4 Seguridad informática

Virus informáticos. Los virus del ordenador adquieren mucha importancia en una sociedad informatizada, pero no son los únicos enemigos contra los que nos debemos proteger.

Entendemos por **seguridad informática** el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad.

Un **sistema es íntegro** si impide la modificación de la información a cualquier usuario que no haya sido autorizado con anterioridad.

Un **sistema es confidencial** si impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.

Estas características que limitan el uso de la información deben ir unidas al concepto de **disponibilidad,** pues los sistemas deben estar disponibles para que los usuarios autorizados puedan hacer un uso adecuado de ellos.

Según todo esto, *¿crees poseer un sistema informático seguro en tu casa o en tu aula de informática? ¿Puede ver tus archivos cualquier usuario que trabaje con tu mismo ordenador? ¿Proteges tu identidad usando contraseñas y claves de acceso?*

A menudo restamos importancia a la seguridad de nuestro ordenador excusándonos en reflexiones como estas: «mi ordenador no es importante», «¿quién va a querer entrar en mis archivos?», «mientras no introduzca discos con virus, mi ordenador estará seguro». La práctica nos demuestra que todo ordenador debe estar protegido en mayor o menor medida y que los usuarios deben acostumbrarse a prácticas que aumenten la seguridad de sus equipos.

4.1. ¿Contra qué nos debemos proteger?

- **Contra nosotros mismos,** que en numerosas ocasiones borramos archivos sin darnos cuenta, eliminamos programas necesarios para la seguridad o aceptamos correos electrónicos perjudiciales para el sistema.
- **Contra los accidentes y averías,** que pueden hacer que se estropee nuestro ordenador y perdamos datos necesarios.
- **Contra usuarios intrusos que,** bien desde el mismo ordenador, bien desde otro equipo de la red, puedan acceder a datos de nuestro equipo.
- **Contra software malicioso o *malware*,** es decir, programas que aprovechan un acceso a nuestro ordenador para instalarse y obtener información, dañar el sistema o incluso llegar a inutilizarlo por completo.

Malware

Software creado para instalarse en un ordenador ajeno sin el conocimiento del usuario. Su finalidad consiste en obtener información y en ralentizar el funcionamiento o destruir archivos. En esta categoría de software se encuentran los virus, los gusanos, los troyanos y los espías.

Actividades

19 ¿Qué factores hacen necesario acostumbrarse a realizar tareas de mantenimiento y seguridad en nuestro equipo informático?

20 ¿Qué entendemos por seguridad informática?

21 ¿Cuáles son los principales objetivos del malware?

22 Accede a la web del Instituto Nacional de Tecnologías de la Comunicación (INTECO: www.inteco.es ▶ **Seguridad** ▶ **INTECO-CERT** ▶ pestaña **Estadísticas**). Analiza qué virus ha tenido más repercusión en los sistemas españoles en las últimas veinticuatro horas y explica su funcionamiento y el método de propagación que utiliza.

4.2. Seguridad activa y pasiva

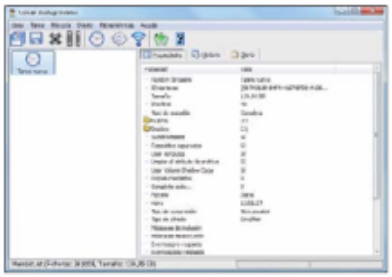
Podemos diferenciar dos tipos de herramientas o prácticas recomendables relacionadas con la seguridad:

- Las **técnicas de seguridad activa,** cuyo fin es evitar daños a los sistemas informáticos:
  1. El empleo de **contraseñas adecuadas.**
  2. La **encriptación de los datos.**
  3. El uso de **software de seguridad informática.**
- Las **técnicas o prácticas de seguridad pasiva,** cuyo fin es minimizar los efectos o desastres causados por un accidente, un usuario o *malware.* Las prácticas de seguridad pasiva más recomendables son estas:
  1. El **uso de hardware adecuado** frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, utilización de dispositivos SAI, etcétera).
  2. La realización de **copias de seguridad de los datos** y del sistema operativo en más de un soporte y en distintas ubicaciones físicas.

Una práctica muy aconsejable ya explicada anteriormente es la **creación de particiones lógicas en el disco duro** para poder almacenar archivos y *back-up* en una unidad distinta que el sistema operativo.

Copias de seguridad

Existen programas que automatizan el proceso de creación de las copias de seguridad. En entorno Windows el programa libre más utilizado es Cobian Backup, que permite realizar copias de seguridad de archivos, carpetas o discos duros completos.

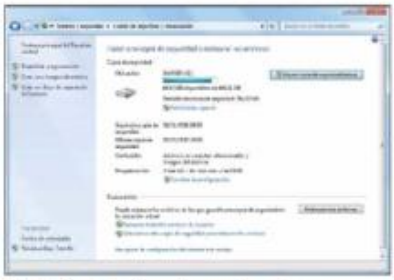


http://www.cobian.se/

Windows 7 incorpora su propia utilidad de copias de seguridad y permite restaurar un ordenador a su última copia de seguridad.

Otra herramienta libre que realiza clonaciones completas de discos y particiones es **Clonezilla.**

En entorno Linux la herramienta más popular es **Back in Time.** Esta utilidad realiza copias de seguridad completas de archivos en la ubicación que determinemos de una forma muy sencilla.



http://backintime.le-web.org/

4.3. Las amenazas silenciosas

Nuestro ordenador se encuentra expuesto a una serie de **pequeños programas o software malicioso** que puede introducirse en el sistema por medio de los correos electrónicos, la navegación por páginas web falsas o infectadas, la transmisión de archivos contaminados desde soportes como discos magnéticos, unidades de memoria, CD, DVD, etcétera.

Podemos encontrar los siguientes tipos de software malicioso:

- **Virus informático.** Es un programa que se instala en el ordenador sin el conocimiento de su usuario y cuya finalidad es propagarse a otros equipos y ejecutar las acciones para las que fue diseñado. Estas funciones van desde pequeñas bromas que no implican la destrucción de archivos, o la ralentización o apagado del sistema, hasta la destrucción total de discos duros.
- **Gusano informático.** Es un tipo de virus cuya finalidad es multiplicarse e infectar todos los nodos de una red de ordenadores. Aunque no suelen implicar la destrucción de archivos, sí ralentizan el funcionamiento de los ordenadores infectados y de toda su red. Suelen acompañar a un correo electrónico malicioso y muchos tienen la capacidad de enviarse automáticamente a todos los contactos del programa gestor de correo. Independientemente de los sistemas de protección que utilicemos en nuestro ordenador, siempre es recomendable ser cauteloso a la hora de abrir correos electrónicos.

Troyano.

- **Troyano.** Es una pequeña aplicación escondida en otros programas de utilidades, fondos de pantalla, imágenes, etc., cuya finalidad no es destruir información, sino disponer de una puerta de entrada a nuestro ordenador para que otro usuario o aplicación recopile información de nuestro ordenador o incluso tome el control absoluto de nuestro equipo de una forma remota. Los sistemas de transmisión que utilizan son el acompañamiento a otras aplicaciones y los medios de transmisión son la web, el correo electrónico, los chats o los servidores ftp.

Espía.

- **Espía.** Un programa espía o *spyware* es un programa que se instala en el ordenador sin conocimiento del usuario y cuya finalidad es recopilar información sobre el usuario para enviarla a servidores de Internet que son gestionados por compañías de publicidad. La información que recopila un espía suele ser utilizada para enviarnos *spam* o correo basura. Los ordenadores infectados con *spyware* ven muy ralentizada su conexión a Internet.

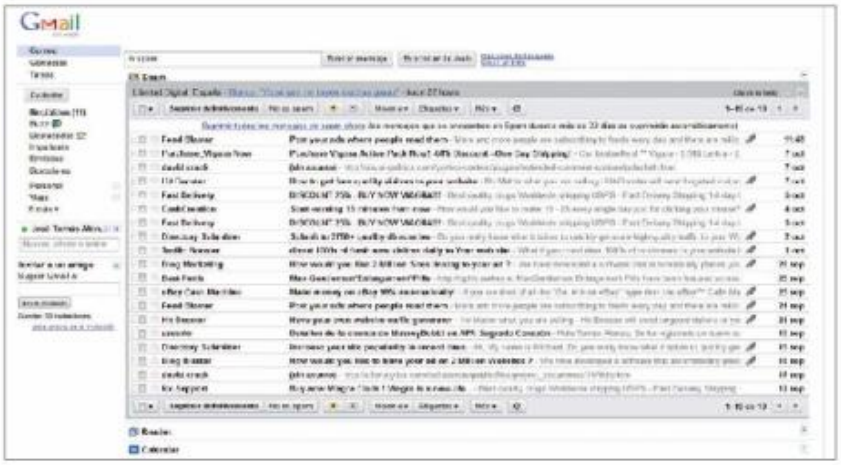
Dialer.

- ***Dialer.*** Son programas que se instalan en el ordenador y utilizan el módem telefónico de conexión a Internet del usuario para realizar llamadas telefónicas de alto coste, lo que provoca grandes gastos al usuario y beneficios económicos al creador del *dialer*. Si la conexión a Internet se realiza mediante un *router* ADSL, se evita este problema. Es aconsejable indicar a nuestro proveedor telefónico que nos bloquee las llamadas a servicios telefónicos de pago (803, 806, 807, etcétera).

Spam.

- ***Spam.*** También conocido como **correo basura,** consiste en el envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Tiene como finalidad vender sus productos. Los principales perjuicios que nos ocasiona es la saturación de los servidores de correo y la ocultación de otros correos maliciosos.

Todos los gestores de correo actuales disponen de listas negras de contactos para bloquear sus envíos y además almacenan los correos sospechosos en una carpeta denominada correo basura o *spam*.



Phishing.

- ***Pharming.*** Consiste en la suplantación de páginas web por parte de un servidor local que está instalado en el equipo sin que el usuario lo sepa. La suplantación suele utilizarse para obtener datos bancarios de los usuarios y cometer delitos económicos.
- ***Phishing*** (pesca de datos). Práctica delictiva que consiste en obtener información confidencial de los usuarios de banca electrónica mediante el envío de correos electrónicos que solicitan dicha información. Esta estafa se disimula dando al correo el aspecto oficial de nuestro banco y utilizando la misma imagen corporativa.

- ***Keylogger*** (registro de teclas). Mediante la utilización de software malicioso o incluso mediante dispositivos de hardware, su función consiste en registrar todas las pulsaciones que el usuario realiza en su teclado, para posteriormente almacenarlas en un archivo y enviarlo por Internet al creador del *keylogger*. De este modo se pueden obtener informaciones sensibles tales como contraseñas, datos bancarios, conversaciones privadas, etcétera.

Keylogger.

Los *keylogger* también pueden presentarse como pequeños dispositivos de hardware que se conectan entre el teclado y la CPU. Con una simple comprobación visual se puede descubrir el dispositivo espía.

- ***Rogue* software** o falso programa de seguridad. Se trata de falsos programas antivirus o antiespías que hacen creer al usuario que su sistema se encuentra infectado por virus o programas espías para hacerle comprar un programa que elimine esta falsa infección.

Rogue software

Si tenemos dudas sobre la autenticidad de un programa de seguridad podemos consultar las numerosas listas que existen para informar a los usuarios.

http://www.infospyware.com/rogue-software/

http://www.spywarewarrior.com/

4.4. Los virus llegan a nuevos dispositivos

La aparición de nuevos dispositivos electrónicos como tabletas, *smartphones,* consolas de juegos, etc. ha hecho que también proliferen los programas *malware* que atacan a estos nuevos aparatos.

Los medios más comunes de propagación de los virus informáticos en estos dispositivos electrónicos son la navegación por páginas web infectadas, la transmisión de archivos por bluetooth o por memorias portátiles, la descarga de aplicaciones gratuitas, la instalación de juegos demo, etcétera.

Actividades

23 Realiza una tabla de las medidas de seguridad activas y las medidas de seguridad pasivas en sistemas informáticos.

24 Explica la diferencia entre un gusano informático, un troyano y un software espía.

25 ¿Cómo podemos evitar los efectos del *dialer*?

26 ¿Para qué sirve un dispositivo *keylogger*? ¿Cómo se conectaría en un ordenador? ¿Hay programas que realizan la misma operación?

27 Localiza en Internet tres capturas de programas identificados como rogue software. Imprímelas para incorporarlas a tu cuaderno o envíalas por medios electrónicos a tu profesor.

Programas antivirus actuales

Se suelen distribuir en paquetes que incluyen numerosas herramientas, como antiespías, cortafuegos, antispam, etcétera. Se denominan **suites de seguridad.**

Herramientas de desinfección

Algunas empresas de seguridad informática facilitan a los usuarios herramientas que, si bien no son antivirus completos, pueden ayudarnos a resolver un problema concreto: un CD de arranque para analizar los programas del inicio, una vacuna para las unidades USB…

4.5. El antivirus

Un programa **antivirus** es un programa cuya finalidad es detectar, impedir la ejecución y eliminar software malicioso (virus informáticos, gusanos, espías y troyanos).

El funcionamiento de un antivirus consiste en **comparar los archivos** analizados del ordenador con su propia base de datos de archivos maliciosos, también llamados **firmas.** Para un buen funcionamiento la base de datos debe estar actualizada, ya que aparecen nuevos virus constantemente. Los antivirus modernos disponen de servicios de actualización automática por Internet.

Muchos programas antivirus también funcionan con **sistemas heurísticos.** La técnica heurística de un antivirus consiste en analizar el código interno del archivo y determinar si se trata de un virus aunque no se encuentre en su base de datos de firmas maliciosas. Esta forma de trabajo es muy importante para detectar los nuevos virus que todavía no se han incluido en las bases de datos. Los programas antivirus tienen distintos niveles de protección:

- **El nivel de residente,** que consiste en ejecutar y analizar de forma continua los programas que se ejecutan en el ordenador, los correos entrantes y salientes, las páginas web, etc. El **antivirus residente** consume recursos de nuestro ordenador y puede ralentizar su funcionamiento.
- **El nivel de análisis completo** consiste en el **análisis de todo el ordenador,** es decir, de todos los archivos de disco duro, del sector de arranque, de la memoria RAM, etc. Los análisis completos del sistema se van haciendo más rápidos cuanto más se repitan, ya que el antivirus marca los archivos en buen estado para evitarlos en posteriores análisis.

Antivirus gratuitos

En los últimos años están apareciendo herramientas que permiten hacer un análisis de un ordenador de forma remota desde Internet; se trata de los antivirus *on-line.* En la siguiente tabla podemos ver ejemplos de **antivirus gratuitos** para los diferentes sistemas operativos y análisis por Internet.

WINDOWS			
Avast 6 Free http://www.avast.com/es-es	**Avira antivir personal** http://www.avira.com/es/avira-free-antivirus	**AVG Free Anti-virus** http://free.avg.com/es-es/inicio	**Microsoft Security Essentials** http://www.microsoft.com/es-es/security_essentials
Panda Cloud Free edition http://www.cloudantivirus.com/es	**Clamwin antivirus** http://es.clamwin.com/	**Comodo Antivirus** http://www.comodo.com	**PCtools Antivirus** http://www.pctools.com/es
MAC OS X	**ANDROID**	**LINUX**	**ON-LINE**
ClamXAV	AVG Mobilation	LINUXAVG Free anti-virus	PANDA Active scan 2.0 http://www.pandasecurity.com
Sophos	NetQin	AVAST Linux free	ESET On-line Scanner http://eos.eset.es/
iAntivirus	Norton Mobile Secure	ClamTK	Bitdefender QuickScan http://www.bitdefender.es/free tools/

4.6. Cortafuegos

Un programa **cortafuegos** o ***firewall*** es un programa cuya finalidad es permitir o prohibir la comunicación entre las aplicaciones de nuestro equipo y la red, así como evitar ataques intrusos desde otros equipos hacia el nuestro mediante el protocolo TCP/IP.

Se encarga de controlar el tráfico entre nuestro equipo y la red local e Internet. Para que el funcionamiento de un cortafuegos sea eficaz, debe tener configuradas una serie de reglas para las aplicaciones que tienen permiso de comunicación con la red (explorador de Internet, cliente de correo, aplicación de actualización del antivirus, etc.) y prohibir la comunicación de aplicaciones que no queremos que interactúen con Internet.

Cuando el cortafuegos detecta que una aplicación intenta comunicarse con Internet y no tiene configuradas las reglas al respecto, emerge una ventana que nos pregunta lo que debe hacer con esa comunicación. Windows XP y Windows 7 tienen su propio cortafuegos, que es fácil de configurar:

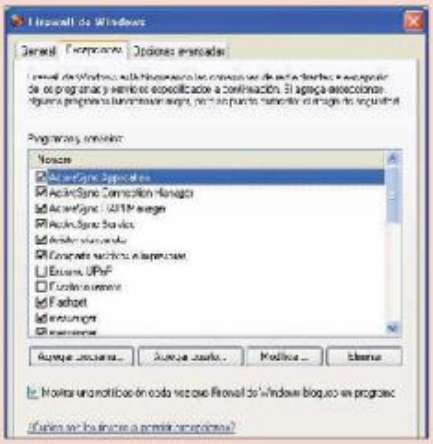
Firewall de los *router* de acceso a Internet

Los *router* de acceso a Internet tienen su propio firewall. Para configurar este firewal debemos entrar en la configuración del router utilizando la IP de la puerta de enlace de nuestra red, en el explorador.

Configuración en Windows XP

Paso 1. Accedemos al menú **Inicio ▶ Panel de control ▶ Centro de seguridad ▶ Firewall de Windows.**

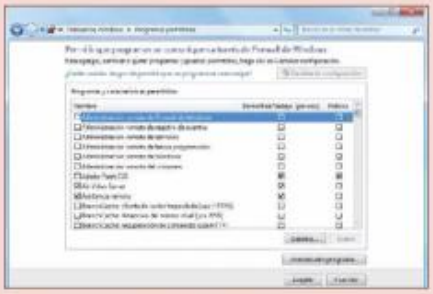
Paso 2. Para que realice su tarea, el cortafuegos debe estar activado. Accedemos a la pestaña **Excepciones** y añadimos los programas permitidos.



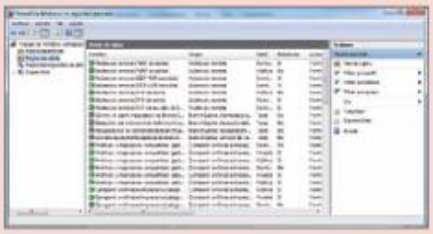
Configuración en Windows 7

Paso 1. Accedemos al menú **Inicio ▶ Panel de control ▶ Sistema y seguridad ▶ Firewall de Windows.**

Paso 2. Con la opción **Permitir que programas se comuniquen a través del firewall de Windows,** podremos añadir excepciones al cortafuegos.

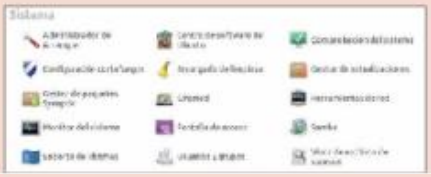


Paso 3. En la configuración avanzada se pueden dar permisos de entrada o de salida de forma independiente a cada programa.



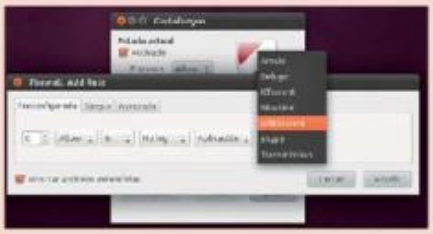
Configuración en Ubuntu

Paso 1. Ubuntu 11 tiene instalado el cortafuegos GUFW. Se accede a su configuración en la ruta **Botón apagado ▶ Configuración del sistema ▶ Sistema.**



Paso 2. Con el cortafuegos activo podemos añadir o borrar reglas de conexión de los programas instalados

Paso 3. Al añadir una nueva regla debemos definir el tipo de permiso y la aplicación o servicio instalado.



Cortafuegos gratuitos

Aunque los sistemas operativos traen consigo su propio cortafuegos, se pueden instalar versiones gratuitas de aplicaciones comerciales.

CORTAFUEGOS GRATUITOS			
ZoneAlarm http://www.zonealarm.com	**Comodo Firewall** http://personalfirewall.comodo.com/	**Ashampoo Firewall** https://www.ashampoo.com/en/eur	**Agnitum Outpost free** http://free.agnitum.com/

FUENTE: Oficina de seguridad del internauta, http://www.osi.es.

4.7. Software antispam

Spam

Término inglés sin traducción literal que tiene su origen en una marca de jamón enlatado americano de no muy buena calidad. Ha sido adoptado para denominar el correo masivo no deseado.

El **software antispam** son programas basados en filtros capaces de detectar el correo basura, tanto desde el punto cliente (nuestro ordenador) como desde el punto servidor (nuestro proveedor de correo).

El *spam* o correo basura es enviado masiva e indiscriminadamente por empresas de publicidad. La lucha contra el correo basura resulta compleja si se pretende respetar al mismo tiempo los correos electrónicos normales.

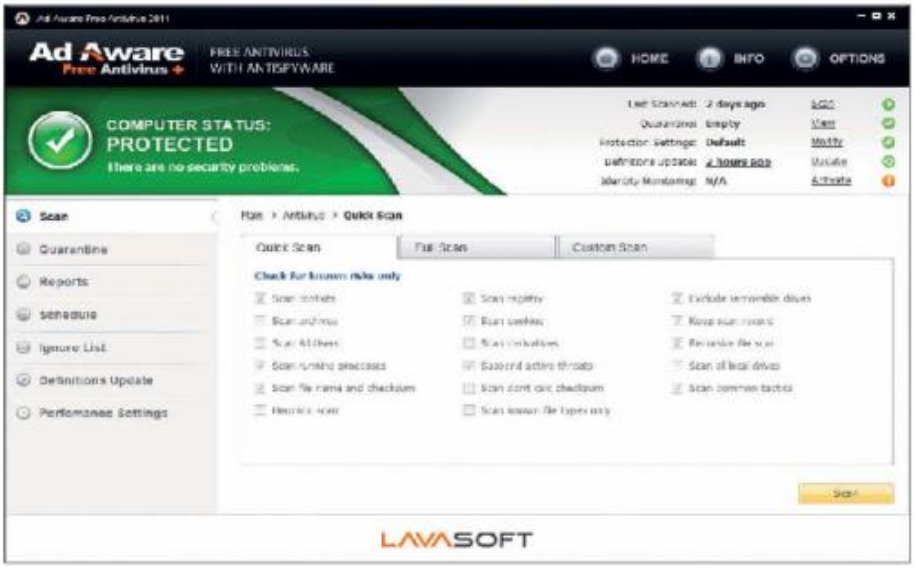
Estos filtros analizan los correos electrónicos antes de ser descargados por el cliente. La forma de detección está basada en listas o bases de datos de correos *spam*, en el análisis de la existencia del remitente, etcétera.

Actualmente la mayoría de los antivirus tienen integrado en sus distribuciones de seguridad un filtro anti-spam.

Existen dos tipos de correo electrónico: el **correo POP3,** que utiliza clientes de correo como Microsoft Outlook, Mozilla Thunderbird o Evolution de Linux Ubuntu para descargar los correos desde el servidor; y el **correo webmail,** que es visualizado a través de páginas web como Hotmail, Gmail, Mixmail o Yahoo. En ambos casos deben existir filtros de correo basura en el servidor, que se pueden completar con programas instalados en nuestro ordenador cliente.

4.8. Software antiespía

Como ya hemos visto, los programas espía se instalan camuflados en nuestro ordenador cuando descargamos desde Internet utilidades gratuitas aparentemente inofensivas. Los *spyware* recopilan información sobre nuestras costumbres de navegación, los programas instalados, etc. y a menudo tienen la capacidad de *secuestrar* nuestra página de inicio del navegador y mandarnos a una página en blanco, de publicidad... mediante un funcionamiento conocido como *hijacking*[1].



El **funcionamiento** de los programas antiespía es similar al de los antivirus, pues compara los archivos de nuestro ordenador con una base de datos de archivos espías. Por eso, también en este caso es de suma importancia.

Antiespías gratuitos

Windows 7 incorpora su propio programa antiespía llamado Windows Defender. Linux no tiene software antiespías incorporado, por tener un bajo índice de ataques, pero sí existen complementos del navegador para cerrar páginas web con *spyware*.

ANTIESPÍAS GRATUITOS			
Ad-Aware http://www.lavasoft.com	**Spybot Search & Destroy** http://www.safer-networking.org	**Malwarebytes Anti-Malware** http://www.malwarebytes.org	**IObit Malware Fighter Free** http://www.iobit.com/malware-fighter.html

Actividades

28 Define qué es un programa antivirus.

29 Explica los dos tipos de funcionamiento de un programa antivirus.

30 Define qué es un programa cortafuegos o *firewall*. ¿Para qué sirve? ¿Existe algún dispositivo físico que pueda actuar como *firewall*?

31 Enuncia los síntomas que pueden indicar la presencia de *spyware* en un ordenador.

[1] **hijacking:** significa «secuestro» en inglés y se utiliza para denominar la práctica de cambiar la página de inicio del explorador de Internet sin permiso del usuario.

5 Interconexión entre dispositivos móviles

Aunque la mayoría de los dispositivos se pueden conectar mediante cables de conectores especiales o de tipo USB, existen dos tecnologías inalámbricas en el mercado que predominan a la hora de conectar dispositivos tales como teléfonos móviles, kits de manos libres, pequeños ordenadores de mano y tabletas: se trata de las conexiones Bluetooth e IrDA (infrarrojos).

5.1. Transmisión de datos por Bluetooth

El uso más habitual de esta conexión es el envío de datos, como por ejemplo una fotografía, un tono de teléfono o un contacto de la agenda. La manera de acceder es la siguiente:

- **Paso 1.** Los dispositivos implicados deben tener activado el servicio Bluetooth. Para hacerlo debemos acudir al menú **Ajustes del dispositivo ▶ Conectividad ▶ Activar Bluetooth** en ambos dispositivos.
- **Paso 2.** Seleccionamos el archivo que queremos enviar y en el menú de opciones elegimos **Enviar por Bluetooth.** Aparecerá en la pantalla una **lista de dispositivos** detectados para seleccionar el destinatario (recuerda que el alcance actual de estos dispositivos ronda los diez metros). El dispositivo destinatario debe aceptar el envío para poder concluir la transmisión.

Proceso de envío de datos entre dispositivos móviles. FUENTE: Nokia, guías y demos (http://www.nokia.es/).

Emparejamientos de dispositivos Bluetooth

Se crea una conexión permanente entre los aparatos mediante el intercambio de sus contraseñas de acceso; de esta manera, siempre pueden intercambiar información. Esta forma de conexión es la utilizada por los sistemas *manos libres* de telefonía.

Virus por Bluetooth

En los últimos años y como consecuencia de la gran expansión de la tecnología Bluetooth, han aparecido pequeños virus, aplicaciones de control remoto y de acceso a datos de los teléfonos. Por este motivo es muy recomendable apagar la conexión bluetooth si no se está utilizando o, al menos, mantener nuestro dispositivo invisible a otros.

5.2. Transmisión de datos por infrarrojos

El mecanismo de funcionamiento es similar a Bluetooth, aunque trabaja en otro tipo de frecuencias. Se utilizan para conectar equipos que se encuentren a uno o dos metros de distancia cuyos emisores infrarrojos tengan un contacto visual con un ángulo inferior a 30° (funcionan con los mismos principios que el mando a distancia del televisor); y requieren la activación del servicio en los dispositivos.

Dispositivo de infrarrojos conectado a Jack de auriculares, con ampliación táctil, funcionando en un Smartphone.

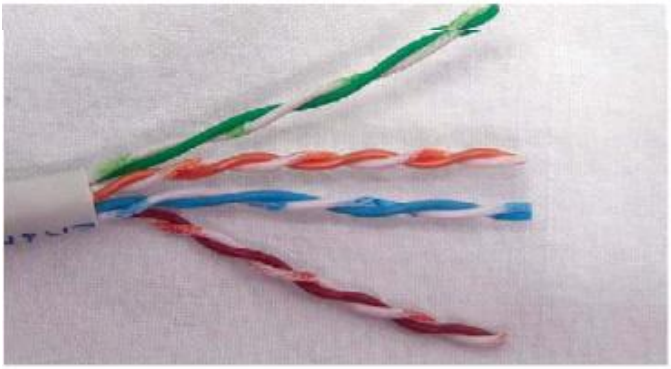
Aunque no todos los teléfonos móviles disponen de emisores infrarrojos, existen dispositivos en el mercado que se conectan a entradas USB o Jack de auriculares para convertir nuestro teléfono en un completo mando a distancia desde donde controlar todos los aparatos domésticos.

Fabricar un cable de red

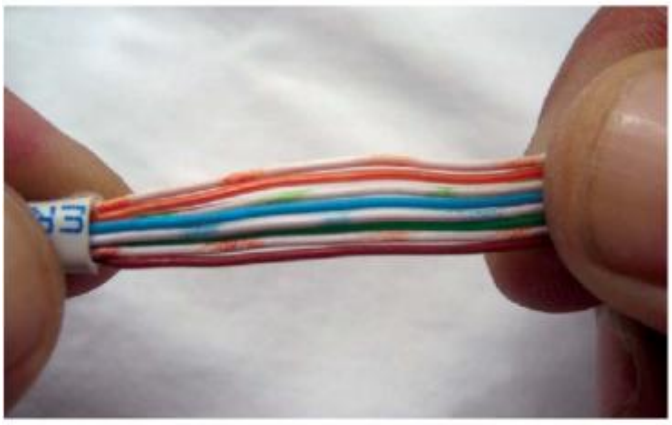
Vamos a explicar detalladamente cómo crear un cable de **red con conectores RJ45** y comprobar después su correcto funcionamiento. El cable que vamos a crear se utilizará para **conectar un ordenador a un *switch*.**

Necesitaremos cable de pares trenzados, cortado a la longitud necesaria (nunca más de 90 m), dos conectores RJ45, una crimpadora RJ45, tijeras y un *tester* RJ45.

Paso 1. Quitar la funda y el aislante exterior del cable cortando unos 3 cm.

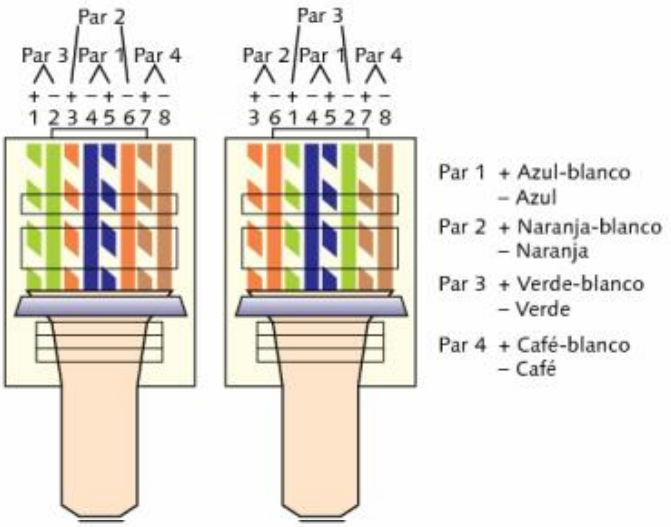


Paso 2. Desenredar los cables y colocarlos según la norma elegida.

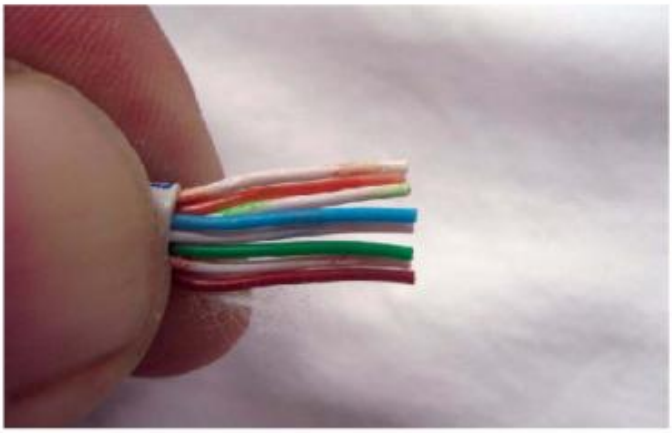


Existen dos normas diferentes de conexión de cables:

- La norma T568A.
- La norma T568B.
- Para hacer un cable paralelo (PC a *switch*) utilizaremos la misma norma en los dos extremos.
- Para hacer un cable cruzado (PC a PC) usaremos una norma distinta en cada extremo.
- En nuestro caso vamos a utilizar la norma T568B en los dos extremos.



Paso 3. Cortar los cables a 1,5 cm procurando que todos los extremos estén alineados.



No es necesario pelar los cables internos: el conector clavará los pines de conexión en el centro de cada uno de ellos con la ayuda de la crimpadora.

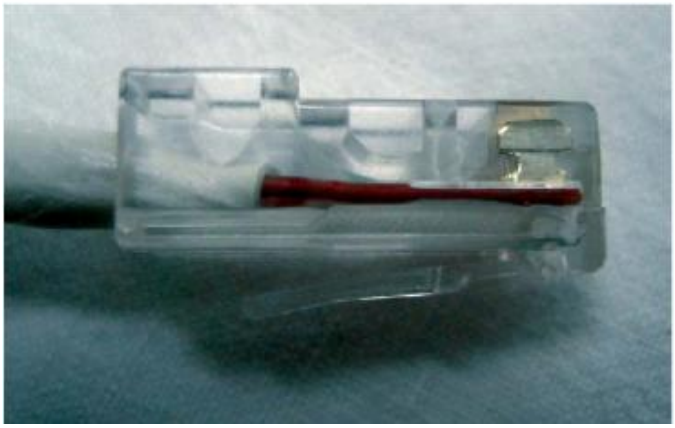
¡Advertencia!

Debemos cuidar de no perder el orden de colocación que la norma exige: una colocación errónea en el conector dejaría este inservible.

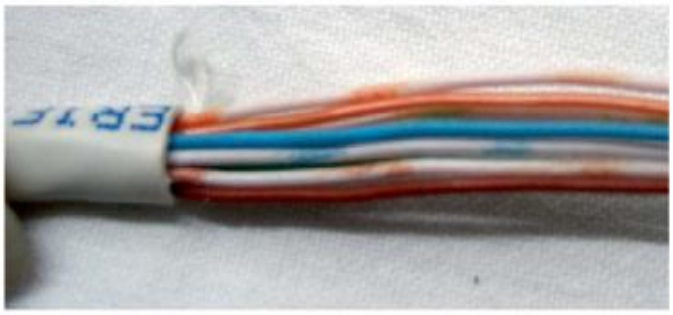
Paso 4. Introducimos los cables en el conector teniendo en cuenta que dispone de unas canalizaciones interiores que evitan que se junten los cables. Debemos coger el conector con la pestaña hacia abajo e introducir los cables por el extremo abierto.

Paso 5. Después de introducir completamente los cables y comprobar que están colocados según la norma, **introducimos en la crimpadora el conector con el cable.**

Paso 6. Apretamos con fuerza la crimpadora hasta comprobar que los pines han entrado en contacto con los cables y que el amarre de plástico del conector sujeta el cable.



Paso 7. Realizamos la misma **operación en el otro extremo del cable,** recordando que se trata de un cable paralelo y que utilizamos la norma **T568B.**



Paso 8. Ya tenemos el cable creado, pero antes de utilizarlo debemos comprobar que se **han realizado bien todos los contactos.** Nos ayudaremos de un ***tester* RJ45.** Conectamos los extremos de nuestro cable a los dos aparatos del *tester.*

Paso 9. Encendemos el *tester* y empieza a emitir una señal cable a cable siguiendo una secuencia ordenada. Si el cable se ha fabricado correctamente, el otro extremo del *tester* recibirá las señales continuando la misma secuencia.

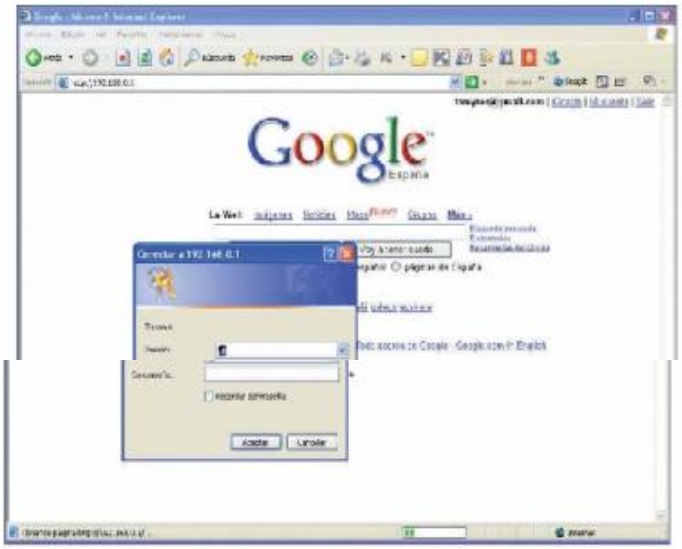
Si no se dispone de *tester* RJ45, se deben realizar las comprobaciones de continuidad *pin a pin* con un polímetro.

Configurar un *router* wifi

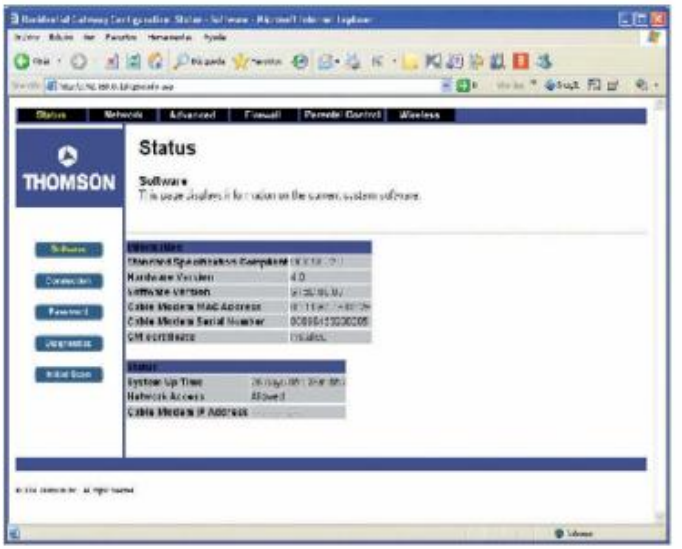
En el siguiente tutorial, aprenderemos a acceder al *router* de nuestra red para poder configurarlo correctamente cambiando sus contraseñas de fábrica, activando el servidor DHCP y estableciendo los parámetros de la red inalámbrica. Este tutorial se ha realizado con un modelo de *router* Thomson inalámbrico. Aunque el funcionamiento es similar en todos, se puede obtener información detallada de otros modelos en la página web **http://www.adslzone.net**.

Paso 1. Conectamos el ordenador al *router* mediante un cable de red y abrimos el **Explorador de Internet.** En la barra de direcciones tecleamos la **dirección IP del *router*** (puerta de enlace). En nuestro caso es 192.168.0.1.

Paso 2. Escribimos el **nombre de usuario** y la **contraseña de acceso** al *router*.

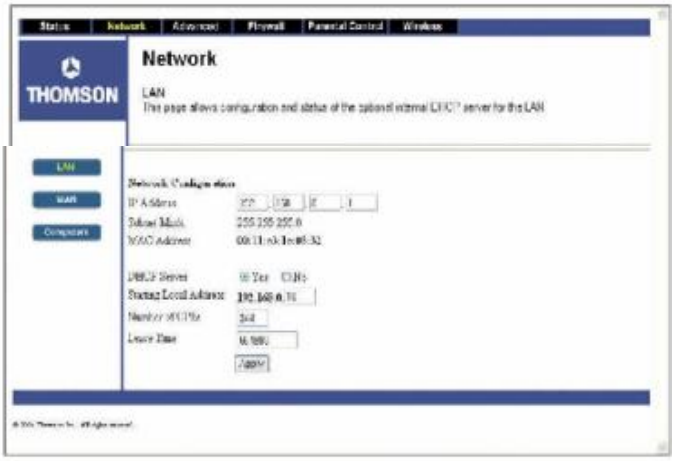


Si no lo hemos cambiado o si reseteamos el *router*, se pondrán por defecto los valores de fábrica; por ejemplo «**admin**» como usuario sin contraseña. Accedemos al menú del *router*.

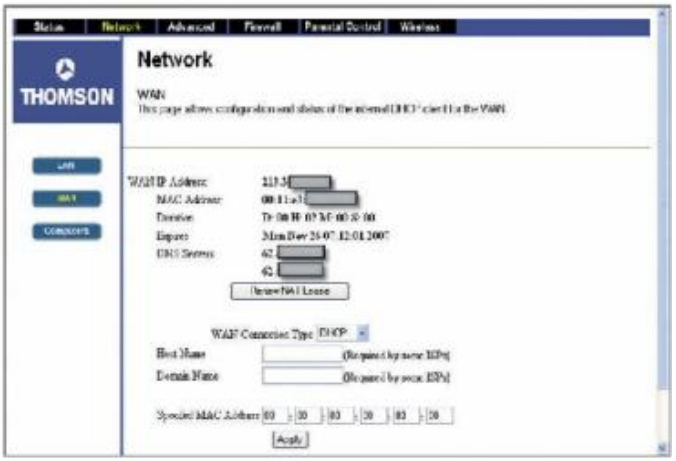


Paso 3. En los distintos menús podemos cambiar algunos parámetros. En **Status ▶ Password** cambiaremos la contraseña de acceso al *router* que acabamos de utilizar.

Paso 4. Activamos el servidor DHCP para que al acceder a **Network ▶ LAN** nos asigne automáticamente la dirección de red.



Paso 5. Comprobamos la dirección IP con la que el *router* sale a Internet y los servidores DNS que utiliza en **Network ▶ WAN.**



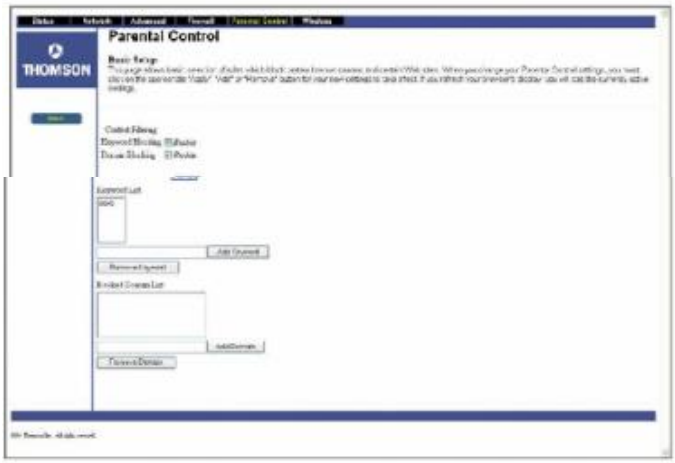
Paso 6. Configuramos los puertos del *router* para dar acceso a determinadas aplicaciones, pues, por defecto, el *router* tiene cerrados la mayoría de los puertos.

Si se desea utilizar software P2P del tipo emule, torrent, etc., se deben abrir una serie de puertos y configurarlos en dichos programas.

Esto se realiza en el menú **Advance ▶ Forwarding.**

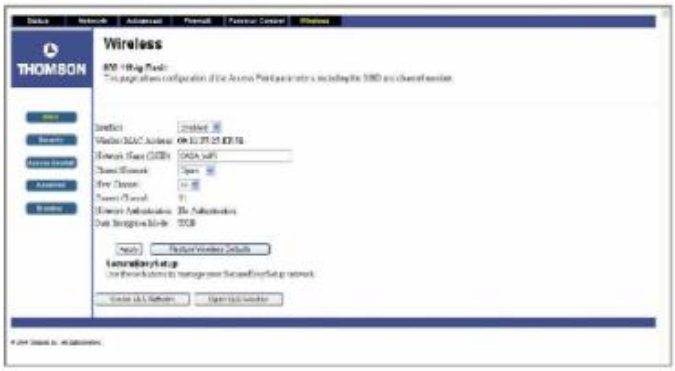
Paso 7. El control parental filtra aquellas webs que contengan palabras definidas por nosotros.

Esto se realiza en el menú **Parental Control ▶ Basic.**



Paso 8. Los **parámetros de red inalámbrica** se modifican en el menú **Wireless.**

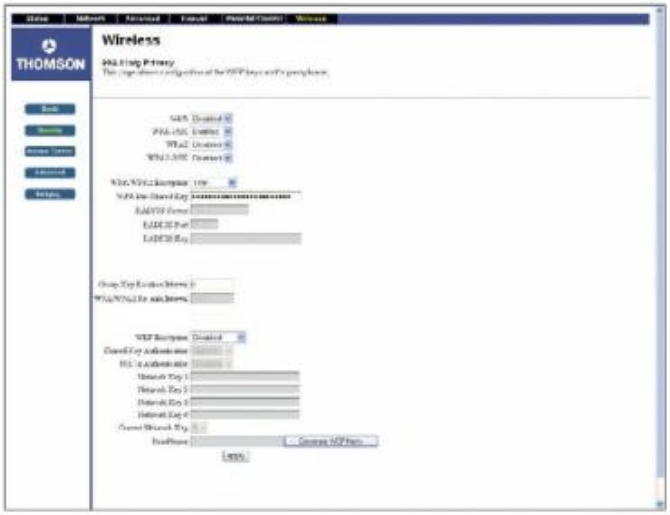
Es importante conocer el nombre de la red para poder luego conectarnos a ella.



Podemos cambiar el número de canal que utiliza si observamos muchas interferencias al conectarnos.

Paso 9. La contraseña de nuestra red inalámbrica es fundamental para evitar intrusos que puedan reducir nuestro ancho de banda.

Para **cambiar la contraseña** debemos acceder al menú **Wireless ▶ Security.**



Hoy en día la encriptación WEP de nuestra contraseña no es del todo segura, pues existen programas capaces de descifrarla.

Es recomendable utilizar encriptaciones del tipo WPA y WPA2 si nuestro *router* lo permite.

Paso 10. Puede que nuestro *router* actúe como puente o punto de acceso en una red inalámbrica con varios puntos de accesos.

En este caso, se deben **configurar las direcciones IP** de los **distintos puntos de acceso inalámbricos** que haya en la red. Esta configuración se encuentra en el menú **Wireless ▶ Bridge.**

Todos los cambios que hagamos en cada pantalla debemos confirmarlos utilizando el botón **Apply** o **Save Settings** de cada menú.