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

Hoy en día lo más normal en una empresa es que esta cuente con un sistema informático en su estructura para poder llevar a cabo su procesamiento de información. Y de manera lógica, este sistema tendrá más o menos complejidad dependiendo del tamaño e importancia de la empresa.

Estos sistemas suelen ser críticos para la empresa además de que cuanto mejores sean los sistemas, más competitiva deberá de ser la empresa en su sector.

Como son tan importantes, hay que asegurar en ellos fiabilidad, disponibilidad, eficiencia e integración para todos los ámbitos de la empresa.

5.1.1. Los mainframes

Los mainframes aparecen en la década de los 50 y experimentan evolución constante conforme van surgiendo nuevos retos tecnológicos.

Hoy en día se siguen usando *mainframes* en muchas empresas a la hora de la protección de los datos y para ejecutar ciertas aplicaciones, como pueden ser las de *deep learning*.

Una empresa y sus clientes quieren asegurarse de que los datos que albergan se encuentran protegidos y que, además, los servicios ofertados van a estar disponibles en la gran mayoría del tiempo, lo que hace necesario que haya una centralización de los datos.

Los servidores *mainframe* ofertan que los datos se encuentren cifrados de manera muy fiable.

Esto hace que, aunque se procesen muchísimas transacciones, se encuentren protegidos frente a ataques externos e internos. La disponibilidad del servicio, además, suele ser de un 99,999%.

Este tipo de servidores suelen usar sistemas operativos hipervisores, como pueden ser:

- Proxmox
- Citrix XenServer

5.1.2. Cloud Computing

Esta tendencia de informática en la nube se está usando cada vez más debido a sus incontables beneficios para las empresas.

Es una táctica empresarial muy usada debido a que no es necesario que se aporte un capital extremadamente alto en un principio y, además, tampoco hay que invertir mucho tiempo y recursos en administración de numerosos equipos o seguridad, ya que de esto se encargará el proveedor.

El funcionamiento siempre es el mismo: se contrata el servicio en la nube y se configura y administra a través de una interfaz web; por otro lado, el proveedor posee los recursos que se administran y se encarga de su mantenimiento *hardware*.

Las ventajas o beneficios de estas arquitecturas son principalmente:

- 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 Infraestructure as a Service. Infraestructura como servicio.** La manera más similar a una administración básica de una organización. Se otorga acceso a las características de red, a los equipos y las bases de datos. El cliente puede administrarlo prácticamente todo ya que es la más flexible de todas.
- **PaaS, Platform as a Service.** No se realiza ninguna tarea de mantenimiento. El cliente únicamente tiene que dedicarse a la administración de las aplicaciones que él vaya instalando.
- **SaaS, Software as a Service.** El cliente no tiene que hacer nada, y que el mismo servicio se encarga también de instalar aplicaciones y administrarlas. Esto se usa muchas veces en aplicaciones muy específicas como el correo electrónico de una empresa entera. Es de los tipos más usados debido a que no se necesita de personal especializado para ejecutarlo e incluso administrarlo con el proveedor.

Tenemos también, diferentes maneras para implementar el *cloud computing*:

- **Totalmente en la nube.**
- **Híbrida.**
- **On-premise.** Esta implementación también se llama *nube privada* y hace referencia a una virtualización en la nube por parte de la propia empresa. Esto se suele usar cuando se necesitan de recursos dedicados que no deban de ser compartidos con otras empresas. Es igual que la estructura clásica, pero virtualizados en la nube.

5.1.3. Ordenadores virtuales

Los ordenadores virtuales son máquinas que se alojan en la nube y a las que accedemos por medio de un escritorio virtual. Estos se están usando cada vez más en las empresas.

Mientras que en un equipo físico quedamos restringidos a los recursos de dicho equipo y en caso de querer cambiarlos debemos de esperar, en un ordenador virtual no. Cuando tenemos un ordenador virtual podemos cambiar la configuración cambiando clics, lo que hace que en cuestión de minutos podamos tener muchos más recursos en nuestra mano. Esta es la mayor diferencia y es llamada escalabilidad.

Funciona exactamente igual que una máquina física. Instalando las mismas aplicaciones o sistemas, pero, por lo tanto, también debe de ser protegido de igual forma.

No importa en que dispositivo estemos mientras que tengamos autorización. Desde cualquier sitio se podría acceder al escritorio virtual y no se observarían cambios.

Por último, comentar como hemos dicho, que se necesita de autorización para acceder a estos ordenadores y que cualquier intercambio de datos va a ser cifrado, al igual que su acceso.

5.2. Estructura de un CPD. Organización

Los CPD o *Centros de procesamiento de datos* son la ubicación de una empresa destina a guardar de manera segura todos los recursos informáticos necesarios para el desempeño de sus funciones.

Aquí, no se guardan ordenadores de sobre mesa o de usuario, lo que se almacena son servidores, *switches*, etc. Los CPD han ido perdiendo importancia y presencia con la aparición del *Cloud Computing*.

La principal función del CPD es que el servicio siempre se encuentre activo, para lo que es necesario en muchos casos que la infraestructura sea lo suficientemente sólida.

Además de asegurar disponibilidad, en un CPD debemos de contar con una seguridad física y lógica para asegurar la información almacenada.

Los principales requisitos con los que debe de contar un CPD son:

- **Diseño.** Es importante que el CPD tenga un diseño concreto de anchura, altura, espacio, etc.
- **Seguridad física del local.** Debe de haber instalados elementos contra incendios e inundaciones para asegurar el mantenimiento de los dispositivos en caso de accidente.
- **Suministro eléctrico.** El suministro eléctrico debe de ser ininterrumpido y asegurar su funcionamiento mediante SAI.
- **Aislamiento acústico.** Muchas máquinas funcionando al mismo tiempo producen mucho ruido, por lo que es importante que cuente con un gran aislamiento para dejar trabajar en los lugares continuos y no perjudicar la saludo.
- **Ubicación.** No debe de construirse un CPD en un sitio propenso a accidentes y menos donde se puedan dar desastres naturales:
  - De manera general, no se suelen ubicar en sótanos por el peligro de inundaciones, la dificultad de escapar del fuego y el peso de las máquinas.
  - Se suelen ubicar en plantas intermedias o zonas centrales del complejo empresarial.
  - No suelen tener ventanas al exterior por seguridad y privacidad.
- **Temperatura y humedad.** Deben de controlarse ambos factores porque en un CPD las máquinas producen mucho calor y, además, la humedad puede que deteriore los dispositivos. La temperatura óptima no debe de superar los 16ºC y la humedad no debería de ser superior al 20%. Se necesita también un correcto sistema de ventilación y filtración del aire.
- **Diseño y dimensiones:**
  - El suelo debe de poder soportar mucho peso. Lo suyo es que se encuentre reforzados y sean capaces de almacenar hasta 2000 kg por metro cuadrado.
  - La distancia entre techo y suelo debe ser mínimo de dos metrosy medio.
  - Para poder pasar y organizar cables, se recomienda el uso de falso suelo y techo.
  - La iluminación debe de ser cuidadosa
  - Las puertas deben de ser suficientemente grandes como para que dejen paso a la maquinaria.

5.3. Seguridad física

Una empresa debe siempre de estar protegida frente a cualquier situación que se pueda presentar y que comprometa su actividad.

A una empresa pueden afectarle múltiples factores económicos, demográficos, ambientales, etc. Además de todos estos factores, es importante que haya planteado un plan de seguridad lógica y física frente a amenazas externas e internas. Hoy en día es común el robo de patentes tecnológicas y de ideas, para lo que también es necesario que se establezca un adecuado nivel de seguridad y privacidad.

La ubicación física del complejo empresarial también es importante, pues dependiendo de donde esté situada, será más o menos propensa a catástrofes naturales como inundaciones o terremotos.

Los riegos por vecindad también tienen que ser evaluados en la ubicación de una empresa, ya no solo por tener cerca empresas competidoras, sino porque haya una buena comunicación, que llegue correctamente la red o la corriente eléctrica y que no esté situada cerca de sitios peligrosos como centrales termonucleares, por ejemplo.

Además de tener en cuenta todo esto, la seguridad física de la empresa también se encarga de preservar el funcionamiento de sus activos. Estos activos se clasifican en nivel de importancia para la empresa, y, dependiendo de este nivel, tendrán más o menos protección.

Por ejemplo, un *switch* que da red a toda la dirección de la organización habrá que protegerlo más que uno que únicamente da a unos pocos usuarios de un departamento de menor importancia.

La medida que hasta ahora ha resultado ser más efectiva es la de los *controles de acceso*. En un control de accesos, solo los trabajadores autorizados podrán acceder a las diferentes zonas de la empresa, como puede ser el CPD,

Si se quiere acceder sin tener autorización, se necesitará una justificación del responsable de manera expresa y, además, estos controles guardan registro de quien accede a los diversos sitios para posteriormente poder auditar los controles.

Los controles de acceso más comunes son:

- **Códigos de acceso.** Es uno de los más débiles porque un atacante podría obtener el código y acceder sin autorización. Estos controles solo nos dicen a quién pertenece el código, pero no quien lo usa.
- **Bandas magnéticas.** Volvemos a lo mismo de antes, estas bandas no verifican la identidad de quien entra. Eso sí, esta es más difícil de burlar porque se necesita de un elemento físico para el acceso.
- **RFID.** Funcionan exactamente igual que las bandas magnéticas, pero en este caso es menos costoso y más fácil de implementar.
- **Biométrico.** La forma de acceso más segura, pues se necesita de un elemento del usuario como puede ser la huella dactilar o el escáner de retina para el acceso, De este modo aseguramos que siempre es la persona que se identifica quien entra.

No solo se usan los mecanismos de acceso para la seguridad física, sino también el sistema de vigilancia. Hay varias formas de vigilar los activos de una organización, como pueden ser:

- Utilización de personas.
- *Utilización de sensores* de acceso, temperatura, movimiento, que alerten en caso de que se cumpla con los parámetros que se usen.
- Utilización de cámaras de seguridad.

5.4. Componentes específicos en soluciones empresariales

Vamos a ver en los siguientes puntos, los principales elementos que usan las empresas para garantizar ciertos niveles de seguridad.

5.4.1. Los SAI. Sistemas de alimentación ininterrumpida

Los SAI son *sistemas redundantes de suministro eléctrico* que se usan para seguir suministrando corriente eléctrica a los aparatos en caso de un corte del suministro momentáneo.

Hay también otros tipos de SAI, que por otro lado son bastante más profesionales y realmente lo que hacen es dar una señal totalmente estable a nuestros dispositivos sin importar como sea la señal eléctrica original y las perturbaciones o alteraciones que sufra.

Dentro de un SAI nos encontramos que existen tanto rectificadores como reguladores de tensión eléctrica para que el equipo no sufra ninguna consecuencia en caso de bajada o subida de tensión eléctrica instantánea.

Aunque tener un SAI es algo bastante recomendable, en empresas en la que su información se almacene en servidores, o en las que estos se usen para cualquiera tarea, tener uno de estos sistemas es prácticamente de carácter obligatorio. Esto es debido a que un apagado inesperado de un servidor puede causar consecuencias nefastas para la organización.

Defectos de la señal eléctrica

IMPORTANTE

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

Las señales eléctricas no son perfectas, sufren diversas alteraciones y dependiendo de que defecto o alteración sufra, los dispositivos electrónicos pueden tener unos u otros problemas.

La siguiente imagen refleja los defectos más comunes de las señales eléctricas:

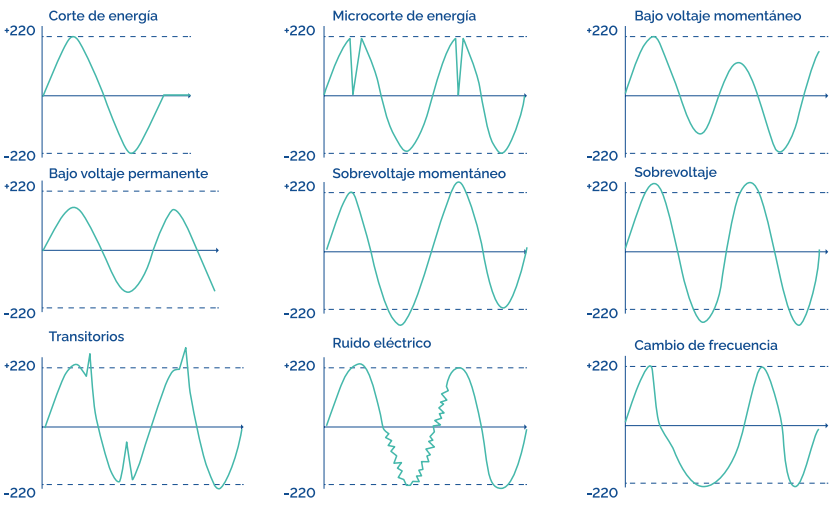

Imagen 1. Defectos de la señal eléctrica

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:

Imagen 2. Tipos de SAI

SAI stand by u offline

Estos son los tipos de SAI más económicos y los de menor capacidad. El interruptor de transferencia de corriente se activa cuando una anomalía en la red eléctrica sucede. So se acciona dicho interruptor, el equipo comienza a coger la corriente del SAI a través del inversor.

No se filtra la señal en ningún momento y se recomienda su uso en sitios donde la señal eléctrica no suele sufrir alteraciones ya que se no se pueden solventar, su principal uso recomendado es el doméstico. Si se necesitan más de 2000 VA tampoco son recomendables.

Su funcionamiento se describe en la siguiente ilustración:

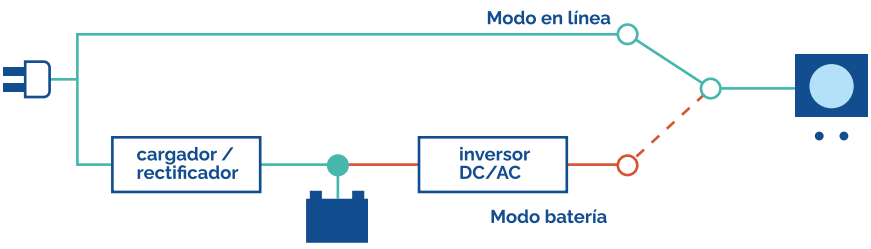

Imagen 3. Funcionamiento de un SAI offline

SAI interactivos

Este tipo de dispositivo es más sofisticado que el anterior ya que incorporan la función AVR. La corriente solo se demanda en caso de fallo de señal, para poder preservar la vida de esta.

Muy eficaces y fiables, no se recomiendan en casos en los que se necesitan más de 5000 VA.

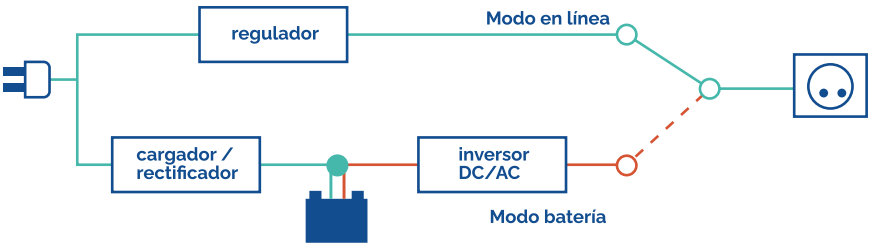

Imagen 4. Funcionamiento de un SAI interactivo

SAI *online* u *online* de conversión *Delta*

Es el tipo de SAI más sofisticado que existe, con el inversor siempre en funcionamiento para que la señal que llega a los equipos conectados siempre provenga del SAI.

Esto hace que la señal que reciben los equipos sea la de mayor calidad y estabilidad. Se suelen usar estos dispositivos en salas de servidores, sistemas de videovigilancia o maquinaria industrial y crítica.

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

   Independientemente del tipo de SAI que sea, un parámetro que hay que tener en cuenta siempre que vayamos a instalar un SAI, es la carga que es capaz de procesar, es decir, cuantos equipos a la vez podemos tener conectados.

   Esta carga la solemos expresar en voltios-amperios (*VA*).

2. **Qué es la autonomía de un SAI**

   La autonomía de un SAI es el tiempo que este puede estar dando corriente a los equipos sin estar conectado directamente a la red eléctrica. Para esto es necesario también tener en cuenta la carga del SAI, puesto que más equipos conectados, menor tiempo de suministro.

   Por ejemplo, un SAI con el 40% de carga que puede ofrecer 40 minutos de autonomía, con el 80% de carga, ofrecerá sobre los 20 minutos de autonomía.

5.4.2. El almacenamiento empresarial en la nube

La memoria en la nube ha cobrado en los últimos años una gran importancia al nivel de que ya se implanta en cualquier empresa e incluso en dispositivos domésticos.

Vamos a explicar que es el almacenamiento en la nube con un ejemplo que vamos a contar a continuación:

Todos hoy en día, o casi todos, manejamos *smartphones* y estos obligan a añadir una cuenta de correo electrónico para trabajar, en el caos de Android de Gmail y en el caso de Apple, su ID. Bien, estas plataformas llevan consigo aplicaciones como Google Drive en el caso de la primera e *iCloud* en el caso de la segunda.

Las dos son aplicaciones de almacenamiento en la nube.

Otros ejemplos serían, *OneDrive* o *Dropbox*.

5.4.3. Servidores de almacenamiento empresarial

El almacenamiento de la información es algo fundamental para una empresa como hemos comentado en otras ocasiones. Es por esta razón anterior por la que se implementan dispositivos de red o servidores en las redes de almacenamiento.

Servidor SAN

El llamado servidor SAN, siglas de *Storage Area Network*, es un servidor de almacenamiento que se encuentra ubicado en la red empresarial y que se conecta al sistema general mediante un cable de fibra óptica, lo que indica que nos dará las mejores prestaciones posibles.

Estos servidores son muy caros y escalables, ya que hay ocasiones en los que estos servidores tienen miles de terabytes, e incluso *petabytes* de almacenamiento.

Almacenamiento *flash*

En los servidores de almacenamiento SAN el sistema de almacenamiento usado ya no es el mecánico, hace mucho tiempo que usan tecnologías *flash* y NVMe, para conservar el gran rendimiento y fiabilidad.0

Almacenamiento en *VVols*

Los volúmenes virtuales, cuya abreviación y termino más usado es *VVols* son volúmenes creados de manera virtual donde se encapsulan los archivos que componen una máquina virtual en su totalidad.

Como se ha dicho en algunas ocasiones, lo más usado hoy en día son los servidores virtualizados por sus numerosas ventajas.

El almacenamiento basado en *VVols* que usan los servidores SAN nos ayudan a que se pueda gestionar todos los datos de las máquinas almacenadas con un único GUID, como si solo hubiera un disco.

Almacenamiento de objetos

Otra tecnología que está en auge es el almacenamiento de objetos como sustitutivo del tradicional almacenamiento de archivos.

Esto se usa sobre todo porque estos objetos no tienen que anidarse como pasaba con los archivos y los directorios, porque los guardamos en un único repositorio.

Con el sistema de almacenamiento de objetos se gana mucho en eficiencia. Su funcionamiento es el siguiente: el servidor asigna un identificador único a un objeto y lo aloja en un espacio de direcciones plano, de modo que con el identificador es muy sencillo acceder al recurso.

Otra ventaja de este sistema es que se soluciona el problema dado por el almacenamiento de archivos que era el problema con el crecimiento de los datos; las empresas pueden ir añadiendo cada vez más almacenamiento conforme a sus necesidades sin problema ni reestructuración alguna.

Como mayor ejemplo de esta tecnología tenemos *Amazon Simple Storage*, el más usado por las grandes empresas.

5.5. Arquitecturas de alta disponibilidad

Cuando hablamos de alta disponibilidad, nos referimos a una disponibilidad prácticamente total, es decir, deseamos que el sistema funcione las 24 horas del día durante los 7 días de la semana, aludiendo al famoso termino 24/7.

Cuando queremos tener alta disponibilidad en un sistema operativo, lo deseamos en un equipo con prestaciones suficientes, porque los equipos de oficina o doméstico no están ni fabricados ni pensados para cubrir estas necesidades.

Cuando una empresa implementa un sistema de alta disponibilidad, necesita la certeza de que, salvo fallo inesperado, el sistema va a funcionar de manera correcta y eficiente todo el tiempo que se necesita, en caso contrario podría causar consecuencias bastantes graves como perdidas de información o corrupción de datos.

Cuando hablamos de alta disponibilidad, hay una serie de términos muy importantes que tener en cuenta:

- **Fiabilidad.** Se trata de una probabilidad que nos indica si pueden haber o no fallos en el sistema durante un cierto tiempo determinado. En alta disponibilidad necesitamos de una fiabilidad muy alta.

  A mayor tiempo sin que ocurra ningún fallo, mayor fiabilidad tenemos. El fallo que considerar para esta medición vendrá determinado por el administrador del servicio.

- **Disponibilidad.** Probabilidad del sistema de que durante un tiempo esté siempre accesible y en funcionamiento. La disponibilidad solemos expresarla como un porcentaje de funcionamiento al año basándonos en la formula siguiente:

Disponibilidad = Uptime/(Uptime + Downtime)

Nos referimos a *uptime* como el tiempo que el sistema se encuentra en funcionamiento y a *downtime* como el tiempo en el que el sistema no otorga ningún servicio. Los tiempos los expresamos en minutos.

El índice deseado en disponibilidad es el de cinco nueves, es decir, 99,999% de disponibilidad.

5.6. Inventariado del hardware

Cuando realizamos un inventariado, lo que queremos es tener controlado y registrado todo el material que tenemos disponible. En nuestro caso específico, el *hardware* almacenado.

La mayoría de *software* de inventariado usan códigos de barras para poder identificar de manera correcta y eficiente los productos o dispositivos intentando minimizar los errores.

En la mayoría de las empresas, un correcto control de productos y dispositivos mediante el inventariado es fundamental.

En nuestro caso, si, por ejemplo, necesitamos montar una red nueva, y no sabemos cuántos cables tenemos disponibles, no sabremos entonces cuantos adicionales hemos de pedir.

El gestor de la empresa también usará el inventario para saber si tiene que tomar unas decisiones u otras acerca de, por ejemplo, los sistemas a implantar en toda la empresa.

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

Las razones para llevar un correcto inventario *hardware* son las siguientes:

- Se reduce el gasto porque tenemos controlados todos los disponibles de la empresa.
- Al saber los dispositivos que tenemos disponibles, su software, y sus prestaciones, podremos tomar decisiones acerca de nuevos equipos o actualizaciones con mayor facilidad.
- Evitamos que sucedan robos, perdidas o malgasto de fondos.
- Conocemos el valor total de los activos informáticos de la empresa.
- Podemos mantere un control sobre la garantía de los dispositivos.
- Podemos tener más o menos previsto los fallos más comunes de *hardware* y la vida útil de los dispositivos.

5.6.2. Control del inventario hardware de una empresa

Tenemos tres métodos que podemos usar para gestionar el inventario *hardware* de nuestra empresa u organización:

- **Hojas de cálculo.** Se trata del más sencillo, pero menos sofisticado de todos. Salvo causas de fuerza mayor, no se conseja su uso `por su poca seguridad.

  Las hojas de cálculo no están destinadas al almacenamiento de datos de este tipo.

- **Ficheros o bases de datos.** El uso de estos es algo más avanzado que las hojas de cálculo, pero tampoco es el más sofisticado, sigue sin existir una manera automática de registrar los activos.

  Aunque tienen una interfaz gráfica de algún modo en ciertos casos, todos los datos se van a insertar de manera manual.

  Una ventaja es que a veces podemos acceder vía web desde cualquier dispositivo sin necesidad de la instalación de terceras aplicaciones.

- **Software de control de inventario automático.** Esta es la mejor de las tres opciones porque siempre va a actualizarse de manera automática.

Estos programas o aplicaciones recogen los datos de manera automática y tienen cierta conexión con el equipo para poder saber si han cambiado de versión de antivirus, por ejemplo, si está desactualizado o si ha habido un cambio de configuración que es necesario tener en cuenta.

Con esto, nos ahorraremos muchos problemas futuros al saber siempre que *software* de importancia tiene el ordenador, por ejemplo, a la hora de adquirir licencias.

Todo programa de estas características debe de cumplir con las siguientes funciones para que sea óptimo a la hora de realizar el inventariado:

- Automatizar la recogida de los datos de los dispositivos *hardware* de la empresa.
- Permitir que en la ficha de equipo se puedan añadir datos de carácter administrativo como garantías, licencias, o servicio técnico disponible, así como el usuario y departamento responsable de dicho equipo.
- Si podemos acceder vía web a este aplicativo, ganamos en gestión y administración, pero no es indispensable.
- Registrar todos los cambios o modificaciones hechas en las fichas de los dispositivos.

Sistema de notificación de modificaciones. Con esto podemos estar alerta sobre *software* no permitidos o maliciosos.

Ejemplos de aplicaciones que ofrecen este servicio son: *GLPI, Jira, iTop.,* etc.

www.universae.com