TEMA

23

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

M.ª de los Ángeles Sampalo, M.ª Luisa Garzón y Esteban Leyva

CUERPO DE PROFESORES TÉCNICOS DE FORMACIÓN PROFESIONAL

ÍNDICE SISTEMÁTICO

1. **INTRODUCCIÓN**

2. **ENTORNO. ELEMENTOS**

3. **CONEXIÓN**

4. **CONFIGURACIÓN**
   - 4.1. Configuración de servidores
   - 4.2. Configuración de estaciones clientes
   - 4.3. Configuración de accesos externos
   - 4.4. Configuración y gestión de usuarios
   - 4.5. Configuración y gestión de datos
   - 4.6. Configuración del sistema de impresión

5. **MEDIDAS DE SEGURIDAD**
   - 5.1. Protección de los equipos informáticos y sus instalaciones
     - 5.1.1. Protección contra la electricidad estática
     - 5.1.2. Protección contra subidas, bajadas de tensión y cortes del suministro eléctrico
     - 5.1.3. Protección contra temperaturas extremas
     - 5.1.4. Protección contra incendios
     - 5.1.5. Protección contra el agua
     - 5.1.6. Control ambienta
     - 5.1.7. Protección física
   - 5.2. Protección de datos
     - 5.2.1. Copias de seguridad
     - 5.2.2. Control de acceso

1. INTRODUCCIÓN

Un sistema está constituido por **elementos funcionales** independientes, aunque relacionados entre sí, que se unen formando un todo complejo.

Cada uno de estos elementos funcionales representa una función básica del sistema, como puede ser: una entrada, un proceso, una salida, almacenamiento de la información, etc.

Los sistemas están enfocados hacia objetivos concretos que suponen su meta, disponen también de un ambiente o entorno que los rodea y que influye en el propio sistema, por proveerle de elementos de entrada y recibir los elementos de salida que éste proporciona.

También el sistema dispone de una serie de **recursos** que componen los medios de que dispone éste para la consecución de sus objetivos.

Los sistemas pueden obtener elementos de su entorno, denominándose en ese caso sistemas abiertos. Por el contrario, los sistemas cerrados sólo tomarán recursos que se encuentren dentro de él; estos recursos podrán ser tanto humanos como físicos o lógicos.

2. ENTORNO. ELEMENTOS

Cualquier empresa, independientemente de su tamaño, necesita una organización interna que lleve a cabo una red de funciones, entre las que se pueden encontrar:

- **Llevar un control de los recursos económicos de la empresa**: función contable.
- **Comercializar sus productos de manera eficiente**: función comercial y de ventas.
- **Fabricar sus productos o crear servicios para ofrecer a sus clientes**: función de producción.

Llevar a cabo todas la funciones de una empresa es muy complicado si la empresa no dispone de un sistema eficaz de intercambio de información. Esto dio lugar a la creación de los **Sistemas de Información** (SI), cuya función es la de encaminar la información de forma correcta, pasando por puestos intermedios hasta llegar a los usuarios finales. Para mejorar el rendimiento de las empresa, éstas han ido incorporando medios informáticos a sus sistemas de información, convirtiéndolos en **sistemas de información automatizados** (SIA). Para realizar esta tarea será necesario el establecimiento de planes y estrategias que deben cumplirse fielmente.

Dicho esto, los sistemas informáticos constituirían el soporte de un sistema de información automatizado, y estaría formado por los equipos informáticos (hardware), el software de base y las aplicaciones. Por lo tanto, y a efectos informáticos, la automatización de un sistema de información conlleva la elección del hardware conforme a las necesidades, la configuración adecuada del software de base y la elección de un software de aplicación que cubra las necesidades concretas de la empresa. En este último aspecto se puede decidir entre la adquisición de un paquete de software listo para instalar, la confección de un software a medida, o la adaptación particular de un software ya confeccionado.

Los elementos básicos de un sistema informático se agrupan en:

1. **Hardware**: dispositivos electrónicos y electromecánicos que proporcionan la capacidad de cálculo y manejo de la información (ordenadores, periféricos, conexiones, cableado, etc.).

2. **Software**: constituido por los programas y los datos que manejan los ordenadores y que solucionan los requerimientos del sistema. El software utilizado se clasifica básicamente en dos grupos:

   a) **Software básico**. El componente principal es el sistema operativo, que varía en función del sistema que se implante y de las distintas ofertas del mercado. Será el encargado de la comunicación entre el usuario y los dispositivos físicos del sistema, permitiendo, además, la configuración así como la gestión de la información almacenada. Se deben tener en cuenta ciertos requisitos como la estabilidad del sistema y la escalabilidad para responder a ampliaciones futuras. De nada nos sirve un software que limite el número de usuarios.

   Podemos hacer una clasificación en función del número de usuarios que accedan al sistema:

   * **Monousuario**: sólo un usuario podrá acceder al mismo.
   * **Multiusuario**: permite la compartición de recursos mediante el acceso desde distintos terminales, ya sea localmente o de forma remota.

   Otro software que se engloba también en este grupo es el software de utilidades, creado para facilitar las tareas del usuario. Existen en el mercado una gran variedad, tanto a nivel de estaciones de trabajo como a nivel de servidores.

   b) **Software de aplicación**. Hace referencia a las aplicaciones creadas por el usuario programador, ya sea por una compañía o por el personal del sistema.

3. **Personal**: son tanto los operadores o usuarios directos de las herramientas del sistema, como las personas encargadas del desarrollo del software.

4. **Documentación, manuales, formularios, y cualquier otra información descriptiva** que detalla o da instrucciones sobre el empleo y operación del sistema.

Por otro lado, un sistema informático tiene un tiempo de existencia o ciclo de vida, es decir, comprende el tiempo que se mantiene desde su implantación hasta su sustitución por otro más eficiente, o la eliminación del sistema por pasar a ser innecesario, por ejemplo, cuando una empresa dejará de producir un determinado producto.

Según el entorno donde se implanten estos elementos variarán en función del tipo de usuarios y de sus necesidades, lo que condicionará la arquitectura aplicable. Por ejemplo, no es lo mismo trabajar en un entorno que se dedique al diseño multimedia que basar su tarea en la gestión de una base de datos.

3. CONEXIÓN

Se está convirtiendo en una norma básica en las empresas el trabajo en grupo, por lo que la instalación de redes locales es hoy en día una generalización, lo que va a permitir la compartición de todos los recursos presentes en toda la red, como unidades de almacenamiento, impresoras, etc.

Si trabajamos en un entorno de red, su utilización conlleva una serie de beneficios que se pueden ver multiplicados si abrimos una puerta en la red que la comunique con el exterior, por ejemplo a la red Internet. Si el trabajo se realiza en un entorno corporativo, esto llega a ser una necesidad.

En las redes se utilizan elementos adicionales para la interconexión de elementos:

- **Repetidores**. Son dispositivos que trabajan en el nivel físico, pudiendo interconectar redes físicamente iguales. En redes Ethernet se utilizan Hubs y en Token Ring existe un elemento similar denominado Mau.

- **Conectores**: utilizados para conexionar tramos de cable entre sí, con las tarjetas de red, con los repetidores o con las rosetas. Entre los más empleados nos encontramos los conectores BNC y RJ45.

Además de los mencionados existen otros dispositivos que trabajan en niveles superiores al físico y que permiten interconectar redes.

- **Puentes (Bridge)**: trabaja a nivel de enlace, pudiendo conectar redes similares con diferente medio físico y forma de acceso.
- **Enrutadores (Router)**: trabaja a nivel de red conectando redes diferentes.

4. CONFIGURACIÓN

4.1. Configuración de servidores

Una red puede tener varios servidores instalados, y la configuración de una máquina en la red como servidor o estación de trabajo se realizará a través del sistema operativo de red.

Un tipo especial de servidores son los servidores de ficheros que, configurados como tales desde el sistema operativo de red, permiten el acceso a sus datos desde estaciones de trabajo.

Los distintos tipos de servidores que se pueden configurar son:

- **Servidores no-dedicados**. Pueden hacer función de servidor y de estación de trabajo aunque en este último caso pueden suponer una caída del rendimiento de la red.
- **Servidores dedicados**. Los que funcionan sólo como servidores de red.
- **Servidores de impresora**. Para la gestión de colas de impresión.
- **Servidores de fax**. Proporcionan servicio de fax a las estaciones de trabajo.

4.2. Configuración de estaciones clientes

En las estaciones de trabajo se tendrán que instalar y configurar los protocolos necesarios para la conexión a los servidores, teniendo en cuenta que la instalación de protocolos innecesarios puede provocar una sobrecarga en el software de red, además de un consumo inútil de memoria.

Se deberá valorar si los usuarios trabajarán con información local o centralizada y decidir entre tres tipos de configuraciones:

- Los programas y los datos estarán en el disco duro local y no son compartidos en la red. Se deberá instalar una copia de la aplicación en cada estación.
- Los programas se instalan en el servidor y los usuarios acceden a éste, pudiendo estar los datos en el disco local o incluso también en el servidor.
- Las aplicaciones se instalan de forma distribuida, parte en el servidor y parte en el cliente.
- Existe una configuración especial para los clientes ligeros que no disponen de disco local, por lo tanto, incluso para arrancar necesitan de un servidor de sistemas operativos.

4.3. Configuración de accesos externos

Además de los servidores y las estaciones clientes se tendrán que configurar los accesos externos, ya sean de la propia organización o de agentes externos a ésta. Estos accesos tendrán las mismas características que los accesos internos, sólo que con un rendimiento menor. Para permitir estos accesos la red deberá disponer de medios de interconexión con el exterior que deberán estar también correctamente configurados.

4.4. Configuración y gestión de usuarios

La división de las personas que trabajan en la red en dos grupos: administradores y usuarios, no siempre es tan simple ya que dentro de estas dos categorías se pueden establecer subgrupos atendiendo a distintos aspectos.

Por ejemplo, se podría establecer cuatro categorías de usuarios que podrían ser: Admin, Group Manager, Usuario Común y Operador. Cada grupo podría tener establecidos ciertos privilegios, que irían desde solamente poder acceder a los programas y datos concretos que utilizan, hasta poder cambiar características o aspectos de uno o varios objetos.

Será tarea del usuario Admin, poseedor de todos los derechos que permita la red, la gestión de la red y la administración de los recursos, por lo tanto, él decidirá los privilegios que tendrán los demás usuarios.

El resto de los Usuarios estará organizado en grupos de trabajo, donde el Group Manager hará las funciones de administrador para ese grupo, creando o borrando elementos, dando altas y bajas de usuarios, pero siempre dentro del grupo. Sin embargo, no tendrá la posibilidad de modificar los derechos individuales de cada usuario.

Los Operadores serán usuarios especiales que, al estar encargados de una labor concreta como pueden ser los operadores del sistema de impresión o del servidor de ficheros, tienen responsabilidades en la manipulación de ciertos recursos, aunque en algunos casos es el mismo Admin el encargado de esta labor.

La primera labor dentro de la gestión de usuarios, es la de creación de usuario y grupos; tanto en un caso como en el otro, esto implicará su configuración con lo que conlleva en cuanto a derechos sobre objetos, directorios y ficheros.

En este sentido existen diversos aspectos a configurar:

- **Restricciones en cuanto a conexión**: número de conexiones simultáneas que puede tener, fecha de caducidad de su cuenta, etc.
- **Restricciones en cuanto a contraseñas**: obligatoriedad de utilizarla, necesidad de cambiarla cada cierto tiempo, etc.
- **Restricciones en cuanto al tiempo de conexión**: indicación del momento en el que puede conectarse, etc.
- **Restricciones en cuanto a direcciones de red**: posibilidad de conectarse desde otro puesto de trabajo o siempre desde el suyo, etc.
- **Equivalencias de seguridad**: posibilidad de establecer equivalencias entre distintos usuarios para facilitar la labor de configuración de derechos.

4.5. Configuración y gestión de datos

Conlleva la instalación y administración del sistema de archivos, o sea, el manejo de archivos y directorios. En ese sentido, se pueden establecer ciertos privilegios que serán asignados indistintamente a grupos o a usuarios. La red Novell Netware, asigna los siguientes derechos:

- Derecho de apertura para leer archivos (***Read***).
- Derecho de apertura para escritura sobre archivos o directorios (***Write***).
- Derecho para crear directorios o ficheros (***Create***).
- Derecho para borrar directorios o ficheros (***Erase***).
- Derecho para ver un directorio y sus ficheros (***File scan***).
- Derecho para modificar los atributos y los nombres de directorios, pero sin posibilidad de cambiar su contenido (***Modify***).
- Derecho para cambiar los derechos de cualquier otro usuario, excepto al Supervisor (*Access control*).
- Derecho total sobre directorios, subdirectorios y archivos (***Supervisor***).

Pero independientemente de los derechos de un usuario, los archivos disponen de unos atributos que en cualquier caso prevalecerán sobre dichos privilegios, de forma que aunque un usuario tenga el derecho a borrar un archivo, si este contiene un atributo que le impide ser borrado, el usuario no conseguirá su destrucción.

En algunos sistemas de red como, por ejemplo, Windows NT, el acceso a los datos se realiza a través de carpetas compartidas a las cuales se les asignan una serie de propiedades como el número de usuarios que la pueden compartir, los distintos permisos que recaerán sobre ella...

Cuatro son los tipos de permisos que admite este sistema:

- **Acceso denegado** (*No Access*): donde se establece la conexión, pero no se puede ver el contenido de la carpeta.
- **Permiso de lectura** (*Read*): donde se pueden ver los atributos de ficheros y carpetas, se pueden ejecutar programas y existe la posibilidad de moverse por las subcarpetas.
- **Permiso de cambio** (*Change*): dispone de los privilegios de lectura y además se pueden crear y borrar carpetas, añadir y borrar ficheros, y cambiar atributos de un archivo.
- **Todos los derechos** (*Full control*): donde se dispone de todos los derechos.

Aunque también este sistema dispone de la posibilidad de asignar permisos locales sobre cada archivo individual, en cuyo caso los derechos serán los enumerados al principio de este apartado para las redes Novell Netware.

En ciertas ocasiones se imponen también restricciones en cuanto a la limitación del espacio que pueden ocupar los archivos o carpetas, o el disponible para un determinado usuario.

4.6. Configuración del sistema de impresión

La impresión en red implica tres conceptos fundamentales:

- **Las impresoras**, que constituyen el elemento principal del que podrán hacer uso los distintos usuarios de forma ordenada, podrán estar conectadas a la red directamente si disponen de tarjetas especiales, o conectadas a un servidor de impresión o de archivos, o

incluso a una estación de trabajo. El controlador de la impresora, que gestionará las tareas de impresión, se cargará en el equipo al que esté conectada o en la misma impresora si está directamente conectada a la red.

- **El servidor de impresión**, que se encarga de recibir y distribuir a las distintas impresoras conectadas a la red los trabajos, permite también distintas opciones sobre ellos como por ejemplo cancelarlos, repetirlos, etc., controla y gestiona las impresoras y las colas de impresión.
- **Las colas de impresión** son los directorios donde se almacenan estos trabajos de impresión temporalmente en forma de archivos. Pueden tener asignadas, o ser asignadas a varias impresoras. En el caso de una cola asignada a varias impresoras, los trabajos se asignarán a la impresora que en ese momento esté libre; en el caso de varias colas asignadas a una sola impresora, cada cola recogerá trabajos de usuarios o prioridades determinadas.

Un sistema de red deberá permitir también que ciertas aplicaciones que no permiten imprimir en impresoras de red puedan dirigir sus trabajos a impresoras locales.

5. MEDIDAS DE SEGURIDAD

5.1. Protección de los equipos informáticos y sus instalaciones

En este apartado, vamos a estudiar las normas que debe regir cualquier instalación informática, pública o privada, para garantizar un mínimo de seguridad sobre sus equipos e instalaciones.

5.1.1. Protección contra la electricidad estática

Todos los equipos informáticos son muy sensibles a las descargas eléctricas. Una pequeña descarga puede averiar nuestro equipo, o alguno de los componentes del mismo.

Para evitar descargas electroestáticas no deseadas todos los puntos de suministro de corriente de nuestras instalaciones deben tener **toma de tierra**. Las tomas de tierra se encargan de encauzar la electricidad estática fuera de nuestro equipo. Si nuestro enchufe no tiene toma de tierra podemos sacar algún cable desde una pieza metálica de nuestro ordenador hasta un tubo de cobre, o cualquier elemento que transmita la corriente. Hace unos años, se pusieron de moda los protectores de pantalla para la vista. La mayoría de estos protectores disponían de una pequeña pinza que se enganchaba a la carcasa del ordenador. Esta pinza tenía un cable que se conectaba al protector. Este dispositivo era una pequeña toma de tierra.

Otras alternativas son emplear unas **alfombrillas antiestáticas** o tratar **químicamente** nuestros equipos con productos antiestáticos.

5.1.2. Protección contra subidas, bajadas de tensión y cortes del suministro eléctrico

El 50% de los problemas que sufren los equipos informáticos son producidos por fallos del suministro eléctrico. En una oficina se producen al año unos 36 picos de tensión, 264 caídas de tensión, 128 sobrevoltajes y 15 apagones de más de 10 segundos. De 100 de estos accidentes, 40 provocan averías serias en los equipos en funcionamiento.

Una **sobretensión** puede quemar componentes electrónicos, su acción puede incendiar transformadores, adaptadores, hasta quemar nuestro equipo. Para evitar efectos devastadores los equipos informáticos están equipados con sistemas que cortan la alimentación en caso de sobretensión. Normalmente disponen de un **fusible**, que se funde en caso de sobrealimentación, cortando el flujo de la corriente eléctrica.

Una **caída de tensión**, o un apagón, puede hacernos perder el contenido de la memoria *RAM* de nuestro ordenador, estropear un disco duro si estábamos accediendo a él en ese momento, etc.

Para evitar estos inconvenientes disponemos de **estabilizadores de tensión**, que se encargan de regular las fluctuaciones de la corriente eléctrica.

Para contrarrestar el efecto de los apagones debemos comprar unidades ***SAI*** *(Sistema de alimentación interrumpida)*. Estas unidades se comportan como una batería auxiliar que se encarga de prolongar la alimentación eléctrica por unos minutos. Es el tiempo necesario para guardar a disco el contenido de la memoria RAM, y apagar de una forma segura nuestros sistemas informáticos.

En algunas empresas es interesante disponer de **generadores de electricidad**, por si el corte del suministro eléctrico se prolonga mucho. En locales públicos y grandes empresas es necesario este sistema para alimentar las luces de emergencia, y los paneles luminosos que indican las salidas.

Otro problema que puede aparecer en la corriente pueden ser los denominados **parásitos**. Los parásitos son electricidad electroestática introducida por máquinas, motores, dispositivos defectuosos, etc. Este problema se agrava aún más cuando no disponemos de toma de tierra. Para eliminar los parásitos existen circuitos especialmente diseñados, que se insertan en regletas, enchufes, etc.

5.1.3. Protección contra temperaturas extremas

Por temperaturas extremas entendemos exceso de calor o de frío.

Los ordenadores son más sensibles al exceso de calor. Un ordenador genera calor al funcionar; además de la temperatura del recinto donde se sitúa, la del interior de éste puede aumentar un par de grados. Para evitar estos problemas los ordenadores vienen equipados con **disipadores** de calor encima del microprocesador, y **ventiladores** que permiten airear el interior del mismo. Otro factor interesante es situar el ordenador en una zona donde circule el aire alrededor de la máquina, evitando tapar total o parcialmente las rejillas de ventilación.

El frío es un inconveniente menor ya que un ordenador puede funcionar sin problemas hasta una temperatura de unos cero grados. En caso de temperaturas menores es recomendable dotar nuestras instalaciones de **calefacción**.

5.1.4. Protección contra incendios

Un fuego producido por productos químicos o electricidad no debe apagarse **nunca con agua**, por el peligro de electrocución o de avivar más aún el fuego. La forma de sofocar un incendio en una instalación informática es mediante el uso de **extintores**. Todos los laboratorios informáticos deben estar dotados como mínimo de un extintor.

Otro elemento que no es obligatorio, pero sí deseable es un **detector de humos**, que debe ir conectado a una **alarma**, o **aspersores** contra incendios.

La protección contra incendios no sólo salva equipos informáticos, sino que también protege vidas humanas, por lo que es un apartado donde es básico prestarle una mayor atención.

5.1.5. Protección contra el agua

El elemento líquido es uno de los agentes más dañinos para nuestro ordenador. El vertido de un líquido sobre un equipo informático puede destrozarlo. Si el equipo está apagado hay que esperar a que se seque. En caso de que los líquidos contengan sales minerales u otras sustancias, es conveniente lavar la pieza con agua destilada.

Cuando se diseñe el aula hemos de tener en cuenta que el paso de tuberías no esté próximo a la localización de los ordenadores. Cualquier fuga de agua podría destrozar nuestro equipo informático. También debemos evitar las goteras.

5.1.6. Control ambiental

Otros elementos como el polvo, la humedad, la suciedad, humo, restos de comida, líquidos procedentes de bebidas, etc., pueden afectar a nuestro equipo informático. Para evitar este deterioro, hemos de mantener el lugar de trabajo limpio y ordenado.

Para proteger nuestro equipo del polvo y la suciedad, la solución más eficaz y sencilla es una funda que lo proteja.

5.1.7. Protección física

El **robo** o **sustracción** de material informático está a la orden del día. Como medidas de prevención podemos instalar **sistemas antirrobo** en las puertas y ventanas. Al finalizar la jornada laboral, y durante los descansos los laboratorios deben permanecer cerrados.

El acceso a estas salas debe estar controlado por **personal** de **seguridad**. Los soportes donde realizamos copias de seguridad como discos, *CDS*, *ZIP*, y el software de uso habitual, han de guardarse bajo llave en archivadores, cajones o armarios preparados para tal efecto.

Debe haber una única persona **encargada** de **instalar** y **desinstalar** el software cuando sea necesario.

Otra barrera de seguridad consiste en instalar **llaves** en los ordenadores. Sin estas llaves no podemos encenderlos.

5.2. Protección de datos

Una vez que tenemos protegidas nuestras máquinas, es conveniente proteger su contenido. Proteger los programas instalados y los datos almacenados en los mismos.

Gran parte de la responsabilidad de este apartado recae en los sistemas operativos que brindan un nivel de seguridad a los datos, que él mismo se encarga de almacenar.

5.2.1. Copias de seguridad

Un mecanismo de seguridad imprescindible son las copias de seguridad. En una copia de seguridad volcamos los nuevos datos que insertamos en el sistema. Así siempre existe la posibilidad de recuperar la información almacenada en nuestro sistema.

Las primeras copias de seguridad volcaban completamente el contenido del sistema en un soporte. Las copias que se hacen actualmente son denominadas **copias incrementales**. En este tipo de copia sólo se graban los datos nuevos en el soporte.

Los soportes en los que se realizan estas copias suelen ser cintas magnéticas, unidades *ZIP*, o *CD-ROM*, por ser baratos y disponer de una gran capacidad.

La **periodicidad** con la que debemos realizar estas copias depende de la cantidad de información que generemos a lo largo de la jornada, la importancia de la misma, y el riesgo de nuestro sistema. Como mínimo se ha de realizar una copia mensual del sistema completo, y una copia semanal; para sistemas de gran riesgo o con mucho movimiento es recomendable realizar copias a diario.

Otro mecanismo de seguridad que resulta interesante aplicar consiste en tener dos copias de seguridad, por si alguna se deteriora.

Una opción interesante son las denominadas copias de seguridad "offsite". Una copia de seguridad offsite es realizada fuera de la oficina donde se almacenan los datos. Emplean redes y podemos tener copias de nuestros datos en una ubicación diferente a la de los datos originales, lo que posibilita en caso de catástrofe (incendio, inundación, terremoto) recuperar los datos perdidos.

5.2.2. Control de acceso

Los sistemas en red son **multiusuario**. Por ser multiusuario entendemos que muchas personas acceden al sistema. Parece necesario entonces introducir un mecanismo de control de acceso a los distintos usuarios del sistema.

Por esta técnica comprendemos que cada usuario de nuestro sistema ha de estar identificado. Hay muchas formas de identificarlo. Atendiendo a la característica por la que identificamos a nuestro usuario podemos clasificar los sistemas de autentificación en:

1. **Por características físicas del usuario (biométrica)**: dentro de estos sistemas tenemos identificación a través de huellas dactilares, reconocimiento de voz, de la retina, etc.
2. **Por la posesión de un objeto**: como tarjetas magnéticas, llaves, etc.
3. **Por el conocimiento de un secreto**: como una palabra o **contraseña**.

De todos estos métodos el más sencillo, barato y extendido es el de la contraseña. Se basa en darle a cada usuario un nombre de **usuario** y una **contraseña**. Al iniciar la sesión, el usuario introduce su identificador o *login*, y posteriormente su clave o *password*. Cuando él escriba el *password*, lógicamente no debe verse en pantalla.

Una clave, para ser eficiente, debe tener las siguientes características:

1. Nunca debe coincidir con el nombre de usuario.
2. No debe ser ninguna palabra del diccionario. Algunos programas usados por *hackers* intentan entrar en un sistema usando un diccionario. Un ejemplo clásico de este programa es *John The Ripper*.
3. Ha de ser secreta, el usuario no debe comunicarla a ninguna otra persona, nunca ha de escribirla en ningún papel o documento.
4. No debe ser una palabra fácil de adivinar como el nombre de un familiar, de tu perro, la marca de tu coche, tu año de nacimiento, etc. Los *hackers* usan técnicas de *"ingeniería social"* para sonsacar datos de los usuarios de un sistema, como dónde viven, el nombre de sus hijos, donde estudió, etc.

5. Debe mezclar, a ser posible, mayúsculas y minúsculas, contener números y letras.
6. Ha de ser lo suficientemente larga como para que sea difícil de adivinar, y lo suficientemente corta como para que sea fácil de escribir.

A cada usuario del sistema se le asignan una serie de **permisos** sobre los archivos. Para simplificar esta tarea, el administrador del sistema se encarga de crear **grupos** con una serie de permisos, preasignados. Cuando damos de alta a un nuevo usuario se le asigna un grupo al que pertenece. Por ejemplo, en una universidad de informática podemos crear grupos de alumnos, alumnos de proyecto, alumnos colaboradores, profesores, profesores de informática, jefes de departamento, y el administrador del sistema, cada uno con permisos diferentes y acceso a distintos programas.

En **UNIX** y **LINUX** podemos cambiar los permisos de un archivo con el comando **chmod**, en *MS-DOS* con **attrib**, en *Windows* se hace accediendo a las **propiedades** del fichero.

Para crear usuarios nuevos en *UNIX/LINUX* disponemos del comando **adduser**, y en *Windows* lo podemos hacer desde el **panel de control**, pulsando el icono de **usuarios**, y a continuación **nuevo usuario**.

A cada usuario se le debe asignar un espacio de disco, para que almacene sus propios ficheros. Este espacio es lo que se denomina **cuota de disco**. El tamaño de la cuota de disco debe ser diferente para cada grupo, intentando ajustarnos a las necesidades reales de cada uno.

En *UNIX/LINUX* podemos ver nuestra cuota de disco con el comando **vquota**.

En el tema anterior puede encontrar más información, sobre cómo se puede administrar una red local.