

Capacitación digital básica I

TECNOLOGÍA DIGITAL II



Tecnología digital II

ICONOS



VER TAMBIÉN



VER EJEMPLO



CONTENIDO COMPLEMENTARIO



PARA SABER MÁS



ACTITUD DIGITAL



ACTIVIDAD



SOLUCIÓN

Presentación	4
Sistemas operativos.....	5
Evolución.....	5
Linux.....	8
Actualizaciones	10
Programas alternativos	13
Actividades	14
Mantenimiento y configuración avanzada del sistema.....	15
Causas y soluciones al bloqueo de Windows	15
Particiones y formato de disco	18
Liberar espacio en disco	20
Desfragmentación del disco duro.....	21
Buscar y reparar errores en el disco duro	23
Restauración del sistema	24
Limpieza del registro	26
Tareas programadas	28
Actividades	30
Montar y configurar una red doméstica	31
Redes locales y tipos de comunicación	31
Conexión y configuración de redes	33
Aplicaciones para conocer los elementos de una red.....	41
Actividades	45
Seguridad en las comunicaciones.....	46
Principios.....	46
Criptografía y otras técnicas de ocultación	47
Certificados digitales y firma electrónica	50
Las transacciones comerciales	52
Seguridad en comunicaciones inalámbricas	53
Actividades	58
Práctica final	59
Ideas clave	61
Soluciones actividades.....	62
Glosario	64

Tecnología digital II

PRESENTACIÓN

En este módulo ampliaremos los conocimientos del sistema operativo Windows para poder llegar a hacer una configuración y un mantenimiento avanzado de todo el sistema.

Empezaremos en el tema 1 con una aproximación a la evolución de los **sistemas operativos** de ordenadores personales, en concreto de las distintas versiones de Windows, llegando a conocer otros sistemas operativos, como **Linux**, con una filosofía de uso distinta a la del sistema operativo Windows de Microsoft. En este tema, también detallaremos las posibilidades de **ayuda y actualización** que nos ofrece el sistema operativo Windows, y que, en diversas situaciones, nos pueden llegar a ser de gran utilidad. Además, veremos que existen algunas aplicaciones que son **programas alternativos** a los que nos ofrece Windows XP.

En el tema 2, conoceremos algunos conceptos (**particiones, formato de discos...**) y algunas aplicaciones que nos facilitan el mantenimiento del ordenador. Entre ellas, la **comprobación de errores en los discos, la desfragmentación, la limpieza de discos, la restauración del sistema, la limpieza del registro...**

En el ámbito de las redes domésticas, en el tema 3, detallaremos los elementos necesarios para **montar y configurar una red local**. Profundizaremos en los protocolos más comunes que utilizan las redes y en las pequeñas aplicaciones que nos facilita el sistema operativo para trabajar con redes (ping, netstat, ipconfig...). Al final del tema, se detallan algunas aplicaciones, utilizadas por administradores de redes, que nos permiten conocer elementos existentes en una red (en un ámbito doméstico, o bien en un ámbito más amplio).

En cuanto al tema de seguridad, en el tema 4 de este módulo, trataremos algunos aspectos avanzados de seguridad informática, presentando algunos conceptos imprescindibles sobre **seguridad en las comunicaciones**. En concreto veremos: una introducción a la **criptografía** y otras técnicas de ocultación de la información, mostrando sus aplicaciones en los **certificados y firmas digitales**; las técnicas de seguridad utilizadas en las **transacciones comerciales por Internet**, y la **seguridad en comunicaciones inalámbricas**, detallando las medidas concretas de seguridad que se pueden adoptar en este ámbito.

Un sistema operativo es un conjunto de programas que actúa como interfaz entre el usuario del ordenador y su hardware (CPU, memoria, dispositivos de entrada y salida...), facilitando, entre otras cosas, la introducción de datos en el ordenador, la gestión de ficheros y la gestión de la comunicación entre el equipo y el usuario mediante los periféricos (ratón, teclado, pantalla...).

En definitiva, su objetivo es facilitar el uso del sistema informático, garantizando que sus recursos se utilizan de forma eficiente.

En este tema, trataremos los siguientes subtemas:

- **La evolución de los diferentes sistemas operativos de ordenadores personales.**
- **Otros sistemas operativos: LINUX.**
- **Actualizaciones del sistema operativo.**
- **Programas alternativos a los propios de Windows XP.**

Al final del tema, encontrarás una actividad para desarrollar que te permitirá conocer si has asimilado los conceptos trabajados en él mismo.

Evolución

Los sistemas operativos son un elemento clave para entender la propia evolución de los ordenadores. La evolución de los sistemas operativos ha ido ligada a la evolución de los ordenadores personales: más capacidad del microprocesador, mayor memoria RAM... Los sistemas operativos y los ordenadores han ido evolucionando de forma paralela. Buena muestra de ello, la tenemos en que un sistema operativo de última generación no podría ni empezar a funcionar en un ordenador antiguo.

La primera generación de sistemas operativos es de los años cincuenta, ya que en los años cuarenta los primeros ordenadores no disponían de sistema operativo y eran los programadores los que interactuaban, directamente, con su hardware.

Hacia los años ochenta, ya en una **cuarta generación**, con la expansión de los ordenadores personales (a raíz de la evolución de los circuitos integrados), los sistemas operativos se centran más en llegar a ofrecer una **interfaz más amigable**, lo que permite que la interacción entre el usuario y el ordenador se haga de forma más sencilla.

Además, con la aparición de las redes, y sobre todo de Internet, hace que los sistemas operativos se orienten para satisfacer estas nuevas necesidades de trabajo. En esta época, los sistemas operativos más utilizados eran **MS-DOS** en los IBM y **UNIX** en los ordenadores Motorola.

Ya, en 1984, aparece el sistema operativo **Apple** de Macintosh, extendiéndose, rápidamente, en el ámbito del diseño gráfico.

Microsoft se crea en 1975 por Bill Gates y Paul Allen. En 1985, aparece la primera versión de Windows (**Windows 1.0**), de entorno gráfico –**GUI**, interfaces gráficas de usuario-, basado en “ventanas”, iconos... Era muy similar a **Mac OS** de Apple.

En estas primeras versiones, el entorno gráfico se ejecuta encima de MS-DOS (también propiedad de Microsoft). Microsoft, a lo largo de los años, ha ido lanzando al mercado distintas versiones de su sistema operativo Windows.

Por divergencias de tipo comercial, IBM y Microsoft dejan de colaborar, de modo que aparece **OS/2 de IBM** y, al poco tiempo, Microsoft comercializa Windows 3.1, con funciones multimedia.

Será con la versión **Windows 3.1** que se populariza este sistema operativo. De esta versión destacaremos su capacidad multitarea, su capacidad de ejecutar al mismo tiempo algunas aplicaciones basadas en MS-DOS. De este modo, IBM PC se convierte en un serio competidor para Apple Macintosh.

Desde la versión inicial, Windows avanza en nuevas versiones, como primer paso hasta llegar a **Windows 3.11** (denominada *Windows for Workgroups*), la primera versión con capacidades reales de trabajo en red.

A finales de los ochenta, Windows empieza a comercializar **Windows NT**, de la que irá lanzando al mercado distintas versiones (Windows NT Server –Windows NT 3.5- en 1994, Windows NT 4.0). De este sistema operativo, destacaremos que permite tener instalados más de un protocolo dentro de una misma red. También merece destacar la gran cantidad de recursos (sólo disponibles en equipos más grandes) que precisaba, lo que hizo que no se extendiera entre los usuarios. Además, presentaba algunos errores en su implementación, con una configuración y mantenimiento complicados.

Con **Windows 95** se llega a una mejorada interfaz gráfica, con las mismas posibilidades del entorno Windows NT. Una de sus primeras ventajas es poder conectar un dispositivo, o incluso una tarjeta, y que el sistema operativo lo reconozca (**Plug and Play**). También se incrementaba el abanico de aplicaciones incorporadas en el mismo sistema operativo. Su interfaz gráfica fue diseñada para competir con OS/2 de IBM. Con éste, un usuario poco experimentado podía manejar, correctamente, el ordenador.



Desde este S.O., Windows ha sido el sistema operativo más utilizado y popular.

1998	Aparece Windows 98 , con soporte a las emergentes tecnologías que van apareciendo en esos años: navegador remodelado, DVD, <i>firewire</i> , USB.. Su versión más estable aparece en 1999 y se denomina Windows 98 second edition .
2000	Aparece Windows Millenium con aplicaciones añadidas a la versión anterior. Su funcionamiento no fue nada óptimo, sobre todo en equipos más antiguos. En ese mismo año aparece Windows 2000 , una evolución de Windows NT. Sistema de gran utilidad para administradores de redes. De esta versión, existen distintas opciones: para las estaciones de trabajo (<i>professional</i>) o para servidores (<i>server</i>).
2001	Con Windows XP se alcanza el punto de confluencia entre los sistemas operativos más específicos de redes, como Windows NT o Windows 2000, y los más dirigidos a usuarios, como Windows 9.x. Su núcleo es el de Windows NT. Dispone de dos versiones, la Home y la Professional . También existe una versión Media Center para ofrecer una interfaz a dispositivos multimedia. Con éste, se incrementan las prestaciones multimedia, se mejora la multitarea, se da soporte a redes inalámbricas...
2007	Aparece Windows Vista , tras algunos retrasos en su comercialización.

Al arrancar el sistema operativo, en concreto Windows XP, disponemos de una aplicación que nos permite hacer un recorrido por sus funcionalidades, desde las más básicas hasta otras más avanzadas. La podemos encontrar en **Inicio/ Todos los programas /Accesorios**, y se denomina: **Paseo por Windows XP**. Es muy recomendable ejecutarla para poder conocer más a fondo el sistema operativo.



Menú Inicio

El menú Inicio apareció automáticamente la primera vez que ejecutó Windows XP. Puede volver al menú Inicio en cualquier momento si hace clic en el botón **Inicio** de la barra de tareas.

El menú Inicio contiene todo lo que necesita para empezar a utilizar Windows. Aquí puede:

- Iniciar programas
- Abrir archivos

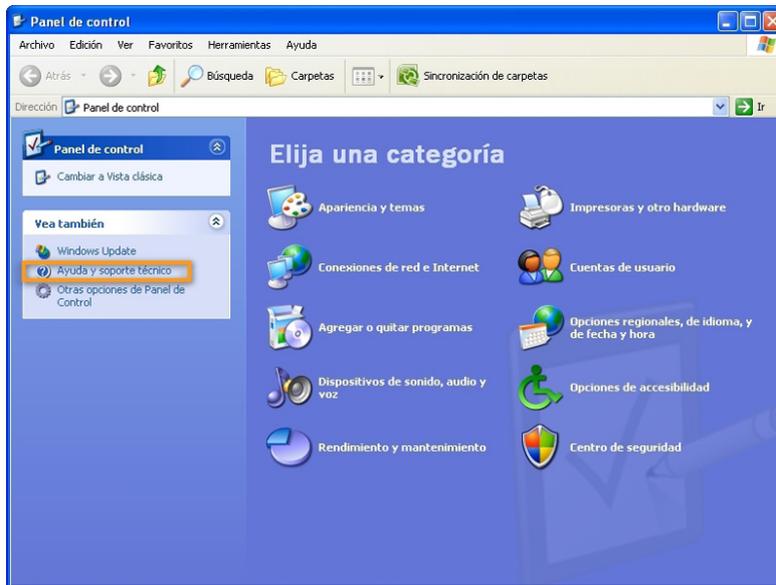
Paseo por Windows XP



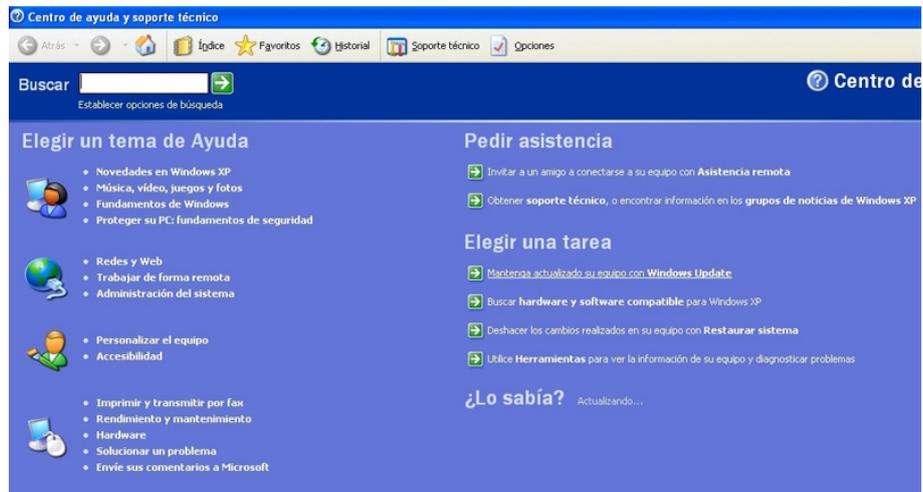
ver simulación

Simulación disponible en la versión web del material

Además, en **Inicio/Panel de control**, encontraremos **Ayuda y soporte técnico** del sistema operativo.



Al hacer clic sobre esta opción, dispondremos de una ayuda en relación al sistema operativo que nos puede ser muy útil:



Las ayudas están clasificadas por temas y por tareas, pero también disponemos de un buscador interno por palabras clave.

Linux

Los sistemas operativos más populares en el mercado de ordenadores pertenecen a la familia Windows de Microsoft: desde Windows 3.1, Windows 95/98/Me y Windows NT/Windows 2000, hasta llegar a Windows XP y Windows Vista.

Pero, ya desde mediados de los años noventa, se hace muy popular el **sistema operativo Linux**, como variante del sistema operativo UNIX (utilizado por

muchos servidores desde los años setenta). Este sistema operativo, gratuito, se ha ido desarrollando por miles de programadores, presentando muchos tipos de distribuciones concretas, como: Red Hat, Suse, Ubuntu...



Hacia los años ochenta, las empresas de informática van creando su propio software con licencias de uso y distribución cada vez más restrictivas, como por ejemplo: patentes sobre los códigos que están en la base de los programas que desarrollan.

Es en este contexto que el físico Richard M. Stallman, por no querer firmar unos acuerdos de confidencialidad con el MIT (Massachusetts Institute of Technology) en el que trabajaba, crea la organización Free Software Foundation (FSF). Esta organización se propone crear un sistema operativo utilizando sólo software libre, partiendo del núcleo del sistema operativo comercial UNIX. A este proyecto, se le da el nombre de GNU (**GNU is Not Unix**). La FSF desarrolla la licencia **GPL** (siglas de **GNU Public License**).

Concretando con Linux, la historia de este sistema operativo va ligada a la de un estudiante de Informática finlandés llamado **Linus Torvalds**. Mientras cursaba la asignatura de sistemas operativos y, en concreto, analizaba el sistema operativo Minix diseñado por Andrew S. Tanenbaum, decidió crear **su propio núcleo de sistema operativo**, que denominó **Linux**, y que empezó a distribuir por Internet con licencia GPL. A partir de aquí, miles de programadores empezaron a implementar mejoras y ampliaciones, basadas también en desarrollos efectuados por el grupo del proyecto GNU, y es en el año **1994** que aparece la primera versión de Linux, un sistema operativo libre y funcional.

En la actualidad existen muchos tipos de **distribuciones Linux**, también denominadas **GNU/Linux**, muchas de ellas con software adicional con licencia de software libre y código abierto. Entre éstas destacaremos: **Debian, Suse, Red Hat, Knoppix, Mandrake, Slackware i Gentoo**. Incluso existen distribuciones derivadas, como **Ubuntu**, que es una distribución basada en Debian; **Fedora**, en Red Hat; **Kororaa**, en Gentoo....

GPL

Esta licencia es la base del software libre. Puedes consultarla en:

<http://www.gnu.org>

En la base de esta licencia está el hecho de que quien lo desee puede mejorar el código de estos programas siempre que, con posterioridad, se difunda nuevamente con esta licencia.

Distribución LINUX

Para tener más detalles sobre las distribuciones, podemos consultar la dirección:

http://es.wikipedia.org/wiki/Anexo:Distribuciones_GNU/Linux

Aunque la mayoría de distribuciones ya incorporan el software necesario (escritorio -Gnome, KDE,...-, navegador, clientes de mensajería, aplicaciones para tratar la información textual, numérica, imágenes, audio, video...), en esta página podemos encontrar detalles de este software para GNU/Linux:

<http://es.wikipedia.org/wiki/Portal:Linux/Software>

En un mismo ordenador, con las particiones del disco duro adecuadas –o en discos diferentes-, podemos tener instalados dos sistemas operativos. Es el que se denomina **instalación dual**. El usuario, al poner en marcha el ordenador, escogerá con qué sistema operativo quiere arrancar el ordenador.

Además de las distribuciones instalables, también tenemos algunas distribuciones denominadas **Live-CD**, que se pueden ejecutar, directamente, desde un CD. Al ejecutar la aplicación desde el CD, en esta sesión podremos trabajar con un entorno Linux.

En los últimos años, tanto la industria como las administraciones públicas están dando un buen impulso al desarrollo y posterior uso de distribuciones propias, de forma que se adapten a sus necesidades.

Actualizaciones

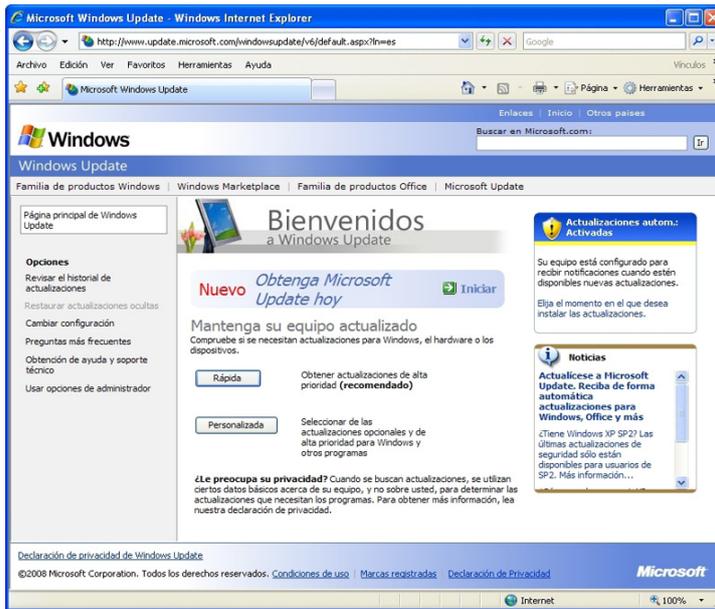
Es habitual que, cuando aparece un nuevo sistema operativo, aunque éste incorpore los últimos avances tecnológicos y haya sido suficientemente testado, se le encuentren posibilidades de mejora.

Para que el sistema operativo pueda dar respuesta a estas novedades que aparezcan (de seguridad –por ejemplo, para hacer frente a nuevos virus que puedan aparecer-, de soporte a nuevos dispositivos –por ejemplo, nuevos controladores...), son necesarias las denominadas actualizaciones (o *updates*). Cada cierto tiempo, dichas actualizaciones se agrupan en los denominados **service pack**, que permiten la instalación directa de todo un grupo de actualizaciones.

Siempre es recomendable que el sistema operativo incorpore las actualizaciones (sobre todo, las relacionadas con la seguridad) que hayan aparecido desde su adquisición.

Para conocer las actualizaciones que nos faltan en nuestro sistema operativo Windows, podemos acceder (con el navegador Internet Explorer) al enlace que encontraremos en el **Panel de control** denominado **Windows Update**.





Si hace tiempo que no se ha actualizado la copia de Windows, se nos solicitará renovar la herramienta **Windows Update**.

Windows XP también se actualiza y necesita ser actualizado. Veamos cómo podemos actualizar el sistema operativo.

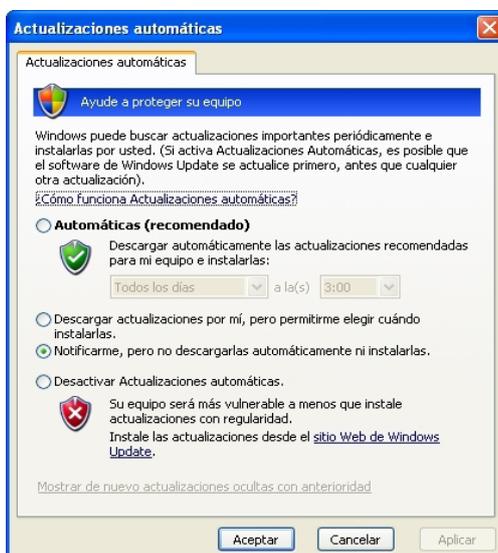
En el **Panel de control** encontraremos la aplicación de **Actualizaciones automáticas**.

Desde la vista clásica del Panel de control, la encontraremos **directamente en la lista de aplicaciones**.

Desde la **vista por categorías**, deberemos ir a **Centro de seguridad**, donde encontraremos un enlace a la aplicación:

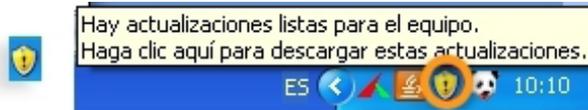


Para poder utilizar esta aplicación, es necesario disponer de conexión a Internet.

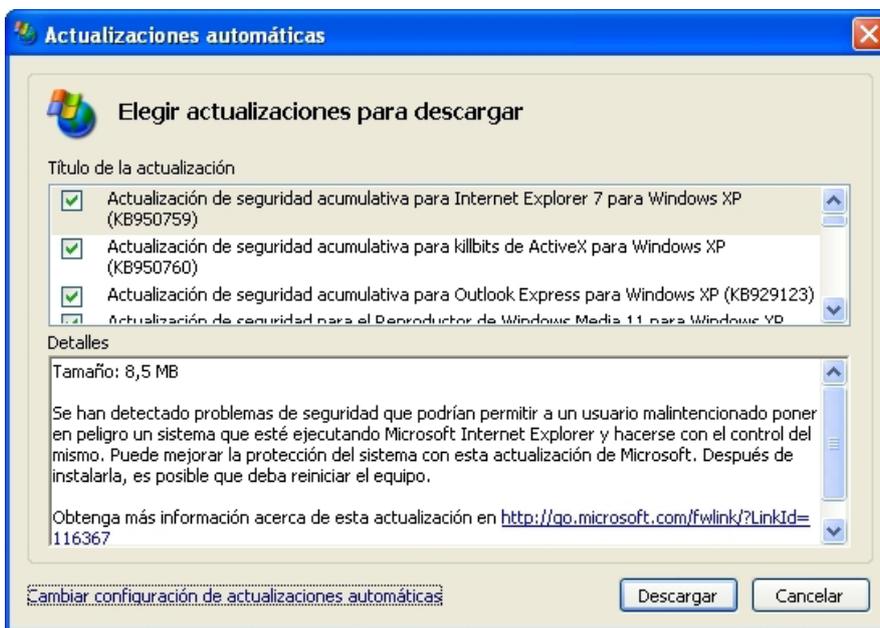


Al abrir la aplicación, podremos configurar cuándo y cómo deseamos que se lleven a cabo las actualizaciones.

En el caso de tener configuradas algunas de las opciones de “**notificar o descargar**” la instalación de las actualizaciones, en la barra de tareas de la parte inferior del escritorio veremos el siguiente icono.



Al hacer doble clic sobre este icono, nos aparecerá una ventana desde la que podremos escoger las **actualizaciones** pendientes de descargar.



Actualizaciones pendientes

Además, tenemos la posibilidad de acceder a la ventana comentada anteriormente para **Cambiar la configuración de las actualizaciones automáticas**.

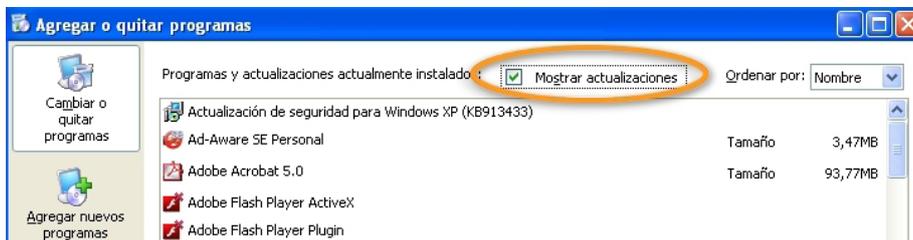
Esta ventana puede ser distinta si no tenemos seleccionada la opción **Notificarme pero no descargarlas automáticamente ni instalarlas** de la ventana de configuración de las actualizaciones automáticas.

Si procedemos a descargar estas actualizaciones, en el proceso se nos puede solicitar que aceptemos las condiciones de la licencia (tenemos en cuenta que Windows es un programa comercial).

Cuando haya finalizado la instalación de las actualizaciones, se nos indicará que es necesario reiniciar el sistema. Una vez hayamos aceptado, el sistema operativo lo efectuará de forma automática.

En el caso de que deseemos **desinstalar alguna de las actualizaciones que hayamos instalado**, podemos hacerlo desde: **Inicio / Panel de control / Agregar o quitar programas**, y desde esta ventana activar la opción de

Mostrar actualizaciones. Entre la lista de programas instalados, nos aparecerá la actualización que deseemos desinstalar. Nos puede ser útil si detectamos que, al instalarse alguna actualización, el sistema no se comporta como deseáramos.



Actualizaciones por desinstalar



Recomendación

Antes de activar alguna de las actualizaciones, deberíamos documentarnos de los posibles problemas que podamos encontrar al instalarla.

Configurar actualizaciones



ver simulación

Simulación disponible en la versión web del material

Programas alternativos

Existen programas alternativos a los que ya incorpora el sistema operativo Windows XP, que es interesante que conozcamos.

Softonic
www.softonic.com

En la web de **Softonic** podemos encontrar muchos programas de este tipo.

En este subtema nos centraremos en dos aplicaciones gratuitas para usos no comerciales.

■ EditPad Lite

Equivaldría al **Bloc de Notas de Windows**, con algunas funcionalidades adicionales, que soporta múltiples ficheros.

Entre otras prestaciones, permite abrir múltiples documentos en una única ventana, y guardar los cambios de todos ellos con un único clic.



■ Xplorer2

Dispone de una versión *freeware* denominada **Xplorer 2 Lite**.

Es un administrador de archivos, del tipo **Explorador de Windows**, que incorpora el sistema operativo. Incluye funciones adicionales como: previsualización de ficheros seleccionados, edición directa de determinados tipos de documentos, potente motor de búsqueda dentro del equipo, localización y eliminación de archivos repetidos... Con una interfaz adaptable

a las necesidades del usuario, con la posibilidad de establecer configuraciones diferentes para cada carpeta.



Actividades

Indica si los siguientes enunciados son verdaderos o falsos.

	V	F
La versión Windows 95 elevó el nivel de popularidad del sistema operativo Windows.		
Windows XP integra prestaciones de Windows NT con las de las versiones de Windows 9.x		
Linux , al igual que Windows XP, es un sistema operativo.		
Existen muchas distribuciones de Linux, entre ellas: Red Hat, Debian, Suse...		
Un Live-CD con Linux nos permite efectuar una copia de seguridad.		
En Inicio/Panel de control , encontraremos Ayuda y soporte técnico sobre el sistema operativo.		
Los denominados Service Pack permiten la instalación directa de todo un grupo de actualizaciones para el sistema operativo.		
Si escogemos una configuración para las actualizaciones automáticas, ya no la podremos cambiar.		
Antes de activar alguna de las actualizaciones, es recomendable que nos documentemos de los posibles problemas que podamos encontrarnos al instalarla.		
Existen programas alternativos a los que ya incorpora el sistema operativo Windows XP, que podemos tener también instalados en nuestro equipo.		

Tecnología digital II

MANTENIMIENTO Y CONFIGURACIÓN AVANZADA DEL SISTEMA

Es evidente que los ordenadores no dejan de ser máquinas, con una interfaz (el sistema operativo) que nos permite trabajar con ellos. Por lo tanto, disfunciones en el hardware, o en el sistema operativo, pueden hacer que nuestro equipo no nos funcione como debería.

Por esta razón, es muy importante ir haciendo un buen mantenimiento de nuestro equipo, conociendo algunas herramientas que denominaremos de configuración avanzada del sistema.

En este tema, trataremos los siguientes subtemas:

- ¿Qué hacer cuando el sistema operativo Windows se bloquea? Causas y posibles soluciones.
- Particiones y formato de discos.
- Liberar espacio en el disco.
- Desfragmentación del disco duro.
- Buscar y reparar errores en el disco duro.
- La herramienta de restauración del sistema: puntos de restauración.
- Limpieza del registro.
- Tareas programadas.

Al final del tema, encontrarás una actividad para desarrollar que te permitirá conocer si has asimilado los conceptos trabajados en él mismo.

Causas y soluciones al bloqueo de Windows

Es muy probable que, al trabajar con nuestro equipo, alguna vez se haya bloqueado (se haya “colgado”) el sistema operativo Windows, de manera que se detiene y nada funciona (ni el teclado ni el ratón).

Además, es muy posible que la causa no esté en un mal funcionamiento del hardware, sino que “algo” del sistema operativo no está funcionando correctamente. La mejor manera de afrontar la situación es con mucha calma, ya que hay distintas opciones para afrontar la situación.

En primer lugar, deberemos desbloquearlo y volver a iniciar el sistema operativo. Para hacerlo, deberemos pulsar de forma simultánea las teclas: **Control-Alt-Supr.**

En el caso de que no funcione, deberemos mantener pulsado el botón de encendido del ordenador hasta que se apague. Posiblemente, así el sistema se podrá reiniciar correctamente.

De no ser así, deberemos ir descartando elementos que puedan funcionar mal.

En el caso de que Windows siga sin abrirse, podremos plantearnos la posibilidad de que no funcione bien a raíz de alguna disfunción de algún controlador de un dispositivo.

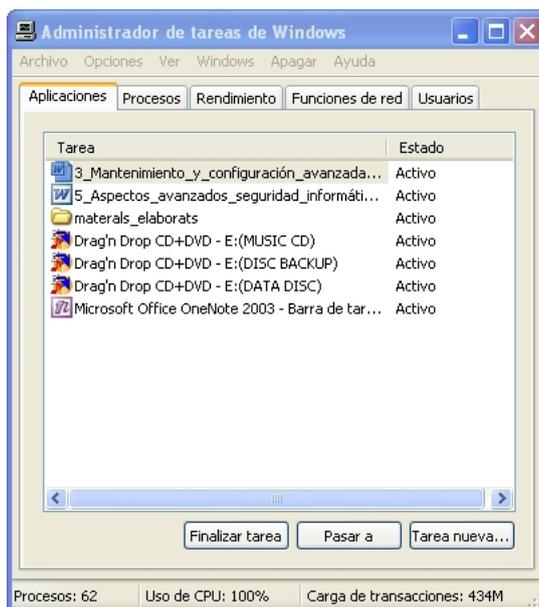
Si intuimos que ésta es la situación, podemos **abrir Windows en modo seguro**.

Para hacerlo, haremos clic en la tecla **F8** antes de que se inicie Windows. De este modo, llegaremos a un menú en el que seleccionaremos **modo seguro**. A continuación, se nos abrirá Windows con una configuración muy simple (sin muchos de los controladores), pero que nos permitirá restablecer la situación mediante las **herramientas de restauración del sistema** que trataremos dentro de este tema.

Pero, a veces, puede bloquearse con alguna aplicación concreta. Entonces, nos podemos plantear de cerrar la aplicación que nos está dando problemas para que, así, el resto de aplicaciones y el sistema puedan seguir funcionando.

Par ver qué aplicaciones se están ejecutando, iremos al **Administrador de tareas del Windows**.

Para acceder a éste, teclearemos de forma simultánea.



Dentro de la pestaña aplicaciones, podemos ver las que se están ejecutando, y si hay alguna que esté bloqueada. Si éste es el caso, seleccionándola podremos hacer clic al botón **Finalizar tarea**, para cerrar esta aplicación bloqueada. De este modo, podremos seguir trabajando en Windows.



Un bloqueo reiterado de varias aplicaciones puede ser un síntoma de memoria RAM insuficiente. Añadiendo más memoria RAM al sistema se podría solucionar.

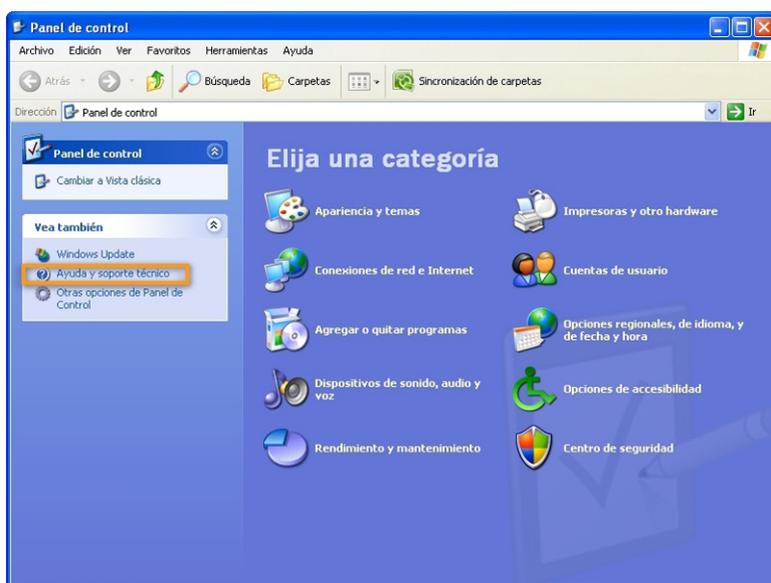
Herramientas de solución de problemas de Windows

El sistema operativo Windows incluye algunas herramientas que nos pueden ayudar a diagnosticar y llegar a solucionar algunos problemas que podamos detectar en nuestro sistema.

El primero que presentaremos será el **Solucionador de Problemas**. Lo podemos encontrar en **Inicio/Ayuda y soporte técnico**.

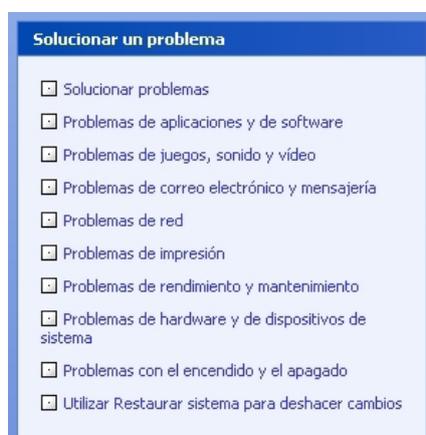


Haremos clic en el enlace **Solucionar un problema**.



Al hacerlo, se nos abrirá un asistente que nos guiará en el procedimiento para llegar a solucionar un problema concreto que planteemos. Este asistente nos conducirá a la solución más probable del problema.

Por defecto, nos aparecerá una lista, **con distintos niveles, donde figurarán los problemas más frecuentes**.



Lista de problemas frecuentes

Haciendo clic en alguno de ellos, seguiremos con el asistente, hasta llegar a esta solución.

Particiones y formato de disco

Una **partición de disco** es una técnica que nos permite dividir un disco en distintas partes. El sistema tratará cada una de estas partes como independientes. Normalmente, las particiones se efectúan en el disco duro del equipo.

Ej.

En el caso de disponer de un disco duro de 500 GB, podríamos dividirlo en dos: una partición C: de 200 GB, en la que iríamos instalando los programas, y otra partición D: de 300 GB para datos (documentos, fotos, vídeos...).

Cada una de estas particiones tendrá su propio formato, y, aunque tengamos un único disco duro de forma física, en realidad, veremos dos unidades independientes (la C: y la D:). Si deseamos tener dos sistemas operativos en un mismo equipo, antes deberemos dividir el disco, a no ser que tengamos dos discos físicos independientes.

En el caso de que no tengamos el disco dividido (sea un disco duro u otra unidad de almacenamiento), de hecho tendremos el disco con una única partición que ocupa todo el disco. En esta situación, hablaremos de formato del disco.

Existen distintos tipos de particiones:

■ Partición primaria

Corresponde a una sencilla división del disco en partes. Si tenemos un disco físico formateado, de hecho tendremos una partición primaria que ocupa todo el espacio del disco. Un disco sólo puede tener 4 particiones primarias.

■ Partición extendida

Actúan como particiones primarias, lo que permite que pueda haber más de 4 particiones de las consideradas primarias. De este tipo, sólo puede haber una en un disco.

■ Partición lógica

Son las partes en las que podemos dividir la partición extendida. Se podrá formatear y asignarle una unidad concreta (E:, F., ...).

Cuando hablamos de **formato de un disco**, realmente estamos hablando de cómo están organizados los datos dentro del disco, de sus sistema de archivos. Antes de poder usar un disco (disco duro, CD, USB...) para guardar información, éste deberá ser formateado. En muchos casos, este formateo ya lo ha realizado previamente el fabricante.

Al formatear un disco o una partición, estamos implantando un sistema de archivos que asigna algunas partes del disco (denominado sectores) a archivos.



Tipos de formato

Hay dos tipos de formato (el físico y el lógico). De todos modos, cuando, como usuarios, hablamos de formato de un disco, lo estamos haciendo del formato lógico. Del formato físico ya se ha encargado el fabricante.

Antes de efectuar un formateo lógico del disco, deberemos dividirlo en particiones, de forma que, posteriormente, se podrá formatear cada partición por separado. Si ya dispone de una partición primaria, e inicialmente no queremos otras, ya podremos formatearlo.

Cada sistema operativo tiene unos sistemas de archivos más habituales (son distintos tipos de formatos), en concreto, en Windows son: **FAT** (16 ó 32) o **NTFS**. En otros sistemas operativos hay otros tipos, como, por ejemplo: ext2, ext4, JFS en Linux.

Para comprobar qué sistema de archivos está utilizando nuestro disco duro, podemos ir a Mi PC, seleccionar la unidad de disco que corresponda y, haciendo clic con el botón derecho del ratón, acceder al menú contextual, en concreto a la opción Propiedades. En esta ventana, entre otros datos (espacio utilizado, espacio libre en el disco...), nos aparecerá el sistema de archivos utilizado:



Es importante señalar que, **al realizar un formateo completo de una unidad, estaremos borrando toda la información anterior** (incluyendo posibles virus). Por lo tanto, normalmente el formateo de un disco que estemos utilizando se efectúa en casos extremos en los que queramos empezar de nuevo con el disco y su contenido, por ejemplo volviendo a reinstalar el sistema operativo.

Formatear un disco

Sólo deberemos seleccionar su unidad, y con el botón derecho del ratón se nos abrirá el menú contextual que nos permitirá formatearlo.

En este caso, iríamos a formatear la unidad D:



Cambiar las particiones de un disco

Para cambiar las particiones de un disco, deberemos recurrir, por ejemplo, a un programa comercial como **PartitionMagic**.

PartitionMagic

Para Windows XP puedes descargarlo en:

<http://www.symantec.com/es/es/norton/partitionmagic>

Origen del PartitionMagic

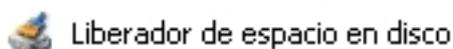


Originalmente, fue creado por *PowerQuest Corporation*, pero en la actualidad es de la empresa *Symantec* (<http://www.symantec.com/es/es/index.jsp>), que también comercializa el antivirus y entorno de seguridad Norton, el programa de copias de seguridad Ghost, entre otros productos.

Este programa nos permitirá cambiar las particiones del disco, creando nuevas o redimensionando las existentes. Aunque puede efectuarlas sin perder la configuración del sistema ni los archivos que tengamos, sí que es conveniente hacer, antes, una copia de seguridad del sistema. Así, en el caso de que a lo largo del proceso ocurra algún problema, podremos restablecer la situación anterior.

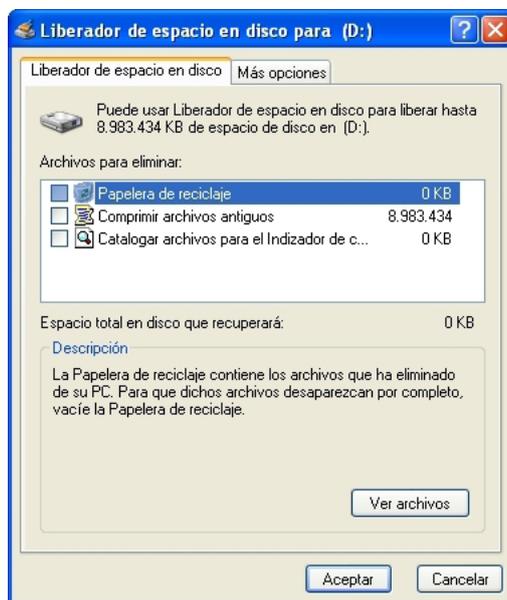
Liberar espacio en disco

Con el tiempo, con el trabajo diario con nuestro ordenador, se van acumulando archivos temporales en el disco duro que ya no se necesitan. Estos archivos quitan espacio al disco duro. Para eliminarlos, debemos utilizar la aplicación **Liberador de espacio en disco**.



Accederás a ésta en **Inicio / Todos los programas /Accesorios / Herramientas del sistema**.

Al ejecutarlo, primero solicita la unidad de la que queremos liberar espacio. Posteriormente, detectará qué espacio puede llegar a liberar y se abrirá un cuadro de diálogo que permite eliminar los archivos temporales de distintas categorías.



En este caso, hemos escogido la unidad de disco D:, y nos presenta lo que podemos liberar. Siempre podremos escoger lo que queramos liberar, además, si queremos más información sobre una categoría, podemos seleccionarla y hacer clic en la opción **Ver archivos**.

Una vez aceptado que se ejecute el proceso, veremos cómo evoluciona el borrado de estos archivos, quedando nuestro sistema limpio de archivos temporales.

Scandisk

 **Simulación disponible en la versión web del material**

[ver simulación](#)

Desfragmentación del disco duro

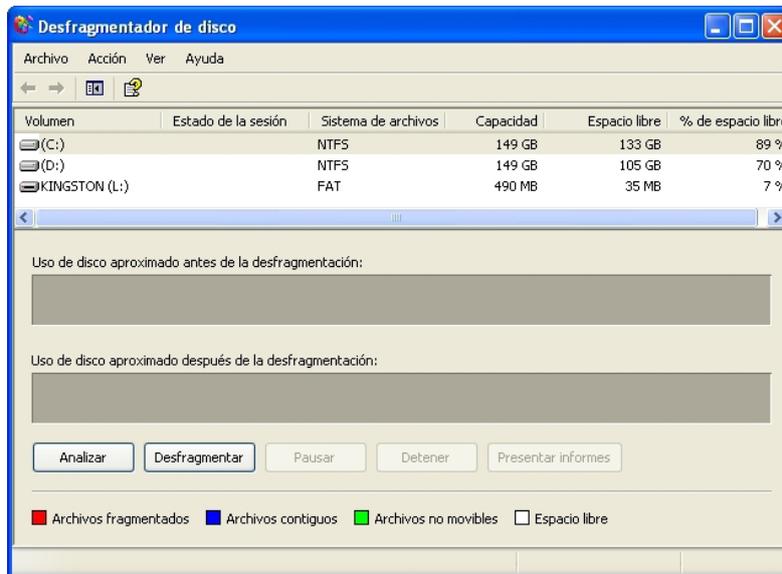
Ésta debería ser una actividad habitual para mantener en estado óptimo nuestro sistema.

La desfragmentación consiste en que los archivos, en lugar de quedar esparcidos por distintos espacios del disco duro, se compacten y queden más organizados.

Para desfragmentar iremos a **Inicio / Todos los programas /Accesorios / Herramientas del sistema**, donde encontraremos la aplicación **Desfragmentador de disco**.

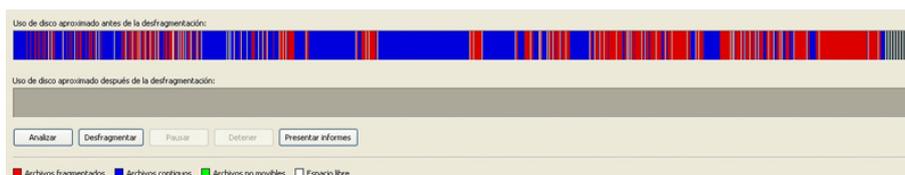


Al ejecutarla, nos aparecerá el siguiente cuadro de diálogo:



Como acciones básicas, podemos **analizar** uno de los discos, o bien proceder a **desfragmentar**.

Después del análisis de uno de los discos, se ha obtenido la siguiente información:



En esta captura de pantalla, podemos ver en **rojo** los archivos que se encuentran fragmentados y en **azul** los que están contiguos. A partir de este análisis, podemos observar la necesidad real de desfragmentar esta unidad de disco.

Este proceso de desfragmentación se llevará a cabo automáticamente escogiendo la opción **Desfragmentar**.



Es importante que el equipo no se apague mientras se está efectuando el proceso de desfragmentación del disco. Por lo tanto, con ordenadores portátiles es recomendable tenerlos conectados a la red, y, con los de sobremesa, se ha de procurar hacerlo en un momento en que se prevea que no habrá interrupción en el suministro de corriente eléctrica.

Desfragmentar disco



ver simulación

Simulación disponible en la versión web del material

Buscar y reparar errores en el disco duro

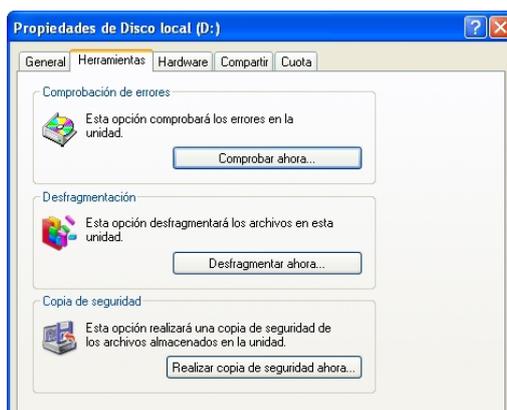
Al ejecutar una aplicación, al mover o eliminar un archivo, cuando se cierra accidentalmente el sistema mientras se está ejecutando... es decir, con un funcionamiento "normal" de nuestro sistema, de forma asociada, se pueden llegar a introducir errores en nuestro disco duro.

El sistema operativo Windows incorpora una herramienta, denominada **Scan-Disk**, que nos permite localizar y reparar buena parte de estos errores.

Si vamos a **Inicio / Mi PC**, podremos seleccionar la unidad de disco que queremos examinar. Una vez seleccionada, haremos clic con el botón derecho del ratón y se nos abrirá el **menú contextual**.



Seleccionaremos la opción **Propiedades** para que se nos abra el siguiente cuadro de diálogo (en el que ya hemos seleccionado la pestaña **Herramientas**).



La primera de las opciones es la comprobación de errores. Al hacer clic en **Comprobar ahora...**, se ejecutará la aplicación Scandisk.



Scandisk

A partir de este nuevo cuadro de diálogo, escogeremos una de las dos opciones:

- Reparar, automáticamente, errores en el sistema de archivos o
- examinar e intentar recuperar los sectores defectuosos.

Una vez escogida una de las dos, al hacer clic en **Iniciar**, se examinará el disco duro y se intentarán reparar los errores que se encuentren.

Restauración del sistema

Una de las mejores herramientas que podemos encontrar en el sistema operativo, en el caso de que éste no arranque, o bien se cierre repentinamente, es la de **Restaurar el sistema**.

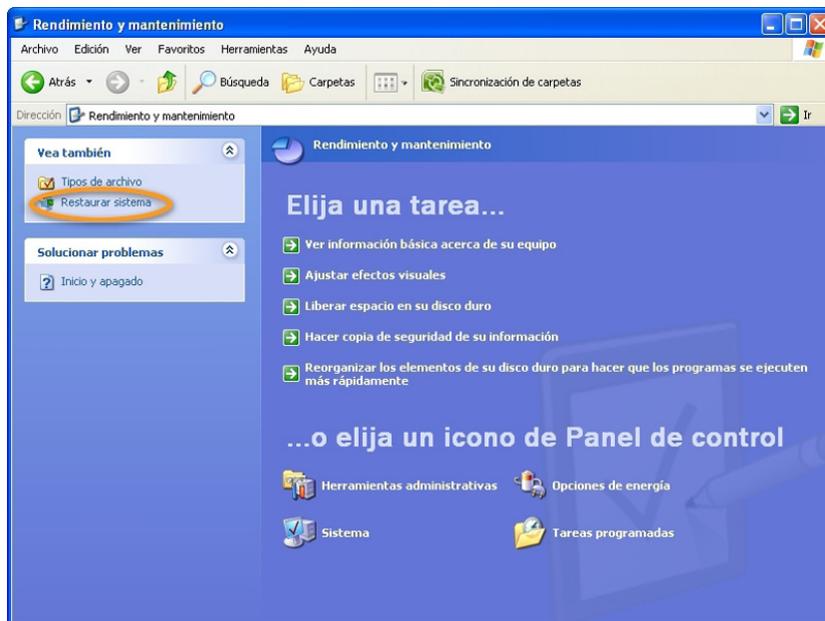
Esta utilidad nos permite devolver nuestro sistema, de forma automática, al punto en el que hayamos efectuado el último punto de restauración. Así, sin que sea necesario ni reinstalar el sistema, ni todos los programas que con el tiempo hayamos instalado, podremos llegar a restablecer esta situación.

La herramienta **Restaurar el sistema** supervisa él mismo, y anota todos los parámetros de configuración de nuestro sistema y los guarda en una base de datos de restauración del sistema.

Debemos tener en cuenta que esta herramienta presenta algunas limitaciones, ya que, aunque nos ayudará a recuperar algunos programas y archivos dañados del sistema, no nos ayudará a recuperar ningún documento o archivo de datos.

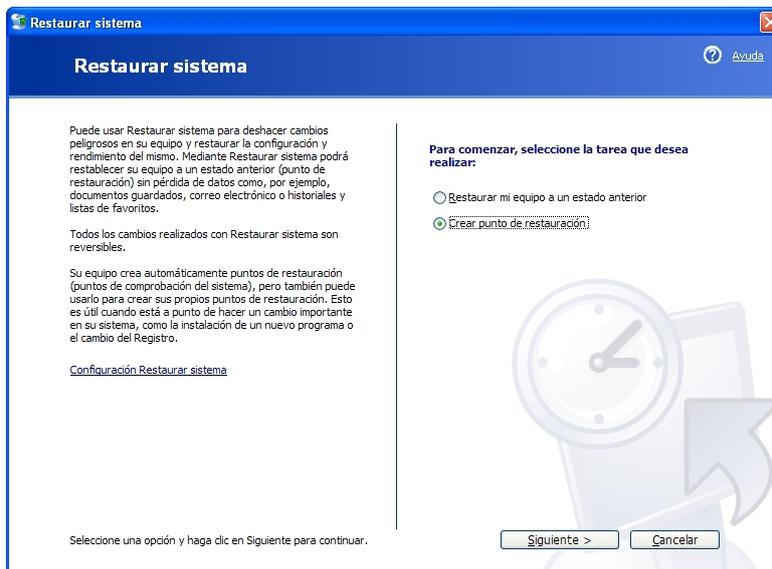
Es muy recomendable crear un punto de restauración antes de instalar un nuevo software o hardware. Así, si después de esta instalación, el equipo no acaba de funcionar correctamente, podemos llegar a restablecer el sistema en el mismo estado en el que estaba antes de esta instalación.

Para crear un **punto de restauración de forma manual**, iremos a **Inicio / Todos los programas /Accesorios / Herramientas del sistema**, y escogemos **Restaurar sistema**.



Al ejecutar esta utilidad, se nos presentarán las dos opciones siguientes:

- Restaurar mi equipo a un estado anterior.
- Crear un punto de restauración.



En primer lugar, deberemos escoger crear un punto de restauración. Y, en el hipotético caso de que nuestro sistema no funcione correctamente, ejecutando esta aplicación, podremos llegar a restablecer la situación en uno de los puntos de restauración que tengamos guardados. Al final del proceso, deberemos reiniciar Windows, teniendo en cuenta que puede tardar algún tiempo en volver a abrirse.

Crear punto de restauración



ver simulación

Simulación disponible en la versión web del material

Limpieza del registro

Si accedemos a la ayuda de Windows, desde **Inicio / Panel de control / Ayuda y soporte técnico**, al solicitar información sobre el Registro de Windows, se nos presenta la siguiente información:



“Windows almacena la información referente a la configuración en una base de datos que se llama registro. (El editor del registro que se incluye en Windows es regedit.exe.) El registro contiene los perfiles de cada usuario del equipo e información acerca del hardware del equipo, los programas instalados y las configuraciones de las propiedades. Windows continuamente hace referencia a esta información durante su funcionamiento.

Los editores del Registro permiten inspeccionar y modificar el Registro. Sin embargo, lo normal es que no necesite hacerlo. En su lugar, permita que los programas de Windows modifiquen el Registro del sistema según lo necesiten. Es muy recomendable que no modifique los valores del Registro.

Advertencia

- **La modificación incorrecta del Registro puede dañar gravemente el sistema. Antes de realizar cambios en el Registro, debe realizar una copia de seguridad de los datos importantes del equipo.**

Si se daña el sistema, podrá reparar el Registro o restaurarlo al estado en el que estaba la última vez que el sistema se inició correctamente. De lo contrario, debe volver a instalar Windows. Cuando se vuelve a instalar el sistema, se pueden perder los cambios realizados, como las actualizaciones de Service Pack, que se deben volver a instalar independientemente. Para obtener información acerca de cómo restaurar el Registro a una versión anterior, haga clic en Temas relacionados.”

Como podemos ver, la manipulación del registro del sistema es un tema delicado, ya que afecta muy directamente al propio funcionamiento del sistema operativo. Y se recomienda que, antes de llevar a cabo cualquier cambio en el registro, se haga una copia de seguridad de los datos importantes del equipo (o mejor, tener una “imagen” de todo el sistema), para poder restablecer la situación en el caso de problemas.

Cada vez que instalamos un programa, creamos un nuevo perfil de usuario, variamos algunas propiedades del sistema, de forma transparente al usuario, se está cambiando el registro. Tengamos en cuenta que el registro almacena toda la información relativa a nuestra configuración.

Para que en el registro no vaya quedando información obsoleta, por ejemplo, por haber desinstalado (de forma incorrecta) un programa, puede ser necesario utilizar alguna de las herramientas que nos “limpian” el registro de Windows.

Con el tiempo, el simple hecho de llegar a instalar y desinstalar muchos programas puede hacer que en el registro vayan quedando entradas (parámetros) que ya no sean necesarios.

Entre estas herramientas (denominadas de **gestión del registro**, dentro de una categoría más general de “limpiadores”), que analizan el registro de Windows de nuestro equipo y detectan sus necesidades de “limpieza”, tenemos:

■ Regseeker



Es un programa *freeware*. Es una utilidad muy sencilla que nos permite gestionar el Registro de Windows, y que no requiere instalación.

Entre otras funciones, dispone de la opción de limpieza automática del Registro, eliminando todas aquellas entradas que no se utilicen. Así, se podría mejorar el funcionamiento del sistema.

<http://www.hoverdesk.net/freeware.htm>

■ Ccleaner



También es un programa *freeware*, que permite la eliminación de ficheros temporales, rastros de navegación... Antes de borrar estos elementos, el programa nos pedirá qué elementos queremos eliminar y cuáles preferimos conservar.

Además, dispone de un limpiador de Registro del Windows, de manera que lo analiza y busca entradas no válidas.

<http://www.ccleaner.com/>

Desde este enlace, podemos tener un buen recorrido sobre su proceso de instalación y su posterior uso:

<http://www.ccleaner.com/help/tour/1-after-installation>

■ Advanced System Optimizer (ASO)



Es una versión comercial, con una versión de prueba de 30 días. De hecho, en la línea de alguna de las anteriores, es más una herramienta de optimización global que no un simple limpiador de registro. Presenta muchas opciones, bien clasificadas por categorías.

Incluye una buena gestión de la seguridad del sistema, ya que, antes de efectuar alguna modificación en el registro, guarda una copia de seguridad del mismo. Incluso, al eliminar archivos duplicados o innecesarios, los pasa a la **Papelera de reciclaje** (y mientras no borremos los elementos de la papelera, siempre podremos restablecerlos).

<http://www.systweak.com/asov2/>

En definitiva, estos programas nos pueden ayudar a mantener nuestro sistema en perfecto estado haciendo una limpieza a fondo, que mejora el rendimiento general y aumenta el espacio libre en el disco.

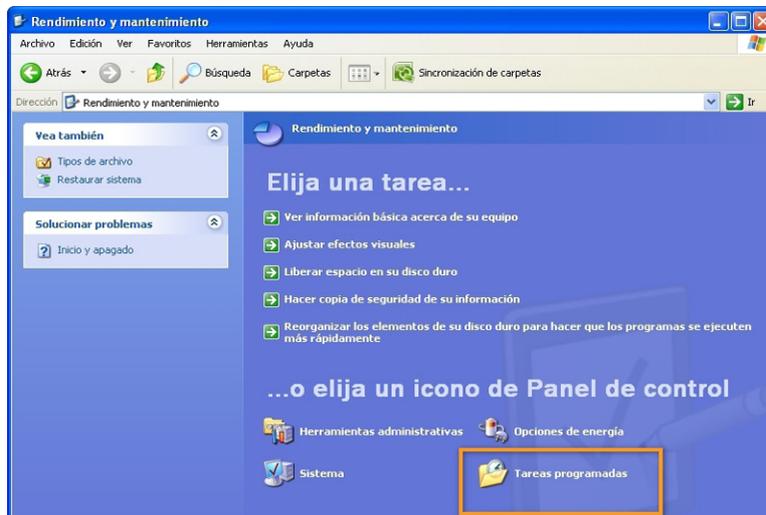
Tareas programadas

El sistema operativo Windows XP dispone de una función, denominada **Tareas programadas**, que permite programar que ciertas tareas se ejecuten, automáticamente, en nuestro equipo en un momento determinado. Así, las aplicaciones que hayamos seleccionado se ejecutarán a la hora más adecuada, o, periódicamente, cada cierto tiempo (días, semanas o meses), o incluso al iniciarse el sistema.



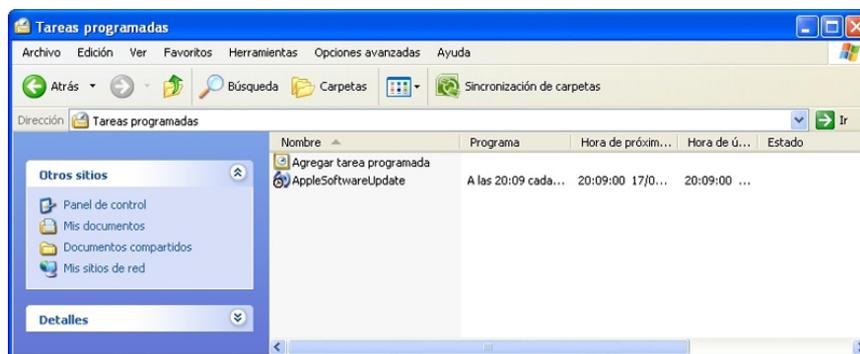
Cada vez que iniciamos el sistema, Tareas programadas se está ejecutando en segundo plano. Otras opciones que permite Tareas programadas es modificar la programación de una tarea, detenerla o personalizar la forma en que se ejecutará.

Desde **Inicio / Panel de control**, en **Rendimiento y mantenimiento** podemos agregar (o, si es el caso, modificar) una tarea programada.



Agregar una tarea programada

Al hacer clic sobre **Tareas programadas**, nos aparecerá el **cuadro de diálogo** desde el que podremos agregar una tarea programada, o bien modificar o eliminar la programación de una cierta tarea.



Haciendo doble clic en **Agregar tarea programada**, aparecerá un asistente que nos guiará en el proceso.

Si deseamos efectuar una configuración avanzada de la tarea, deberemos activar la casilla de verificación **Abrir propiedades avanzadas de esta tarea** al hacer clic en **Finalizar**, que nos aparece en la página final del asistente.

Tarea programada


ver simulación

Simulación disponible en la versión web del material

Actividades

Indica si los siguientes enunciados son verdaderos o falsos.

	V	F
Cuando algo no nos funciona en nuestro equipo, lo más probable es que sea un error de hardware.		
La tecla F8 nos servirá para reiniciar el ordenador.		
Mediante la combinación de teclas Ctrl - Alt – Supr podemos acceder al <i>Administrador de tareas del Windows</i> .		
El <i>Administrador de tareas del Windows</i> nos permite comprobar si hay alguna tarea bloqueada.		
Windows dispone de una ayuda que nos permite obtener la posible solución de un problema.		
No hay posibilidad de cambiar las particiones de un disco cuando éste ya está en funcionamiento, y por lo tanto ya tiene guardada información.		
Antes de formatear un disco, debemos tener muy en cuenta que, si lo hacemos, perderemos toda la información (documentos, aplicaciones, datos...) que tenga guardada.		
Regcleaner es una herramienta del sistema operativo que nos permite limpiar el disco duro de archivos temporales.		
La desfragmentación consiste en que los archivos, en lugar de quedar esparcidos por distintos espacios del disco duro, se compacten y queden mejor organizados.		
Scandisk sirve para comprobar errores en el disco.		
La herramienta <i>Restaurar el sistema</i> lo supervisa, pero no anota los parámetros de configuración de nuestro sistema.		
La manipulación del <i>registro del sistema</i> es un tema delicado, por lo que se recomienda que antes de efectuar cualquier cambio en el registro, se haga una copia de seguridad de los datos importantes del equipo.		
La función del sistema operativo denominada <i>Tareas programadas</i> permite programar que ciertas tareas se ejecuten, automáticamente, en nuestro equipo en un momento determinado.		

Tecnología digital II

MONTAR Y CONFIGURAR UNA RED DOMÉSTICA

En este tema veremos cómo crear una red con cables o inalámbrica, cómo montarla y cómo configurarla. El proceso no es complicado y, a partir de éste, iremos conociendo conceptos más teóricos de redes que nos permitirán llegar a conocerlas mejor.

En primer lugar, veremos qué elementos necesitamos (tarjetas de red, *hubs*...), cómo instalarlos y cómo configurarlos hasta llegar a conseguir la configuración de la conexión del PC dentro de la red.

Finalmente, veremos algunas utilidades que nos pueden ayudar a conocer los parámetros y los equipos de nuestra red.

Al final de tema, encontrarás una actividad para desarrollar que te permitirá conocer si has asimilado los conceptos trabajados en él mismo.

Redes locales y tipos de comunicación

Una red local (o LAN, *local area network*) se define como aquella red de ordenadores que ocupa un área geográfica reducida, generalmente limitada a un edificio o una planta dentro de un edificio. Estas redes son de carácter privado, gestionadas por una única organización, que ofrecen velocidades de transmisión de datos del orden de Mbps (megabits por segundo), o de centenares de Mbps.

Sus principales funciones son:

- Compartir periféricos como impresoras, escáneres...
- Compartir soportes de almacenamiento masivo, como discos duros, y otros recursos como conexiones a Internet.
- Centralizar la información en organizaciones grandes. De este modo, los servidores de ficheros y los de bases de datos estarán ubicados en máquinas distintas de las que utilizan los usuarios.
- Facilitar la gestión de los equipos.

La comunicación entre los distintos equipos de una red puede ser **por cable** o sin hilos, **de forma inalámbrica**.

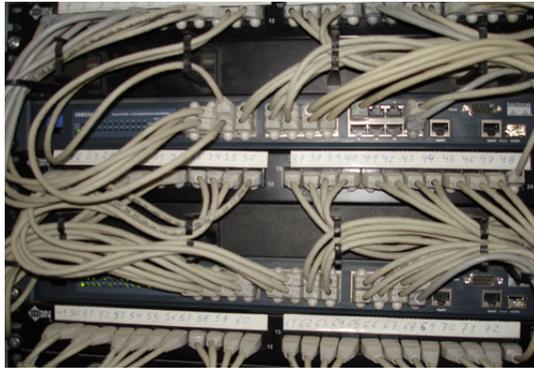
Las tecnologías de comunicación inalámbricas ya forman parte de nuestro día a día, sobre todo a raíz de la telefonía móvil. Pero éstos no son los únicos dispositivos que se comunican de forma inalámbrica. Seguro que podemos pensar en otros: desde el portátil que se conecta a la red, consolas de videojuegos, PDA, hasta teclados y ratones inalámbricos. Todos ellos posibilitan llegar a transferir información al equipo o a otro dispositivo sin necesidad de cables.

■ Por cable



En términos de redes, y en concreto de redes LAN cableadas, el protocolo más utilizado es Ethernet. Éstas son las redes más extendidas en el ámbito de las redes locales. Siguen la norma que se denomina IEEE 802.3. Las velocidades de transmisión van desde los 10 Mbps hasta los 100 Mbps.

En esta imagen, podemos observar un armario de conexiones de una red Ethernet, con algunos switches (que permiten la interconexión de equipos en red), con sus puertos y el correspondiente cableado (la terminación de cada uno de estos cables se denomina **RJ-45**). Como podemos intuir por la imagen, es una red que presenta un gran número de ordenadores y dispositivos.



■ Inalámbricas

Las redes sin hilos (o redes wireless) permiten la conexión de dispositivos sin cables. Siguen los estándares desarrollados por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos, que es la organización encargada de la elaboración de muchas de las normas relativa a redes).

Desde Windows XP podemos conectarnos a una red inalámbrica siempre que dispongamos, en el equipo, de una **tarjeta o adaptador wireless** (inalámbrico) y estemos dentro del alcance de una red que nos permita la conexión.

Conexión y configuración de redes

Una red de ordenadores se puede definir como un conjunto de ordenadores conectados entre sí, de forma que entre ellos se puede intercambiar información y compartir sus recursos.

Las redes permiten compartir información entre usuarios de distintos equipos y también diferentes recursos asociados a cada equipo, como impresora, conexión a Internet...

Hardware específico para montar una red

Seguro que en algún momento nos habremos planteado cuáles son los elementos hardware que precisamos para montar una red (con cables o inalámbrica).

1. **Tarjeta de red.** Cada equipo (PC, portátil...) precisa de una tarjeta. En los PC de sobremesa, a menudo esta tarjeta de red ya está incorporada dentro de la misma placa base del equipo, de modo que no necesitaremos de una tarjeta adicional que conectaríamos en una de las ranuras de la placa base (tarjeta interna de red).



En el caso de que queramos incorporar este equipo a una red inalámbrica, sí que deberemos añadir una **tarjeta de red inalámbrica** adicional dentro del PC, o bien utilizando algún **dispositivo externo** (USB o tarjeta) que permita esta conexión. La mayoría de portátiles también incorporan tarjetas de red con cables, e incluso un **adaptador WI-FI integrado** para la conexión a una red doméstica inalámbrica, o a un punto de conexión WI-FI público. En el detalle de las características técnicas del ordenador, podremos comprobar si incorpora estos elementos de conexión.



Tarjeta de red inalámbrica



Dispositivo externo

2. **Router de red (o enrutador).** [Después necesitamos un router de red o enrutador. Conectando todos los equipos a este router, por cable o de forma inalámbrica si el router también lo permite, tendremos interconectados todos nuestros equipos, e incluso otros dispositivos (impresoras...). Este router será el que también nos facilitará la conexión a Internet. Con la configuración adecuada de cada equipo de la red, todos ellos podrán conectarse a Internet de forma simultánea.

En el caso de redes con muchos equipos, podemos tener **hubs** (o concentradores) [], o bien **switchs**, a los que conectaremos todos los equipos que estén conectados a la red con cable. Conectando el *hub* con el router estaremos proporcionando la salida a Internet de los distintos equipos de la red.



Router de red



Switchs

3. **Cable UTP.** En el caso de redes con cables, precisaremos un cable UTP –cable de par trenzado no apantallado–, por ejemplo de categoría 5E, con terminación (conector) RJ45, cada uno de ellos con la longitud suficiente (2 m, 5m, 10 m...) para conectar cada ordenador con el router o con el hub.



Tengamos en cuenta que en una red podemos llegar a tener equipos conectados con cable y otros que se conecten a la red de forma inalámbrica. En el caso de que el router tenga la opción inalámbrica, ya no precisaremos de ningún dispositivo adicional. Y en el caso de que el router no sea inalámbrico, y deseemos conectar a nuestra red un portátil con conexión inalámbrica, deberemos incorporar a la red un dispositivo denominado **punto de acceso inalámbrico** (físicamente son muy parecidos a los enrutadores). Sólo deberemos conectarlo por cable al *hub* o router de la red. De ese modo, el portátil accederá a este punto de acceso y desde él, a toda la red.

Una **configuración típica de una red doméstica** sería la de un router con posibilidad de conectar 4 equipos por cable, y con la conexión inalámbrica incorporada, y que tengamos un ordenador de sobremesa, con una ubicación cercana a la del router, con la tarjeta de red integrada en la placa base, que conectaremos con un cable RJ45 al router, y un portátil con adaptador inalámbrico incorporado, desde el que nos conectaremos al router de forma inalámbrica. De esta forma, tendremos dos equipos conectados a un router que nos permitirá tenerlos en red y con conexión a Internet.

A partir de aquí, siempre podremos ir ampliando la red con nuevos equipos, impresoras...

Algunas impresoras incorporan una tarjeta de red o, incluso, un adaptador inalámbrico, lo que permite conectarlas a la red directamente. En el caso de que queramos conectar en red una impresora que no tenga ni tarjeta de red ni adaptador, tenemos dos opciones para conectarla a la red y que pueda ser utilizada por varios equipos:

1. **Conectarla a uno de los equipos**

Desde el equipo donde se ha conectado la impresora, se debe activar la opción de que sea una impresora compartida. Desde **Inicio/Panel de Control** localizaremos la impresora que se tiene que compartir, y con el botón derecho del ratón abriremos el menú contextual. Seleccionaremos **Propiedades** y, desde el cuadro de diálogo que se abrirá, iremos a **Compartir**. El inconveniente de esta opción es que, al estar la impresora conectada a este ordenador, para que pueda ser utilizada por otros equipos, este ordenador deberá estar encendido.

2. **Utilizar un dispositivo que haga de servidor de impresoras**

Esta opción consiste en conectar la impresora a un dispositivo que nos haga de **servidor de impresoras**, al que se conectará la impresora, y, con un cable RJ45, se conectará a la red.

Después de detallar los elementos hardware que podemos llegar a tener en nuestra red, seguiremos con el detalle de aspectos de su configuración.

Configuración de la red y de sus elementos

En principio, cada elemento hardware que hemos detallado tendrá su proceso de instalación. Será el mismo fabricante quien nos facilitará un pequeño manual para poder conectarlo y configurarlo convenientemente. Además, en muchos casos, son dispositivos **Plug and Play**, de manera que al conectarlos ya son reconocidos por el sistema, instalándose los controladores necesarios para que funcionen.

La tarjeta de red, si ya viene instalada en la placa base, ya será reconocida por el sistema. Lo mismo ocurre con el adaptador inalámbrico que pueda incorporar el portátil. Sólo un pequeño detalle: tengamos en cuenta que esté encendida la conexión inalámbrica del portátil, ya que a menudo dispondremos de un botón que nos permitirá activarla o desactivarla.

El router y, si es el caso, el *hub* ya nos vendrán con una configuración de fábrica que deberemos valorar si es necesario adaptar para que funcionen en nuestra red.

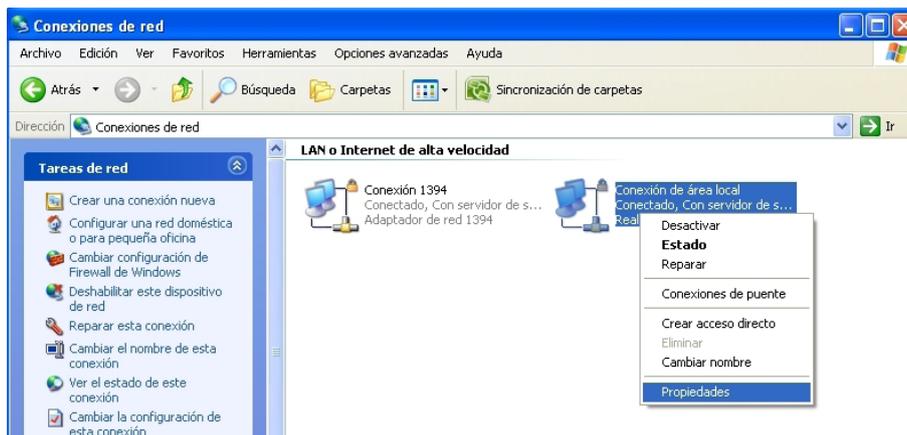
Una vez instalado el hardware de la red, deberemos configurar el sistema operativo para que reconozca y trabaje con la red.

El sistema operativo Windows XP dispone de un asistente, denominado **Asistente de configuración de red** [que nos permitirá configurarla.

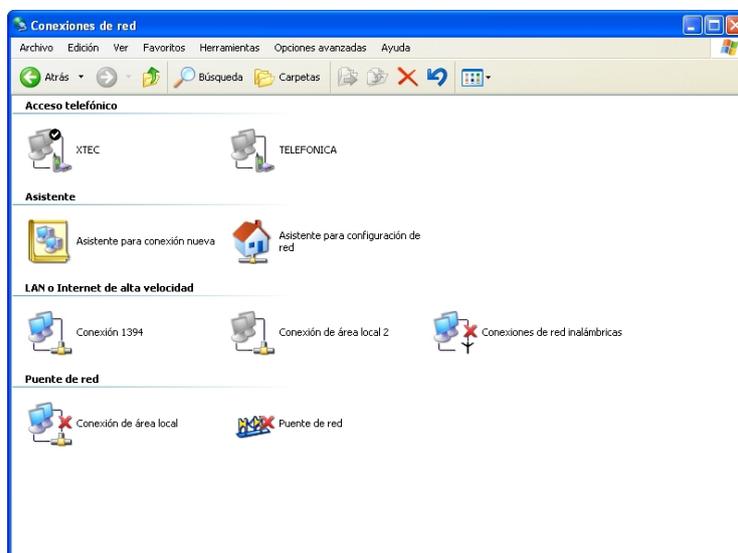
Los elementos de configuración de la red, podemos encontrarlos en **Inicio/Panel de control/ Conexiones de Red**.



Al hacer clic en **Conexiones de red**, se nos abrirá una ventana en la que nos aparecerán todas las conexiones de red que tengamos, entre ellas, la conexión de área local o, en su caso, la conexión inalámbrica.



Como segundo ejemplo: en este caso se trata de un portátil. Para conectarse a la red utiliza o bien la **Conexión de red inalámbrica** (en el momento de la captura de pantalla podemos ver que está inactiva), o bien la **Conexión de área local**.



Conexión de red inalámbrica

Si seleccionamos una de estas conexiones, y hacemos clic con el botón derecho del ratón a **Propiedades**, llegaremos a la ventana clave para las configuraciones de red.

Si deseamos comprobar cómo está configurado este equipo dentro de la red, deberemos llegar a localizar la información que nos aparecerá en esta ventana. Son las **propiedades de la conexión del equipo a la red**.



En esta ventana aparecen algunos conceptos relacionados con redes de ordenadores que deberemos conocer.

Nos interesará el siguiente elemento de la conexión: **Protocolo Internet TCP/IP** (*Transmission control protocol/Internet protocol*).

El funcionamiento de Internet se basa en la tecnología denominada de “**conmutación de paquetes**”. En este tipo de redes, la información se fragmenta en pequeños paquetes del mismo tamaño, denominados “**datagramas**”. Cada paquete de datos contiene la dirección del ordenador al que va dirigido, y va circulando por los distintos nodos de la red, siguiendo la ruta óptima, dependiendo de lo que se va encontrando en la red en cada momento. Por lo tanto, cada paquete circula por la red “con su propio camino”, independientemente del resto de paquetes, y es el ordenador destino (el receptor) el que se encarga de reagruparlos con el orden correcto, para así poder recuperar la información original. De hecho, este funcionamiento es la base del denominado protocolo TCP/IP (*transport control protocol / Internet protocol*).



El protocolo **TCP/IP** (*transport control protocol / Internet Protocol*) define un conjunto de normas que rigen la transmisión de datos entre ordenadores conectados a Internet.

El **protocolo TCP** (*transport control protocol*) se encarga de fragmentar la información en paquetes, garantizando la transmisión fiable de datos entre el equipo emisor y el receptor.

El **protocolo IP** (*Internet protocol*) se encarga de conducir los paquetes de datos por la red, seleccionando la ruta que deberá seguir cada uno de ellos hasta llegar a su destino.

Este protocolo es el que permite salvar la principal dificultad de interconexión dentro de Internet de distintos tipos de redes y sistemas informáticos, en muchos casos incompatibles entre sí. Estos protocolos de comunicación son los que permiten esta interconexión, de forma que todos ellos se puedan llegar a “entender”.

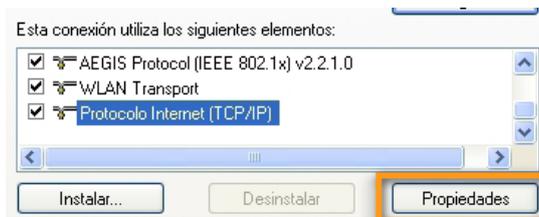
Además, para cada uno de los servicios proporcionados por Internet se ha desarrollado un protocolo específico: HTTP –hypertext transfer protocol- para el World Wide Web (para la transmisión de páginas HTML), SMTP –single message protocol- para la transferencia de mensajes de correo electrónico...

Cada equipo que se conecta a esta red tiene asignado un número que lo identifica de forma única. Este número se conoce con el nombre de “**dirección IP**”. Actualmente, una dirección IP está formada por una secuencia de 4 bytes (32 bits). Normalmente, suele representarse como cuatro cifras decimales comprendidas entre 0 y 255 (ambos inclusive). Por ejemplo: **172.26.0.135**. Con la nueva versión del protocolo (denominado IPv6), esta secuencia se amplía a 16 bytes, con la finalidad de solucionar la necesidad de nuevas direcciones IP, y así poder dar respuesta al gran crecimiento que ha tenido y está teniendo la red Internet a lo largo de los últimos años.

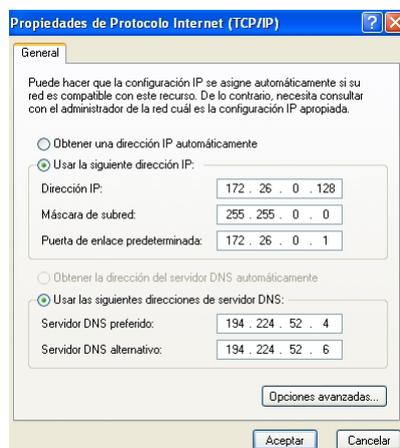
Otro elemento relevante, al hablar de las propiedades de la conexión, es el de los servidores **DNS**. Cuando nos conectamos a un determinado servidor dentro de Internet, no nos es necesario que recordemos cuál es su dirección IP, ya que, con una nomenclatura paralela, cada máquina tiene, además, un nombre asignado. Esta asociación nombre-dirección IP está guardada en bases de datos, accesibles desde cualquier lugar, denominadas DNS (servidor de nombres de dominios, en inglés, *domain name server*). Así, cuando, a una aplicación, le damos el nombre de la máquina a la que debe conectarse, esta aplicación consulta el DNS para conocer la dirección IP que le corresponde, y de esta forma poderla trasladar a los protocolos que utilizará para la comunicación.

Estos conceptos nos permitirán entender mejor las propiedades del protocolo TCP/IP que podemos encontrar en nuestra conexión de red.

Si, seleccionando el **elemento protocolo Internet TCP/IP** de la ventana anterior, hacemos clic en **Propiedades**, podremos observar los parámetros de esta conexión.



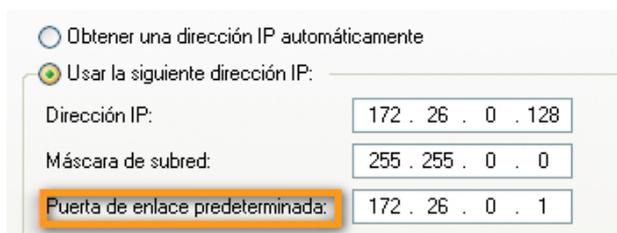
Elemento protocolo Internet TCP/IP



Propiedades

Estos parámetros de configuración dependen de algunos parámetros de configuración asociados al router y al proveedor de servicios de Internet que nos facilita la conexión.

En primer lugar, nos centraremos en la **dirección IP**. El router puede estar configurado de forma que cada vez que un equipo se conecte a él dentro de la red, se le asigne una dirección IP de manera automática (se estará utilizando el protocolo denominado **DHCP**). Si no está configurado así, a cada equipo le deberemos asignar una IP concreta. Por ejemplo, en esta red podríamos utilizar un valor 172.26.0.z, donde z sería un valor entre 2 y 254, viendo que el router tiene asignada la dirección IP 172.26.0.1. Este parámetro es uno de los de configuración del propio router. Además, será el que utilizaremos para poner en el apartado **Puerta de enlace predeterminada** (corresponde a la dirección IP del router):



Formulario de configuración de IP con los siguientes campos:

- Obtener una dirección IP automáticamente
- Usar la siguiente dirección IP:
- Dirección IP: 172 . 26 . 0 . 128
- Máscara de subred: 255 . 255 . 0 . 0
- Puerta de enlace predeterminada: 172 . 26 . 0 . 1

La **máscara de subred** puede que nos salga, automáticamente, al introducir el valor de dirección IP. Nos permite implantar una red del tipo adecuado dentro del segmento de área local. Los valores habituales son: 255.255.255.0 ó 255.255.0.0.

En cuanto a las DNS, utilizaremos las que nos facilite nuestro ISP, aunque se podrían utilizar otras. También dependerá de cómo esté configurado el router que esta asignación se pueda efectuar de forma automática, sin tener que entrar esta información en cada equipo.

Las ventajas de una asignación automática de IP y DNS son evidentes, aunque, si queremos controlar exactamente con que IP se conecta cada equipo, una asignación manual de IP (y DNS) puede llegar a ser una mejor opción.

Configurar TCP/IP



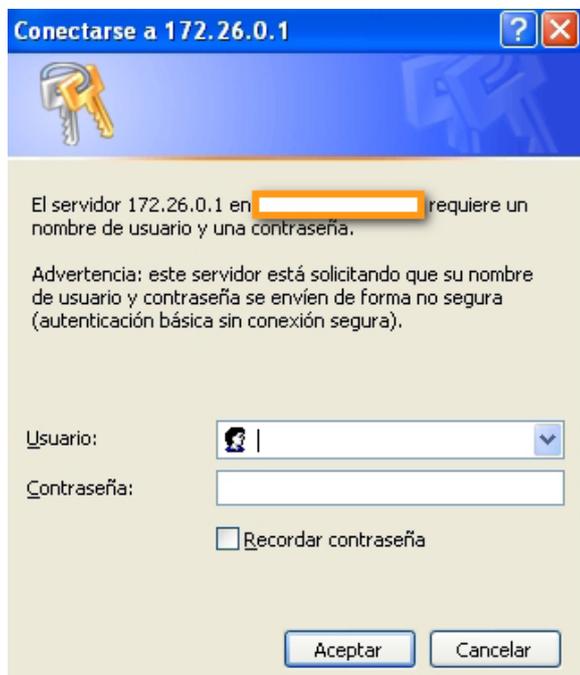
ver simulación

Simulación disponible en la versión web del material

Configuración del enrutador (router)

Antes de modificar algunos de los parámetros internos de configuración de nuestro router, debemos anotarnos la configuración inicial que nos encontremos. De este modo, si después de una modificación de algún parámetro no nos funciona el enrutador, siempre podremos restablecer la situación inicial.

Para acceder a su configuración interna, abriremos el navegador y, en la barra de direcciones, escribiremos la dirección IP del enrutador, por ejemplo: <http://172.26.0.1>. Nos aparecerá una ventana en la que se nos pide el **nombre de usuario y contraseña** que nos habrá facilitado o bien el fabricante, o bien nuestro proveedor de servicios de Internet.



Al introducir estos datos, accederemos al **menú de configuración del enrutador** (en este caso es un router **Zyxel**). Desde esta ventana tendremos acceso a todos sus **parámetros de configuración**.



Entre estos parámetros tenemos los de configuración de la red local. En este caso, podemos ver dentro de la opción **Advanced Setup / LAN** que DHCP está desactivado, y también podemos observar la dirección **IP del enrutador**.

Aplicaciones para conocer los elementos de una red

Existen aplicaciones específicas, como las que detallaremos en este apartado, que nos permiten reconocer y obtener las características de los equipos que se encuentran conectados a una red.

Analizadores del sistema

Pero, antes de entrar en detalle con estas aplicaciones, presentaremos una utilidad (de las denominadas **analizadores del sistema**) que nos facilita información sobre un equipo, esté en red o no. Y, en el caso de que esté en red, nos presenta detalles de su configuración de red.

Se trata de **EVEREST home edition** (inicialmente, se denominaba **AIDA32**). Con un simple ejecutable, en pocos segundos efectúa un completo análisis del ordenador, mostrando, prácticamente, todos los aspectos del sistema referentes a hardware, software, configuración de red y más. En la ventana de una sencilla interfaz, presenta una estructura de árbol en la que se clasifican los distintos elementos analizados por esta aplicación.

EVEREST home edition



EVEREST home edition es un programa *shareware* que encontrarás en:

<http://www.lavalys.com/products/download.php?pid=1&lang=en&pageid=3>

Ej.

Con esta aplicación, podemos obtener datos (muy detallados) sobre la **configuración de nuestro ordenador**: velocidad, memoria instalada, dirección IP del equipo, placa base, sistema operativo, configuración de la red local y de Internet, identificación de programas que se ejecutan al iniciar el equipo... Además, permite generar informes en distintos formatos.

Su interfaz es sencilla y muy intuitiva.

Una utilidad concreta de esta aplicación podría ser llegar a detectar el **modelo y fabricante de algún componente hardware del equipo**, lo que nos permitiría llegar a localizar, rápidamente, el *driver* o controlador necesario para sustituir el que tengamos funcionando incorrectamente.

Pero también dispone de otras utilidades como:

- El **sensor**. Nos da información de la temperatura de nuestros dispositivos.
- La **memoria**. Nos facilita, en caso de querer o necesitar una ampliación de memoria, el fabricante, el modelo y todas las características principales para acertar en el momento de hacer el cambio o la ampliación de la tarjeta.

Además, dispone de otros apartados que nos permiten reconocer y obtener características de los equipos conectados a una red.

Utilidades dentro del sistema operativo

El sistema operativo también incorpora algunas utilidades que nos facilitan información sobre nuestra configuración de red, o de las conexiones. Por lo tanto, nos pueden ser de utilidad para averiguar y solucionar problemas de conectividad dentro de una red local.

Para ejecutarlas, podemos ir a **Inicio/Ejecutar** y escribir el nombre del comando asociado a la aplicación. Otra forma de ejecutarlos es ir a **Inicio/Todos los programas/Accesorios** y hacer clic en **Símbolo del sistema**.

 Símbolo del sistema

Tendremos activa una línea de órdenes desde la que podremos ejecutar las aplicaciones que presentaremos. Veamos algunas de estas utilidades:

- **ipconfig**
En concreto, **ipconfig** nos puede ser de utilidad para solucionar un problema de red TCP/IP, ya que nos permite comprobar la configuración de TCP/IP en el equipo que tiene el problema. Podemos utilizar el comando **ipconfig** para obtener información de la configuración del equipo, incluidas la dirección IP, la máscara de subred y la puerta de enlace predeterminada. En versiones anteriores a Windows XP (por ejemplo, Windows 95 y Windows 98), este comando se denominaba **winipcfg**, en lugar de **ipconfig**.
Permite visualizar los valores de configuración de la red del TCP/IP.
Para visualizar sus parámetros principales podemos ejecutar **/all**: visualiza los parámetros de la configuración.

■ ping

El comando **ping** ayuda a comprobar la conectividad en el nivel IP, es decir permite comprobar si un equipo o dispositivo de la red, con una IP asignada, se encuentra activo dentro de esta red. Podemos utilizar **ping** para enviar una solicitud, un nombre de *host* o una dirección IP de destino. Así, podremos comprobar si podemos conectarnos a otros equipos u otros recursos de la red.

Es una orden que envía paquetes a un ordenador remoto, y espera su respuesta.

■ hostname

Permite visualizar el nombre de la máquina local.

■ tracert

El programa “tracert” de Windows permite ver por qué routers (o encaminadores) pasa una conexión Internet. También facilita información sobre el tiempo que tardan los paquetes en ir y volver a estos routers.

Para ejecutar “tracert”, se debe ir a Inicio/Ejecutar y escribir, por ejemplo: **tracert www.yahoo.com**.

Un detalle de la información que presenta tracert:

```
 4 74 ms 71 ms 71 ms 85.Red-80-58-88.pooles.rima-tde.net [80.58.88.85]
 5 76 ms 71 ms 72 ms 9.Red-80-58-86.pooles.rima-tde.net [80.58.86.9]
 6 73 ms 74 ms 73 ms 189.Red-80-58-73.pooles.rima-tde.net [80.58.73.189]
 7 72 ms 70 ms 75 ms 242.Red-80-58-73.pooles.rima-tde.net [80.58.73.242]
 8 70 ms 71 ms 73 ms 110.Red-80-58-72.pooles.rima-tde.net [80.58.72.110]
 9 72 ms 74 ms 71 ms 213.140.39.9
10 72 ms 71 ms 76 ms So6-2-0-grtmadde2.ri.telefonica-data.net [213.140.36.114]
11 161 ms 163 ms 158 ms So1-3-1-grtmiatc3.ri.telefonica-data.net [213.140.37.11]
12 161 ms 160 ms 160 ms ibr01-p0-1.miam01.exodus.net [213.140.39.254]
13 195 ms 191 ms 190 ms bbr02-g6-0.miam01.exodus.net [64.253.193.181]
14 214 ms 211 ms 211 ms bbr02-p3-0.atln01.exodus.net [206.79.9.77]
15 222 ms 221 ms 219 ms bbr02-p1-0.ftwo01.exodus.net [206.79.9.190]
16 225 ms 227 ms 231 ms bbr01-g2-0.ftwo01.exodus.net [216.39.64.1]
17 256 ms 258 ms 255 ms bbr01-p5-0.sntc04.exodus.net [209.185.9.109]
```

Tracert se ejecuta bajo MSDOS. Aparecen el número de nodo, tres mediciones del tiempo de respuesta en ms y la dirección IP de cada nodo, o nombre de servidor.

■ nslookup

Con esta aplicación, nos estamos conectando a nuestros servidores DNS para poder llegar a conocer la IP de un nombre de *host* concreto.

Por ejemplo, si escribimos **nslookup www.yahoo.com**, obtendremos la IP de este servidor.

■ getmac

Muestra las **direcciones MAC** de los adaptadores de red que tengamos instalados en el sistema. Este número identifica de forma única cada adaptador de red.

■ netstat

Windows (y también Linux) nos ofrece una herramienta que nos va a mostrar qué conexiones de red tenemos en cada momento. Esa herramienta es el programa netstat. Para ejecutarla podemos ejecutar: **netstat -an**.

Para entender mejor qué conexiones tenemos abiertas, lo mejor es que antes de ejecutar esta orden cerremos todos los programas a excepción de MSDOS (el que tenemos activo con **símbolo del sistema**), para, así, ir desde el principio comprobando qué conexiones tenemos y cuáles se van abriendo.

Si queremos que se actualice, automáticamente, la información, podemos escribir **netstat -an 5** (poner el número en segundos del intervalo que queramos que actualice la información).

Para obtener una pequeña ayuda en relación a netstat, ejecutaremos: **netstat/help**.

Un ejemplo de la información que nos facilita **netstat** es la que se muestra en esta imagen:

```
Conexiones activas
Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135          0.0.0.0:0             LISTENING
TCP    0.0.0.0:445          0.0.0.0:0             LISTENING
TCP    0.0.0.0:1025         0.0.0.0:0             LISTENING
TCP    0.0.0.0:1027         0.0.0.0:0             LISTENING
TCP    0.0.0.0:3022         0.0.0.0:0             LISTENING
TCP    0.0.0.0:3284         0.0.0.0:0             LISTENING
TCP    0.0.0.0:3286         0.0.0.0:0             LISTENING
TCP    0.0.0.0:3287         0.0.0.0:0             LISTENING
TCP    0.0.0.0:5000         0.0.0.0:0             LISTENING
TCP    127.0.0.1:3001       0.0.0.0:0             LISTENING
TCP    127.0.0.1:3002       0.0.0.0:0             LISTENING
TCP    127.0.0.1:3003       0.0.0.0:0             LISTENING
TCP    193.153.12.193:3284 207.46.106.87:1863    ESTABLISHED
TCP    193.153.12.193:3286 213.73.40.217:80      CLOSE_WAIT
TCP    193.153.12.193:3287 213.73.40.217:80      CLOSE_WAIT
TCP    193.153.12.193:3289 213.73.40.60:80      TIME_WAIT
TCP    193.153.12.193:9396 0.0.0.0:0             LISTENING
UDP    0.0.0.0:135          *:*
UDP    0.0.0.0:445          *:*
UDP    0.0.0.0:500          *:*
UDP    0.0.0.0:1026         *:*
UDP    0.0.0.0:3006         *:*
UDP    0.0.0.0:3014         *:*
UDP    0.0.0.0:3031         *:*
UDP    127.0.0.1:123        *:*
UDP    127.0.0.1:1900       *:*
UDP    127.0.0.1:3013       *:*
UDP    127.0.0.1:3077       *:*
UDP    127.0.0.1:3285       *:*
```

En ella podemos apreciar que, al principio, al no estar conectados a internet, tenemos direcciones locales, pero no tenemos dirección remota (equipos a los que nos conectamos). Todos los estados están en *listening*, lo cual significa que el puerto está listo.

Al conectarnos a Internet, vemos que se nos abren nuevos puertos, entre los que hay el 3284, que sería la conexión con el servidor. Al otro lado, vemos el puerto 1863, que es el que utiliza el Messenger, y su estado es establecido, con lo que la conexión está completa.

Cuando utilizamos Internet Explorer para intentar conectarnos a una dirección web, podemos ver que se nos abre, automáticamente, el puerto 80, que sería el de WWW.

Utilidades específicas

Tal y como hemos comentado al principio del tema, existen **aplicaciones específicas** que permiten reconocer y obtener algunas características de los equipos conectados a una red.

Entre ellas destacaremos:

■ Look@LAN Network Monitor



Este programa (aplicación *freeware*) lleva a cabo un completo análisis de la red local, de forma sencilla y totalmente automatizada. La interfaz principal de la aplicación muestra toda la información recopilada como resultado del análisis: dirección IP, estado, grupo de red, sistema operativo, nombre de *host*, usuario... Las gráficas e información que facilita se pueden exportar a texto o a HTML.

www.looktlan.com

Instalación de Look@LAN Network Monitor



ver simulación

Simulación disponible en la versión web del material

Funcionamiento de Look@LAN Network Monitor



ver simulación

Simulación disponible en la versión web del material

■ NetworkView 3.50



Ésta es una aplicación *shareware* de gran utilidad para efectuar estudios de redes locales y crear diagramas con la distribución de los ordenadores y las conexiones existentes entre ellos. Con NetworkView se puede trazar, en poco tiempo, un completo esquema de tu red local y detectar todos los nodos de TCP/IP y sus rutas utilizando la información facilitada por los DNS, SNMP y los puertos TCP.

www.networkview.com

Actividades

Indica si los siguientes enunciados son verdaderos o falsos.

	V	F
La terminación del cable de red se denomina RJ45.		
El protocolo TCP/IP (<i>transport control protocol / Internet protocol</i>) define un conjunto de normas que rigen la transmisión de datos entre ordenadores conectados a Internet.		
Everest es un programa que se utiliza para configurar una red.		
Tcpip configura es la aplicación del sistema operativo que nos puede ser de utilidad para solucionar un problema de red TCP/IP, ya que nos permite comprobar la configuración de TCP/IP en el equipo que tiene el problema.		
Abriendo el navegador e introduciendo la dirección IP podremos acceder (si conocemos el usuario y la contraseña) a la configuración interna del enrutador .		
Ping permite comprobar si un equipo o dispositivo de la red, con una IP asignada, se encuentra activo dentro de esta red.		
Netstat es una herramienta del sistema operativo que nos puede mostrar las conexiones de red que tenemos en cada momento.		
La utilidad tracert permite ver por qué routers (o encaminadores) pasa una conexión Internet.		
Con el programa NetworkView podemos trazar, en poco tiempo, un completo esquema de nuestra red local.		

Tecnología digital II

SEGURIDAD EN LAS COMUNICACIONES

En este tema trataremos aspectos avanzados de seguridad, empezando con los tipos de servicios a los que deben dar respuesta las redes de comunicaciones y siguiendo con una introducción a la criptografía, con las medidas de seguridad que se adoptan en las transacciones comerciales por la red, los certificados y las firmas digitales, hasta finalizar con los protocolos de seguridad que podemos llegar a establecer en una red inalámbrica.

Es conocido que Internet no es segura en muchos aspectos, de ahí la necesidad de disponer de herramientas, basadas en algoritmos criptográficos, que permitan proteger la información que se intercambia.

Ej.

Podemos estar enviando un número de tarjeta de crédito para efectuar un pago a una tienda virtual en la que estamos haciendo una compra por Internet, y esta información debe estar protegida para que no sea apropiada de forma indebida.

Además, cada vez con más asiduidad, se está utilizando Internet para determinadas transacciones en las que es importante que el emisor esté bien identificado por el receptor cuando lleve a cabo una determinada operación, para que no pueda darse el caso de suplantación de su identidad.

Y también al revés, que, cuando estamos haciendo alguna compra por Internet, una operación de comercio electrónico (*e-commerce*), deberemos asegurarnos de que la tienda virtual sea realmente la que dice ser, y no se trate de un fraude.

Muchas de estas situaciones se pueden llegar a resolver implementando protocolos de comunicación segura usando la criptografía. De este modo, la seguridad de estos protocolos recae, directamente, en las propias técnicas criptográficas que se utilicen. Su finalidad es que se efectúen transmisiones seguras a través de las redes de comunicaciones.

Al final del tema, encontrarás una actividad para desarrollar que te permitirá conocer si has asimilado los conceptos trabajados en él mismo.

Principios

Los servicios de seguridad que deben proponer las redes de comunicaciones pueden resumirse en la siguiente tabla.

Servicios	Significado
Confidencialidad	Que sólo las personas o máquinas autorizadas puedan acceder a la información transmitida. Por lo tanto, se deberán proteger los contenidos de los mensajes y las identidades del emisor y del receptor.
Integridad	La información debe ser transmitida sin que llegue a ser modificada por otro usuario antes de llegar a su destino.
Autenticación	El emisor del mensaje debe estar correctamente identificado, al igual que el receptor.
No repudio	Si realmente se ha efectuado una transmisión de información entre un emisor y un receptor, debe quedar constancia de la misma, de forma que ni el uno y el otro lo puedan negar.
Control de acceso	Sólo los usuarios autorizados deberán tener permiso para acceder a ciertos recursos del sistema.
Disponibilidad	El sistema no puede dejar de funcionar (ni total ni parcialmente) a raíz de actuaciones de usuarios no autorizados.

De esta forma, hablaremos de sistemas que aseguran la **confidencialidad** y la integridad de la información, por ejemplo en operaciones de comercio electrónico, o la **autenticación**, como, por ejemplo, cuando efectuamos trámites con la Administración (declaración de la renta, obtención de datos mediante nuestro e-dni –dni electrónico...). Existen situaciones en las que es más importante la autenticación que la confidencialidad, por ejemplo, al llevar a cabo gestiones bancarias por Internet.

Criptografía y otras técnicas de ocultación

La palabra **criptografía** proviene de **criptos** (oculto) y **graphos** (escribir). Es la disciplina que se encarga de diseñar procedimientos para ocultar (cifrar) la información a todo aquél que no sea su destinatario.

De forma paralela, se ha ido desarrollando el **criptoanálisis**, ciencia que estudia la forma de romper los algoritmos criptográficos, y así recuperar la información original.

Estas dos parcelas también se engloban dentro de lo que conocemos como **criptología** (viene de **criptos**, oculto, y **logos**, ciencia), disciplina científica que se encarga del estudio de lo relacionado con la confidencialidad en el intercambio de información.

La criptografía no es un concepto nuevo, de nuestra sociedad de la información actual, ya que es tan antigua como la propia escritura. En todos los tiempos se ha tenido la necesidad de ocultar, de una forma u otra, la información escrita. Pero no será hasta el año 1949 que **Claude Shannon** publica la **Teoría de la comunicación de los sistemas secretos**, momento en el que la criptografía pasa a considerarse una ciencia aplicada, con una relación muy directa con otras disciplinas, como la estadística, la teoría de la información...

Claude Shannon



En la actualidad nadie duda de la importancia de la criptografía: para el envío de datos bancarios por Internet, compras por la red utilizando tarjetas, envío de mensajes confidenciales...

Actualmente, en muchos de los procesos de firmado y cifrado de información se utiliza la criptografía **simétrica** y también la **asimétrica**.

■ **Criptografía simétrica o de clave secreta**

En el caso del cifrado simétrico, tanto para el cifrado como para el descifrado se utiliza la misma clave. Así, con una clave, el emisor puede cifrar la información y el receptor podrá descifrarla si también conoce la clave utilizada por el emisor. De este modo, sólo ellos podrán interpretar la información que se envíe.

Algunos métodos basados en criptografía simétrica son: DES, doble DES, triple DES, RC4, RC5, CAST, IDEA, AES...

Estas técnicas se utilizan, primordialmente, para la protección de la información almacenada y/o intercambiada.

■ **Criptografía asimétrica o de clave pública**

En ella se utilizan dos claves, una, que denominaremos clave pública, y otra, que es la clave privada. El emisor cifrará la información utilizando su clave privada (sólo él la conoce) y, al llegar la información cifrada al receptor, éste podrá descifrarla utilizando la clave pública del emisor. Además, cualquier receptor que tenga esta clave pública del emisor podrá recuperar la información. Este tipo de cifrado suele utilizarse para garantizar que detrás del envío está el emisor (el único que ha podido utilizar la correspondiente clave privada para cifrarla).

Algunos métodos que se basan en este tipo de cifrado son: RSA, Diffie-Hellman, DSA, ElGamal...

De este modo, las técnicas de cifrado son indispensables en las redes de ordenadores. Veamos, brevemente, en qué consisten.

También hay técnicas híbridas que utilizan ambos sistemas de encriptación/descriptación.

Existen algunas aplicaciones que permiten cifrar (encriptar) mensajes de correo electrónico y/o ficheros, de forma que sólo puedan acceder a ellos los usuarios que determinemos.

Muchos gestores de correo (como **Outlook** o **Thunderbird**) ya incorporan la posibilidad de encriptación de mensajes, soporte para certificados digitales, para firma digital... que trataremos en un próximo subtema del tema.

Esteganografía

La **esteganografía** es la rama de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba su existencia.

Viene de un tratado de Johannes Trithemius llamado *Steganographia*, del griego 'escritura secreta'. Este tratado habla de la criptografía y de la esteganografía.

La esteganografía es el arte y la ciencia de escribir mensajes secretos de tal forma que nadie, fuera de quien los envía y de quien los recibe, sabe de su existencia; en contraste con la criptografía, en donde la existencia del mensaje es clara, pero su contenido está oculto. Por lo general, un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etc.

Los mensajes, en la esteganografía, muchas veces son cifrados, primero por medios tradicionales, para, posteriormente, ocultarlos, por ejemplo, en un texto que pueda contener dicho mensaje cifrado, resultando el mensaje esteganográfico. Un texto puede ser manipulado en el tamaño de letra, el espaciado, el tipo y otras características para ocultar un mensaje; sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.

En algunos casos, en los que se precise mucha seguridad al compartir la información, se pueden combinar las técnicas criptográficas con los métodos esteganográficos. Primero, se aplicaría algún algoritmo criptográfico y, posteriormente, algún método esteganográfico. Todo ello, para dificultar la interceptación no deseada de la información.

Actualmente, la esteganografía está suscitando mucho interés. En primer lugar, porque las empresas de difusión de información están interesadas en técnicas para ocultar marcas, derechos de autor codificados, números de serie de películas digitales, discos compactos, libros y productos multimedia, y, en segundo lugar, porque, a raíz de las limitaciones que están introduciendo algunos gobiernos en el usos de métodos criptográficos, se están planteando otros métodos de ocultación de mensajes confidenciales.

Aplicaciones

Existen algunas aplicaciones que permiten ocultar información dentro de imágenes.

Entre otras:



Xiao Steganography de <http://www.nakasoft.net/>, se puede descargar de http://www.download.com/Xiao-Steganography/3000-2092_4-10550224.html?tag=pdp_prod, haciendo clic en la opción *Download Now*.

AdaStegano (http://www.canalada.org/recursos/adastegano_win_bin.zip).

A continuación, verás un vídeo tutorial sobre el funcionamiento de **Xiao Steganography**. A una imagen con formato bmp, se le han “incorporado” dos archivos de texto ocultos. La imagen que se obtiene con la información oculta no muestra ningún indicador que permita apreciar esta ocultación de información.

IMAGEN ORIGINAL



IMAGEN CON TEXTO OCULTO



Xiao Steganography



ver simulación

Simulación disponible en la versión web del material

Certificados digitales y firma electrónica

En determinadas operaciones que se efectúan por Internet, es muy importante que el usuario esté bien identificado.

Para la **autenticación** se utilizan los denominados **certificados digitales (certificados electrónicos o certificados de usuario)**.

Un certificado digital es un **documento** electrónico, un fichero intransferible y no modificable, emitido por una tercera entidad de confianza (distinta a la del emisor y receptor), denominada **autoridad de certificación (o prestador de servicios de certificación)**, que asegura que determinadas claves pertenecen a quien realmente deben corresponder (un individuo, una empresa...). La autoridad de certificación lo confirma. Así, este documento identifica a este individuo o a esta empresa a una clave (pública) que se le ha asignado, para poder llevar a cabo procesos de firma y/o cifrado.

Ley de firma electrónica 59/2003



De un modo más formal, según la Ley de firma electrónica 59/2003, un certificado electrónico es un documento firmado, electrónicamente, por un prestador de servicios de certificación que vincula unos datos de verificación de firma (clave pública) a un firmante y confirma su identidad. Según esta misma Ley existen diversos tipos de certificados digitales, que se denominan perfiles de certificados.

Los certificados digitales son muy utilizados en el ámbito de determinadas administraciones para facilitar la ejecución de gestiones a través de la red. Un buen ejemplo de ello lo tenemos en la **Agencia Tributaria**. En este portal podemos encontrar **ayuda adicional para obtener un certificado de usuario**, y así poder llevar a cabo gestiones con la Agencia Tributaria de forma segura por ambas partes.

Agencia Tributaria

The screenshot shows the homepage of the Agencia Tributaria website. At the top, there is a navigation bar with the website name 'www.aeat.es' and the logo. Below the navigation bar, there is a search bar and a 'Oficina Virtual' button. The main content area is divided into several sections: 'Ciudadanos' (Citizens), 'Empresas y profesionales' (Companies and professionals), and 'Colaboradores' (Collaborators). Each section lists various services and documents available. There is also a 'Novedades' (News) section with recent updates and an 'Acceda directamente' (Access directly) section with links to various services like 'A un clic' (One click), 'Calendario del contribuyente' (Taxpayer calendar), and 'Carta de Servicio' (Service card).

Firma electrónica

Éste también es un concepto que va asociado a las técnicas criptográficas, en concreto de la criptografía de clave pública. También es denominado firma digital. La firma electrónica es un medio de identificación del firmante y de su envío.



Cuando un mensaje se ha firmado digitalmente, con posterioridad el destinatario puede asegurarse de que el mensaje que recibe es enviado por quien dice ser el remitente.

La firma digital no implica que el mensaje esté cifrado; es decir, un mensaje firmado podría ser legible, dependiendo de si está cifrado o no.

El firmante, antes de enviar el mensaje, generará un “resumen” o huella digital del mensaje mediante una función. Este resumen o huella digital, los cifrará con su clave privada. El resultado es lo que se denomina firma digital y se enviará de forma adjunta al mensaje original.

Quien reciba el mensaje podrá comprobar dos cosas. Por un lado, que el mensaje no fue modificado desde que se creó (porque podrá generar el mismo resumen o la misma huella digital aplicando la misma función al mensaje) y, por el otro, podrá comprobar su autoría, descifrando la firma digital con la clave pública del firmante que le ha enviado el mensaje firmado, lo que dará como resultado, de nuevo, el resumen o la huella digital del mensaje.

Existen **utilidades** que permiten asegurar la confidencialidad y la autenticidad de nuestros correos mediante la **firma y encriptación** de los mismos. Una empresa concreta (de hecho es una entidad certificadora) que lo facilita es **Thawte**.



<http://www.thawte.com/email/index.html>

Para enviar mensajes encriptados y firmados, podemos hacerlo con el propio **Outlook Express** con la certificación de **Thawte** después de completar el proceso de alta, que nos instala en nuestro PC una clave privada y otra pública.

Un buen ejemplo de la utilidad de los certificados digitales y la firma electrónica la tenemos en el nuevo **DNIE** (DNI electrónico). Este carnet, además de incorporar los datos de identificación personal, incorpora un chip electrónico con los datos del titular, su foto, la imagen digitalizada de la firma manuscrita, la huella dactilar y los certificados electrónicos de autenticación y firma electrónica reconocida. Así, este documento permite efectuar transacciones telemáticas con la Administración.



Se puede obtener más información sobre este documento en:
www.dnielectronico.es

Las transacciones comerciales

Es evidente que Internet se ha convertido en un medio excelente para la realización de transacciones (compras, ventas...), en definitiva, para el comercio electrónico.

De este modo, y de forma paralela, se han ido desarrollando protocolos que nos aseguran la seguridad (confidencialidad y autenticidad) de estas transacciones.

El **protocolo SSL** (*secure socket layer*) es uno de los más utilizados. Seguro que al hacer alguna compra hemos visto que en la parte inferior del navegador aparece un **candado**, y que, incluso, la dirección URL queda modificada en su inicio (**https** en lugar de **http**). Veamos en qué consiste este protocolo, detallando, brevemente, su funcionamiento interno.

SSL son unos protocolos desarrollados originariamente por Netscape que ofrecen conexiones seguras a cualquier aplicación. Ofrece todos los niveles de seguridad exigidos:

- **confidencialidad,**
- **integridad y**
- **autenticidad.**

Es un protocolo que utiliza encriptación simétrica (encriptación del mensaje), asimétrica (encriptación de las claves) y función **hash**.

SSL incluye dos subprotocolos:

- **SSL record protocol** (protocolo de registro SSL) y
- **SSL handshake protocol** (handshake significa "apretón de manos", lo que nos da una idea de su función).



SSL permite garantizar la autenticidad del servidor, la privacidad de la transferencia y la integridad del mensaje.

El primer paso que da SSL es poner de acuerdo al cliente y al servidor en el tipo de algoritmos que se va a utilizar. Una vez hecha esta tarea, se procede al intercambio de la clave simétrica. A partir de este punto, se generan las claves de sesión que se utilizarán para cifrar los datos. Se procede a la verificación del servidor ante el cliente, se realiza la autenticación del cliente y se finaliza el proceso.

Ej.

Muchas tiendas virtuales utilizan este protocolo.

Un ejemplo concreto es: www.elcorteingles.es

En esta web, se comenta: *“las transacciones comerciales son realizadas en un entorno de servidor seguro bajo protocolo SSL (Secure Socket Layer) y todas las comunicaciones se transmiten encriptadas bajo un cifrado de 128 bits, que asegura el mayor nivel de protección a las comunicaciones.”*

Seguridad en comunicaciones inalámbricas

Las comunicaciones inalámbricas, sin cables, por el medio que utilizan, suelen ser muy vulnerables en temas de seguridad. Nuestros datos irán emitiéndose a través del aire vía ondas de radio, de manera que cualquiera puede interceptarlos o, incluso, “introducirse” dentro de nuestra red.

Por esta razón, los puntos de acceso o los enrutadores inalámbricos, que nos permiten acceder a la red, se deberían configurar dotándolos de un buen nivel de seguridad para nuestras comunicaciones inalámbricas.

Para entrar en la configuración del punto de acceso o del enrutador, deberemos conocer su dirección IP dentro de la red y la contraseña a fin de poder entrar en su configuración. Si queremos conocer esta información, deberemos consultar el manual de funcionamiento de estos dispositivos.

Ej.

El punto de acceso inalámbrico **WAP54G de Cisco Systems** [link 158], familia Linksys, permite la conexión de usuarios remotos mediante los protocolos IEEE 802.11g y b.

En la web de este fabricante, también puedes encontrar enrutadores (routers) como el modelo: **WRT54G**, con un formato físico muy parecido al del punto de acceso.

WAP54G de Cisco Systems

Su manual de funcionamiento, lo puedes localizar dentro de la web del fabricante (buscando este producto dentro de productos inalámbricos / red básica / puntos de acceso): <http://www-es.linksys.com/>

Hemos de tener en cuenta que, a menudo, en la configuración por defecto de estos puntos de acceso y enrutadores inalámbricos, no hay ningún tipo de autenticación para conectarnos a la red inalámbricas. De este modo, cualquier usuario que se encuentre en el campo de acción del punto de acceso o del router podría conectarse, directamente, a nuestra red y utilizar, por ejemplo, nuestra conexión a Internet. No es nada recomendable mantenerlo así.

La autenticación a la red inalámbrica deber efectuarse de forma segura utilizando alguno de estos tipos de autenticación.

Control de acceso por dirección MAC

Dentro del punto de acceso o del enrutador, se activará este tipo de control de acceso, y se irán introduciendo las direcciones MAC de cada uno de los equipos o dispositivos que queremos autorizar para conectarse y trabajar con nuestra red. Una dirección MAC de una tarjeta de red es un valor numérico que lo identifica de forma única. Tendrá este formato: 00:0E:1F:D6:E5:C2.

Por ejemplo, en el caso de que tengamos un punto de acceso del tipo **WAP54G** de Cisco Systems de la familia Linksys, al entrar en la **configuración** de este punto de acceso podríamos activarlo:

- En el apartado **Wireless / Wireless Mac Filter**, tenemos la opción de activarlo, de manera que sólo daremos acceso a este punto de acceso a los equipos que tengan una de las direcciones MAC introducidas.



Haciendo clic en **Edit Mac Filter List** podríamos introducir estas direcciones MAC.

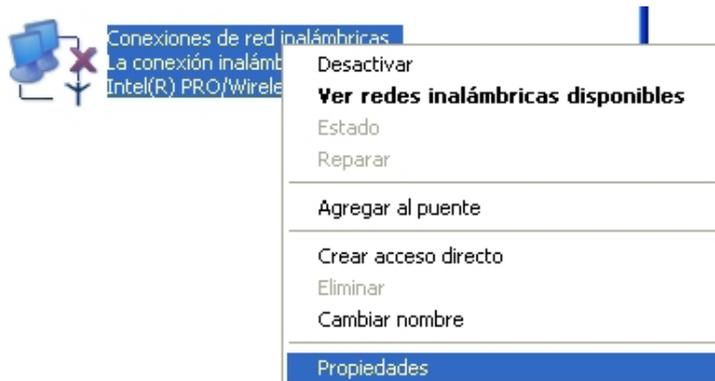
En el caso de no tener, exactamente, este modelo, el proceso para introducir las direcciones MAC será parecido. Puede ser de utilidad, tanto para entrar en la configuración del router como para localizar estas opciones, consultar el manual del fabricante.



Antes de hacer cualquier cambio en la configuración del punto de acceso (o, si es el caso, del enrutador inalámbrico), es importante anotarse la configuración previa, para, en caso de posteriores dificultades, poder llegar a restablecer la situación inicial.

Así, cada vez que un dispositivo (con su correspondiente tarjeta de red integrada) desee conectarse al punto de acceso o al enrutador, éste comprobará que su dirección MAC está dada de alta en la lista introducida dentro de la configuración del punto de acceso.

Para poder dar de alta una dirección MAC de la tarjeta de red de nuestro dispositivo, es necesario que antes tengamos este valor. Si se trata de un equipo con Windows XP, podemos localizarlo en: **Inicio / Panel de Control / Conexiones de Red**.

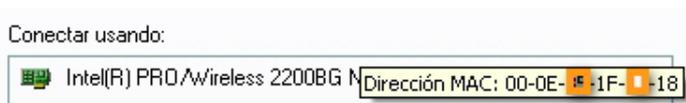


Deberemos localizar el icono de las **Conexiones de red inalámbricas**, y haremos clic sobre él mismo con el botón derecho del ratón y, posteriormente, sobre la opción **Propiedades** del menú contextual que se abrirá.

Nos aparecerá el cuadro de diálogo **Propiedades de Conexiones de red inalámbricas**:



Al mover el cursor del ratón sobre el tipo de tarjeta de red que utiliza el equipo, veremos su **dirección MAC**.



También podemos ver las direcciones MAC de todos los controladores ejecutando el comando **getmac** desde **Inicio/Todos los programas/Accesorios/Símbolo de sistema**.

Y éste será el valor que deberemos dar de alta en el punto de acceso o dentro del enrutador inalámbrico.

Ej.

Dentro del router **ZyXel**, ésta es la ventana de **configuración de las direcciones MAC** (en esta imagen podemos ver que en este router no está activada esta opción de seguridad):



Autenticación por clave WEP (wired equivalent privacy)

Se trata de configurar el punto de acceso o el enrutador con una clave denominada clave WEP. Se podrá escoger entre una longitud de 64 ó de 128 bits. A menudo, esta clave se genera a partir de una palabra clave, pero tengamos en cuenta que, si queremos utilizar esta clave en el dispositivo que se tenga que conectar a la red inalámbrica, deberemos introducir el valor generado, y no directamente la palabra clave que hemos utilizado. De este modo, cuando un equipo quiera entrar en la red inalámbrica, el punto de acceso les solicitará esta clave WEP.

No es un método cien por cien seguro, ya que utiliza claves estáticas (fijas), haciéndolo vulnerable.

Ej.

Entrando en la configuración del punto de acceso **WAP54G** Linksys, al entrar en la **configuración** de este punto de acceso, tendremos la posibilidad de activar esta opción:



En el apartado **Wireless / Wireless Security** vemos que tenemos activado el modo de seguridad **WEP** con clave de 64 bits, generada con una palabra clave. La palabra clave se localizará en el campo **Key 1**.

Otras opciones de **modo de seguridad (security mode)** que podríamos escoger en lugar de WEP, son:

■ Disable

■ **WPA Pre-Shared Key**

Es una evolución del anterior. Utiliza claves dinámicas, que van cambiando cada cierto tiempo. Por lo tanto, mejora la seguridad.

Para poder acceder a la red, será necesario disponer de una clave de acceso que se introducirá en la configuración del punto de acceso o del enrutador inalámbrico.

■ WPA RADIUS

■ RADIUS

RADIUS es el acrónimo de *remote authentication dial-in user service*. Es un sistema de autenticación que autoriza a distintos usuarios a entrar en él. Cada usuario deberá ser dado de alta en un servidor (denominado servidor RADIUS), con un nombre de usuario de identificación y una contraseña.

La mejora en este tipo de autenticación radica en que el usuario, además de necesitar su identificador y contraseña, precisará un certificado válido emitido por este servidor de autenticación.

Configuración de la seguridad inalámbrica mediante Windows XP

Windows XP incorpora un **asistente** que nos permite efectuar la configuración de una red inalámbrica, dotándola de medidas de seguridad.

Podemos acceder a este asistente si abrimos el **Panel de control**, y desde su **vista clásica** accederemos a **Configurar red inalámbrica**.

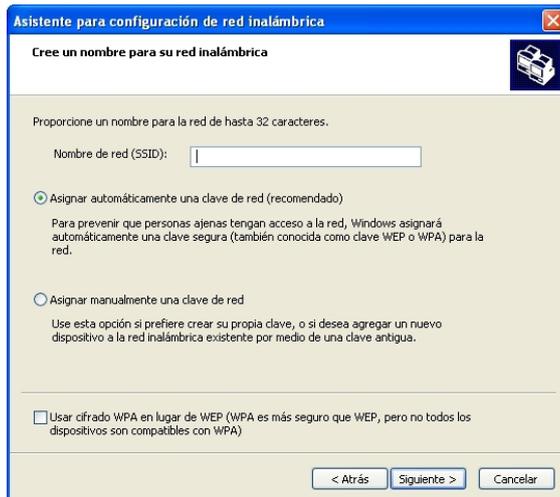
También desde la **vista por categorías**, dentro de Conexiones de red e Internet, veremos la misma opción.



Al hacer doble clic sobre esta opción, se nos abrirá el asistente que nos guiará en la configuración de la red inalámbrica:



En primer lugar, nos solicitará el **SSID (Service Set Identifier)** de la red; en definitiva, un nombre para la red, con una clave que será utilizada para configurar la seguridad inalámbrica. Esta clave, la deberemos anotar, ya que la necesitaremos para configurar otros equipos de la red inalámbrica. De este modo, nos aseguramos de que nadie podrá entrar en nuestra red a no ser que conozca esta clave.



SSID

A lo largo del proceso de configuración irán apareciendo términos como los que hemos ido tratando a lo largo del tema: distintos tipos de seguridad inalámbrica...

Actividades

Indica si los siguientes enunciados son verdaderos o falsos.

	V	F
La confidencialidad hace referencia a que el emisor del mensaje debe estar correctamente identificado, al igual que el receptor.		
La integridad hace referencia a que la información debe ser transmitida sin que llegue a ser modificada por otro usuario antes de llegar a su destino.		
La autenticación hace referencia a que sólo las personas o máquinas autorizadas puedan acceder a la información transmitida. Por lo tanto, se deberán proteger contenidos de los mensajes y las identidades del emisor y del receptor.		
Al hecho de que, si realmente se ha efectuado una transmisión de información entre un emisor y un receptor, debe quedar constancia de la misma, de forma que ni el uno y el otro lo puedan negar, se le denomina disponibilidad.		
AES es un método basado en criptografía asimétrica.		
La criptografía asimétrica se suele utilizar para autenticar mensajes.		
La esteganografía es la rama de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba su existencia.		
El protocolo SSL (<i>secure socket layer</i>) es uno de los protocolos utilizados en transacciones comerciales por Internet.		
Para obtener un certificado digital no es necesario ninguna autoridad de certificación que lo certifique.		
Si tenemos un mensaje firmado digitalmente , también deberá estar cifrado y, por lo tanto, su contenido no será legible.		
Thawte es una entidad certificadora.		
Las comunicaciones inalámbricas , por el medio que utilizan, suelen ser muy vulnerables en temas de seguridad.		
Si ejecutamos getmac , podremos observar el valor de las direcciones MAC de los distintos controladores de nuestro equipo.		
WEP es más seguro que WPA .		

Tecnología digital II

PRÁCTICA FINAL

1. Escoge uno de los sistemas operativos que aparecen en el apartado de **evolución de los sistemas operativos de ordenadores personales** y amplía la lista de sus características. Para ello, deberás hacer una búsqueda en Internet.
2. Haz una pequeña comparativa entre tres **distribuciones Linux**, una de las cuales deberá ser **Ubuntu**. Puedes detallar aspectos de funcionamiento, quien las distribuye...
3. Haz un recorrido por la aplicación **Paseo por Windows XP**.
4. Escoge una de las **ayudas** que facilita el sistema operativo (dentro del **Centro de ayuda y soporte técnico**) y presenta su contenido.



5. Debes ir al panel de control de tu equipo y presentar cómo tienes configurada la aplicación de las **Actualizaciones automáticas**.
6. Localiza en Internet y presenta una aplicación que sea un **programa alternativo a uno de los que incorpora Windows XP** (que no sean los que se muestran en el tema 1 del módulo, apartado programas alternativos a los propios de XP).
7. Recuerda alguna situación problemática que te haya ocurrido con el sistema operativo, y mediante el **solucionador de problemas de Windows** presenta la posible solución. Si no recuerdas ninguna, puedes acceder, directamente, a este solucionador y presentar una de las soluciones a un hipotético problema.
8. ¿Cuál es el **sistema de archivos** que utiliza tu disco duro (o discos duros, si tienes más de uno)?
9. Con el **liberador de espacio de disco**, elimina los archivos temporales de tu disco duro.
10. Utiliza **ScanDisk** para localizar y reparar errores en tu disco duro.
11. Crea un **punto de restauración** en tu equipo. En el nombre, incluye la fecha en que lo has creado.

12. Desde tareas programadas del sistema operativo, debes comprobar si tienes alguna **tarea programada**. Valora si la eliminas, la modificas o la mantienes.
13. Agrega una **tarea programada** para que un determinado programa de tu ordenador se ejecute con una cierta periodicidad.
14. Anota los parámetros que tienes en tu equipo de tu conexión de red. Para ello deberás localizar **Propiedades de TCP/IP**.
15. Accede a los parámetros de configuración del enrutador (**router**) con el que te conectas a Internet y anota o imprime todos sus parámetros de configuración.
16. Utilizando el comando **netstat**, muestra en una tabla unas cinco conexiones de red establecidas y el significado de la información obtenida (direcciones, red a la que pertenecen detallando su clase, detalle de los puertos, protocolos...).
17. ¿Qué otros elementos facilita el programa **Everest** relacionados con redes? Presenta algunas capturas de pantalla con esta información.
18. Cita dos de las utilidades más interesantes que le encuentras al programa Everest.
19. En el caso de tener el equipo conectado a una red local, ¿cuál es el adaptador que utiliza? ¿cuál es el fabricante? ¿cuáles son las direcciones de red? Complementa los resultados que presentes mediante capturas de pantalla. **Observación:** Puedes disponer de esta información a partir de la aplicación **Everest**.
20. Una vez seleccionada una de las aplicaciones que nos permiten conocer los elementos de una red (**Look@LAN Network Monitor** o **Network-View**), presenta uno de los informes con las características de tu red.
21. Cita dos de las utilidades más interesantes que pueden tener este tipo de aplicaciones para un determinado ámbito que también deberás detallar.
22. ¿Qué **aplicación criptográfica** utilizarías si deseas enviar mensajes o contenido de mensajes encriptados y firmados? Además, deberás valorar si permite una firma digital de los mismos.
23. Presenta algunos detalles de funcionamiento de una **aplicación esteganográfica** con algunas capturas de pantalla.
24. La seguridad es un punto que se debe tener muy en cuenta en toda instalación inalámbrica. Después de escoger un **punto de acceso** o **enrutador inalámbrico ADSL** concreto (puede ser el que tengas instalado, o uno en el que estés interesado) de un fabricante concreto (D-link, Linksys, 3com...). Revisa las especificaciones técnicas que aparecen en la web de este fabricante y detalla los protocolos de seguridad que se pueden activar en este dispositivo. Para ello, deberás consultar los protocolos que se han presentado en el tema 5, apartado sobre seguridad en comunicaciones inalámbricas.
25. En el caso de disponer de un **enrutador (router) inalámbrico**, accede a su configuración y anota qué tipo de seguridad inalámbrica implementa.

Tecnología digital II

IDEAS CLAVE

En este módulo seguiremos profundizando en aspectos relacionados con la tecnología digital. Empezaremos haciendo un recorrido por la historia de los sistemas operativos con la finalidad de poder llegar a conocer su evolución. En este contexto, se hace necesario hablar del sistema operativo Linux, enumerando algunas de sus distribuciones. Además, veremos que existen algunas aplicaciones que son programas alternativos a los que nos ofrece Windows XP.

Para poder hacer un buen mantenimiento, y así mejorar el rendimiento de nuestro equipo, presentaremos consejos y herramientas que en algún momento nos pueden llegar a ser muy útiles: liberación de espacio de disco, desfragmentación del disco duro, scandisk, limpieza del registro... En este contexto, empezaremos con una breve introducción sobre términos, como particiones y formatos de disco, y más hacia el final de este tema trataremos de la herramienta de restauración del sistema, que nos permite crear puntos de restauración para poder llegar a restablecer el sistema en el caso de que éste sufra algún daño. También, en este apartado, veremos cómo las tareas programadas son una herramienta que nos permite automatizar la ejecución de determinadas aplicaciones.

El montaje y la configuración de una red local también se tratarán en este bloque: desde los elementos hardware necesarios hasta detalles de configuración de esta red y del enrutador. Como complemento a este tema, se presentan algunas herramientas que permiten conocer los elementos de una red: analizadores del sistema, utilidades dentro del sistema operativo y utilidades más específicas.

Finalmente, para seguir ampliando el abanico de competencias relacionadas con la seguridad informática, abordaremos algunos aspectos más avanzados de seguridad; en concreto, la seguridad en las comunicaciones. Iniciaremos el tema presentando algunos conceptos clave en seguridad, y también haremos una pequeña descripción de algunas de las técnicas criptográficas que se utilizan.

La seguridad en las transacciones comerciales, los certificados digitales, la firma digital, la seguridad en comunicaciones inalámbricas, son temas que se tratan en esta última parte del módulo como aplicación directa de técnicas criptográficas.

Tecnología digital II

SOLUCIONES ACTIVIDADES

Sistemas operativos

	V	F
La versión Windows 95 elevó el nivel de popularidad del sistema operativo Windows.	X	
Windows XP integra prestaciones de Windows NT con las de las versiones de Windows 9.x	X	
Linux , al igual que Windows XP, es un sistema operativo.	X	
Existen muchas distribuciones de Linux, entre ellas: Red Hat, Debian, Suse...	X	
Un Live-CD con Linux nos permite efectuar una copia de seguridad.		X
En Inicio/Panel de control , encontraremos Ayuda y soporte técnico sobre el sistema operativo.	X	
Los denominados Service Pack permiten la instalación directa de todo un grupo de actualizaciones para el sistema operativo.	X	
Si escogemos una configuración para las actualizaciones automáticas, ya no la podremos cambiar.		X
Antes de activar alguna de las actualizaciones, es recomendable que nos documentemos de los posibles problemas que podamos encontrarnos al instalarla.	X	
Existen programas alternativos a los que ya incorpora el sistema operativo Windows XP, que podemos tener también instalados en nuestro equipo.	X	

Feedback 6 o más respuestas correctas: Muy bien. Has entendido de forma correcta los conceptos de este tema.

Feedback menos de 6 respuestas correctas: Deberías repasar este tema antes de continuar, porque no tienes claros algunos conceptos.

Mantenimiento y configuración avanzada del sistema

	V	F
Cuando algo no nos funciona en nuestro equipo, lo más probable es que sea un error de hardware.		X
La tecla F8 nos servirá para reiniciar el ordenador.		X
Mediante la combinación de teclas Ctrl - Alt - Supr podemos acceder al <i>Administrador de tareas del Windows</i> .	X	
El <i>Administrador de tareas del Windows</i> nos permite comprobar si hay alguna tarea bloqueada.	X	
Windows dispone de una ayuda que nos permite obtener la posible solución de un problema.	X	
No hay posibilidad de cambiar las particiones de un disco cuando éste ya está en funcionamiento, y por lo tanto ya tiene guardada información.		X
Antes de formatear un disco, debemos tener muy en cuenta que, si lo hacemos, perderemos toda la información (documentos, aplicaciones, datos...) que tenga guardada.	X	
Regcleaner es una herramienta del sistema operativo que nos permite limpiar el disco duro de archivos temporales.		X
La desfragmentación consiste en que los archivos, en lugar de quedar esparcidos por distintos espacios del disco duro, se compacten y queden mejor organizados.	X	
Scandisk sirve para comprobar errores en el disco.	X	
La herramienta <i>Restaurar el sistema</i> lo supervisa, pero no anota los parámetros de configuración de nuestro sistema.		X
La manipulación del <i>registro del sistema</i> es un tema delicado, por lo que se recomienda que antes de efectuar cualquier cambio en el registro, se haga una copia de seguridad de los datos importantes del equipo.	X	
La función del sistema operativo denominada <i>Tareas programadas</i> permite programar que ciertas tareas se ejecuten, automáticamente, en nuestro equipo en un momento determinado.	X	

Feedback 8 o más respuestas correctas: Muy bien. Has entendido de forma correcta los conceptos de este tema.

Feedback menos de 8 respuestas correctas: Deberías repasar este tema antes de continuar, porque no tienes claros algunos conceptos.

Montar y configurar una red doméstica

	V	F
La terminación del cable de red se denomina RJ45.	X	
El protocolo TCP/IP (<i>transport control protocol / Internet protocol</i>) define un conjunto de normas que rigen la transmisión de datos entre ordenadores conectados a Internet.	X	
Everest es un programa que se utiliza para configurar una red.		X
Tcpip configura es la aplicación del sistema operativo que nos puede ser de utilidad para solucionar un problema de red TCP/IP, ya que nos permite comprobar la configuración de TCP/IP en el equipo que tiene el problema.		X
Abriendo el navegador e introduciendo la dirección IP podremos acceder (si conocemos el usuario y la contraseña) a la configuración interna del enrutador .	X	
Ping permite comprobar si un equipo o dispositivo de la red, con una IP asignada, se encuentra activo dentro de esta red.	X	
Netstat es una herramienta del sistema operativo que nos puede mostrar las conexiones de red que tenemos en cada momento.	X	
La utilidad tracert permite ver por qué routers (o encaminadores) pasa una conexión Internet.	X	
Con el programa NetworkView podemos trazar, en poco tiempo, un completo esquema de nuestra red local.	X	

Feedback 5 o más respuestas correctas: Muy bien. Has entendido de forma correcta los conceptos de este tema.

Feedback menos de 5 respuestas correctas: Deberías repasar este tema antes de continuar, porque no tienes claros algunos conceptos.

Seguridad en las comunicaciones

	V	F
La confidencialidad hace referencia a que el emisor del mensaje debe estar correctamente identificado, al igual que el receptor.		X
La integridad hace referencia a que la información debe ser transmitida sin que llegue a ser modificada por otro usuario antes de llegar a su destino.	X	
La autenticación hace referencia a que sólo las personas o máquinas autorizadas puedan acceder a la información transmitida. Por lo tanto, se deberán proteger contenidos de los mensajes y las identidades del emisor y del receptor.		X
Al hecho de que, si realmente se ha efectuado una transmisión de información entre un emisor y un receptor, debe quedar constancia de la misma, de forma que ni el uno y el otro lo puedan negar, se le denomina disponibilidad.		X
AES es un método basado en criptografía asimétrica.		X
La criptografía asimétrica se suele utilizar para autenticar mensajes.	X	
La esteganografía es la rama de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba su existencia.	X	
El protocolo SSL (<i>secure socket layer</i>) es uno de los protocolos utilizados en transacciones comerciales por Internet.	X	
Para obtener un certificado digital no es necesario ninguna autoridad de certificación que lo certifique.		X
Si tenemos un mensaje firmado digitalmente , también deberá estar cifrado y, por lo tanto, su contenido no será legible.		X
Thawte es una entidad certificadora.	X	
Las comunicaciones inalámbricas , por el medio que utilizan, suelen ser muy vulnerables en temas de seguridad.		X
Si ejecutamos getmac , podremos observar el valor de las direcciones MAC de los distintos controladores de nuestro equipo.	X	
WEP es más seguro que WPA .		X

Feedback 8 o más respuestas correctas: Muy bien. Has entendido de forma correcta los conceptos de este tema.

Feedback menos de 8 respuestas correctas: Deberías repasar este tema antes de continuar, porque no tienes claros algunos conceptos.

Tecnología digital II

GLOSARIO

Actualizaciones del sistema operativo

Reemplazan o añadiendo archivos para lograr un mejor funcionamiento del sistema. Algunas de estas actualizaciones resuelven problemas de seguridad.

Administrador de dispositivos

Herramienta del sistema operativo con la que se pueden administrar los dispositivos del equipo. Con el Administrador de dispositivos podemos ver y cambiar las propiedades de cada dispositivo, actualizar sus controladores y configurar y desinstalar dispositivos.

ADSL (*asymmetric digital subscriber line*)

Tecnología que permite conectar un router a la línea telefónica convencional, o de par de cobre, y transmitir información a velocidades de 1 a 9 Mbps al usuario y de 16 a 800 Kbps de éste al servidor. Con ésta, se consigue una velocidad mucho más alta que con los módems habituales. La distancia a la central y la calidad de la línea telefónica determinan la velocidad de transmisión real.

Asistente

Los asistentes son aplicaciones del sistema operativo que nos ayudarán en algunos de los procesos que debemos llevar a cabo (instalar un periférico, crear una red local...).

Backups

Véase *Copias de seguridad*.

Banda ancha

Sistema de comunicaciones que permite la transferencia de información a gran velocidad, compatible con la retransmisión de voz, imágenes y vídeo casi en tiempo real.

Cable UTP

Cable de par trenzado no apantallado (UTP). Es el cable de red utilizado en redes locales. Su conector (terminación) más frecuente es el RJ45.

Certificado digital

También denominado certificado electrónico o certificado de usuario. Un certificado digital es un documento electrónico, un fichero intransferible y no modificable, emitido por una tercera entidad de confianza (distinta a la del emisor y receptor), denominada autoridad de certificación (o prestador de servicios de certificación), que asegura que determinadas claves pertenecen a quien realmente deben corresponder (un individuo, una empresa...).

Concentrador

Es un dispositivo de red que se utiliza para conectar otros dispositivos o equipos a la red. Cuando un dispositivo emite un mensaje y llega al concentrador, éste lo reenvía a todos los dispositivos o equipos que tenga conectados.

Conmutación de paquetes

Técnica de transmisión en una red en la que los mensajes se dividen en unidades llamadas paquetes, que se envían a través de la red de forma independiente.

Contraseña (password)

Código secreto normalmente alfanumérico utilizado para acceder a un determinado servicio, como el de correo electrónico, acceso a Internet, acceso con un determinado perfil de usuario al sistema operativo...

Copias de seguridad

Selección de archivos que se guardan de forma agrupada, por si, en algún momento, necesitamos recuperarlos.

Cortafuegos o firewall

Dispositivo hardware o software, o una combinación de ambos, destinado a detectar conexiones y comunicaciones por red, dando acceso o bloqueándolas respecto a unas reglas definidas por el usuario. Principalmente, se usa para bloquear intentos de intrusión no deseada a sistemas por parte de terceros.

Criptografía

Ciencia que se encarga de estudiar las técnicas y los algoritmos empleados para encriptar la información antes de ser transmitida o almacenada, de modo que no pueda ser ni modificada ni visualizada por un falso destinatario.

Desfragmentador de disco

Es una utilidad del sistema operativo que permite analizar unidades locales (discos, lápices USB...) y encontrar carpetas y archivos fragmentados. Una vez localizados, posibilita su reagrupación reagruparlos para mejorar el funcionamiento del sistema.

DHCP

Este servidor asigna de manera automática direcciones IP a cada uno de los equipos de la red.

Dirección MAC

Dirección física y única que permite identificar un dispositivo dentro de una red local.

Distribución Linux

Es una variante del sistema Linux, de manera que esté bien adaptada a las necesidades de los usuarios a los que va dirigida.

DNS (domain name server)

Servidor de nombres de dominio. Es el sistema que se utiliza para relacionar el nombre de un equipo con su dirección IP.

Encriptación (cifrado)

Es el tratamiento de un conjunto de datos con la finalidad de impedir que nadie, excepto su destinatario, pueda leerlos.

Enrutador (o router)

Es un dispositivo creado para facilitar la conexión de redes informáticas. La palabra enrutador o router deriva del hecho de que esta máquina pone en ruta, a través de la red, los paquetes de datos que un usuario ha ordenado transmitir.

Esteganografía

Es la técnica que permiten ocultar información dentro de un objeto (fichero, imagen...) de manera que no se perciba su existencia. El destinatario, con el programa y la clave apropiada que le habrá facilitado el emisor, podrá recuperar esta información.

Ethernet

Es un estándar de red de área local. Se corresponde con el estándar IEEE 802.3

Firma digital

Datos que se añaden a un mensaje que permiten al receptor poder comprobar la autenticidad del emisor, protegiendo, al mismo tiempo, el mensaje de falsificaciones.

Freeware

Tipo de software de ordenador que se distribuye de forma gratuita y sin límite de tiempo. Hay programas que, inicialmente, tienen una licencia *freeware* pero que, en nuevas versiones, o más completas, adquieren un carácter comercial y, en consecuencia, pasan a ser de pago. Este software está en contraposición al *shareware*.

GUI

Véase *Interfaz gráfica de usuario*.

Hardware

Término inglés que se usa para referirse a la parte física de un ordenador y, por extensión, a todo dispositivo electrónico relacionado con la informática.

Host

Dispositivo de red con capacidad para ofrecer servicios a un usuario. De este modo, por este nombre podemos tener un ordenador, un servidor de red, etc.

Hub

Véase *Concentrador*.

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

Es la organización encargada de la elaboración de muchas de las normas relativa a redes. Publica los estándares que regulan muchos de los dispositivos que utilizamos, haciendo que entre ellos exista una buena compatibilidad en el caso de que utilicen la misma norma.

Infrarrojos

Es una tecnología por ondas de luz, por lo que requiere que los dispositivos estén próximos y en visión directa. Su alcance suele ser inferior a 1 m. Se suele utilizar en PC portátiles, teléfonos móviles, teclados, cámaras digitales...

Interfaz gráfica de usuario GUI (*graphics user interfaces*)

Permite al usuario comunicarse con el ordenador de forma rápida e intuitiva.

IP

Véase *TCP/IP*.

Liberador de espacio de disco

Es una herramienta del sistema operativo que busca, en la unidad seleccionada, archivos temporales, archivos de caché de Internet y archivos de programa innecesarios que puede eliminar de forma segura. El mismo eliminador, si así lo autoriza el usuario, se encarga de su eliminación.

Linux

Sistema operativo creado por Linus Torvalds. Está basado en Unix. Existen numerosas distribuciones Linux: Red Hat, Suse, Debian..., la mayoría, de software libre.

Live CD o Live DVD

Es un sistema operativo que suele ir acompañado de algunas aplicaciones que se pueden ejecutar, directamente, desde su soporte (CD o DVD) sin que sea necesario efectuar ningún tipo de instalación en el disco duro de la máquina en la que se ejecute. Utiliza la misma memoria RAM como disco duro virtual.

Máscara de subred

Es una dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

MÓDEM

Es un dispositivo que puede o bien estar insertado en la placa base del ordenador, o bien ser externo, que sirve para *modular* y *demodular* una señal portadora de información (de ahí, por contracción de esos términos, el origen del nombre de dispositivo). La aparición de Internet popularizó este dispositivo, ya que era el mecanismo ideal para convertir la señal, transmitida por cables telefónicos, en una señal digital, y por lo tanto comprensible para el ordenador.

P2P

Son redes entre iguales o de igual a igual (en inglés, *peer to peer*). Tienen una serie de nodos que se comportan, simultáneamente, como clientes y servidores de los demás nodos de la red. Se utilizan para compartir archivos.

Panel de control

Es un programa específico incluido en Windows desde su aparición que permite al usuario ajustar y configurar el sistema operativo con el objeto de conseguir una personalización de la interfaz gráfica.

Protocolo

Conjunto de reglas que definen cómo se debe establecer y ordenar la comunicación de datos entre dos o más equipos.

Proveedor de servicios de Internet (ISP)

Son empresas y organizaciones que ofrecen acceso a Internet, además de otros servicios relacionados. Tienen una línea de comunicaciones dedicada, conectada permanentemente a Internet para que sus usuarios puedan acceder a la red.

Puerta de enlace

También conocida con el nombre de gateway. Permite la interconexión de sistemas.

Puerto

Es **una interfaz entre nuestro PC y otro dispositivo**. El puerto puede ser **interno** (son unas ranuras dentro del PC) o **externo** (a través de un conector que se encuentra en la parte trasera del PC). Cada dispositivo se conecta a un puerto u otro.

Punto de restauración

Creado en un momento concreto por el usuario mediante la correspondiente herramienta del sistema operativo, permite restaurar el equipo a un estado anterior en el que funcionaba como se desea.

RADIUS

Son las siglas de *remote authentication dial-in user service* (servicio de autenticación de conexiones de usuarios remotos). Es un protocolo de autenti-

cación y autorización para aplicaciones de acceso a la red. Se emplea como técnica de seguridad en comunicaciones inalámbricas.

Red

Una red informática es una expresión que se usa para hablar de una serie de ordenadores conectados mediante cables, señales, ondas u otros medios que pueden intercambiar información (aplicaciones), compartir recursos (como una impresora) y servicios (acceso a Internet).

Red de área local LAN (local area network)

Comunica ordenadores en una zona limitada, dentro de un edificio o una planta. En la mayoría de casos, esta red está conectada a Internet.

Registro

Controla el funcionamiento del sistema operativo. Son un conjunto de archivos que contienen información acerca de cómo funciona nuestro ordenador. De hecho, es una pequeña base de datos donde el sistema operativo Windows guarda la información sobre la configuración y el comportamiento del sistema operativo, hardware, aplicaciones instaladas, personalizaciones de usuario, etc. El registro es fundamental para el sistema operativo, puesto que, si se daña, podemos tener serios problemas y llegar, incluso, a que el sistema operativo quede inservible.

Router

Véase enrutador.

Service Pack

Conjunto de actualizaciones del sistema operativo.

Shareware

Se aplica a una modalidad de distribución de software que consiste en que el usuario, durante un tiempo limitado, puede utilizar una aplicación para probarla. Pasado este período de tiempo, que puede oscilar entre 30 y 60 días, la aplicación puede dejar de funcionar o de tener habilitadas todas sus funcionalidades. Para rehabilitar las funciones del programa, el usuario deberá pagar por el uso de éste a su creador.

Sistema operativo

Es el programa básico que permite que el usuario pueda comunicarse con la máquina que utiliza un lenguaje binario o digital. El sistema operativo es un programa de carácter general que incluye, habitualmente, otros programas y aplicaciones que tienen una misión concreta, como los procesadores de texto o los programas de retoque de imagen.

Software

Con este término, procedente del inglés, se acostumbra a hacer referencia a los componentes lógicos de los sistemas informáticos. En contraposición a *hardware*, el *software* indica los programas que sirven para hacer funcionar un ordenador. Hay que diferenciar entre el software de sistema, como el sistema operativo, y el software de *aplicación*, que es el que tiene una función más específica.

Switch

Concentrador "inteligente" en una red Ethernet, ya que retransmite la información recibida sólo por el puerto al que se encuentra conectado el equipo al que va dirigida la información.

Tarjeta de red

Permite conectar un dispositivo a la red. También se la conoce como NIC (*network interface card*).

TCP/IP (*transmission control protocol/Internet protocol*)

Grupo de protocolos de comunicación que gobiernan el funcionamiento básico de Internet independientemente del sistema operativo. Son la base de la transmisión y enrutado de la información.

UNIX

Sistema operativo desarrollado por K. Thompson, D. Ritchie y D. McIlroy en 1969.

Updates

Véase *Actualizaciones del sistema operativo*.

WEP

Acrónimo de *wired equivalent privacy*. Es el sistema de cifrado incluido en el estándar IEEE 802.11. Se utiliza en redes inalámbricas como protocolo que permite cifrar la información que se transmite.

Wi-Fi

Acrónimo de *wireless fidelity*. Es una tecnología de comunicación inalámbrica que está regulada bajo la norma IEEE 802.11.

WPA

Acrónimo de *Wi-Fi protected access* (acceso protegido Wi-Fi). Es una evolución del protocolo WEP. Utiliza claves dinámicas que van cambiando cada cierto tiempo.

