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

Caso práctico

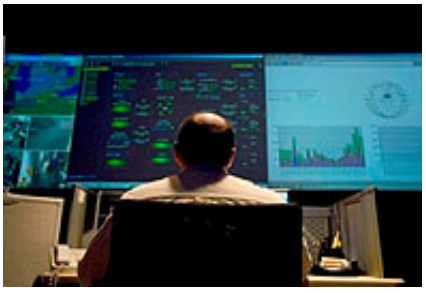
La gerencia de nuestra empresa EntreTuyYo, S.L. estudia realizar inversiones en el área informática.

Ese estudio deberá valorar la necesidad de implantar un Centro de Proceso de Datos (CPD) tanto por su aporte estratégico como por su aporte funcional a la empresa.

Desde gerencia nos pide que el nuevo CPD debiera dar soporte tanto a las dependencias de la propia empresa como a delegaciones territoriales mediante conexiones remotas.

Una vez que la gerencia tenga el informe, deberá evaluar si su coste económico puede asumirlo la empresa o se decide delegar en terceros.

Por esta razón, nos pide al departamento de informática un informe de los requerimientos necesarios para la instalación y puesta en funcionamiento de un CPD. Así como, dentro del propio informe, de la repercusión que afectará al funcionamiento del resto de departamentos y qué estrategia debería seguir la empresa en general para adaptarse a la nueva situación.



El jefe del departamento de informática nos ha repartido el trabajo. A mí me ha tocado ver el inventario de todo el hardware y software de la empresa. Debo emitir un informe indicando la vigencia, tanto de los equipos informáticos como del software soporte y demás aplicaciones, para su posterior adaptación al sistema del CPD.

Arquitecturas de ordenadores personales, sistemas departamentales y grandes ordenadores.

Caso práctico

Partiendo de la idea primigenia de ordenador: **Computadora** u **ordenador** es una máquina capaz de aceptar información de entrada, efectuar operaciones lógicas y aritméticas, y proporcionar la información resultante a través de un medio de salida, todo ello sin intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en el mismo.

En esta definición pueden englobarse todo tipo de máquinas que realicen esta función. Desde un ordenador personal hasta un mainframe pasando por equipos tales como ordenador de bolsillo, consolas de videojuego, etc.

A partir de aquí podemos crear una división por tipos de ordenadores y sus características principales.

Tipos y subtipos de ordenadores. Tipo Subtipo Descripción Ordenadores personales: Sistemas servidores:

Terminales, netPC.	Necesita un servidor conectado en red.
Microordenador (PC).	Trabajo, aplicaciones genéricas.
Estaciones de trabajo (workstations).	De gran potencia. Utilizado en trabajos de ingeniería.
Portátil, netBook.	Microordenador portátil y con menos prestaciones.
PDA y teléfono móvil.	Microordenador pequeño con pequeñas prestaciones.
Miniordenadores.	También se les domina ordenadores departamentales.
Mainframes.	De gran capacidad. Tanto en procesamiento como en almacenamiento, comunicaciones, etc.

Superordenadores.	Ordenadores de gran potencia y elevadísimas prestaciones.

Autoevaluación

¿Se puede utilizar un móvil 3G y conectar con un servidor, de forma remota?
No, ningún móvil puede conectarse a ninguna red de área local.
Sí. No hace falta ninguna configuración adicional.
Sí, sólo puede conectarse a través de un sincronizador.
Sí, pero debe estar el router de la LAN configurado para que el móvil u otro equipo (por ejemplo ordenador) pueda llegar hasta dicho equipo.

Ordenadores personales.

Los ordenadores personales o PC's son computadoras de uso típico en oficinas o entornos llamados SOHO.

Para este tipo de equipos no se requieren grandes prestaciones (habitualmente se les denomina, también, ordenadores estándar). Suelen trabajar con gráficos 2D en resoluciones no muy altas. Permiten que haya comunicaciones entre distintos equipos y ordenadores, así como tener la posibilidad de acceder a Internet. Y su precio es relativamente bajo.

Podríamos englobar en este tipo de ordenadores a aquellos calificados como portátiles.

Para clasificar este tipo de ordenadores podemos tomar como referencia la siguiente tabla:

Tipos de ordenadores personales. Tipo de ordenadorImagenDescripciónTerminal Microordenador Portátil, tablet-PC Pda (personal digital assistent) y teléfono móvil.

	Es un ordenador que necesita de un servidor para realizar tareas propias de un ordenador. Sólo tiene el software necesario para arrancar y comunicarse con un servidor remoto (LAN o Internet). Se les denomina terminal "tonto".
	Llamados popularmente PC. Podemos distinguir entre equipos preparados para el hogar o para oficinas.

	Dependiendo de la utilidad variará las características. Pero, básicamente, su arquitectura es la misma.
	Los portátiles, tablets-PC; son, realmente, microordenadores pero transportables.
	Se emplean como sustitución de agendas y apoyo a las comunicaciones y son todo un mercado emergente con el abaratamiento de costes. Actualmente las PDAs están integradas en los teléfonos móviles. Tiene una serie de funciones típicas: cuaderno de notas, calendario, agenda, ofimática básica, GPS, WI-FI, etc.

Servidores (I).

Por definición, **un servidor es un ordenador que**, formando parte de una red (local o intranet, extranet, Internet) **provee de servicios a otros ordenadores denominados clientes.**

También es verdad que se llaman servidores a aquellas aplicaciones que realizan algunas tareas en beneficio de otras aplicaciones llamadas clientes.

Tipos de servidores. Tipo de servidor Utilización conceptual Servidor de archivo. Servidor de impresiones. Servidor de correo. Servidor de fax. Servidor de la telefonía. Servidor proxy. Servidor del acceso remoto (RAS). Servidor de uso. Servidor web. Servidor de Base de Datos. Servidor de reserva.

Es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.
Controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión.

Almacena, envía, recibe, enruta y realiza operaciones relacionadas con correo electrónico para los clientes de la red.
Almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
Realiza funciones relacionadas con la telefonía: como es la de contestador automático, funciones de sistema interactivo para la respuesta de la voz, encaminando las llamadas y controlando también la red o el Internet (VoIP).
Realiza cierto tipo de funciones para otros clientes de la red y, así, aumentar el funcionamiento de ciertas operaciones. También suele proporcionar servicios de seguridad como cortafuegos.
Controla las líneas de módem u otros canales de comunicación de la red externa para que dichas peticiones conecten con la propia red. Reconoce la petición de la red y realiza autentificación y otros procedimientos necesarios para registrar a un usuario en la red.
Realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que realice las operaciones de un puesto de trabajo y sirviendo, a su vez, los resultados. Mientras que en el puesto de trabajo se realiza la interfaz del operador (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.
Almacena documentos HTML, imágenes, archivos de texto, multimedia, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que solicitan en la red. También almacena programas y guiones (programas interpretados).
Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor.
Tiene el software de reserva de la red instalado y tiene gran cantidad de datos almacenados de la red en discos duros u otras formas de almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clúster.

Servidores (II).

Una vez hechas las divisiones de servidores de forma lógica, debemos realizar una separación de ordenadores desde el punto de vista físico, de la máquina.

Tipos de ordenador como servidor. Tipo de servidorImagenDescripciónMiniordenador Mainframe Superordenador

Es una clase de ordenador multiusuario, que se encuentra en el rango intermedio del espectro computacional; es decir, entre los grandes sistemas multiusuario (mainframes), y los más pequeños sistemas monousuario (microordenadores o PCs).

Un ordenador central o mainframe es una computadora grande, potente y costosa usada principalmente por una gran compañía o institución para el procesamiento de una gran cantidad de datos; por ejemplo, para el procesamiento de transacciones bancarias.

Supercomputadora o superordenador es aquella con capacidades de cálculo muy superiores a las comunes, según la época. Por ejemplo: MareNostrum utiliza nodos BladeCenter JS21 con procesadores duales IBM PowerPC 970FX de 64 bits a una velocidad de reloj de 2,2 GHz. El superordenador cuenta con una capacidad de cálculo de 62,63 Teraflops con picos de 94,208 Teraflops.

Para saber más

Una visión general de qué es un Miniordenador.

Miniordenador

¿Qué es un ordenador central?

Mainframe

Más información en Wikipedia sobre superordenadores.

Superordenador

Sirva como ejemplo un superordenador.

MareNostrum

Del entorno personal al entorno empresarial.

Caso práctico

El departamento de recursos humanos de nuestra empresa EntreTuyYo, S.L. nos solicita asesoramiento al departamento de informática para confeccionar diversos test aptitudinales que se utilizarán para valorar los conocimientos informáticos de los aspirantes a diversos puestos dentro de la empresa.

Después de reunirnos, el departamento de informática determina enviarles varios test dependiendo del nivel de informática que requiere cada uno de los distintos puestos. Desde un nivel de usuario a un nivel avanzado.

Dependiendo de la utilización de los equipos informáticos, (personal, oficina, empresarial, etc.), los sistemas informáticos deberán tener una arquitectura y unas prestaciones específicas para que cumplan con la función o funciones por las que han sido adquiridos.

Podemos estudiar los tipos de arquitectura clasificándolos en función de qué tareas pueden o están destinados a realizar.

Ordenador y su función. Ordenador Función Descripción Ordenador personal Sistemas servidores Equipos empotrados

PC para ofimática	Suele utilizarse para trabajar con aplicaciones ofimáticas y genéricas, como aplicaciones de contabilidad o de facturación.
Estaciones de trabajo (Workstation)	Deben tener altas prestaciones. Destinados para trabajos técnicos o científicos. Suelen estar conectadas a otros ordenadores, servidores, mediante la red de datos a través de una tarjeta de red.
Hogar	Estos tienen la característica de utilizarse para ofimática y juegos.
Portátiles	Similar al PC pero debido a su transportabilidad deben ser reducidos de tamaño y peso y esto redunda en menor capacidad de desarrollo.
PDA y telefonía	Su tamaño limita mucho sus prestaciones. Aparte del uso de

móvil	telefonía, se utiliza para aplicaciones ligeras. Estas suelen sincronizarse con ordenadores mediante técnicas como bluetooth.
Servidores de ficheros, web, correo, etc.	Su función es permitir el acceso remoto a archivos almacenados en él o accesibles por este. Cualquier ordenador conectado a una red, con un software apropiado, puede funcionar como servidor de archivos. Pero es aconsejable un equipo con hardware adecuado.
Servidores de almacenamiento masivo	Similar a los servidores de ficheros. Su diferencia estriba del uso que se da. Contienen dispositivos de almacenamiento masivo grandes y rápidos para dar el servicio correctamente.
Servidores de aplicaciones y cálculo	A diferencia de los anteriores, su procesador debe ser potente. Y se considera necesario que tenga más de un procesador con capacidad de sincronización entre ellos.
Equipos industriales	Son equipos especializados en realizar tareas específicas de índole industrial. Suelen tener conectados equipos robotizados.
Equipos especializados	Hoy en día hay ordenadores que realizan tareas muy específicas. Como GPS, navegadores de coche, multimedia y otros.

Autoevaluación

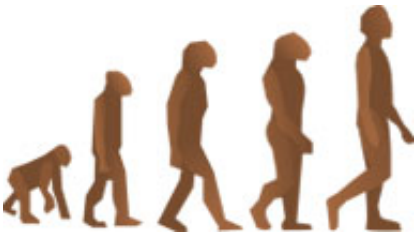
¿Podríamos utilizar un PC de sobremesa como servidor?

Si, con el software adecuado.
No, debe ser un hardware adecuado a servidores.
Si, si añadimos más memoria principal.
No, en ningún caso.

Evolución actual y tendencias en dispositivos hardware.

Caso práctico

El departamento de informática estudia posibles formas de interactuar con los distintos servidores. Desde ordenadores de sobremesa, portátiles, netbooks, PDAs, etcétera. Ante lo cual, realizará un manual de configuración de los distintos dispositivos que puedan interactuar con los servidores y será entregado a los responsables de cada departamento.



El puesto de trabajo en la empresa, en un futuro, no va a ser como lo imaginamos en la actualidad. ¿Por qué? Porque las tareas que se realizan, en muchos de esos perfiles profesionales, se comprobarán que con recursos tecnológicos no requieren de la presencia física en el lugar de trabajo; dentro de las instalaciones de la empresa. Es decir, no requiere la presencia del trabajador en la oficina para atender el teléfono, recibir notificaciones, elaborar documentación, gestionar el correo e, inclusive, mantener reuniones.

Para llevar a cabo este tipo de tareas se emplea lo que se conoce como la informática móvil, que tiene como consecuencia más inmediata la mejora de la productividad laboral. Todo ello gracias a la flexibilidad de horarios y a la motivación del trabajador a través de la conciliación de la vida laboral con la personal.

Formarían parte de esta forma de trabajar la telefonía móvil, a través de potentes móviles y smartphones con sistemas operativos como iOS (iPhone OS), Windows Phone, Symbian, Android o BlackBerry OS, las PDA, que usan Windows Mobile, Palm OS, Symbian e incluso Linux, los NetPC y los portátiles en general así como un conjunto de periféricos que los complementan como webcams, impresoras portables, etc.

Autoevaluación

¿Ahora mismo, hay tecnología suficiente para realizar teletrabajo?:

Sí, pero desde un punto con acceso ADSL.
Sí, hay tecnología pero aún es cara y es difícil controlar al teletrabajador.
No, porque aún se utiliza el papel y siempre se debe realizar en el puesto de trabajo.
No, estamos lejos de conseguirlo todavía.

Para saber más

Información del sistema operativo iOS en la wikipedia.

iOS

Y en la web del propietario.

Apple

El sistema operativo de Windows para dispositivos móviles.

Windows Phone

Otro popular sistema operativo móvil.

Symbian

Estructura de un CPD. Organización.

Caso práctico

Un Centro de Procesamiento de Datos (CPD) es el conjunto de recursos físicos, lógicos y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa.

Las funciones que tiene que desarrollar un CPD son:

Explotación de sistemas y/o aplicaciones.
Soporte técnico a los usuarios.
Gestión y administración del propio CPD.

LOCALIZACIÓN E INFRAESTRUCTURAS

La localización e infraestructura de un Centro de Procesamiento de Datos (CPD) en una empresa debe responder a diversos factores: tamaño de la empresa, servicio que se pretende obtener, disponibilidad de espacio físico adecuado al servicio que debe soportar, distancia desde el CPD hasta las instalaciones que deben dar servicio, etc.

Otros factores en cuanto a su localización e infraestructuras son:

Local físico: Donde se analizará el espacio disponible, el acceso de equipos y personal, instalaciones de suministro eléctrico, acondicionamiento térmico y elementos de seguridad disponibles.
Coste económico: Coste de terreno, locales, impuestos, etc.
Riesgos: De carácter natural, incendios, robos, etc.
Infraestructuras ajenas disponibles: Energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
Espacio y movilidad: Características de las salas, altura, anchura, posición de las

columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
Iluminación: El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
Tratamiento acústico: Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados, por ejemplo en habitaciones donde estén estos equipos aislados.
Seguridad física del local: Se estudiará el sistema contra incendios, teniendo en cuenta que los materiales sean incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.). También se estudiará la protección contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
Suministro eléctrico: El suministro eléctrico a un Centro de Procesamiento de Datos, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

Desde el punto de vista funcional, el CPD tiene una estructura orgánica similar a la siguiente: Director del CPD, Jefes de proyecto, Analistas, Programadores, Jefe de Explotación o del centro de cálculo, Operadores, Técnicos de sistemas, Administradores de la base de datos.

Autoevaluación

¿Un CPD debe tener previsto y seguir funcionando ante un apagón general?

Sí, siempre debe disponer de un generador eléctrico industrial.
No necesariamente, dependerá del objetivo empresarial y del nivel crítico de los datos.
No, en ningún caso.
Ninguna respuesta es correcta.

Para saber más

Diseño y Construcción de Infraestructuras Seguras de CPD.

Aquads

Mapa de la implantación de los CPD en Europa.

Visualweb

Condiciones ambientales.

Caso práctico

Como parte de la respuesta del departamento de informática con respecto a las deficiencias del centro de proceso de datos, se requiere la instalación de un sistema de climatización. El objetivo no es otro que conseguir que los equipos funcionen en condiciones aceptables manteniendo la temperatura y la humedad constantes y conseguir que no se recalienten y, simultáneamente, mantengan un nivel de humedad aceptable.

Llegado a este punto, se solicita asesoramiento de personal técnico cualificado para realizar el estudio de las infraestructuras necesarias y las mejoras apropiadas para el centro.

Las condiciones ambientales de un CPD juegan un papel fundamental, en algunos casos pueden ser determinantes, en el rendimiento óptimo del centro.

Cuando se habla de ambientación, se trata de la climatización de todas las dependencias donde se ubica el CPD.

Es importante que el CPD se adecue a la norma en función del tipo de climatización.

Podemos distinguir dos sistemas de climatización:

Compartido o común a todo el edificio: Es una solución no conveniente. ¿Por qué? Porque coexisten diferentes ambientes climáticos.
Dedicado: Con instalación propia e independiente del resto de la edificación. Puede instalarse una potencia frigorífica adecuada con terminales en uso y en reserva. Permitiría una climatización redundada y protegida.

Existen unos criterios más o menos estandarizados en cuanto a la instalación de la climatización:

Nivel de temperatura: a un metro del suelo, entre 18º y 22º.
Nivel de humedad relativa: a un metro del suelo, entre 40% y 60%.
Nivel de limpieza del aire: se debe tener filtrado el aire evitando en la medida de lo posible tener partículas en suspensión.

Autoevaluación

Para mantener constante la temperatura, ¿podemos abrir las ventanas de la habitación dónde se encuentren los equipos?

Si, conseguiremos que baje la temperatura.
Sólo si hace calor.
No, en ningún caso.
Sí, si la temperatura así lo aconseja.

Para saber más

Podemos apreciar la visión de expertos.

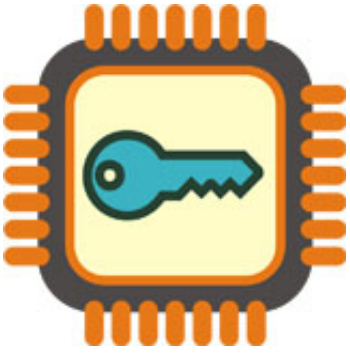
Blog de cliatec

Informe del consejo superior de administración electrónica.

CSAE

Seguridad física.

Caso práctico



Siguiendo con el informe que solicitó la gerencia de la empresa con respecto al CPD, el departamento de informática considera necesaria una infraestructura adecuada para controlar el acceso de personal autorizado a las dependencias. Comprendiendo niveles de acceso y a qué instalaciones puede acceder cada nivel.

El CPD debe disponer de medidas de seguridad que protejan al propio CPD de posibles daños al equipamiento. Bien sean por actos vandálicos, accidentes, catástrofes, accesos no autorizados que provoquen fugas de datos, etc.

El primer sistema que se debe implantar es un sistema de rescate de los datos. Hay momentos que son inevitables, si no se pueden evitar, si podemos mantener uno o varios servidores de reserva implantados en modo clúster que permitan activarlo en cuanto se detecta el fallo. Esto evitaría que el resto de infraestructuras que están conectadas al servidor caído tenga un alto índice de tiempo de inactividad por falta de acceso a los datos.

Como pautas para desarrollar el estudio en cuanto a la seguridad física del CPD podríamos tomar, como referencia, los siguientes puntos:

Acceso externo: Debe existir un control de acceso a las dependencias.
Acceso personal autorizado según nivel de acceso: Base de datos donde quede constancia de todo el personal de acceso, indicando la tarea, horario de permanencia y en qué dependencias tiene acceso.
Controles de seguridad: tarjetas magnéticas, código de barras, lector digital, lector de la retina. Verificar la existencia de alarmas, quien la ejecuta, sonido, donde suena, conexión con la policía, etc.

Estos controles se basan en la utilización de barreras de contención. Como ejemplos podemos apreciar en las imágenes:

1. Control de acceso al edificio.
2. Control de acceso a las dependencias mediante lector de tarjeta y utilizando torniquete como barrera de acceso.

1. En caso de que exista personal ajeno a la empresa (subcontrata): información detallada de la empresa, de los empleados de la empresa, contrato blindado, etc.
2. Verificación de los respaldos de seguridad, procesos por lotes (batch).
3. Revisar los cuadernos de bitácora: incidencias de todo tipo.
4. Medidas de evacuación en caso de catástrofes tanto naturales como espontáneas: (natural: inundación, espontánea: incendio por cortocircuito). Comprobar que existen medidas de evacuación y que estén debidamente señalizadas. Realizar simulaciones de evacuación de personal.
5. Revisión periódica de equipos contraincendio, ventilación, instalaciones eléctricas, etc.

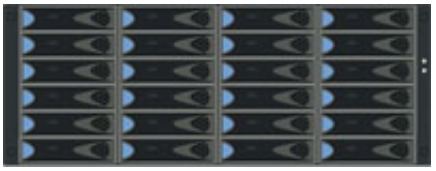
Autoevaluación

De las siguientes respuestas sólo hay una correcta. ¿Cuál es?
Todas las entradas, a cualquier CPD, debe estar controlado por un

guarda jurado.
Todo CPD debe tener un sistema de respaldo dentro de las instalaciones con responsabilidad por custodia.
Todo CPD debe tener las ventanas enrejadas.
Todo CPD debe tener, al menos, un extintor.

Componentes específicos en soluciones empresariales.

Caso práctico



Se solicita, por parte del departamento de gerencia, un informe de las necesidades globales, en materia informática. Dichas necesidades se centran en la necesidad de crear soluciones globales al entorno empresarial. Sobre minimización de hardware, soporte digital suficiente y accesible, armarios "rack" para cableado y hardware (electrónica en general), seguridad física del equipamiento, soporte software de acceso remoto, etc.

En el ámbito empresarial se debe realizar un proyecto del impacto que produce el equipamiento informático y, consecuentemente, minimizarlo.

En el caso de que se realicen las instalaciones de ordenadores, instalaciones de cableado, discos NAS, etc. sin ningún requisito previo, producirá un efecto de caos en dichas instalaciones y las posibilidades de crecimiento en servicios se verá limitada. La empresa debe realizar un estudio de qué tiene, qué necesita ahora y qué prevé que necesite en un futuro no muy lejano. Una vez definida todas las necesidades, deberá proyectar cómo realizar las instalaciones e infraestructuras. De esta manera, podrá disponer de una instalación e infraestructura con posibilidades de crecimiento. Podrá tener una **infraestructura** totalmente **modular**.

Podemos tomar como ejemplo los armarios rack con toda la "electrónica" (hubs, switchs, routers, etc.), panel de parcheo y cableado. Tiene su propia complejidad en cuanto a configuración y organización.

Otros ejemplos serán aquellos dispositivos de conexión en caliente o "hot plug" como discos duros, dispositivos como cámaras que se conectan a través, por ejemplo, de firewire.

En la imagen podemos observar cómo son los cables de conexión firewire.

El izquierdo se conecta al ordenador y el derecho al dispositivo.

Habitualmente este tipo de conexión aparecerá, en nuestro sistema operativo, como interfaz de red.

Autoevaluación

A la hora de realizar una instalación. Debemos afrontar el informe, ¿Cómo?

De forma modular.
De forma global.
Según las necesidades actuales.
Depende de los requerimientos de gerencia.

Bastidores o «racks».

Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones, tanto de voz como datos. Las medidas para la anchura están normalizadas para que sea compatible con equipamiento de cualquier fabricante, siendo la medida más normalizada el de 19".

Los racks son un simple armazón metálico con un ancho interno normalizado de 19 pulgadas, mientras que el alto y el fondo son variables para adaptarse a las distintas necesidades.

En cuanto a la altura y fondo, es totalmente variable. En la imagen podemos ver un conjunto de armarios o bastidores racks donde se podrá instalar: paneles de parcheo, HUB, SWITCH, servidores blade, servidores enrackables, etc.

Las alturas que ocupa cada electrónica se mide en base a "U". Dependiendo de su grosor podremos observar que un servidor enrackable o cualquier tipo de electrónica es: 1U, 2U, 3U. Por ejemplo: un servidor enrackable su caja tendría las dimensiones 44 cm x 71.1 cm x 4.3 cm., es decir, es 1U.

Una unidad rack o simplemente U es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 ó 23 pulgadas de ancho. Una unidad rack equivale a 1,75 pulgadas (44.45 mm) de alto.

Una unidad de rack se escribe normalmente como "1U"; del mismo modo dos unidades se escribe "2U" y así sucesivamente. La altura de una pieza del equipamiento de un rack es frecuentemente descrita como un número en "U".

Las unidades de medio rack describen unidades que caben en cierto número de U pero ocupan sólo la mitad del ancho del rack de 19 pulgadas. Éstas son usadas cuando un equipo no requiere el ancho entero del rack pero necesita más de 1U de altura. Por ejemplo, una pletina DVCAM de 4U de medio rack ocupará 4U de alto × 19/2 pulgadas y, en principio, se podrán montar dos pletinas una al lado de la otra ocupando el espacio entero de las 4U.

El tamaño de la unidad rack está basado en las especificaciones estándar de racks definidas en la EIA-310.

Para saber más

Cálculo de espacio utilizado por rack estándar para equipos.

Informe de Telefónica. (0.20 MB)

Dispositivos de conexión en caliente.

En principio los dispositivos de conexión en caliente (en inglés hot plug) son aquellos elementos hardware que, aún estando el ordenador encendido, el ordenador es capaz de detectarlo una vez que se conecta a un elemento de E/S adecuado a la conexión del dispositivo.

Por ejemplo: un pendrive podemos "pincharlo" en el equipo si y solo si el ordenador tiene conexión USB.

Habitualmente, la capacidad de conexión en caliente se circunscribe a todos aquellos periféricos cuya conexión está basada en conexión del tipo: USB, FIREWIRE, SATA y SAS.

Algunas conexiones serie o paralelo tienen la capacidad de conectarse en caliente. Pero lo más habitual es hacerlo por los medios mencionados anteriormente.

Ejemplos de dispositivos que utilizan conexiones serían: discos externos, pendrives, cámaras digitales, etc.

Hay que tener en cuenta que en los ordenadores ATX (todos los producidos desde 1998) siempre circula corriente aunque estén "apagados". En realidad están en una especie de modo de espera, por ello siempre existiría un riesgo si no estuviesen blindados para una conexión en caliente.

Además, son tantos los dispositivos que se conectan por puertos USB que en muchos casos son necesarios HUBs de USB para conectarlos todos al equipo o instalar una nueva controladora USB en un SLOT de expansión, siempre que dispongamos de uno libre. Habitualmente las cajas de los equipos tienen dos, cuatro, seis; pero en muchas ocasiones son insuficientes. Por ejemplo, si conectamos una impresora, un escáner, dos discos duros externos no tendríamos suficientes conectores y habrá que recurrir a otras alternativas como instalar una tarjeta controladora USB o un HUB.

Independientemente de que el equipo, como soporte hardware, detecte la conexión en caliente de un dispositivo, debe ser el sistema operativo quién deba ser capaz de recepcionar dicho dispositivo. Es decir, debe tener, el sistema operativo, un software soporte o controlador capaz de interpretar la señal, conocer qué dispositivo se ha conectado, qué función tiene e, inclusive, realizar el montaje automático para ser accesible por el usuario. Y, en caso contrario que no detecte el controlador adecuado, debe informar al usuario que debe obtener el controlador adecuado al dispositivo para acceder a las funcionalidades de éste.

Debes conocer

Concepto de conexión en caliente.

"hot plug"

Para saber más

Conexión de dispositivos externos a la CPU.

Blog educastur

Autoevaluación

Hoy en día es posible conectar dispositivos en caliente o hot plug prácticamente en cualquier equipo.

Verdadero.
Falso.

Discos.

En informática, **un disco duro o disco rígido** (hard disk drive), también denominado **memoria secundaria**, es un dispositivo de almacenamiento masivo de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada y al vacío. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

En la imagen podemos observar la estructura de los discos. Cada cilindro tiene dos caras, en cada cara del disco está dividido en pistas, cada pista, en sectores.

Los tipos de controladores son: IDE, SCSI, SATA y SAS. Actualmente los controladores más utilizados son los SATA. Van por la versión SATA-3.

La primera generación específica en transferencias de 150 MB por segundo, también conocida por SATA 150 MB/s o Serial ATA-150. Actualmente se comercializan dispositivos SATA II, a 300 MB/s, también conocida como Serial ATA-300 y los SATA III con tasas de transferencias de hasta 600 MB/s.

Las Unidades que soportan la velocidad de 3Gb/s son compatibles con un bus de 1,5 Gb/s.

En la siguiente tabla se muestra el cálculo de la velocidad real de SATAI 1.5 Gb/s y SATAII 3 Gb/s:

Velocidades de los discos SATA.
SATA I SATA II SATA III Frecuencia Bits/clock Codificación 8b10b bits/Byte Velocidad real

1500 MHz	3000 MHz	6000MHz
1	1	1
80%	80%	80%
8	8	8
150 MB/s	300 MB/s	600 MB/s

Para saber más

Completa descripción de los discos duros incluyendo enlaces.

Disco duro

Interesante vídeo sobre el funcionamiento de un disco duro.

Cómo funciona un disco duro

Fuentes de alimentación.

Las fuentes de alimentación son un elemento, dentro del hardware, muy importante. Es un dispositivo que convierte la tensión alterna de la red de suministro en una o varias tensiones, prácticamente continuas, que alimentan los distintos circuitos del aparato electrónico al que se conecta (ordenador, televisor, impresora, router, etc.).

En la imagen podemos observar cómo es una fuente de alimentación conmutada fuera de una caja de ordenador y destapada.

Las fuentes de alimentación pueden dividirse en: fuentes de alimentación lineales y fuentes de alimentación conmutadas.

Fuente de alimentación lineal: Siguen el siguiente esquema: transformador, rectificador, filtro, regulador y salida a placa y dispositivos.

Fuente de alimentación conmutada: Una fuente conmutada es un dispositivo electrónico que transforma energía eléctrica mediante transistores en conmutación.

¿Qué debemos tener en cuenta a la hora de elegir una fuente de alimentación? A qué tipo de ordenador va destinado, por ejemplo un equipo de sobremesa o servidor. Cuántos dispositivos internos y externos vamos a conectar habitualmente. Si es un servidor, ¿convendría que fuera redundante?

Como regla general, podemos seguir el siguiente criterio: No adquirir una fuente de alimentación muy exacta, ya que calentará mucho y el ventilador hará ruido, ni muy potente, ya que el rendimiento no será bueno. El rendimiento de una fuente de alimentación es óptimo entre el 20% y 100% de carga, con un máximo en el 50% aproximadamente.

¿Qué es una fuente de alimentación redundante? Una fuente de alimentación "redundante" es aquella que está compuesta internamente por dos fuentes de alimentación. Expongo un ejemplo: Una fuente de alimentación de 300W redundante es en realidad dos fuentes de 150W en una misma carcasa.

De este modo, si una de las fuentes falla, la otra puede seguir funcionando y el equipo no deja de funcionar. Estas fuentes se suelen utilizar, sobre todo, en servidores.

Para saber más

Guía sobre Fuentes de Alimentación: tipos, características e instalación.

Fuentes de Alimentación: tipos, características e instalación

Un interesante artículo sobre Fuentes de alimentación conmutada.

Fuente de alimentación conmutada

Información detallada de las fuentes de alimentación lineales.

Fuentes de alimentación lineales

Control remoto (I).

Cualquier sistema informático requiere de un medio de control que permita manipular y garantizar el funcionamiento de éste. En principio, los medios por los que se puede controlar el equipo está físicamente unido al propio equipo pareciendo que es un todo. Es habitual que entre los neófitos se considere al ordenador como equipo electrónico compuesto por una caja, un monitor, un teclado, un ratón y, a veces, si llega el presupuesto, una impresora y/o scanner.

En ocasiones, un empleado necesita acceder a su ordenador desde ubicaciones físicas no posibles. Por ejemplo: en la presentación de un informe a su jefe no tiene por que ir dicho jefe hasta el ordenador para presenciarlo, sino que el empleado podrá mostrar ese informe desde el propio equipo del jefe siguiendo las indicaciones del empleado.

Existen herramientas de software que permiten el control remoto de un equipo desde otro. Pero, además, el equipo a ser controlado, debe habilitar la posibilidad de que puedan controlarlo. Bien desde software incrustado en el propio equipo, bien desde software de utilidad descargado. Además, si tiene cortafuegos, deberá configurar este para que las peticiones de acceso le permitan realizar dicha tarea.

Normalmente este tipo de herramientas suelen ser aplicaciones que se dividen en dos partes: un servidor y un cliente. El servidor es el que esperará ser manipulado por los ordenadores que actúan como clientes.

Para que podamos acceder de forma remota, debemos valorar unos elementos que son importantes:

- Debe existir un ancho de banda que permita una alta velocidad de transferencia de archivos o ficheros. Esto incluye una LAN o WAN.
- Que exista una alta flexibilidad en la operación de los técnicos de soporte a la que puedan acceder desde distintas plataformas, sistemas y/o dispositivos (Windows, Linux, Macintosh, Mobile, Windows CE, Pocket PC, etc.).
- También, y no lo olvidemos, unos niveles de seguridad que cumpla con los estándares de seguridad como LOPD.

Hay herramientas que permiten un acceso remoto con una interfaz con línea de comandos. Por ejemplo: telnet, ssh, ftp, etc.

Y otras que permiten una interfaz gráfica, como los clientes "terminal service" de Windows o emuladores Xwindows para Linux.

Autoevaluación

¿Se debe habilitar un acceso remoto a un servidor a todos los usuarios sin distinción?

Sí, debemos dar la oportunidad a realizar tareas de teletrabajo.
Sí, siempre y cuando cumpla con los requisitos previos y bajo supervisión del administrador del servidor.
Sí, si el responsable del departamento al que está adscrito así lo ordena.
No, en ningún caso.

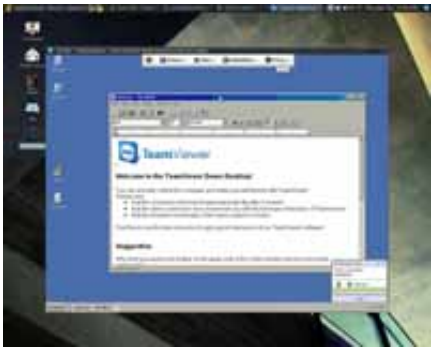
Control remoto (II).

O bien software como VNC que permite control remoto total. Este tipo de software simula un entorno igual que si estuviéramos sentados delante de nuestro monitor.

En la imagen podemos observar como desde una máquina con S.O. Linux podemos acceder a otro ordenador que tiene S.O. Windows.

La mecánica de funcionamiento de este servicio es de conexión punto a punto. Es decir, hay una comunicación directa y sin intermediarios entre el ordenador cliente y el equipo que va a ser controlado. Esto supone el inconveniente de que tenemos que conocer exactamente qué IP tiene el equipo remoto y otras consideraciones que se estudian en el módulo servicios de red e Internet.

Hay otras herramientas de control remoto similares a VNC. Consiste, básicamente, en que el equipo a ser controlado y el cliente se comunican, simultáneamente, a un enlace o servidor que, realmente, realiza las tareas de intermediación entre ambos equipos. Como ejemplo tenemos el software gratuito TeamViewer.



Este tipo de herramientas permiten a los operadores de soporte técnico controlar, de forma remota, los ordenadores de sus clientes que solicitan asistencia técnica. Este tipo de herramientas le permite, aparte de controlar la consola, realizar transferencias de archivo, ejecutar instalaciones y/o parches, reparaciones de software, chequear el equipo. Además, puede resolver una consulta guiada.

Esta herramienta es utilizada por los soportes técnicos pues tiene asociadas el ahorro en coste temporal y, por supuesto, económico.

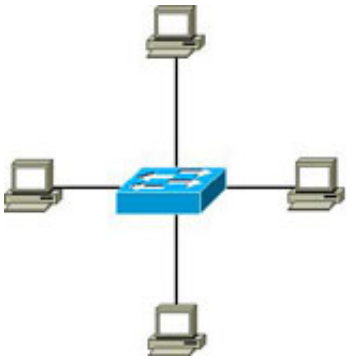
Servidores de archivos.

Los servidores de archivos son aquellos equipos que tienen como función, o una de sus funciones, permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este.

En principio, cualquier ordenador conectado a una red con un software apropiado, puede funcionar como servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente. O sea, normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

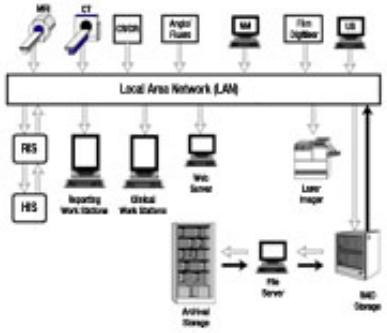
Este tipo de servidor es el más común de los servidores en todo tipo de empresas.

Este sistema de servidores, facilitan las estrategias de copias de seguridad centralizando las copias a un único emplazamiento.



Es común que en una red de iguales, cada ordenador reparta recursos entre el resto de ordenadores. ¿Cómo? Ejemplos como: un ordenador tiene una impresora conectada a su equipo y deja que el resto de equipos que están físicamente en su red puedan imprimir. Otro tiene mucho espacio en su disco o tiene un disco USB conectado a su equipo y permite que el resto de equipos puedan realizar copias de respaldo en ese disco.

Los protocolos más utilizados son:



SMB/CIFS (Windows, Samba en Unix o Linux): Permite que, en una red de difusión, los equipos de una misma red compartan recursos. Es decir, un equipo puede tener un recurso, por ejemplo, una carpeta o directorio o una impresora, a cuyo recurso se puede acceder desde otro equipo debidamente autorizado (si estuviera restringido el acceso).
NFS (Unix): Permite integrar un directorio de una máquina que utilice Unix, Linux o Mac, como si fuera miembro del sistema de archivos del propio equipo.

Motivos para tener un servidor de archivos:

Se obtendrá mayor rendimiento al sistema de archivos.
Los datos estarán protegidos contra fallos de corriente y otras incidencias.
Posibilidad de automatización de las copias de seguridad.
Los servidores son intrínsecamente inmunes a virus informáticos.
Pueden actuar como pasarelas para intercomunicar diferentes sistemas como Macintosh, Windows o Linux.
Es más difícil de que se cuelguen.
Tienen sistemas de archivos journaling que permiten la recuperación instantánea ante un apagón o errores comunes como el cierre del sistema de forma brusca.

Son servidores de alta seguridad, que pueden tener los datos distribuidos, con alta disponibilidad o cifrado automático.

Autoevaluación

En caso de desastre en el servidor, la responsabilidad última recaerá sobre el último usuario que accedió a este. ¿Verdadero o falso?

Verdadero.
Falso.

SAIS y estabilizadores de tensión.

El SAI (sistema de alimentación ininterrumpida) o, en sus siglas en inglés, UPS (Uninterrupted Power System) es un dispositivo que lleva incluida una o varias baterías que proporciona energía eléctrica, tras un apagón, a un sistema informático y/o periféricos a los que esté conectado.

Además de dar soporte ante un apagón, mejora la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna. Los SAI dan energía eléctrica a equipos que requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión). Este tipo de equipos los denominamos de carga crítica.

Los fallos a los que el SAI debe dar soporte son:

Corte de energía: Pérdida total de tensión de entrada. Condición de tensión cero.
Sobretensión: Tiene lugar cuando la tensión supera el 110% del valor nominal.
Caída de tensión: Cuando la tensión es inferior al 85-80% de la nominal.
Picos de tensión: ocurren cuando hay repentinos incrementos de tensión en pocos microsegundos ante causas como la caída cercana de un rayo, etc.
Ruido eléctrico: Es la interferencia de radio frecuencia (RFI) e interferencia electromagnética (EMI) ante interferencias de motores eléctricos, relés, dispositivos de control de motores, transmisiones de radiodifusión o tormentas eléctricas.
Inestabilidad en la frecuencia: Son corrientes que generan efectos negativos. Es corriente trabajar únicamente con valores correspondientes a la distorsión armónica total (THD).
Distorsión armónica, cuando la onda sinusoidal suministrada no tiene esa forma.

Ejemplos de SAI frontal y posterior.

Hay una característica específica de los servidores y no es otra que tardan más tiempo en arrancar y, por supuesto, más tiempo en apagarse. ¿Por qué? Porque al ser un sistema informático complejo y que, aparte de dar servicio como estación de trabajo (no es aconsejable pero se puede utilizar), debe dar servicio y soporte a otros equipos. Ante esta situación, un servidor no puede permitirse el "lujo" de que existan apagados no deseados.

Por esta razón, existen en el mercado varios tipos de SAIs:

SAI "On-Line": Se intercalan entre el suministro de red normal y la carga que se quiere alimentar. Proporcionan una salida de corriente alterna independiente de la de la red normal, autogenerada a partir de una corriente continua. Es decir, el equipo se alimenta permanentemente de la energía que genera el propio SAI.
SAI "Off-Line": Estos tipos de SAI son más sencillos que los anteriores. Se utilizan en instalaciones de baja potencia y bajo coste. No se intercalan entre el suministro de red normal y la carga a alimentar. Ésta es alimentada normalmente por la red. Tan solo cuando ésta falla la carga se alimenta de la corriente alterna generada por el SAI.

En el momento de la transferencia de carga, durante un fallo en el suministro de red, se produce una interrupción momentánea de la alimentación hacia la carga.

SAI de Línea Interactiva o "In-Line": En una zona intermedia se encuentran los SAI de Línea Interactiva. Se intercalan entre la red normal y la carga, por medio de un AVR o Acondicionador de Red. Pero no aíslan completamente a ésta de la red normal.

En el funcionamiento normal, la carga se alimenta de la red, a través del AVR. Tan solo durante un corte de la red, la carga se alimenta de red alterna generada directamente por el SAI, a partir de una tensión continua.

Las conmutaciones, cuando falla la red, se realizan en el orden de los milisegundos, por lo que se puede decir que no afectan a la continuidad del suministro a la carga.

Alimentación monitorizada.

Los SAIs son, en la actualidad, equipos o dispositivos accesibles desde un ordenador u

otro dispositivo a través de comunicaciones por el puerto serie.

Actualmente, aunque se va imponiendo poco a poco, los SAIs disponen, además, de un software soporte incrustado con las suficientes funcionalidades como para manipularlo, bien desde el ordenador o dispositivo a quien da soporte como, en algunos casos, a través de la red de datos, bien sea a través de la LAN o, inclusive, Internet.

Instalándolo en un PC o un servidor conectado al SAI, el software de comunicación permite al administrador del sistema ordenar y gestionar el SAI directamente. Se pueden gestionar todos los mandos del SAI directamente. Esta funcionalidad incluye a las estaciones remotas.

Un ejemplo de funcionamiento de un SAI en modo batería:

1. Todo está funcionando perfectamente.
2. Se va la luz, y el SAI entra en modo batería.
3. La batería llega a su carga mínima.
4. El sistema maestro notifica a los esclavos que dentro de poco se deben apagar.
5. Cuando los esclavos reciben la orden:
    1. Generan un evento NOTIFY_SHUTDOWN.
    2. Esperan el tiempo definido en FINALDELAY.
    3. Ejecutan el comando definido en SHUTDOWNCMD.
    4. Se apagan correctamente.
6. El sistema maestro espera que todos los clientes se desconecten.
7. El maestro empieza la secuencia de apagado:
    1. Genera un evento NOTIFY_SHUTDOWN.
    2. Espera el tiempo definido en FINALDELAY.
    3. Crea el fichero definido en POWERDOWNFLAG.
    4. Ejecuta el comando definido en SHUTDOWNCMD.
8. El proceso de apagado se lleva a cabo normalmente, y el sistema va parando los servicios y desmontando unidades.
9. El sistema encuentra en fichero definido en POWERDOWNFLAG, y ejecuta el apagado del SAI.
10. Cuando vuelve la luz, todos los sistemas se activan y todo vuelve a su estado normal.

Todos los cambios de estado que se produzcan quedan reflejados en los archivos históricos. Los cuales pueden ser revisados y nos permitirá realizar acciones de mantenimiento si fueran necesarios.

Para saber más

En la siguiente página podemos aprender sobre como enfoca una empresa de servicios el equipamiento de SAIS.

Socomec-sicon (0.35 MB)

Autoevaluación

¿Todos los equipos deben tener la alimentación monitorizada?

Sí, en otro caso pueden perderse los datos.
No, solamente aquellos que se consideren como “críticos”. Por ejemplo, servidores de datos.
No, no hace falta que ningún equipo esté monitorizado.
No, porque la propia monitorización eleva el consumo eléctrico.

Sistemas NAS. «Arrays» de discos. Discos SAS (I).

El sistema NAS (Network Attached Storage) es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un ordenador con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos SMB, NFS, FTP o TFTP.

Generalmente, estos dispositivos vienen, de fábrica, con el software soporte base incorporado. Con lo cual no es necesario realizar ninguna instalación. Aunque sí suele ser necesario utilizar software de firmware para su actualización.

Dependiendo a qué van destinados este tipo de almacenamiento, obtendremos diversas soluciones, bien empresariales, bien PYMES.

Como ejemplo de NAS podemos observar:

Este dispositivo de almacenamiento masivo es compacto, admite hasta cuatro discos duros de 2.5 pulgadas de tamaño, con dos conexiones Ethernet en la parte trasera, dos puertos USB y otros tantos eSATA, todos ellos para conectar otros dispositivos de almacenamiento externos, como por ejemplo discos duros.

La alternativa a los sistemas de almacenamiento NAS son los SAN (storage area network – red de área de almacenamiento). Su principal diferencia estriba en que es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología cableado de fibra y, más recientemente, en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Los arrays de discos o matrices de discos son sistemas de almacenamiento masivo que

enlazan o pueden enlazar múltiples discos duros físicos en una unidad grande para el control avanzado de datos y seguridad de estos.

El disco duro es el único dispositivo de los componentes críticos de un sistema informático que no es totalmente electrónico, sino que depende de las partes mecánicas móviles que a menudo fallan, por ejemplo, ante un apagón el campo magnético desaparece, al cabezal no le da tiempo a retrotraerse y "aterriza" sobre el disco rayándolo. Cuando esto sucede, los datos son irrecuperables a menos que haya un sistema de copia de seguridad del que pueda realizarse un rescate en otro disco.

Aquí es donde los arrays de disco marcan una diferencia. Los arrays de disco incorporan controles y una estructura que anticipa el desastre. El más común es la tecnología de matriz de discos RAID (Redundant Array of Independent Disks). Las matrices de discos RAID utiliza una serie de configuraciones opcionales que benefician al usuario. Una de las ventajas de las matrices de discos RAID es la redundancia de datos, escribe de manera que si un archivo está dañado o almacenado en un clúster no válido, puede ser sustituido de inmediato y totalmente transparente al sistema en otro punto de la matriz. El RAID también permite el intercambio en caliente de discos dañados y una mayor escalabilidad y flexibilidad en el almacenamiento.

Hay muchas variedades de RAID, y aunque diseñado principalmente para servidores, los arrays de discos se han vuelto cada vez más populares entre los usuarios debido a sus muchos beneficios.

Los controladores RAID por hardware pueden estar integrados en la placa base o bien ser insertados en un slot de expansión. Generalmente, en la configuración del controlador, a través del controlador software o utilidad de gestión, debemos realizar una serie de tareas como son: definir qué tipo de RAID vamos a utilizar, sincronizar los datos de los discos, comprobaciones, etc.

Sistemas NAS. «Arrays» de discos. Discos SAS (II).

Hay sistemas operativos, como Windows 2008 o Linux, que soportan RAID por software, no todos los tipos pero sí integran RAID 0, RAID 1 y RAID 5 que son los utilizados de forma estándar.

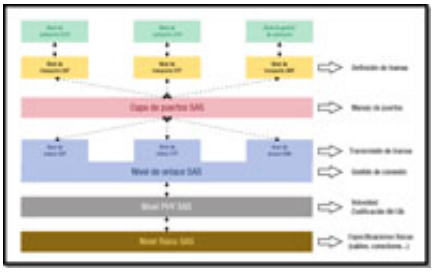
SAS (Serial Attached SCSI): es una controladora con la transferencia de datos en serie, sucesor del SCSI (Small Computer System Interface) paralelo, aunque sigue utilizando comandos SCSI para interaccionar con los dispositivos SAS. Aumenta la velocidad y permite la conexión y desconexión de forma rápida.

En la imagen podemos ver un rack de discos SAS, los cuales pueden ser cambiados en caliente o "hot plugging".

Una de las características de estas controladoras es la compatibilidad tanto con discos SCSI como con discos SATA.

Inclusive, pueden conectarse discos SATA junto con discos SCSI.

En la imagen podemos observar un conector interno SFF 8484. Está conectado al adaptador (controladora de disco o controladora RAID), mientras que el otro punto está conectado al disco duro con una entrada SAS/SATA (Serial Attached SCSI/Serial ATA) adaptada al conector.



Para saber más

Una visión de soluciones NAS actualizados.

NAS y monitorización

Concepto ampliado de un sistema SAN.

Red de área de almacenamiento

Debes conocer

Página oficial del organismo que lo estandariza los SAS.

SCSI Trade Association (SCSITA)

Los tipos de RAID y sus características.

RAID

Arquitecturas de alta disponibilidad.

Caso práctico

En el informe resultante que solicitó gerencia, se aborda la necesidad de que el nuevo equipamiento del CPD cumpla una serie de requisitos por encima del coste. Por ejemplo, que los equipos que se instalen hayan superado una serie de pruebas de calidad. Así como que cumplan con el condicionamiento de estar permanentemente disponibles tanto para los empleados de la empresa como para el personal responsable de dichos equipos.

Cuando hablamos de arquitecturas de alta disponibilidad no sólo estamos pensando en productos caros en el ámbito de las soluciones informáticas para empresas, tanto en el apartado hardware como software. Las soluciones que necesitan de este tipo de arquitecturas son aquellas que deben estar a pleno rendimiento las 24 horas de día, los 7 días de la semana.

Dicho esto, este tipo de arquitectura debe conllevar asociada los términos de fiabilidad y disponibilidad.

La fiabilidad que ofrezca el sistema informático debe basarse en que un sistema funcione normalmente durante un período de tiempo dado. Es decir, que exista una continuidad no interrumpida salvo casos excepcionales.

El fallo surgirá cuando un servicio no funciona correctamente. Se genera un estado de funcionamiento anormal. Por ejemplo, tomando como referencia un servidor web, si

presentara páginas incompletas o tarda excesivamente en presentarlas al usuario.

Estos fallos se suelen atribuir a un funcionamiento incorrecto del sistema.

La alta disponibilidad consiste en una serie de medidas cuyo objetivo no es otro que garantizar la disponibilidad del servicio de una forma fiable. Que funcione correctamente durante las 24 horas.

Existe una norma, la **TIA-942** que determina una serie de niveles de disponibilidad básicos llamados Tier I, Tier II, Tier III y Tier IV.

Este tipo de estándares suelen ser referente de los centros de datos.

Autoevaluación

Si se cayera un servidor, ¿qué tiempo estimas que se necesita para recuperar la normalidad?

No existe tiempo de respuesta, es impredecible.
Veinticuatro horas como mucho.
Lo razonable son cuarenta y ocho horas.
Debe existir un protocolo de respuesta rápida.

Para saber más

La Telecommunications Industry Association tiene definidos varios estándares recogidos en la norma TIA-942.

TIA-942

Ejemplo de utilización de los estándares TIA-942.

Grupo Electrotécnica

Inventariado del hardware.

Caso práctico

En los CPDs existe equipamiento que debe ser controlado, supervisado desde

el punto de vista informático, administrativamente o como carácter burocrático.

En todo momento se debe conocer de qué equipamiento se dispone, estado, incidencias sufridas y su correspondiente estado de resolución.

De esta situación debemos llegar a la conclusión de se debe realizar un recuento físico de todos los sistemas implicados que estén instalados en el CPD (aunque es extensible a otros tipos de instalaciones dónde exista un número aceptable de equipamiento informático).

¿Cómo se debe realizar? De forma individual, contándolos uno por uno, así como sus componentes, tanto internos como externos, e incluyendo los periféricos y demás elementos que integran cada equipo (por ejemplo: teclado, ratón, monitor, etc.).

Una vez hecho el inventario individual, realizaremos el global. Contando los sistemas de ordenadores, después sus componentes, seguidamente sus periféricos y dispositivos y también, por separado, todos los elementos adicionales a los sistemas.

Una vez realizado el inventario físico, seguiremos con la revisión documentada. Es decir, todo el hardware debe estar registrado en documentos modulares de la empresa: registros inventariados, facturas, registros de otra índole que sea homologable por la empresa.

¿Por qué estos pasos? De esta forma se pretende cotejar que los equipos, dispositivos y demás componentes recogidos en el inventario físico, realmente estén reflejados en el registro, en papel, de la empresa.

Una vez realizada la comparación podremos obtener resultados:

Que no haya diferencias entre el registro de la empresa y el hardware que se ha revisado físicamente.
Que haya hardware del que la empresa no tenga registro ni documento que lo refleje. Entonces es nuestra labor a qué es debido: que esté de forma provisional con conocimiento de algún responsable del área.
Que una persona responsable, por ejemplo, del departamento dónde se ha detectado la diferencia lo haya instalado sin conocimiento del responsable del área de sistemas.
Que se desconozca dónde se encuentra el documento que acredita su procedencia.
Que la empresa tenga registro del hardware, pero esté "traspapelado".
Que haya hardware obsoleto pero que no se ha dado de baja del registro.
Que se haya dado de baja pero no está reflejado en los documentos de la empresa.
Que esté desmontado y fuera del área de competencia pero no esté reflejado en documento alguno.
Que se haya extraviado o sustraído y no haya sido anotada la incidencia y, por lo tanto, notificada.
Que esté prestado externamente y no se haya notificado.

Que haya hardware instalado sin que la empresa tenga registro ni documentos que acrediten la permanencia en las instalaciones.

En una auditoría será conveniente realizar el inventario de consumibles. Aunque en este caso, únicamente se debería hacer para el conocimiento financiero. De esta manera, se podrá valorar qué materiales se consumen en el área departamental que contribuyen al desarrollo de las actividades propias de la empresa.

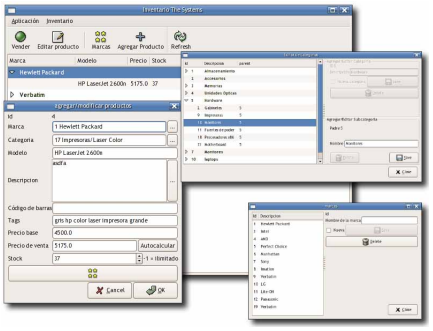
Autoevaluación

¿Se debe catalogar todo el hardware?

No, sólo aquellos elementos más importantes como equipos servidores.
Sí, pero a nivel de hardware con sus elementos internos como discos, memorias, etcétera.
Sí, pero sin catalogar aquellas unidades externas conectadas al equipo, como discos duros externos.
Ninguna es correcta.

Herramientas para el inventariado hardware.

Caso práctico



El departamento de informática, siguiendo con el plan de catalogación e inventariado de todo el equipamiento hardware, determina la necesidad de utilizar un software específico que permita controlar todo el hardware de una manera ordenada y clasificada dentro de una base de datos.

Para la realización de un inventario es conveniente realizar una estrategia que nos permita recoger metodológicamente toda la información necesaria para llevar a buen término el inventario de todo el hardware competencia del área de sistemas.

Existen aplicaciones de software que nos permiten realizar el seguimiento. Podemos reducir la estrategia a dos técnicas habituales para obtener información a cabo en un área de red.

En una empresa con cierto nivel en cuanto a dimensión, tendrá un sistema de red más o menos heterogéneo. En cuyo caso no valdrá una sola herramienta y tendrás que recoger la información con mecanismos adicionales. Una vez obtenida esta información la introduces "manualmente" en la herramienta de inventariado escogida e implantas controles para detectar nuevos equipos. En algunos casos, como pequeñas empresas, con una simple hoja de cálculo o base de datos sencilla bastaría.

Si te enfrentas "a ciegas" a una red desconocida o te enfrentas a una red en la que se realiza un inventario por vez primera las técnicas que debes evaluar utilizar para obtener información de ésta son de dos tipos:

Análisis activo: extraer la topología de la red y sistemas "vivos" a base de búsquedas recursivas: empezando por un punto de la red, consultar a sistemas adyacentes (a través, por ejemplo de ICMP, SNMP, u otros protocolos de gestión específicos de dispositivo), obtener información adicional de la red (nuevas subredes) y volver a hacer el proceso iterativo. Esto es lo que hacen herramientas de gestión de red y sistemas como HP Openview Network Node Manager (o Aprisma de Spectrum, o Netview de IBM, que es un fork de NNM) o más modestos como el de Solarwinds. En el mundo de software libre tienes Cheops-NG. Una vez se tenga un inventario de direcciones IP en uso también puede ser de ayuda (aunque sea un poco más agresivo y te recomiendo andar con cuidado) utilizar Nmap [insecure.org] y, más específicamente, su módulo de análisis de servicios y aplicaciones.

Análisis pasivo (del tráfico de la red): en principio sólo (en el caso de una red conmutada) si puedes capturar tráfico a través de un tap o un puerto en port span (o escaneo de puertos) aunque no siempre sea necesario (si la red no es conmutada y se basa en HUBs). En este caso aquí puedes obtener mucha información en base al intercambio de tráfico entre equipos aunque depende de que, en el tiempo de monitorización, los equipos respondan. Con el análisis pasivo puedes obtener información de servicios, sistemas operativos (con p0f) o, en tu propia red local, de hardware (en base a la MAC de los equipos obtienes el fabricante del mismo).

Autoevaluación

Un inventario en modo activo seria.

Partiendo de un inventario manual, realizar el control a través de la red de datos mediante un software adecuado.
No hace falta un inventario manual, se hace todo a través de la red.
Sólo es válido si el inventario se realiza manualmente.
Ninguna es correcta.

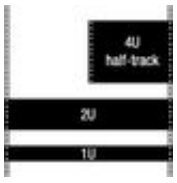
Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo. Recurso (1) Datos del recurso (1) Recurso (2) Datos del recurso (2)

	Autoría: Ddxc . Licencia: Public Domain Procedencia: http://en.wikipedia.org/wiki/File:NetworkOperatio
	Autoría: Wtshymanski Licencia: Public domain Procedencia: http://es.wikipedia.org/wiki/Archivo:Televideo925
	Autoría: Oliver Regelmann Licencia: CC BY-NC-SA Procedencia: http://www.flickr.com/photos/oliverregelmann/38260991/sizes/
	Autoría: warszawianka Licencia: Dominio Público Procedencia: http://www.openclipart.org/detail/36565
	Autoría: Pchow98 Licencia: CC by-nc-nd Procedencia: http://www.flickr.com/photos/pchow98/25452814
	Autoría: Earle Winslow / johnny_automatic Licencia: Dominio público Procedencia: http://www.openclipart.org/detail/15447
	Autoría: Gmaxwell Licencia: GNU Procedencia: http://es.wikipedia.org/wiki/Archivo:Datacenter-te
	Autoría: pgbrandolin Licencia: Dominio Público Procedencia: http://www.openclipart.org/detail/101407
	Autoría: Daquellamanera Licencia: CC by

Procedencia:
http://www.flickr.com/photos/daquellamanera/194372296/sizes

Autoría: Mikkel Paulson
Licencia: CC nc
Procedencia: http://commons.wikimedia.org/wiki/File:FireWire_



Autoría: Easyas12c
Licencia: CC nc
Procedencia: http://es.wikipedia.org/wiki/Archivo:Rackunit.svg

Autoría: Clemente
Licencia: Copyright (cita)
Procedencia: http://es.wikipedia.org/wiki/Archivo:Cilindro_Cabe

Autoría: Tuur
Licencia: CC by-nc-sa
Procedencia:
http://www.flickr.com/photos/tuuur/4257007700/sizes/l/in/photc

Autoría: tuxtorm
Licencia: CC by-nc-nd
Procedencia:
http://www.flickr.com/photos/tuxstorm/4524557408/sizes/z/in/p

Autoría: Kieranmaher
Licencia: Public Domain
Procedencia: http://commons.wikimedia.org/wiki/File:PACSdia

Autoría: Hundehalter
Licencia: CC by-sa
Procedencia: http://commons.wikimedia.org/wiki/File:Apc_ups_

	
	Autoría: Jemimus Licencia: CC by-nc-sa Procedencia: http://www.flickr.com/photos/jemimus/446137959/sizes/m/in/ph
	Autoría: rgtaylor_csc Licencia: Dominio Público Procedencia: http://www.openclipart.org/detail/17666
	Autoría: markuz Licencia: CC by-nc-nd Procedencia: http://www.flickr.com/photos/markuz/124884262/sizes/o/in/pho