Unidad 5

Implantación de hardware en centros de proceso de datos (CPD)

Fundamentos de Hardware

5

Índice

Introducción

Durante todos los temas anteriores hemos ido viendo como funcionan los diferentes dispositivos de hardware de una red, pero estos necesitan de una férrea infraestructura donde se almacenen y comuniquen entre ellos.

Estas infraestructuras son conocidas como CPD y vamos a ver durante esta unidad sus principales componentes y cómo funcionan.

Para poder desgranar estos conceptos, hablaremos también de cómo llevar una correcta gestión de los dispositivos de la empresa, de sus principales medidas de seguridad eléctricas y de la aseguración de la integridad de los componentes.

Veremos el termino SAI, sus soluciones a ciertos problemas y los principales tipos.

Al finalizar esta unidad

- Sabremos cuales son las arquitecturas más usadas en entornos empresariales y departamentales.
- Conoceremos cuales son las características de un CPD.
- Sabremos analizar los entornos empresariales y conoceremos los sistemas informáticos más adecuados para los mismos.
- Seremos capaces de manejar los componentes específicos en soluciones empresariales como los SAI, los servidores de almacenamiento, los racks o bastidores y el almacenamiento en la nube.
- Podremos diferenciar los conceptos de fiabilidad y disponibilidad.
- Conoceremos como analizar el concepto de inventariado de hardware con sus características y las soluciones presentes en el mercado.

5.1. Arquitecturas de ordenadores personales, sistemas departamentales y grandes ordenadores

5.1.1. Introducción a las arquitecturas informáticas según su escala

En el entorno empresarial moderno, los sistemas informáticos se han convertido en un componente esencial para el procesamiento de datos, la automatización de procesos y la gestión eficiente de la información. La elección de la arquitectura adecuada para estos sistemas depende directamente del tamaño de la organización, su actividad principal, su grado de digitalización y los requisitos de disponibilidad y seguridad.

Podemos clasificar las arquitecturas de sistemas informáticos en tres grandes grupos, según su escala y propósito:

- **Ordenadores personales (PC)**
- **Sistemas departamentales (servidores de propósito específico)**
- **Grandes ordenadores (mainframes y superordenadores)**

Cada uno de estos grupos responde a necesidades distintas y presenta ventajas y limitaciones que deben ser evaluadas en función del contexto empresarial.

5.1.2. Ordenadores personales

Los ordenadores personales (PC, por sus siglas en inglés) son sistemas diseñados para el uso individual. Se caracterizan por tener una arquitectura basada en microprocesadores estándar (generalmente x86 o ARM en arquitecturas más recientes), y están diseñados para ejecutar aplicaciones de **propósito general** como suites ofimáticas, navegadores web, editores gráficos, entornos de desarrollo, entre otros.

En el **ámbito empresarial**, los PC se utilizan principalmente como estaciones de trabajo en departamentos de administración, atención al cliente, diseño o programación. Aunque no están diseñados para soportar cargas críticas, su bajo coste y versatilidad los convierten en una opción rentable para tareas no intensivas.

5.1.3. Sistemas departamentales

Los sistemas departamentales, también conocidos como servidores intermedios o de propósito específico, son infraestructuras informáticas diseñadas para ofrecer servicios compartidos dentro de un área o departamento de una organización. Estos equipos tienen mayor capacidad de procesamiento, almacenamiento y disponibilidad que un PC convencional.

Características técnicas

- Procesadores multinúcleo de alto rendimiento (Intel Xeon, AMD EPYC)
- Memoria RAM de tipo ECC para evitar errores de memoria
- Discos duros redundantes (RAID)
- Fuente de alimentación dual y ventilación reforzada
- Sistema operativo de servidor (Windows Server, Linux Server, etc.)

Casos de uso

- Servidores de archivos compartidos (NAS/SAN)
- Servidores de impresión o correo electrónico
- Bases de datos departamentales
- Aplicaciones internas (intranet, ERP, CRM)

5.1.4. Grandes ordenadores: mainframes y superordenadores

Mainframes

Los **mainframes** son grandes sistemas centralizados desarrollados originalmente en la década de 1950 y continuamente mejorados para soportar operaciones de misión crítica. Su arquitectura está diseñada para gestionar un número muy elevado de procesos concurrentes y usuarios simultáneos, con una altísima disponibilidad (hasta un 99,999%).

Características destacadas:

- Capacidad de procesamiento masivo y multitarea real.
- Alta disponibilidad (sistemas redundantes de energía, refrigeración y red).
- Seguridad avanzada y cifrado a nivel de hardware.
- Sistemas operativos específicos (z/OS, z/VM) y soporte para virtualización masiva.
- Integración con soluciones de inteligencia artificial y deep learning.

Hipervisores habituales:

- IBM PR/SM (para mainframes IBM).
- z/VM.

Superordenadores

Aunque no son comunes en entornos corporativos tradicionales, los superordenadores (HPC, High Performance Computing) merecen ser mencionados. Se utilizan en investigación científica, simulaciones climáticas, desarrollo farmacológico o cálculos aeroespaciales.

EJEMPLO

Una entidad bancaria puede utilizar un mainframe para procesar millones de transacciones financieras al día mediante sistemas OLTP (Online Transaction Processing), garantizando integridad, disponibilidad y trazabilidad de los datos.

5.1.5. Cloud Computing

El cloud computing se ha vuelto cada vez más popular debido a sus numerosos beneficios para las empresas. Al contratar servicios en la nube, las empresas pueden ahorrar en costos iniciales y en administración de hardware, ya que el proveedor de servicios se encarga de estas tareas.

Las ventajas de esta arquitectura incluyen:

- Economía a gran escala.
- No se realizan inversiones en servidores o CPD sin saber que uso se les va a dar.
- Mucho más ágil.
- Consumo eléctrico reducido.
- Fomenta la informática móvil y el teletrabajo.
- Beneficia a empresas descentralizadas.

Tenemos tres tipos principales de servicios en la nube:

- ***IaaS o Infrastructure as a Service.*** En este modelo, se proporciona acceso a características de red, equipos y bases de datos. El cliente tiene un mayor control y flexibilidad, ya que puede administrar y configurar prácticamente todos los aspectos de la infraestructura.
- ***PaaS, Platform as a Service.*** En este caso, el proveedor se encarga de mantener y administrar la infraestructura subyacente, y el cliente se centra en la administración de las aplicaciones que desarrolla e implementa en la plataforma proporcionada.
- ***SaaS, Software as a Service.*** En este modelo, el cliente no tiene que preocuparse por la administración o el mantenimiento de la infraestructura o las aplicaciones. El proveedor se encarga de instalar, administrar y proporcionar acceso a las aplicaciones a través de la nube. Es uno de los tipos más utilizados, especialmente para aplicaciones específicas como el correo electrónico empresarial.

EJEMPLO

Una empresa puede utilizar IaaS para desplegar una red de servidores en la nube y almacenar sus datos, mientras que utiliza SaaS para gestionar su correo electrónico y PaaS para desarrollar y alojar su propia aplicación web.

IMPORTANTE

La elección del tipo de servicio en la nube (IaaS, PaaS, SaaS) depende en gran medida de las necesidades específicas de la empresa y del nivel de control que quiera tener sobre la infraestructura y las aplicaciones.

Tenemos también, diferentes maneras para implementar el cloud computing:

- **Totalmente en la nube:** Esta implementación implica que todos los servicios, aplicaciones y datos de una empresa se ejecutan y almacenan en la nube. No se requiere infraestructura local y todo se gestiona a través de proveedores de servicios en la nube. Este enfoque ofrece flexibilidad, escalabilidad y reduce la carga de mantenimiento y administración para la empresa.

EJEMPLO

Un startup que recién comienza su negocio puede optar por un enfoque totalmente en la nube para evitar inversiones iniciales en hardware y software, y para poder escalar sus operaciones de manera más eficiente a medida que crece el negocio.

- **Híbrida:** En una implementación híbrida, la empresa combina el uso de servicios en la nube con infraestructura local existente. Algunas aplicaciones y servicios pueden ejecutarse en la nube, mientras que otros se mantienen en servidores locales. Esta configuración es útil cuando hay necesidades específicas o requisitos de seguridad que requieren mantener ciertos datos o aplicaciones en la infraestructura local, mientras se aprovechan los beneficios de la nube para otros aspectos.

EJEMPLO

Una empresa con un sistema de base de datos local que contiene información sensible puede optar por un enfoque híbrido, manteniendo la base de datos en su servidor local para seguridad y control, mientras utiliza servicios en la nube para tareas menos críticas como correo electrónico y colaboración en documentos.

IMPORTANTE

En una configuración **híbrida**, es crucial asegurar la correcta integración y la seguridad de la comunicación entre los recursos locales y los de la nube.

- **On-premise (Nube privada):** Esta implementación se refiere a la virtualización de la infraestructura local de la empresa en la nube. La organización crea su propia nube privada utilizando recursos dedicados que no se comparten con otras empresas. Esto permite a la empresa tener un mayor control y seguridad sobre sus datos y aplicaciones, al tiempo que aprovecha las ventajas de la virtualización y la escalabilidad que ofrece la nube. Es similar a la infraestructura clásica local, pero virtualizada en la nube privada de la empresa.

EJEMPLO

Una empresa que necesita cumplir con estrictos requisitos de privacidad y seguridad, como una institución financiera, puede optar por una implementación on-premise, creando una nube privada en su propia infraestructura.

IMPORTANTE

En un escenario de **nube privada on-premise,** la empresa es responsable del mantenimiento y la gestión de la infraestructura, lo que puede requerir recursos y experiencia técnica significativos.

5.1.6. Ordenadores virtuales

Los ordenadores virtuales son máquinas alojadas en la nube a las que se accede mediante un escritorio virtual. Su uso está en aumento en las empresas.

A diferencia de un equipo físico, donde estamos limitados por los recursos disponibles y debemos esperar para realizar cambios, en un ordenador virtual podemos ajustar la configuración con solo unos clics. Esto significa que en cuestión de minutos podemos tener a nuestra disposición una mayor cantidad de recursos. Esta capacidad de ajuste rápido y fácil se conoce como escalabilidad.

Un ordenador virtual funciona exactamente igual que una máquina física. Podemos instalar las mismas aplicaciones y sistemas, por lo tanto, también debe ser protegido de la misma manera en términos de seguridad.

La ventaja de los ordenadores virtuales es que podemos acceder a ellos desde cualquier dispositivo, siempre que tengamos autorización. Podemos acceder a nuestro escritorio virtual desde cualquier ubicación sin que se observen cambios visibles. Esto proporciona flexibilidad y movilidad a los usuarios.

Es importante mencionar que se requiere autorización para acceder a estos ordenadores virtuales y que cualquier intercambio de datos está cifrado, al igual que el acceso, para garantizar la seguridad y la protección de la información.

5.2. Estructura de un Centro de Procesamiento de Datos (CPD). Organización

Los **Centros de Procesamiento de Datos (CPD)** son espacios técnicos especialmente diseñados para alojar de forma segura y controlada los recursos informáticos esenciales para el funcionamiento continuo de una organización. A diferencia de otras áreas informáticas, en un CPD no se instalan ordenadores personales o de usuario final, sino **infraestructura crítica**, como servidores, switches, dispositivos de almacenamiento masivo y sistemas de red.

Con la expansión del **Cloud Computing**, la presencia física de CPD propios ha disminuido en muchas empresas, especialmente en pequeñas y medianas. Sin embargo, siguen siendo **infraestructuras fundamentales** en organizaciones que requieren un alto control sobre sus datos, baja latencia, o cumplen normativas específicas de seguridad o confidencialidad.

La función principal de un CPD es **garantizar la disponibilidad continua del servicio**, lo que implica una infraestructura robusta, redundante y segura. Además de esta disponibilidad, es imprescindible implementar medidas de **seguridad física y lógica** para proteger la información y los sistemas frente a amenazas tanto internas como externas.

A continuación, se detallan los principales requisitos técnicos y estructurales que debe cumplir un CPD:

- **Diseño.** Es fundamental que el CPD disponga de un diseño específico y planificado en cuanto a dimensiones, distribución del espacio, organización del cableado y flujos de aire. La planificación debe considerar aspectos como:
  - Accesibilidad a los equipos
  - Facilidad de mantenimiento
  - Capacidad de expansión
  - Eficiencia energética
- **Seguridad física del local.** Para preservar la integridad de los equipos frente a incidentes, el CPD debe estar protegido con sistemas de **detección y extinción de incendios**, así como medidas contra **inundaciones** o filtraciones de agua.

  Algunas medidas habituales incluyen:
  - Detectores de humo de alta sensibilidad (tipo VESDA)
  - Extinción mediante gases inertes (por ejemplo, FM-200 o Novec 1230)
  - Sensores de humedad o fugas en suelo técnico
  - Sistemas de videovigilancia y control de acceso

- **Suministro eléctrico.** El CPD debe contar con un suministro eléctrico ininterrumpido y redundante. Es habitual el uso de:
  - Sistemas de alimentación ininterrumpida (SAI o UPS) para cubrir microcortes
  - Grupos electrógenos para emergencias prolongadas
  - Circuitos de alimentación duales
  - Tableros de distribución con balanceo de cargas

  La estabilidad del suministro es crítica para evitar caídas inesperadas de los sistemas y daños al hardware.

- **Aislamiento acústico.** Dado que muchas máquinas funcionando simultáneamente generan mucho ruido, es importante contar con un buen aislamiento acústico para preservar un entorno de trabajo cómodo y no perjudicar la salud.

- **Ubicación.** La localización del CPD dentro del edificio es un factor clave para su seguridad y operatividad. No debe instalarse en áreas con **riesgo de inundación** (como sótanos), ni en zonas propensas a **desastres naturales** o de difícil acceso en caso de emergencia.
  - Recomendaciones habituales:
  - Situarlo en **plantas intermedias** o zonas centrales del edificio
  - **Evitar ventanas al exterior**, tanto por seguridad como por control térmico
  - Mantener **accesos controlados y restringidos**
  - Proteger el perímetro contra impactos, filtraciones y accesos no autorizados

IMPORTANTE

Una ubicación adecuada es crucial para el CPD, ya que tanto los desastres naturales como los incidentes de seguridad pueden afectar seriamente la operación del negocio.

- **Temperatura y humedad.** Las condiciones ambientales dentro del CPD deben mantenerse dentro de parámetros técnicos definidos por estándares como **ASHRAE**. Esto garantiza el correcto funcionamiento de los equipos, su durabilidad y seguridad.

  Requisitos típicos:
  - **Temperatura:** mantener entre **18 °C y 27 °C**. Temperaturas por debajo de 16 °C no son recomendables por razones de eficiencia energética y condensación.
  - **Humedad relativa:** entre **45 % y 55 %** para evitar tanto descargas electrostáticas como condensación.
  - **Sistemas de climatización redundantes:** uso de aire acondicionado de precisión (CRAC), flujo bajo falso suelo, y filtración de partículas.

- **Diseño y dimensiones.** un CPD debe estar diseñado para soportar las **cargas físicas** de los equipos y facilitar tanto el trabajo diario como futuras ampliaciones:
  - El suelo debe ser capaz de soportar cargas pesadas, generalmente reforzado para soportar hasta **2000 kg por metro cuadrado**.
  - La **altura libre mínima** entre suelo y techo debe ser de **2,5 metros** para permitir una buena circulación del aire, iluminación y acceso cómodo.
  - Se recomienda utilizar **falso suelo y falso techo** para distribuir adecuadamente cables eléctricos, de red y refrigeración.
  - La iluminación debe ser homogénea, sin deslumbramientos, y preferiblemente mediante luces LED regulables.
  - Las puertas deben tener un ancho suficiente (mínimo 90 cm) y apertura doble o desmontable para permitir el acceso de servidores, racks y otros equipos voluminosos.

IMPORTANTE

El **diseño y las dimensiones** de un CPD son vitales, ya que deben permitir un espacio de trabajo adecuado, el fácil acceso a los equipos y la capacidad de escalar o reorganizar el espacio si es necesario en el futuro.

5.2.1. Zonificación propuesta para un CPD

El diseño interno de un **Centro de Procesamiento de Datos (CPD)** se basa en una organización funcional que permite distribuir los equipos y sistemas por áreas especializadas. Esta distribución mejora la seguridad, el mantenimiento, la eficiencia energética y la escalabilidad del sistema.

En la siguiente imagen se muestra un ejemplo esquemático de CPD donde se identifican las principales zonas operativas:

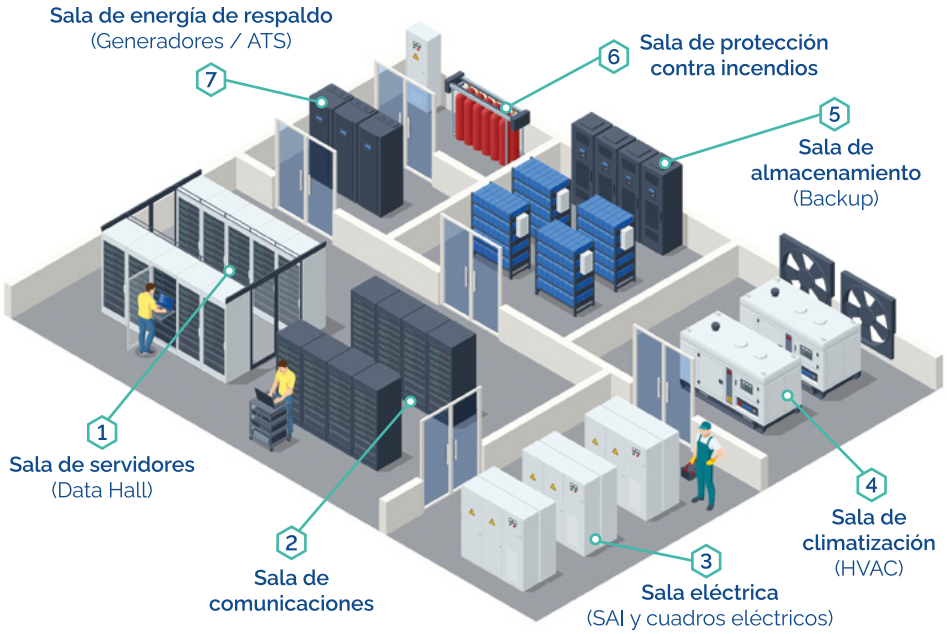


Imagen 1. Zonificación de un CPD

1. Sala de servidores (Data Hall)

Es el **núcleo operativo** del CPD. Contiene los **racks de servidores**, sistemas de almacenamiento y equipos activos. Es la zona con mayor concentración de calor, tráfico de datos y actividad informática.

- Requiere refrigeración de precisión, control de humedad y acceso restringido.
- Suele implementarse en configuración de **pasillos fríos y calientes** (cold aisle / hot aisle) para mejorar la eficiencia térmica.

2. Sala de comunicaciones

Aloja los elementos clave del **cableado estructurado** y la conectividad de red: switches de núcleo, routers, patch panels y enlaces de fibra óptica. Es el **punto central de distribución de red**.

- Debe mantenerse organizada, con cableado etiquetado y separaciones entre voz, datos y energía.
- Puede estar conectada a varios puntos de red redundantes para garantizar disponibilidad.

3. Sala eléctrica (SAI y cuadros eléctricos)

Contiene los **sistemas de alimentación ininterrumpida (SAI o UPS)**, **cuadros eléctricos**, y **paneles de distribución de energía**. Su función es proporcionar una fuente eléctrica estable, filtrada y continua a todo el CPD.

- Requiere separación física de otras salas por motivos de seguridad.
- Debe contar con protección contra sobretensiones, cortocircuitos y fallos eléctricos.

4. Sala de climatización (HVAC)

Agrupa los sistemas de **refrigeración industrial**, como unidades CRAC, condensadores, ventiladores y climatizadores de precisión. Su función es mantener la **temperatura y humedad relativa** dentro de los rangos establecidos por la norma **ASHRAE**.

- Imprescindible para evitar el sobrecalentamiento de los equipos.
- La refrigeración debe tener **redundancia (N+1 o 2N)** y control ambiental constante.

5. Sala de almacenamiento (Backup)

Espacio reservado para los sistemas de **copias de seguridad y almacenamiento secundario**, como cabinas NAS/SAN o librerías de cintas (LTO). Se usa para asegurar la **recuperación de datos** en caso de fallo o incidente.

- Requiere condiciones ambientales estables, pero puede estar físicamente separada del Data Hall.
- Dependiendo del entorno, también puede integrarse en soluciones híbridas (backup local + en la nube).

6. Sala de protección contra incendios

Almacena los sistemas de **extinción automática mediante gas inerte**, como FM-200, Novec 1230 o CO_2. Estos sistemas permiten extinguir incendios sin dañar los equipos electrónicos.

- Las botellas presurizadas deben estar correctamente etiquetadas y mantenidas.
- Su activación automática se vincula a sensores de humo y temperatura, y su instalación debe cumplir normativas como **UNE-EN 15004** o **NFPA 2001**.

7. Sala de energía de respaldo (Generadores / ATS)

Contiene los **grupos electrógenos** (generalmente diésel) y el **sistema automático de transferencia (ATS)**. En caso de fallo del suministro eléctrico principal, estos equipos garantizan la **alimentación continua** del CPD.

- Debe estar aislada del resto de las salas por seguridad y ventilación.
- Su activación debe ser automática y supervisada mediante sistemas de control remoto

IMPORTANTE

En un CPD real, estas salas deben estar **físicamente separadas o compartimentadas** para reducir riesgos (incendios, sobrecalentamiento, accesos no autorizados) y garantizar el cumplimiento de normativas como **TIA-942** o **ISO/IEC 27001.**

5.3. Seguridad física

Una organización debe estar protegida frente a múltiples amenazas que puedan comprometer la **continuidad de su actividad empresarial** y la **seguridad de sus activos críticos**. Estos activos no solo incluyen bienes materiales y equipos, sino también información sensible, propiedad intelectual y recursos tecnológicos esenciales para el funcionamiento de la empresa.

Además de factores **económicos, demográficos y ambientales**, resulta indispensable implementar planes de **seguridad física** y **seguridad lógica**, complementarios entre sí, con el fin de reducir riesgos y proteger los activos frente a amenazas tanto **externas** (robos, sabotajes, intrusiones) como **internas** (mal uso, negligencia o accesos indebidos).

Una amenaza común en el entorno empresarial actual es el **robo de información sensible**, como **patentes tecnológicas, diseños estratégicos o ideas de negocio**, lo que puede tener graves consecuencias económicas y legales. Por tanto, la protección de los espacios físicos debe ser parte integral de una **estrategia de seguridad global**.

Ubicación del complejo empresarial

La **ubicación física** del complejo empresarial influye directamente en el nivel de exposición a riesgos. Algunos factores a considerar son:

- **Riesgo geológico:** zonas propensas a terremotos, deslizamientos o inundaciones.
- **Entorno industrial:** proximidad a instalaciones peligrosas (centrales nucleares, fábricas químicas).
- **Infraestructura crítica:** calidad de las comunicaciones, estabilidad del suministro eléctrico, accesos viarios.
- **Entorno competitivo:** concentración de empresas del mismo sector, riesgo de espionaje industrial.

Una **evaluación de riesgos del entorno** debe formar parte del estudio de viabilidad y diseño del CPD o sede empresarial, aplicando metodologías como **análisis DAFO**, **análisis de impacto** o estándares de continuidad del negocio como **ISO 22301**.

Clasificación de activos según nivel de criticidad

No todos los activos requieren el mismo nivel de protección. Por tanto, es fundamental **clasificar los activos** en función de:

- Su importancia para la operación diaria.
- Su sensibilidad frente a accesos no autorizados.
- Su valor económico o estratégico.

Por ejemplo

- Un **switch principal de núcleo** que da servicio a toda la red corporativa debe tener mayor nivel de protección física que un **switch de acceso** que da conectividad a un solo departamento.

Este enfoque **permite optimizar los recursos** de seguridad, enfocándose en proteger con mayor intensidad los activos más críticos.

Control de accesos físicos

Uno de los **métodos más efectivos** en materia de seguridad física es la **gestión del control de accesos**. Esta estrategia se basa en **limitar el acceso físico** a áreas sensibles (como el CPD o salas técnicas) exclusivamente al personal autorizado, registrando todos los accesos para fines de **auditoría, trazabilidad y prevención**.

NOTA

Las políticas de acceso deben incluir:

- Autorización previa documentada.
- Validación de identidad.
- Registro automatizado de entradas y salidas.
- Alertas ante intentos de acceso no autorizados.

Principales sistemas de control de acceso

- **Códigos de acceso:** Consisten en una combinación numérica que permite abrir puertas electrónicas. Son fáciles de implementar, pero poco seguros, ya que pueden ser **copiados o compartidos**. No verifican realmente la identidad del usuario, solo su conocimiento del código.
- **Bandas magnéticas:** Tarjetas físicas con una banda codificada que se desliza por un lector. Mejoran la seguridad al requerir un **dispositivo físico**, aunque también pueden ser **clonadas** si no están encriptadas.
- **RFID (Radio Frequency Identification):** Etiquetas o tarjetas que se leen por proximidad mediante radiofrecuencia. Son más económicas y resistentes al desgaste que las bandas magnéticas, y permiten el acceso sin contacto físico directo. Su nivel de seguridad depende del cifrado y del sistema de autenticación que las respalde.
- **Biometría:** Es el método más avanzado, ya que se basa en características **únicas e intransferibles del usuario**, como la **huella dactilar**, **iris**, **reconocimiento facial** o **patrón venoso**. Este sistema garantiza un nivel de seguridad elevado, aunque puede tener costes de implementación más altos y consideraciones legales respecto a la privacidad (GDPR).

Vigilancia y monitoreo físico

Además del control de accesos, es fundamental contar con sistemas de **supervisión continua** que permitan detectar actividades anómalas, intrusiones o incidentes antes de que se produzcan daños graves.

Algunas herramientas y métodos habituales incluyen:

- **Personal de seguridad:** Vigilantes o técnicos especializados que patrullan las instalaciones, controlan accesos y responden ante alarmas o emergencias. Su presencia física actúa también como medida disuasoria.
- **Sensores y sistemas de detección:** Instalación de sensores de movimiento, apertura de puertas, rotura de cristales, cambios bruscos de temperatura o humedad, etc. Estos sensores se integran con sistemas de alarma y automatización (domótica industrial).
- **Cámaras de seguridad (CCTV):**Sistemas de videovigilancia distribuidos por zonas estratégicas (entradas, CPD, pasillos técnicos). Permiten grabar en tiempo real y consultar grabaciones en caso de incidente. Su eficacia depende de la resolución, el ángulo de cobertura y el almacenamiento seguro de las imágenes.

5.4. Componentes específicos en soluciones empresariales

A continuación, se presentan los principales elementos utilizados en entornos empresariales para garantizar la disponibilidad del servicio y la protección de la infraestructura informática frente a fallos eléctricos y otros riesgos tecnológicos.

5.4.1. Los Sistemas de alimentación ininterrumpida (SAI).

Los **SAI (Sistemas de Alimentación Ininterrumpida)** son dispositivos diseñados para proporcionar energía eléctrica de forma continua durante un fallo en el suministro, aunque este sea momentáneo. Su función principal es evitar apagados bruscos en equipos críticos como **servidores, sistemas de red o almacenamiento**, permitiendo que continúen funcionando durante un corto periodo de tiempo o se apaguen de forma segura.

En entornos profesionales, disponer de un SAI no es solo recomendable, sino **obligatorio** cuando existen servidores o dispositivos que gestionan datos sensibles o sistemas de misión crítica. Un apagado inesperado puede ocasionar **pérdida de datos, corrupción de sistemas operativos o daños físicos en los discos duros**.

Tipos de SAI

Existen varios tipos de SAI, clasificados según su funcionamiento:

- **Offline (Standby).** Solo se activan cuando detectan una interrupción. Son los más básicos.
- **Línea interactiva.** Incorporan estabilizadores de tensión, protegiendo contra subidas y bajadas de voltaje.
- **Online (Doble conversión).** Proporcionan una señal eléctrica **estable y continua**, sin interrupciones perceptibles, incluso si la red sufre variaciones. Son los más adecuados para entornos profesionales.

Los **SAI online** incluyen componentes como:

- **Rectificadores.** Convierten la corriente alterna en continua para cargar las baterías.
- **Inversores.** Transforman la corriente continua de las baterías en corriente alterna limpia y estable.
- **Reguladores de voltaje.** Mantienen una tensión constante frente a fluctuaciones.

Imagen 1. Tipo de SAI

Defectos de la señal eléctrica

Las señales eléctricas no siempre son estables o ideales. Existen múltiples tipos de **alteraciones eléctricas** que pueden afectar el correcto funcionamiento de los dispositivos electrónicos. Los SAI avanzados pueden proteger frente a la mayoría de estos defectos.

A continuación, se presenta una imagen con los defectos más comunes en las señales eléctricas:

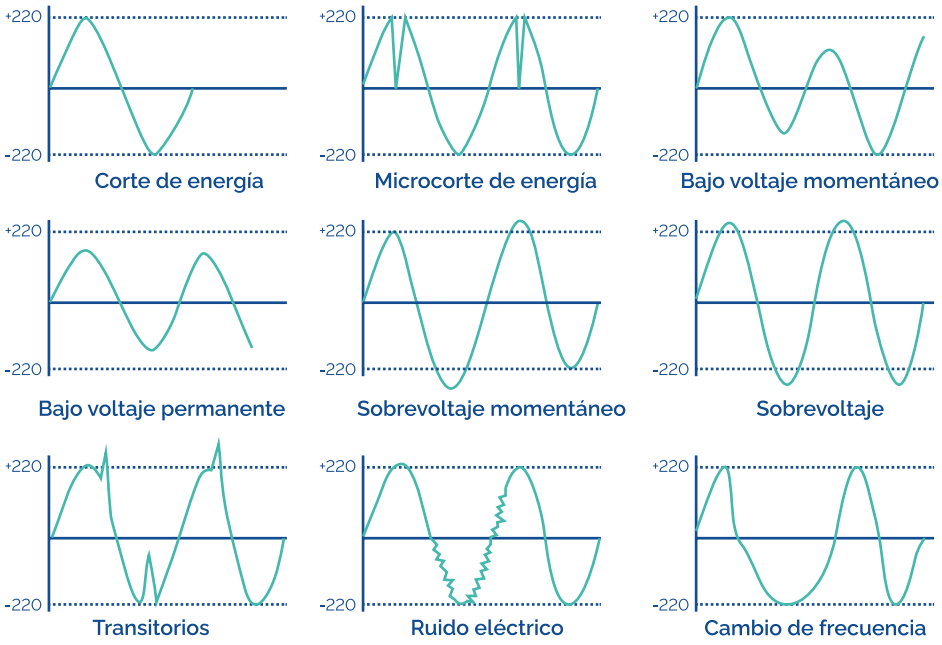


Imagen 2. Defectos de la señal eléctrica

IMPORTANTE

La señal eléctrica de alta calidad es la más parecida a la que sería teóricamente la señal perfecta.

Los principales problemas que pueden sufrir las señales son:

- **Interrupción o corte de energía.** Se puede decir que un corte de energía ha sucedido si la energía ha caído por debajo de un 10% de su capacidad. Los cortes pueden ser producidos por cualquier circunstancia, como un mantenimiento programado o la rotura de un cable de la instalación.
- **Microcortes.** Son momentáneas caídas del suministro eléctrico con rápida recuperación. Estos son peligrosos para algunas baterías.
- **Bajo voltaje momentáneo.** Más frecuentes que los cortes de energía, se sufre una bajada de tensión de entre un 10% y un 90%. Estos afectan a numerosos aparatos que no están diseñados para funcionar con tan poca energía.
- **Bajo voltaje permanente.** El voltaje cae más del 90% durante más de 60 segundos. Hay ocasiones en las que las mismas compañías eléctricas realizan estas acciones cuando tienen una gran demanda de conexión eléctrica. Existen estabilizadores de voltaje que solventan estos problemas.
- **Sobrevoltaje momentáneo.** Se supera el 110% del voltaje nominal por unos momentos, pero se puede arreglar con un estabilizador. Es más común que el bajo voltaje momentáneo.
- **Sobrevoltaje permanente.** Esto sucede si se ha superado el voltaje nominal en más de un 110% y su duración ha sido superior a un minuto.

Es de los peores defectos para los dispositivos porque suele acarrear consecuencias fatídicas debido al sobrecalentamiento que sufren.

- **Sobretensiones transitorias o transitorios.** Son picos de tensión de muy poca duración. Esto puede suceder por ejemplo con n la caída de un rayo. Un SAI de calidad protegerá de estos en casi su mayoría.
- **Ruido eléctrico.** La onda eléctrica sufre distorsiones, lo que puede acarrear perdida de datos en algunos dispositivos o una corrupción de estos, además de otros problemas derivados de la diferenciación de la señal. También puede ser eliminado por un SAI profesional.
- **Cambio en la frecuencia.** Esta es casi imposible de ocurrir, pero a veces ocurre, y esto provoca que los dispositivos electrónicos funcionen de manera errónea directamente, pero no conlleva graves consecuencias futuras de funcionamiento.

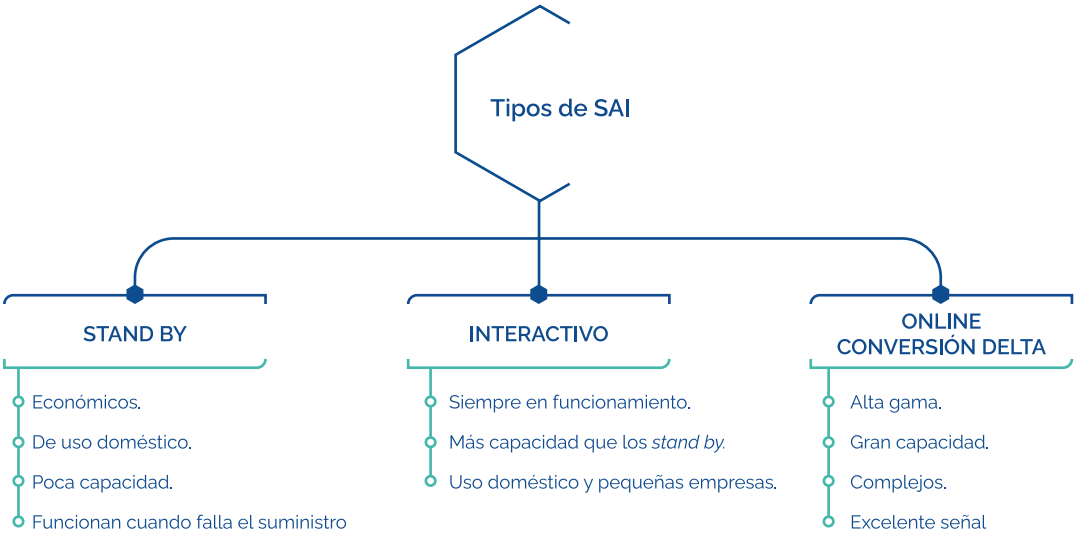
SAI

Como hemos introducido anteriormente, los SAI se usan además de para que la señal eléctrica se mantenga, para solucionar la mayoría de los defectos que vimos anteriormente.

Hay que saber diferenciar entre los SAI de ámbito empresarial, mucho más profesionales y con capacidad para solventar problemas, y uno de uso doméstico, que por lo general solo seguirá emitiendo señal.

En la gama baja de SAI nos encontramos con los interactivos y los *stand by*, mientras que en gama alta nos podemos encontrar con los *online*.

Aquí tenemos un breve resumen de los tipos de SAI:



SAI stand by u offline

Este tipo de SAI es el **más económico** y simple del mercado. Su funcionamiento se basa en un **interruptor de transferencia automática** que se activa cuando detecta una **anomalía en la red eléctrica**. En ese momento, el equipo cambia la fuente de alimentación desde la red hacia el inversor del SAI, que entrega corriente alterna a los dispositivos conectados.

Características clave:

- No filtra ni estabiliza la señal eléctrica.
- No actúa si la señal está distorsionada, pero no cortada.
- Recomendado únicamente en entornos **domésticos** o lugares con red estable.
- **No apto para cargas superiores a 2000 VA**.

Su funcionamiento se describe en la siguiente ilustración:

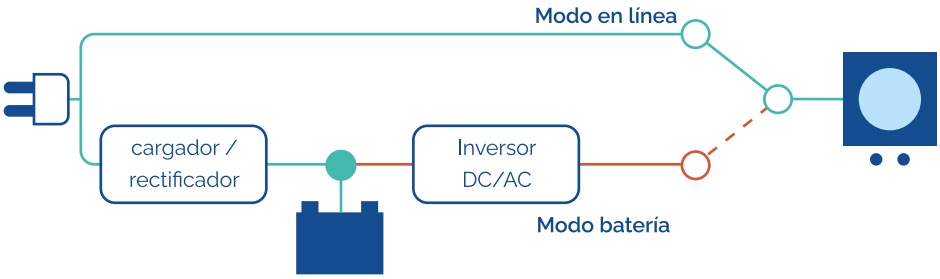


Imagen 3. Funcionamiento de un SAI *offline*

SAI interactivos

Es una evolución del modelo anterior. Incorpora un **sistema de regulación automática de voltaje (AVR)** que le permite compensar bajadas o subidas leves de tensión sin tener que recurrir a las baterías. El inversor solo entra en funcionamiento cuando hay un corte de red.

Características clave:

- Ofrece una señal más estable que el stand-by.
- Preserva la vida útil de las baterías al no activarlas constantemente.
- Adecuado para **pequeñas empresas** y estaciones de trabajo sensibles.
- No se recomienda para cargas superiores a **5000 VA**.

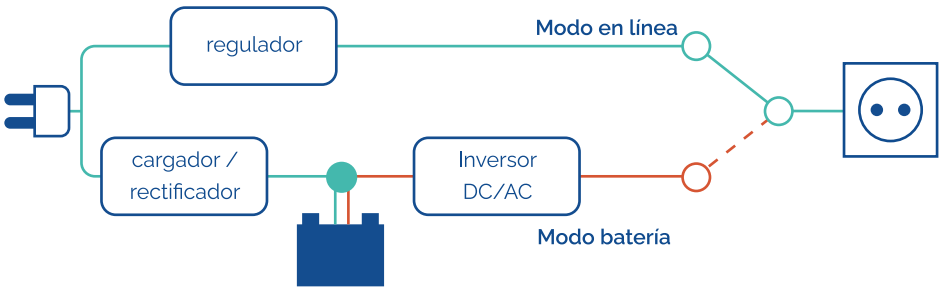
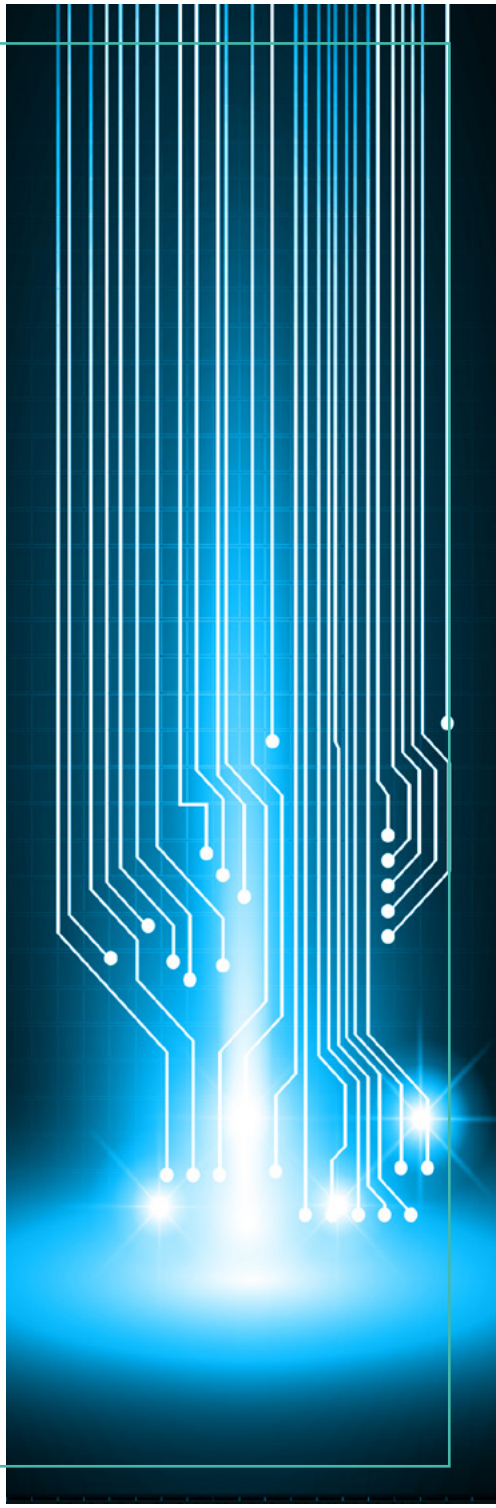


Imagen 4. Funcionamiento de un SAI interactivo

SAI Online (Conversión doble / Delta)



Es el sistema más completo y profesional. El inversor está **siempre en funcionamiento**, de modo que los equipos conectados **reciben la energía directamente desde el SAI**, independientemente de las condiciones de la red eléctrica.

Características clave:

- Proporciona una señal **totalmente limpia y constante**.
- Protege frente a **todos los defectos eléctricos**, incluidos ruido, transitorios y cambios de frecuencia.
- Ideal para entornos **críticos**, como CPD, videovigilancia, sanidad o industria.
- **Alta capacidad** y funcionamiento continuo.

1. ### Como se calcula la carga de un SAI

   La **carga** es la suma de la potencia total de los dispositivos conectados al SAI, y se expresa normalmente en **voltios-amperios (VA)**. Este dato es fundamental para seleccionar el modelo adecuado.

   #### Fórmula básica:

   - El factor de potencia típico en entornos informáticos es **0,8**.
   - Se recomienda sobredimensionar el SAI en un **20–30 %** para garantizar fiabilidad.

2. ### Qué es la autonomía de un SAI

   La **autonomía** representa el tiempo durante el cual el SAI puede mantener en funcionamiento los equipos conectados **sin estar alimentado por la red**. Esta duración depende de dos factores:

   - Capacidad de las baterías
   - Porcentaje de carga activa

   Ejemplo práctico:

   - Un SAI con autonomía de **40 minutos al 40 % de carga**
   - Tendrá solo **20 minutos de autonomía al 80 % de carga**

Cuantos más equipos estén conectados al SAI, **menor será el tiempo** de respaldo disponible.

5.4.2. El almacenamiento empresarial en la nube

En los últimos años, el **almacenamiento en la nube** se ha consolidado como una solución esencial en el entorno empresarial. Su adopción se extiende desde pequeñas empresas hasta grandes corporaciones, así como en el ámbito doméstico, gracias a su escalabilidad, accesibilidad y bajo coste de implementación.

¿Qué es el almacenamiento en la nube?

El almacenamiento en la nube consiste en **guardar información en servidores externos** a través de Internet, en lugar de hacerlo en dispositivos locales. Los datos se alojan en **centros de datos gestionados por terceros**, lo que permite acceder a ellos desde cualquier lugar, siempre que se tenga conexión y autorización.

Ejemplo cotidiano:

Los smartphones actuales requieren asociar una cuenta para su funcionamiento. En Android, es una cuenta de **Google (Gmail)**; en iOS, es el **Apple ID**. Ambas plataformas integran servicios de almacenamiento en la nube:

- **Google Drive** (Google)
- **iCloud** (Apple)

Estas soluciones permiten **almacenar y sincronizar** automáticamente fotos, documentos, contactos y otros archivos.

Otras soluciones populares de almacenamiento en la nube:

- Microsoft OneDrive
- Dropbox
- Amazon Drive
- Box

Ventajas para las empresas:

- Acceso remoto y multiplataforma
- Reducción de costes en hardware local
- Escalabilidad según la demanda
- Copias de seguridad automáticas
- Compartición segura de archivos entre usuarios y equipos

5.4.3. Servidores de almacenamiento empresarial

El **almacenamiento de la información** es un pilar estratégico para cualquier empresa. Para gestionar grandes volúmenes de datos de forma eficiente, se utilizan servidores y tecnologías de almacenamiento profesional, que ofrecen **fiabilidad, rendimiento y escalabilidad**.

A continuación, se describen los sistemas más relevantes en entornos empresariales.

Servidores SAN (Storage Area Network)

Los servidores SAN son dispositivos de almacenamiento que forman parte de una **red de área de almacenamiento independiente**, conectados al resto de la infraestructura mediante **cables de fibra óptica**.

Características principales:

- Alta velocidad de transferencia
- **Escalabilidad**: permiten alcanzar capacidades de **múltiples terabytes o incluso petabytes**
- **Red separada del tráfico de datos tradicional**
- Uso habitual en entornos de **virtualización, bases de datos y CPD**

Almacenamiento Flash y NVMe

Los sistemas SAN modernos **ya no utilizan discos mecánicos tradicionales**. En su lugar, emplean tecnologías como:

- **Discos de estado sólido (SSD)**
- **Unidades NVMe (Non-Volatile Memory Express)**

Ventajas clave:

- Mayor velocidad de acceso a los datos
- Menor latencia
- Mayor durabilidad y eficiencia energética

Almacenamiento en VVols (Volúmenes virtuales)

Los **VVols (Virtual Volumes)** son volúmenes virtuales que encapsulan por completo los archivos de una **máquina virtual**. Cada VVol se gestiona como una unidad lógica independiente, lo que facilita su administración y movilidad.

Ventajas de los VVols:

- Cada máquina virtual tiene su propio GUID (Identificador Único Global)
- Gestión centralizada y simplificada
- Integración con **sistemas de virtualización** como VMware vSphere

Almacenamiento de objetos

El **almacenamiento de objetos** es una arquitectura emergente que está sustituyendo al almacenamiento tradicional por archivos. A diferencia de los sistemas jerárquicos (carpetas y subcarpetas), los objetos se almacenan en un **espacio de direcciones plano** y se accede a ellos mediante un **identificador único**.

Ventajas principales:

- No requiere estructuras de carpetas complejas
- Facilita la **escalabilidad horizontal** sin reestructuración
- Ideal para grandes volúmenes de datos no estructurados (copias de seguridad, archivos multimedia, logs, etc.)

Por ejemplo, **Amazon S3 (Simple Storage Service)** es uno de los sistemas de almacenamiento de objetos más usados en el mundo empresarial.

5.5. Arquitecturas de alta disponibilidad

El concepto de **alta disponibilidad (HA, High Availability)** hace referencia a la capacidad de un sistema para mantenerse en funcionamiento de forma continua y sin interrupciones significativas. En entornos empresariales, esto se traduce en un funcionamiento **24 horas al día, 7 días a la semana (24/7)**.

Implementar una arquitectura de alta disponibilidad implica diseñar sistemas informáticos que **minimicen el tiempo de inactividad (downtime)** y garanticen el acceso constante a los servicios, incluso ante fallos o incidentes técnicos.

Requisitos técnicos

Un sistema de alta disponibilidad debe estar instalado sobre **infraestructura robusta y redundante**, ya que los **equipos domésticos o de oficina no están diseñados** para soportar cargas críticas ni ofrecer fiabilidad a largo plazo.

Las empresas que optan por este tipo de arquitectura lo hacen con el objetivo de **evitar pérdidas de servicio, corrupción de datos o interrupciones operativas** que podrían suponer un impacto económico o reputacional.

Fiabilidad (Reliability)

La fiabilidad es una medida estadística que **indica la probabilidad de que un sistema funcione correctamente durante un periodo determinado sin sufrir fallos**. Cuanto más tiempo permanece operativo sin interrupciones, **mayor es su fiabilidad**.

EJEMPLO

Si un servidor ha estado operativo durante 6 meses sin registrar errores ni fallos de servicio, se considera que presenta un **alto nivel de fiabilidad.**

El tipo de fallo considerado relevante para este análisis debe ser **definido por el administrador del sistema**, ya que puede variar según el tipo de servicio o el nivel de criticidad.

Disponibilidad (Availability)

La disponibilidad mide la **probabilidad de que un sistema esté en funcionamiento y accesible** durante un periodo de tiempo específico. Se expresa como un **porcentaje de funcionamiento anual**, utilizando la siguiente fórmula:

Disponibilidad = Uptime / (Uptime + Downtime)

Donde:

- **Uptime:** tiempo total en el que el sistema está funcionando correctamente (en minutos)
- **Downtime:** tiempo en el que el sistema está inoperativo o fuera de servicio

EJEMPLO DE CÁLCULO

Si un sistema ha estado operativo 525 600 minutos en un año (365 días), pero ha sufrido 5 minutos de inactividad, la disponibilidad sería:

Disponibilidad = 525 595 / (525 595 + 5) = 0,999990 = **99,999%**

Este nivel de disponibilidad se conoce como **"cinco nueves",** el estándar ideal en sistemas de misión crítica como bancos, hospitales, infraestructuras gubernamentales o servicios cloud.

EJERCICIO PRÁCTICO: CALCULANDO LA DISPONIBILIDAD

Una empresa tiene un servidor dedicado a la gestión de clientes. Durante el último año, el servidor ha estado en funcionamiento durante 525 500 minutos, pero ha sufrido una serie de interrupciones que suman un total de 25 minutos de inactividad.

1. Calcula la **disponibilidad anual** del sistema expresada en porcentaje.
2. Reflexiona si crees que se trata de una arquitectura de alta disponibilidad según los estándares explicados.

SOLUCIÓN GUÍA

Paso 1 – Aplica la fórmula:

- Disponibilidad = Uptime / (Uptime + Downtime)
- Disponibilidad = 525 500 / (525 500 + 25) = 525 500 / 525 525 ≈ 0,999952

Paso 2 – Convierte a porcentaje: 0,999952 × 100 = 99,9952 %

Reflexión final (puedes comentarme tus reflexiones por el chat):

- ¿Se cumple el estándar de "cinco nueves" (99,999 %)?
- ¿Qué medidas podrían adoptarse para mejorar la disponibilidad?

IMPORTANTE

Conseguir niveles de disponibilidad superiores al **99,9 % implica inversiones significativas en hardware redundante, virtualización, redes, climatización y mantenimiento especializado.** Por esta razón, cada organización debe **evaluar cuidadosamente el equilibrio entre el nivel de disponibilidad necesario y los recursos disponibles para alcanzarlo.**

5.6. Inventariado del hardware

El **inventariado de hardware** es una práctica esencial en toda organización que utilice recursos tecnológicos. Consiste en llevar un **registro completo y actualizado de todos los dispositivos físicos disponibles**, con el objetivo de tener control sobre los activos, planificar mantenimientos, evitar pérdidas y optimizar la toma de decisiones.

Un inventario bien gestionado permite conocer **qué equipos hay, dónde están ubicados, quién los utiliza y en qué condiciones se encuentran**, lo cual es especialmente importante para los departamentos de TI y gestión empresarial.

La mayoría de los sistemas de inventario modernos utilizan **códigos de barras** o **etiquetas QR** para identificar de forma rápida y precisa cada dispositivo, minimizando errores humanos y mejorando la eficiencia en la gestión.

EJEMPLO PRÁCTICO

Si una empresa debe desplegar una nueva red local, pero no sabe cuántos metros de cable tiene en almacén o qué switches están disponibles, es probable que haga compras innecesarias o retrase el proyecto. El inventario permite **anticiparse a estas situaciones y optimizar recursos.**

5.6.1. Por qué es necesario tener un sistema de inventario hardware

Las razones para mantener un correcto inventario de hardware son las siguientes:

- **Reducción de gastos:** evita compras innecesarias al conocer el material disponible.
- **Facilita la toma de decisiones:** permite saber qué equipos pueden reutilizarse o deben actualizarse.
- **Disminuye riesgos de pérdida o robo:** se puede asignar un responsable a cada dispositivo.
- **Valoración del patrimonio tecnológico:** registra el valor económico de todos los activos informáticos.
- **Control de garantías:** facilita el seguimiento de las garantías de fábrica y servicios técnicos.
- **Prevención de fallos y obsolescencia:** al conocer la vida útil de los equipos, se pueden planificar sustituciones.

5.6.2. Control del inventario hardware de una empresa

Existen tres métodos principales para gestionar el inventario de hardware de nuestra empresa u organización:

- **Hojas de cálculo.** Este es el método más sencillo, pero menos sofisticado. Salvo causas de fuerza mayor, su uso no es recomendable debido a su baja seguridad. Las hojas de cálculo no están destinadas al almacenamiento de datos de este tipo.
- **Ficheros o bases de datos.** Este método es más avanzado que las hojas de cálculo, pero sigue sin ofrecer una manera automática de registrar los activos. Aunque algunos cuentan con una interfaz gráfica, todos los datos deben ser insertados manualmente. Un punto a favor es que a veces podemos acceder a ellos vía web desde cualquier dispositivo sin necesidad de la instalación de aplicaciones adicionales.
- **Software de control de inventario automático.** Esta es la mejor de las tres opciones porque siempre se actualizará automáticamente. Estos programas o aplicaciones recogen los datos de manera automática y mantienen una conexión con el equipo para poder rastrear cambios como actualizaciones de antivirus o modificaciones de configuración que es necesario tener en cuenta. Con esto, nos ahorraremos muchos problemas futuros al tener siempre información actualizada sobre el software importante del ordenador, por ejemplo, a la hora de adquirir licencias.

IMPORTANTE

Todo programa de control de inventario debe cumplir con las siguientes funciones para ser óptimo en la realización del inventariado:

Características que debe cumplir un buen sistema de inventario

Para ser efectivo, cualquier software de inventario debe incluir las siguientes funciones mínimas:

- **Recogida automatizada de datos técnicos de los equipos.**
- **Posibilidad de registrar datos administrativos** (fecha de compra, garantía, responsable, ubicación…).
- **Acceso remoto vía web,** para una gestión centralizada.
- **Historial de cambios en cada dispositivo.**
- **Sistema de alertas** sobre modificaciones no autorizadas, software malicioso o configuraciones críticas.

Ejemplos de software de inventario automatizado

- **GLPI** (software libre de gestión de servicios).
- **iTop** (software de código abierto para la gestión de servicios).
- **Jira + Asset Management.**
- **OCS Inventory NG.**
- **Spiceworks IT Asset Management.**

www.universae.com