

*Redes en educación 2*

*Capítulo 6*

*Gestión y administración  
de redes*





### Í N D I C E

1. Introducción.	3
2. Localización de archivos y datos.	4
2.1. Sistemas operativos.	4
2.2. Servidor de aplicaciones.	5
2.3. Archivos de datos.	5
3. Gestión de usuarios.	7
3.1. El entorno de trabajo.	7
3.2. Autenticación de usuarios y permisos de red.	8
a) Linux.	10
b) Windows.	10
4. Detección y solución de problemas de red.	12
4.1. Problemas físicos.	13
4.2. Problemas de conectividad.	14
4.3. Utilidades TCP/IP para el chequeo de la red.	16
4.4. Analizadores de red.	17
4.5. Tester.	17
5. Seguridad en la red.	18
5.1. Políticas de seguridad.	19
5.2. Cortafuegos.	20
a) Tipos de cortafuegos.	20
b) Arquitecturas de cortafuegos.	21
c) Cortafuegos embebidos.	22
5.3. Sistemas antivirus.	22
a) Tipos de virus.	23
b) Antivirus.	25
c) Otras medidas de seguridad antivirus	26
5.4. Copias de seguridad.	28
a) Dispositivos para la copia de seguridad.	28
b) Software de copia de seguridad.	30
c) Planificación y automatización del proceso.	31

### Anotaciones

## Capítulo 6

5.5. <i>Imágenes.</i>	33
<b>6. Diseño y funcionamiento de un aula en red dentro de un centro docente.</b>	<b>34</b>
6.1. <i>Introducción.</i>	34
6.2. <i>¿Cómo empezar?</i>	36
a) Tipo de red.	37
b) Decisiones técnicas.	37
c) Decisiones pedagógicas.	42
6.3. <i>Seguridad.</i>	43
a) Seguridad del sistema.	44
b) Seguridad de contenidos.	44
c) Seguridad antivirus.	45
d) Seguridad ante intrusos.	46
6.4. <i>Aplicaciones.</i>	46
a) Utilidades.	47
6.5. <i>Organización y mantenimiento.</i>	48
6.6. <i>Propuesta.</i>	49
<b>Ilustraciones</b>	<b>50</b>

### Anotaciones

### 1. Introducción.

La administración de redes debería crear sistemas estandarizados de trabajo de manera que su tratamiento técnico fuera lo más sencillo posible. Sin embargo, en numerosas ocasiones nos encontramos con que esto no es posible debido a que los usuarios intervienen de forma sistemática en el sistema cambiando dichas configuraciones. Para evitar que estas actuaciones deterioren el sistema el administrador debe imponer una serie de restricciones para la modificación de la configuración de las estaciones de trabajo por parte de los usuarios. En los centros educativos esta tarea es mucho más ardua debido a sus peculiares condiciones:

- En las redes de centros docentes coexisten distintos objetivos: académicos y administrativos que, necesariamente, deben ser considerados.
- La informática es, en muchos centros, materia formativa, de manera que es necesario utilizar los equipos como herramienta de aprendizaje y modificar de forma consciente los equipos.
- Intervención consciente o inconsciente sobre la configuración de los equipos de manera que se pierde de forma completa o parcial su funcionalidad.
- Actualmente no existe un sistema eficiente y generalizado de mantenimiento del hardware en los centros docentes, en algunos casos depende del propio profesorado y, en otros, las empresas responsables de estas tareas no ofrecen el tiempo de respuesta adecuado.
- Las aulas y equipos informáticos son usados de forma intensiva a lo largo del periodo lectivo.
- El nivel de los usuarios es muy heterogéneo debiendo ser, en muchas ocasiones, responsabilidad de profesorado, poco conocedor de los elementos de hardware y software instalados en los equipos, el responsable en cada momento de su utilización por el alumnado.

Todos estos factores nos obligan a establecer una serie de restricciones de utilización y políticas de usuarios que deben ser aplicados a los sistemas informáticos de los centros educativos. Además, estas restricciones deben ser entendidas por el profesorado y la dirección del centro de manera que se eviten susceptibilidades y se llegue a comprender la importancia de su aplicación por la seguridad y el beneficio del centro.

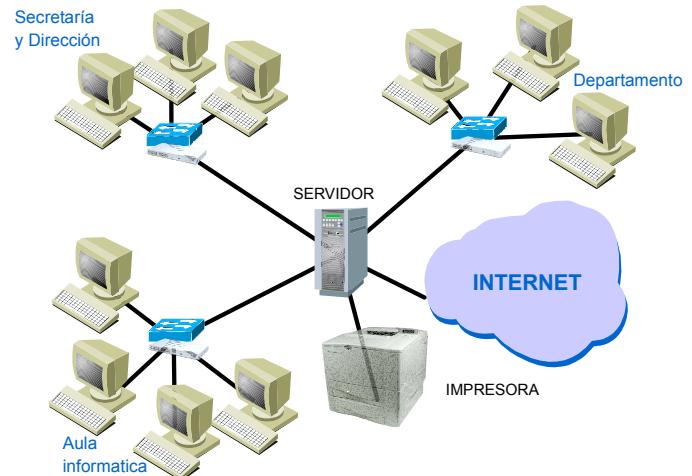


Ilustración 1: Las redes escolares están dedicadas a múltiples propósitos que dificultan la definición de su estructura

### Anotaciones

### 2. Localización de archivos y datos.

Una de las funciones básicas de un sistema informático de red es la de compartir archivos. Estos pueden ser de distinto tipo, desde aplicaciones informáticas a documentos elaborados tanto por los alumnos como por el profesorado. Por lo tanto, una de las decisiones que deben ser tomadas en primer lugar es dónde se deben instalar los programas y cuál debe ser la ubicación de los archivos.

En los centros docentes se instalan mayoritariamente PC, es decir, ordenadores autónomos capaces de gestionar programas, por lo que cuando se instale cualquier aplicación, esta se instalará, por defecto en el directorio o carpeta asociada a dicha aplicación. El problema radica en quién o quiénes pueden realizar esta función.

Por otro lado, existen distintas posibilidades a la hora de ubicar los archivos de datos, por regla general, y si se pretende que existan documentos o ficheros compartidos, se deben establecer unos criterios que faciliten el acceso a estos archivos a todos los usuarios en función de las políticas de seguridad establecidos, es decir, todos los usuarios deben seguir los mismos criterios a la hora de ubicar este tipo de archivos. Ahora bien, este proceso debería ser completamente flexible y transparente para el usuario puesto que, en muchos casos, no tiene la formación suficiente para actuar con autonomía y eficacia en esta labor.

#### 2.1. Sistemas operativos.

Desde el punto de vista del administrador, el sistema operativo es el software más importante de la red de ordenadores en su conjunto y de cada PC individual, de ahí, que las decisiones sobre su instalación, configuración y acceso sean las más importantes a adoptar en los primeros momentos, no debiéndolas dejar a la improvisación en ningún caso. Existen distintas posibilidades de instalación:

- Sistema operativo basado en servidor: el sistema operativo se ejecuta en el servidor y los equipos acceden a él a través de la red. Esta opción puede ejecutarse también con un sistema mixto de programa cliente que se ejecuta en cada PC, sin llegar a descargarse todo el sistema operativo.
- Sistema operativo instalado en los equipos: Este sistema permite que los equipos puedan trabajar en red o de forma autónoma, tiene el inconveniente de que el sistema operativo se debe instalar y actualizar en cada uno de los puestos. Sobre este sistema podemos administrar distintos tipos de redes tales como sistemas cliente-servidor, sistemas igual a igual, o sistemas mixtos.

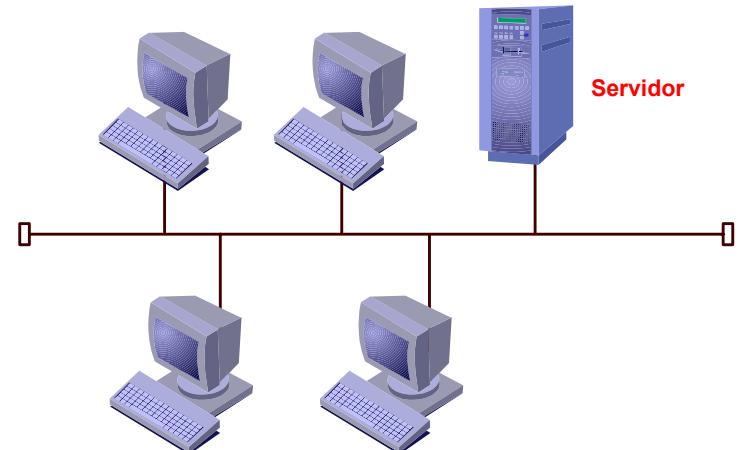


Ilustración 2: Una red basada en servidor consta de terminales "tontos" que dependen completamente de un servidor.

#### Anotaciones

## Capítulo 6: Gestión y administración de redes.

Una instalación de red con un sistema operativo basado en servidor se encuentra actualmente obsoleto debido, fundamentalmente, a que ya existen múltiples herramientas que facilitan la instalación del sistema operativo y a la bajada de los precios de los pc, que permiten una mayor capacidad y velocidad en el tratamiento de datos con un precio menor. Por otro lado, se evita la saturación del servidor y se consigue una disminución del tráfico de red.

Con respecto a la segunda opción, deberemos optar por un sistema u otro en función de las necesidades del centro. Tal como ya se ha reflejado en los capítulos anteriores, el modelo basado en servidor, donde la gestión de las políticas de seguridad está centralizada y la realizan herramientas especialmente diseñadas y preparadas para garantizar eficacia y flexibilidad, debe ser el utilizado en los centros docentes, si bien, no deberemos descartar las otras soluciones en función de las necesidades académicas y administrativas.

### 2.2. Servidor de aplicaciones.

Las aplicaciones basadas en servidor permiten ofrecer a los usuarios un entorno estable de trabajo, a la vez que evitan la carga de tareas al administrador. Este diseño presenta las mismas ventajas que el disponer de un sistema operativo instalado únicamente en el servidor, sin embargo, presenta los mismos inconvenientes.

Para que una red disponga de un servidor de aplicaciones y que estas funcionen de forma adecuada en cada equipo, se necesita que en estos se instalen y configuren:

- El registro.
- Las librerías.
- Accesos desde el menú inicio e iconos de la aplicación.

Estas tareas son bastante complejas de realizar en un entorno Windows, aspecto que debe ser tenido en cuenta, pues si bien las ventajas de administración pueden ser interesantes, su instalación puede ser, realmente, difícil. Por otro lado, y dentro de las restricciones que impongamos, cada usuario debería poder configurar, hasta cierto punto, su entorno de trabajo, por lo que deberíamos crear un sistema en el que estas opciones quedaran almacenadas en algún lugar del servidor o del equipo local.

### 2.3. Archivos de datos.

Los datos que se generan en un centro son de características muy distintas y que requieren un tratamiento, por lo tanto, diverso. Desde un punto de vista funcional, deberemos hablar de dos tipos de archivos de datos, los generados por el profesorado y que podríamos considerar como documentos de trabajo y los documentos almacenados en bases de datos.

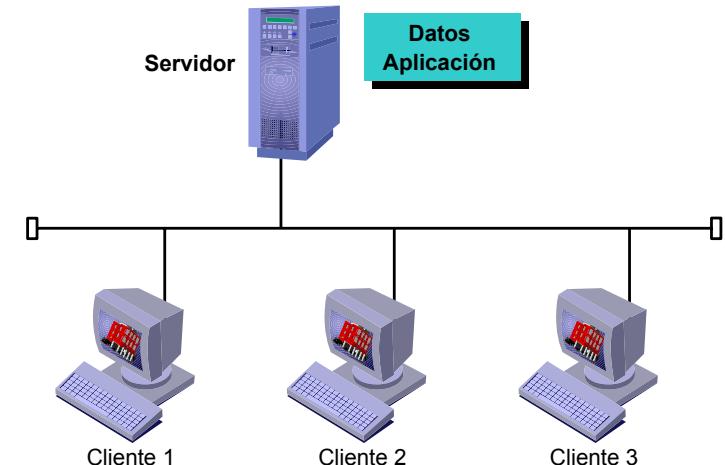


Ilustración 3: Un servidor de aplicaciones permite la utilización de un mismo programa desde los distintos equipos de la red.

### Anotaciones

## Capítulo 6

Los documentos administrativos deben ser accesibles sólo para un número muy limitado de personas en función de su cargo en el centro. Director y secretario desempeñan unas funciones que requieren el uso conjunto de diferentes documentos, mientras que el Jefe de estudios y los jefes de departamento o coordinadores de ciclo generan y deben compartir otro tipo de documentación.

Las bases de datos que gestionan la información que se almacena en un centro son herramientas de uso habitual, IES2000 y ESCUELA, entre otros, almacenan datos confidenciales de los alumnos y sus familias y su acceso por personas no autorizadas, la manipulación o la pérdida son acontecimientos que deben ser evitados. Con el fin de solucionar estos problemas, los programas de base de datos suelen estar pensados para instalarse en un servidor y que puedan ser accesibles desde distintos equipos en función de una serie de criterios.

En general, debemos indicar que la seguridad de los documentos, desde cualquier punto de vista, es un elemento crítico de la administración de una red. Para conseguir esta seguridad de una forma eficaz y sencilla deberemos considerar la posibilidad de almacenar todos estos datos en un servidor, fundamentalmente por dos razones:

- Mayor facilidad a la hora de aplicar las políticas de seguridad al encontrarse en un único sitio.
- Mayor seguridad ante pérdidas, puesto que si los datos se almacenan en un único lugar, la realización de copias de seguridad es mucho más sencilla.

Por otro lado, si los documentos de trabajo generados por el profesorado están pensados para ser compartidos por todo el claustro o partes significativas del mismo nos encontramos con la necesidad de situarlos en el servidor, y no en equipos locales debido a:

- Una única ubicación de los archivos facilita su localización con independencia de quién los puede haber creado.
- El servidor es una máquina que siempre se encuentra en funcionamiento, mientras que un equipo local puede encontrarse apagado por lo que el acceso a la información almacenada en él sería imposible.
- La seguridad a la hora de definir los accesos de los distintos tipos de usuario y a la hora de realizar los correspondientes backups.

Así, debemos tener como criterio fundamental la centralización de los documentos de datos para facilitar su compartición y garantizar su seguridad.

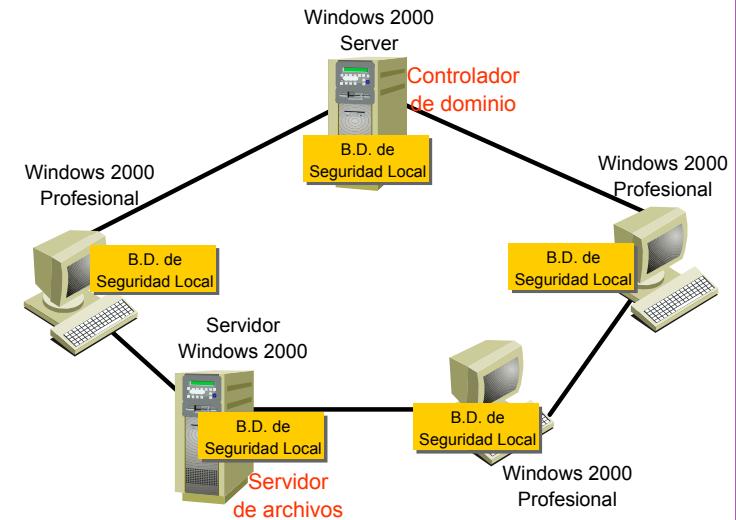


Ilustración 4: Al acceder todos los equipos a un mismo administrador de archivos se simplifica la realización de copias de seguridad de los documentos.

### Anotaciones

### 3. Gestión de usuarios.

En un centro educativo son muchos los usuarios que han de utilizar la red informática. Su nivel de conocimiento de las distintas herramientas y servicios es muy variado, pero, además de este factor de heterogeneidad, debemos tener en cuenta, que el nivel de responsabilidad también va a ser muy distinto (administrador, profesorado, alumnos, etc.) por lo que debemos establecer unas directrices, o políticas, que permitan un uso adecuado de la red.

Podemos considerar la existencia de grupos de usuario ya que de esta forma facilitamos la gestión de las políticas de seguridad, pero, del mismo modo, debemos establecer unos parámetros para cada usuario individual.

Cuando hablamos de políticas de seguridad y de gestión y control de acceso a archivos y documentos debemos tener en cuenta las posibilidades de trabajo que ofrece el sistema operativo con el que estemos trabajando. Tanto Linux como Windows aportan opciones que pueden considerarse, en función de las experiencias y expectativas de los administradores, igualmente válidas. Por ello, no vamos a entrar a analizar en profundidad cada uno de estos elementos, simplemente, vamos a aportar una serie de variables que deben ser tenidas en cuenta, más, teniendo en cuenta, que pueden coexistir equipos con ambos sistemas operativos en una misma red.

#### 3.1. El entorno de trabajo.

El principal problema que nos encontramos cuando un profesor o un alumno acceden a un equipo conectado en una LAN es que, en la mayoría de las ocasiones desconoce cómo puede y debe actuar. Evidentemente, la formación en este sentido sería un elemento fundamental, sin embargo, ésta, debería estar dirigida a la utilización como usuario y no a su administración.

El administrador debe contemplar todos los factores que pueden incidir en facilitar el trabajo de los usuarios a la vez que lo protege de posibles cambios, por lo que debería, en primer lugar, procurar que el entorno que apareciera en cada equipo, fuera similar y, que los procedimientos que deba ejecutar el usuario sean similares con independencia de la máquina que esté empleando.

Para lograr este objetivo es necesario la utilización de diversas herramientas, sea cual sea el sistema operativo con el que se esté trabajando. En general, el entorno de trabajo de un usuario es el escritorio y el software que tiene instalado en su equipo, por lo que es conveniente adoptar las siguientes medidas:

- Garantizar que un usuario no autorizado pueda modificar la configuración del escritorio o realizar instalaciones de programas.

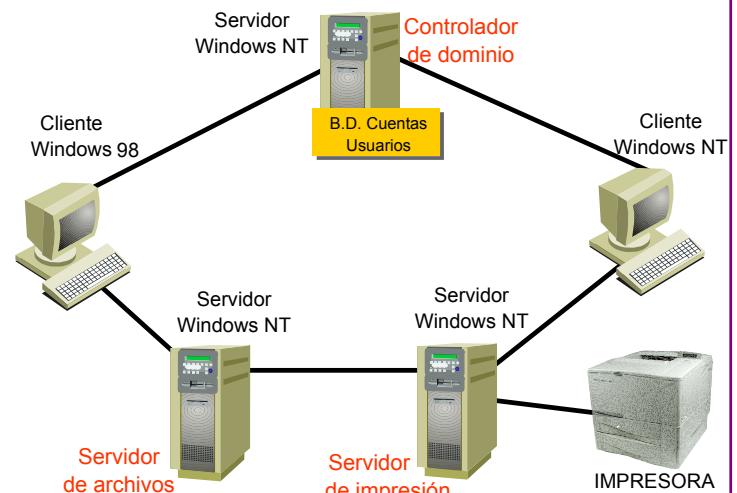


Ilustración 5: El controlador de dominio gestiona la base de datos de usuarios de manera que cualquier persona que acceda a un equipo deba identificarse para poder utilizar los distintos servicios.

### Anotaciones

- Crear un sistema que permita que las sesiones de trabajo de cada usuario sean almacenadas en servidor de manera que cuando inicie una sesión en un equipo distinto, le aparezca el mismo entorno que estaba empleando hasta ese momento.
- Mantener un sistema común a la hora de establecer la nomenclatura de las distintas conexiones a unidades de red.
- Configurar un acceso común a las impresoras.

### Para pensar:

*En numerosas ocasiones encontramos que, por ejemplo, el fondo de escritorio ha sido modificado por algún alumno después de una visita a Internet, ¿se te ocurre alguna medida para evitar que esto se produzca?*

Otro de los factores a tener en cuenta es que el usuario es muchas veces, y debido a la falta de conocimiento, el causante de errores en los equipos y, por ello, es también conveniente crear sistemas que permitan un sistema eficiente de autenticación y de gestión de permisos. Con usuarios autenticados se permite, por un lado, un acceso restringido a la red de usuarios que no pertenezcan al centro y, por otro, restringir el acceso a determinados elementos de la red, y, por tanto, un control exhaustivo de quién puede hacer qué.

La forma óptima de conseguir esto es, por un lado, la creación de un perfil estándar a partir del cual se generen los perfiles de todos los usuarios y, por otro, almacenar todos estos perfiles en un servidor de manera que cuando un usuario se identifique al acceder a la red, la máquina local en la que se encuentre cargue la configuración de su escritorio (ya sea en Windows o en Linux) y los parámetros de la última sesión guardada.

### 3.2. Autenticación de usuarios y permisos de red.

Cuando estamos trabajando con un sistema operativo multiusuario, debe existir un método que permite identificar a cada uno de los usuarios.

Tanto en windows como en linux o netware, existe un procedimiento para realizar esta operación. Esto es necesario ya que en función de cada usuario el sistema debe facilitarle unos privilegios.

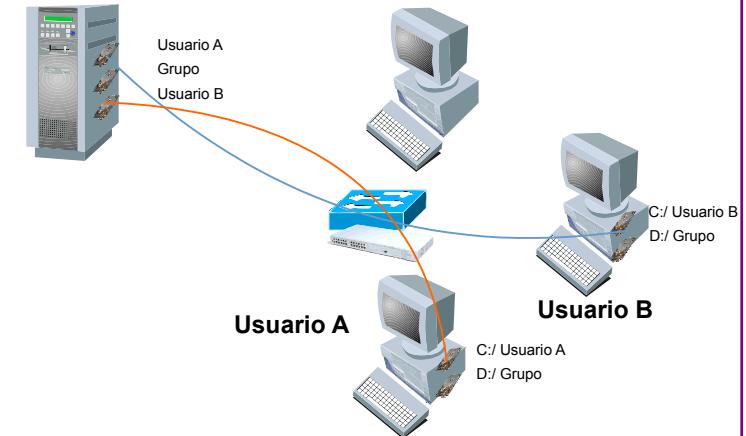


Ilustración 6: Entorno de trabajo: Un sistema centralizado permite mantener un entorno similar de trabajo en cualquier estación

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

Todas estas acciones están encaminadas, por un lado, a que sólo determinadas personas puedan acceder a archivos, elementos del sistema operativo o programas en general en base a las funciones de administración que se les haya otorgado. Por otro lado se pretende que cada persona acceda a sus archivos de forma automática una vez que sea identificado por el sistema. Establecemos, por lo tanto, dos sistemas de seguridad:

- Acceso al sistema de archivos: Todos los datos que disponemos en la red se almacenan en forma de archivos. Cuando implantamos un sistema de seguridad pretendemos que personas no autorizadas puedan acceder a dichos archivos o que puedan modificarlos o borrarlos. Para evitar este acceso se suelen emplear dos sistemas:
  - Permisos de acceso controlados mediante listas de control de usuarios en las que se recoge los permisos que de forma particular se asigna a cada usuario o grupos de usuarios. Estos permisos suelen ser de lectura, escritura, copia, etc.

### Nota:

*Los sistemas operativos que emplean sistemas de archivos fat16 y fat 32 no pueden asignar permisos ya que no tienen una lista de control de acceso para cada archivo. Cuando empleamos un sistema NTFS sí podemos establecer estos permisos.*

- El cifrado de datos permite que los datos de acceso a los archivos y los permisos se encuentren cifrados de manera que no puedan ser interpretados por terceras personas.
- Verificación de identidad. Es evidente que si no se verifica correctamente qué usuario quiere acceder a un archivo, el sistema descrito anteriormente no sería válido. De este modo, los sistemas operativos deben establecer mecanismos que garanticen la identidad de los usuarios, estos son los mecanismos de verificación que suelen consistir en un intercambio de información entre el servidor donde se encuentran los datos de cada usuario y la máquina que accede a la red y a la que se solicita el envío de un login y un password que es cotejado con la base de datos de usuarios y le concede el acceso al sistema de archivos con las restricciones asignadas a su cuenta específica. Existen múltiples sistemas de verificación de identidad:
  - Autentificación ante un servidor FTP mediante los comandos USER y PASS.

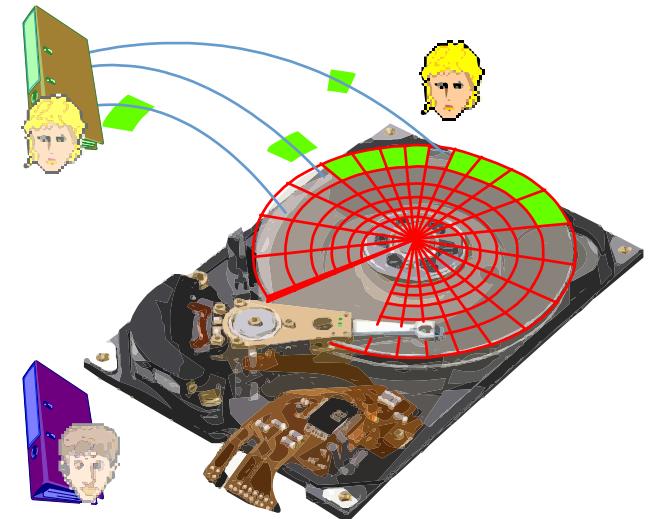


Ilustración 7: NTFS: Almacena en su lista de archivos de datos que permiten controlar el acceso de los usuarios a cada directorio

## Anotaciones

- o Kerberos es el sistema de autentificación usado en windows 2000/Active directory. Todos los datos trasmidos a la hora de identificarse el usuario lo hacen de forma cifrada.
- o Los certificados digitales son certificados de instituciones que garantizan que la información del usuario y su clave pública son veraces.
- o La autentificación biométrica es una de las tecnologías que se están incorporando actualmente a los equipos domésticos y que permiten la identificación del usuario mediante su huella dactilar.

### a) Linux.

Ya desde sus orígenes Linux nació como un sistema multiusuario y desde el mismo proceso de instalación exige la existencia de un administrador denominado “root” y solicita la creación de otros usuarios con una serie de privilegios. La única forma de acceder al sistema es poseer una cuenta que habilite a cada usuario. Cada usuario, además, pertenece a un grupo propio y pueden crearse nuevos grupos con el fin de compartir carpetas, puntos de montaje u otros elementos que puedan tener en común distintos usuarios. Tanto los usuarios como los grupos son identificados con un número único asignado a la conexión.

La capacidad de linux a la hora de otorgar permisos es muy amplia ya que este sistema operativo permite determinar qué usuarios pueden acceder a qué carpetas y con qué derechos permitiendo así una absoluta flexibilidad. Si accedemos a cualquier archivo en linux observamos cómo, en función de si se trata del root, del usuario propietario de ese archivo o de un grupo de usuarios, dispone de una serie de privilegios sobre dicho archivo.

### b) Windows.

Los sistemas de windows han sufrido una gran evolución desde sus orígenes. La versión 3.x de windows comenzó a implementar opciones de trabajo en grupo, posteriormente, y a partir, sobre todo, de Windows 98 y, especialmente, de windows NT se crearon opciones de trabajo en red de gran potencia dentro de sistemas igual a igual o cliente-servidor. Las últimas versiones de windows se asimilan bastante en prestaciones a las proporcionadas por linux, si bien presentan grandes diferencias en lo que respecta a su arquitectura interna y funcionalidad. Las directivas del sistema permiten realizar este control en los distintos sistemas operativos windows, pudiéndose aplicar restricciones mediante la creación de archivos de directivas de sistema que pueden ser aplicados a usuarios individuales o a grupos. Otra forma de realizar esta tarea es accediendo directamente al registro de Windows mediante los programas poledit (windows 98) o regedit (windows 2000), sin embargo, se pueden cometer errores tipográficos de difícil localización y que generen mal funcionamiento del equipo.



Ilustración 8: Sistemas de autentificación: Las últimas tendencias en seguridad se dirigen a la autentificación biométrica de usuarios

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

La idea fundamental en la que se basa la autenticación de usuarios es conocer, con certeza, quién está accediendo a la red en cada momento y qué permisos tiene para modificar la estructura de software creada. Algunas de las operaciones que pueden realizarse son:

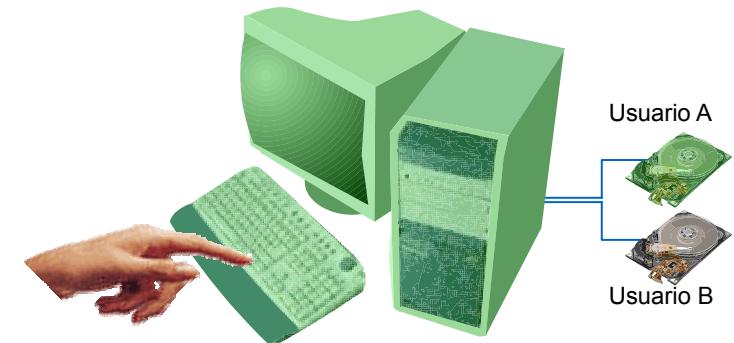
- Restricción de las aplicaciones de manera que se instalen aquellas que se consideran necesarias y altamente estables y compatibles entre sí, evitando la instalación de otras que no tengan esas garantías.
  - Impedir que aparezca el comando ejecutar en el menú inicio, impidiendo así, que puedan ejecutarse aplicaciones del sistema o programas no deseados.
  - Crear una lista común de archivos ejecutables accesibles a los usuarios, eliminando de ella aquellos ejecutables que no deseemos que puedan ser empleados por personas que no sean administradores o no dispongan de determinados privilegios.
  - Evitar el acceso al símbolo del sistema evitando que se puedan ejecutar comandos de MS-DOS.
- Evitar la modificación del interfaz creando uno estándar de manera que no se tenga acceso a determinadas funciones del escritorio.
  - Restringir las opciones de configuración de los distintos elementos del panel de control.
  - Evitar el acceso a las distintas herramientas de configuración del registro.
  - Evitar que se modifiquen elementos de configuración del monitor.

### Nota:

Windows 98 dispone de la herramienta *poledit* para la edición del registro del sistema operativo, mientras que windows 2000 dispone de *regedit*. Estos editores se pueden utilizar desde el comando ejecutar del menú inicio.

*TweakUI* es otra herramienta de Windows que facilita el control del entorno de trabajo.

- Evitar el acceso a determinados archivos o unidades de disco y de red.



**Usuario A**

Ilustración 9: Restricciones del SO: Permiten eliminar el acceso a unidades de disco en función del usuario que acuda al sistema

## Anotaciones

### Analogía:

Cuando ocultamos una unidad de disco, lo que estamos haciendo, realmente, es quitar el ícono de acceso a dicha unidad. La unidad sigue existiendo, sin embargo no es accesible a cualquier usuario. Estaríamos tapiando una puerta de comunicación entre dos habitaciones, el entorno del usuario y el lugar donde se almacenan los programas y archivos.

## 4. Detección y solución de problemas de red.

El mantenimiento de una red de ordenadores es una de las tareas que más tiempo conlleva cuando no se han tenido en cuenta las medidas de seguridad que hemos expuesto hasta ahora. En general, los problemas que pueden aparecer a la hora de trabajar con una red de ordenadores pueden tener los siguientes orígenes:

- Problemas físicos: rotura de algún cable, avería de un concentrador, fallos eléctricos, etc.
- Problemas de conectividad debido a una configuración incorrecta de los protocolos en los equipos, routers, servidores, etc. de nuestra red.
- Incompatibilidades entre aplicaciones.
- Ataques de virus o intrusos.
- Errores de usuarios.

La aparición de cualquiera de estos problemas es una situación habitual, teniendo en cuenta que el orden de aparición será, probablemente, inverso al que hemos empleado a la hora de presentar los problemas.

Para detectar y solucionar estos problemas, debemos emplear un protocolo de actuación eficaz. En primer lugar, debemos ser conscientes de las limitaciones con las que nos encontramos, por lo que es posible que lleguemos a detectar el problema sin poder llegar a solucionarlo por nosotros mismos.

Los pasos que deberemos realizar son:

1. Adquirir la mayor cantidad de indicios o pruebas del fallo que se está produciendo.
  - a. Anotar mensajes de error.
  - b. Hablar con las personas que han detectado los fallos.

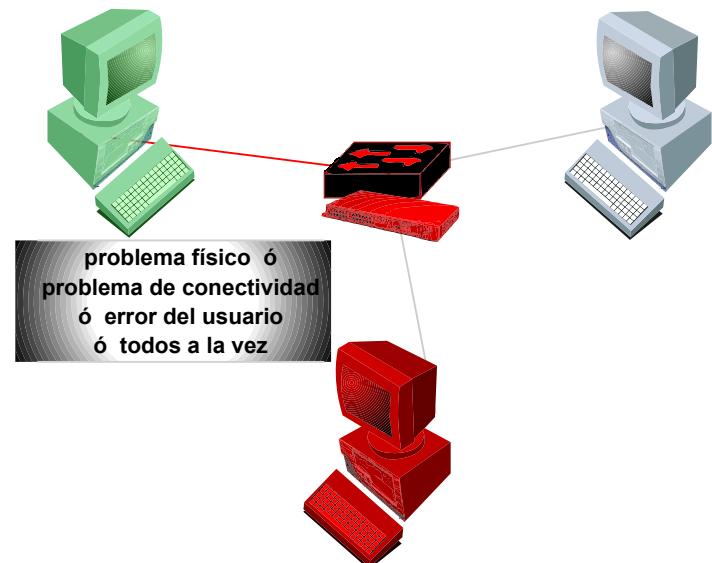


Ilustración 10: Problemas de red: El origen de los fallos de comunicación en una red pueden ser de muy distintos tipos

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

- c. Comparar el rendimiento del equipo con otros con las mismas características y configuración.
  - d. Descartar aspectos de conexión eléctrica, cableado, encendido, etc.
2. Recabar datos que puedan facilitar la elaboración de una hipótesis y las acciones a tomar.
    - a. Analizar manuales y realizar búsquedas en Internet que nos hablen de ese mismo problema u otros similares.
  3. Formular una hipótesis sobre la causa del fallo una vez que hemos analizado todos los datos.
  4. Efectuar las acciones necesarias en función de la hipótesis formulada.
  5. Evaluar los cambios realizados.
  6. Crear una ficha de actuación ante esa avería.

Sobre estas acciones, deberemos tener en cuenta que una actitud ordenada y sistemática nos va a facilitar la tarea, y dentro de esta actitud deberemos anotar todos y cada uno de los pasos que vamos adoptando para que sepamos que operaciones hemos realizado en cada momento. Se trata, en definitiva, de un método inductivo de trabajo que se ha de sustentar, sobre todo, en la información de la que se disponga y de las experiencias previas.

De los distintos problemas que hemos comentado, vamos a pasar a analizar los dos grupos que más pueden interesar.

### 4.1. Problemas físicos.

Las redes de ordenadores suelen ser altamente confiables y, una vez que se ha realizado la instalación del cableado y ha sido adecuadamente testeado es muy difícil que aparezcan los problemas. Sin embargo, debido a accidentes o acciones conscientes se pueden producir el deterioro de los cables o su desconexión. Por lo tanto, deberemos, en primer lugar, observar que se encuentran en perfecto estado y conectados adecuadamente, analizar los leds de las tarjetas de red y observar cómo actúa el equipo cuando solicitamos el acceso al entorno de red.

Una pista que nos puede indicar claramente si nuestro cable está en mal estado o desconectado es cuando aparece el mensaje en la barra de tareas de que el cable de red se encuentra desconectado, aunque nosotros observemos que está perfectamente insertado en la roseta de conexión.



Ilustración 11: Problemas físicos: Uno de los problemas más frecuentes es el fallo del conector en la tarjeta, por lo que deberá comenzar cualquier operación revisando esta conexión

### Anotaciones

## Capítulo 6

En ocasiones y cuando la instalación de la red no ha sido convenientemente probada puede suceder que algún elemento del subsistema horizontal presente fallos. Por ejemplo, conexiones internas en rosetas, latiguillos, conexiones en el patchpanel, etc. Por eso, cuando nos encontramos en una situación de este tipo un procedimiento adecuado sería el testeo de los cables (si es posible) o el cambio de conexión para comprobar si el mensaje es similar.

### 4.2. Problemas de conectividad.

En numerosas ocasiones observamos como, después de realizar una conexión a una red, configurar una tarjeta o intentar agregar un equipo a un grupo nos podemos encontrar problemas. Por regla general, estos problemas se deben a errores en la configuración de protocolos.

Cuando nuestra red dispone de un servidor de DHCP, todo el proceso de configuración de la conexión es bastante sencillo. Sin embargo, si debemos introducir nosotros los datos (direcciones IP, direcciones de servidor DNS, puerta de enlace, máscara de subred, etc.) podemos cometer pequeños errores que van a impedir la comunicación.

#### Nota:

*Un servidor de DHCP proporciona a una red de ordenadores los datos de configuración de una forma dinámica evitando los posibles errores a la hora de introducirlos manualmente. Optimiza el proceso de configuración y realiza una gestión más racional de la red.*

Los errores más habituales pueden deberse a no disponer de forma adecuada los protocolos, por ejemplo, no emplear los mismos protocolos en todos los equipos, introducir mal una dirección IP, no haber instalado adecuadamente la tarjeta de red, etc. Cada problema nos va a ofrecer un error distinto.

- No aparece nuestro equipo ni disponemos de entorno de red: el problema se deberá, probablemente a la configuración de la tarjeta.
- No tenemos acceso a la red: mala configuración de la dirección IP.
- No tenemos acceso a Internet: errores al introducir la puerta de enlace o las direcciones de los servidores DNS.
- Mensaje de error al acceder el equipo a la red: posible conflicto con otras direcciones IP.

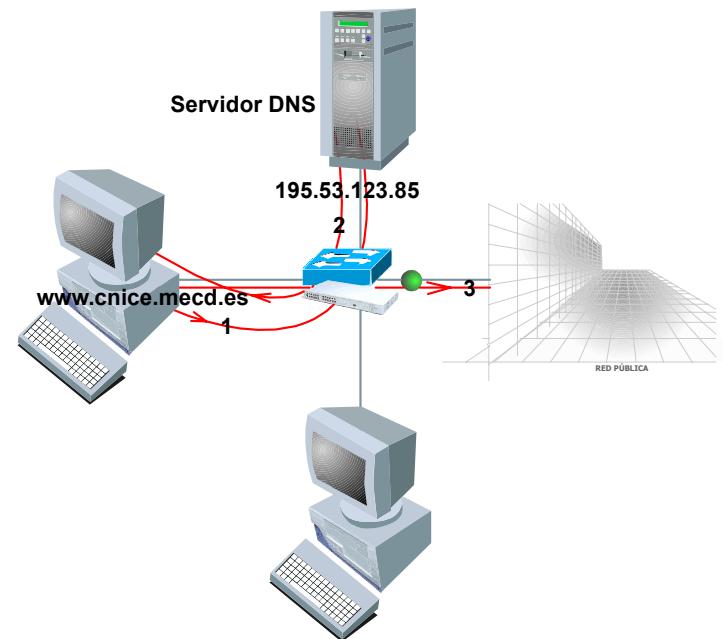
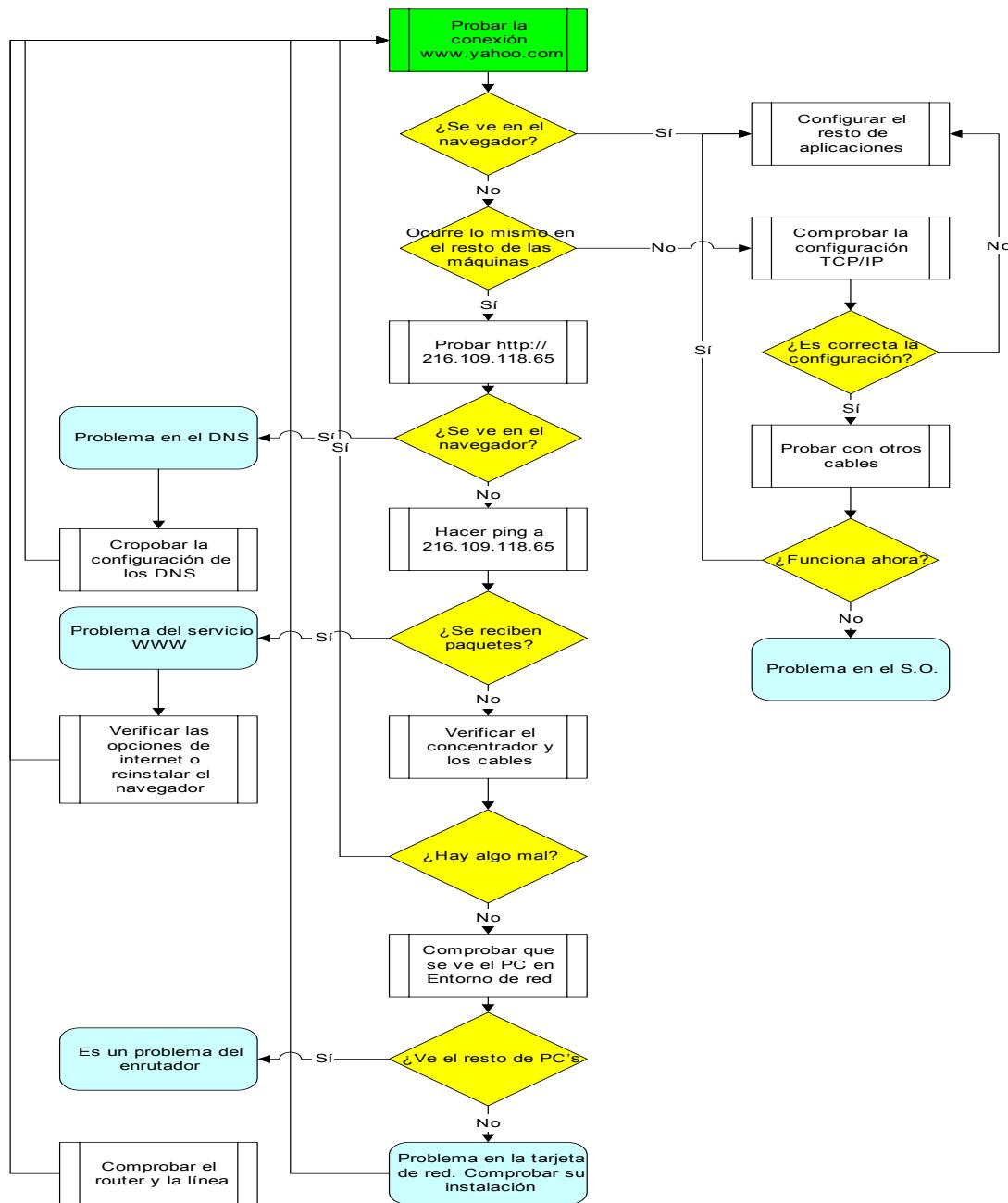


Ilustración 12: Servidor DNS: La caída del servidor DNS impide la traducción de nombre de dominio a dirección IP y, por lo tanto, el acceso a Internet

### Anotaciones



### Anotaciones

### 4.3. Utilidades TCP/IP para el chequeo de la red.

Superados todos los problemas de configuración y una vez que hemos conseguido que exista una comunicación óptima entre nuestros equipos pueden surgir pequeñas anomalías o, simplemente, deseamos conocer la calidad de la comunicación de nuestra red.

Para realizar unas tareas básicas de chequeo de la red disponemos de una serie de programas tanto en Windows como en Linux que nos pueden ofrecer información básica de nuestra red. Estos programas pueden incorporar una serie de variables que nos permiten mejorar su aplicación para el análisis de nuestra red.

- **Ping:** es el programa más sencillo y su función consiste en enviar un mensaje a un equipo y esperar su respuesta, realizando un informe de las características de dicha respuesta. La orden es similar en Linux y en Windows, aunque su comportamiento al ejecutarse es distinto. Permite comprobar la conectividad de los equipos.

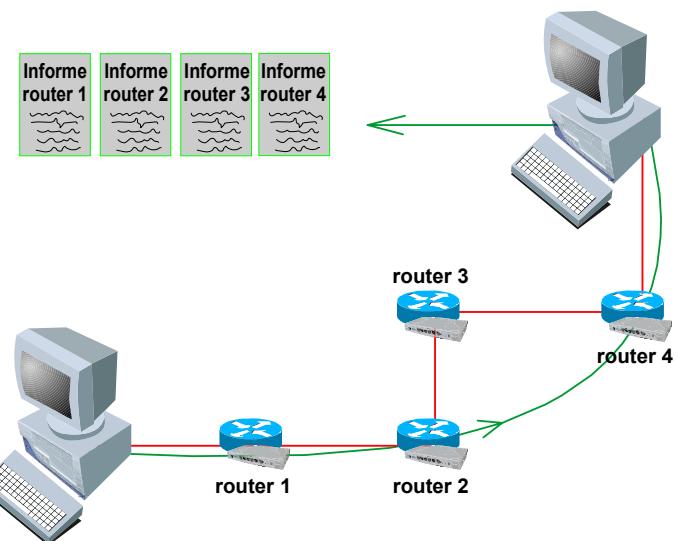
#### Para pensar:

Ejecuta la orden ping [www.google.es](http://www.google.es), comprueba los resultados devueltos por el programa. ¿Qué sucedería si no funcionara el servidor de nombres de dominio?

- **Traceroute** (tracert en windows) Detalla el camino seguido entre el equipo que ejecuta el programa y el equipo al que se llama indicándonos el nombre de dominio y las máquinas por las que transita el mensaje indicándonos posibles fallos en nuestros routers si no llegamos a salir de nuestra red.
- **Ipconfig** (ifconfig en linux): Muestra la configuración de red de nuestro equipo. Con esta orden podemos averiguar si nuestro equipo ha adquirido una dirección IP dinámica a través de un servidor DHCP, además de mostrarnos todos los datos de configuración de nuestro equipo.

#### Para pensar:

Ejecuta la orden ipconfig para averiguar todos los datos de la configuración de red de tu equipo de trabajo.



## Anotaciones

- **Netstat:** Esta utilidad nos permite averiguar las estadísticas del tráfico de red para los protocolos TCP/IP. Informa de los paquetes transmitidos y recibidos empleando cada uno de los protocolos TCP/IP y proporciona datos de error en las transmisiones.
- **Nslookup:** Este comando permite averiguar la dirección IP de cualquier máquina haciendo una consulta a un servidor de nombres de dominio específico. De forma indirecta permite averiguar si nuestros DNS están correctamente configurados.

### Para pensar:

¿Cómo emplearías Nslookup para averiguar porqué no funciona correctamente tu navegador de Internet?

Además de estos programas TCP/IP existe gran cantidad de software dedicado a las tareas de administración de la red que completan a las utilidades que incorporan las distintas versiones de Windows y Linux de análisis y control de la red que ya hemos explicado en el capítulo 5.

### 4.4. Analizadores de red.

Un analizador de red es un programa que se dedica a investigar el tráfico de paquetes de datos que circula por una red mostrando al administrador información sobre el contenido de dichos paquetes.

Estos programas se pueden incluir en versiones servidor del sistema operativo o pueden ser software propietario, que en ocasiones podemos encontrar con licencia shareware o freeware. Mediante las distintas herramientas que incorporan estos programas podemos llegar a determinar si la red se encuentra en un estado óptimo, cuáles son los tipos de datos que más se utilizan, cómo están siendo empleadas las conexiones e incluso acceder a la información de cada paquete.

Se trata pues de una herramienta muy potente que permite una optimización de la red a partir de los datos que nos aporta.

### 4.5. Tester.

Un tester es un dispositivo físico que se emplea para comprobar comprobar la capacidad de enviar señales de los cables. Detectan problemas físicos del cableado.

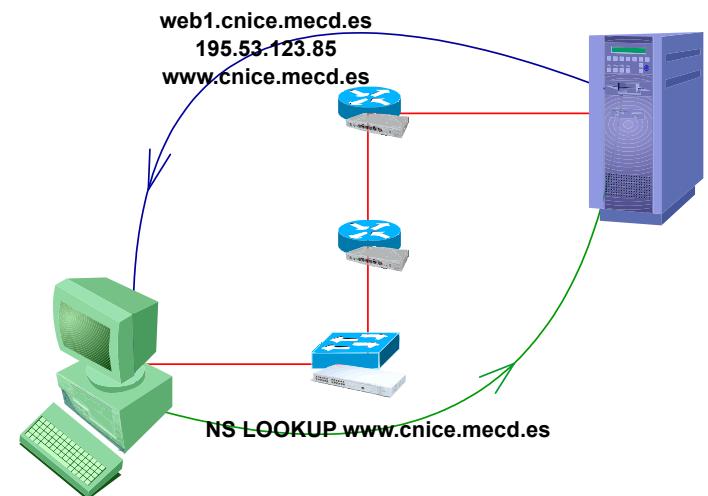


Ilustración 14: Nslookup: Permite averiguar la dirección IP de cualquier máquina

### Anotaciones

### 5. Seguridad en la red.

La expansión de Internet y la utilización masiva de redes de ordenadores en el ámbito empresarial, educativo y doméstico han propiciado el auge de sistemas para la intromisión en redes privadas, el desarrollo de virus informáticos y toda una serie de prácticas que atentan contra la seguridad de las comunicaciones informáticas.

En este escenario nos encontramos con que al igual que aumentan los sistemas de compras, transacciones, acceso a la información, etc. también han aumentado los mecanismos para saltarse las medidas de seguridad en estas operaciones. La confidencialidad de los datos, la seguridad de las transacciones comerciales y la estabilidad de los sistemas comerciales hacen necesaria la utilización de medidas de seguridad tanto de los datos como de las comunicaciones.

El ámbito educativo no debe ser ajeno a esta situación y, aunque el aspecto comercial y económico no afecte en gran medida a las redes escolares, si que pueden verse influidas por el ataque de virus, el acceso a datos confidenciales u otras medidas encaminadas a atacar el sistema. Así, si queremos mantener nuestra red en una situación óptima debemos contemplar la necesidad de establecer medidas de seguridad orientadas a:

- Evitar la infección por virus informáticos.
- Evitar la pérdida de datos.
- Impedir el acceso de personas ajenas a nuestra red.
- Garantizar el uso adecuado por parte de nuestros usuarios.
  - Evitar el deterioro de las aplicaciones.
  - Acceso a contenidos.

En este sentido, deberemos considerar puntos críticos en la seguridad de nuestra red:

- Conexión a Internet.
  - Cortafuegos.
  - Sistemas de detección de intrusiones.
  - Filtrado de contenidos.
- Entorno LAN.
  - Sistemas de autenticación de usuarios.
  - Sistemas antivirus,
  - Establecimiento de Redes privadas virtuales.

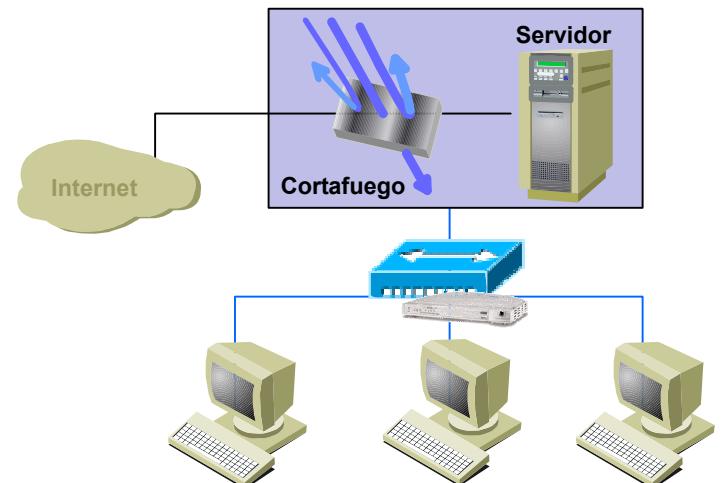


Ilustración 15: Un cortafuegos controla la puerta de acceso de nuestra red al exterior filtrando el tráfico en ambas direcciones.

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

En cualquier caso, todas las medidas de seguridad que adoptemos pueden ser insuficientes y, por regla general, nos daremos cuenta cuando ya hayamos sufrido el daño. Por ejemplo, aunque dispongamos de un programa antivirus actualizado, éste recogerá en sus firmas los virus conocidos, es decir, que ya han actuado; siendo susceptible de no detectar virus desconocidos. Sin embargo, cuanto más medidas adoptemos menos posibilidades de pérdidas de información o deterioro del sistema tendremos, es decir, seremos menos vulnerables a cualquier tipo de ataque.

### 5.1. Políticas de seguridad.

El concepto de políticas de seguridad ya ha sido tratado anteriormente desde el punto de vista de la administración de usuarios. A la hora de trabajar este tema, en el apartado de seguridad debemos focalizar nuestra atención en otros aspectos no recogidos en dicho apartado.

Las políticas de seguridad se refieren a las medidas que se deben adoptar para proteger nuestra red. Estas políticas deben ser recogidas en un documento de manera que sean conocidas por todos los usuarios de la red y estarán encaminadas al mantenimiento de la operatividad de nuestro sistema, siendo más estrictas en los puntos críticos y manteniendo un menor nivel de control en las zonas menos importantes de nuestra red.

Debemos recordar que en los sistemas informáticos de las redes escolares se recoge distinto tipo de información: datos personales, académicos, económicos, etc. siendo muy necesaria su protección. Se trata de asegurar la privacidad de los datos, su integridad y el acceso adecuado a los mismos por parte de los distintos usuarios.

Una política correcta de seguridad debe desarrollarse a partir de un análisis lo más completo posible de los puntos que deben ser protegidos, determinando qué usuarios deben acceder a cada recurso o elemento del sistema, protegiendo en distintos niveles los elementos de hardware, software y datos de nuestra red. Es importante tener en cuenta que los ataques o acciones perniciosas pueden venir tanto del interior como del exterior de nuestra LAN, por lo que las medidas que adoptemos deben estar dirigidas para realizar una protección eficaz en ambos sentidos.

La utilización inadecuada de la red por parte de nuestros usuarios puede ser controlada mediante las distintas herramientas que incorporan los sistemas operativos, mientras que el acceso desde el exterior, nuestra puerta de entrada y salida a Internet, será el punto crítico para evitar los ataques externos. En este sentido, deberemos establecer medidas de seguridad como la utilización de cortafuegos y el control periódico de tráfico que podamos considerar sospechoso, el análisis de nuestros puertos y otras medidas básicas de prevención y control.

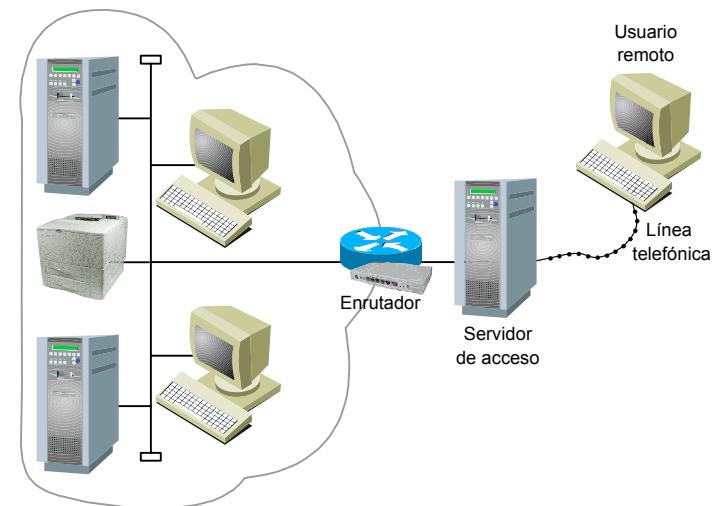


Ilustración 16: Uno de los elementos críticos de que deben ser tenidos en cuenta a la hora de elaborar las políticas de seguridad es el servidor de acceso a Internet

### Anotaciones

## Capítulo 6

Todas las medidas de seguridad que adoptemos para proteger nuestra red deberán estar recogidas en el documento sobre políticas de seguridad entendiendo que se trata de un plan integral de protección basado en los riesgos y recursos disponibles y no en una serie de medidas aisladas.

### 5.2. Cortafuegos.

Los cortafuegos son las herramientas más apropiadas para evitar el acceso a nuestra red por parte de usuarios externos no autorizados, al igual que controla la salida de los usuarios de la red hacia el exterior.

#### a) Tipos de cortafuegos.

Los cortafuegos pueden ser dispositivos de hardware o de software y pueden basarse, fundamentalmente, en la utilización individual o asociada de alguna de las siguientes tecnologías:

- **Cortafuegos de inspección de paquetes.** Mediante la utilización de routers con reglas de filtrado comprueban las direcciones IP de destino y origen de los paquetes y en función de estos datos dejan pasar la comunicación. Son rápidos y flexibles pero ofrecen un nivel mínimo de seguridad. Una vez que se ha superado este tipo de cortafuegos se tiene un acceso completo a la red.
- **Pasarelas de aplicación.** Son servidores proxy que analizan las peticiones de acceso, filtran y reenvían la información al host al que va dirigido el paquete. Pueden solicitar la autenticación de los usuarios y aparecen como única máquina de la red (dirección IP externa única), es decir, convierten la red en invisible. El proxy presta todos los servicios de red tanto internos como externos (telnet, ftp, http,...) y si el dispositivo no dispone de alguno de dichos servicios, no lo presta.
- **Basados en técnicas multinivel de estados.** Examinan los paquetes a todos los niveles de la pila de protocolos combinando las tecnologías anteriores. Dispone de un motor de inspección que analiza cada paquete y lo coteja con los datos almacenados en sus tablas de manera que no permite el paso a aquellos paquetes que no están asociados a una conexión.

Cuanto más sofisticado y complejo sea el cortafuegos mayor seguridad ofrecerá, sin embargo, en ningún caso podrán proteger de acceso ocasional por un uso inadecuado de los usuarios o el acceso por "puertas traseras" vía MODEM.

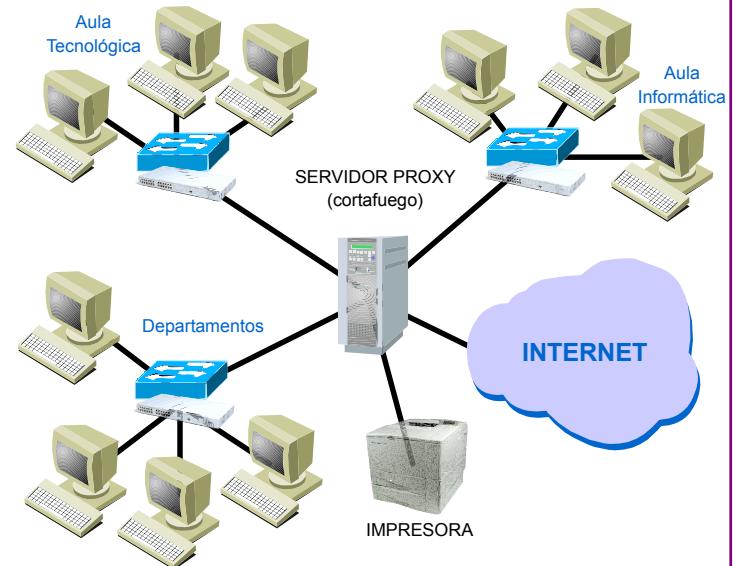


Ilustración 17: Esquema de una red en la que un servidor proxy actúa como cortafuegos.

## Anotaciones

### Analogía:

Podríamos comparar un cortafuegos más que con el término similar en español concebido como barrera antiincendios, con un vigilante que solicita el salvoconducto a todas aquellas personas que desean introducirse en una fortaleza. Imaginemos un castillo con un gran foso. El vigilante les solicita que se identifiquen y hagan saber de donde vienen y hacia dónde se dirigen, además de poderles preguntar las razones por las que desean introducirse en el castillo. Si la información que obtiene le satisface, baja el portón de la fortaleza, si no es así, la mantiene cerrada.

A la hora de decidir la implementación de un determinado tipo de cortafuegos debemos tener en cuenta las políticas de seguridad que hemos diseñado.

Podemos considerar necesario el filtrado de todo el tráfico de acceso a nuestro servidor (excepto por ejemplo a la página web del centro) o al contrario, que sean los alumnos del centro los que no puedan acceder, salvo en determinadas situaciones, al exterior. Una vez que sabemos qué nivel de seguridad queremos implementar debemos definir cómo hacerlo, es decir indicar qué no es accesible (una opción de configuración) o, al contrario, estableciendo qué servicios y en qué condiciones pueden atravesar el cortafuegos. Por último, y en función del presupuesto del que dispongamos determinaremos qué tipo de cortafuegos instalaremos, por ejemplo, un pc con linux o un software propietario.

La instalación del cortafuegos, en muchas ocasiones, va a depender de la infraestructura existente. Así, si disponemos ya de un router, podremos establecer en él el cortafuegos y dejaremos detrás de él toda nuestra red. Por otro lado, si instalamos un equipo servidor con un doble interfaz de red, podríamos establecer distintos sectores en nuestra red protegiendo determinadas zonas y dejando al descubierto otras. En cualquier caso, el sistema cortafuegos que creemos, deberá regirse por el principio de mayor protección y simplicidad.

### b) Arquitecturas de cortafuegos.

La combinación de los distintos elementos de hardware (router y host servidor) pueden proporcionar distintas arquitecturas de cortafuegos yendo de la más sencilla y permeable, a la más compleja y difícil de superar:

- **Cortafuegos de filtrado de paquetes:** aprovechamos la utilidad del router para filtrar los paquetes. Presenta dificultades de monitorización y la configuración y control son difíciles.

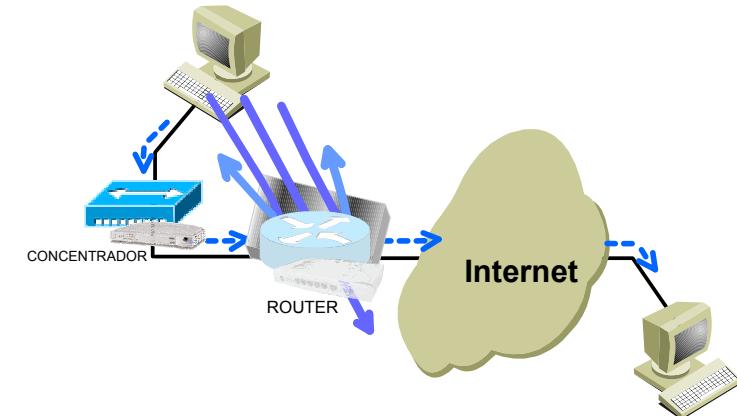


Ilustración 18: Router actuando como cortafuegos mediante el filtrado de paquetes

### Anotaciones

- **Anfitrión de dos bases:** Se trata de un servidor proxy con dos interfaces de red que filtra los paquetes a nivel de aplicación evitando el tránsito directo de paquetes entre la red interna y la red externa.
- **Screened-Host:** Combina un router y un host de doble interfaz de red. Ambos dispositivos pueden comutar su posición dentro de la red dejando en unos casos el router en contacto con la red externa y en otros el servidor proxy. En ambos casos aparecen ventajas e inconvenientes y, debido a la complejidad de su configuración, es una tecnología que se encuentra en desuso. La mayor seguridad de este sistema proviene del filtrado de paquetes que realiza el router.
- **Screened subnet:** Mediante el uso de dos routers y un servidor proxy se crea un filtrado previo al servidor proxy, tal como en la arquitectura screened-host, pero genera dos sus redes empleando el segundo router, de manera que se evita el acceso directo del host a la red interna. Este sistema proporciona elevados niveles de seguridad aunque es muy complejo de implementar.

Las redes escolares deben estar suficientemente protegidas pero, en muchos casos, la imposibilidad de disponer del tiempo y los recursos necesarios hacen inviable la utilización de tecnologías o arquitecturas complejas. La opción más utilizada en la mayoría de los centros es un servidor proxy con doble interfaz de red y sistema operativo linux que, entre otras funciones (servidor web, servidor de correo, etc.) actúa como cortafuegos y control de acceso a contenidos.

### c) Cortafuegos embebidos.

Se trata de la última generación de cortafuegos que combinan hardware y software y se implementan en la tarjeta de red de cada uno de los host y servidores de la red. Estos cortafuegos proporcionan una gran seguridad ya que actúan en los dos extremos de la red, ofreciendo a su vez flexibilidad en su configuración, siendo independientes del sistema operativo del equipo, puesto que se encuentran en la memoria de la tarjeta de red.

Entre otras funcionalidades estos dispositivos pueden ser administrados desde el sistema servidor de manera que se optimice su configuración. Actualmente es una opción muy interesante para las empresas pero se encuentra totalmente ajena al entorno educativo.

### 5.3. Sistemas antivirus.

Los enemigos externos por anonomasia de la estabilidad de la red de un centro escolar son los virus informáticos. Esto es debido, en principio, a la gran cantidad de programas de este tipo existentes en la actualidad y a la facilidad de propagación que

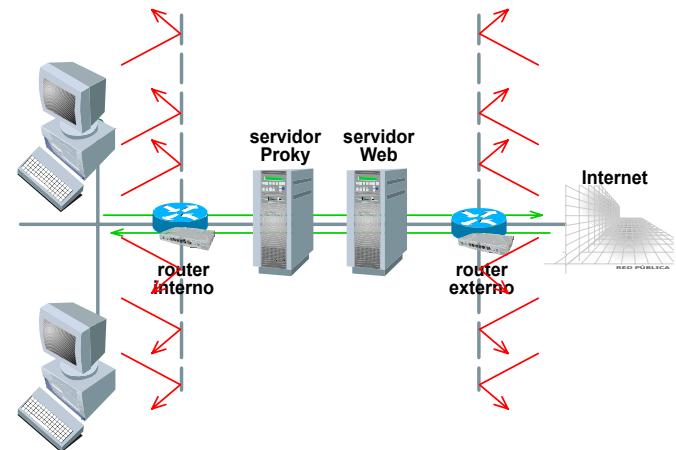


Ilustración 19: Screened subnet: Los routers detienen a ambos lados de los servidores el tráfico interno y externo

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

encuentran en Internet, más teniendo en cuenta que su diseño esta especialmente pensado para utilizar esta red, a través de sus distintos servicios, como medio de propagación empleando para ello las vulnerabilidades de los navegadores, programas de correo electrónico e ICR.

Podemos considerar un virus como un programa cuyo objetivo es reproducirse dentro de un anfitrión sin ser detectado causando en el ordenador en el que reside un determinado daño.

La historia de los virus tiene apenas 20 años ya que la creación del primer virus para un seminario de seguridad informática data de 1983. Actualmente se crean unos 500 nuevos virus al mes.

### Nota:

*El primer virus fue creado en un tiempo de ocho horas el 17 de noviembre de 1983.*

*El concepto de virus informático fue introducido en 1983 por el estadounidense Fred Cohen para referirse a los programas informáticos capaces de reproducirse por sí mismos.*

A pesar de su peligrosidad no existe ningún virus que no pueda ser destruido, aunque esto no quiere decir que no pueda ocasionar graves trastornos en nuestro sistema, pues actualmente están llegando a un alto nivel de sofisticación de manera que si bien antes necesitaban de la acción del usuario para activarlos en la actualidad se pueden ejecutar automáticamente o llegar incluso a mutar u ocultarse.

### a) Tipos de virus.

Existen varias formas de catalogar los virus, tarea difícil debido a la gran cantidad y variedad que aparecen cada año, por lo tanto, vamos a optar por una clasificación amplia que recoge no sólo los virus, también todo tipo de archivos dañinos a los sistemas informáticos.

- **Bombas lógicas:** Son programas que se activan ante determinadas condiciones, por ejemplo Viernes 13.
- **Caballos de troya:** Programas que pueden ser utilizados por el usuario pero que en la medida en la que éste los usa, van atacando el sistema.

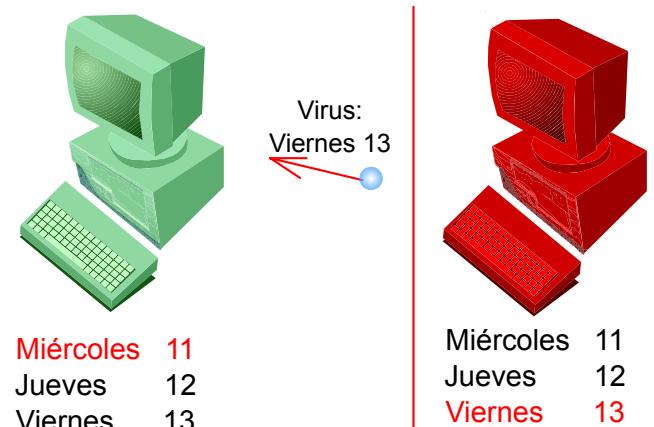


Ilustración 20: Bomba lógica: Es un virus que se activa ante determinadas condiciones

### Anotaciones

- **Gusanos:** programa cuyo objetivo es propagarse y reproducirse a través de distintos ordenadores utilizando las tablas de ruta del sistema o el correo electrónico.
- **Virus propiamente dicho:** Programas cuyo objetivo es reproducirse dentro de un sistema y atacarlo. Dentro de esta categoría encontramos:
  - **Virus de archivo:** Se activan cuando el programa en el que residen es activado, se suelen introducir en los archivos .com y .exe.
  - **Virus de sector de arranque:** Se introducen en el sector de arranque de un disco y actúan cuando éste se inicia.
  - **Virus multipartición:** Son virus que infectan tanto el sector de arranque como los archivos.
  - **Virus de macro:** Se introducen en las macros de visual basic y se transmiten a través de los documentos que incorporan dichas macros.

**Nota:**

*Blaster es un gusano surgido en Agosto de 2003 que en menos de un día ha infectado equipos por todo el mundo. Aprovecha una vulnerabilidad de Windows RPC DCOM para introducirse en los ordenadores a través del puerto 135 y provocar un desbordamiento del buffer de la máquina infectada para propagarse al mayor número de ordenadores posible. Otra de sus acciones es enviar cientos de paquetes a la página de windowsupdate los días 16 de agosto de 2003 y 31 de diciembre de 2003.*

Además de la clasificación anterior, podemos encontrar otras clasificaciones en función de distintos criterios

- **Encriptados:** Virus que se ocultan a sí mismo, encriptándose para no ser detectados por los programas antivirus. Se trata más bien de una técnica de ocultamiento que de un tipo de virus.
- **Polimórficos:** Son virus que se encriptan y desencriptan adoptando distintas formas cada vez que producen una infección con el fin de dificultar su identificación.
- **Retrovirus:** Virus que detectan fallos (bug) en los programas antivirus, se introducen en ellos y los intentan destruir.

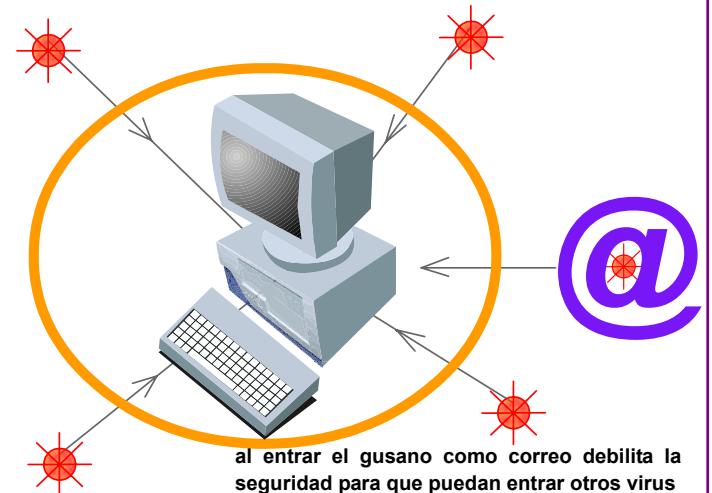


Ilustración 21: Gibe.C: Es un gusano que al infectar el sistema facilita la entrada de otros virus

## Anotaciones

- **Bulos:** Mensajes que se envían por correo haciendo creer que un archivo determinado del sistema es un virus y se solicita que sean borrados.
- **Bromas:** Programas que emulan virus pero que no resultan en absoluto perniciosos.
- **Trampas:** Vías de entrada que dejan los programadores en los distintos programas para poder acceder a ellos posteriormente sin ser detectados por los controles de seguridad.
- **Bacterias:** Virus cuyo objetivo es reproducirse dentro del sistema operativo hasta llegar a saturarlo.

Los programas antivirus permiten una gestión centralizada desde un servidor o distribuida en cada uno de los equipos. Dependiendo de la estructura de nuestra red y de su arquitectura deberemos evitar, en la medida de lo posible, que la optimización de los programas antivirus, actualización, procesos de detección, etc. corra a cargo de los usuarios de la red. Así, buscaremos opciones que centralicen y automaticen todas estas funciones desde un servidor, o configuraremos la instalación para que todos estos procesos se realicen de forma automática.

### b) Antivirus.

Los programas antivirus son las soluciones de software para detectar y neutralizar los virus. Para que un programa antivirus sea realmente eficaz debe estar actualizado con una periodicidad máxima de una semana (en función de la empresa de software propietaria del programa).

Cualquier programa de este tipo debe disponer de un motor antivirus potente y que implemente tecnologías proactivas de detección de virus. Estos programas deberían:

- Detectar todo tipo de virus, gusanos y troyanos ya conocidos resolviendo los problemas que puedan haber ocasionado. Esta funcionalidad es conocida como de defensa clásica.

#### Nota:

Existen distintos tipos de instituciones que certifican el número y tipo de virus capaces de ser detectados por cada programa. Algunas instituciones de reconocido prestigio en esta materia son Virus Bulletin 100%, ICSA's o West Coast Labs

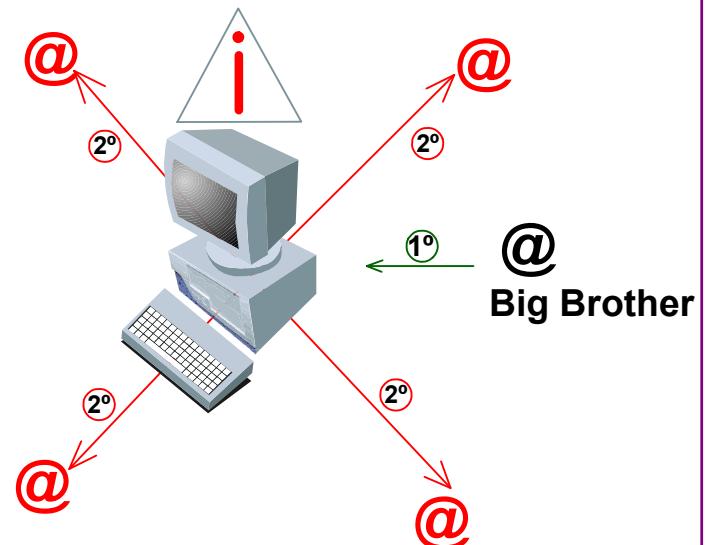


Ilustración 22: Big Brother: Es un hoxo que informa del peligro de un virus relacionado con "gran hermano". Su objetivo es causar alarma

## Anotaciones

- Detectar y bloquear scripts que exploten las vulnerabilidades del software de nuestros equipos. Por ejemplo, que detecte virus y gusanos que se ejecuten al acceder a una página web o al visualizar un mensaje de correo electrónico.
- Detectar, mediante técnicas heurísticas, virus camuflados que empleen técnicas de ofuscación.

### Nota:

*Las técnicas heurísticas consisten en la búsqueda dentro del código del programa que desea ejecutarse, o que se está analizando, porciones de código que se emplean de forma habitual en el diseño de virus.*

- Detectar actuaciones anómalas de nuestro software, por ejemplo, el envío de un número poco habitual de mensajes de correo electrónico con el mismo asunto.
- Detectar virus que se presentan en un determinado formato clásico comprimido o en formatos comprimidos ejecutables.
- Detectar modificaciones en los archivos mediante sistemas de control de sumas.
- Consumir de forma moderada memoria RAM mientras realizan los procesos de detección y desinfección de virus.
- Incorporar firewall que detecten los procesos de Windows y las aplicaciones de uso más habitual.

Además de todas estas opciones es muy interesante disponer de un teléfono de consultas 24 horas que permita resolver todas las dudas que surjan u orientar técnicamente en procesos de desinfección complejos.

### c) Otras medidas de seguridad antivirus

La elección de un buen programa antivirus puede no ser suficiente medida de seguridad si no adoptamos otras medidas complementarias de protección ya que, como hemos indicado, los virus aprovechan todas las vulnerabilidades de sistemas y usuarios.

Las acciones que debe emprender al administrador para paliar, en la medida de lo posible, los problemas que los virus puedan ocasionar en un sistema deben orientarse en varias direcciones:

- Configuración y actualización del programa antivirus.
- Actualizaciones de los programas más susceptibles de ser atacados.

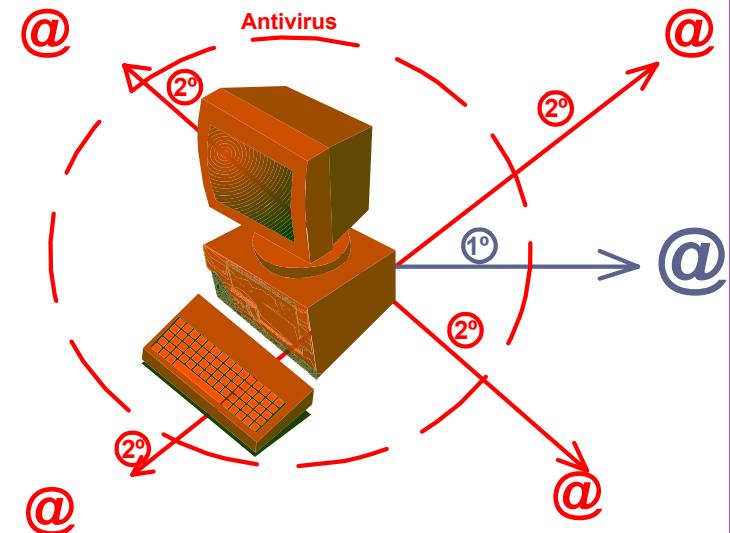


Ilustración 23: Antivirus: Los antivirus, entre otras cosas, comprueban el tráfico de correo electrónico buscando comportamientos análogos

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

- Configuración de programas navegadores y de correo web.
- Formación y orientación a los usuarios.
- Copias de seguridad.

Para paliar las vulnerabilidades de los sistemas deberemos tener instaladas las últimas actualizaciones críticas y los Service packs de nuestros sistemas operativos y programas de uso habitual que permiten cerrar todas las puertas de entrada que se van detectando periódicamente y que usan los troyanos para introducirse en nuestro sistema y tomar el control del mismo.

La configuración del navegador y de los programas de correo electrónico es vital como segunda medida de seguridad. Muchos gusanos se propagan simplemente con ver el mensaje de correo en el que se encuentran o dentro de scripts que se ejecutan en páginas web. Si nuestro programa antivirus no se desenvuelve especialmente bien ante estas situaciones deberemos limitar la configuración del navegador para evitar la ejecución de los scripts y ejecutar el programa de correo sin la vista previa de los mensajes, de manera que podamos eliminar correos sospechosos sin llegar a abrirlos.

Aunque en la actualidad existen virus que no necesitan de la acción del usuario para infectar el sistema, en la mayoría de los casos y debido a actuaciones imprudentes, somos nosotros quienes al abrir un correo sin garantías, un archivo adjunto, descargar un determinado programa, etc. estamos permitiendo la infección de nuestra red. Por lo tanto, la educación de los usuarios es otra de las medidas que debe adoptar un administrador de red procurando, igualmente, establecer un protocolo de actuación ante la detección de una infección, en definitiva, crear unas políticas de seguridad entre los usuarios de la red.

Por último, puede suceder que, a pesar de adoptar todas las medidas posibles, se produzca la infección y el deterioro de archivos o de todo el sistema. Para paliar, en la medida de lo posible, que se produzcan daños irreparables debemos realizar periódicamente copias de seguridad de nuestros documentos y crear un sistema eficaz de restauración de los equipos.

### Nota:

*Como ha quedado patente, la utilización en una única línea de las medidas de seguridad es un error, más en un centro escolar. Si no hemos establecido unas políticas de seguridad para los usuarios, limitando los sistemas en función de la persona que lo utilice, nos encontraremos con gran cantidad de problemas posteriormente. Un documento sobre políticas de seguridad aprobado por el claustro va a garantizar el estado óptimo de la red.*



Ilustración 24:Niveles y actuaciones de seguridad

### Anotaciones

## 5.4. Copias de seguridad.

Hasta ahora hemos comprobado los distintos problemas que nos podemos encontrar en el funcionamiento de una red, muchos de ellos pueden afectar a los datos con los que en ella se trabajan y generar, como ya hemos indicado, pérdidas irreparables. Así, podríamos hablar de medidas de protección activas y pasivas. Por un lado, las activas intentan evitar que se produzcan los daños (cortafuegos, antivirus,...) por otro, las pasivas intentan minimizar las consecuencias.

Por regla general, los datos en una red deben estar centralizados en un servidor de archivos tal como indicamos en este mismo capítulo, tres son las razones que lo avalan:

- Los archivos que se encuentran en un servidor están siempre disponibles y localizables para todos los usuarios.
- El acceso al equipo servidor es mucho más restringido (física y lógicamente) que a cualquier otro PC de la red.
- La realización de copias de seguridad es mucho más sencilla.

En este caso, la copia de seguridad se realizaría del disco del servidor de archivos. Sin embargo, en ocasiones puede considerarse conveniente que los archivos se encuentren distribuidos por varios equipos. En este caso optaríamos por un equipo que se encargara de centralizar las copias de seguridad de todos ellos, empleando la red para todo este proceso.

La realización de las copias de seguridad de los equipos debe estar automatizada en la medida de lo posible, evitando que dependa de la intervención del administrador, estableciendo momentos en los que el tráfico de red es escaso o nulo y que no se estén empleando los archivos de datos.

Por último debemos considerar qué datos deben ser especialmente protegidos. En los centros docentes disponemos de bases de datos que gestionan la administración del centro, documentos de trabajo, documentos pedagógicos, documentos administrativos, etc. Cuando determinemos cómo se va a realizar la gestión documental del centro y dónde se van a ubicar los archivos deberemos tener en cuenta la necesaria protección de los mismos (activa y pasiva) y el papel que van a tener los usuarios en su utilización, comprometiéndonos a garantizar la seguridad de todos aquellos documentos que se encuentre en el lugar prescrito.

### a) Dispositivos para la copia de seguridad.

Las realizaciones de copias de seguridad “Backups” requieren de la utilización de un hardware específico, unidad de disco para realizar la copia. En general, cualquier dispositivo de almacenamiento extraíble puede ser empleado para esta tarea, sin embargo debemos tener en cuenta las limitaciones de velocidad, capacidad y coste de unas de estas unidades con respecto a otras.

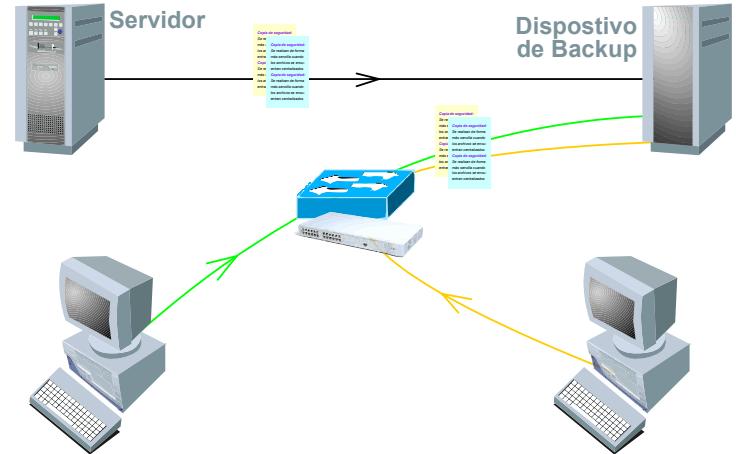


Ilustración 25: Las copias de seguridad se realizan de forma más sencilla cuando los archivos se encuentran centralizados

## Anotaciones

## Capítulo 6: Gestión y administración de redes.

Unidades de CD-ROM, unidades de cartucho Zip o Iomega Jaz, discos duros o unidades de cintas magnéticas son susceptibles de ser empleados para las tareas de backup, siendo estas últimas específicas para este tipo de trabajo.

Además de estos sistemas de copia mediante unidades extraíbles existe la tecnología RAID (conjunto redundante de discos independientes) que se encarga de crear imágenes gemelas de los discos duros. Sin embargo, esta tecnología presenta el problema de la pérdida de datos por catástrofe, es decir, si nosotros almacenamos una serie de datos en una cinta, esta puede ser guardada en un lugar protegido, evitando su deterioro por un accidente (inundación, incendio, etc.) o robo mientras que el sistema RAID no es susceptible de ser protegido de igual modo.

### Para pensar:

*Uno de los aspectos que más puede influir a la hora de decidirse por un sistema de almacenamiento de datos es su coste. Calcula el precio equivalente por megabyte almacenado de un CD-RW, una unidad ZIP y una cinta lineal digital.*

La decisión que tomemos a la hora de optar por un sistema de copias de seguridad, debe ponderar los elementos que hemos señalado anteriormente. El coste suele ser el mayor problema con el que nos vamos a encontrar ya que, por regla general, los centros no disponen de presupuesto holgado. Sobre la base ya de un margen económico debemos manejar las otras dos variables: velocidad y capacidad.

En los centros docentes se producen períodos de tiempo amplio en los que la red informática no se emplea, por lo que la velocidad en la realización de las copias no debe ser un factor determinante, sin embargo, la capacidad sí que debe influir en la decisión. Cada sistema de copia presenta unos valores máximos de capacidad, por lo que a la hora de optar por uno u otro deberemos seleccionar aquél que nos garantice un rango de espacio suficiente para posibles ampliaciones.

Tipo	Capacidad máxima (sin comprimir)	Velocidad máxima de transferencia
Cartucho de cuarto de pulgada (QIC)	20 GB	120 MB/min
Cinta de audio digital (DAT)	20 GB	144 MB/min
8 mm	60 GB	180 MB/min
Cinta lineal digital	40 GB	360 MB/min
Cinta lineal abierta	100GB	1920 MB/min

### Anotaciones

## Capítulo 6

La capacidad de almacenamiento no es real, ya que en muchos casos se ve afectada por factores como la calidad del flujo de datos y los errores de escritura que se puedan producir. Para lograr la máxima calidad a la hora de realizar las copias de seguridad, deberemos disponer de unidades de disco de alta velocidad, una red fase ethernet, interface SCSI de conexión de la unidad de cinta y un equipo que gestione la copia suficientemente potente. Además, deberemos aprovechar momentos en los que este equipo y la red no tengan una gran carga de trabajo.

### Nota:

En 1995 apareció IOMEGA ZIP con una capacidad de 100 mgbyte, actualmente se pueden almacenar en formato comprimido hasta 220 Gbytes en una unidad de cinta súper DLTTape.

### b) Software de copia de seguridad.

Las unidades de cinta no admiten la opción de copiar y pegar o arrastrar del resto de las unidades de disco de un sistema, ya que son dispositivos de acceso lineal y no disponen de tablas con información de los archivos que en ellas se almacenan. Esto supone que se requiere de un software específico que permita el control de estas unidades y la ejecución de las copias de seguridad.

Existen dos tipos de programas de copia de seguridad, para equipos individuales y para red. En general, es mejor optar por esta segunda opción, ya que si bien con software para un equipo individual se pueden realizar copias de seguridad de unidades de red, solo guardan los archivos, no pudiendo hacer imágenes de los discos. Los sistemas operativos suelen incluir herramientas de este tipo por lo que, en muchos casos, si las necesidades no son excesivas, se puede evitar la adquisición de este software.

Un software de este tipo debería incluir, al menos:

- Adecuación al tipo de sistema operativo que estemos utilizando.
- Entorno de administración sencillo e intuitivo.
- Posibilidad de trabajo en red para facilitar la realización de copias de seguridad en los equipos de la red a través de un agente (o demonio) instalados en los mismos incluyendo su registro.
- Filtro para la selección de archivos de manera que podamos determinar qué archivos deseamos copiar en función de distintos criterios.

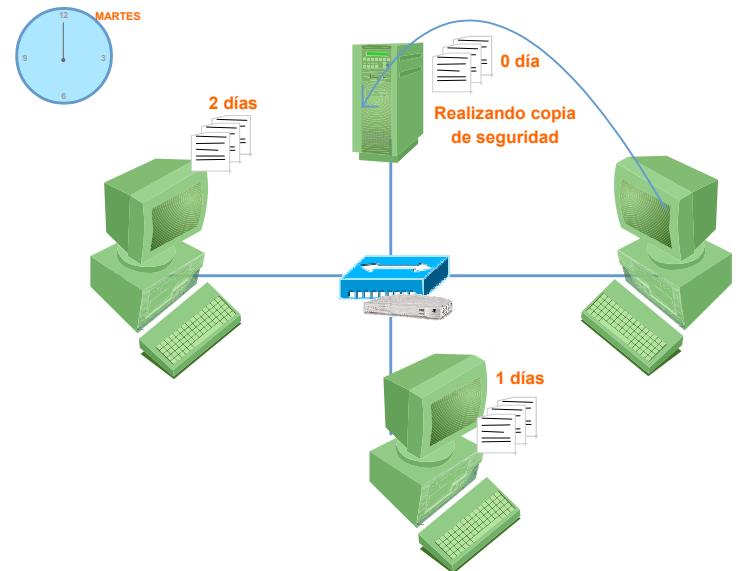


Ilustración 26: Protección de archivos: La copia de seguridad en red facilita el proceso de protección de archivos distribuidos

## Anotaciones

## Capítulo 6: Gestión y administración de redes.

- Posibilidad de determinar el tipo de copia a realizar para establecer cuándo deseamos copiar un determinado archivo en función de su posible modificación.
- Programador de trabajos de manera que se pueda automatizar todo el proceso limitándonos al cambio y archivo de las cintas.
- Administración de copias que nos permita analizar el estado de las copias y cómo se han desarrollado.
- Facilidad a la hora de realizar el proceso de restauración.

Todas estas opciones suponen un mayor gasto en este tipo de software, ya que, normalmente, tanto los programas de copia de los distintos sistemas operativos, como los que incorporan las unidades de disco al adquirirlas, suelen tener muchas menos opciones.

### c) Planificación y automatización del proceso.

Cuando planificamos la realización de copias de seguridad debemos adoptar una serie de decisiones que, dependiendo de las características del programa que hayamos adquirido serán más fáciles de aplicar. Estas decisiones son:

- ¿Qué tipo de archivos deseamos copiar?
- ¿Cada cuánto tiempo queremos realizar la copia?
- ¿Cómo queremos que sean las copias en función de la modificación de los archivos?

Estas cuestiones no pueden ser expuestas de forma lineal, ya que todas las opciones que adoptemos deben ir asociadas. Por ejemplo, podemos querer hacer una copia de un fichero una vez al mes, pero si se modifica queremos que se actualice a diario, o, no queremos que se haga nunca copia de seguridad de los ficheros tmp mientras que deseamos una copia diaria de todas las bases de datos.

Por lo tanto, y en función de lo expuesto en el párrafo anterior, cuando hablamos de tipo de copia de seguridad podemos establecer las siguientes categorías:

- **Copia:** Realiza una copia de los archivos.
- **Normal:** Realiza una copia completa y señala como punto 0 el momento de realización de la copia indicando que todos los archivos ya están respaldados.
- **Incremental:** Realiza una copia únicamente de los archivos que han cambiado.
- **Diferencial:** Realiza una copia de los archivos que se han modificado, indicando como punto 0 el momento de hacer dicha copia.
- **Diario:** Realiza copia de los archivos que han cambiado cada día.

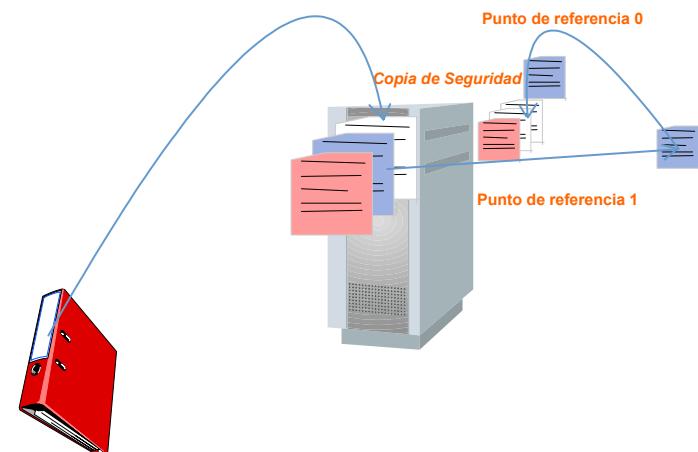


Ilustración 27: Copia diferencial: selecciona los archivos modificados para hacer copia y pone a 0 el punto de referencia de copia

## Anotaciones

### Para pensar:

*¿Qué sistema de copia emplearías para saber cuándo se han modificado uno o más archivos determinados? ¿Qué sistema emplearías para asegurar la base de datos del centro?*

El sistema que más se emplea de copias de seguridad se denomina Abuelo-padre-hijo, donde las copias hijo son diarias y de tipo incremental o diferencial, empleando para ello una cinta diaria que se reescribe semanalmente. De esta forma protegemos los archivos más utilizados o los documentos elaborados en la última semana.

El Padre es la copia completa de todos los archivos que se realiza una vez a la semana, reutilizando las cintas cada mes. Por último, el abuelo sería una copia mensual de todo el sistema que se guardaría durante un año. La rotación de copias quedaría del siguiente modo:

	Cintas necesarias	Periodicidad y tipo de copia	Reutilización
Hijo	5	Diaria. Cada día de la semana una cinta. Diferencial o incremental	Se sobrescribe a la semana siguiente
Padre	4 ó 5	Semanal. Una vez a la semana. Generalmente los viernes. Normal	Se sobrescribe al mes siguiente.
Abuelo	10 a 12	Mensual. Una vez al mes. Generalmente el mismo día del mes. Normal.	Se sobrescribe una vez al año.

Todo este proceso debe estar perfectamente automatizado de manera que la labor del administrador de la red o del responsable de esta tarea solo deba de cambiar las cintas de la unidad y guardarlas en un lugar seguro con el fin de salvar las copias en caso de accidente.

### Nota:

*A la hora de adquirir un software de copias de seguridad es muy importante conocer el número de licencias que se adquieren y si estas son válidas para el equipo servidor o para las distintas máquinas clientes que se encuentran conectadas a la red y de las que queremos realizar una copia.*

### Anotaciones

### 5.5. Imágenes.

La realización de imágenes de discos es una operación que se encuentra a caballo entre las labores de administración y de seguridad. No se trata exactamente de una copia de seguridad aunque permite recuperar de forma rápida un equipo.

Por un lado, las aulas de informática necesitan la instalación y desinstalación de múltiples programas. La realización de copias de seguridad carece de sentido cuando sólo se emplean los PC's como elementos donde se ejecutan programas multimedia o se realizan conexiones a Internet, guardando los archivos de los usuarios en carpetas dentro del servidor.

Todo proceso de instalación tiene el riesgo de crear incompatibilidades de aplicaciones y llega a tocar en mayor o menor medida el registro. Por lo tanto, resulta muy interesante tener una imagen de los PC's de manera que en un momento determinado, sin riesgo a perder datos, se restaure el sistema al primer momento de su completa instalación con una configuración estándar.

Por otro lado, podemos encontrarnos con un problema de virus, corrupción del sistema operativo, deterioro del registro, etc. El proceso de instalación de todo el software y el sistema operativo puede llegar a ser de horas, mientras que la recuperación de una imagen de un equipo puede ser un proceso de minutos, lo que facilita la recuperación y optimización inmediata de ese PC.

Existen en el mercado distintos programas que permiten la realización de este tipo de copias. En general estos equipos trabajan en modo local, es decir, que debemos desplazarnos a cada equipo para restaurarlo, sin embargo, podemos encontrar software que permite levantar un equipo en remoto y cargarle una imagen, aunque para ello es necesario que las tarjetas de red permitan esta opción y que la configuración de la BIOS sea la adecuada.

**Nota:**

*Los programas que realizan y restauran imágenes de discos realizan, también, un particionado y formateado siendo la forma más rápida de recuperar un equipo cuando no se disponen de otros medios de protección adicionales.*

### 5.6. Protección del sistema.

Además de los sistemas de copias de seguridad existen dispositivos de hardware (tarjetas recuperadoras de particiones o discos) y de software que permiten restaurar automáticamente el sistema a una situación inicial o punto de seguridad. El sistema de tarjetas es el más empleado en equipos de sobremesa y el software de recuperación en equipos portátiles. Si bien este último también puede ser aplicado a los equipos de sobremesa.

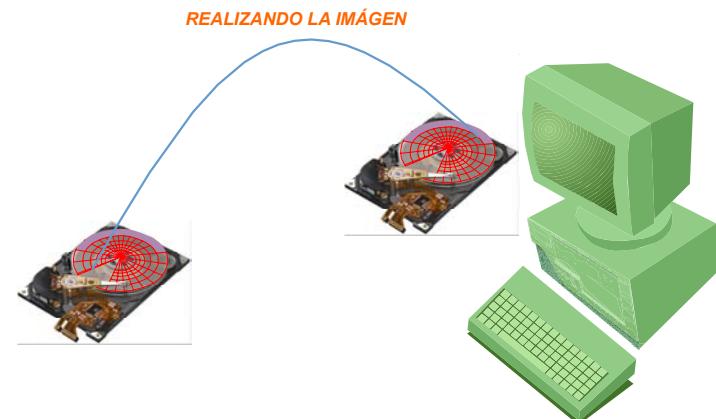


Ilustración 28: Imagen de disco: permiten guardar una copia de los archivos de un disco en un formato comprimido

### Anotaciones

Las tarjetas de seguridad permiten almacenar en sectores de memoria físicos o de memoria de disco los datos de configuración del sistema en un momento determinado, por ejemplo, una vez instalados todos los elementos de software o de hardware. Una vez que la configuración del equipo es la adecuada, bloqueamos contra cambios un disco o una partición del mismo donde se encuentre ubicado el sistema. Así, cuando un usuario que no sea administrador de la red intente realizar algún cambio, éste no quedará grabado en el disco protegido evitando posibles errores y problemas de incompatibilidad.

Por otro lado, se pueden determinar particiones del disco para compartir, de manera que todos los datos que se deseen guardar en el equipo puedan ser almacenados en una unidad compartida por todos los usuarios.

El software de restauración presenta unas funciones similares a las de las tarjetas aunque, permiten una mayor flexibilidad a la hora de restaurar los equipos, a la vez que protegen (aunque en algunos casos con menos eficacia) tanto la configuración del sistema como los datos almacenados. Su función no consiste en evitar la modificación intencionada de la configuración, más bien, resolver los problemas que se puedan haber producido por dichos cambios.

En la actualidad algunas versiones de sistemas operativos incluyen esta función.

## 6. Diseño y funcionamiento de un aula en red dentro de un centro docente.

### 6.1. Introducción.

El diseño de un aula informática debe atender a criterios de muy distinto tipo: económicos, técnicos y didácticos. En general, deberemos considerar el factor económico como el determinante fundamental del proyecto que deseamos desarrollar. El presupuesto para la adquisición y mantenimiento de los equipos, la adquisición de software, la conexión a Internet, etc. va a condicionar todas y cada una de las decisiones que debamos tomar.

Con independencia del factor económico, que debe estar presente a la hora de realizar un proyecto viable, debemos considerar la utilización que vamos a dar a esta red. Así, deberemos analizar:

- Tipo y edades de los usuarios.
  - Profesores.
  - Alumnos.
  - Usuarios.

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

- Administrador
- Utilidades.
  - Docencia.
  - Trabajo.
  - Gestión.
  - Compartición de recursos.
  - Acceso exterior.
- Extensión.
  - Espacio único.
  - Múltiples dependencias.
  - Varios edificios independientes.
- Posibilidades de ampliación.

Los usuarios de un aula educativa en red son, evidentemente, los alumnos y los profesores. Cuando configuramos su funcionamiento debemos considerar estos dos tipos de usuarios a la hora de decidir qué sistema operativo vamos a implementar y cuáles son los permisos que debe tener cada uno de ellos en función de sus características personales o grupo al que pertenezca. Los permisos, además, deberán estar en función de cómo, para qué y cuando deban ser utilizados.

Las aulas informáticas pueden ser consideradas como elementos aislados dentro del centro educativo o como una parte más de una red integrada de comunicación. Por lo tanto, deberemos plantear el proyecto dentro de un elemento más amplio que es la cultura del centro. Evidentemente, puede suceder que ya exista una red informática de gestión en el centro y que, por razones obvias deseemos querer emplear los datos que en esta subred ya existan pero, a la vez, que se encuentren protegidos. Por otro lado, deberíamos poder acceder al aula informática desde cualquier equipo del colegio o instituto, sin mayor problema.

El espacio físico en el que queremos instalar nuestra red es otro elemento a tener en cuenta. En muchas ocasiones, los centros apenas si disponen de locales donde poder localizar el aula, o, estos locales no son los más adecuados. Por otro lado, un fenómeno que está sucediendo en multitud de centros es que, a partir de la creación del aula, comienza a extenderse una red informática por todas y cada una de las dependencias de los centros.

### Anotaciones

## Capítulo 6

En definitiva, estas reflexiones nos deben conducir a la idea de que la creación de una red informática en un centro docente es un tema complejo, influido por múltiples factores que, puede ser planificado pero de manera flexible para poder adaptarse a los múltiples cambios que se puedan producir sin llegar a perder la funcionalidad y los propósitos para los que se ha creado.

### 6.2. ¿Cómo empezar?

Como ya hemos dicho, una red en un centro educativo puede tener múltiples usos. Por lo tanto, lo que debemos realizar, en primer lugar, es formular los propósitos, las funciones a las que vamos a dedicar nuestra red.

Conocidos estos propósitos, deberemos establecer y clarificar los recursos de los que disponemos:

- Económicos.
- Espaciales.
- Materiales.
- Humanos.

La importancia, o la extensión que vayamos a dar a nuestra red dependerá de estos recursos y condicionará otras decisiones; ya que, si deseamos realizar un macroproyecto y disponemos de amplios recursos económicos es evidente que podemos encargar el trabajo a una empresa. Sin embargo, en la mayoría de los casos nos encontramos con que los recursos de los que disponemos son muy escasos.

Cuando hablamos de los propósitos que deseamos alcanzar con nuestra aula en red debemos centrarnos en una serie de temas:

- Pedagógicos.
- Docentes.
- Administrativos.

Por regla general, el aula en red tendrá una dedicación fundamentalmente pedagógica, de utilización por los alumnos, y una segunda función como herramienta docente. Evidentemente, si integramos este aula en una red superior, podremos optar por ofrecer también unos servicios de índole administrativo.

### Anotaciones

### a) Tipo de red.

En este apartado debemos analizar si deseamos una red “peer-to-peer” o basada en servidor. Evidentemente, para seleccionar un sistema u otro deberemos considerar diversos aspectos:

- Tamaño.
- Seguridad.
- Propósitos.
- Recursos humanos y económicos de los que se disponen para su administración y mantenimiento.

Dado que una red en un centro puede dedicarse a múltiples tareas se pueden contemplar la posibilidad de instalar un sistema lo más sensible posible. Desde este punto de vista la utilización de sistemas operativos servidores en redes de igual a igual puede ser la opción más adecuada para solventar este problema.

### b) Decisiones técnicas.

#### *Subsistema horizontal*

Dentro del tipo de red que podemos crear, la más eficaz para nuestros propósitos va a ser una LAN ETHERNET, con topología en estrella. Posteriormente decidiremos la existencia o no de un servidor. Elegimos esta red puesto que no requiere un gran mantenimiento, es bastante rápida y su instalación es sencilla.

Emplearemos un cableado UTP con conectores RJ45 ya que su conexión e implementación es muy sencilla.

Conviene igualmente la existencia de un RAS en el que preparamos la instalación posterior de un switch o un hub.

La localización del cableado y de las tomas de corriente eléctrica dependerán de la ubicación que queramos dar a los puestos de los alumnos. Aspecto que veremos posteriormente.

#### *Concentradores o conmutadores.*

En un aula escolar con un número de puestos que no va a superar en muchos casos las quince máquinas y que el tráfico de información no es excesivamente elevado la decisión entre el tipo de concentrador no es especialmente significativa. Actualmente la diferencia de precios no es elevada por lo que optaremos por el montaje de un switch 10/100Mbps de 24 puertos.

### Anotaciones

### **Tarjetas.**

Las tarjetas de red que instalaremos en los equipos serán 10/100 fast ethernet.

### **Equipos.**

Las características técnicas de las máquinas van a incidir más en la calidad del trabajo que queramos desarrollar con el alumnado que en el propio funcionamiento de la red, por lo que la decisión de optar más por unas características u otras dependerá del software que tengamos pensado utilizar.

Un aspecto para el que es necesario prestar especial atención es la configuración del equipo servidor y que, va a depender, las prestaciones que deba realizar. De entre los aspectos a los que debemos atender, cabría destacar:

- Caja o chasis: Debemos adquirir un tipo de caja suficientemente amplia para contener las unidades de disco que podamos necesitar a lo largo de sucesivas ampliaciones a la vez que debería estar equipada con ventiladores que proporcionen una refrigeración extra. Existen también cajas de servidores rækkeables para armarios de 19" que permiten que el servidor se encuentre perfectamente instalado junto con la electrónica de la red.
- Alimentación: Un servidor debe atender a un mayor requerimiento de energía que cualquier equipo de sobremesa, de ahí que la unidad de alimentación que vayamos a adquirir (suele acompañar a la caja) pueda ofrecer, al menos, 350 vatios de potencia.
- Procesador: los equipos servidores pueden tener uno o más procesadores; evidentemente, el número de procesadores mejorará la velocidad en el tratamiento de las tareas. El número de procesadores depende de la placa base que instalaremos. Si tenemos en cuenta que los requisitos de nuestra red pueden ir creciendo, podemos adquirir placas base para, por ejemplo, cuatro procesadores e instalar únicamente dos, para, según las necesidades, ir aumentando el número.

Es importante indicar que no todos los procesadores son válidos para trabajar en una placa que admite el uso conjunto de este dispositivo.

- Memoria: los equipos servidores deben ser capaces de ofrecer múltiples servicios a la vez, de ahí que un aspecto fundamental de su configuración sea la memoria. NO debemos escatimar en este aspecto puesto que por un desembolso relativamente bajo, podremos conseguir muchas mejores prestaciones.
- Interfaces: actualmente existen tres tipos de interfaces, SCASI, IDE y serial ATA. Cualquiera de estos tres interfaces puede ser empleado en un servidor, sin embargo, SCASI ofrece mejores prestaciones.

### **Anotaciones**

## Capítulo 6: Gestión y administración de redes.

La diferencia de precio es significativa, siendo Small Computer System Interface el más caro; una alternativa más económica sería el nuevo interfaz Serial ATA. Un servidor requiere dispositivos de almacenamiento de gran tamaño a los que se pueda acceder de una forma rápida.

- Bus de expansión: El bus de expansión estándar es el PCI, lo encontramos montado en la mayoría de las placas base. Un servidor incorporará más ranuras PCI y, probablemente no disponga ya de las obsoletas bahías de expansión ISA.
- Adaptador de video: esta es la parte menos importante de un servidor. Los administradores de red no necesitan la ejecución de ningún programa concreto que requiera el uso de altas prestaciones. Debemos tener en cuenta que muchas de las operaciones que se realizan en un servidor son a través de líneas de comandos, por lo que los requisitos de vídeo suelen ser muy bajos.

Por último conviene indicar que, el servidor debe encontrarse en un lugar protegido al que no puedan acceder los usuarios de la red. Así, su ubicación más adecuada es el rack, junto con la electrónica.

La diferencia fundamental entre una estación servidora y un equipo cliente la encontraremos en:

- Placa base y número de procesadores.
- Adaptador de vídeo y disponibilidad de puerto AGP.
- Interfaz de unidades.
- Cantidad de memoria.
- Número de unidades de almacenamiento y capacidad de las mismas.

### Sistema operativo.

Partiendo siempre de que cualquier sistema operativo que deseemos implementar debe estar debidamente registrado, vamos a pasar a analizar las características básicas de cada uno (conscientes de que ya existen sistemas descatalogados) y sus ventajas e inconvenientes para la utilización en cada caso.

- Windows 9/x

Con este sistema operativo podemos crear redes de igual a igual, permiten compartir recursos a la vez que se puede desarrollar trabajo independiente. La creación de usuarios es automática y las restricciones sólo se pueden conseguir mediante la configuración de las políticas de usuario (comando poledit). Sin embargo, el acceso al sistema operativo y al resto del software no puede ser limitado una vez que se ha arrancado el equipo.

### Anotaciones

## Capítulo 6

Las redes de estas características son fáciles de administrar y sencillas de configurar, pero se tiene el problema de la seguridad.

### Windows NT

Este sistema es mucho más seguro que el anterior. Se puede tener un puesto configurado con NT server y el resto con NT workstation. Son redes en las que todos los servicios los puede ofrecer una máquina servidora. Se puede crear una política de usuarios mucho más restrictiva por lo que se obtiene un sistema más seguro.

Como inconveniente podemos indicar que el fallo del servidor provoca que todo el sistema se venga abajo. Por ello, se pueden crear sistemas mixtos:

- o Servidor NT y equipos con windows 9/x.
- o Unidades con particiones NFTS o FAT 32 que permitan arrancar los equipos con un sistema que no sea windows NT.

Se trata, en definitiva, de un sistema muy seguro, que requiere de un administrador, lo que le confiere flexibilidad, y que puede ser muy recomendable cuando se corra peligro real de desconfiguración del sistema.

- Windows 2000 profesional y server.

Es un sistema operativo intermedio entre los dos anteriores. Recoge los aspectos positivos de independencia del la serie 9/x y hereda las opciones de seguridad del NT. Evidentemente, si se han de comprar nuevas licencias, al estar descatalogadas las dos versiones anteriores, deberíamos optar por instalar este sistema.

Tiene una política de perfiles más amplia que el Windows 9/x, cada usuario puede tener un perfil que se almacena localmente, pero que se crea automáticamente al entrar en un nuevo equipo, por lo que debemos configurarlo.

El sistema operativo servidor es el Windows 2000 server, que sería la versión evolucionada del Windows NT server. Permite un control total sobre la red y la administración de los usuarios de forma flexible, pudiendo crear perfiles ad hoc.

Evidentemente, si la administración de la red debe ser realizada por un usuario de nivel medio, recomendaremos utilizar redes de igual a igual sin un sistema operativo que actuara como servidor. En el caso de usuarios avanzados, sería conveniente optar con un sistema operativo de usuario en cada una de las estaciones y un server en otro equipo que realizará las funciones de servidor y administrador de políticas.

### Anotaciones



## Capítulo 6: Gestión y administración de redes.

- Windows XP.

Se trata de un sistema híbrido que se adapta perfectamente a situaciones de administración centralizada con perfiles móviles y directivas de grupo que se almacenarán en un servidor con sistema Windows XP profesional con otras en el directorio local.

Implementa más medidas de seguridad encriptando archivos, implementando certificados digitales e impidiendo la ejecución de scripts en determinados lugares del PC. Básicamente es la evolución de Windows 2000 implementando mayores medidas de seguridad y una administración más sencilla.

Por último, conviene destacar que incorpora herramientas para el desarrollo de trabajo colaborativo compartiendo aplicaciones e incorporando herramientas mejoradas de comunicación.

- Linux.

Linux es un sistema operativo que está siendo implementado en centros de toda España tras la iniciativa desarrollada en Extremadura. Se trata de un sistema multiusuario idóneo para los centros docentes.

Existen distintas distribuciones de Linux como Mandrake, Suse o Red hat que permiten la instalación personalizada de equipos clientes o servidores de forma totalmente gratuita.

Las dificultades de instalación y manejo han sido ampliamente solventadas y las tareas de administración han sido simplificadas pudiéndose ejecutar la mayoría de ellas mediante web o en entorno gráfico. Los escritorios kde o gnome son muy similares a los que incorpora Windows y a la hora de trabajar con usuarios noveles resulta indiferente la enseñanza de uno u otro entorno.

Su estabilidad, adaptación a entornos multiusuarios y su coste nulo hacen de este sistema operativo una opción francamente interesante para instalarla en un centro docente, más, teniendo en cuenta, que muchas de las necesidades que se deben cubrir en un centro se están realizando en servidores que disponen de este sistema y que existen numerosas aplicaciones bajo linux que reemplazan perfectamente a programas propietarios bajo windows.

Conviene indicar que en una misma red pueden convivir equipos con sistemas operativos distintos y que, un proceso de análisis de las necesidades reales del centro puede aconsejar la utilización de un servidor linux, junto a otro equipo con un Windows Server 2000 (está próxima la aparición de Windows Server 2003) y estaciones de trabajo XP o linux. En cualquier caso, cada centro debe adecuar sus sistemas a sus necesidades y posibilidades.

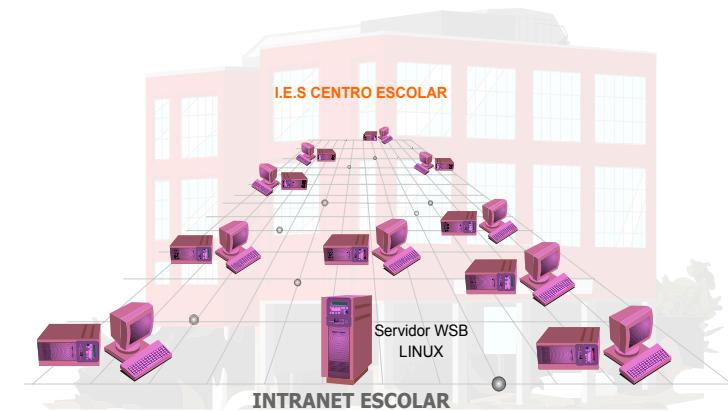


Ilustración 29: Intranet escolar

### Anotaciones

## Capítulo 6

### Conexión a Internet.

La conexión a Internet nos va a permitir acceder a servicios de gran valor educativo. Cuando estamos trabajando con varios alumnos a la vez necesitamos un ancho de banda suficiente. Los distintos tipos de conexión disponibles son:

- **Conexión telefónica RTC:** Ofrece hasta 56 kbytes de ancho de banda. Se puede hacer a través de un equipo que actúa como servidor de acceso mediante windows o creando un servidor proxy mediante un programa específico.
- **Conexión RDSI:** Mejora el ancho de banda de la telefonía ordinaria y permite dos conexiones, una de voz y otra de datos. Se puede realizar mediante una tarjeta conectada a un equipo o un modem-router conectado a un concentrador. Para aulas con más de ocho equipos se puede demostrar ineficiente.
- **Conexión ADSL:** El ancho de banda contratado es variable, pero permite la conexión simultánea de más de 10 equipos en su contrato básico y un funcionamiento óptimo de más de veinte equipos en red. Se conecta mediante un modem-router adsl a un concentrador comutado o con un hub-router al que pueden acceder varios equipos.

La conexión a Internet lleva aparejado otro tipo de decisiones que estudiaremos más adelante.

### c) Decisión pedagógicas.

#### Ubicación de los puestos y distribución del aula.

Independientemente de la topología física y lógica de la red, debemos plantearnos la ubicación de los equipos dentro del aula. Esta decisión, al igual que todas las comentadas hasta ahora, va a estar condicionada por otros factores:

- Tamaño.
- Estructura del aula.
- Papel docente.

El tamaño del aula, la disposición de las puertas y ventanas, etc. Condiciona en cierta medida la distribución y número de los puestos. En general, solemos trabajar con aulas de hasta quince puestos en los que podemos encontrar uno o dos alumnos trabajando.

El tamaño de cada puesto debería tener las siguientes medidas:

- Altura 65 a 75 cm.
- Anchura 100 a 120 cm.
- Profundidad 80 a 90 cm.

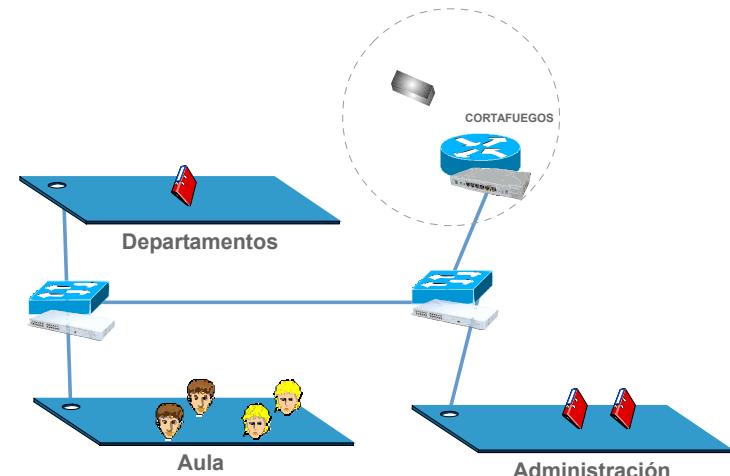


Ilustración 30: Esquema de una red de centros

### Anotaciones

- Espacio interior:
  - 60 cm de ancho.
  - 60-70 cm de profundidad.

Con estas medidas, que deberían ser respetadas para facilitar la comodidad de los alumnos mientras trabajan, deberíamos pensar en cómo los puestos pueden ser distribuidos en el aula.

Existen dos tendencias más extendidas:

- Disposición en U.
- Disposición en filas y columnas.

Cada una de estas disposiciones tiene una serie de ventajas e inconvenientes.

En la disposición en U los alumnos deben girarse para atender a las posibles explicaciones del profesor, mientras que pueden realizar un trabajo individual más autónomo. La estructura en filas y columnas facilita la atención a las explicaciones por parte del profesor, sin embargo supone la utilización de mucho más espacio para la realización de desplazamientos.

En ambos casos, la comunicación visual entre los alumnos se ve dificultada o requiere desplazamiento, por lo que convendría analizar otras opciones alternativas.

### **Recursos disponibles.**

Cuando nos planteamos el montaje de un aula no debemos olvidar la posibilidad de su ampliación. Así, si deseamos que las explicaciones que estemos realizando puedan ser vistas por todos los alumnos, deberemos instalar un programa que gestione los equipos y permita visualizar los distintos entornos o prever una posible salida de señal para un cañón de vídeo o un monitor de televisión. Por lo tanto, es necesario establecer la ubicación de estos dispositivos y los posibles sistemas de cableado para su conexión.

### **Perfiles de usuarios.**

En función de las tareas que queramos que desarrollemos nuestros alumnos deberemos determinar cuáles van a ser su perfil de usuario en cada equipo o en la red. Ya comentamos en el apartado de seguridad las restricciones que podía tener cada uno de los programas que instaláramos.

### **6.3. Seguridad.**

Dentro del concepto de seguridad vamos a tratar aspectos de muy distinto tipo:

- Seguridad del sistema: que sea estable y no susceptible de modificación intencionada o accidental por parte de usuarios no cualificados.

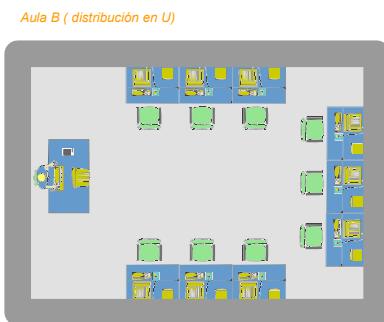
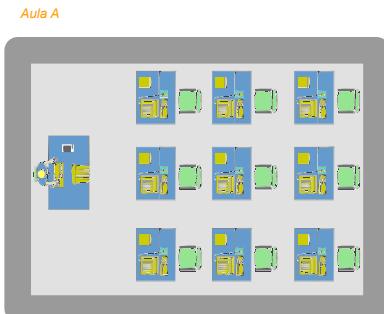


Ilustración 31: Distribución de un aula informática: la localización y distribución de los equipos dentro de un aula va a condicionar de forma definitiva el tipo de método que en ella se aplique.

### **Anotaciones**

- Seguridad de contenidos: Evitar que el alumnado pueda acceder a contenidos indebidos.
- Seguridad antivirus: Establecer medidas para que no puedan ser introducidos virus en los equipos mediante la instalación de programas, la descarga de páginas web o archivos o la recepción de correos.
- Seguridad de intervención remota: para que se evite el acceso a nuestra red desde el exterior a personas no cualificadas.

### a) Seguridad del sistema.

Los usuarios son los principales enemigos de la estabilidad de un sistema. Cuando nos proponemos la creación de una red debemos considerar la capacidad que pueden tener los usuarios para modificar la configuración del sistema y de los equipos. Para conseguir la máxima seguridad deberemos crear una red que esté configurada con un programa servidor que gestione los perfiles de usuario.

Una propuesta sería:

- Administrador: Responsable del aula. Control total del sistema.
- Usuario avanzado: Profesores. Pueden instalar programas que no afecten al sistema, además pueden crear grupos de usuarios y personalizar los recursos del sistema.
- Usuario: alumnado. Sólo puede actuar con control total en los archivos del sistema creados para él.

Aunque estas medidas pueden mejorar la seguridad de la integridad del sistema, no se puede estar absolutamente seguro. Por ello, resulta conveniente la realización diaria de copias de seguridad (siguiendo criterios de optimización de este proceso) y la creación de imágenes de los equipos que puedan ser cargadas en remoto o desde un cd-rom.

### b) Seguridad de contenidos.

El acceso a los contenidos de Internet es uno de los temas que más preocupan al profesorado cuando accede a la red. Los Navegadores suelen tener herramientas que permiten controlar el acceso a contenidos en función de sistemas de clasificación. Todos los sitios que no estén clasificados también pueden ser bloqueados y se pueden añadir páginas específicas.

Otra opción es la instalación de programas que filtran la información creando una separación de los contenidos que puedan ser considerados nocivos, evitando que los alumnos puedan llegar a tener acceso a esos contenidos:

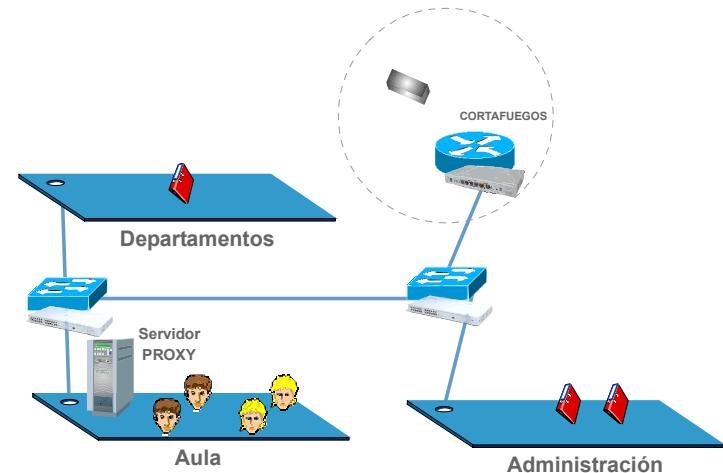


Ilustración 32: Control de acceso: el servidor proxy controla el acceso a contenidos desde el aula mientras que el router hace de cortafuegos para Departamentos y red administrativa

## Anotaciones

- [Cyber Patrol](#)
- [CYBERsitter](#)
- [Net Nanny](#)
- [SurfWatch](#)
- Ministerio de ciencia y tecnología.

Al igual que sucede en el apartado anterior, estos programas tienen una efectividad del 99%.

### c) Seguridad antivirus.

Todos los expertos señalan que es prácticamente imposible conseguir que un equipo informático conectado a Internet no sea susceptible de ser infectado con un virus. Pero, evidentemente, si no se dispone de ningún programa antivirus que se actualice con una cierta periodicidad, es mucho mayor el riesgo.

Por lo tanto, para poder tener ciertas garantías de no contagiarse con algún virus es conveniente tener el software antivirus instalado y actualizado.

La instalación de este tipo de programas va a depender de la configuración que tenga nuestra red. Si disponemos de un equipo configurado con un programa servidor podemos centralizar la actualización del fichero de firmas y del propio programa a través de él. En caso de no disponer de este equipo, deberíamos configurar la actualización en cada uno de los puestos.

Las tareas que deben estar programadas o han de realizarse con un programa antivirus son:

- Actualización del fichero de firmas (diario)
- Actualización del programa (mensual)
- Analizar el sector de arranque de C: (al iniciar windows)
- Analizar el correo electrónico (activo)
- Analizar todo el equipo (semanal)

Existen, además, otras opciones para evitar que se ejecuten archivos dudosos a través del correo o del navegador. Por ejemplo, en el correo deberemos desactivar la vista previa, mientras que en el navegador deberemos limitar la ejecución de controles ActivX, evitar las descargas y establecer el nivel de seguridad alta.

### Anotaciones

## Capítulo 6

Por último, resulta muy conveniente crear particiones en los discos duros de los equipos de manera que no perdamos toda la información que tengamos en los equipos en caso de una infección crítica.

### d) Seguridad ante intrusos.

La invasión de Redes por parte de intrusos se está convirtiendo en un hecho habitual. Para evitar esta intromisión debemos montar un sistema cortafuegos. Este elemento de una red se trata, básicamente, de un sistema (equipo o programa) que puede controla desde el nivel 3 al nivel 7 del sistema OSI el acceso de paquetes o aplicaciones a nuestra red.

Un cortafuegos es la primera línea para la defensa de nuestra red y permite bloquear nuestros puertos, evitar la ejecución de scripts y filtrando la información. Algunos pueden realizar también funciones de control de acceso a contenidos. Tres programas gratuitos son:

- Freedom.
- Tiny.
- Agnitum outpost firewall

Existen cortafuegos gratuitos o de pago, e incluso con un ordenador pentium y linux se puede configurar uno. En definitiva, lo que se trata es de controlar el flujo de mensajes que entran y salen de nuestros equipos. Su acción es perimetral, por lo que conviene establecer también una serie de normas a los usuarios avanzados para que no instalen determinados programas.

Por último, existen programas que permiten escanear nuestros equipos con el fin de averiguar si tenemos intrusos, puesto que, en muchos casos, los cortafuegos dan una errónea sensación de seguridad.

### 6.4. Aplicaciones.

Uno de los problemas más graves que tiene la informática educativa es la carencia de recursos económicos. Una vez que hemos podido crear nuestra red nos encontramos con que no disponemos del software necesario para su utilización.

Independientemente del sistema operativo (linux es una opción que no podemos pasar por alto), debemos instalar otra serie de programas para la utilización de los equipos. Existen en la red gran cantidad de software gnu y freeware que pueden resultar de gran utilidad, evitando así la utilización de programas sin licencia.

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

Un paquete básico estaría constituido por:

- Suite ofimática (por ejemplo Staroffice 5.2 u OpenOffice 1.0)
  - Editor de texto.
  - Presentaciones.
  - Hoja de cálculo.
  - Programa de dibujo.
- Navegadores y programas de correo electrónico y chat.
- Compresor (Winzip o Netzip)
- Visor multimedia (Real player, Windows mediaplayer, Quicktime for windows)
- Lector de pdf (Adobe acrobat o similar)
- Emulador de CD.
- Programa para la realización de particiones: Partition magic o similar
- Software para la realización de copias de seguridad.
- Programas para el análisis del sistema.
- Programa antivirus, firewall y de búsqueda de intrusos.
- Programa para la creación de imágenes de disco o particiones: Ghost.
- Software de grabación: Clone cd o Nero burning.
- Programas de monitorización del aula y control remoto de los equipos.
- Aplicaciones didácticas. Se pueden encontrar en distintas páginas web. Muy recomendable la página de los premios de materiales multimedia del cnice.

[http://www.cnice.mecd.es/educacion/programas\\_edu.htm](http://www.cnice.mecd.es/educacion/programas_edu.htm)

### a) Utilidades.

En general, estas aplicaciones informáticas pueden ser trabajadas con los alumnos, aunque en muchos casos requieren gran trabajo de preparación. Por ejemplo, la elaboración de una presentación de diapositivas o la utilización de un procesador de texto con fines didácticos es una tarea ardua.

### Anotaciones

## Capítulo 6

Por otro lado, existen programas informáticos educativos que pueden ser utilizados, en algunos, casos en red. Su aplicación a nivel de aula es difícil ya que requiere tener un número elevado de copias, que, como ya hemos dicho, en muchos casos no es posible. Por lo tanto, deberemos realizar una selección muy buena de los materiales que vayamos a adquirir para evitar un uso precario de nuestro aula.

Por último, debemos pensar en el gran recurso que es Internet. El acceso a datos, buscadores, diccionarios, encyclopedias en línea, etc. Nos ofrece una gran cantidad de posibilidades que no debemos olvidar.

### 6.5. Organización y mantenimiento.

El mantenimiento y la organización de un aula es un trabajo que requiere de un esfuerzo continuado. Esto es debido, sobre todo, a que a diario pueden llegar a pasar más de 100 usuarios distintos que requieren de los equipos funciones muy distintas. Al ser uno de los recursos más utilizados del centro sufre un enorme desgaste, de manera que, a pesar de todas las medidas que se puedan adoptar, nos encontramos con que se pueden producir:

- Fallos de hardware y periféricos: ratones que no funcionan, fallos de tarjetas de red, rotura de un disco, averías en tarjetas de memoria, fallos en las fuentes de alimentación, etc.
- Fallos de software y deterioro del sistema.

El problema fundamental para resolver las situaciones creadas es la falta de tiempo, ya que para reparar uno a varios equipos se necesita su tiempo. Por otro lado, un responsable de aula o administrador no tiene por qué tener conocimientos específicos sobre reparación de hardware. Por lo tanto, deberemos plantearnos la adopción de diversas medidas:

- Crear un equipo de personas que colaboren en la gestión del aula.
- Reemplazar las limitaciones que pueda tener estas personas a través de las garantías de los equipos y/o servicios de mantenimiento.

En general, deberemos establecer momentos para poder realizar las tareas de mantenimiento y reparación, además de determinar claramente las responsabilidades de cada individuo.

Las tareas más habituales son:

- Instalación y desinstalación de programas.
- Control de políticas de usuarios.
- Control de los registros.
- Reposición de piezas dañadas.

### Anotaciones

- Restauración de sistemas deteriorados.
- Análisis del sistema del sistema.

Como ya venimos señalando a lo largo de este capítulo, todas las medidas de seguridad son pocas, pero, evidentemente, siempre deberemos estar preparados para lo peor. Por lo tanto, debemos plantearnos las siguientes medidas.

- Disponer de un servidor.
- Disponer de copias de seguridad diarias.
- Disponer de imágenes de los discos y particiones en discos y que se puedan aplicar en remoto o local.

Por último, la circulación correcta de la información es otra herramienta de gran ayuda ya que nos va a permitir saber qué, cómo y cuándo se ha producido alguna avería. La creación de un tablón donde se indiquen las incidencias puede ser de gran ayuda para realizar esta función.

### 6.6. Propuesta.

Todas las decisiones descritas anteriormente nos van a permitir definir una aula informática para el trabajo con alumnos, desde los aspectos técnicos a los didácticos. Evidentemente, cada centro representa una situación peculiar y lo que es válido para uno puede demostrarse nefasto para otro.

Como propuesta de trabajo formularíamos la siguiente:

- Red Ethernet en estrella con switch (100Mbps).
- Equipos Pentium IV o similar (AMD), multimedia y con tarjeta de red fast ethernet 10/100.
- Aula con disposición abierta y posibilidad de ampliar los mecanismos de salida.
- Conexión a Internet ADSL premium a través de MODEM y conexión a switch.
- Equipo servidor con sistema operativo configurado para gestionar los perfiles de los usuarios.

### Anotaciones

### Ilustraciones

<b>Ilustración 1:</b> Las redes escolares están dedicadas a múltiples propósitos que dificultan la definición de su estructura	3
<b>Ilustración 2:</b> Una red basada en servidor consta de terminales "tontos" que dependen completamente de un servidor.	4
<b>Ilustración 3:</b> Un servidor de aplicaciones permite la utilización de un mismo programa desde los distintos equipos de la red.	5
<b>Ilustración 4:</b> Al acceder todos los equipos a un mismo administrador de archivos se simplifica la realización de copias de seguridad de los documentos.	6
<b>Ilustración 5:</b> El controlador de dominio gestiona la base de datos de usuarios de manera que cualquier persona que acceda a un equipo deba identificarse para poder utilizar los distintos servicios.	7
<b>Ilustración 6:</b> Entorno de trabajo: Un sistema centralizado permite mantener un entorno similar de trabajo en cualquier estación	8
<b>Ilustración 7:</b> NTES: Almacena en su lista de archivos de datos que permiten controlar el acceso de los usuarios a cada directorio	9
<b>Ilustración 8:</b> Sistemas de autentificación: Las últimas tendencias en seguridad se dirigen a la autentificación biomédica de usuarios	10
<b>Ilustración 9:</b> Restricciones del SO: Permiten eliminar el acceso a unidades de disco en función del usuario que acuda al sistema	11
<b>Ilustración 10:</b> Problemas de red: El origen de los fallos de comunicación en una red pueden ser de muy distintos tipos	12
<b>Ilustración 11:</b> Problemas físicos: Uno de los problemas más frecuentes es el fallo del conector en la tarjeta, por lo que deberá comenzar cualquier operación revisando esta conexión	13
<b>Ilustración 12:</b> Servidor DNS: La caída del servidor DNS impide la traducción de nombre de dominio a dirección IP y, por lo tanto, el acceso a Internet	14
<b>Ilustración 13:</b> Traceroute: La orden Traceroute devuelve e informa del camino seguido por un paquete de datos hasta un host determinado	16
<b>Ilustración 14:</b> Nslookup: Permite averiguar la dirección IP de cualquier máquina	17
<b>Ilustración 15:</b> Un cortafuegos controla la puerta de acceso de nuestra red al exterior filtrando el tráfico en ambas direcciones.	18
<b>Ilustración 16:</b> Uno de los elementos críticos de que deben ser tenidos en cuenta a la hora de elaborar las políticas de seguridad es el servidor de acceso a Internet	19
<b>Ilustración 17:</b> Esquema de una red en la que un servidor proxy actúa como cortafuegos.	20
<b>Ilustración 18:</b> Router actuando como cortafuegos mediante el filtrado de paquetes	21

### Anotaciones

## Capítulo 6: Gestión y administración de redes.

<b>Ilustración 19:</b> Screened subnet: Los routers detienen a ambos lados de los servidores el tráfico interno y externo	22
<b>Ilustración 20:</b> Bomba lógica: Es un virus que se activa ante determinadas condiciones	23
<b>Ilustración 21:</b> Gibe.C: Es un gusano que al infectar el sistema facilita la entrada de otros virus	24
<b>Ilustración 22:</b> Big Brother: Es un hoxo que informa del peligro de un virus relacionado con "gran hermano". Su objetivo es causar alarma	25
<b>Ilustración 23:</b> Antivirus: Los antivirus, entre otras cosas, comprueban el tráfico de correo electrónico buscando comportamientos análogos	26
<b>Ilustración 24:</b> Niveles y actuaciones de seguridad	27
<b>Ilustración 25:</b> Las copias de seguridad se realizan de forma más sencilla cuando los archivos se encuentran centralizados	28
<b>Ilustración 26:</b> Protección de archivos: La copia de seguridad en red facilita el proceso de protección de archivos distribuidos	30
<b>Ilustración 27:</b> Copia diferencial: selecciona los archivos modificados para hacer copia y pone a 0 el punto de referencia de copia	31
<b>Ilustración 28:</b> Imagen de disco: permiten guardar una copia de los archivos de un disco en un formato comprimido	33
<b>Ilustración 29:</b> Intranet escolar	41
<b>Ilustración 30:</b> Esquema de una red de centros	42
<b>Ilustración 31:</b> Distribución de un aula informática: la localización y distribución de los equipos dentro de un aula va a condicionar de forma definitiva el tipo de método que en ella se aplique.	43
<b>Ilustración 32:</b> Control de acceso: el servidor porky controla el acceso a contenidos desde el aula mientras que el router hace de cortafuegos para Departamentos y red administrativa	44

### Anotaciones