestión en la red.
- En el modelo SAN hay dos redes locales: la de acceso al medio de almacenamiento (SAN, red de área de almacenamiento) y la LAN habitual de los cliente de red.
- La red SAN que conecta los servidores a los discos suele ser una red de alta velocidad basada en los estándares FC sobre fibra óptica o iSCSI sobre Gigabit Ethernet.

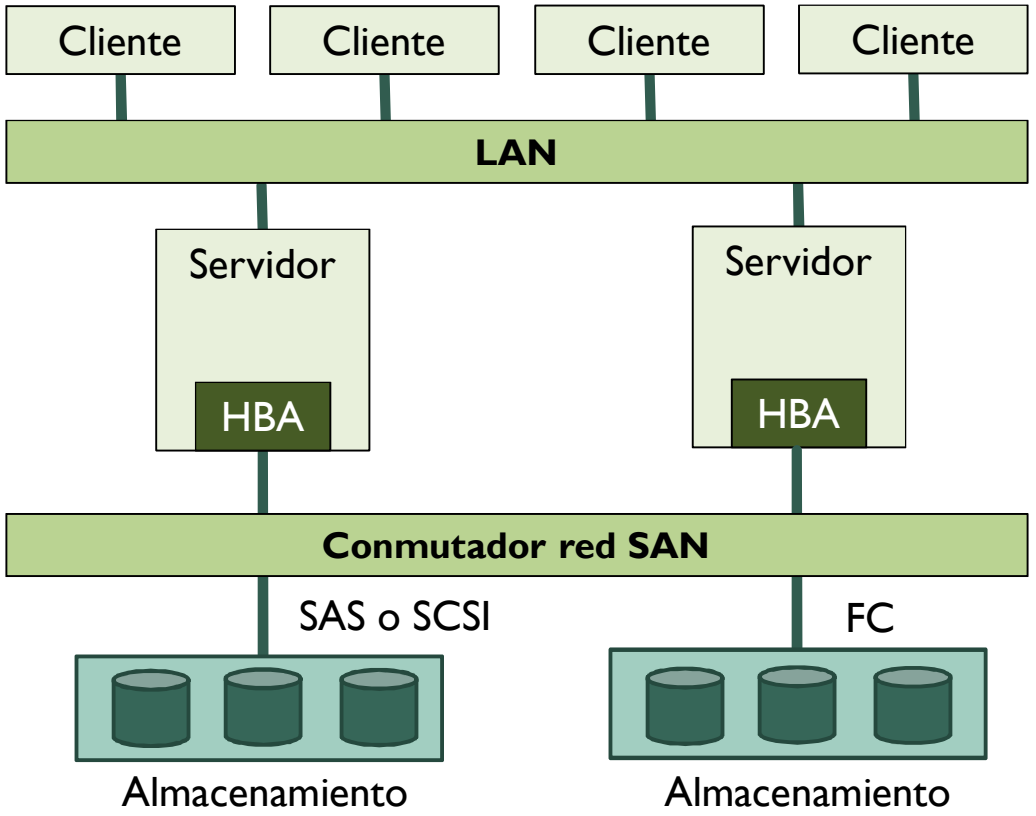
3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

SAN (Storage Area Network)

- Otra característica importante es que los discos son servidos como dispositivos de bloques, que no de ficheros como el caso de DAS y NAS: la unidad de acceso al medio de almacenamiento no es un fichero sino una porción del disco (un bloque).
- Cuando un sistema necesita escribir un fichero en un dispositivo de bloques solicita al sistema SAN una relación de bloques libres para escribir en ellos los datos que componen el fichero.
- Sin embargo, la información de cómo deben unirse los bloques para reconstruir el fichero no reside en la SAN sino que es propio del sistema cliente.
- Por eso el sistema SAN no entiende de ficheros, solo sabe escribir o leer bloques numerados por un identificador unívoco.

3.5.2 SEGURIDAD EN LOS MEDIOS DE ALMACENAMIENTO ONLINE

SAN (Storage Area Network)



3.5.3 COPIAS DE SEGURIDAD

- El **backup** o copia de seguridad es el procedimiento más inútil mientras todo funciona bien, pero el que más se echa de menos en caso de problemas.
- No basta con hacer copias de seguridad de los sistemas, además, hay que comprobar que están bien realizadas y que se hacen las que se deben y no otras.
- **Razones para realizar las copias de seguridad**:
  - Salvaguardar los datos de los usuarios.
  - Salvaguardar las configuraciones de los equipos.
  - La prevención de problemas frente a fallos en el hardware.
  - Asegurar los datos de usuarios frente a borrados o alteraciones indebidas.
  - Poder restituir la información dañada o alterada por virus u otro malware.

3.5.3 COPIAS DE SEGURIDAD

- Hacer un **backup** es sinónimo de salvaguardar información, pero junto con la información salvada se asocian a cada copia de seguridad un conjunto de parámetros que dependen de la utilidad empleada para realizar la copia de seguridad.
- Los más habituales son los siguientes:
  - Ficheros, directorios o discos de origen que se pretenden salvar.
  - Lugar de destino de la información salvada. Se trata del medio de almacenamiento, directorio o fichero en el que se depositará el backup realizado.
  - Tipo de backup: completo, diferencial, incremental…
  - Programación automática del backup. Se trata de especificar un calendario, horario y automatismos relacionados con la ejecución del backup.
  - Otros parámetros, frecuentemente dependientes del fabricante del sistema de backup.

3.5.3 COPIAS DE SEGURIDAD

- **DESVENTAJA**
  - Las copias de seguridad no protegen contra todas las pérdidas de información.
  - Por ejemplo, si el backup realizado en un momento dado contiene virus, la restauración de esta información también los contendrá.
  - En otro caso, si la información salvada ya tiene datos perdidos y el operador de backup no tiene una copia anterior a la pérdida, la restauración tampoco arreglará el problema.
- **Según el lugar de destino de la información en relación al origen:**
  - **LOCALES**
  - **REMOTAS**

3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD

- **LOCAL:**
  - Es el backup en el que el origen y el destino de la información salvada residen en el mismo equipo (USB, disco duros…)
  - Tienen el inconveniente de que son más sensibles a amenazas físicas.
- **REMOTAS:**
  - El medio de almacenamiento es un lugar distinto en la estructura de la red que aquel en el que reside la información a salvar, (servidor backup en la nube…).
  - Son menos sensibles a estos problemas físicos, pero pueden sufrir más problemas de custodia, puesto que tendremos que asegurar no solo el acceso a los datos originales, sino también a los datos salvados, que ahora residirán en otro equipo.

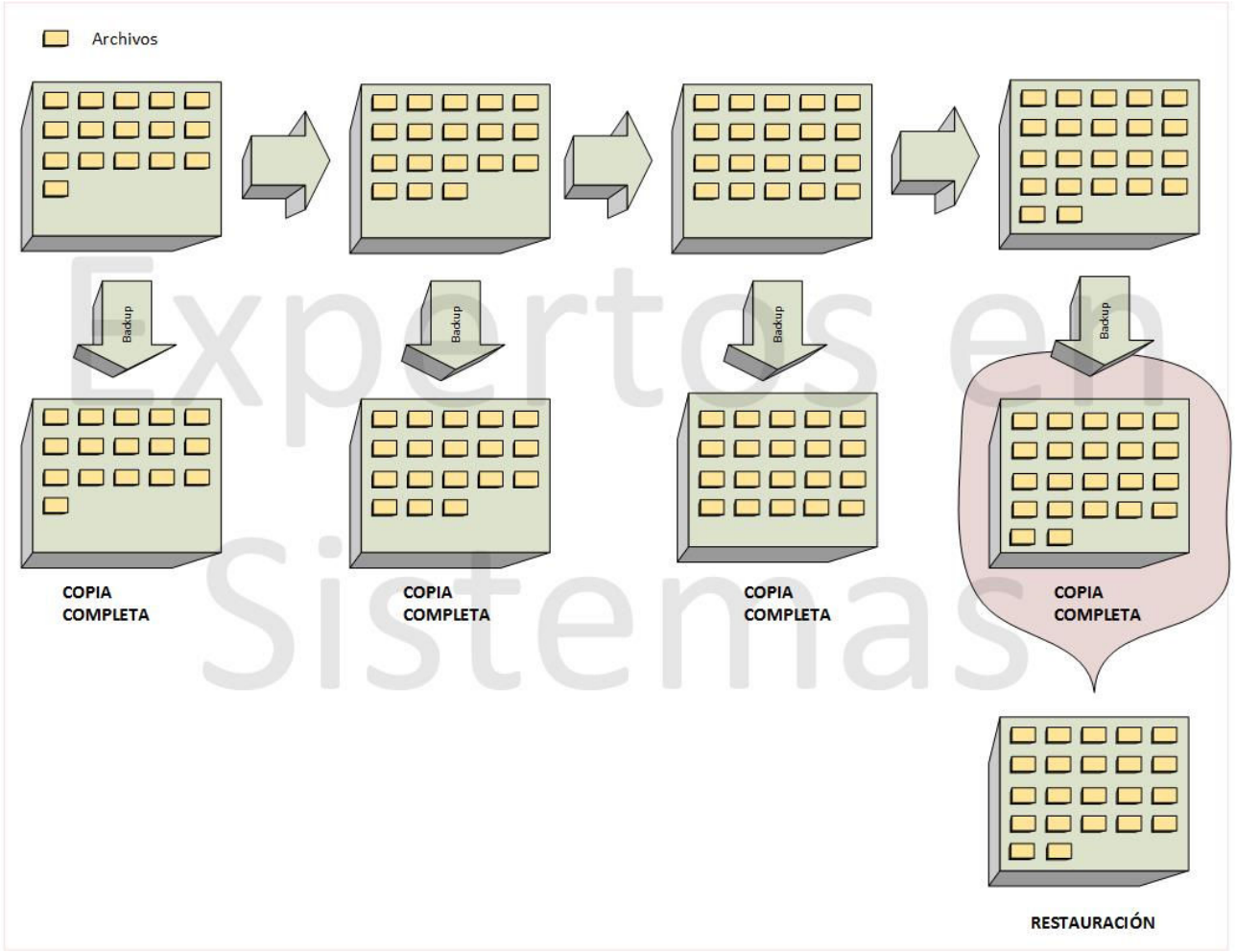
3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD

- En una instalación real, lo más frecuente es disponer de equipos especializados (almacenes de backup) que recojan los backups de toda la organización.
- La información de origen de un backup puede estar estructurada de diversos modos:
  - **Copias de seguridad de ficheros.**
  - **Copias imagen o de volúmenes**.
  - **Copias de equipos completos**.
- **El formato de salida de la copia de seguridad puede ser:**
  - El backup puede realizar copias de ficheros tal y como están en el origen reproduciendo la estructura del sistema de ficheros de origen en la salida.
  - Otro formato es el de archivado o empaquetado en el que toda la información de origen se empaqueta en un único fichero de salida, que contiene no solo los contenidos informativos de origen, sino que también incluye metadatos sobre cómo estaba estructurada en origen para ser reproducida en una posible restauración.

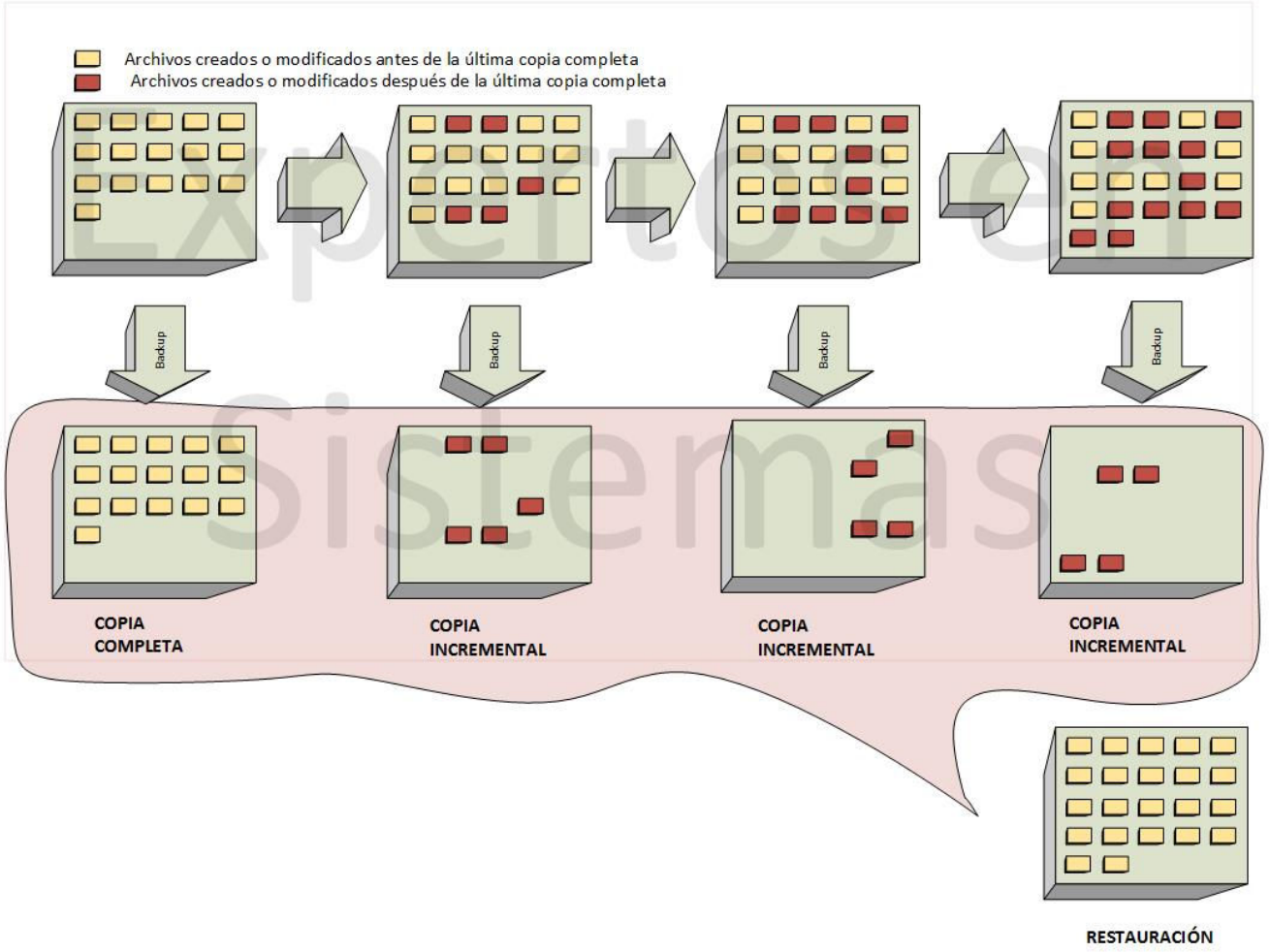
3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD

- Tipos habituales de copias de seguridad:
  - **Normal**: copia todos los ficheros seleccionados y los marca como copiados, limpiando el atributo A. Si los ficheros se modifican después del backup, la restauración hará que se pierdan los datos posteriores a la fecha del backup.
  - **Incremental**: copia todos los archivos que han cambiado desde la última copia, marca como copiados, limpiando el atributo A. La restauración exige una copia de seguridad normal y aplicar posteriormente todas las copias de seguridad incrementales que se hubieran realizado desde entonces, en el mismo orden en que se realizaron.
  - **Diferencial**: copia todos los archivos que han cambiado desde la última copia normal, no limpia el atributo A. Para restaurar es necesario disponer de una copia normal, aplicar las copias incrementales (si las hubiera) y aplicar la última (y sola la última) copia diferencial realizada.

3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD



3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD



3.5.3.1 TIPOS DE COPIAS DE SEGURIDAD