ESCUELA DE PREPARACIÓN DE OPOSITORES
E. P. O.
C/. La Merced, 8 – Bajo A Telf.: 968 24 85 54
30001 MURCIA

SAI23

Instalación de un sistema Informático. Entorno. Elementos. Conexión. Configuración. Medidas de seguridad.

Esquema.

1 Introducción.

La ISO define un sistema informático como el sistema compuesto de equipos y de personal pertinente, que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos.

En este tema vamos a estudiar todos aquellos aspectos fundamentales para el buen funcionamiento de un sistema informático. Para ello, empezaremos dando una visión del sistema informático dentro del sistema de información de las organizaciones. A continuación estudiaremos los principales aspectos de la instalación y conexión, para, seguidamente, pasar a los parámetros de configuración. Concluiremos nuestro estudio con un estudio de la seguridad desde diferentes puntos de vista.

2 Elementos y entorno de un sistema informático.

Un sistema de información es un conjunto formal de procesos que, operando sobre una colección estructurada de datos, recopilan, elaboran y distribuyen la información necesaria para las operaciones de la organización y para las actividades de dirección y control correspondientes para desempeñar su actividad.

Que los datos deban estar adaptados a las necesidades de la organización significa que deben reflejar la percepción de la información que tienen las personas que los utilizan. También se resalta que, tanto las operaciones diarias como las actividades de dirección y control basadas en la toma de decisiones, requieren información para su realización y deben ser atendidas por el sistema de información. Por último, el sistema debe estar al servicio de la estrategia de la organización, ya que sólo se trata de un elemento más que ésta emplea para conseguir sus objetivos. La estructura de los sistemas de información depende totalmente de la organización concreta a la que pertenezca, aunque se puede identificar una base común a la mayoría de las organizaciones.

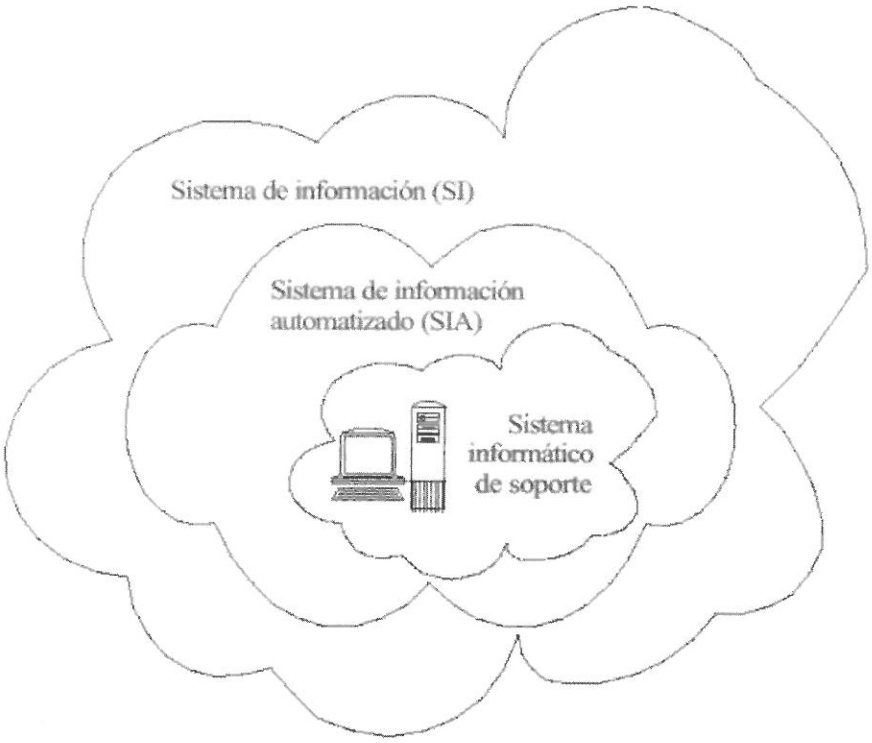
Para comprender mejor el concepto de sistema de información, debemos conocer los elementos que lo componen. Existe unanimidad en la bibliografía sobre sistemas de información en designar como componentes de un sistema a los siguientes:

- Los procedimientos y las prácticas habituales de trabajo que se siguen al ejecutar toda clase de actividades necesarias para el buen funcionamiento de la organización. El sistema de información existe porque debe dar un soporte a la gestión de información que hay que proporcionar en función de todas estas formas de trabajar.
- La información. Es el elemento fundamental del sistema y su razón de ser. Se debe adaptar a las personas que la manejan y al equipo disponible, según los procedimientos de trabajo que la organización ha creado para que las actividades se realicen de forma eficaz.
- Las personas o usuarios. Se trata de individuos o unidades de la organización que introducen, manejan o usan la información para realizar sus actividades en función de los procedimientos de trabajo establecidos.
- El equipo de soporte para la comunicación, el procesamiento y el almacenamiento de información. Constituye la parte más visible del sistema de información, su realidad física y tangible. Este sistema físico puede incluir elementos de los más variados niveles tecnológicos: papel, lápiz, máquina de escribir, archivadores, ordenadores, cintas magnéticas, etc.

Además, existen relaciones entre los distintos elementos del sistema de información. El sistema de información estará al servicio de los objetivos generales de la organización. Para lograr dichos objetivos, la organización y sus individuos adoptan las maneras de trabajar que resultan más útiles y eficaces. Pero las relaciones también funcionan en sentido inverso, y los procedimientos de trabajo se deben adaptar a los elementos disponibles.

Las organizaciones han ido incorporando nuevas tecnologías para mejorar el rendimiento y la eficacia de los sistemas de información. Se comenzó con calculadoras mecánicas, cintas de papel perforado, etc. y se ha llegado a utilizar tecnologías sofisticadas de tratamiento de información: informática, ofimática, etc., a las que se ha denominado genéricamente tecnologías de la información. En nuestro caso, nos centraremos en la informática como tecnología de la información que podemos aplicar a la automatización de los sistemas de información.

Así, podemos distinguir entre lo que es el sistema de información total y lo que es el sistema de información automatizado, como se muestra en la siguiente figura.



Además, el sistema de informatización automatizado deberá contar con un soporte informático para funcionar. En este sentido, la informática constituye sólo una herramienta más o menos sofisticada para implementar lo que está incluido en el sistema de informatización automatizado. Por tanto, no debe confundirse informática y sistema de información, ni el sistema de informatización automatizado con el soporte físico o sistema informático asociado (constituido por el hardware, el software de base y las aplicaciones.)

3 Instalación y conexión.

3.1 Ubicación del sistema

Una vez recibidos todos los componentes físicos del sistema, se procederá a la instalación del conjunto completo, de una sola vez, lo que resulta más fácil que hacerlo en distintas fases.

En principio, el sistema informático trabajará eficazmente en distintos ambientes. Para su instalación, debemos tener en cuenta las siguientes indicaciones:

- Colocar los componentes sobre superficies planas.
- Situarlo en lugares relativamente limpios y libres de polvo. (El polvo en suspensión, la suciedad, la ceniza y el humo pueden causar un excesivo desgaste de las superficies móviles, así como errores de lectura/escritura.)
- El equipo principal está refrigerado por medio de un ventilador, por lo cual deben mantenerse las entradas de aire libres de papeles u otros objetos que obstruyan la circulación del mismo.
- Conviene aislar el sistema de las fuentes que generan distorsiones eléctricas y de los aparatos que producen variaciones o fluctuaciones en la tensión de la red de alimentación (acondicionadores de aire, ventiladores, extractores, transformadores, alternadores, motores eléctricos, transmisiones de radio o televisión, sistemas de seguridad, etc.).

A la hora de instalar un sistema, uno de los factores más importantes, son las tomas de corriente: todos los componentes deben conectarse a tomas de fluido eléctrico con conexión de tierra. Los equipos alimentados con enchufes sin toma de tierra no trabajan correctamente y pueden ser peligrosos para el usuario. Si se utilizan alargadores, también deberán tener la misma característica.

Los problemas que se presentan, si no se dispone de la correspondiente derivación a tierra, además de la posibilidad de descargas eléctricas, son:

- Ejecución anormal de los programas.
- Imposibilidad para el equipo de recuperar la información de los discos.
- Costosos daños al hardware de la máquina.

3.2 Conexión de periféricos.

Los componentes externos o periféricos pueden ser múltiples y variados. Indudablemente debemos examinar la parte trasera del equipo principal o panel posterior, donde irán conectados a la unidad central mediante conectores diferentes y específicos para cada función. Una vez vista la disposición de los conectores en el panel posterior del módulo base, puede empezarse a conectar los diferentes componentes del sistema. Se prepara el destornillador, si se precisa, y no se enchufa el sistema a la red eléctrica.

3.3 Conexión entre equipos. Cableado estructurado.

Un sistema de cableado estructurado es una red de cables y conectores en número, calidad y flexibilidad de disposición suficientes que nos permita unir dos puntos cualesquiera dentro de un edificio para cualquier tipo de red (voz, datos o

imágenes). Consiste en usar un solo tipo de cable para todos los servicios que se quieran prestar y centralizarlo para facilitar su administración y mantenimiento.

El primer estándar sobre sistemas de cableado fue EIA/TIA-568. Durante años ha sido la referencia para los sistemas de cableado pues no había otro documento de referencia similar. Actualmente ya existe un estándar internacional sobre sistemas de cableado aprobado por ISO: es el IS-11801. En Europa se llama EN-50173.

Ya que el sistema de cableado recibe el nombre de estructurado, sería conveniente conocer su estructura. Al conjunto de todo el cableado de un edificio se le conoce con el nombre de SISTEMA y cada parte en la que se divide se da el nombre de SUBSISTEMA. Existen 4 subsistemas: área de trabajo, subsistema horizontal, subsistema vertical, y subsistema campus.

Área de trabajo

Se define como la zona donde están los distintos puestos de trabajo de la red. En cada uno de ellos habrá una roseta de conexión que permita conectar el dispositivo o dispositivos que se quieran integrar en la red.

Subsistema horizontal.

Desde la roseta de cada una de las áreas de trabajo irá un cable a un lugar común de centralización llamado panel de parcheo. El panel de parcheo es donde se centraliza todo el cableado del edificio. Es el lugar al que llegan los cables procedentes de cada una de las dependencias donde se ha instalado un punto de la red. Cada roseta colocada en el edificio tendrá al otro extremo de su cable una conexión al panel de parcheo. De esta forma se le podrá dar o quitar servicio a una determinada dependencia simplemente con proporcionarle o no señal en este panel.

Se conoce con el nombre de cableado horizontal a los cables usados para unir cada área de trabajo con el panel de parcheo. Todo el cableado horizontal deberá ir canalizado por conducciones adecuadas. En la mayoría de los casos, se eligen para esta función las llamadas canaletas que nos permiten de una forma flexible trazar los recorridos adecuados desde el área de trabajo hasta el panel de parcheo.

Es muy conveniente que el panel de parcheo junto con los dispositivos de interconexión centralizada (concentradores, latiguillos, routers, fuentes de alimentación, etc.) estén encerrados un armario de comunicaciones. De esta forma se aíslan del exterior y por lo tanto de su manipulación accidental. También facilita el mantenimiento al tenerlo todo en un mismo lugar.

Subsistema vertical.

El cableado vertical (o de "backbone") es el que interconecta los distintos armarios de comunicaciones. Éstos pueden estar situados en plantas o habitaciones distintas de un mismo edificio o incluso en edificios colindantes. En el cableado vertical es usual utilizar fibra óptica o cable UTP, aunque en algunos casos se puede usar cable coaxial.

En el cableado vertical están incluidos los cables del backbone, los mecanismos en los paneles principales e intermedios, los latiguillos usados para el parcheo, así como los mecanismos que terminan el cableado vertical en los armarios de distribución horizontal.

Subsistema campus.

Lo forman los elementos de interconexión entre un grupo de edificios que posean una infraestructura común (fibras ópticas, cables de pares, sistemas de radioenlace, etc.).

3.4 Seguridad física.

3.4.1 Sistemas de alimentación interrumpida (SAI).

El paso siguiente es la configuración del sistema de alimentación ininterrumpida (SAI), y si es necesario, instalar placas de control de SAI (UPS). La placa de control de SAI se utiliza para conectar el cable de señal entre el servidor y el SAI. El SAI usa este cable para informar al servidor de que el SAI está trabajando con la alimentación de reserva.

Debemos asegurarnos de que el SAI tiene suficiente potencia para alimentar todos los dispositivos que vamos a conectarle. Sumaremos la potencia en vatios de los equipos que vamos a conectar, y comprobaremos que el total no supera la potencia suministrada por el SAI.

3.4.2 Equipos de reserva.

Es necesario disponer de hardware de reserva ya que en caso de un fallo el sistema puede volver a ponerse en marcha una vez reemplazado el dispositivo defectuoso.

3.4.3 Control ambiental.

El polvo, la suciedad, el calor y la humedad son los mayores enemigos del hardware informático. Las personas y el equipo funcionan mejor donde el aire está limpio, fresco, y con la humedad adecuada. En los lugares donde hay ordenadores y sistemas informáticos el aire acondicionado ha dejado de ser un lujo y ha pasado a ser una necesidad.

Hay que tener mucho cuidado con elementos tales como el polvo de una pequeña obra, la electricidad estática, la humedad excesiva, etc. A esto hay que añadir el potencial peligro que representan los propios usuarios, una taza de café por encima de la pantalla o migas de pan en el teclado pueden paralizar el ordenador e incluso inutilizarlo por completo. La ceniza de los cigarrillos puede dañar las cabezas y la superficie de los discos, y por lo tanto la información en ellos contenida.

4 Configuración.

Hay una serie de medidas que se pueden tomar para configurar un sistema informático:

- Ajuste de parámetros del sistema operativo: hay algunos parámetros que el administrador del sistema puede modificar. Estos parámetros son, por ejemplo, el tamaño del quantum asignado a cada uno de los programas, la prioridad interna asignada a un programa de usuario, tamaño de la partición de memoria, frecuencia de fallo de página e índice de supervivencia de las páginas, y todo lo demás relacionado con el usuario y los procesos.
- Ajuste de parámetros del hardware, es decir, examinar la configuración hardware del sistema y ver qué parámetros se pueden alterar, tales como por

ejemplo la activación de cachés hardware, el reloj del sistema, frecuencia del bus, etc.

- Equilibrado de cargas: repartir las cargas a las que son sometidos los diversos dispositivos, como red, discos duros, entre las diferentes máquinas que las gestionen y personas que lo usan, o repartir los ficheros entre los diferentes sistemas de ficheros del sistema.
- Ampliación: se pueden comprar dispositivos nuevos, o cambiar los dispositivos por otros más rápidos. Previamente, habrá que realizar un análisis de cuáles son los dispositivos que están limitando las prestaciones del sistema.
- Cambio del software: se puede cambiar el software que se está usando por otra versión u otra marca.

4.1 Gestión de carga y prestaciones en el sistema operativo

En general, un administrador de un sistema tiene que plantear la gestión de un sistema de la siguiente forma:

- Planificación de la carga y definición de la carga del sistema: es conveniente acordar de antemano qué se considera unas prestaciones aceptables. Una vez llevada a cabo esta planificación, hay que comprobar si con el sistema se puede llevar a cabo ese acuerdo; y si en el futuro previsible, con los usuarios y la carga pico prevista, se va a poder producir.
- Configurar las herramientas de monitorización del sistema: se deberán poner en funcionamiento las herramientas que monitorizan en cada momento los subsistemas principales: CPU, E/S, red, y memoria; estos monitores indicarán como se usa el sistema en cada momento y a lo largo del tiempo, y permitirán prever los fallos y arreglarlos cuando se produzcan; también habrá que escribir una serie de scripts que avisen de que alguna cosa vaya mal.
- Tratar de resolver problemas mediante políticas de gestión del sistema, tales como limitación de uso interactivo, limitación de uso de disco mediante cuotas, etc.

4.2 Políticas de gestión del sistema.

Tanto los usuarios como el administrador pueden mejorar el funcionamiento del sistema. Por ejemplo, algunas medidas que pueden tomar los usuarios son:

- Usar comandos internos del shell en vez de los comandos externos. Este tipo de medidas será útil siempre que todos los usuarios estén trabajando sobre un solo sistema.
- Evitar los caminos largos, que hacen que el ordenador tenga que leer muchos directorios cada vez que se ejecuta un comando. Evitar los directorios con muchos ficheros; el tamaño del fichero de directorio crece con el número de ficheros. Cuando un fichero de directorio es demasiado grande, no queda otro remedio que crear un nuevo directorio y mover todos los ficheros a él.
- Usar las versiones más eficientes de cada tipo de programa.

En cuanto al administrador, hay muchas cosas que puede llevar a cabo para aligerar la carga del sistema:

- Eliminar demonios inútiles. En general, es conveniente echar un vistazo a los demonios que se activan por defecto cuando se enciende el ordenador y eliminar los más innecesarios.
- Limitar tiempos de ejecución interactivos y cambiar la prioridad de un proceso en función de los otros procesos que estén ejecutándose.
- Modificar los parámetros del sistema operativo. Una serie de parámetros controlan, por ejemplo, el número de procesos máximos que puede abrir el sistema, procesos por usuario, ficheros por proceso, etc.

Este tipo de políticas son utilizables en el caso genérico. En particular, para cada sistema, hay una serie de parámetros a los que habrá que controlar.

4.3 Sintonización de la memoria.

Algunas de las medidas que pueden tomarse de cara a la sintonización de la memoria son:

- Limitar el tamaño de los procesos.
- Animar a la gente a usar librerías compartidas.
- Modificar el algoritmo de paginación.
- Cambiar el tamaño de la partición de swap.

4.4 Mejora de prestaciones de entrada/salida.

Aunque el subsistema gráfico tiene su importancia, no es algo de lo que el administrador del sistema se pueda preocupar, ya que afecta más a las prestaciones de un ordenador local que a las del sistema en general; lo mismo ocurre con impresoras; lo que sí afecta las prestaciones del sistema en general son los discos duros, y en ellos nos vamos a fijar en este apartado.

Los discos duros incluyen tanto los locales como aquellos accesibles mediante red. La eficiencia de estos sistemas estará en tres factores diferentes: rendimiento por proceso, rendimiento total, y eficiencia en el almacenamiento.

El optimizar los primeros dos factores es hasta cierto punto compatible, si un sistema tiene unas buenas prestaciones por proceso, también lo serán las totales, pero no necesariamente. Un proceso suele acceder a un solo fichero en un solo disco duro, mientras que el sistema en total accede a muchos ficheros simultáneamente en muchos discos duros, o, lo que es peor, en el mismo. El que interese más uno u otro factor dependerá del uso prioritario de cada disco duro y del sistema en total.

El tercer factor, eficiencia en el almacenamiento, es incompatible con el rendimiento; si se trata de optimizar el rendimiento disminuye la eficiencia en el uso del disco. Por ejemplo, incrementar el tamaño del bloque hace que vaya más rápido a la hora de leer o escribir, pero aumenta el número de bytes que cada fichero ocupa, y viceversa.

4.4.1 Consideraciones sobre la configuración.

Cada disco va unido a una controladora de disco que es determinante de sus prestaciones. En muchos casos, a cada controladora van conectados varios discos; cada uno de esos discos tiene que "compartir" la velocidad de transferencia de la controladora. A su vez, la controladora va conectada al bus del sistema. Todos estos elementos influirán en las prestaciones del disco.

Las dos controladoras más habituales hasta hace relativamente poco tiempo eran la SCSI (*Small Systems Computer Interface*), y la EIDE (*Extended Independent Drive Electronics*). En ambos casos, se pueden conectar varias unidades a cada controlador. El conectar diversos dispositivos al mismo conector habitualmente afecta las prestaciones; ya que las peticiones de lectura o escritura y su respuesta deben de viajar por el mismo conjunto de cables. En la actualidad estas controladoras se han visto reemplazadas por la SATA (*Serial Advanced Technology Attachment*), en la cual solo se conecta un dispositivo en cada interfaz (no se comparte el cable).

Últimamente se están poniendo de moda otro tipo de controladores: los USB y los FireWire (o IEEE 1394), dos tipos de buses serie que permiten conectar todo tipo de dispositivos externos al ordenador, y en particular discos duros.

En cuanto al segundo factor, el bus, sucede lo mismo: PCI es el más usado en el segmento de los PCs, y diferentes buses propietarios en los servidores y estaciones de trabajo. En algunas estaciones de trabajo hay diferentes buses; por ejemplo, PCI y alguno propietario, cada uno con sus características. La elección del bus al que se va a conectar el disco duro es previa a la compra del mismo, y de la controladora que va con él.

Asimismo, habrá que elegir a qué ordenador se van a conectar los discos duros; aunque el conectar todos los discos duros a un solo servidor hace la gestión mucho más fácil, el que cada grupo de trabajo tenga un disco duro normalmente aumenta las prestaciones. Cuando se haya tomado una decisión, y esté funcionando, el análisis de prestaciones del sistema nos revelará si la elección es adecuada o no.

Otro factor es la organización del sistema de discos duros: almacenamiento en red, RAID, discos duros distribuidos en diferentes ordenadores, etc. La organización distribuida tiene la ventaja de no crear cuellos de botella, mientras que el almacenamiento en red o en un sólo ordenador tiene más facilidad de mantenimiento.

Los siguientes factores son las características físicas del disco duro. Hay dos parámetros principales: la velocidad de transferencia, y el tiempo medio de búsqueda; ambas están relacionadas con la capacidad del disco. Habitualmente, a mayor capacidad, mayor velocidad de transferencia y menor tiempo medio de búsqueda. También están relacionados con la velocidad de rotación del disco duro. De los dos, el más importante es el tiempo de búsqueda. El tiempo de búsqueda no es lineal, y depende del sitio donde se encuentra la cabeza y donde tenga que ir; normalmente se especifica el tiempo mínimo de búsqueda. Esto es cierto principalmente en entornos multiproceso/multiusuario, donde es más habitual que el cabezal del disco esté saltando buscando diferentes ficheros. Habitualmente, la tasa de tiempo empleado buscando con respecto al tiempo empleado transfiriendo es de 10 a 1; por eso es interesante que sea lo menor posible. En cuanto a la tasa de transferencia, aunque de ella hay que descontar toda la información de formateo y el tiempo que se tardaría en saltar de una pista a otra, suele ser un buen indicador de rendimiento para un solo proceso.

En resumen, si hay que comprar un nuevo sistema de E/S, dado que hay poca elección en cuanto al controlador y al ordenador que hay que conectar, lo más importante es el tiempo mínimo de búsqueda.

4.4.2 Sistemas de ficheros.

En la mayoría de los casos y de los sistemas operativos actuales, hay varios sistemas de ficheros donde elegir. Algunos de ellos son:

- En el mundo Windows, los más habituales son FAT, FAT32, y NTFS. Cada uno de ellos tiene sus limitaciones y ventajas; por ejemplo, los antiguos tenían limitaciones en cuanto al tamaño de discos duros que podían manejar.
- En el mundo UNIX, hay muchos sistemas de ficheros. Para empezar, está NFS, pero se trata únicamente de cómo los ordenadores en la red ven los sistemas de ficheros de otros ordenadores. UFS es el más habitual en las implementaciones BSD de UNIX, pero hay otros, como EFS (en Irix), ext2fs (en Linux), XFS, reiserfs, etc.

Algunos sistemas de ficheros tienen características tales como compresión, permitir recuperar ficheros eliminados, o similares.

En cada partición suele haber un sistema de ficheros. Hay que seguir unas cuantas reglas a la hora de distribuir las particiones:

- Distribuir la carga de trabajo tan parejamente como sea posible.
- Mantener tipos similares de ficheros en los mismos sistemas de ficheros, para que sea más fácil elegir configuraciones adecuadas para cada uno.
- Mantener proyectos o grupos dentro del mismo sistema de ficheros, así es más fácil su manejo para los usuarios.
- Dar a cada sistema de ficheros un tamaño de bloque adecuado para los ficheros que contiene. Por ejemplo, a un sistema de ficheros con una base de datos le vendrá mejor un tamaño grande de bloque, para hacer el acceso más eficiente, mientras que uno para desarrollo de software estará mejor servido con tamaño de bloque pequeño, para hacer el almacenamiento más eficiente.
- Tener el número mínimo de particiones.

4.4.3 Equilibrio de la carga de trabajo de E/S

Idealmente, el número de lecturas y escrituras, y el número de transacciones debe de estar repartido uniformemente entre todos los discos; pero lo más habitual es que alguno de los discos se lleve toda la carga. En caso de que eso suceda, lo que se debe de hacer es reequilibrar la carga, de la forma siguiente:

- Colocar los ficheros a los que más se acceda en los discos duros más rápidos.
- Repartir los usuarios entre diferentes discos duros, y colocar los ficheros de los usuarios que más uso tenga en los más rápidos.

4.4.4 Conservando el espacio del disco duro.

Algunos de los trucos para ahorrar espacio de disco son los siguientes:

- Configurar los sistemas con tamaños pequeños de bloque, aunque eso hará que vaya todo un poco más lento.
- Usar utilidades de compresión para comprimir ficheros que no se accedan a menudo.
- Instituir cuotas de disco por usuario.
- Borrar ficheros que no se usan como demos o juegos, o que se usan demasiado como el IRC, juegos, etc. Borrar ficheros temporales periódicamente. Borrar los ficheros *core* y temporales periódicamente.

5 Medidas de seguridad.

El trabajo informático conlleva una serie de riesgos, en especial en relación con la pérdida de la información archivada en el ordenador. Los problemas pueden provenir de diversos frentes: destrucción física del equipo (hardware), avería física del equipo (avería hardware), averías lógicas, pérdidas de información producidas por acciones indebidas del operador, problemas por funcionamiento anómalo de los programas, problemas ocasionados por virus informáticos, problemas derivados de las conexiones remotas, etc.

5.1 Destrucción física del equipo informático.

Conviene no exponer todo el sistema a las mismas situaciones de riesgo. Por ejemplo, hay que meditar si es operativo mantener una copia de seguridad en un segundo disco duro del mismo ordenador, puesto que un mismo suceso puede inutilizar ambos conjuntos de datos. Las copias de seguridad realizadas en dispositivos independientes preferiblemente serán trasladadas a otro lugar.

Por otro lado conviene tomar algunas precauciones de tipo físico: los ordenadores y las copias de seguridad no se llevan bien con las humedades o inundaciones, por lo que no conviene situar los elementos informáticos de forma que puedan ser afectados. No debe permitirse que los componentes técnicos se vean sometidos a temperaturas extremas, al sol directo o a otros bruscos cambios ambientales. No deben apilarse objetos pesados en torno al ordenador, por el riesgo de caídas. Las mesas y soportes utilizados deberán ser suficientemente robustos y estables. Los cables no deben estar en zonas de paso o de trabajo, para evitar que los podamos arrollar provocando accidentes, etc.

Un riesgo peculiar puede ser la avería por sobretensión de la red de alimentación eléctrica. Existen aparatos (llamados estabilizadores de voltaje) destinados a prevenir esta posibilidad. Por otro lado la interrupción imprevista del fluido eléctrico también puede ocasionar un posterior mal funcionamiento del equipo, por el deterioro de los archivos que estaban siendo utilizados durante la interrupción. Otros aparatos (SAI) evitan este suceso. También hay dispositivos que combinan ambos funcionamientos.

También hay que considerar la posibilidad del robo físico del equipo (hardware). Para prevenir esta desventura reforzaremos las barreras de acceso con puertas seguras, cerraduras de seguridad, barrotes en las ventanas, etc. Por otro lado, tal vez podamos tomar alguna medida para evitar que durante las horas de trabajo otras personas puedan acceder indebidamente a nuestro equipo, o llevar algún tipo de registro para saber quien ha entrado y salido.

5.2 Avería física del equipo.

El desgaste natural, el sobrecalentamiento, pequeños golpes, malas condiciones ambientales, falta de calidad en los elementos, etc., pueden ser algunas de las causas de fallo. Conviene insistir en la prevención de ambientes húmedos o temperaturas extremas, los impactos o colisiones, las sobretensiones eléctricas; etc. Además habrá que cuidar de la adecuada ventilación, pues la falta de aireación del ordenador puede ocasionar sobrecalentamientos y averías.

Habrá que cuidar especialmente las labores de limpieza del equipo, pues muchas veces el exceso de celo en estas tareas puede ocasionar problemas funcionales (los productos químicos son poco recomendables, en general).

Al introducir discos, cintas y otros elementos en el ordenador conviene cuidar su correcta colocación y nunca forzar la entrada o salida de los mismos. Esto también es aplicable a la colocación del papel en la impresora; y a los cambios de cinta o cartuchos de tinta (realizarlos siempre con la impresora apagada). Lo mismo puede aplicarse a la inserción y retirada de discos duros extraíbles, tarjetas PCMCIA, baterías y otros elementos encajables. Debe prestarse la máxima atención a la correcta colocación de estos elementos, no forzar su inserción o extracción y realizar estas actividades siempre con todos los elementos apagados.

5.3 Averías lógicas.

El sistema informático no solo depende del hardware, y de los programas de utilidad que empleamos. En primer lugar debemos considerar que los campos magnéticos pueden ocasionar problemas de gravedad variable. Sobre un monitor tradicional (tubo de rayos catódicos) el magnetismo puede producir una alteración en la visualización, pero esto no será una avería física porque el problema desaparecerá al distanciar el monitor de la fuente de magnetismo. Sobre los discos, cintas y otros dispositivos de almacenamiento, el campo magnético puede llegar a distorsionar o eliminar toda la información archivada. Es una precaución alejar todos los equipos informáticos de los fuertes campos magnéticos y emisiones intensas de radiofrecuencia.

Por otro lado los discos y cintas que almacenan ficheros necesitan tener una estructura lógica concreta que permite al ordenador leer y grabar la información. El fallo de esta estructura puede ocasionar que la información contenida en el soporte no pueda ser accesible, y ello puede producirse ocasionalmente sin razón aparente. En estos casos se puede recuperar la utilidad del elemento reformateándolo, pero eso no nos permitirá recuperar la información. Para prevenir esto conviene utilizar algún programa que nos permita comprobar periódicamente la coherencia de esta estructura y de la información albergada en el elemento. Estos programas deben usarse cada cierto tiempo y siempre que se pueda suponer algún problema de este tipo. Suelen ser capaces de reparar la mayoría de los problemas que puedan encontrar en el dispositivo. Estos programas de comprobación también deben aplicarse a los disquetes cada cierto número de usos.

Un fallo en el sistema operativo también puede considerarse una avería lógica, porque no se trata de un deterioro físico. Esto puede producirse de forma aleatoria y el mal funcionamiento puede ser ocasional o permanente. Si el problema es ocasional probablemente desaparezca en la próxima ocasión que encendamos el ordenador; si el fallo es permanente probablemente se deba a un fichero que contiene información errónea y en tal caso será necesario reinstalar el sistema operativo. Para prevenir esta posibilidad siempre es conveniente disponer de discos de arranque que nos permitan

reinicializar el ordenador en condiciones estables, chequear/reparar el disco duro y reinstalar el sistema operativo.

Hay un caso de avería difícilmente catalogable. Se trata de la situación que se produce cuando un elemento electrónico funciona inadecuadamente. Esto puede producirse de forma sistemática, y en tal caso estaríamos ante una avería física. Pero también puede suceder que esa disfunción sea solo para una sesión de trabajo (y no se reproduce después de apagar y encender el ordenador) o inclusive cabe la posibilidad de que el fallo se produzca puntualmente en una única ocasión momentánea; en tales casos se puede considerar como una avería lógica. Las consecuencias pueden ser desastrosas o inapreciables. Muchos fabricantes de componentes declaran la calidad de los mismos midiendo el "tiempo medio entre fallos"; por tanto los propios fabricantes ya reconocen esta posibilidad de fallo "ocasional" de sus propios dispositivos.

5.4 Pérdidas de información producidas por acciones indebidas del operador.

Frecuentemente las pérdidas de información y otros problemas son ocasionados por la actuación inadecuada del operador. Esto puede deberse a la excesiva carga de trabajo o por inexperiencia o por falta de serenidad o por cualquier otra razón; todo ello contando con la mejor voluntad del operario. El caso es que en demasiadas ocasiones un usuario elimina del ordenador un fichero valiosísimo, formatea el disco inadecuado o sustituye un documento importante por otro intranscendente. Para prevenir estos problemas solo se pueden dar consejos muy generales.

En primer lugar es conveniente que los trabajos informáticos sean realizados por personas que no pierdan los nervios con facilidad. Es evidente que quien tiene un espíritu más nervioso puede cometer más errores.

En segundo lugar conviene que los operarios de informática tengan una buena formación técnica en cuanto al trabajo que están haciendo; esto tiene una doble vertiente en casi todos los casos: por un lado debe tener un razonable control sobre el funcionamiento y posibilidades del equipo que está manejando; por otro lado debe controlar igualmente el otro posible aspecto de su profesión. No se pretende que todos los usuarios de ordenadores sean expertos en informática, pero indudablemente trabajarán mejor y con más seguridad si tienen un nivel de conocimiento razonable.

La mayoría de los desastres ocasionados por acciones del usuario tienen una relación directa con la presión laboral y el nivel de estrés al que está sometido el trabajador. Para mejorar el rendimiento del trabajador se pueden cuidar algunos aspectos ergonómicos y de confort que evitarán el descontento y la distracción del operario: una temperatura normal, una silla cómoda, una iluminación que no provoque reflejos en la pantalla, etc.

Finalmente es de destacar que muchos de los problemas de los operadores vienen condicionados por la inadecuación del sistema informático para el trabajo que se exige. Es un despropósito ahorrarse algún dinero adquiriendo un software menos adecuado a la tarea pretendida, porque ello acabará provocando mayores pérdidas en el rendimiento y la concentración del trabajador; estas situaciones suelen derivar en actuaciones incorrectas (involuntarias) que pueden tener fatales consecuencias. Solo puede esperarse que un operario cumpla correctamente con su misión si se le suministran los elementos adecuados y sabe manejarlos correctamente.

La actividad informática requiere que se dedique un cierto tiempo a realizar tareas de control y mantenimiento del sistema, tales como chequear discos o hacer

copias de seguridad. La necesidad de culminar tareas profesionales de forma urgente puede postergar estas actividades, lo que incrementa peligrosamente los riesgos en cuanto a la seguridad y operatividad de la información. Por tanto conviene siempre reservar ciertos ratos para la prevención e "higiene" técnica.

5.5 Problemas por funcionamiento anómalo de los programas.

Un programa es algo así como un gran juguete construido con un mecano. Se supone que debe funcionar de una forma determinada bajo cada situación concreta. Sin embargo el equipo técnico que desarrolla el programa puede haberse equivocado al planear o desarrollar el programa. También puede suceder que el programa esté bien diseñado pero esté mal archivado en el ordenador; y por último cabe una última posibilidad, consistente en que el programa este mal copiado en la memoria electrónica. Este tipo de incidentes pueden tener consecuencias muy variables, y la gravedad de los efectos es poco previsible.

Cuando el programa está mal copiado a la memoria bastará con reiniciar el ordenador. El programa puede estar mal grabado en el disco duro, con lo cual el fallo persistirá tras reiniciar el sistema. Esto puede producirse por un fallo ocasional producido durante la instalación, o por otro fallo que haya trastocado los ficheros que contienen el programa; en tal caso habrá que reinstalar el programa. Pero también puede suceder que el programa no esté construido correctamente o como nosotros esperamos.

Frecuentemente culpabilizamos al programa de hacer mal su trabajo sin haber leído la documentación o manual que acompaña al programa, y luego resulta que el problema está originado por una incorrecta configuración o una utilización inadecuada del usuario. Siempre es recomendable perder algún tiempo averiguando cómo funciona el programa, antes de empezar a utilizarlo en serio. También conviene hacer algunas pruebas de funcionamiento antes de comenzar el uso normal del programa.

Puesto que no sabemos el cuidado o esmero que se ha aplicado en la construcción del programa, tenemos que guiarnos por premisas generales como las siguientes: Las probabilidades de que un programa cause problemas suele estar en relación inversa a su coste, al prestigio de la marca que lo avala y a la difusión que alcanza en el mercado. Las empresas más prestigiosas suelen tomar mayores precauciones en la calidad de los productos que comercializan. Un producto mejor normalmente tiene un coste de fabricación mayor, por lo que probablemente nos exigirá un desembolso superior. Los programas utilizados por miles de usuarios suelen ser mejores que los elegidos por una minoría. Es cierto que las estrategias comerciales pueden variar estos planteamientos, por lo que cada uno debe responsabilizarse de lo que elige. Por otro lado ningún productor de software puede asegurar que su producto está totalmente libre de errores.

Este apartado está muy relacionado con el que se dedica a las averías lógicas, y ambos temas se solapan o coinciden en muchos aspectos.

5.6 Problemas ocasionados por los virus informáticos.

Los virus informáticos son programas que interfieren en el trabajo normal del ordenador realizando acciones indeseadas por el usuario. Un virus es un programa que se duplica de forma silenciosa y sin apercibimiento del usuario. Para que el virus no sea detectado fácilmente se "disfraza" aparentando ser otro tipo de programa. También hay virus que se "infiltran" en los ficheros que albergan a otros programas. La mayoría de los virus tienen un efecto denominado "bomba lógica". Esto consiste en que, pasado

algún tiempo o cuando se producen determinadas circunstancias, el virus empieza a realizar otras tareas.

Hay muchas clases de virus con funcionamientos muy distintos y con efectos de lo más variados. Algunos infectan a los programas, mientras que otros se infiltran en el sistema operativo o en la estructura de los discos. Los hay que esperan a una fecha determinada para comenzar su labor destructiva, otros tienen un período de latencia fijo. Se consideran virus malignos aquellos que destruyen o modifican la información archivada en ficheros de datos, mientras que otros solo interfieren en el funcionamiento del sistema pero sin afectar a los archivos de datos.

Se han construido programas antivirus que son capaces de detectar y combatir a los virus reconocidos. En muchos casos los programas antivirus son capaces de "extirpar" el virus y recuperar la normalidad del sistema. Los programas antivirus pueden funcionar chequeando la memoria y los discos, pero también pueden funcionar haciendo tareas de vigilancia preventiva, para evitar que podamos activar inadvertidamente un programa que contiene un virus. Esta actividad ralentiza el rendimiento del sistema, pero en ocasiones puede merecer la pena este pequeño inconveniente. Algunos programas funcionan incluso en modo semi-inteligente advirtiendo de los programas que, sin contener un virus reconocido, podrían comportarse como un virus (por similitud a algunos de los virus reconocidos).

El problema se agrava porque cada día circulan tres nuevos virus informáticos por algún ordenador, con lo cual siempre estamos expuestos a nuevos peligros. Para paliar esto, los productores de programas antivirus siguen a la caza de nuevos virus, ampliando continuamente el catálogo de los que ya han sido reconocidos. Cada cierto tiempo se ofrece al usuario una nueva versión del programa capaz de reconocer y bloquear más virus.

5.7 Problemas derivados de las conexiones remotas.

A medida que aumenta la independencia de los ordenadores colocados en red, necesitamos protegernos contra diversas amenazas. Hay una necesidad de asegurar las transacciones que se realizan por las redes de ordenadores que unen los centros de datos, ya que por la red se puede enviar información crítica, como, por ejemplo especificaciones de diseño, estrategias de productos y planes de desarrollos futuros. Otra de las motivaciones para la seguridad es la dependencia significativa en aplicaciones de red como el correo electrónico como medio de comunicarse.

Las amenazas a la seguridad de un sistema se pueden clasificar como accidentales o intencionadas, y pueden ser activas o pasivas. Las amenazas accidentales son las que se producen sin necesidad de un intento premeditado. Un ejemplo puede ser una avería en el sistema. Las amenazas intencionadas pueden variar desde el examen casual de un ordenador hasta ataques sofisticados utilizando conocimientos especiales sobre el sistema.

Las amenazas pasivas son las que, si se realizan, no conllevan ninguna modificación en la información que posee el sistema, y no se modifican ni la operación ni el estado del sistema. La alteración de información o los cambios en el estado de operación del sistema se conocen como amenaza activa. Un ejemplo podría ser la modificación por parte de un usuario no autorizado de las tablas de encaminamiento del sistema.

Los sistemas que están conectados a redes son susceptibles de sufrir diversos tipos de ataques. En una mascarada, una entidad pretende pasar como una entidad diferente. Generalmente, la mascarada se combina con otras formas de ataque activo, como la réplica y modificación de mensajes.

Los ataques internos tienen lugar cuando los usuarios legítimos de un sistema se comportan de forma no prevista o autorizada. La mayoría de los delitos informáticos se han realizado mediante ataques internos contra la seguridad de los sistemas.

Entre las técnicas que se pueden utilizar para realizar ataques externos se encuentran la intervención, la intercepción de emisiones, las mascaradas como usuarios autorizados del sistema, y el rodeo de los mecanismos de identificación y de control de acceso. Una puerta trasera se añade a un sistema cuando una entidad del mismo resulta alterada para permitir que un atacante produzca un efecto no autorizado al ejecutarse un comando, o al producirse un determinado evento o secuencia de eventos. Un ejemplo podría ser la modificación de una validación de contraseña de forma que, además de su efecto normal, valide también la contraseña del atacante.

Los mecanismos de seguridad implementan los servicios de seguridad. Estos mecanismos pueden ser de dos tipos: mecanismos de seguridad específicos y mecanismos de seguridad generalizados.

Entre los mecanismos de seguridad específicos podemos citar:

- El cifrado, que se puede emplear para dotar de confidencialidad tanto a los datos como a la información de flujo del tráfico.
- Los mecanismos de firma digital, que se emplean mediante dos procedimientos: firma de una unidad de datos y verificación de una unidad de datos.
- Los mecanismos de control de acceso, que se pueden emplear en el origen o en cualquier punto intermedio, para determinar si el remitente está autorizado para comunicarse con el destinatario o para utilizar los recursos.
- Entre los mecanismos de integridad de datos podemos citar el marcado temporal, los números de secuencia o el encadenamiento criptográfico.
- La información de verificación, como contraseñas, uso de características o posesiones de la entidad, firma digital o notarización.
- El relleno del tráfico se puede utilizar para proporcionar varios niveles de protección contra el análisis del tráfico.
- El control de encaminamiento, mediante el que las rutas se pueden escoger dinámicamente o mediante acuerdo previo, de forma que sólo se utilicen rutas, enlaces o sistemas de reenvío físicamente seguros.

Para cada comunicación concreta, se puede utilizar la firma digital, el cifrado y los mecanismos de integridad apropiados al servicio que se esté proporcionando. Utilizando un mecanismo de notarización es posible asegurarse de propiedades como el origen de los datos, la fecha y hora y el destino.

5.8 Las copias de seguridad.

Las copias de seguridad son el procedimiento más eficaz y necesario para asegurar la disponibilidad de la información archivada electrónicamente. Hacer una

copia de seguridad consiste en duplicar la información en un dispositivo independiente, a fin de poder recuperar esta información en caso de pérdida o deterioro de la información original.

Las copias de seguridad pueden hacerse utilizando los procedimientos de duplicación normal de ficheros, pero existen programas específicos destinados a estas tareas. El principal inconveniente de los duplicados realizados con estos programas de copias de seguridad suele radicar en que la información guardada como copia no es operativa en sí misma: para reutilizarla se hace necesario realizar un proceso inverso denominado recuperación. Cada vez que tengamos modificaciones substanciales en nuestros archivos, debemos hacer una nueva copia de seguridad; por contra en muy pocas ocasiones tendremos que recurrir a recuperar esta información.

Las copias de seguridad pueden realizarse sobre disquetes, sobre un segundo disco duro, sobre otro disco extraíble o sobre cintas magnéticas. La ejecución sobre disquetes tiene el inconveniente de que estos tienen una capacidad más limitada y funcionan más lentamente, por lo que probablemente necesitaremos un buen montón de discos y una proporcional dosis de paciencia. Para colmo de males no podemos desatender la operación, puesto que cada pocos minutos deberemos cambiar el disquete. Estas circunstancias hacen que este procedimiento sea bastante tedioso y habitualmente ocurre que acabamos no haciendo esta tarea con la frecuencia deseada.

Las copias sobre un segundo disco interno del mismo ordenador solo cubren ciertos riesgos, puesto que no nos previenen suficientemente de la destrucción del hardware o de los virus informáticos; por tanto no debemos considerar que estas copias nos puedan salvaguardar de todos los accidentes posibles. Sin embargo se realizan con una agilidad asombrosa y completándose en forma desatendida.

También es posible realizar copias en otros discos extraíbles, normalmente discos de gran capacidad que utilizan diversas tecnologías. Estos discos suelen funcionar de un modo más lento que los discos duros internos, pero más rápidamente que los disquetes y probablemente pueda completarse la copia en modo desatendido.

Otra alternativa es utilizar cintas magnéticas igualmente extraíbles. Utilizan dispositivos y programas específicos y suelen estar destinadas únicamente al servicio de copias de seguridad.

Dependiendo de las posibilidades de inversión y de las necesidades previstas para cada caso habrá de seleccionarse uno u otro procedimiento para realizar las copias de seguridad. Entre los factores a considerar están el volumen de información a duplicar, el tiempo que se puede destinar a esta tarea, la frecuencia con que se prevé que habrá que ejecutar la copia y si es un factor importante que el duplicado se complete sin intervención del operador. En algunos casos pueden utilizarse varios procedimientos que se complementan.

Las propias copias de seguridad tampoco están exentas de riesgos: no podemos confiar ciegamente en que los datos copiados nos permitirán siempre recuperar de un modo eficaz la información. Los soportes que contienen los datos copiados también pueden deteriorarse. Además es posible que hayamos realizado una copia de los archivos después de que estos hayan sido desfigurados por una operación inadecuada o por un virus. Igualmente cabe la posibilidad de un fallo ocasional durante la realización de la copia. Cualquiera de estos sucesos imposibilitará la recuperación de los datos. Por tanto, vamos a redoblar nuestras cautelas:

- Realizaremos copias de seguridad sobre soportes alternativos. Se considera muy prudente guardar los soportes en sitios distintos en previsión de incendios, robos, etc.
- Periódicamente convendrá comprobar la integridad y funcionamiento de los soportes empleados para albergar las copias de seguridad.
- No es necesario realizar copias de seguridad de los archivos correspondientes a programas o al propio sistema operativo. Sin embargo sí necesitaremos algún disco que nos permita arrancar el sistema en caso de que falle el disco duro; este disco debe incluir las utilidades mínimas para chequear el disco duro y reinstalar el sistema operativo. Por otro lado también necesitaremos copias actualizadas de los archivos de configuración del sistema. Algunos sistemas operativos disponen de programas de utilidad destinados específicamente a salvaguardar estos ficheros de configuración, y se recomienda encarecidamente su uso cada vez que se varíe esta configuración, ya sea por instalación de nuevos dispositivos de hardware como por otras modificaciones del sistema. En algunas ocasiones lo más cómodo puede ser realizar una copia de seguridad completa del disco duro interno, y ello tampoco presenta otro inconveniente técnico que el mayor tiempo necesitado para una tarea tan completa.

6 Conclusiones.

Los componentes de un sistema de información son: los procedimientos y las prácticas de trabajo, la información, las personas o usuarios, y el equipo de soporte. Las organizaciones han ido incorporando nuevas tecnologías para mejorar el rendimiento y la eficacia de los sistemas de información, llegando a utilizar tecnologías sofisticadas de tratamiento de información: informática, ofimática, etc., a las que se ha denominado genéricamente tecnologías de la información.

La informática constituye una herramienta para implementar la automatización del tratamiento de información, de forma que el sistema informático es el soporte para realizar dicha automatización. La automatización de un sistema de información debe contemplar el hardware y el software de base y, por supuesto, las aplicaciones software que permitan cubrir las necesidades de información que marca la estructura del sistema de información.