

USERS

Redes desde Cero

**Armado y configuración
de redes hogareñas y Wi-Fi**



- /// **Cómo hacer el cableado y la instalación sin complicaciones**
- /// **Configurar y administrar redes inalámbricas**
- /// **Compartir Internet, archivos e impresoras**
- /// **Evitar todo tipo de amenazas de seguridad**
- /// **¡Y mucho más!**

DESCUBRA QUÉ FÁCIL ES REPARAR Y ACTUALIZAR SU PC



Esta obra es fundamental para ganar autonomía al momento de reparar la PC. Aprenderemos a diagnosticar y solucionar las fallas, así como a prevenirlas a través del mantenimiento adecuado, todo explicado en un lenguaje práctico y sencillo.

- » HARDWARE / HOME
- » 192 PÁGINAS
- » ISBN 978-987-1773-01-5



SOBRE LA COLECCIÓN desde **Cero**

- » Aprendizaje práctico, divertido, rápido y sencillo.
- » Lenguaje simple y llano para una comprensión garantizada.
- » Consejos de los expertos para evitar problemas comunes.
- » Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS



LLEGAMOS A TODO EL MUNDO VÍA **»OCA*** Y **DHL****

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

🌐 usershop.redusers.com // ✉ usershop@redusers.com

Redes desde Cero

**Armado y configuración
de redes hogareñas y Wi-Fi**




USERS

TÍTULO: Redes

COLECCIÓN: desde Cero

FORMATO: 15 X 19 cm

PÁGINAS: 192

Copyright © MMX. Es una publicación de Fox Andina en coedición con Gradi S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. No se permite la reproducción parcial o total, el almacenamiento, el alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u otros métodos, sin el permiso previo y escrito del editor. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en XII, MMX.

ISBN 978-987-1773-02-2

Redes / coordinado por Daniel Benchimol. - 1a ed. -

Buenos Aires: Fox Andina;

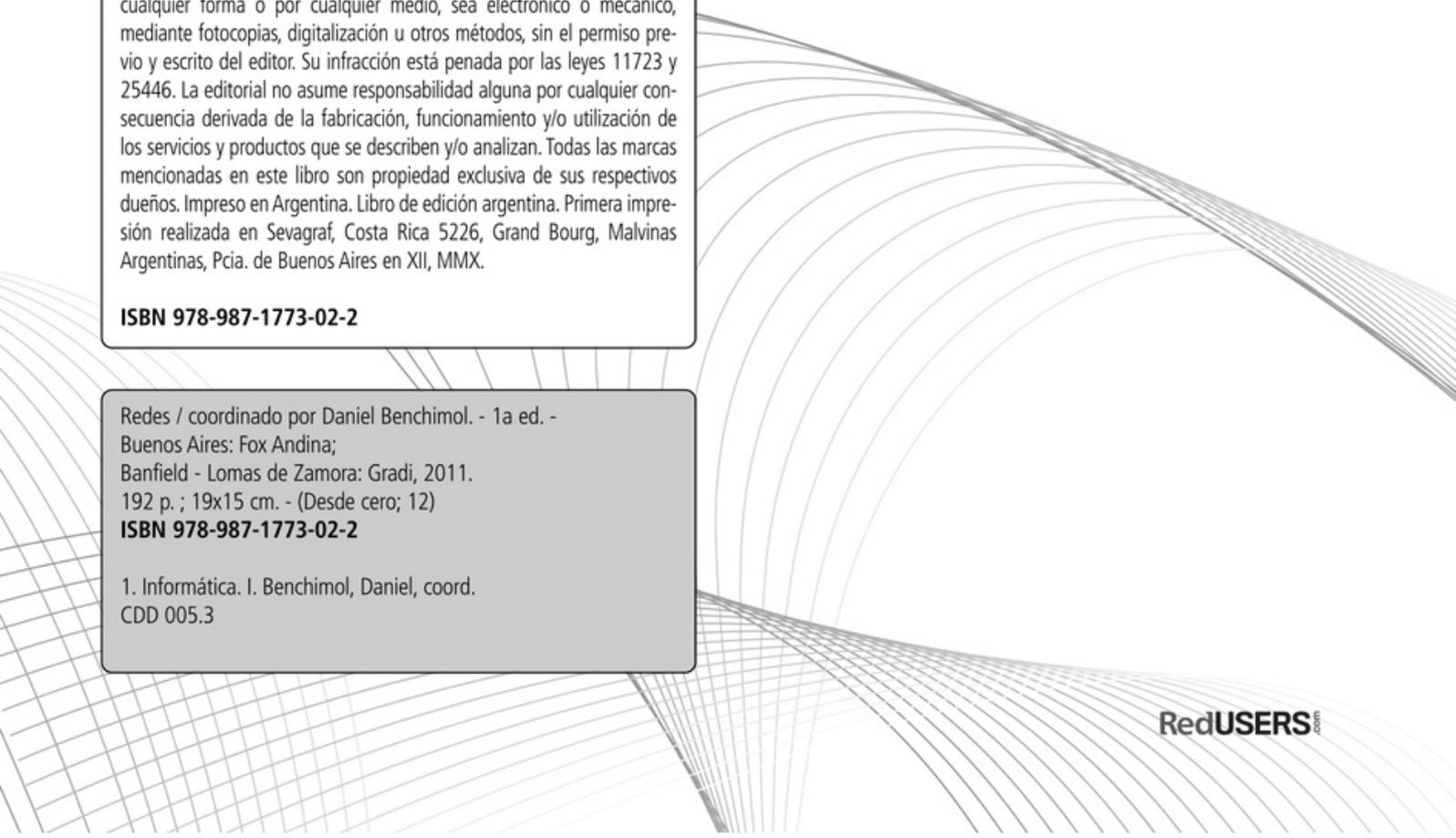
Banfield - Lomas de Zamora: Gradi, 2011.

192 p. ; 19x15 cm. - (Desde cero; 12)

ISBN 978-987-1773-02-2

1. Informática. I. Benchimol, Daniel, coord.

CDD 005.3



RedUSERS^{.com}

Prólogo al contenido

Soy usuario de computadoras personales desde, digamos, el comienzo. Evitaré las polémicas: diré que entiendo por *el comienzo* la época en la que los sistemas operativos en modo gráfico no eran más que ideas fantásticas pensadas por directores de fotografía que hacían películas de ciencia ficción como **Juegos de guerra** o **Jurassic Park**. En estos films, los protagonistas hacían cosas geniales –abrir puertas de secciones alejadas de edificios, jugar con aplicaciones gráficas potentísimas contra contrincantes que habitan el otro extremo del planeta– con las que nosotros, los computómanos jóvenes, ni siquiera podíamos soñar.

La llegada de los sistemas operativos en modo gráfico y la popularización del acceso a las nuevas tecnologías mejoró mucho la situación, pero para cuando se lanzó la primera versión beta de **Windows 2000**, los fanáticos de la tecnología, o al menos muchos de nosotros, creíamos que ya no teníamos nada para aprender.

Fue la entrada al mundo de las redes domésticas lo que lo cambió todo realmente. Conocer los secretos de las configuraciones de redes y estaciones de trabajo, además de aprender a configurar routers, puntos de acceso y adaptadores de red nos tomó a todos cerca de 10 años y, de alguna manera, devolvió a la computación su costado más fascinante y enigmático.

Hoy, diez o doce años después de aquel redescubrimiento, quienes nos especializamos en el periodismo y la pedagogía en el área de tecnologías tenemos como una de nuestras principales metas acercar el manejo de redes a todos los usuarios de computadoras. Porque hoy, conocer cómo aprovechar las ventajas de una red hogareña o de pequeña oficina supone tener al alcance de la mano un potencial con el que los más atrevidos técnicos no podían soñar hace un tiempo.

No hay necesidad de insistir, lo dice más de una canción: el futuro llegó hace rato. Es cuestión de estudiarlo un poco y sacar lo mejor de él.

El libro de un vistazo

Este libro está enfocado a usuarios principiantes e intermedios que deseen aprender cómo reparar y mantener su computadora personal. En cada uno de los capítulos, se estudiarán los diferentes problemas y las soluciones, de diversas partes de la PC: discos ópticos, periféricos, redes, entre otras.

► **CAPÍTULO 1** **¿QUÉ ES UNA RED?**

En este primer capítulo, a modo de introducción, aprenderemos los conceptos básicos sobre las redes informáticas: su utilidad, componentes y tipos. Estudiaremos las redes en acción y, además, aprenderemos los siete niveles del modelo OSI.



► **CAPÍTULO 2** **INSTALACIÓN DE LA RED: PRIMEROS PASOS**

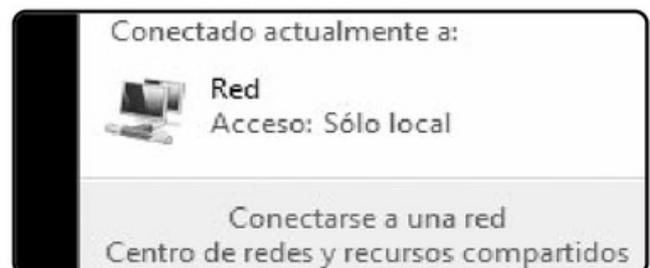
Estudiaremos los primeros pasos de la instalación de la red. Conoceremos las diferencias de los

hubs, respecto de los switches. Aprenderemos a armar un cable de red y analizaremos los elementos necesarios para esto.



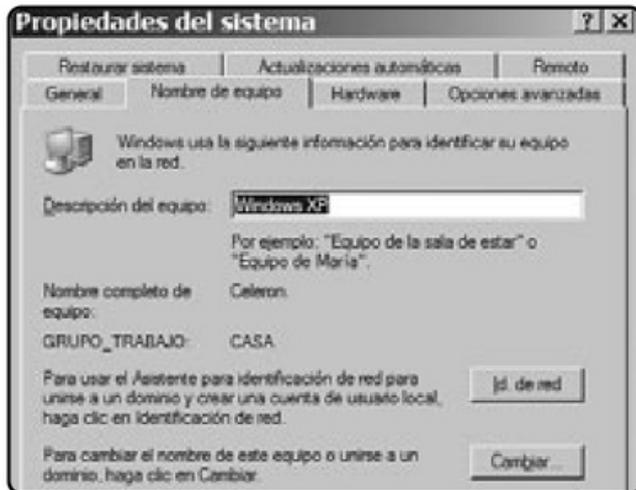
► **CAPÍTULO 3** **CONFIGURACIÓN DE LA RED**

Conoceremos cómo configurar la red. Aprenderemos a conectarnos a la red e instalar el controlador de un dispositivo. Analizaremos todo sobre la dirección IP, DNS, el protocolo TCP/IP, los drivers y los puertos.



▶ **CAPÍTULO 4** **USO DE LA RED**

En este capítulo, dedicado al uso de la red, conoceremos los tipos de ubicaciones, aprenderemos qué es un grupo de trabajo y analizaremos cómo compartir nuestros archivos con otros usuarios. Veremos de qué manera controlar el uso de la impresora compartida.



▶ **CAPÍTULO 5** **REDES WIFI**

Analizaremos las redes WiFi. Estudiaremos los diferentes tipos y, además, aprenderemos a habilitar el filtraje por dirección MAC y a configurar una red ad hoc, entre otros procedimientos útiles.



▶ **CAPÍTULO 6** **INTERNET**

Conoceremos todo sobre Internet: los navegadores y sus diferentes características. También aprenderemos sobre el correo electrónico: Windows Mail y otras opciones disponibles. Además, estudiaremos el concepto de chat con sus alternativas.



▶ **CAPÍTULO 7** **SEGURIDAD**

En este capítulo, dedicado a la seguridad de nuestro sistema informático, aprenderemos a instalar un antivirus, mantener Windows actualizado y realizar backups. Además analizaremos los conceptos de spam, virus, spyware, phishing, firewall, entre otros.

▶ **SERVICIOS** **AL LECTOR**

En este apartado final incluimos el índice temático, que nos permitirá acceder a cualquiera de los temas tratados en esta manual en forma rápida y precisa.

Contenido del libro

Prólogo al contenido	003
El libro de un vistazo	004
Introducción a Redes	010

► CAPÍTULO 1 ¿QUÉ ES UNA RED? 011

¿Qué es una red?	012
La utilidad de las redes	012
Redes en acción	013
• Los 7 niveles del modelo OSI	014
Componentes de una red	015
Tpos de redes	017
Multiple choice	022



► CAPÍTULO 2 INSTALACIÓN DE LA RED: PRIMEROS PASOS 023

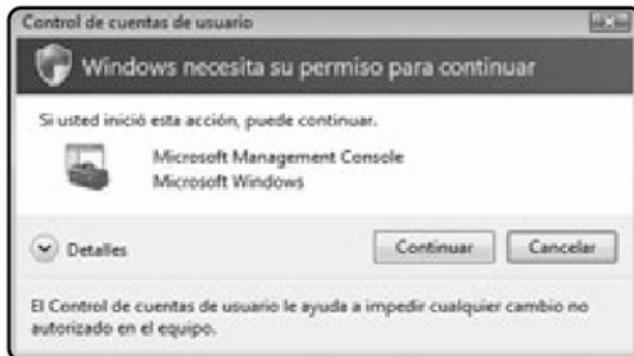
Instalación de la red: primeros pasos	024
Hubs vs. switches	025

Los cables	026
Armar un cable de red	029
De compras	033
Instalar una tarjeta de red interna	036
Multiple choice	040



► CAPÍTULO 3 CONFIGURACIÓN DE LA RED 041

Configuración de la red	042
Drivers, controladores	043
• Comprobar la correcta instalación de los controladores	049
Las propiedades de los controladores	055
Conexiones de red	056
El protocolo TCP/IP	058
• Una gran familia	059
La dirección IP	060
DNS	062
Con ustedes, los puertos	062
Windows Vista y las redes	064
Multiple choice	066



CAPÍTULO 4 **USO DE LA RED** **067**

Uso de la red	068
Tipos de ubicaciones de la red	069
¿Qué es un grupo de trabajo?	070
Configurar un grupo de trabajo	071
Compartir archivos con otros usuarios	072
Compartir los archivos de mi equipo en la red	076
Compartir mis carpetas personales en la red	078
Restringir el acceso al compartir una carpeta	084
Compartir una unidad completa	088
Compartir mi impresora con otros usuarios	091
Acceder a una impresora conectada a otra PC	092
Controlar el uso de mi impresora compartida	093
Multiple choice	096



CAPÍTULO 5 **REDES WIFI** **097**

Redes WiFi	098
Establecer una conexión inalámbrica	101
Configurar el router inalámbrico	102
Evitar que alguien utilice el router sin autorización	104
• Clonar la dirección MAC	109
Proteger mi red	110
Buscar redes, conectarnos a ellas	112
Modificar mis redes inalámbricas	114
Armar una red inalámbrica sin comprar un router	116
Multiple choice	120

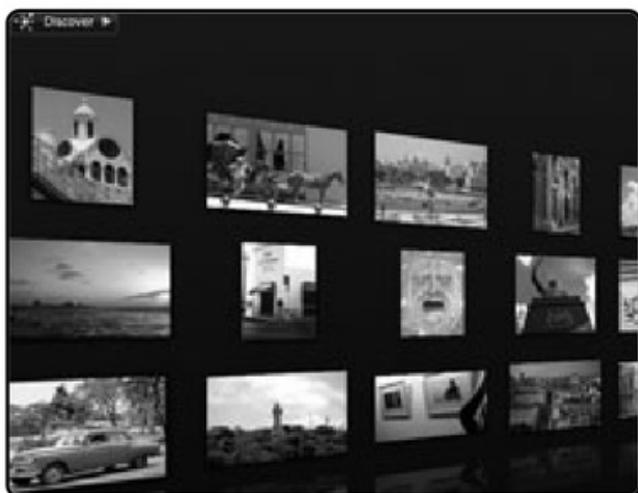


CAPÍTULO 6 **INTERNET** **121**

Internet	122
Conectarse a Internet desde casa	123
¿Necesito permisos para conectarme a Internet?	124
Configurar la conexión a Internet	125

► PRELIMINARES

Configurar la computadora para tener Internet	128
Compartir la conexión a Internet en mi red	129
Configurar el acceso a Internet de los otros equipos	130
Las opciones de Internet en el Panel de control	131
Microsoft Internet Explorer	134
• Configurar Internet Explorer	138
Otros navegadores	140
El correo electrónico	142
Windows Mail	143
Otros clientes de correo para utilizar	144
Chatear con amigos	145
Multiple choice	148



► **CAPÍTULO 7**
SEGURIDAD 149

Seguridad	150
Mantener Windows actualizado	150

El firewall	152
Las cookies	155
El filtro de suplantación de identidad (phishing)	157
Spyware	159
Windows Defender	160
Acerca de los virus informáticos	162
El antivirus	163
Instalar un antivirus en la PC	165
Spam	170
• Combatir el spam	171
Backups	173
Multiple choice	174



► **SERVICIOS**
AL LECTOR 175

Índice temático	176
Sitios web recomendados	179
Catálogo	189



**Desarrollos temáticos
en profundidad**

Libros.

Coleccionables.

**Cursos intensivos
con multimedia**



**Capacitación
dinámica**

Revistas.

Introducción a Redes

Bienvenidos a *Redes desde Cero*, un nuevo volumen de la colección de libros USERS, que nos permitirá aprender todo lo que hay que saber de los temas más importantes de la informática contemporánea de la manera más simple y dinámica.

En *Redes desde Cero*, aprenderemos todo lo que necesitamos saber para armar, configurar, usar y aprovechar al máximo una red hogareña. Empezaremos desde los conceptos más básicos: qué es una red, para qué sirve y de qué manera puede mejorar nuestro trabajo y nuestra cotidianidad informática. Seguiremos con el armado de la red, proceso que explicaremos en detalle y con prácticas guías paso a paso.

Una vez que nuestra red esté montada, con este libro aprenderemos a configurarla y utilizarla. Conoceremos, además, los conceptos más importantes que cualquier usuario que trate con redes informáticas debe manejar y aprenderemos cómo compartir recursos, cómo asegurarlos y cómo ofrecer nuestros contenidos a la red.

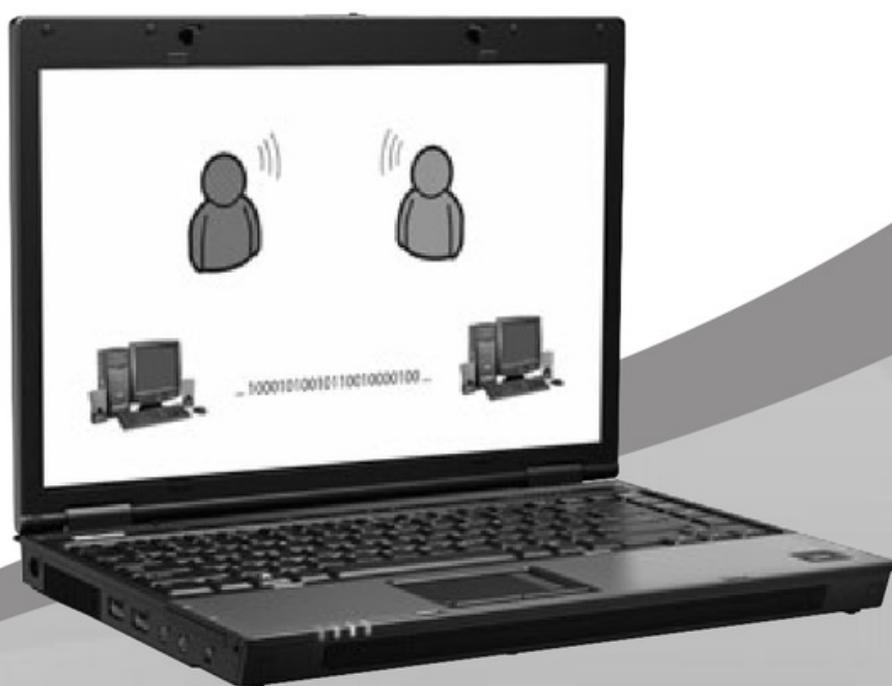
Nada queda afuera de *Redes desde Cero*. Con este libro, aprenderemos también a utilizar y configurar redes inalámbricas, un tipo de red que hasta hace unos años se pensaba como ajeno a las redes cableadas, pero que hoy por hoy no hace más que complementarlas, cuando no prescinde lisa y llanamente de ellas.

Cerraremos este volumen resumiendo los principios de seguridad que debemos conocer para que el uso de la red no suponga un peligro para nuestro equipo, nuestros datos personales y la información que tenemos almacenada en los discos duros de los equipos del grupo de trabajo.

Los lectores de *Redes desde Cero* tendrán la capacidad de manejar sin problemas las redes informáticas y todo el poderío que ellas despliegan, en un mundo donde el acceso a la información es cada día más importante. Por esta razón, este libro, entonces, resulta imprescindible para cualquiera que aún no disfrute del increíble mundo del *networking* o quiera mejorar sus conocimientos al respecto.

Capítulo 1

¿Qué es una red?



Aprenderemos los conceptos básicos sobre las redes informáticas: su utilidad, componentes y tipos.

¿Qué es una red?

Si nos atenemos a la definición que nos proporciona la **Real Academia Española (www.rae.es)**, en su décima acepción encontramos lo siguiente:

10. f. Conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden intercambiar información.

Ya es un buen inicio. El mismo concepto de **red** implica el de pluralidad. No existe una red formada por un equipo, es el **intercambio entre equipos** el que crea una red. Nuestra computadora

recién desembalada no es un equipo en red, pero si la conectamos a Internet lo será. Si no tenemos Internet, pero sincronizamos los contactos de la agenda de nuestro teléfono móvil con la agenda de la computadora, también estamos ante una red (aunque no del tipo del que nos interesa en este libro).

Si no tenemos Internet, pero sí dos computadoras, también podríamos tener una red (esta sí es del tipo que nos interesa). Basta con que dos dispositivos diferentes intercambien información entre ellos para estar en presencia de una red (**Figura 1**).

LA UTILIDAD DE LAS REDES

A partir del momento en que usamos la computadora para conectarnos, ya estamos utilizando las redes. Si tenemos dos computadoras, la red nos va a permitir



FIGURA 1.
Las redes están alrededor nuestro en la actualidad.



compartir recursos entre ellas ¿A qué llamamos un **recurso**? Puede ser una carpeta en el disco duro de otra computadora, una lista de CDs o DVDs compartida para ser accedida a través de la red, etcétera.

Si conectamos una impresora a una computadora, podemos imprimir desde la otra. Si tenemos una máquina conectada a Internet, podemos compartir esa conexión y navegar desde la otra. Si tenemos una sola computadora y nos conectamos a Internet, podemos acceder a todos los servicios que se encuentran en ella: correo electrónico, información, programas para descargar música y videos (siempre respetando los derechos de autor). Y como no todo es trabajo en esta vida, si bien resulta divertido jugar en la computadora, a veces lo es aún más cuando podemos jugar contra otros contrincantes, ¿y cómo lo-gramos esto? A través de la red.

El mismo concepto de red implica el de pluralidad

REDES EN ACCIÓN

Las personas utilizan el lenguaje para comunicarse entre sí. Los chinos utilizan el idioma chino, en Iberoamérica usamos el español, etcétera. Cada idioma tiene sus propias peculiaridades, las cuales están definidas minuciosamente.

Para utilizar el lenguaje, contamos con diferentes medios: la escritura, la oralidad y la gestualidad. La palabra escrita utiliza un alfabeto y un conjunto de reglas que definen su uso; la palabra hablada también respeta las reglas del idioma; y hasta el lenguaje de gestos tiene sus propios signos. Cada tipo de comunicación posee sus propios medios que, a su vez, pueden mezclarse, por ejemplo, en una transmisión televisiva donde un conductor utiliza el lenguaje de signos para comunicarse con personas con discapacidades auditivas.

Podemos determinar, entonces, que se utilizan distintos **niveles** a la hora de establecer una comunicación. Primero está el idioma (inglés, portugués,



VERSIONES DE VISTA

Microsoft lanzó al mercado seis versiones de Windows Vista. Esta división responde tanto a decisiones técnicas, no hacerle pagar al usuario por una característica que no necesita, como a mercadotecnia, tener presencia en un segmento determinado.

español, italiano, etcétera), luego la forma en que se utiliza (palabra escrita, vía oral o gestual) y podríamos agregar la vía por la que se transmite (de persona a persona, a través de una carta, de una conversación telefónica, etcétera).

Las computadoras no son menos y para comunicarse entre sí también requieren un lenguaje común y estándar entre todas. Podríamos agregar, además, que las computadoras son "tontas" y necesitan que les digamos exactamente qué es lo que tienen que hacer y cómo (aclaramos que estamos hablando exclusivamente de computadoras). En realidad, en la vida cotidiana los seres humanos funcionamos de la misma manera, pero no nos damos cuenta ya que lo hacemos de manera inconsciente. Por eso, a las computadoras, tenemos que definirles el lenguaje y el medio que van a emplear para comunicarse y cómo lo van a utilizar (**Figura 2**).

Existe una organización dedicada a crear estándares, llamada **Organización Internacional para la Estandarización**, más conocida por sus siglas

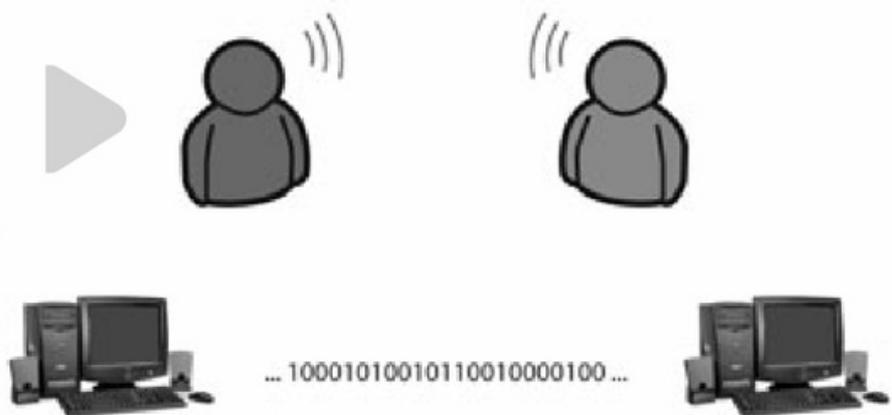


en inglés: **ISO** o *International Organization for Standardization*. Los especialistas de la ISO definieron un **modelo de referencia**, una especie de guía para crear un lenguaje común, de manera tal que todas las computadoras que quisieran comunicarse entre sí pudieran lograrlo si respetaban ese modelo. Dicho modelo es conocido como el **modelo OSI** (*Open System Interconnection* o interconexión de sistemas abiertos) y se compone de **7 niveles**.

Los 7 niveles del modelo OSI

En redes se habla de **capas** (**layers** en inglés) o niveles. El modelo OSI define **7 capas**: la **capa 1** se refiere a la capa física, que es la que cubre desde las señales eléctricas que se van a transmitir hasta los

FIGURA 2.
Así como las personas tenemos un lenguaje para comunicarnos, las computadoras también tienen el suyo.



En redes se habla de capas (layers en inglés) o niveles

pinos que lleva cada tipo de conector; ejemplos de estándares de esta capa son RS-232 (los conectores COM, también puertos serie o seriales), 100Base-T (el protocolo que utilizan las redes UTP a 100 Mbps). La **capa 2** define cómo van a estar organizadas esas señales eléctricas de forma tal que se pueda transmitir información a través de ellas. Se la conoce como capa de enlace de datos; ejemplos de esta capa son PPP (empleado en las conexiones por acceso telefónico), 802.11 a/b/g (para las redes inalámbricas). La **capa 3** se encarga de mover la información a un nivel más reconocible por nosotros, es llamada capa de red y agrupa una serie de protocolos para mover la información, el más conocido es el IP (Internet Protocol), que veremos en

detalle más adelante. La **capa 4** se encarga de mover información directamente entre aplicaciones.

La aplicación le entrega la información a esta capa de transporte y depende de la capa asegurar que llegue a su destino final de manera íntegra. Las tres restantes: la **capa de sesión**, la **capa de presentación** y la **capa de aplicación** se refieren exclusivamente a las aplicaciones (**Figura 3**).

COMPONENTES DE UNA RED

Como suele ser costumbre en informática, en redes también encontramos la separación entre **hardware** y **software**. Para comprender mejor estos conceptos, voy a hacer referencia a una anécdota que me contó un amigo. Para explicar la diferencia entre hardware y software, un profesor utilizó la siguiente expresión: "hardware es lo que golpeás, software es lo que insultás". Evidentemente, ese profesor se refería a esos raros casos en los que la computadora anda mal y uno se desespera, y aunque bajo



FIGURA 3.

A través de la red, podemos trabajar con un documento almacenado en otro equipo.



Ya sea una conexión alámbrica o inalámbrica, va a existir un dispositivo que actúe como enlace entre la conexión y la computadora

ningún concepto aprobamos dicha conducta, la anécdota no deja de ser simpática y esclarecedora a la vez. El hardware es algo que podés tocar y el software, por el contrario, no tiene un componente físico, sino que es algo inmaterial, que solo existe cuando se ejecuta a través de los circuitos electrónicos de una computadora.

En primer lugar, vamos a hacer referencia a los componentes que podemos ver y tocar: el hardware. Para armar una red, necesitamos una manera de establecer un **enlace** entre las computadoras. Si deseamos transmitir una señal, lo más rápido y conocido es utilizar un **cable** entre los dos puntos: el tipo más empleado hoy en día es el **UTP**, que es un cable de cobre integrado por tres pares de alambres. UTP son las siglas en inglés de **par trenzado no apantallado** (*Unshielded Twisted Pair*), donde cada

par se trenza para reducir las interferencias electromagnéticas. Existe una variante que es un cable similar (de todas maneras, su uso no es tan común como el del UTP), pero cubierto por una malla metálica que lo protege de las interferencias, conocido como **STP** (*Shielded Twisted Pair* o **par trenzado apantallado**). En las primeras redes se utilizaba el cable **coaxial** mientras que, en las más modernas, se empleaban con más frecuencia cables de **fibra óptica**.

Estas redes se conocen como redes **alámbricas**. Sin embargo, no es obligatorio el uso de cables para establecer una comunicación. Existen equipos que nos permiten utilizar **señales inalámbricas** similares a la forma en que la radio transmite su programación por aire. Las redes creadas de esta manera se conocen como redes **inalámbricas** o **WiFi** y las veremos en detalle en el **Capítulo 5 (Figura 4)**.

► SISTEMA BINARIO

La escritura de nuestro idioma se basa en el alfabeto, y las computadoras utilizan su propio alfabeto, uno numérico basado en dos cifras: el 1 y el 0. Este sistema se llama **binario** (como su prefijo lo indica bi = dos) y con esas dos cifras se representan todos los demás números.

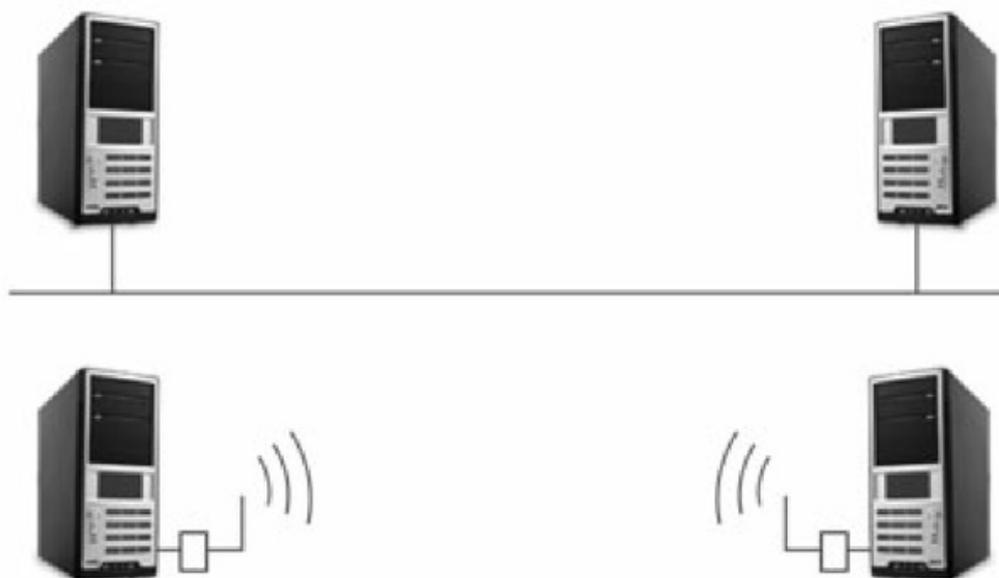


FIGURA 4. Las conexiones entre computadoras pueden ser tanto alámbricas como inalámbricas.

Ya sea una conexión alámbrica o inalámbrica, va a existir un dispositivo que actúe como enlace entre la conexión y la computadora. Este dispositivo es conocido como placa, tarjeta o **adaptador de red**, si vamos a ir familiarizándonos con la terminología que utiliza Windows.

Por último, el software que va a hacer uso de estos medios también forma parte de la red y llega a influenciar en gran medida en su diseño. La parte del software la veremos en detalle en los capítulos siguientes. La comunicación final es el resultado de la unión de un

grupo de etapas intermedias. El medio de conexión es la forma de transmitir las señales a través de él, es decir, la conexión del medio al equipo. El software es el que recibe la información transmitida y la procesa. Cada una de estas etapas se conoce como **capas** o niveles. El modelo OSI que mencionamos en la pregunta anterior se creó precisamente para estandarizar estos niveles (**Figura 5**).

TIPOS DE REDES

En las primeras redes que se implementaron, cada fabricante de equipamiento utilizaba su propia



ARPA

A finales de los 60, la Agencia de Investigación de Proyectos Avanzados (**ARPA**) de los EE.UU. comenzó un proyecto para crear una red de transmisión de datos que enlazara equipos remotos a través de las líneas telefónicas. La consecuencia de ese proyecto fue Internet.



FIGURA 5. Las capas del modelo OSI se componen por 7 niveles.

tecnología (propietaria) como una forma de atar al cliente a sus productos. Con el tiempo, el número de redes comenzó a crecer y, con ellas, la necesidad de interconectarlas. Las incompatibilidades entre equipamientos de distintos fabricantes se convirtió en un problema. Como solución a este problema, el modelo propietario cedió lugar a uno abierto (el modelo **OSI**).

Existe una lengua creada con el objetivo de convertirse en lenguaje universal: el esperanto, aunque, en la realidad, el inglés se utiliza como vía de comunicación cuando nos encontramos ante una persona que habla otro idioma. De la misma manera, los protocolos que se utilizaban en la red Internet que se desarrolló en los Estados Unidos se han convertido en la



COMPARTIR ARCHIVOS

La forma habitual de compartir archivos en una red es designando una máquina para que los almacene, a la que se conectará todo aquel que quiera subir o descargar un archivo. De esta manera, tenemos un **servidor**, y muchos equipos conectándose a él, llamados **clientes**.



FIGURA 6.
Podemos conectarnos a Internet sin utilizar cables.

lengua universal de las redes de hoy en día (**Figura 6**). Existen tantos tipos de redes como aspectos estamos evaluando. En base al medio de comunicación, ya sabemos que podemos tener redes alámbricas e inalámbricas. Entre las primeras, tenemos por cable de cobre y por fibra óptica. A su vez, dentro del cable de cobre, encontramos cables UTP, STP, o coaxial,

y así podríamos seguir. Entre las segundas, tenemos desde las conexiones satelitales hasta las que utilizamos con una notebook cuando nos conectamos en una cafetería que nos brinda WiFi. Podemos clasificar las redes basándonos en la ubicación de los recursos. Existen redes **centralizadas** y redes **descentralizadas** (**Figura 7**).

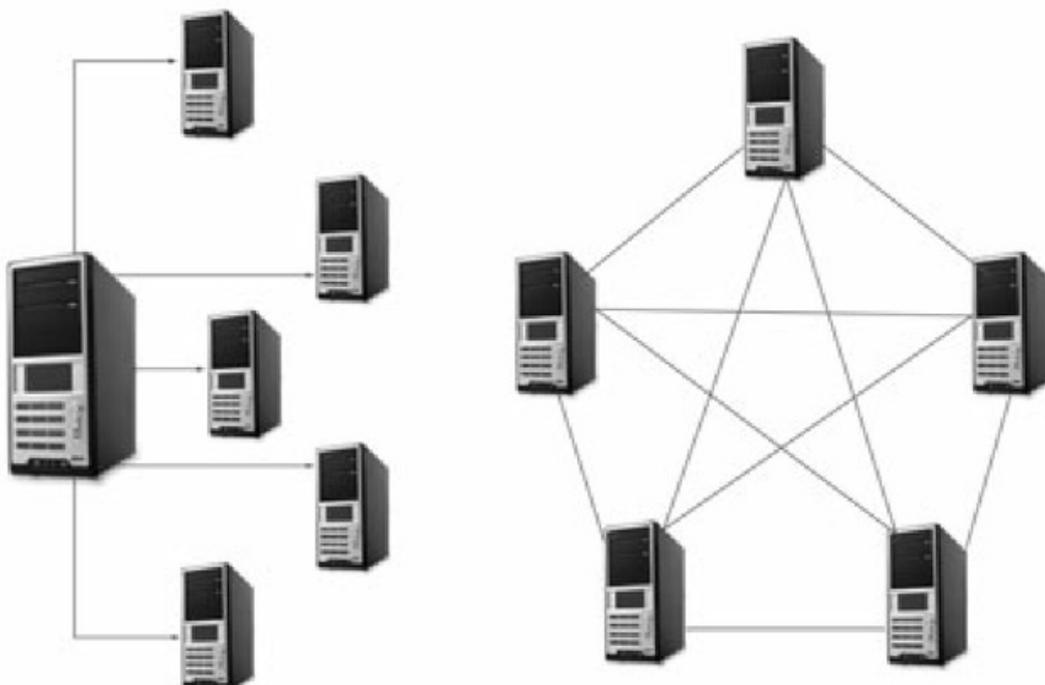


FIGURA 7. Las redes centralizadas concentran toda la información en un servidor. En las descentralizadas, todos los equipos intercambian entre sí la información.

► 1. ¿Qué es una red?

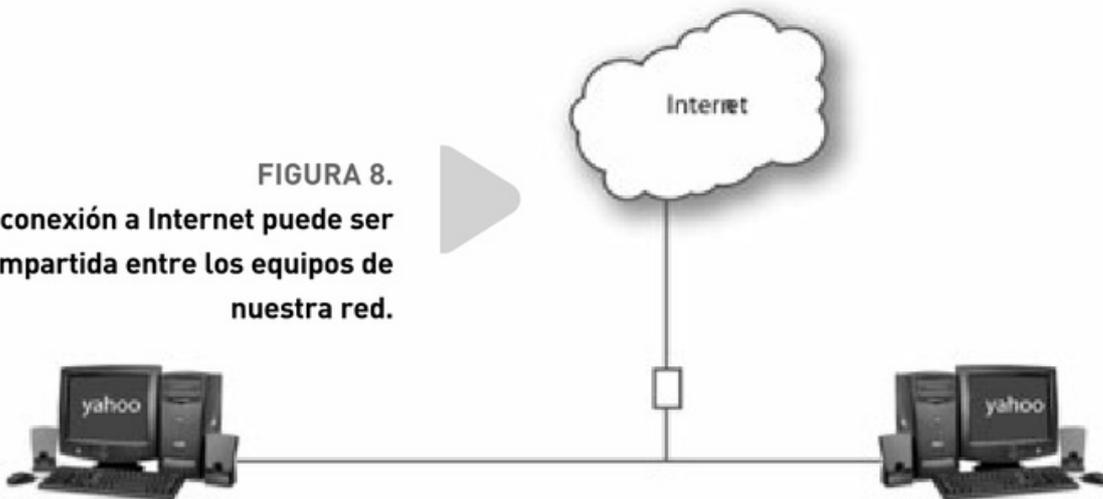
En las primeras, toda la información está concentrada en un solo lugar y, en las segundas, la información se reparte. Es decir, puede ser que cada parte de los recursos vaya para un equipo específico o que se replique entre varios equipos una misma información y que, a la hora de recuperarla, pueda hacerlo desde cualquiera de ellos. Estas últimas suelen llamarse redes *Peer to Peer* o **P2P** (de par a par, o entre iguales).

Un grupo de equipos conectados entre sí es una red. Si esta red la conectamos con otra y con otra y con otra, empezamos a tener redes de redes. Si todas las redes del mundo se conectan unas a otras, vamos a tener la red de redes, más conocida como **Internet**.

Hoy en día, muchas empresas utilizan computadoras en su operación cotidiana. Para aprovechar los recursos, estas computadoras suelen estar conectadas entre sí y permiten no solo compartir los recursos dentro de la empresa, sino, además, la comunicación fuera de ella. El correo electrónico ha sustituido en gran medida al correo tradicional y al propio fax.

Las redes han permitido que, en vez de comprar una impresora por cada computadora en la oficina, podamos comprar solo una y compartirla entre todos los equipos. Este tipo de red que existe dentro de una empresa es interna y recibe el nombre de **Intranet (Figura 8)**.

FIGURA 8.
La conexión a Internet puede ser compartida entre los equipos de nuestra red.



P2P

Con el objetivo de superar las imitaciones del modelo cliente-servidor, surgieron las redes **P2P**. El nombre es una contracción de *Peer-to-Peer*: una traducción literal sería redes **de igual a igual** o como sugiere Wikipedia **entre iguales**.



Una Intranet nos permite imprimir en una impresora conectada a otra computadora

Una Intranet nos permite imprimir en una impresora conectada a otra computadora y acceder directamente a los archivos almacenados en el disco duro de otro equipo. Incluso, podemos tener correo electrónico entre todos los trabajadores de la empresa y un sitio web donde se publica información. Sin embargo, la empresa necesita interactuar con otras empresas. Así como la solución interna para compartir los equipos fue conectarlos en red, se aplicó el mismo concepto entre empresas. De esta manera, las redes comenzaron a conectarse entre sí. Una empresa se conectó a otra y a otra.

Como ya existía Internet, no eran necesarias las redes **punto a punto** entre empresas, con conectarse a Internet se podía enviar y recibir información con el resto del mundo. Pero había un problema: no todas las empresas utilizaban el mismo software para sus redes

internas; había redes **Novell**, redes **Windows** y redes **Mac**, llamadas así por el fabricante del software empleado. Por eso, una de las tecnologías desarrolladas por el proyecto **ARPANET** fue el protocolo **TCP/IP** (que analizaremos en detalle en el **Capítulo 3**), que se convirtió en el estándar para las redes **Unix** y, más adelante, para conectarse a la naciente Internet.

Con el paso del tiempo, los fabricantes de software para redes terminaron reemplazando sus protocolos propios por TCP/IP y, en la actualidad, es el protocolo de red más utilizado en el mundo.

Éstas son, a grandes rasgos, las clasificaciones de redes que podemos encontrar comúnmente hoy en día, pero debemos aclarar que no son las únicas y, de hecho, esperamos que en el futuro cercano este número siga creciendo.



RESUMEN

En este primer capítulo, a modo de introducción, aprendimos los conceptos básicos sobre las redes informáticas: su utilidad, componentes y tipos. Estudiamos las redes en acción y, además, aprendimos los siete niveles del modelo OSI.

Multiple choice

► **1** ¿Qué es una red informática?

- a- Un conjunto de equipos informáticos.
 - b- Un tipo de implemento diseñado para la pesca en aguas abiertas.
 - c- Un sistema de protección para los ventiladores de las computadoras.
 - d- Un tipo de media femenina.
-

► **2** ¿Para qué sirve una red informática?

- a- Para captar adeptos a una causa.
 - b- Para mejorar la venta de una línea de productos.
 - c- Para compartir recursos entre diferentes equipos informáticos.
 - d- Para pescar.
-

► **3** El modelo OSI tiene...

- a- 3 capas.
 - b- 5 capas.
 - c- 6 capas.
 - d- 7 capas.
-

► **4** Los cables de una red son de tipo:

- a- Bipolares.
 - b- Blindados.
 - c- RJ11
 - d- UPT/STP
-

► **5** ¿Cuál de las siguientes opciones no es un tipo de red?

- a- Centralizada.
 - b- Descentralizada.
 - c- P2P
 - d- Circular.
-

► **6** TCP/IP son las siglas de:

- a- Transferencia Contable Patriótica/ Integración de los Pueblos.
 - b- Transmission Checking Port/Internet Port.
 - c- Transmission Control Program/Internet Program.
 - d- Transmission Control Protocol/ Internet Protocol.
-

Respuestas: 1-a, 2-c, 3-d, 4-d, 5-d, 6-d.

Capítulo 2

Instalación de la red: primeros pasos



Estudiaremos los primeros pasos de la instalación de la red y armaremos el cable para ésta.

Instalación de la red: primeros pasos

Deberemos tener en cuenta al armar la red, en principio, la **cantidad de equipos** que necesitamos conectar, tanto ahora como en un futuro. Es muy probable que hoy en día tengamos solo presupuesto para una computadora, pero quizás en un año podríamos tener la necesidad y el presupuesto para comprar una segunda, y así debemos planificarlo.

De hecho, suele ocurrir que en ese plazo de tiempo el hardware ya está obsoleto y decidimos mejorar la computadora y dejarle a los chicos la que teníamos hasta ese momento. De esta manera vamos planificando la compra de equipos: mejorar la computadora, comprar un monitor más grande, una impresora, etcétera. Éstas son compras de alto costo, pero fáciles de instalar.

Con las redes sucede lo contrario. El precio del metro de cable no es excesivamente caro, no vamos a tener un gran ahorro en comprar 100 metros ahora y 50 el próximo año. Por otro lado, cuando instalamos el **cableado** en la casa, tenemos que colocar cable canales, probablemente utilizar el taladro, etcétera. Si de aquí a un año decidimos instalar un



equipo en otra habitación, tendríamos que repetir todo el proceso. El punto radica en establecer un equilibrio, buscar la forma de considerar la red, no como lo que ésta va a hacer de manera inmediata, sino a corto o mediano plazo. Es preferible instalar dos cables de una vez que colocar hoy uno y, de aquí a seis meses, volver a repetir todo el proceso para instalar un segundo cable. No se trata, por supuesto, de llenar la casa de cables, de hecho, cada vez aparecen más opciones para no utilizarlos, pero es importante tomar en cuenta estos consejos a la hora de armar nuestra red.

Cuando se construye una ciudad, lo primero que se hacen son las calles. El equivalente en redes sería el cableado. Insistimos en hablar de cableado porque sigue siendo una de las principales formas de interconexión entre equipos, es la más barata de todas las alternativas, muy segura y con excelente rendimiento.

▶ MBPS

En las redes, la velocidad del enlace es importante, pero lo que nos debe preocupar es el **caudal** del enlace. Los Mbps o **Megabits por segundo** no son una medida de velocidad, sino que nos indican la cantidad de datos que se pueden mover por la red en una medida de tiempo.

Deberemos tener en cuenta al armar la red, en principio, la cantidad de equipos que necesitamos conectar

Entre los equipos por conectar, no debemos olvidar la conexión a Internet si estamos contando con ella. El proveedor tiene ciertas limitaciones a la hora de instalar el servicio en nuestra casa y debemos tenerlo en cuenta porque es un punto más para conectar y, de hecho, muy importante. Por eso, debemos considerar los equipos que se conectarán, el lugar de la casa donde se encuentran y el tipo de red que vamos a utilizar. Una vez definidos estos tres parámetros, solo tenemos que ponernos manos a la obra.

HUBS VS. SWITCHES

El **hub**, primer tipo de concentrador en la historia de las redes, tenía un problema en la forma en que trabajaba: cada vez que una computadora conectada a un puerto Ethernet del hub enviaba un paquete de datos a la red, éste lo transmitía a todos los puertos restantes que tenía. En redes chicas, eso no era un problema, pero cuando la red empezaba a crecer y

comenzaban a enlazarse hubs entre sí, el tráfico que circulaba por la red podía llegar a congestionarla. Si de cuatro equipos, dos empiezan a transferir archivos grandes entre ellos, los otros dos van a encontrar congestión en la red, aun cuando no participen en la transferencia.

Los ingenieros desarrollaron entonces otro equipo, el **switch** (en castellano **conmutador**, pero se acepta la palabra en inglés), que es similar al hub en lo externo, pero en su interior funciona muy diferente; esto lo podemos ver en la **Guía visual 1**.

Cuando el switch recibe un paquete de datos para un equipo, busca en su listado interno a qué puerto está conectado ese equipo y le envía el paquete directamente a través de ese puerto. Esto fue una gran ventaja con respecto a los hub, que no tenían ese listado interno y reenviaban el paquete a todos los puertos, tanto al equipo destino, como al resto. Imaginemos la cantidad de tráfico innecesario que se ahorró con la introducción de los switches.

Toda nueva tecnología tiene un período inicial en el que su costo es alto; luego, en la medida que su uso se masifica, los costos comienzan a bajar hasta llegar al punto donde reemplaza a la anterior. Así, el switch reemplazó al hub y, en un futuro,



BYTE

En computación se maneja el concepto de 1 **byte**, que está compuesto por 8 bits. Podemos traspolar esto a las redes y utilizar 1 Mbps en algunos casos. Se utiliza la **B** mayúscula para referirse a los bytes y la **b** minúscula para referirse a los bits.

GUÍA VISUAL /1

Partes de un switch



- 1 PWR LED:** el Power LED o LED de encendido nos permite conocer el estado del switch, si está encendido o apagado.
- 2 Puertos Ethernet:** éstos son los puertos a donde se conectan los cables de red.
- 3 LEDs de los puertos Ethernet:** muestran cuándo el enlace está activo y cuándo transmite.

los **enrutadores** (más conocidos por su término en inglés, **routers**) reemplazarán a los switches. En la actualidad, un switch sigue resultando más barato, pero ya el precio de un router es accesible para el usuario promedio (**Figura 1**).

LOS CABLES

Una red puede utilizar muchos tipos de cable, cada uno con sus ventajas y desventajas. En el **Capítulo 1**, mencionamos los principales tipos de cables que se

utilizan para redes. De ellos, el UTP es el más extendido. Es el más económico de todos los restantes y sirve perfectamente para la mayoría de las instalaciones hogareñas. Además, es más fino, por lo que se manipula mejor y ocupa menos espacio.

El cable UTP está compuesto por cuatro pares de alambres de cobre; cada par (como su nombre lo indica) está trenzado con el fin de disminuir las **interferencias electromagnéticas**.



FIGURA 1.

En las empresas se utilizan switches con funcionalidades de enrutadores incorporadas.

Existen varias **categorías** de cable UTP, las más utilizadas son la **5**, la **5e** y la **6**. Estas categorías están definidas por un comité internacional y se refieren a especificaciones técnicas que deben cumplir los fabricantes de cables.

Lo que nos interesa saber es que el cable categoría 6 es más caro y más rígido que el de categoría 5, y resulta más complicado de instalar. Por suerte, se definió un estándar intermedio: el cable categoría 5e, que acepta hasta 1000 Mbps y es muy similar físicamente al de categoría 5. Es común referirse a estos cables con las abreviaturas: **Cat-5**, **Cat-5e** y **Cat-6**.

En ocasiones, tenemos que conectar dos habitaciones, una encima de la otra, y el lugar de la casa por

donde podríamos pasar un cable queda en el otro extremo de la planta. Ambas habitaciones tienen ventanas, por lo que si el cable viaja por el exterior nos ahorramos mucho trabajo. En esos casos, es necesario tener en cuenta dos sugerencias: primero, que el tendido por el exterior quedará expuesto a la intemperie, motivo por el cual debemos proteger el cable pasándolo por dentro de una tubería; segundo, que en el exterior existen fuentes de interferencia adicionales, por ejemplo, una **descarga eléctrica** podría inducir una corriente eléctrica en el cable, si llegara a suceder cerca.

En estos casos, la mejor opción es utilizar un cable **apantallado**, del tipo **STP**, que cuenta con un

Una red puede utilizar muchos tipos de cable, cada uno con sus ventajas y desventajas



NIVELES DEL MODELO OSI

Según el modelo OSI que mencionamos en el **Capítulo 1**, podemos decir que un hub trabaja a nivel de la capa 1 (capa física), mientras que un switch trabaja en el nivel 2 (capa de enlace de datos). Los routers lo hacen un nivel por encima de los switches, en la capa 3 (nivel de red).



FIGURA 2.
El cable STP cuenta con una malla interna que protege los cables de datos contra interferencias.

recubrimiento interno (una **malla metálica**) que se conecta a la tierra eléctrica para proveer esta protección (**Figura 2**). Otros tipos de cables utilizados para redes Ethernet son el cable **coaxial** y la **fibra óptica**. Los cables STP y UTP utilizan conectores similares, pero no es el caso en estos cables, que requieren conectores diferentes. Esto implica, además, tarjetas de red y switch que los soporten. El cable coaxial está en desuso, permite velocidades solo de hasta 10 Mbps. El cable de fibra óptica, por el contrario, es el futuro. Permite altas velocidades de transmisión, bajas pérdidas, es inmune a interferencias electromagnéticas y permite tramos de enlace más largos.

Seguramente, a esta altura nos preguntaremos: ¿qué tipo de cable me conviene usar? Como suele suceder,

no hay respuestas absolutas, sino, más bien, soluciones de compromiso. De entrada, el cable coaxial queda descartado por obsoleto; el cable de fibra óptica es muy complicado de instalar para una red hogareña, tanto por lo caro de los equipos como por la propia instalación.

En la actualidad, la opción inalámbrica es válida ya que los costos han disminuido y, prácticamente, el tiempo de instalación se reduce a conectar los equipos, encenderlos y configurarlos.

Sin embargo, es muy probable que la mayoría de los equipos que ya tenemos instalados en casa tengan una tarjeta de red disponible. Además, la velocidad de una red cableada sigue siendo superior a una inalámbrica, y la seguridad también es mayor (**Figura 3**).

CAMPO ELECTROMAGNÉTICO

Los cables de transmisión de electricidad, al igual que todo motor eléctrico, generan un **campo electromagnético**. Debemos tener en cuenta este concepto para tomar medidas que nos permitan atenuar o reducir los efectos de estas interferencias en nuestra red.

FIGURA 3.
El cable UTP está compuesto por cuatro pares de alambres.



En cuanto al tipo de cable, también tendremos que tomar una decisión. Para una red que vaya solo por dentro de la casa, recomendamos el cable UTP. Ahí entra a jugar la categoría del cable. El más barato es el Cat-5, un poco más caro es el Cat-5e, mientras que el Cat-6 es el más caro de los tres. El Cat-5 solo permite hasta 100 Mbps: ésa es una limitación, pero también es cierto que para navegar por Internet, utilizar el correo electrónico y jugar en red, ese ancho de banda es suficiente. Si el presupuesto nos lo permite, por un poco más de dinero podríamos instalar el cable Cat-5e y así dejaríamos la red lista si, en un futuro cercano, adicionamos equipos o tarjetas de red a 1 Gbps. El cable Cat-6, si bien es más robusto, resulta más difícil de instalar, más caro, y para redes chicas no se justifica.

ARMAR UN CABLE DE RED

Los cables se arman siguiendo un ordenamiento específico, que no es aleatorio en absoluto, todo lo contrario, está definido por una norma internacional

llamada **EIA/TIA568**. Podemos ver el procedimiento en el **Paso a paso 1**. Todos los conectores que se armen deberán respetar esta norma.

Ésta fue producto de la necesidad de mercado de establecer un estándar y fue emitida por una alianza compuesta por las organizaciones y empresas más importantes del ramo, incluyendo fabricantes, consultores y usuarios. A partir de allí, se desarrollaron las normas **EIA/TIA/568-A (Tabla 1)** y **EIA/TIA/568-B**,



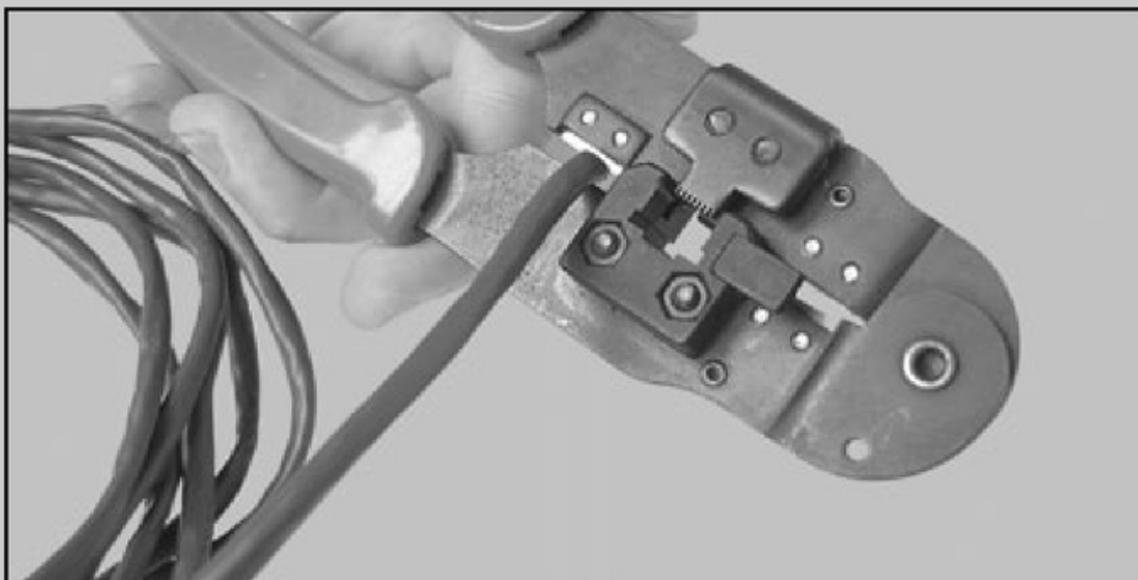
CONVERSIÓN MEGA BYTE/ SEGUNDO A MEGA BITS/ SEGUNDO

Si queremos saber el equivalente en Mb/s, hay dos formas de hacer esta conversión: la primera es utilizar una calculadora. Por ejemplo, si queremos convertir 133 MB/s en Mb/s lo multiplicamos por 8 (1 byte = 8 bits) y obtenemos el resultado: 1064 Mb/s.

PASO A PASO /1

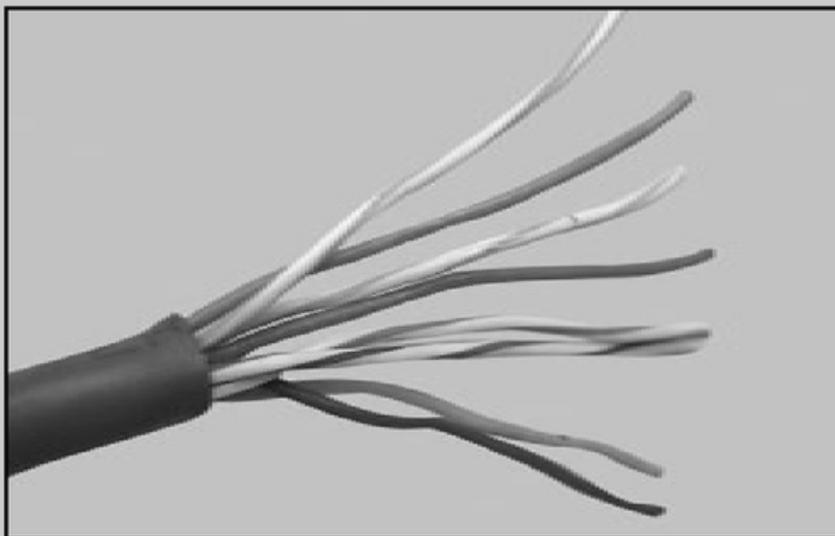
Armado de un cable de red

1



Tome la punta del cable y, con la pinza crimpadora, quítele una parte de la cubierta para dejar los pares trenzados a la vista. Éste es el mejor momento para poner el capuchón.

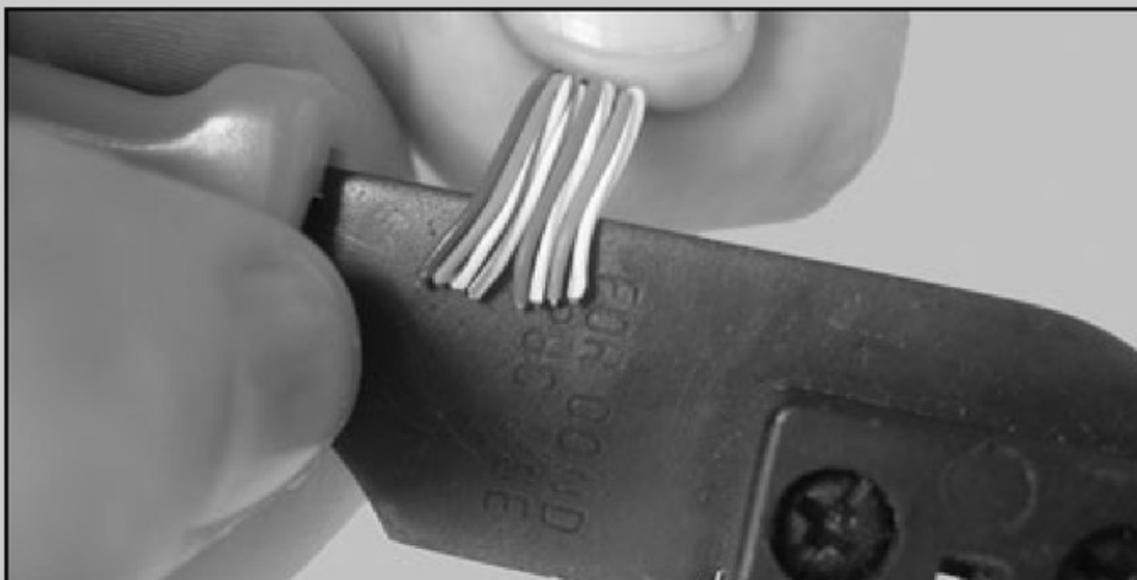
2



Identifique los cuatro pares que vienen trenzados y sepárelos. Esto lo va a ayudar a no perder de vista cuál es el blanco de cada color.

PASO A PASO /1 (cont.)

3



Organice los alambres siguiendo el orden establecido por la norma.
Debe acomodar ahora los alambres buscando que queden lo más unidos posible.

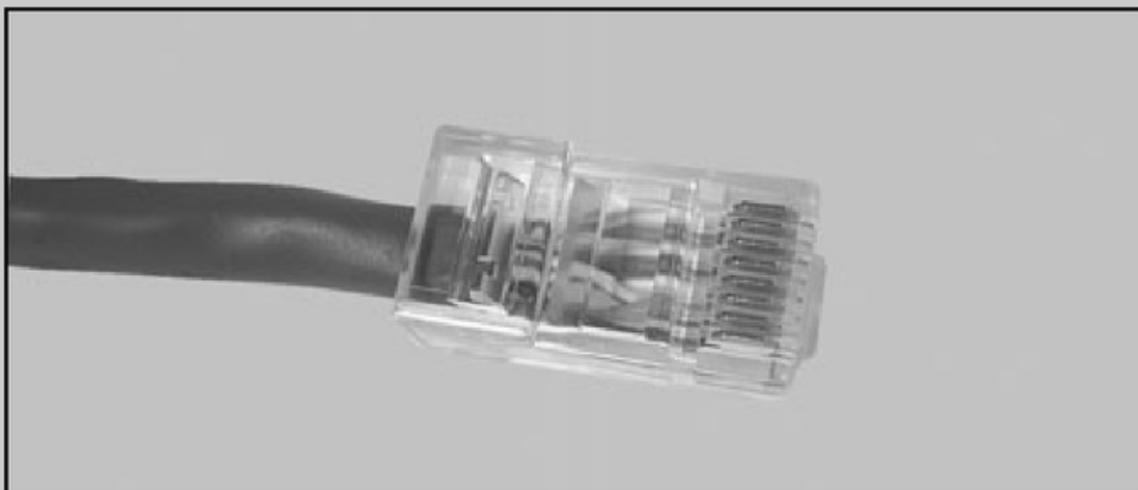
4



Ya están organizados y acomodados, pero las puntas han quedado disperejas. No se pueden introducir así en el conector pues se corre el riesgo de que alguna no haga contacto con los pines. La pinza crimpeadora tiene una cuchilla que le permitirá emparejarlos.

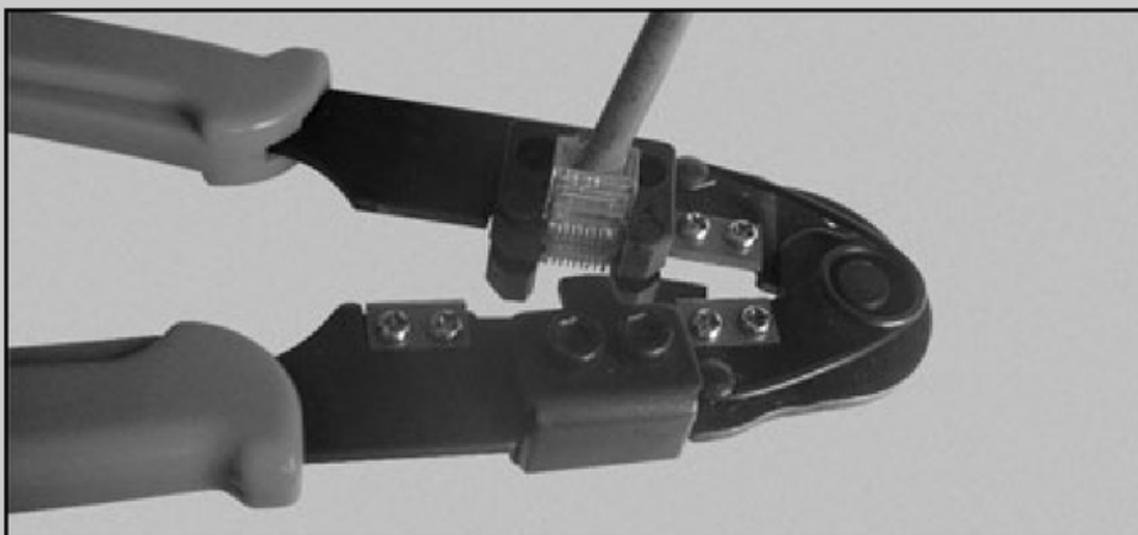
PASO A PASO /1 (cont.)

5



Ahora ya puede colocar el conector. Con cuidado y sin apuro, vaya insertando los alambres lentamente para que cada uno haga contacto con el fondo de su canal, donde está el pin que le corresponde. El largo de los alambres fuera del cable debe ser de 1 cm solamente, acorde con la norma. Además, si quedan largos es probable que sufran un corte accidental al quedar más sueltos.

6



Por último, presione con firmeza el conector con la pinza crimpadora para que quede bien firme. Sólo tiene una forma posible de insertar el conector.

PIN	COLOR
1	Blanco y verde
2	Verde
3	Blanco y naranja
4	Azul
5	Blanco y azul
6	Naranja
7	Blanco y marrón
8	Marrón



TABLA 1. Colores de los pines de la Norma 568 A.

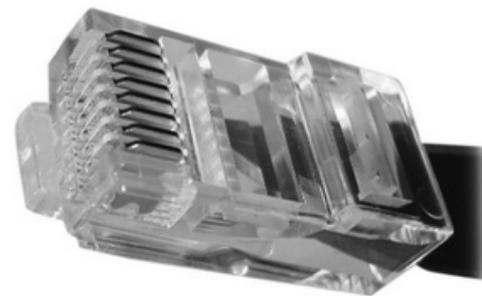
para regularizar los sistemas de cableado para telecomunicaciones. Esto fue necesario con la difusión del cableado estructurado en los edificios y construcciones. Así, se garantizaba que los productos de distintos fabricantes pudieran funcionar correctamente entre sí. Para el caso que nos concierne, esta norma define el orden en el cual vamos a conectar los alambres cuando se introducen en el conector (**Figura 4**).

Un cable UTP tiene ocho alambres en cuatro pares. Cada par está compuesto por un alambre de color entero y otro que es blanco con franjas del color entero.

DE COMPRAS

Ya definimos el tipo de red que satisface nuestras necesidades. A los efectos de nuestro ejemplo, hemos seleccionado una red cableada, con cable Cat 5e, y funcionando a 100 Mbps. Ha llegado el momento de poner manos a la obra. Supongamos que vamos a instalar una red en un departamento, que enlaza dos computadoras ubicadas en habitaciones distintas. Primero debemos ubicar dónde vamos a tener el switch. Es muy probable que si tenemos conexión a Internet, ésta se encuentre cerca de una de las dos computadoras.

FIGURA 4.
El conector siempre se coloca con los alambres metálicos mirando hacia nosotros, y se numeran los pines de izquierda a derecha.



Este podría ser el punto central. Ahí ya tenemos dos equipos (el router de Internet y una computadora). Es bueno centralizar ya que nos ahorra tiempo a la hora de comprobar el estado de las conexiones, aunque podríamos instalar el switch en otro lugar.

En cualquier caso, debemos hacer un recorrido del trazado que seguiría el cableado para evaluar las alternativas posibles hasta quedarnos con la que nos convenga. Este trazado mental nos va a permitir realizar el cálculo de la cantidad de cable que necesitamos. La distancia a la que se encuentra un equipo del otro no es una buena medida ya que el cableado muchas veces tiene que seguir un recorrido que a simple vista no notamos.

El cable puede utilizar un cable canal, tuberías interiores en la pared o sencillamente rodar por el borde del zócalo. Cada uno de estos métodos implica compras específicas. Los cables canales se venden en distintos tamaños. En una red hogareña, la cantidad de cables no va a ser grande por lo que la más chica debe resultar suficiente. Por un lado, es la más económica y, por otro, la más discreta.

En definitiva, es nuestra casa y no debemos descuidar la estética. Los cables canales chicos se pueden fijar con cinta adhesiva bifaz. Es la opción

más rápida y, dado el escaso peso que ésta transporta (uno o dos cables de red), no vamos a tener problemas. Para el caso de cables canales más grandes (y pesados) que requieren una fijación más firme, tendremos que visitar la sección de tornillos y expansiones de la tienda más cercana. Es decir, se aplica el mismo principio que si colgáramos un cuadro en la pared.

El cable que viene del switch se puede conectar directamente a la computadora, pero es recomendable utilizar un paso intermedio, una caja con conectores también conocida como **roseta (Figura 5)**. Esta caja tiene un conector hembra RJ45 que va conectado al cable que viene del switch y se fija a la pared.



FIGURA 5. Las rosetas para cables de red son similares a las de los teléfonos.

RJ

El concepto de RJ proviene del inglés **Registered Jack**, o **conector registrado** en español. Es un conector que respeta ciertas normas establecidas, acordadas o “registradas”, que son de estricto cumplimiento por los fabricantes que producen equipos que lo utilizan.

Entonces, con un cable más corto conectamos la computadora a esta cajita y, así, queda establecida la conexión entre la computadora y el switch. Esta alternativa tiene varias ventajas: si en el futuro necesitamos mover el equipo y el cable no alcanza, no tendremos que tirar un nuevo cable hasta el switch, sino solo sustituir el cable que va de la cajita a la PC. También, si quitamos la computadora de ese lugar, no dejamos detrás un cable suelto en el piso, lo desconectamos y solo quedará la cajita fijada en la pared, como solemos tener las de teléfono.

Respecto del cable, podemos armarlo nosotros o comprarlo directamente armado. En las tiendas especializadas, se venden con sus conectores y capuchones. Si no tenemos un pedazo de cable suelto disponible, se nos acabaron los conectores o no queremos com-



prar una pinza solo para armar un cable por única vez, los cables armados son una buena opción. Estos cables son conocidos por su nombre en inglés: **patch**.

Para armar los cables, vamos a necesitar los conectores RJ45 y también es aconsejable utilizar **capuchones** para protegerlos, aunque no es obligatorio. Y por supuesto, la pinza para fijar los conectores al cable, denominada **pinza crimpeadora** (Figura 6).



FIGURA 6.
Cable, pinza crimpeadora, conectores RJ45 y capuchones son algunos elementos que necesitamos para instalar nuestra red.

FIGURA 7.

Los testers no son caros y son muy convenientes a la hora de asegurarnos de si el problema en la red está o no en el cable.

Existen kits que incluyen la pinza crimpadora y el **tester** para cables UTP. El tester nos permite asegurarnos de que el cable haya quedado correctamente armado y darnos cuenta de si existe alguna falla.

Un tester es un dispositivo muy sencillo (**Figura 7**). Por lo general, consta de dos piezas, donde cada una se conecta a un extremo del cable. Estas piezas tienen 8 LEDs, uno para cada alambre del cable UTP. Al encenderse, los LEDs deberían encenderse en cada pieza al mismo tiempo. Si en uno se enciende el LED, pero no en el otro extremo, es que hubo algún problema con el conector de ese lado.

Como los conectores no se pueden desarmar, cuando uno quedó mal armado, no hay que pensarlo dos veces, debemos cortarlo, tirar el viejo, conectar uno nuevo y volver a probarlo. Si tomamos en cuenta todo lo anterior, un listado de compras podría quedar como el que vemos en la **Tabla 2**.



INSTALAR UNA TARJETA DE RED INTERNA

El procedimiento para instalar una tarjeta de red no es complicado, pero implica acceder al interior de nuestra PC, lo podemos ver en el **Paso a paso 2**. Si nuestro equipo se encuentra en garantía, debemos consultar con el proveedor antes de abrirlo.

Como los conectores no se pueden dearmar, cuando uno quedó mal armado, debemos cortarlo

ELEMENTO	ESPECIFICACIONES	RECOMENDACIONES
Cable	UTP Categoría 5e	Muchos proveedores venden el cable en cajas con un rollo de un largo determinado.
Tarjetas de red	Tarjetas PCI Ethernet 100 Mbps	Comprobar si las computadoras no la tienen incluida.
Conectores	RJ45 (8P8C)	Cada cable que se tire lleva dos conectores, uno en cada punta. Comprar siempre algunos de más para compensar por los que no queden bien y haya que repetir.
Capuchones	Capuchones para conectores RJ45	Uno por cada conector.
Cable canal	Cable canal para cables UTP	De acuerdo con la cantidad de cables será el ancho. La cantidad se estima sobre la base del trazado de la red que hicimos y qué tramos utilizarían cable canal.
Uniones de cable canal	Piezas en forma de V, L, T.	Son las piezas que utilizamos cuando el recorrido del cable canal se interrumpe y necesitamos unirlos con el nuevo.
Rosetas	Cajas para Jack RJ45	Es importante revisar si la caja trae o no incluidos los conectores hembra RJ45. Algunos modelos requieren que los conectores se compren por separado.
Elementos de fijación	Tornillos, expansiones, cinta adhesiva.	De alguna manera, la canaleta va a quedar fija a la pared. Debemos comprar estos elementos. Siempre es preferible comprar un poco por encima del estimado a fin de que no nos quedemos cortos durante la instalación y haya que interrumpir el trabajo para ir hasta la tienda.
Pinza	Pinza crimpeadora	Para poner los conectores RJ45.
Cúter	Un cúter estándar	Es útil para quitar el recubrimiento externo del cable UTP al poner los conectores. Algunas pinzas crimpeadoras integran esta funcionalidad.
Cables Patch	Cables patch Cat 5e	Serán de la misma categoría del cable que compramos para el cableado. El tamaño dependerá de la distancia que exista entre la cajita con el punto de red y el equipo.
Tester	Comprobador de cables UTP RJ45	No es excesivamente caro, y si estamos haciendo nuestros primeros cables, es una buena forma de asegurarnos de que el cable quedó bien armado.

TABLA 2. Elementos para el armado de la red.

PASO A PASO /2 Instalar una tarjeta de red

1



Lo primero que se debe hacer al instalar una tarjeta de red es desconectar la PC del enchufe eléctrico, para que el procedimiento se efectúe de manera segura.

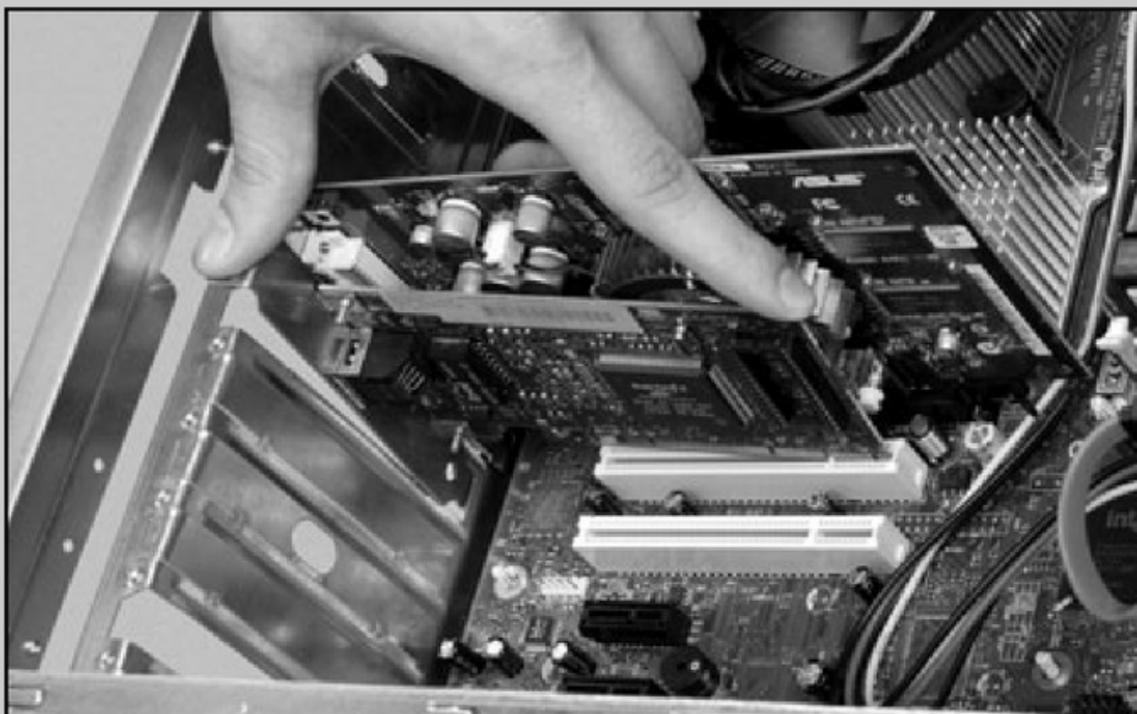
2



El segundo paso de este procedimiento consiste en retirar la tapa para acceder al interior de la computadora personal y poder instalar la tarjeta.

PASO A PASO /2 (cont.)

3



Los conectores están diseñados para permitir interconexión solo entre dispositivos similares. Un **slot PCI** solo va a permitir que se inserten **tarjetas PCI**. Presente la tarjeta y asegúrese de que, en efecto, el conector de la tarjeta coincida con el diseño de la ranura. Colóquele el tornillo para asegurar que no se mueva, lo cual puede provocar mal funcionamiento o eventualmente su rotura. Cierre otra vez el chasis. Conecte el cable, y el equipo habrá quedado listo para conectarse a la red.



RESUMEN

En este capítulo, estudiamos los primeros pasos de la instalación de la red. Conocimos las diferencias de los hubs, respecto de los switches. Aprendimos a armar un cable de red y analizamos los elementos necesarios para esto.

Multiple choice

► **1** ¿En cuál capa del modelo OSI funciona un router?

- a- 2
 - b- 3
 - c- 5
 - d- 7
-

► **2** A diferencia de un router, un hub no puede:

- a- Funcionar a 110v.
 - b- Interconectar más de 4 equipos.
 - c- Asignar direcciones IP.
 - d- Soportar el estándar Ethernet.
-

► **3** ¿Qué color tiene el pin 8 Norma 568 A?

- a- Rosa.
 - b- Rojo.
 - c- Verde.
 - d- Marrón.
-

► **4** La velocidad del cableado categoría 6 es superior a:

- a- 10 Mbps
 - b- 100 Mbps
 - c- 500 Mbps
 - d- 1000 Mbps
-

► **5** ¿Cuál herramienta no es necesaria al momento de armar una red?

- a- Pinza crimpeadora.
 - b- Alicata para cable UTP.
 - c- Tester UTP/STP.
 - d- Llave inglesa.
-

► **6** ¿Cuál herramientas es útil para quitar el recubrimiento externo del cable UTP?

- a- Cúter.
 - b- Llave inglesa.
 - c- Roseta.
 - d- Cable canal.
-

Respuestas: 1-b, 2-b, 3-d, 4-c, 5-d, 6-a.

Capítulo 3

Configuración de la red



Conoceremos todo sobre las direcciones IP, DNS, el protocolo TCP/IP, los drivers y los puertos.

Configuración de la red

En Windows Vista, es el **Centro de redes y recursos compartidos** el que nos permitirá ajustar la configuración de la red y especificar todos sus parámetros de funcionamiento.

Podemos acceder al **Centro de redes y recursos compartidos** de varias formas: una de ellas es a través del **Panel de control**, con un clic en **Ver el estado y las tareas de red** (dentro del grupo **Redes e Internet**). Si usamos la **Vista clásica** del **Panel de control**, hacemos clic directamente en el icono **Centro de redes y recursos compartidos**. Otra forma es a través del icono de **Red** en el **Área de notificación**, como podemos observar en la **Figura 1**. En la ventana que aparece, tenemos la opción de abrir el **Centro de redes y recursos compartidos**.

La ventana del **Centro de redes y recursos compartidos** (**Figura 2**) se divide en dos paneles:

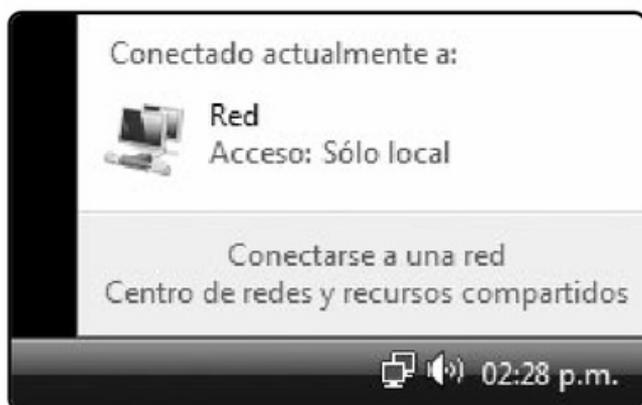


FIGURA 1. El icono de Red nos permite consultar su estado actual.

Podemos acceder al Centro de redes y recursos compartidos de varias formas



FIGURA 2. El Centro de Redes y recursos compartidos nos brinda un resumen del estado de la conectividad de nuestro equipo.

en el izquierdo aparecerá un listado de tareas relacionadas con este tema y, en el derecho, veremos cuatro secciones diferentes.

La primera opción es el mapa de la red; la segunda se refiere a las redes y conexiones de red; la tercera es **Compartir y detectar**, donde se muestran los servicios, su estado (**Activado** o **Desactivado**) y la posibilidad de modificarlo (**Figura 3**).



FIGURA 3. Es muy sencillo cambiar el estado de los servicios de nuestra computadora.

Esto se logra con un clic sobre el estado de la conexión o sobre la flecha de la derecha: entre las opciones que se desplegarán, podemos cambiar la configuración.

Por último, la cuarta sección, ubicada al final del panel, muestra dos enlaces que nos permiten visualizar, de manera sencilla, el listado de archivos y carpetas que estamos compartiendo en la red (Figura 4).

Ahora que nos familiarizamos con esta ventana, llegó el momento de conectarnos a una red (Paso a paso 1).

DRIVERS, CONTROLADORES

Para trabajar con un documento, utilizamos un procesador de textos, es decir, una aplicación para abrir el archivo, editarlo y salvarlo. El sistema operativo es el que nos permite ejecutar la aplicación para procesar el documento.

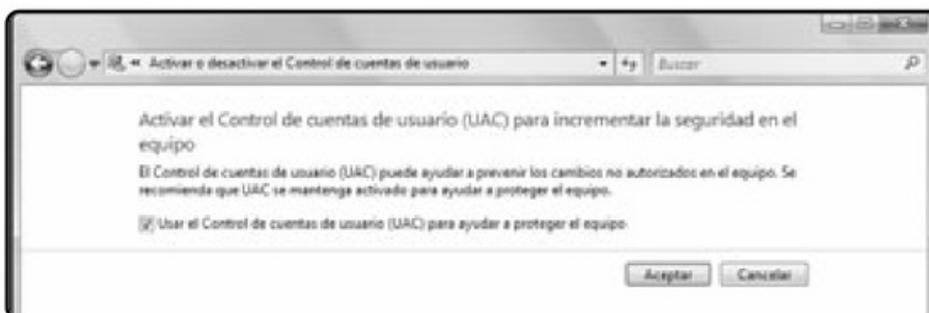


FIGURA 4. El Control de cuentas de usuario se encuentra activado de manera predeterminada en Windows Vista.



LAN

A menudo encontraremos la sigla **LAN** (*Local Area Network*, **Red de área local**). Se utiliza para hacer referencia a redes que comparten una misma subred (en terminología TCP/IP, que ya explicaremos más adelante). En general, una **red hogareña** va a ser una LAN.

PASO A PASO /1

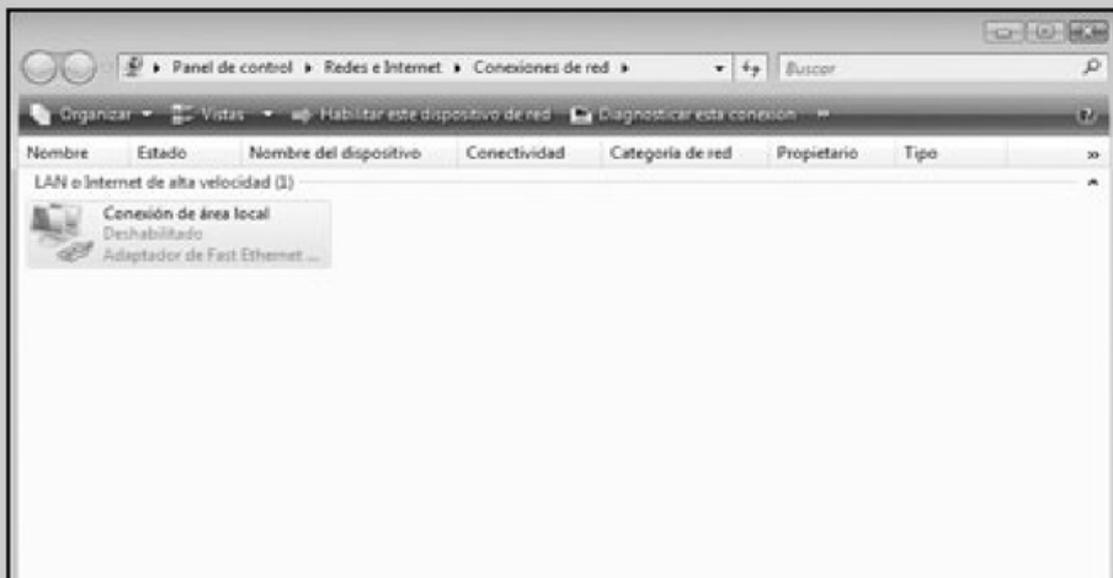
Conectarse a una red

1

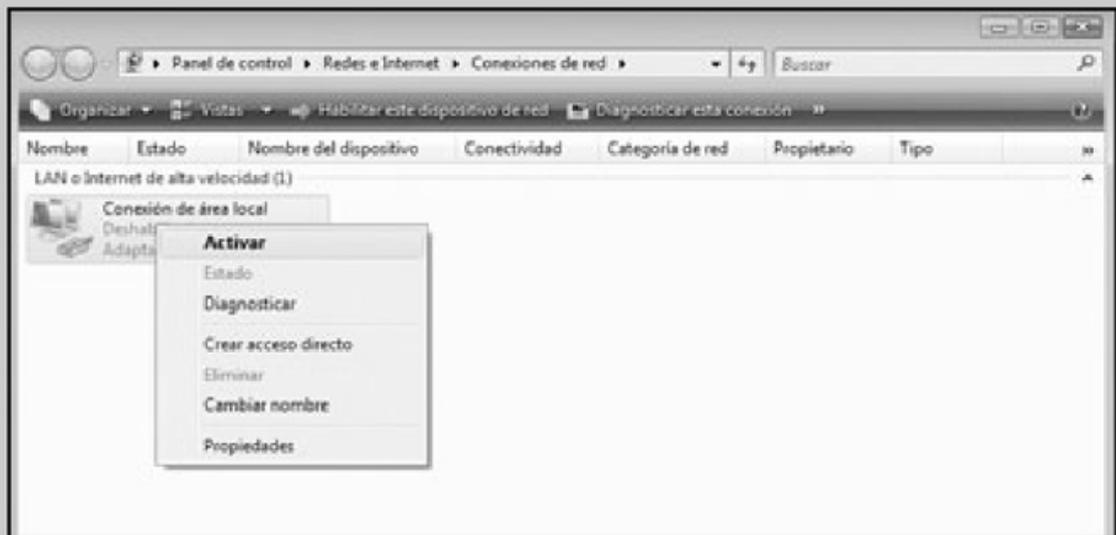


Abra el **Centro de redes y recursos compartidos**. En el panel que aparece a la izquierda, seleccione **Administrar conexiones de red**.

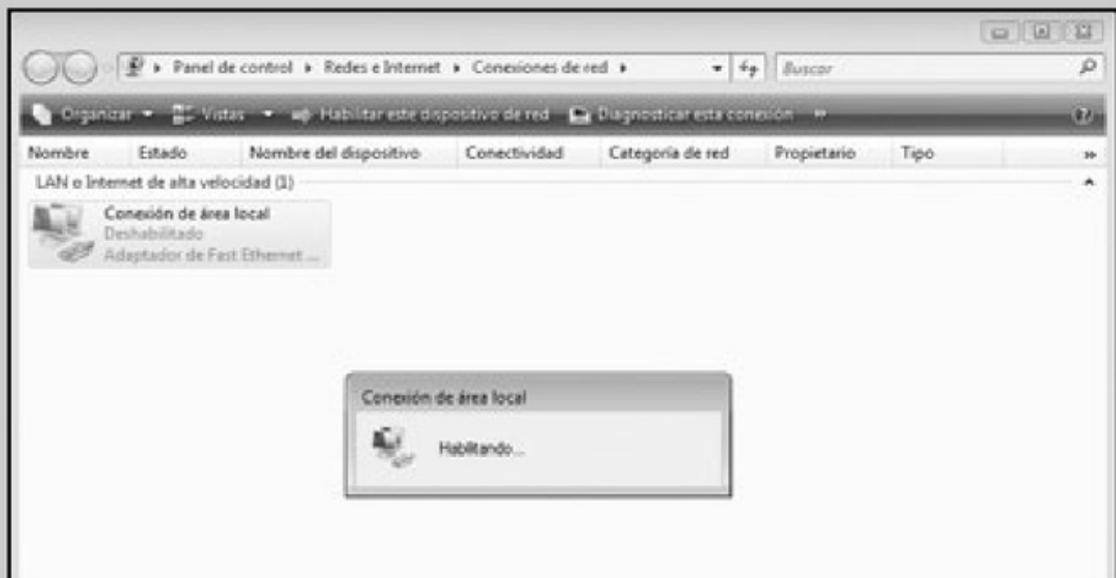
2



Se abrirá la ventana **Conexiones de red**, donde podrá ver los dispositivos que tiene configurados en su equipo y su estado actual.

PASO A PASO /1 (cont.)**3**

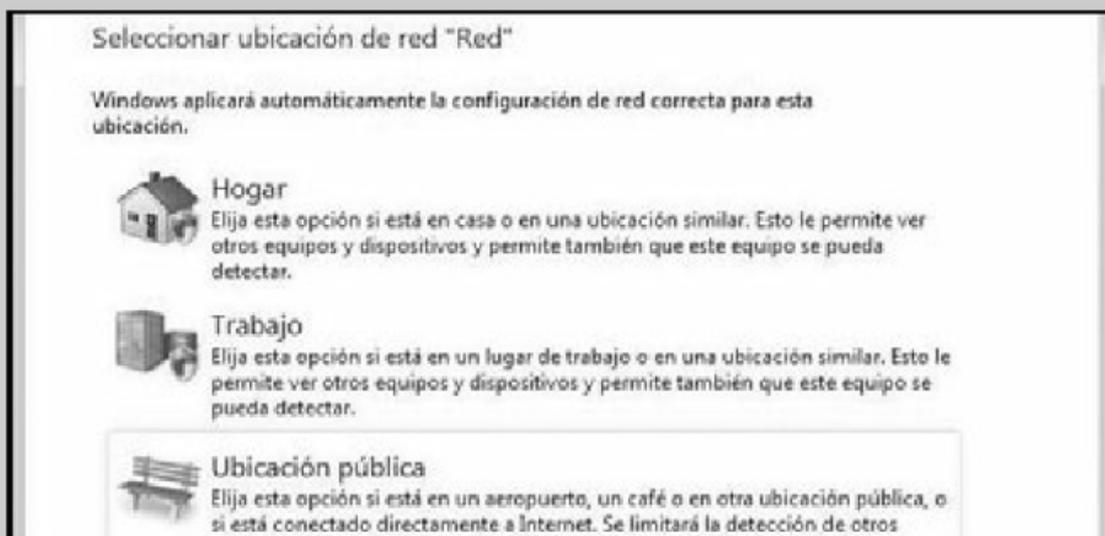
Si el dispositivo aparece en estado **Deshabilitado**, haga clic derecho sobre él y seleccione la opción **Activar** del menú que aparece.

4

Como cuarto paso del procedimiento de conectar la computadora personal a una red, debe esperar un momento mientras la conexión cambia de estado.

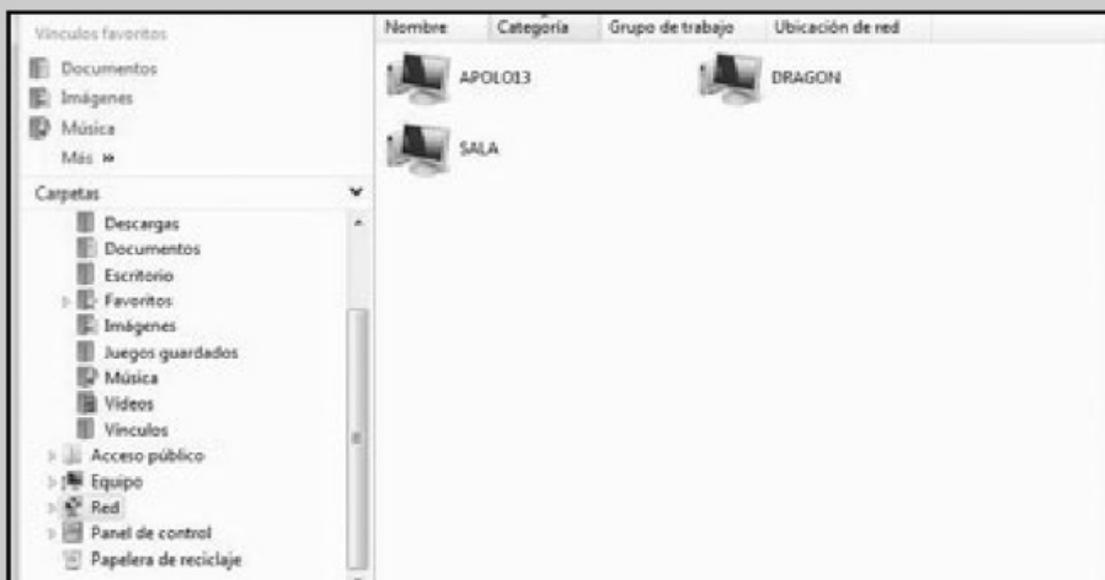
PASO A PASO /1 (cont.)

5



Aparecerá una ventana donde podrá seleccionar la ubicación de red. Cuando se conecte por primera vez a una red, se le presentarán tres opciones: **Hogar**, **Trabajo** y **Ubicación pública**.

6



Una vez definido que su ubicación de red va a ser **Hogar**, quedará conectado. Llegado este punto, si va a **Inicio/Red**, podrá ver los otros equipos que están conectados en su red.

El archivo puede almacenarse en el disco duro del equipo o en una memoria externa USB. Pero al procesador de textos no le preocupa dónde se almacena, le delega esa tarea al sistema operativo.

Cuando trabajamos con la red, tiene lugar una separación de tareas similar: utilizamos un navegador para visitar los sitios web o el **Explorador de Windows** para acceder a los recursos compartidos por otros equipos. Éstas son las aplicaciones que utilizamos con la red. Es el sistema operativo quien se encarga de que esas aplicaciones puedan brindar esa funcionalidad (**Figura 5**).

La conexión del equipo con la red se logra a través de las tarjetas de red, y el sistema operativo interactúa con ellas a través de pequeños programas que

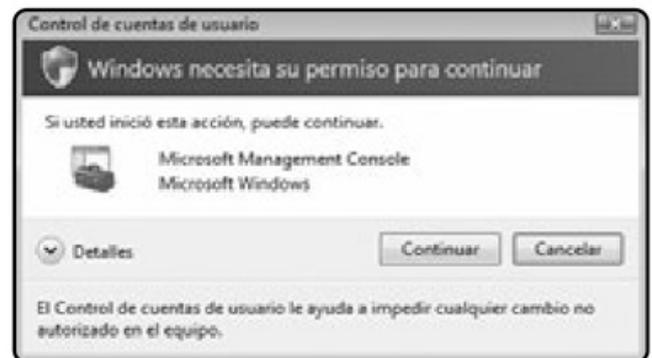


FIGURA 5. Windows nos pide confirmación antes de realizar cualquier acción que pueda poner en peligro el sistema.

reciben el nombre de **controladores**, muy conocidos también por su nombre en inglés: *drivers*. Cada dispositivo que existe en una computadora va a interactuar con el sistema operativo por medio de su controlador o driver. Windows Vista incluye, de manera predeterminada, un gran número de controladores para los dispositivos más comunes, lo que simplifica su instalación y uso.

La conexión del equipo con la red se logra a través de las tarjetas de red



SEGURIDAD

Garantizar la seguridad de nuestros equipos debe ser una prioridad: por un lado, debemos asegurar nuestro sistema lo más posible con el objetivo de cerrarle la entrada a intentos de acceso no autorizados por él y, por el otro, asegurar el acceso sencillo a equipos conocidos.

En aquellos casos en los que Windows Vista no sea capaz de detectar e instalar los controladores apropiados para un dispositivo, quedará por parte del fabricante o proveedor suministrárnoslo, ya sea mediante un CD de instalación que viene empaquetado junto con el dispositivo, o por medio de algún enlace para su descarga en Internet, citado en la documentación. De una forma u otra, siempre es necesario contar con los drivers adecuados para que un dispositivo funcione correctamente.

Es importante destacar que no todos los controladores son compatibles con Windows Vista. Utilizar uno disponible para otra versión de Windows es un riesgo que debemos evitar. Su instalación podría llevar el sistema operativo a un estado de operación inestable. Windows Vista nos permite gestionar los controladores a través de una opción del **Panel de control**, llamada **Administrador de dispositivos**. Esta ventana clasifica los dispositivos de acuerdo con categorías, sobre la base de su funcionalidad (**Figura 6**).



FIGURA 6.
El Administrador de dispositivos clasifica los dispositivos de acuerdo con categorías, sobre la base de su funcionalidad.



UBICACIONES DE LA RED

Vista denomina **Ubicación de red** al tipo de red al que nos conectemos. Las opciones son **Hogar**, **Trabajo** y **Ubicación pública**. Las dos primeras definen una ubicación privada, mientras que la última se clasifica como red pública.



Comprobar la correcta instalación de los controladores

Como mencionamos, Windows Vista incluye controladores para un gran número de dispositivos. Es muy probable que, cuando instalamos la tarjeta de red en nuestro equipo, Vista automáticamente la haya detectado y haya instalado el controlador correspondiente, pero ¿si ése no fuera el caso?

El primer paso será comprobar que el controlador esté bien instalado y, con este objetivo, debemos asegurarnos de tener el controlador correcto. Por lo general, las tarjetas incluyen un CD de instalación donde se encuentra el controlador. Si nuestro equipo tiene la tarjeta en el motherboard, entonces el controlador estará en el CD de instalación que trajo nuestra placa madre o equipo, si lo compramos ya armado.

Windows Vista incluye controladores para un gran número de dispositivos

También podemos conectarnos al sitio web del fabricante y descargar manualmente el controlador directamente desde allí. Esto tiene la ventaja de que tendríamos el controlador más actual disponible.

Los controladores, como todo programa, pueden tener errores de programación que el fabricante corrige y pone a disposición de los usuarios como nuevas versiones disponibles para la descarga. Un error corregido no es la única razón para una nueva versión, ya que también puede ser una nueva funcionalidad o una mejora en el rendimiento. Por eso, es recomendable que siempre visitemos el sitio web del fabricante para instalar los últimos controladores disponibles para nuestros dispositivos.

Si no sabemos cuál es, podemos teclear en un buscador (**www.google.com** es una buena elección) todos los datos que encontremos del dispositivo: nombre del fabricante, modelo de la tarjeta, sistema operativo, y las palabras **controlador** y **descargas**,



UBICACIÓN HOGAR Y TRABAJO

Si nuestra ubicación de red es **Hogar** o **Trabajo**, el nivel de seguridad nos permitirá ver otros equipos y dispositivos conectados en la red, así como que el nuestro se pueda detectar. Esto es conveniente en entornos controlados donde podemos confiar en los otros equipos.

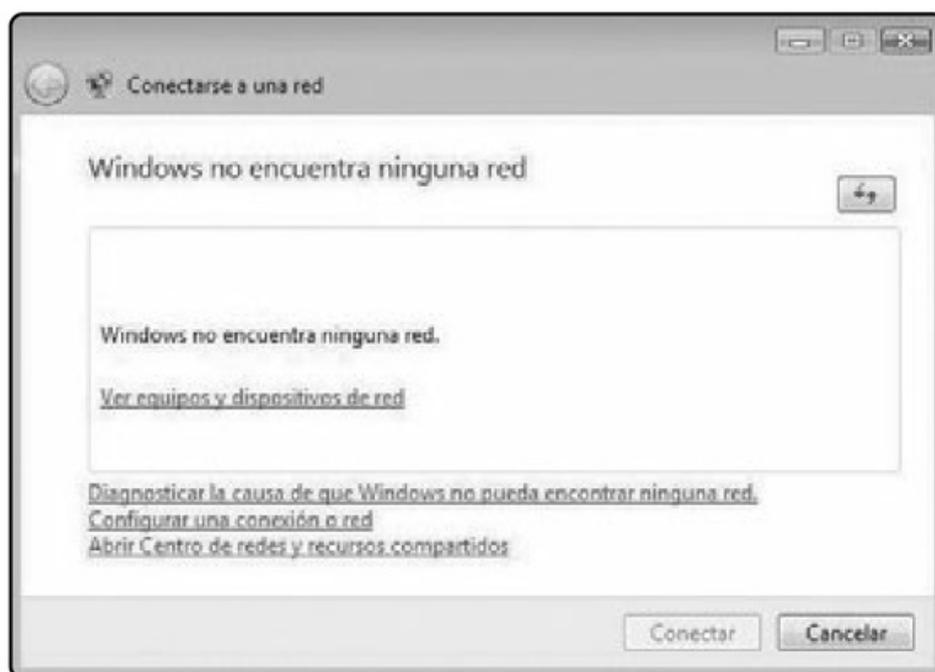
para identificar que estamos buscando el controlador y queremos que nos localice las páginas que tienen vínculos para la descarga. En los sitios de los fabricantes, por lo general, los controladores se encuentran en las páginas de **Soporte técnico (Figura 7)**.

Si no tenemos el controlador a mano, tampoco es motivo de preocupación. Windows Vista nos brinda la posibilidad de ayudarnos en esta tarea. A través del **Administrador de dispositivos**, podemos comprobar los controladores instalados

y realizar las acciones necesarias para solucionar este problema (**Paso a Paso 2**).

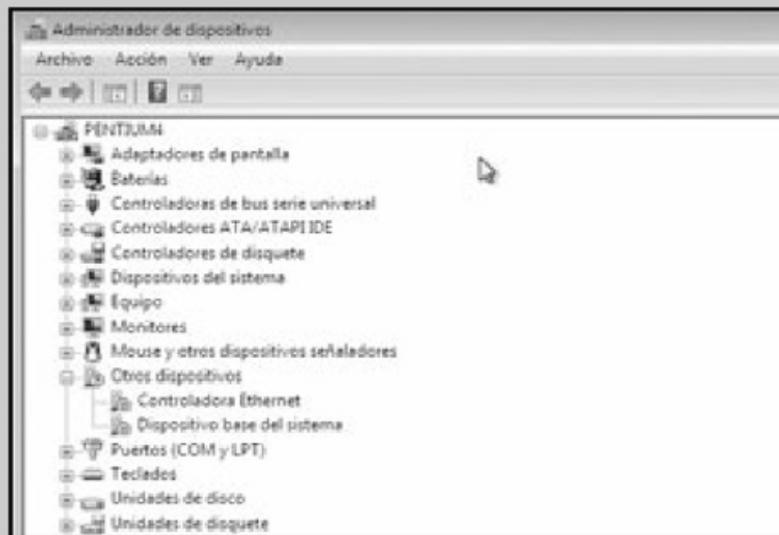


FIGURA 7.
No confundir con un problema: por defecto, Vista solo muestra las redes que hemos configurado. Es lógico entonces que, de manera predeterminada, no encuentre ninguna red.

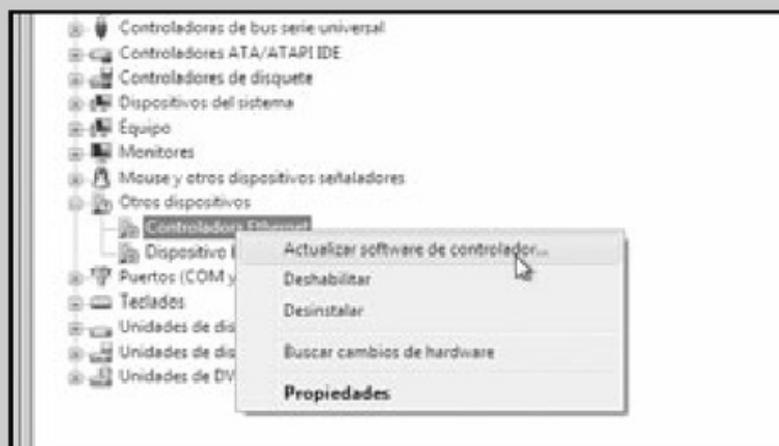


► UBICACIÓN PÚBLICA

Para la red que queremos configurar, vamos a seleccionar siempre el tipo de ubicación **Hogar**. El caso de **Ubicación pública** se utiliza cuando hay una conexión directa a una red sobre la cual no tenemos control, ya sea conectándonos a Internet o en un lugar público.

PASO A PASO /2**Instalar el controlador de un dispositivo****1**

Abra el **Administrador de dispositivos** desde **Inicio/Panel de control/Sistema y mantenimiento/Ver hardware y dispositivos**. Vista ubica cada dispositivo dentro de la categoría que le corresponde. Por lo general, en **Otros dispositivos** aparecen los que no tienen una categoría definida y los que no han sido correctamente reconocidos. En su caso, le interesará el llamado **Controladora Ethernet**.

2

Haga clic derecho sobre el dispositivo y, en la ventana que se abre, seleccione la primera opción: **Actualizar software de controlador**.

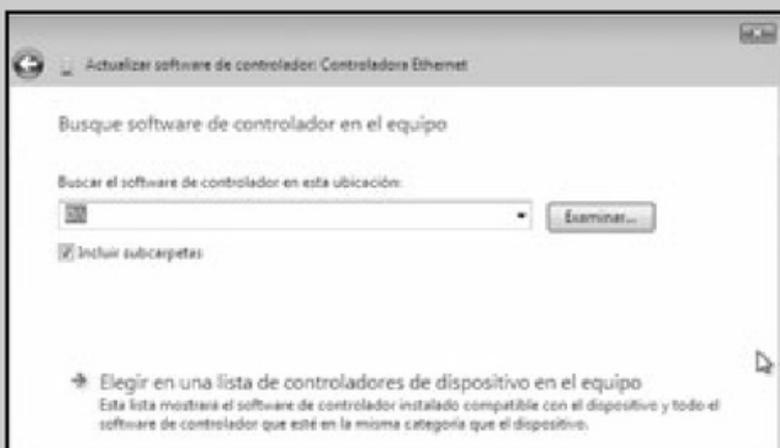
PASO A PASO /2 (cont.)

3



Vista le brinda dos formas de obtener el software del controlador: la primera es dejar que el sistema haga una búsqueda en Internet, directamente en el sitio de Microsoft; la segunda es para aquellos casos en los que tiene los controladores proporcionados por el fabricante previamente, o no tiene Internet. Si tiene el CD de instalación del fabricante, seleccione **Buscar software de controlador en el equipo**.

4



Teclee la ubicación donde se encuentra el software o búsquela a través de la ventana que se abre si selecciona el botón **Examinar...** La segunda opción de esta ventana, **Elegir en una lista de controladores de dispositivo en el equipo**, lo conduce al listado de controladores que Vista incluye de manera predeterminada. En algunos casos, no contará con el controlador específico, pero tendrá conocimiento de uno similar que sí está disponible. Esta opción es conveniente en esos casos.

PASO A PASO /2 (cont.)

5



Si seleccionó la búsqueda en línea, encontrará tres opciones: **Sí, buscar en línea (recomendado)**; **Sí, buscar en línea sólo esta vez** y **No buscar en línea**. Con la primera opción, puede señalarle a Vista que siempre busque en Internet automáticamente. Si no cuenta con conexión a Internet, o prefiere enterarse cada vez que Windows necesite instalar un dispositivo, seleccione la segunda opción. La tercera es por si cambia de opinión.

6

Cuando seleccione la opción de buscar el controlador en Internet, Vista le mostrará una ventana de progreso, mientras dura el proceso de búsqueda. En este caso, como se decidió instalar el controlador desde el CD, la instalación comenzará al instante.

EL PORQUÉ DE LA UTILIZACIÓN DEL SISTEMA BINARIO

La elección del sistema binario tiene que ver con que, en el mundo electrónico, son muy comunes las situaciones de dos opciones: la polaridad del voltaje (positivo o negativo), la presencia de voltaje (hay o no hay), el nivel de voltaje (por encima o por debajo de un valor).

PASO A PASO /2 (cont.)

7



Al finalizar la correcta actualización del software de controlador, aparecerá una ventana que lo indica.

8



De esta manera, el **Administrador de dispositivos** le mostrará, ahora, el controlador debidamente instalado bajo la categoría correspondiente, en este caso **Adaptadores de red**.

LAS PROPIEDADES DE LOS CONTROLADORES

Además de poder actualizar el controlador de un dispositivo, el **Administrador de dispositivos** nos permite tener acceso a todo el grupo de propiedades que le corresponden (**Figuras 8 y 9**).

El acceso a las propiedades se obtiene con un clic derecho sobre el dispositivo y con la selección de la opción **Propiedades** del menú. Otras opciones de ese menú son la posibilidad de **Habilitar** o **Deshabilitar** el dispositivo (acorde con el estado en que se encuentre, si estuviese activado, se muestra solo la opción de **Deshabilitar**); **Desinstalar** el dispositivo, y la de actualizar el controlador.



FIGURA 8. Al hacer clic derecho sobre un dispositivo, en el Administrador de dispositivos, veremos este menú contextual.



FIGURA 9. La pestaña General nos muestra información sobre el dispositivo y su estado.

La ventana de **Propiedades** se divide en varias pestañas. En la primera, llamada **General**, podemos verificar el estado en que se encuentra el dispositivo y sus datos generales. En **Opciones avanzadas** aparecen un conjunto de propiedades que nos permiten controlar distintos aspectos del funcionamiento del controlador. Estas propiedades varían de acuerdo con el dispositivo y el controlador instalado. En el caso de los adaptadores de red, aquí podemos configurar el tamaño de los paquetes que se transmiten por la red, el tipo de conexión y la velocidad.

El acceso a las propiedades se obtiene con un clic derecho sobre el dispositivo y con la selección de la opción **Propiedades** del menú

Estas propiedades en muy rara ocasión podrían necesitar una modificación y, en esos casos, deberá ser realizada por profesionales en el tema.

En ocasiones, un dispositivo puede entrar en **conflicto** con Vista, ya sea porque la versión del controlador no es compatible con este sistema operativo, o porque otro dispositivo está provocando el conflicto.

Si hiciera falta desinstalar el controlador de este dispositivo, sería en la pestaña **Controlador (Figura 10)** donde lo haríamos. También se puede deshabilitar desde aquí, pero además tenemos la opción de hacerlo directamente desde el menú contextual del dispositivo.

Las pestañas **Detalles** y **Recursos** nos brindan información adicional sobre el dispositivo y los recursos que ocupa en el sistema. La última pestaña, **Administración de energía** le permite al sistema operativo controlar el consumo de energía que realiza el dispositivo.

CONEXIONES DE RED

Como ya dijimos, la computadora se conecta a la red a través de una interfaz o adaptador de red (también conocidos como placas o tarjetas de red). Ya tenemos la placa funcionando y su controlador correctamente instalado. El dispositivo de red está listo para



FIGURA 10. Podemos actualizar el controlador del dispositivo desde la pestaña Controlador.

trabajar. Pero esa es solo la primera parte. Windows Vista utiliza los dispositivos de red para crear las **Conexiones de red**, que son las responsables de brindar la conectividad al sistema operativo.

Las conexiones de red se clasifican de acuerdo con el alcance de la red a la cual brindan acceso. De la misma manera, Windows Vista les asigna automáticamente un nombre que identifica el tipo de red. Es importante tener en cuenta que cada equipo va a mostrar aquellos dispositivos y redes a las que tenga acceso.



WoL

Existe una funcionalidad llamada *Wake on LAN (WoL)* o **iniciar por la red** que le permite a un equipo ser encendido sin interacción humana, a través de los adaptadores de red. Es una funcionalidad que está incorporada en la tarjeta de red, aunque no todas la tienen.



Es normal que lo que vemos en el **Panel de control** de una computadora, sea distinto de lo que vemos en el de otra. El ejemplo más directo lo encontramos en las imágenes de este libro. Por eso, no debemos preocuparnos si no coinciden con lo que vemos en la pantalla de nuestro monitor, ya que eso es normal debido a que el hardware y las conexiones varían.

Podemos acceder a las **Conexiones de red** a través del menú **Tareas** que aparece a la izquierda de la ventana del **Centro de redes y recursos compartidos** del **Panel de control**. En el panel **Conexiones de red**, la categoría más frecuente es **LAN o Internet de alta velocidad** (Figura 11), pero esto no quiere decir que sea la única. De acuerdo con los tipos de conexiones que tengamos configurados, podemos tener otros como **Red privada virtual** y **Banda ancha**. Cada adaptador que Vista detecta se identifica con un nombre. De manera predeterminada, el primer adaptador recibe el nombre de **Conexión de área local** y, los siguientes, Vista los distingue numéricamente. Por ejemplo, si tuviéramos un segundo adaptador (como otra tarjeta de red, por caso), se llamaría **Conexión de área local 2**.

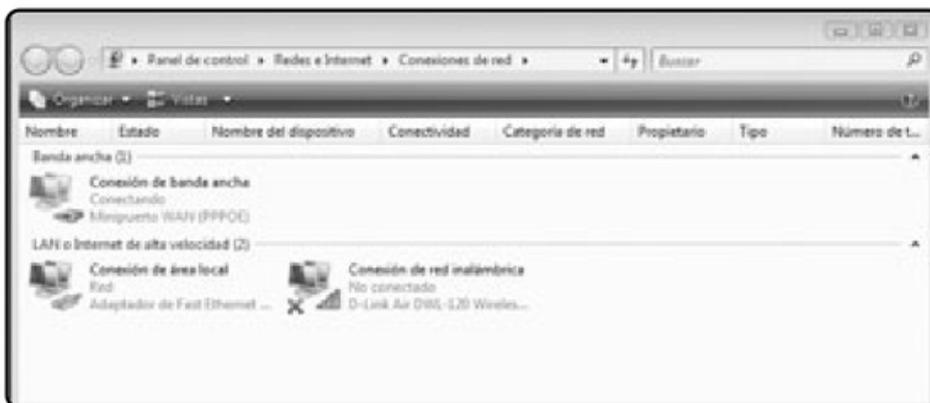


FIGURA 11.
Algunos proveedores de Internet nos brindan la conexión a través de un enlace de Banda ancha.



WAN

La necesidad de conectar las redes LAN entre sí da lugar a la aparición de las **WAN**, siglas del inglés *Wide Area Network* o **red de área amplia**. Las WAN son redes que se extienden más allá del ámbito local en un edificio y sirven para interconectar varias redes entre sí.



Las computadoras utilizan estándares que definen la forma en que establecen la comunicación entre ellas

EL PROTOCOLO TCP/IP

Las computadoras utilizan **estándares** que definen la forma en que establecen la comunicación entre ellas. Los **protocolos** son parte importante de esos estándares. Un protocolo determina una serie de parámetros que deben ser respetados para establecer una comunicación. Si dos equipos utilizan el mismo protocolo, van a ser capaces de poder comunicarse entre sí. Parece sencillo, pero en cualquiera de las operaciones que realizamos cotidianamente a través de una red intervienen un sinnúmero de protocolos.

En las redes de Windows, se utiliza la denominación de protocolo para referirse, en particular, a los protocolos de red, la parte que se encarga del envío de los paquetes de información a través de la red (**Figura 12**). Las primeras versiones de Windows utilizaban un protocolo llamado **NetBEUI** descendiente, a su vez,

de otro diseñado por **IBM (NetBIOS)**. Por esa época, era normal que cada fabricante tuviera un protocolo propietario. **Novell** tenía uno muy conocido (**IPX/SPX**), incluso **Apple** también tenía el suyo (**AppleTalk**). Y en el mundo académico de las universidades, donde variantes del sistema operativo Unix eran familiares, era muy frecuente un protocolo llamado **TCP/IP**.

No fue casualidad que todos los grandes fabricantes de sistemas operativos hayan decidido abandonar sus variantes **propietarias** de protocolos a favor de uno común. Fue el desarrollo de Internet el que impulsó (más bien podríamos decir *impuso*) esta modificación. A diferencia de grandes cambios que han sucedido en la historia de la computación motivados por los intereses económicos de una o un grupo de empresas, la migración hacia TCP/IP estuvo motivada



TCP/IP

Hasta aquí hemos mencionados **protocolos propietarios**, pero existen **protocolos abiertos**, como es el caso de TCP/IP. En este caso, la separación viene marcada por el acceso a las especificaciones del protocolo, publicación que depende del creador del protocolo.



FIGURA 12.
Si es la primera
vez que ejecutamos
Inicio/Red, la ventana
aparecerá vacía.

por las ventajas técnicas que dicho protocolo ofrecía. Los protocolos existentes en ese momento (NetBEUI, Appletalk) cumplían cabalmente la función para la cual fueron diseñados: brindar conectividad entre grupos reducidos de equipos en una red de área local. Pero las redes fueron creciendo, expandiéndose no solo en el ámbito local, sino también geográfico, y cuando se tenía una oficina en una ciudad y se abría una segunda en otra, la conexión de ambas no era tarea fácil. Los protocolos para redes LAN tenían limitaciones para las redes WAN. Sin embargo, TCP/IP se había diseñado para funcionar a través de

este tipo de redes, distribuidas geográficamente. Y los fabricantes de sistemas operativos empezaron a utilizar este protocolo en sus productos para facilitarles a sus clientes el trabajo y la interconexión.

Una gran familia

Aquí amerita hacer una corrección. La forma apropiada de referirse es la **familia de protocolos** TCP/IP. Pero no debemos preocuparnos, el uso del singular está tan extendido que se acepta sin problema alguno. Esto no quita la aclaración. No existe un protocolo que se llame así, lo que sí hay es una



RED HOGAR

En las redes externas pueden encontrarse personas con la intención de conectarse a nuestro equipo para introducirnos virus o robar nuestra información. Por eso, si ubicamos nuestra red como **Hogar** limitaremos la detección de otros equipos y, también, la del nuestro.

familia de protocolos de los cuales TCP es uno, IP es otro, y existen unos cuantos más que hacen su trabajo desde el "anonimato" sin que nos enteremos de sus nombres, aunque sí utilizamos a diario sus beneficios. Por ejemplo, cada vez que nuestra computadora actualiza la hora por Internet, no lo hace con TCP, sino con otro protocolo llamado **UDP** (tanto TCP como UDP utilizan IP). Ya son demasiadas siglas para un solo apartado, mejor continuemos con el próximo.

La dirección IP

Cuando queremos establecer comunicación entre dos equipos, éstos deben saber cómo encontrarse. Pero ¿cómo se encuentran las máquinas entre sí? Al igual que nosotros, a través de una dirección. En este caso, como utilizamos el protocolo TCP/IP, la dirección la determina el **protocolo IP** (*Internet Protocol*) y se llama, casualmente, **dirección IP**.

Cada vez que escuchamos el término dirección IP, se está haciendo referencia a una forma de encontrar un equipo en una red. La dirección IP es un **número** que va a ser único para cada equipo que se conecte a la red. En Internet, cada equipo que se conecta tiene un número asignado: su dirección IP,

gracias a la cual se podrá encontrar una computadora en Internet (**Figura 13**).

Las direcciones siempre van a ser direcciones. Quizás un taxista de Buenos Aires sea incapaz de indicarle a otro cómo llegar a una dirección en Madrid. Sin embargo, si enviamos una carta por correo postal desde la Argentina a España, podemos estar seguros



FIGURA 13. Al Panel de control, desde donde configuraremos direcciones y protocolos, accedemos con solo dos clics.

▶ IPv6

El crecimiento de Internet y los requerimientos de nuevas asignaciones de direcciones IP provocarán su agotamiento en un futuro no muy lejano. Por esta razón, se está migrando a IPv6, que tendría suficientes direcciones como para no necesitar un cambio en el futuro.

de que la dirección de destino va a ser encontrada. Al enviar una carta, es muy probable que lo primero que escribamos sea el nombre del destinatario, luego la calle y el número del edificio o casa; más abajo el nombre de la ciudad y estado o provincia, y por último el país (por ahora me reservo el código postal). En la oficina de correos, van a utilizar un orden inverso al que usamos para escribir la dirección a la hora de encaminarla rumbo a su destino. Primero se van a fijar en el último ítem, el país, y separarán la carta junto con las demás que vayan, por ejemplo, a la Argentina. Luego, cuando la carta esté en la Argentina, van a clasificarla de acuerdo con el estado o provincia, y así sucesivamente hasta llegar a su destinatario. El código postal sirve como un atajo en el ámbito nacional que le indica a la oficina de correos

local cuál es la oficina de correos específica donde le va a corresponder a un cartero entregar la carta y, de esta manera, se hace más rápida su entrega.

Las direcciones IP funcionan exactamente de la misma manera. Cada país tiene asignado un **bloque** de números IP (en terminología de redes se utilizan indistintamente los términos de número IP y dirección IP). Cuando una computadora necesita acceder a otra, lo hace a través de la dirección IP, y para que el paquete llegue al destino, se lo entrega su **enrutador**, que funciona como la oficina de correos local. El enrutador, también conocido como **puerta de enlace** o por su nombre en inglés **router**, es un equipo que permite conectar varias redes entre sí. A partir de ahí, existe un grupo de enrutadores



El enrutador, también conocido como puerta de enlace o por su nombre en inglés router, es un equipo que permite conectar varias redes entre sí



NÚMERO DE DIRECCIÓN IP

Una dirección IP es un número de 32 bits. Se representa como cuatro octetos que toman uno de los 255 valores disponibles: de 0 a 254. La cantidad de números que se puede armar con la combinación de ocho bits es, precisamente, de 256 valores.

conectados entre sí que garantizan la conexión entre dos puntos cualquiera en Internet. De a poco, el paquete va a ir pasando de enrutador en enrutador hasta llegar al que se encarga de manejar el bloque de direcciones al cual pertenece la dirección IP destino.

DNS

Supongamos que queremos visitar el sitio web de nuestra editorial: **www.redusers.com**. Esto no es una dirección IP, por lo que necesitamos una para que nuestra máquina pueda acceder al equipo donde está ese sitio web. La respuesta es: no va a necesitar conocerla. Al teclear en nuestro navegador el nombre del sitio web, le estamos indicando a dónde queremos ir.

Es nuestra computadora la que se va a encargar, a partir de ese nombre, de encontrar la dirección IP que le corresponde, de conectarse al servidor, de descargar la página web y mostrárnosla en nuestro navegador. El servicio que se encarga de **traducir los nombres de sitios** y direcciones IP se llama **DNS (Servicio de Nombres de Dominio** o *Domain Name Service*) y es uno de los pilares de Internet.

Gracias al DNS es que nuestro navegador puede contactar los sitios web. También es el responsable de que los correos electrónicos lleguen a su destinatario final. Para utilizar el DNS, existen servidores de-



dicados a ofrecer ese servicio. Este dato también se le asigna a nuestro equipo de manera automática.

CON USTEDES, LOS PUERTOS

Ya conocemos todo lo que necesitábamos saber sobre TCP/IP. Un último detalle: los **puertos**. Imaginemos ahora que alguien quiere enviarme una carta. Ya tiene mi nombre, le podremos dar la calle donde vivimos y el número, la ciudad, el país y el código postal. Si somos los únicos que vivimos en esa dirección, vamos a recibir la carta sin problemas. Pero ¿si vivimos en un edificio? Todos los inquilinos vamos a compartir

Gracias al DNS es que nuestro navegador puede contactar los sitios web

PPP

PPPoE son las siglas de *PPP over Ethernet*. PPP, a su vez, son las siglas de *Point to Point Protocol* o **Protocolo de punto a punto**, un protocolo que surgió para comunicar vía TCP/IP a través de los cables de cobre. Las líneas telefónicas son un ejemplo de este tipo de cable.

la misma dirección. Nosotros vivimos en un departamento que tiene un identificador único en el edificio entonces, si les damos el número de departamento, la carta nos va a llegar a nosotros directamente.

Algo similar sucede con los **servicios** que se ofrecen en Internet. Por un lado está el sitio web, por otro el correo electrónico, y por otro la transmisión de archivos. Si dependiéramos de la dirección IP para cada servicio, se crearía un caos, ya que necesitaríamos una dirección para cada servicio. Por suerte, en terminología TCP/IP, existe lo que se denomina puertos (TCP/IP *ports*). Cada servicio que se ejecuta en un servidor utiliza un puerto determinado (**Figura 14**).

Por ejemplo, los sitios web funcionan con el **puerto 80**, la mensajería utiliza el **puerto 25** (si alguna vez hemos tenido que configurar un cliente de e-mail es probable que nos sea familiar), además del **puerto 110** que se utiliza para descargar los mensajes y que también es conocido por el nombre del protocolo: **POP3** (es la versión 3 del protocolo **POP** que, vale la pena aclarar, significa *Post Office Protocol* o **protocolo de oficina de correos**).

El concepto de puertos es tan irrelevante en el entorno de una red hogareña como relevante si nos conectamos a Internet. Solo debemos tener en cuenta que las conexiones TCP/IP utilizan un puerto para



FIGURA 14.
Es recomendable utilizar la Vista clásica del Panel de control hasta que nos acostumbremos a la nueva, sobre todo si tenemos que hacer modificaciones complejas como la de los puertos.



NETBIOS

Hoy en día, todo el mundo habla de TCP/IP, pero esto no fue así en un inicio. El primer protocolo usado por las redes de computadoras personales fue el **NetBIOS** (*Network Basic Input/Output System* o **sistema básico de entrada/salida para la red**), desarrollado por IBM.

establecer la comunicación entre dos equipos y que se utiliza un puerto tanto en el **destino** como en el **emisor**. Más adelante, cuando hablemos de los **firewalls**, el tema de los puertos tendrá más sentido.

WINDOWS VISTA Y LAS REDES

Una de las tareas que aparecen en el **Centro de redes y recursos compartidos** es **Configurar una conexión o red**. En el menú **Inicio** vimos que la opción que aparece debajo de **Red** es **Conectar a**. Si hacemos clic en esta última, veremos una ventana con las redes disponibles y a las que estamos conectados. Desde esta ventana, se ejecutarán distintos asistentes que nos ayudarán a configurar el tipo de conexión o red seleccionada.

La primera opción (**Figura 15**) es **Conectarse a Internet**. De acuerdo con el tipo de conexión a Internet que tengamos en nuestro hogar, es probable que debamos emplear esta opción.

Si el tipo de servicio que nuestro proveedor nos ofrece es **PPPoE** (*PPP over Ethernet*) y nos estamos conectando a Internet a través de un equipo con Windows Vista, este asistente nos va a guiar en el proceso de conexión. Es tan sencillo como teclear el nombre de usuario y la contraseña que nos entregó nuestro proveedor y, a continuación, decidir si esta conexión va a poder ser utilizada o no por otros usuarios en ese equipo.

Si tenemos una red inalámbrica, es la segunda variante, **Configurar un enrutador o punto de acceso inalámbrico**, la que debemos seleccionar. Estos pasos los veremos en detalle en el **Capítulo 5**.

En algunas ocasiones, necesitamos recurrir a las líneas telefónicas como medio de comunicación. Aun cuando los proveedores de Internet no ofrezcan servicio en nuestra zona, es muy probable que las empresas telefónicas tengan líneas instaladas y en



FIGURA 15.
Después de seleccionar la opción Configurar una conexión o red veremos esta ventana.



En algunas ocasiones, necesitamos recurrir a las líneas telefónicas como medio de comunicación

funcionamiento desde años atrás. Para estos casos, debemos **Configurar una conexión de acceso telefónico**. Previamente, debimos haber instalado el módem a nuestro equipo.

El asistente nos permite crear una conexión al teclear el número telefónico al que vamos a conectarnos, el nombre de usuario y la contraseña. Opcionalmente, le podemos dar un nombre identificativo, como por ejemplo, el del proveedor que estamos utilizando, y decidir si esta conexión va a estar disponible para el resto de los usuarios del equipo.

Una de las razones para utilizar una conexión telefónica de acceso remoto era para conectarnos a nuestra oficina. La cuarta variante nos asiste en estos casos si seleccionamos **Conectarse a un área de trabajo**. A la configuración de un acceso

remoto telefónico (es igual a la tercera variante), se suma la conexión mediante una VPN a través de Internet. Más adelante, hablaremos de las VPN o redes privadas virtuales (*Virtual Private Network*), que es una forma de armar una red local entre puntos distantes geográficamente (**Figura 16**).

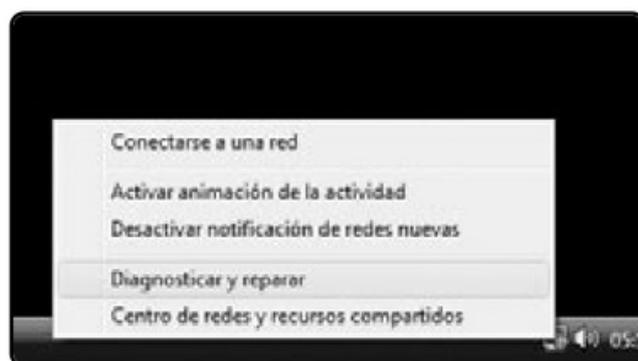


FIGURA 16. Podemos reparar la red desde el icono de red ubicado en el Área de notificación.



RESUMEN

En este capítulo, conocimos cómo configurar la red. Aprendimos a conectarnos a la red e instalar el controlador de un dispositivo. Conocimos todo sobre la dirección IP, DNS, el protocolo TCP/IP, los drivers y los puertos.

Multiple choice

► **1** El Centro de redes y recursos compartidos nos permitirá, entre otras cosas:

- a- Conocer el estado de los controladores de audio y video del equipo.
 - b- Definir la configuración de seguridad de la computadora.
 - c- Conocer el mapa completo de la red, y su configuración.
 - d- Navegar la web.
-

► **2** ¿Qué significa la sigla LAN referida a redes informáticas?

- a- Los Autos Nuevos.
 - b- Líneas Auto Negociables.
 - c- Linux, Apple, Novell.
 - d- Local Area Network.
-

► **3** Un controlador o driver se utiliza con el fin de:

- a- Cuidar la seguridad del equipo.
- b- Jugar a juegos de rol.

- c- Manejar la conexión a internet.
 - d- Poder utilizar un dispositivo correctamente.
-

► **4** Una WAN es:

- a- Una red que interconecta diferentes redes LAN.
 - b- Una comida oriental.
 - c- Internet.
 - d- Una red intercontinental.
-

► **5** El protocolo TCP/IP es:

- a- Producido por Apple.
 - b- Compatible con Linux.
 - c- Compatible con Mac.
 - d- Un estándar abierto.
-

► **6** El servicio DNS:

- a- Convierte números binarios a decimales.
 - b- Convierte números hexadecimales a binarios.
 - c- Convierte octetos a pares.
 - d- Traduce direcciones IP en direcciones web.
-

Respuestas: 1-c, 2-d, 3-d, 4-a, 5-d, 6-d.

Capítulo 4

Uso de la red



Conoceremos los tipos de ubicaciones de red y aprenderemos a formar parte de un grupo de trabajo.

Uso de la red

La forma más rápida de ver los otros equipos en la red es a través del menú **Inicio**, con un clic en **Red**. La ventana que se abre es el **Explorador de la red**, y allí veremos los equipos, las impresoras u otros dispositivos que estén conectados en la red. Esta ventana es el sucesor de **Mis sitios de red** que traía Windows XP.

Como suele suceder, primero aprendemos a gatear, después a caminar y luego a correr. De la misma manera, primero nos conectaremos a nuestra red local y veremos los otros equipos, después compartiremos recursos entre los equipos y, finalmente, conectaremos nuestra red a Internet. Es importante tener en cuenta este concepto porque la estructura del libro asume ese orden. No debemos conectar una computadora a Internet hasta no haber leído el capítulo relacionado con ésta.

Cuando hacemos clic en **Red** y se carga la ventana del explorador, ésta puede estar vacía. Si éste es el caso, en su lugar, un mensaje en la parte superior de la ventana nos alerta: **La detección de redes y el uso compartido de archivos están desactivados. No se podrá ver ningún equipo ni dispositivo de red (Figura 1).**



Windows Vista toma recaudos en su configuración predeterminada. Por ejemplo, inicialmente el sistema deshabilita un grupo de servicios. Si tenemos nuestro equipo en una red local y sin conexión a Internet, podemos hacer clic en dicho mensaje y activar los servicios que se nos piden.

Una de las novedades del explorador de la red en Windows Vista es que, más allá de mostrarnos las PCs y sus recursos compartidos, es capaz de utilizar iconos distintivos para enseñarnos otros servicios o dispositivos que existan en la red.

En la ventana del explorador de la red, deben aparecer todos los equipos que nuestro sistema operativo reconozca. Por ahora, no debemos preocuparnos si solo está nuestro equipo, ya que todavía quedan algunos detalles por configurar.

CENTRO DE SINCRONIZACIÓN

El Centro de sincronización nos permite mantener copias sincronizadas de archivos y carpetas no solo con otras computadoras personales, sino con dispositivos móviles, tan en uso hoy en día, como teléfonos celulares.

La forma más rápida de ver los otros equipos en la red es a través del menú Inicio, con un clic en Red

TIPOS DE UBICACIONES DE RED

Windows Vista se toma en serio el tema de la seguridad, y uno de sus recursos es el concepto de **ubicaciones**. Una ubicación no es más que la descripción de un entorno. Vista nos presenta tres opciones: **Hogar**, **Trabajo** y **Ubicación pública**. Estas tres opciones se reducen en dos alternativas: **redes privadas**, a las que pertenecen las ubicaciones **Hogar** y **Trabajo** y **red pública**, a la que pertenece la tercera opción.

La seguridad es un tópico complicado, y Windows Vista intenta establecer un punto intermedio entre la complejidad del tema y la facilidad de uso para nosotros, como usuarios del sistema. Al determinar si estamos en el hogar o en una cafetería, le permitimos al sistema operativo seleccionar el nivel de seguridad que debe asumir de manera predeterminada. Los usuarios avanzados podrán ajustar a su preferencia el nivel de seguridad a través de las opciones del **Panel de control**, pero para la mayoría, que solo necesitamos conectarnos a la red y saber que estamos protegidos, resulta más cómodo cambiar solamente el tipo de ubicación y saber que los ajustes necesarios se harán en forma automática.

El servicio de detección de redes recién mencionado es un ejemplo de esto. En una red pública, se deshabilita al instante. Evita que si estamos en una cafetería u otro sitio y utilizamos una red abierta,

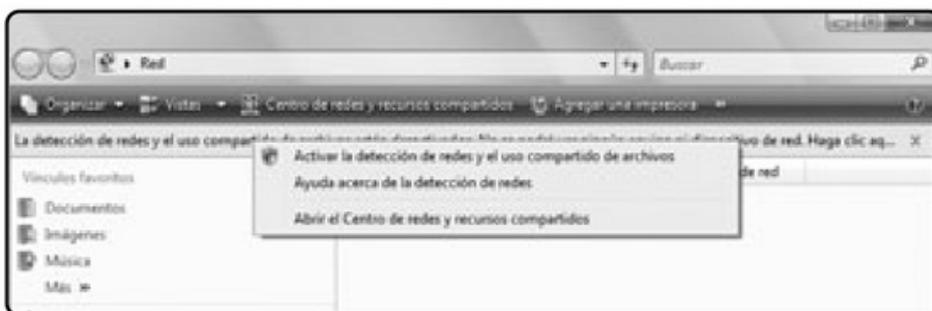


FIGURA 1.
Solo un usuario con permisos administrativos puede activar servicios de red.



ÁREA DE ENCUENTRO DE WINDOWS

El Área de encuentro de Windows (*Windows Meeting Space* en la versión en inglés) es una herramienta colaborativa que introduce Windows Vista. Con ella, podemos compartir con otros usuarios nuestro escritorio o una aplicación específica.

otras personas puedan obtener información sobre nuestro sistema.

Otro servicio muy importante para la red hogareña y que depende de la ubicación de red es el **uso compartido de archivos**. Este servicio se habilita de manera predeterminada en las redes privadas (**Hogar** y **Trabajo**), mientras que se deshabilita en las redes públicas. Está claro que no queremos que la carpeta de nuestros **Documentos** esté visible en esa cafetería donde nos conectamos para revisar el correo. De todas formas, Windows Vista nos permite compartir archivos en una red con **Ubicación pública** si así lo decidimos, a través del **Centro de redes**

y recursos compartidos. Pero eso sería una decisión consciente. De la forma en que ahora funcionan las cosas, se evita que el sistema quede desprotegido por equivocación o sin que el usuario tenga noticia de ello (**Figura 2**). Hay más cambios que realiza Windows Vista al hacer la elección del tipo de ubicación, como ajustes en el **Firewall de Windows**, que conoceremos próximamente.

¿QUÉ ES UN GRUPO DE TRABAJO?

Tanto **Hogar** como **Trabajo** son consideradas por Windows Vista como ubicaciones de red privadas. Sin embargo, hay servicios como la detección de redes, que funcionan bajo una, pero no bajo la otra.

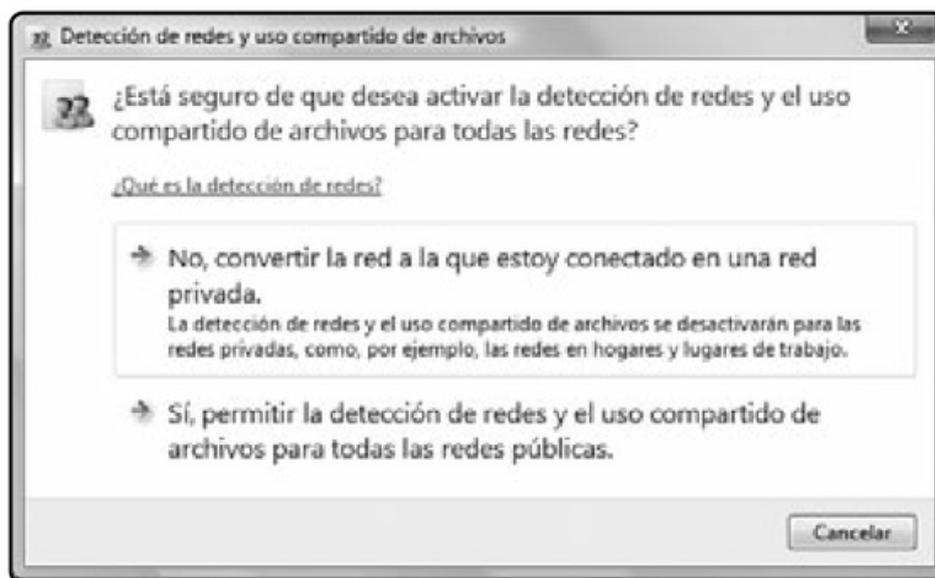


FIGURA 2.
Se recomienda compartir
archivos solo
en redes privadas.



AYUDA SOBRE REDES

¿Dudas sobre cómo utilizar la red? Microsoft ha puesto a nuestra disposición un excelente sitio: <http://windowshelp.microsoft.com/Windows/es-ES/default.msp>, donde podremos encontrar respuesta a casi cualquier inquietud que tengamos.

La razón está dada por la forma en que se maneja la seguridad en las redes Windows.

Uno de los requerimientos de Windows para que los equipos sean visibles entre sí es que pertenezcan al mismo **grupo**. En un inicio, las redes de Windows eran para **Trabajo en Grupo** (*Windows for Workgroups*: ¿alguien recuerda Windows 3.11?). Esto funcionaba sin problemas en una red hogareña, pero en las empresas empezaron a presentarse inconvenientes.

El área administrativa creaba su grupo de trabajo, mientras que el área comercial creaba otro, y así el resto de las áreas. Esto producía un grave conflicto para los administradores de red, ya que no era una tarea fácil administrar cuentas de usuario, compartir recursos entre grupos de trabajo, y garantizar la seguridad de la red sin volvernos locos en el intento.



Para solucionar este problema, Microsoft introdujo los **dominios**. Un dominio se administraba centralizadamente (gracias a un servidor dedicado corriendo Windows NT por aquellos tiempos). Todos los usuarios pertenecían al mismo dominio, al tiempo que se podía mantener una separación por grupos.

A los administradores de redes, les cambió la vida. Ahora podían configurar todos los usuarios y grupos de la red desde un punto central único. Si bien el trabajo en dominios es excelente para el mundo empresarial, para las redes hogareñas, los grupos de trabajo se han mantenido como la elección óptima.

CONFIGURAR UN GRUPO DE TRABAJO

Un grupo de trabajo es muy sencillo de configurar (**Paso a paso 1**). Esto es importante porque vamos a necesitar que todos los equipos de nuestra red

Tanto Hogar como Trabajo son consideradas por Windows Vista como ubicaciones de red privadas



UNIÓN A DOMINIOS Y GRUPOS DE TRABAJO

Las ediciones **Windows Vista Home Basic** y la **Home Premium** solo permiten conexiones a grupos de trabajo. **Vista Enterprise** y **Vista Business** posibilitan unirse a dominios, así como a grupos de trabajo. La edición **Ultimate** incorpora las características de todas las anteriores.

estén en el mismo grupo de trabajo. No es obligatorio, pero simplifica mucho el funcionamiento de la red y es uno de los primeros pasos que debemos hacer a la hora de configurar la red.

El nombre de nuestro grupo de trabajo puede ser cualquier palabra. Sin embargo, Windows nos va a permitir utilizar solo mayúsculas. Es aconsejable no usar espacios ni un nombre que ya le hayamos asignado a un equipo.

Es muy probable que tengamos una computadora con Windows XP dando vueltas por la casa, por lo que, si queremos unirla al nuevo grupo, los pasos son similares a los de Windows Vista. La única diferencia radica en que, para acceder a las propiedades del sistema, en el **Panel de control**, la categoría se llama **Rendimiento y mantenimiento**. Una vez seleccionada, hacemos clic sobre el icono **Sistema**, y aparecerá la ventana **Propiedades del sistema** (**Figura 3**), donde seleccionamos la pestaña **Nombre de equipo** para realizar los cambios necesarios.

COMPARTIR ARCHIVOS CON OTROS USUARIOS

No necesitamos una red para compartir archivos. Basta con tener varios usuarios en nuestra computadora y la necesidad de compartir va a surgir en algún

momento. Windows Vista entiende este problema y nos brinda una solución: la carpeta **Acceso público**. La encontramos en el listado de carpetas del explorador y contiene, a su vez, un grupo de cinco carpetas, similares a las que ya tenemos en nuestro perfil:

- **Descargas públicas**
- **Documentos públicos**
- **Imágenes públicas**
- **Música pública**
- **Videos públicos**



FIGURA 3. El procedimiento de unirse a un grupo de trabajo es similar en Windows XP.



CONEXIÓN WEB A ESCRITORIO REMOTO

La Conexión Web a Escritorio remoto es un software que nos permite conectarnos remotamente a un equipo, iniciar una sesión de **Escritorio remoto**, pero utilizando como cliente el navegador de Windows, Internet Explorer.

PASO A PASO /1

Configurar un grupo de trabajo

1



Vaya al **Panel de control** y seleccione la opción **Sistema y mantenimiento**. Allí, bajo el ítem **Sistema**, verá la tarea **Mostrar el nombre de este equipo**, sobre la cual deberá hacer clic.

2



En la ventana **Sistema**, verá la opción **Cambiar la configuración** para modificar el nombre, dominio y grupo de trabajo del equipo. Haga clic sobre ella.

PASO A PASO /1 (cont.)

3



A continuación, aparecerá la ventana **Propiedades del sistema**. En ella puede teclear una corta descripción del equipo. Más abajo encontrará el botón **Id. de red...** que permite unir el equipo a un dominio. Como no es el caso, haga clic sobre el botón **Cambiar...** que le va a permitir definir el grupo de trabajo al cual va a pertenecer ese equipo.

4



En la ventana **Cambios en el dominio o el nombre del equipo**, puede definir el nombre del equipo y si es miembro de un dominio o un grupo de trabajo. Tilde la casilla **Grupo de trabajo** y teclee el nombre que va a utilizar para él. En este caso, se cambió el dominio que Windows Vista utiliza de manera predeterminada: **WORKGROUP** por **CASA**. Cierre la ventana aceptando los cambios.

PASO A PASO /1 (cont.)

5



A continuación, el sistema le notificará, mediante una ventana, que el grupo de trabajo ha sido cambiado exitosamente y funciona de manera correcta.

6



En el último paso, le aparecerá otra ventana que le señala que, para que la nueva configuración se active, debe reiniciar el equipo, pero antes debe guardar todos los archivos abiertos.

El uso de estas carpetas queda a discreción nuestra. Lo importante es que este grupo de carpetas les van a aparecer a todos los usuarios del equipo. Así, cualquier archivo o carpeta que copiemos o guardemos allí, va estar disponible para todos (**Figura 4**).

COMPARTIR LOS ARCHIVOS DE MI EQUIPO EN LA RED

Para compartir archivos entre usuarios, lo primero que hizo Windows fue crear para nosotros una carpeta pública. Para compartir archivos a través de la red, Windows repite la fórmula, pero en vez de crear de nuevo una carpeta, lo que hace es compartir la carpeta pública ya existente en la red. Por supuesto, Windows Vista también nos permite compartir información almacenada en carpetas personales, como veremos en el siguiente apartado (**Figura 5**).

Cada una de estas dos variantes tiene sus ventajas y desventajas: utilizar las carpetas públicas es muy cómodo ya que, cada vez que necesitemos compartir algo, lo copiaremos allí y listo.

En cambio, si la información está en nuestras carpetas personales, cada vez que necesitemos compartir algo, tendremos que ejecutar el proceso correspondiente.

Sin embargo, existen ocasiones en las que podríamos necesitar compartir directamente una carpeta personal. Por ejemplo, supongamos que tenemos una carpeta donde guardamos nuestras fotos digitales, que está dentro de nuestras carpetas personales, y es muy probable que queramos mantenerlo así ya que es la ubicación donde la aplicación que utilizamos para descargar y organizar nuestras imágenes las almacena por defecto.

Para compartir esas fotos, tenemos dos opciones: la primera sería utilizar la carpeta pública. De esta manera, una vez que descargamos las fotos y las organizamos, las copiamos a la carpeta pública. Esto tiene el inconveniente de que hay que repetir el proceso constantemente y, además, ocupamos el doble de espacio en el disco duro. La otra opción es compartir directamente nuestra carpeta personal.

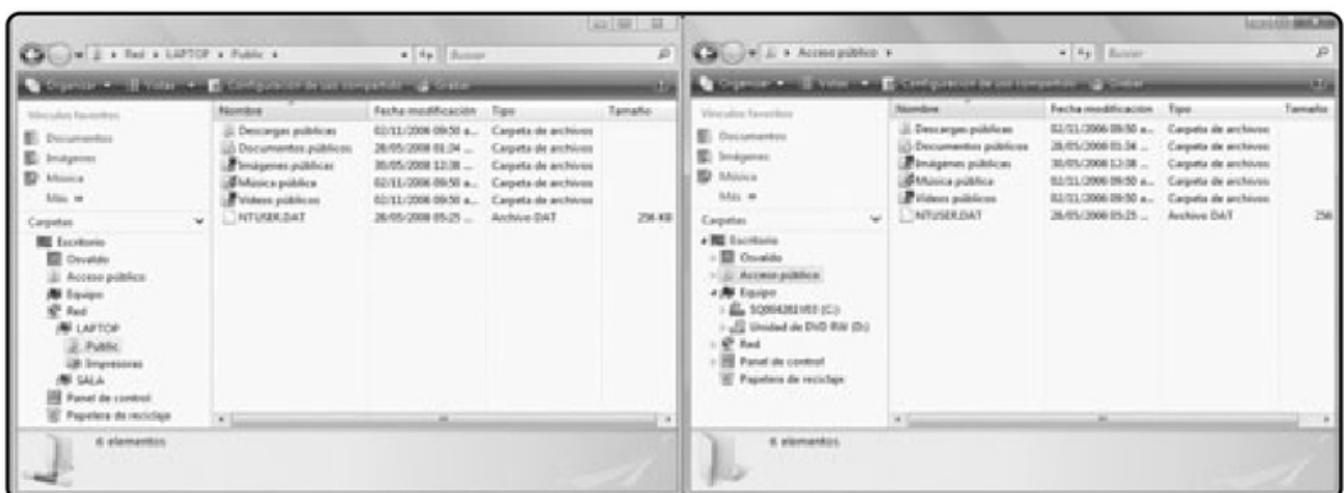


FIGURA 4. El acceso por la red a nuestro propio equipo nos muestra las carpetas públicas de la misma manera que si navegáramos localmente.



Para compartir archivos entre usuarios, lo primero que hizo Windows fue crear para nosotros una carpeta pública

Las carpetas públicas aportan una forma sencilla de compartir, pero esa facilidad tiene desventajas en determinados casos, como en el ejemplo anterior.

Al ser carpetas públicas, todo lo que ahí se copie será accesible por todos los usuarios, pero podríamos tener la necesidad de compartir cierta información en la red solo con algunos usuarios. Esto lo haríamos compartiendo carpetas personales, donde sería posi-

ble tener un control más detallado del acceso a nuestras carpetas y documentos por parte de otros.

En cualquier caso, el primer paso para compartir archivos en la red es habilitar en el **Centro de redes y recursos compartidos** la opción **Uso compartido de archivos**. Para esto, debemos cerciorarnos antes que la red se encuentre en estado **Activado** (Figura 6).



FIGURA 5.
Podemos tener una carpeta de red al alcance de un clic en nuestro Escritorio.



FIGURA 6.
El uso compartido de archivos puede ser activado o desactivado desde el Panel de control.

En resumen, Windows Vista nos brinda dos formas básicas de compartir información en la red. Veamos los pasos por seguir para ponerlas en acción.

COMPARTIR MIS CARPETAS PERSONALES EN LA RED

Ya vimos que las carpetas públicas sirven para compartir entre los usuarios del equipo y tienen una ubicación predeterminada por Windows Vista. Además, el sistema operativo nos brinda la posibilidad de

compartir en la red dichas carpetas. Por ser una funcionalidad propia de Windows Vista, para habilitar o deshabilitar esta opción, tenemos que situarnos en el **Centro de redes y recursos compartidos**. Cualquier cambio realizado, afectará a todos los usuarios.

Nuestras carpetas no tienen accesos compartidos de manera predeterminada. Cuando queramos compartir una carpeta o un archivo que se encuentre en nuestro perfil, deberemos hacerlo manualmente.



UNIVERSAL NAMING CONVENTION

Cuando creamos un acceso directo a un recurso compartido por la red, ya sea un archivo o una impresora, estamos haciendo uso del **UNC**, que son las siglas de *Universal Naming Convention* (**Conversión universal de nombramientos**).



Suele darse el caso que necesitemos compartir un documento en particular con otra persona (**Figura 7**). En las versiones anteriores de Windows, solo se podían compartir carpetas. Si teníamos ese archivo dentro de una carpeta donde había varios archivos que no nos interesaban compartir, teníamos que crear una nueva carpeta, copiar o mover el archivo allí y recién entonces, compartirla. A partir de Windows Vista podemos compartir tanto carpetas como archivos. Esto resuelve esa limitación y nos simplifica el trabajo en red.

Esta nueva versión de Windows introduce otra mejora: cada vez que seleccionemos una carpeta o un archivo en el **Explorador de Windows**, nos aparecerá la opción de **Compartir** en la barra de herramientas, la cual inicia el asistente **Archivos compartidos (Paso a paso 2)**.

Veamos un ejemplo práctico. Estoy escribiendo este libro y, en mis **Documentos**, tenía una carpeta crea-

da con el material de la editorial. Ahí tengo la carpeta del libro y, dentro de ella, una carpeta con las imágenes de cada capítulo. Estoy haciendo capturas de pantalla en otro equipo y quiero copiarlas a la carpeta correspondiente.

No me interesa tener esa carpeta en los documentos públicos. Veamos qué pasos debo realizar para poder copiar las imágenes en su carpeta correspondiente a través de la red.



FIGURA 7. Al seleccionar la opción **Compartir** esta carpeta, podemos teclear el nombre que deseamos asignarle al recurso compartido.



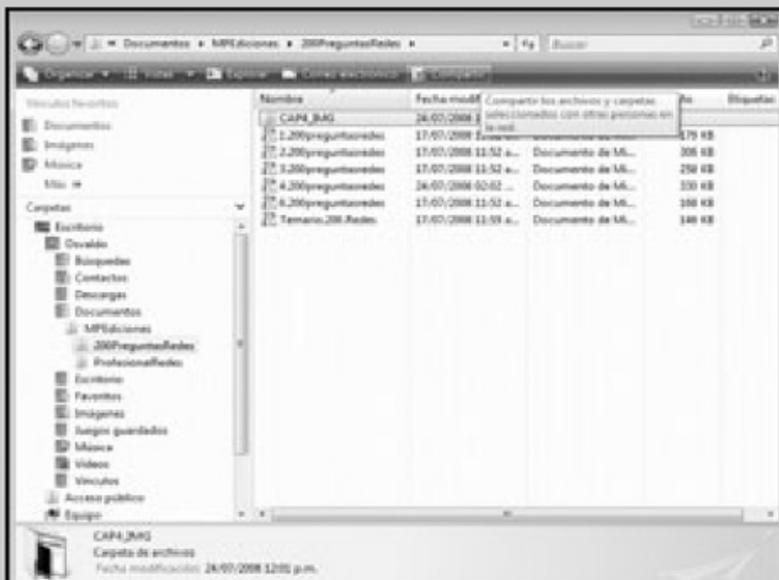
CARPETAS COMPARTIDAS

Para acceder a una carpeta compartida desde una PC con Windows XP, debemos ir al **Explorador de Windows** y hacer clic en **Mis sitios de red**. Desplegamos las ramas **Toda la red/Red de Microsoft Windows/Casa/Pentium/Users/[Nombre de usuario]** hasta llegar a la carpeta.

PASO A PASO /2

Compartir una carpeta con el asistente

1



Ubique, en el explorador, la carpeta que desea compartir. Selecciónela con un clic en el panel de la derecha y luego haga clic en el botón **Compartir** para que se abra el asistente.

2



Se presentará la ventana del asistente **Archivos compartidos**. Ahora deberá agregar otros usuarios. En este ejemplo, se agregó al usuario **Invitado**, lo cual implica que cualquier persona por la red podrá tener acceso a dicha carpeta. El listado de usuarios aparece al hacer clic sobre el menú desplegable. Una vez seleccionado el usuario, haga clic en el botón **Agregar**.

PASO A PASO /2 (cont.)

3



De manera predeterminada, a los nuevos usuarios se les otorga solo permisos de lectura. En este caso, el usuario invitado necesitará escribir en esa carpeta, por lo que deberá hacer clic en el **Nivel de permiso** correspondiente para modificarlo. En el ejemplo, se le otorgan permisos de **Copropietario** al usuario **Invitado**.

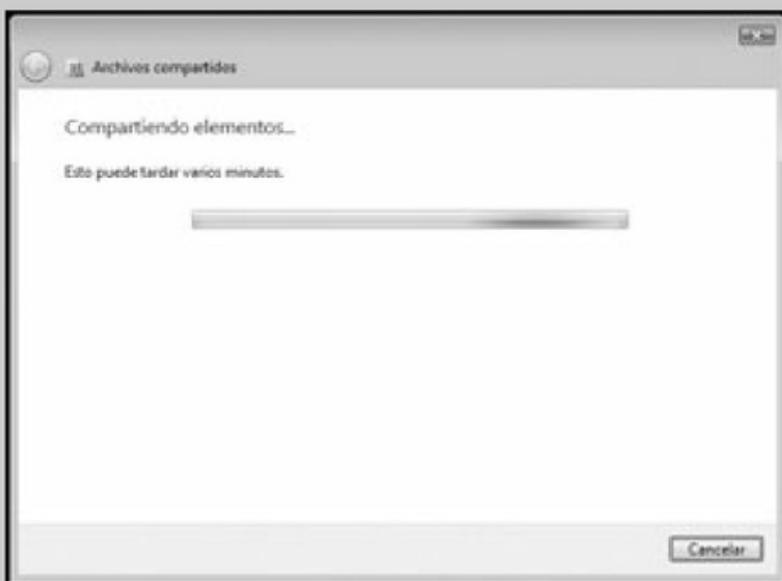
4



Una vez agregados los usuarios y configurados sus niveles de permiso, proceda a compartir con un clic en el botón **Compartir**.

PASO A PASO /2 (cont.)

5



El asistente se encargará de realizar las modificaciones necesarias en el sistema para poder compartir los elementos en la red informática.

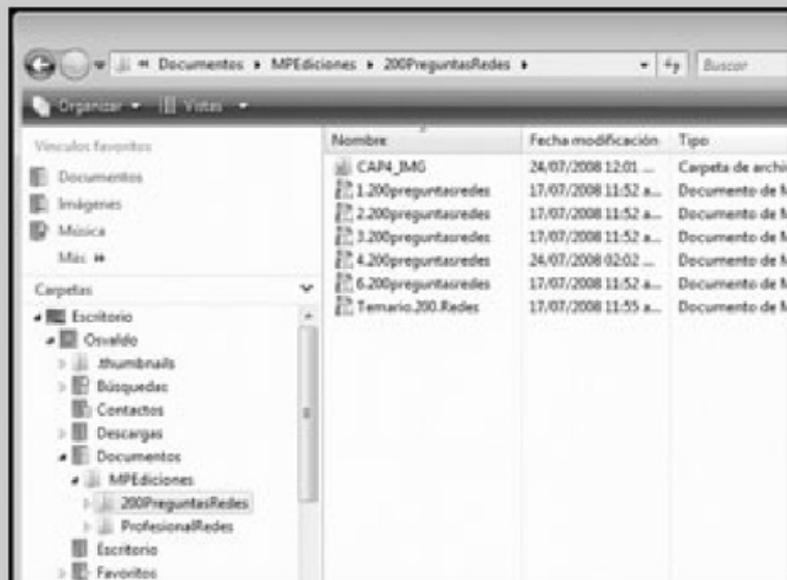
6



De esta manera, la carpeta ha quedado compartida. La ventana le mostrará la ruta completa bajo la cual ha quedado compartida la carpeta en la red.

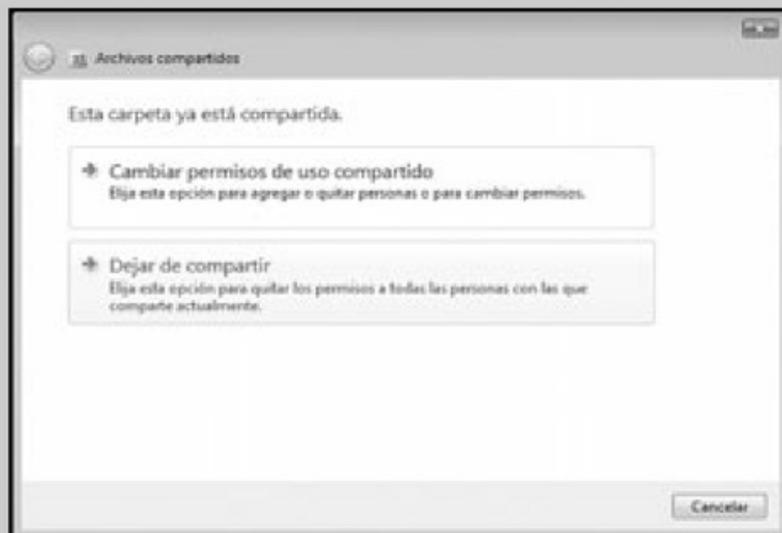
PASO A PASO /2 (cont.)

7



Si regresa al explorador, podrá fijarse ahora cómo Windows Vista identifica la carpeta compartida con un icono.

8



Si luego desea dejar de compartir la carpeta, deberá seleccionarla en el explorador y hacer clic en **Compartir**. Volverá a ver el asistente **Archivos compartidos** donde deberá hacer clic en la opción **Dejar de compartir**.

Cuando compartimos un archivo, los pasos son similares. La diferencia es que el asistente de **Uso compartido de archivos** utiliza tres tipos de permisos: **Lector**, **Colaborador** y **Propietario**. La diferencia entre cada uno es sencilla. Los usuarios con permiso de **Lector** tendrán accesos de solo lectura al recurso; el permiso de **Colaborador** posibilitará modificar archivos, pero no crearlos ni eliminarlos; el **Copropietario** podrá crear, modificar y eliminar archivos.

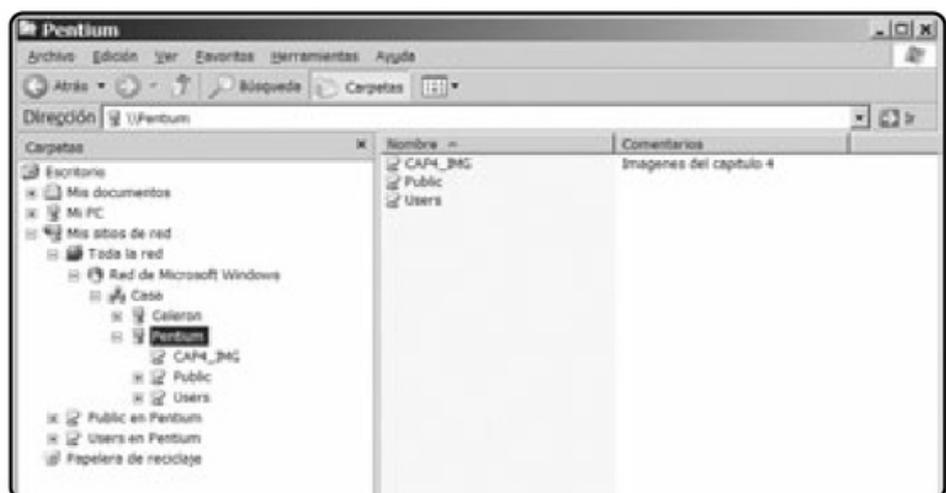
Cuando accedimos a la carpeta compartida por la red, encontramos un detalle curioso: quedó expuesta la estructura de carpetas que la contenían. Esto se debe a la manera en la que trabaja el asistente de **Archivos compartidos**. En ocasiones, podríamos necesitar tener una carpeta compartida bajo el viejo

sistema de Windows, es decir, que cuando buscáramos el equipo en la red, apareciera solo la carpeta. En esos casos, necesitamos recurrir al **Uso compartido avanzado** (Figura 8 y Paso a paso 3).

RESTRINGIR EL ACCESO AL COMPARTIR UNA CARPETA

En el procedimiento **Paso a paso 3: Compartir una carpeta mediante uso compartido avanzado**, hicimos una trampa. Windows Vista nos brinda los asistentes como una forma de simplificar tareas complicadas para el usuario, y utilizar el asistente **Archivos compartidos** no es la excepción. A través de los pasos del asistente, Windows Vista realiza un grupo de acciones en segundos sin que tengamos que preocuparnos por ellas.

FIGURA 8.
Podemos acceder a los recursos compartidos en nuestro equipo desde una PC con Windows XP.



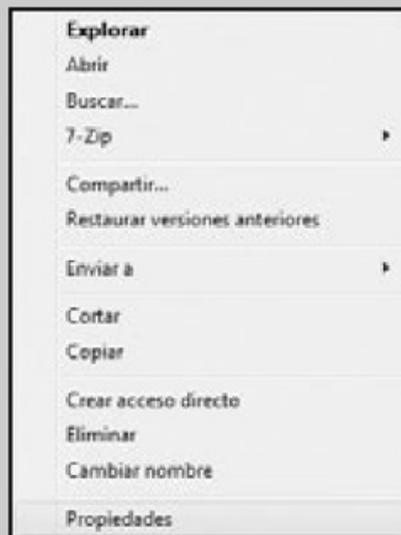
► TERMINAL SERVER

El nombre de **Terminal Server** para la aplicación **Escritorio remoto** proviene del mundo Unix. Un equipo Unix permitía que varios usuarios se conectaran al mismo tiempo al sistema. Para permitir la conexión de los usuarios se utilizaban **terminales**.

PASO A PASO /3

Compartir una carpeta mediante uso compartido avanzado

1



Ha decidido compartir la misma carpeta nuevamente. Selecciónela en el explorador y haga clic secundario sobre ella. En el menú contextual que se presenta, realice un clic en **Propiedades**.

2



En la ventana de **Propiedades** de la carpeta, seleccione la pestaña **Compartir**. El botón **Compartir** ejecuta el asistente **Archivos compartidos** que se utilizó en el procedimiento anterior, de modo que deberá hacer clic sobre el botón **Uso compartido avanzado**.

PASO A PASO /3 (cont.)

3



En la ventana **Uso compartido avanzado** tilde la casilla **Compartir esta carpeta**. Si lo desea, puede modificar el nombre con que la va a compartir. De manera predeterminada, Windows Vista comparte con permisos de solo lectura. Con un clic en el botón **Permisos**, podrá modificar esta característica.

4



Luego de presionar **Permisos**, le aparecerá el grupo de usuarios **Todos**, sólo con permiso de lectura. Ese grupo de usuarios agrupa a las cuentas de usuario creadas en el equipo. Como pretende acceder por la red sin restricciones, debe agregar un usuario con el botón **Agregar**.

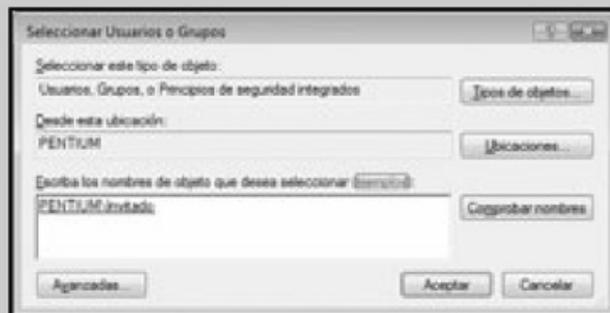
5



En **Seleccionar Usuarios o Grupos**, Windows Vista tiene un usuario predeterminado que le permite acceder a un recurso en el equipo sin crear una cuenta de usuario. Teclee **invitado** y haga clic en el botón **Comprobar nombres**.

PASO A PASO /3 (cont.)

6



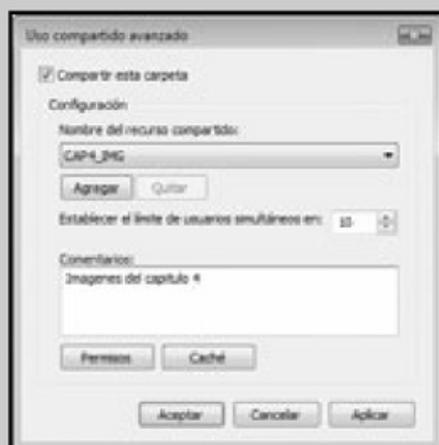
Le aparecerá el nombre correcto de la cuenta. En este caso, **Pentium\ Invitado**. Presione **Aceptar**.

7



Asígnele permisos de **Control Total** al usuario **Invitado** y haga clic en **Aceptar** y luego en **Aplicar**.

8



Por último, puede agregar un comentario que describa el contenido de la carpeta compartida. Para finalizar oprima **Aceptar**.



Windows maneja dos tipos de permisos por separado: los permisos en el sistema de archivos y los permisos del recurso compartido

Al utilizar un método avanzado, tenemos más flexibilidad, pero el costo será que tendremos que realizar por nuestra cuenta la totalidad de los pasos (**Figura 9**).

Cuando utilizamos el **Uso compartido avanzado**, hubo un paso donde le asignamos permisos al usuario **Invitado** para que pudiera leer y escribir en la carpeta compartida. Entonces, ¿cómo puede ser que después nos diera un error el acceso si le habíamos dado permisos al usuario? Es el momento de recordar los perfiles de usuario y cómo el sistema de archivo manejaba permisos individuales para cada uno. Debemos saber que Windows maneja dos tipos de permisos por separado: los permisos en el sistema de archivos

y los permisos del recurso compartido. Cuando utilizamos el asistente, Windows se encarga de ajustar todos los permisos necesarios, pero cuando utilizamos el **Uso compartido avanzado**, nos corresponde a nosotros asegurarnos de que, a nivel del sistema de archivo, también existan los permisos correctos para el usuario **Invitado** (**Paso a paso 4**).

COMPARTIR UNA UNIDAD COMPLETA

Windows Vista nos facilita mucho compartir una carpeta, pero si intentamos compartir el disco entero, no vamos a tener un asistente a mano.

FIGURA 9.
Al intentar acceder a una carpeta por la red, debemos tener permisos en el recurso compartido y en el sistema de archivos, de lo contrario, obtendremos un mensaje de error.



PASO A PASO /4 Modificar los permisos en el sistema de archivos

1



En la ventana de **Propiedades** de la carpeta, seleccione la pestaña **Seguridad**, donde verá los usuarios o grupos que tienen permisos sobre la carpeta y los tipos de permisos que tiene asignado cada usuario o grupo. Haga clic en el botón **Editar**.

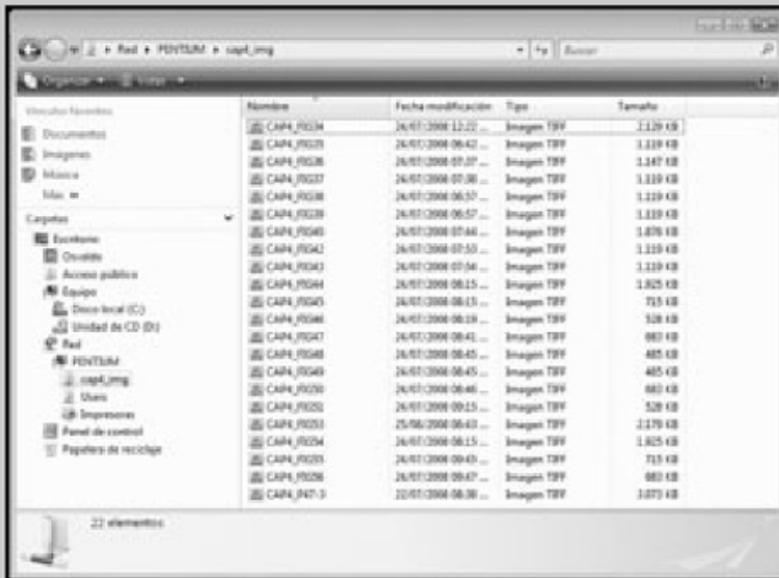
2



En la nueva ventana, presione **Agregar** para adicionar al usuario **Invitado**, como lo hizo en el procedimiento anterior. Asígnele permisos de **Control Total** a este usuario.

PASO A PASO /4 (cont.)

3



Seleccione **Aceptar** en las ventanas abiertas, para hacer efectivos los cambios. Ahora podrá conectarse desde otros equipos sin que le aparezca el mensaje de error. Cuando desee dejar de compartir esta carpeta, será conveniente quitar los permisos que asignó en el paso anterior.

La razón es sencilla, no es aconsejable hacer esto y, por lo tanto, el sistema no lo permite. De todas maneras, podemos ejecutar el procedimiento de forma manual (**Figura 10**). Si hacemos clic secundario sobre la unidad, vemos que el botón **Compartir** que abriría el asistente está deshabilitado. Por eso, una vez más, debemos utilizar el **Uso compartido avanzado**. Nos aparecerá la ventana ya conocida, por lo que solo resta mencionar que las unidades raíz no se pueden compartir de forma oculta, es decir, adicionar el signo \$ al final de la letra de la unidad. Esto se debe a que el sistema operativo utiliza de

manera predeterminada ese nombre. Si queremos compartir la unidad de manera oculta, lo podemos hacer de todos modos, pero con otro nombre, por ejemplo **DiscoC\$**.



Windows considera las impresoras instaladas en la PC como un recurso más que puede ser compartido

COMPARTIR MI IMPRESORA CON OTROS USUARIOS

Windows considera las impresoras instaladas en la PC como un recurso más que puede ser compartido de manera similar a como lo hacemos con una carpeta. Es obvio que, para compartir una impresora, en primer lugar, debemos tenerla instalada. En el **Centro de redes y recursos compartidos** se encuentra la opción de **Activar** o **Desactivar** el **Uso compartido de impresoras** (Figura 11). Este servicio depende, a su vez, del servicio de

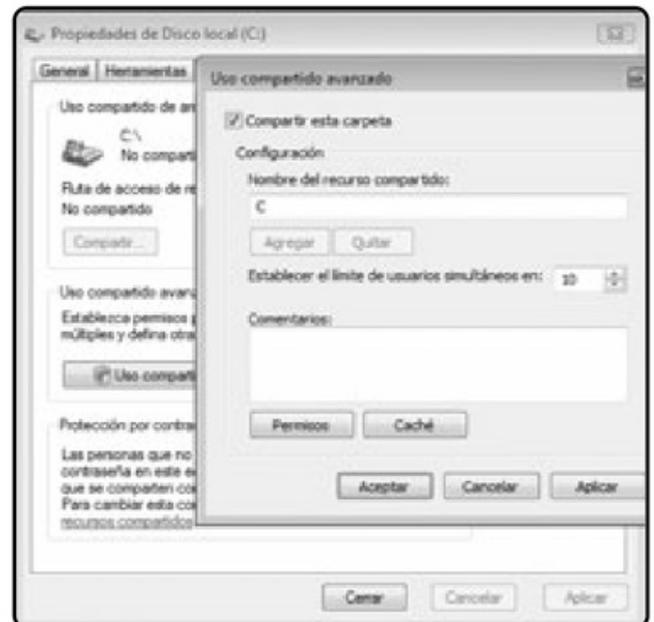


FIGURA 10. Para compartir una unidad raíz, debemos acceder a sus propiedades.

Uso compartido de archivos, el cual deberá estar activado también (Figura 12). Asimismo, tenemos que revisar que la ubicación de red que estamos utilizando sea **Hogar**.



FIGURA 11. Una vez instalada la impresora, la podemos compartir a través del Centro de redes y recursos compartidos.



FIGURA 12.
Una vez establecida la configuración, ya podemos acceder a la impresora por la red.

ACCEDER A UNA IMPRESORA CONECTADA A OTRA PC

Cuando navegamos por la red, vamos a descubrir las impresoras compartidas en otros equipos. Para acceder al contenido de una carpeta compartida en la red, hacemos doble clic sobre ella. Si el doble clic lo hacemos a una impresora compartida, Windows

Vista se conectará y comenzará el proceso de instalación automáticamente (**Figura 13**).

Siempre que instalamos un nuevo dispositivo, vamos a necesitar su controlador. Cuando compramos una impresora, debemos asegurarnos de que en la caja esté incluido un CD con el controlador para

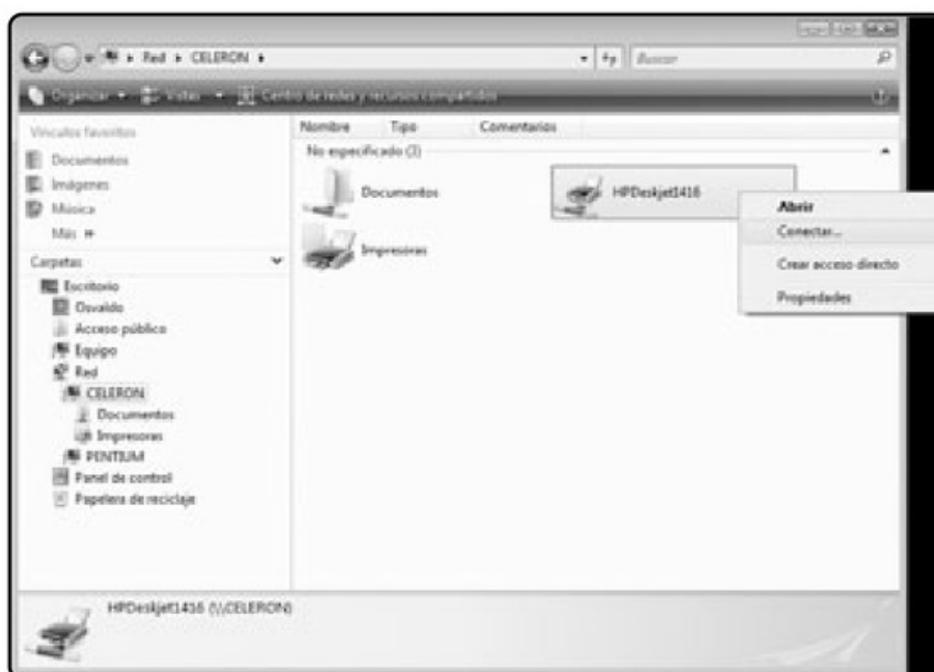


FIGURA 13.
Para instalar una impresora, también podemos hacer clic derecho sobre ella y seleccionar la opción Conectar en el menú contextual que aparece.

Windows Vista, que tendremos que utilizar cuando instalemos la impresora en nuestra PC (**Figura 14**).

Las primeras versiones de Windows requerían que, cuando se instalaba una impresora de red, hubiera que utilizar el CD de instalación para tomar de ahí sus controladores. A partir de Windows XP, cuando instalamos una impresora local, Windows almacena una copia de los controladores. Por esta razón,

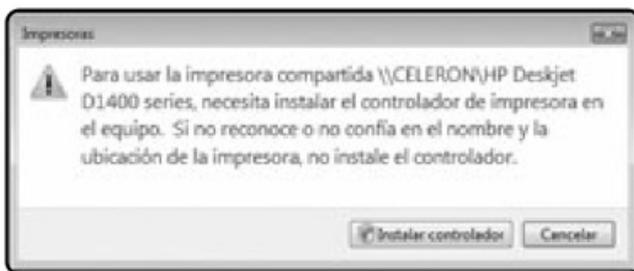


FIGURA 14. Siempre que instalemos un nuevo controlador, Windows Vista nos pedirá que autoricemos la acción.

cuando conectemos una impresora que esté compartida en un equipo con Windows XP o Windows Vista, el controlador se instalará automáticamente.

Si todavía poseemos algún equipo con Windows 98 en casa, debemos tener a mano el CD de instalación de la impresora (**Figura 15**).

CONTROLAR EL USO DE MI IMPRESORA COMPARTIDA

En ocasiones, necesitamos restringir el acceso a un archivo o una carpeta por cuestiones de privacidad. Con las impresoras sucede lo mismo, pero por razones menos filosóficas: una impresora compartida sin restricción alguna es una invitación a gastar papel y cartuchos de tinta para las generaciones más jóvenes de la casa. El mismo principio de restricción de accesos que se aplicaba para el caso de las carpetas y archivos rige para las impresoras.



FIGURA 15. En el Panel de control conviven las impresoras locales y las de red.



El mismo principio de restricción de accesos que se aplicaba para el caso de las carpetas y archivos rige para las impresoras

A través del **Centro de redes y recursos compartidos**, podemos activar esta opción. A partir de que activemos esta opción (**Figura 16**), solo se podrán acceder a los recursos compartidos por la red con el nombre de usuario y la contraseña de una cuenta de usuario que haya sido creada localmente en el equipo. Si el usuario al que intentamos restringir el acceso ya tiene una cuenta local creada en ese equipo, necesitamos un procedimiento más avanzado, a través de las propiedades de la impresora.

En el **Panel de control**, en la sección **Impresoras**, hacemos clic derecho sobre la impresora instalada y, en el menú contextual que aparece, seleccionamos **Propiedades**.

En la ventana, encontraremos la pestaña llamada **Seguridad** (**Figura 17**), que funciona como si fuera una carpeta o un archivo, solo que en el caso de las impresoras los permisos son otros (como podemos ver en la **Tabla 1**).

FIGURA 16.
Windows Vista
deshabilita de manera
predeterminada
el uso compartido
con protección
por contraseña.





FIGURA 17.
De manera predeterminada, todas las cuentas pueden utilizar la impresora. Basta con desmarcarle este permiso al grupo Todos y asegurarnos de que los usuarios con permisos lo tengan marcado.

PERMISO	DESCRIPCIÓN
Imprimir	Permite utilizar la impresora para imprimir archivos.
Administrar impresoras	Permite instalar, pausar y desinstalar impresoras en el equipo.
Administración de documentos	Permite pausar la impresión de documentos así como eliminarlos de la cola de impresión.
Permisos especiales	Son permisos de uso infrecuente, como por ejemplo, llevar un registro de auditoría sobre eventos de impresión.

TABLA 1. Descripción de los diferentes permisos de impresión.



RESUMEN

En este capítulo, dedicado al uso de la red, conocimos los tipos de ubicaciones, aprendimos qué es un grupo de trabajo y analizamos cómo compartir mis archivos con otros usuarios. Además, vimos de qué manera controlar el uso de la impresora compartida.

Multiple choice

- **1** Con un grupo de trabajo, en la PC, podemos realizar la siguiente acción:
- a- Jugar al fútbol cada jueves de la semana.
 - b- Compartir una oficina.
 - c- Llevar adelante proyectos.
 - d- Compartir recursos: archivos e impresoras.
-

- **2** Una cuenta de usuario estándar es la indicada para:
- a- El trabajo cotidiano.
 - b- Los usuarios avanzados.
 - c- Los usuarios principiantes.
 - d- Los técnicos especializados.
-

- **3** Una cuenta de administrador debe ser usada:
- a- Todo el tiempo.
 - b- Solo en ocasiones especiales.
 - c- Cuando sea necesario.
 - d- Por los administradores de la red de una empresa.
-

- **4** ¿Qué debo tener instalado en el equipo para poder utilizar una impresora compartida?
- a- Un programa específico.
 - b- Una aplicación que comparta la impresora.
 - c- Windows.
 - d- El controlador correcto de la impresora.
-

- **5** Las carpetas públicas se muestran:
- a- A los usuarios registrados.
 - b- A los usuarios conectados a nuestra LAN.
 - c- A los usuarios del grupo de trabajo.
 - d- A cualquiera.
-

- **6** ¿Qué permiso nos permite pausar la impresión de documentos y eliminarlos de documentos de la cola de impresión?
- a- Imprimir.
 - b- Administrar impresoras.
 - c- Administración de documentos.
 - d- Permisos especiales.
-

Respuestas: 1-d, 2-c, 3-d, 4-d, 5-b, 6-c.

Capítulo 5

Redes WiFi



Aprenderemos a habilitar el filtraje por dirección MAC, configurar una red ad hoc y mucho más.

Redes WiFi

Es un buen momento para aclarar cómo se transmite la información por el aire. En las redes cableadas es sencillo, viaja a través de señales eléctricas que se transmiten a lo largo del cable. En las redes inalámbricas, la información se transmite a través de señales de **radiofrecuencia**, que son producidas a partir de señales eléctricas y se transmiten por el aire en la forma de **ondas de radio**. De esta manera, un receptor es un dispositivo capaz de detectar estas ondas de radiofrecuencia y convertirlas en señales eléctricas.

Para escuchar la radio, sintonizamos una emisora y, al hacerlo, estamos seleccionando una señal de radiofrecuencia determinada, por la cual esa emisora está transmitiendo. Queda claro entonces que cada emisora transmite por una frecuencia específica. Los radios no son los únicos dispositivos que utilizan estas señales, también las emplean la televisión para transmitir su programación por aire, los celulares, los *walkies-talkies*, etcétera.

De la misma manera en que cada emisora tiene asignada una frecuencia, cada grupo de dispositivos tendrá un grupo de frecuencias asignado. La televisión tiene el suyo, la radio tiene dos, uno para transmitir en

En las redes inalámbricas, la información se transmite a través de señales de radiofrecuencia

AM (Amplitud Modulada) y otro en FM (Frecuencia Modulada) y los celulares también tienen su espacio en el espectro de radiofrecuencias. Estos grupos de frecuencias se llaman **bandas**.

Algunas de ellas son comerciales (hay que pagar por su uso, como es el caso de las bandas que utiliza la radio para transmitir por AM o FM), mientras que otras son libres (como la banda que utilizan los radioaficionados para comunicarse).

Los equipos WiFi (**Figura 1**) utilizan dos bandas que son libres. Esto tiene la ventaja de que no se necesita ningún permiso para usar uno de estos equipos. Pero al mismo tiempo, tiene la desventaja de que otros equipos también se sirven de esta banda, entre ellos, los teléfonos inalámbricos que tenemos en casa y los hornos de microondas.

SIGNIFICADO DE LA PALABRA WIFI

WiFi no tiene relación con *Wireless Fidelity* (Fidelidad Inalámbrica). *Wireless Fidelity* es un juego de palabras con el concepto de *High Fidelity* (Alta Fidelidad), denominación empleada para referirse a equipos de música de alta calidad de reproducción.



FIGURA 1.

Una tarjeta PCI es todo lo que necesitamos para conectar nuestra PC a una red WiFi.

Los parámetros que definen de manera práctica a una norma son la **frecuencia** a la que transmite, el **ancho de banda** que permite y su **alcance**. El ancho de banda se publica con los valores óptimos, pero en realidad, la velocidad que utilizamos es menor. El alcance tiene dos valores, uno para interiores y otro para exteriores. El de interior es menor ya que se cuenta la interferencia que causan las paredes, los pisos y techos.

El estándar 802.11 utiliza las bandas de **2.4 GHz** y **5 GHz** del espectro libre de radiofrecuencias. A su vez, este estándar está compuesto por variaciones. Cada una se identifica con la adición de una letra en minúscula al final del estándar. Así, tenemos el **802.11a**, el **802.11b**, y así sucesivamente hasta el **802.11z**. Cada variación define un **área de operación** del protocolo. Nos interesan en especial las que definen la transmisión por el aire, ya que son las que influyen directamente sobre la **velocidad de transmisión** que se obtiene y el alcance que permiten (**Figura 2**).

Existen modelos de routers WiFi a los que les podemos conectar un disco duro externo USB y compartirlo en la red inalámbrica.

FIGURA 2.



Como dijimos, la primera versión que existió fue la 802.11, pero duró muy poco porque fue superada por las modificaciones al protocolo que permitían más velocidad (**Tabla 1**).

La versión 802.11a permitía mayor velocidad que la versión original y operaba en la banda de 5 GHz, lo que evitaba los problemas de interferencia con la banda 2.4 GHz donde operaban otros dispositivos caseros. Pero tenía un problema: no era compatible con la 802.11, por lo que los equipos soportaban uno u otro protocolo. Casi al mismo tiempo surgió la norma 802.11b, que transmitía a menor velocidad que la 802.11a en la frecuencia conflictiva, pero sí era compatible y de menor costo. A la larga, terminó imponiéndose. La desaparición de la 802.11a se completó cuando surgió la 802.11g que transmitía a



su misma velocidad, al tiempo que mantenía la compatibilidad. La compatibilidad entre normas es importante. Así como las tarjetas de red Ethernet son capaces de funcionar con cualquier switch independientemente de la velocidad que tenga, los equipos inalámbricos se benefician de la misma manera. Debemos tener la precaución de utilizar siempre equipos que utilicen igual norma o sean compatibles con los que ya tenemos (**Figura 3**).

PROTOCOLO	FRECUENCIA	ANCHO DE BANDA	ALCANCE M (INTERIORES)	ALCANCE M (EXTERIORES)
802.11	2.4 GHz	2 Mbit/s	20	100
802.11a	5 GHz	54 Mbit/s	35	120
802.11b	2.4 GHz	11 Mbit/s	38	140
802.11g	2.4 GHz	54 Mbit/s	38	140
802.11n	2.4 Ghz, 5 GHz	248 Mbit/s	70	250

TABLA 1. Comparación entre los estándares WiFi.

▶ WLAN

A los conceptos de LAN y WAN, con las redes inalámbricas se les suma el que nombra un nuevo tipo de red, las **WLAN** (*Wireless LAN* o **Redes LAN inalámbricas**): similares a las redes LAN, solo que en lugar de un switch Ethernet, se comunican a través de un router WiFi.

ESTABLECER UNA CONEXIÓN INALÁMBRICA

Las redes WiFi utilizan menos componentes que una red cableada. Ambas suelen trabajar con un punto central, aunque es posible establecer conexiones punto a punto entre equipos.

En la red cableada, todos los equipos comparten la misma subred (si hablamos en lenguaje TCP/IP). Cuando armemos una red inalámbrica, los equipos también compartirán una misma subred, solo que, si ya teníamos una cableada, vamos a tener dos subredes. Para



FIGURA 3. El icono de red nos indica la conexión a Internet (WiFi o cableada). A través del mensaje de notificación, podemos conocer si estamos empleando la red inalámbrica.

Las redes WiFi utilizan menos componentes que una red cableada

enlazar subredes se utilizan los routers. Como por lo general vamos a terminar por utilizar la red inalámbrica para conectarnos a una cableada, el equipo que debemos comprar será un **router inalámbrico**.

El otro componente de nuestra red deberá ser la **tarjeta de red inalámbrica** que utilice nuestra PC. Las notebooks, en la actualidad, suelen traerlas incorporadas. Si no es la situación, o si queremos conectar una PC, tenemos un grupo de alternativas a mano. Para el caso de las notebooks, existen tarjetas de red inalámbricas en formato **PC-Card**, o las más modernas **miniPCI** o **PCI-Express**. Para las PCs existen tarjetas en formato **PCI** y, para ambos equipos, se encuentran disponibles las tarjetas **USB**.

Si ya tenemos en casa algún equipo con conectividad inalámbrica, debemos fijarnos en qué **norma** trabaja. Esta precaución es válida porque, a la hora de comprar el router, debemos asegurarnos de que pueda trabajar con esa norma. Para garantizar la compatibilidad con equipos más viejos, los routers incorporan un modo doble de trabajo.



ESTÁNDAR 802.11

El estándar 802.11 lo desarrolla la **IEEE** (*Institute of Electrical and Electronics Engineers*, en español, el **Instituto de Ingenieros Eléctricos y Electrónicos**). Entre las tareas a las que se dedica esta organización está la elaboración de protocolos y estándares.

Por lo general, los modelos actuales pueden operar en 802.11g y 802.11b. Si todo nuestro equipamiento es moderno y trabaja en modo 802.11g, será conveniente configurar el router para que utilice sólo ese modo y así obtener el máximo rendimiento de la red. Si tenemos algún equipo que trabaja con la norma 802.11b, entonces debemos habilitar en el router el **modo dual** para que sea capaz de trabajar en ambas normas. Esto reduce un poco el rendimiento, pero le garantiza la conectividad a todos los equipos de la casa.

Si 11 Mbps parecen poco, debemos recordar que si utilizamos la red para navegar por Internet es muy común una conexión de 1Mbps, con lo que el ancho de banda de la red WiFi alcanza y sobra para nuestras necesidades.

Otro componente que se puede llegar a necesitar en determinados casos sería **antenas**, pero esto lo veremos más adelante ya que es una situación especial (**Figura 4**).

Existen muchos modelos de routers en el mercado

CONFIGURAR EL ROUTER INALÁMBRICO

Existen muchos modelos de routers en el mercado, pero todos comparten semejanzas que vamos a ver a continuación. Lo primero que debemos tener en cuenta es que antes de utilizar la red inalámbrica del router, tenemos que configurarla. Esto lo hacemos mediante la red cableada del router y, para eso, necesitamos tener a mano un cable de red, para conectar nuestra PC al router cuando el procedimiento de instalación así lo indique (**Figura 5**).

Existen dos formas básicas para configurar un router: la primera es con el CD de instalación y la segunda es con la guía de instalación impresa que provee el fabricante. Al menos, uno de estos elementos debería estar dentro de la caja del router, sino los dos. En el momento de la compra hay que consultar al vendedor si esto es así, el fabricante siempre incluye alguna forma de guiar al usuario durante la instalación y la configuración del router. La decisión del método por utilizar queda a elección del usuario.



FIGURA 4.

Si además queremos conectar una impresora a la red inalámbrica, necesitamos un print server WiFi.



Para uno más avanzado, la guía impresa le permitirá acceder directamente al router y lograr un mayor control sobre las opciones de configuración. Un usuario con menos experiencia podría preferir introducir el CD en la PC y comenzar a realizar los pasos que ahí se le indiquen. En cualquier caso, las opciones son similares y se refieren a parámetros comunes de la operación de una red inalámbrica. Antes de comenzar la configuración del router, debemos tener definidos estos valores. A lo largo de este capítulo, explicaremos en detalle cada uno de ellos y las distintas alternativas de configuración que existen.

Cuando decidimos configurar el router sin el CD de instalación, el primer paso es encender el router y conectarlo por medio de un cable de red a nuestra PC.

La configuración del router se realiza a través de un **servidor web** que se ejecuta en el router. No hace falta hacer ninguna configuración adicional en la PC

dado que el router está configurado para asignar **direcciones IP dinámicas** a los equipos que se conecten a él. De manera predeterminada, los routers reservan para ellos la dirección IP **192.168.1.1**, que es la dirección que debemos colocar en nuestro navegador para acceder a la página de configuración del router (**Figura 6**).

Antes de llegar a la página de configuración, se presentará una ventana que nos pedirá **autenticarnos**. Esto es una medida de seguridad del router, por lo que en la guía de instalación se especifican los datos que debemos utilizar. Por ejemplo, para los routers **Linksys**, el nombre de usuario se deja en blanco y como contraseña debemos colocar **admin**.



FIGURA 5. Los equipos que contengan este logo están certificados para operar en redes WiFi.



PANEL DE CONTROL DEL ROUTER

Los routers inalámbricos suelen tener dos botones en cada página de configuración de su panel de control. Uno salva los cambios realizados de manera permanente (**Save**) y el otro los activa en ese momento (**Apply Settings**). Así, podemos probar distintas variantes.

En la **TABLA 2**, resumimos los datos generales que vamos a necesitar para configurar exitosamente el router: dirección IP del router, datos de autenticación, tipo de acceso a internet y modo de red inalámbrica. A los ya explicados, se les agregan otros que se analizan en detalle más adelante.

EVITAR QUE ALGUIEN UTILICE EL ROUTER SIN AUTORIZACIÓN

En la actualidad, todos hemos sido testigos de cómo se ha diversificado la televisión. Existen canales públicos y pagos. Los primeros son los que se transmiten por el aire, mientras que los segundos se

DATO	DESCRIPCIÓN
Dirección IP del router	Tenemos que consultar la documentación del router donde se aclara este dato. De manera predeterminada, muchos utilizan la dirección IP 192.168.1.1.
Datos de autenticación	La mayoría de los routers requieren el uso de un nombre de usuario y una contraseña para poder conectarse a la página web de configuración. Podemos encontrar este dato en la documentación del router.
Internet Configuration Type (Tipo de acceso a Internet)	Para los routers que van a tener conexión directa al enlace con Internet, debemos conocer cómo está configurada.
Wireless Network Mode (Modo de red inalámbrica)	Determina la compatibilidad que va a soportar el router entre los distintos estándares 802.11 que admite. La regla es sencilla, primero debemos fijarnos en la versión que soporta cada equipo que tenemos. Si todos nuestros equipos trabajan en el mismo estándar, debemos seleccionar el que corresponda (B-Only para 802.11b o G-Only para 802.11g). Si tenemos equipos en ambos modos o queremos la mayor compatibilidad posible, seleccionaremos el modo Mixed . El modo Disable es cuando queremos deshabilitar la red inalámbrica (debemos tener en cuenta que las opciones del ejemplo pertenecen a un router Linksys y pueden variar en otros modelos, pero el significado siempre es similar).
Wireless Network Name (Nombre de red inalámbrica)	Es el nombre que va a identificar a nuestra red.

TABLA 2. Datos generales para la configuración del router.



FIGURA 6.
Si todos nuestros equipos soportan el protocolo 802.11g, configurar la red en modo Mixed (Mixto) la haría más lenta innecesariamente.

transmiten con cable o antenas satelitales. No es casualidad que sea de esta manera, una vez que la señal sale al aire, cualquiera la puede recibir.

Las redes WiFi también utilizan señales que viajan por el aire, entonces aquí aparece un detalle interesante: cuando encendemos nuestro router, ¿cualquiera puede conectarse a nuestra red? La respuesta es sencilla: sí. De hecho, así funcionan los llamados **Hotspots** (puntos calientes), que son lugares públicos donde

existen routers WiFi a los cuales nos podemos conectar. Son comunes en los hoteles, aeropuertos, cafeterías, e incluso en algunas plazas públicas.

El acceso a estas redes es gratis en algunos casos, cualquiera que se encuentre dentro del rango de la red puede conectarse, mientras que en otros es solo para clientes del lugar. Para lograr controlar los accesos a nuestra red WiFi, los proveedores del servicio utilizan aplicaciones especializadas (**Figura 7**).



FIGURA 7.
La configuración del SSID, que indica el nombre de nuestra red, se encuentra siempre entre los parámetros básicos del router.



Cuando encendemos nuestro router, ¿cualquiera puede conectarse a nuestra red?

Los routers hogareños son muy sencillos, pero también cuentan con mecanismos que nos permiten controlar el acceso a nuestra red WiFi. De manera predeterminada, el router va a tener **acceso libre**. Si es la primera vez que vamos a conectarnos a una red WiFi, resulta conveniente dejarlo así para probar si podemos conectarnos. Establecer el enlace a una red WiFi es mucho más complicado que con una red Ethernet. Por eso, es aconsejable probar primero conectarnos al router con la conexión más sencilla posible, en este caso, sin mecanismos de seguridad. Cuando ya hemos establecido una conexión al router, hemos sido capaces de navegar por la red, e incluso por Internet si tuviéramos un enlace activo, recién entonces podemos conectarnos de nuevo al router y **restringir el acceso**.

Es posible hacer esto de dos maneras: la primera es habilitar su seguridad, y la segunda, restringir el acceso por la **dirección física** de la tarjeta, también conocida como **dirección MAC (Mac Address)**.

La primera variante la veremos en los próximos apartados, por lo que vamos a concentrarnos ahora en explicar la segunda. Toda tarjeta de red tiene un número que la identifica, asignado por el fabricante cuando la produce, por lo que no existen dos tarjetas en el mundo que compartan el mismo número. Este detalle es el que nos permite identificar de manera única los equipos que queremos que se conecten a nuestra red y permitirles el acceso, mientras que se le niega al resto.

El **filtraje** basado en la dirección MAC es una opción genérica que se encuentra en casi todos los modelos de router, y podemos consultar el manual del fabricante para ver su configuración. Debemos tener en cuenta que no existe una medida de seguridad infalible, más bien se trata de utilizar capas de seguridad que dificulten hasta hacer casi imposible el acceso no autorizado. El filtraje por **dirección MAC** representa una capa más de seguridad y, como tal, es válida y efectiva. Podemos ver su habilitación en el **Paso a paso 1**.

DIRECCIÓN MAC

La dirección **MAC** (*Media Access Control Address* o **dirección de control de acceso al medio**) es un número de 48 bits que cada fabricante le asigna a la tarjeta. Trabaja en la Capa 2 del modelo OSI y permite encontrar un equipo en una red Ethernet.

PASO A PASO /1

Habilitar el filtraje por dirección MAC

1



En primer lugar, deberá conectarse a la interfaz web de administración del router. Como esta función es de la red inalámbrica, deberá ir a la pestaña correspondiente. Haga clic en **Wireless**.

2

De las opciones disponibles, presione aquella que le indique el uso de filtraje por MAC. Puede ser **MAC Filter** o **Wireless MAC Filter**. Tilde la opción **Enable** para habilitar el filtraje.

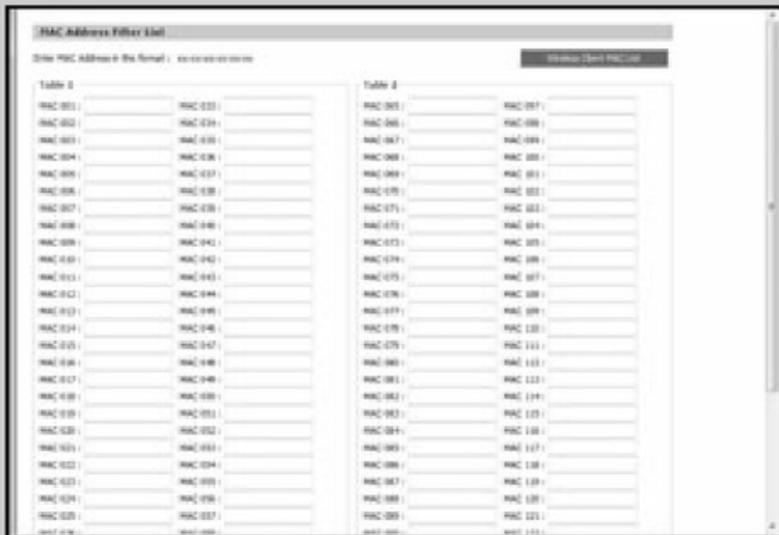
3



Deberá seleccionar el modo de filtrado (**Filter Mode**). Existen dos opciones basadas en el listado de direcciones MAC: permitir la conexión solo a los clientes que aparezcan en el listado (**Permit only clients listed to access the wireless network**) o bloquear la conexión a los clientes del listado y permitir al resto (**Prevent clients listed from accessing the wireless network**). Seleccione la primera y presione **Apply Settings**. Después, cuando compruebe que todo este funcionando correctamente, haga clic en **Save**.

PASO A PASO /1 (cont.)

4



Presione el botón **Edit MAC Filter List** para cargar la ventana para editar la lista de direcciones MAC. Debe recordar que las direcciones MAC se deben introducir en el formato indicado. Una vez que haya completado las direcciones, haga clic en **Save** primero, luego **Apply Settings** y **Close** para cerrar la ventana.

5



Para determinar la dirección MAC de la conexión de red inalámbrica tiene dos opciones. Puede hacer clic en el botón **Wireless Client MAC List** para ver una ventana con los clientes conectados y las direcciones MAC que están utilizando.

PASO A PASO /1 (cont.)

6



```

Administrador: Símbolo del sistema
Configuración IP de Windows

Nombre de host. . . . . : Pentium
Sufixo DNS principal. . . . . :
Tipo de nodo. . . . . : b1611d0
Encastillamiento IP habilitado. . . . . : sí
Proxy WINS habilitado. . . . . : no

Adaptador LAN inalámbrico Conexión de red inalámbrica:

Estado de los medios. . . . . : medios desconectados
Sufixo DNS específico para la conexión. . . :
Descripción. . . . . : D-Link Air DWL-120 Wireless USB A
AdapterCase.IP)
Dirección física. . . . . : 00-02-00-15-2C-46
DHCP habilitado. . . . . : sí
Configuración automática habilitada. . . . : sí

Adaptador de Ethernet Conexión de área local:

Sufixo DNS específico para la conexión. . . :
Descripción. . . . . : Adaptador de Fast Ethernet V18 10/
---
  
```

La otra forma de determinar la dirección MAC es a través del comando **ipconfig**. Busque el **Adaptador LAN inalámbrico** y el valor de la **Dirección física**.

7

Por último, recuerde que debe hacer efectivos los cambios (**Apply Settings**), probar que todo funcione correctamente y, entonces, salvarlos definitivamente con un clic en **Save**.

Clonar la dirección MAC

De la misma manera que podemos utilizar las direcciones MAC para restringir el acceso a nuestra red WiFi, algunos proveedores de Internet evitan accesos no autorizados filtrando la dirección MAC de los equipos que se conectan. Esto no es un problema normalmente, pero ¿qué pasaría si compramos un router inalámbrico y lo queremos conectar directamente a Internet en vez de a la PC? Tendríamos que llamar al proveedor, esperar que nos atienda, explicarle que necesitamos cambiar la dirección MAC, etcétera. Por eso existe una opción llamada **MAC Address Clone** o **Clone Your PC's MAC Address** (clonar la dirección MAC).

Si bien las direcciones MAC son únicas, podemos modificarlas y hacer que nuestro equipo utilice una diferente de la que tiene la tarjeta de red de manera predeterminada. Tenemos la posibilidad de obtener la dirección MAC de nuestra PC mediante el comando **ipconfig**.



Algunos modelos de routers tienen un botón **Get Current PC MAC Adress** (obtener la dirección MAC de la PC actual) que, si estamos conectados al router desde la PC que tiene la dirección MAC que queremos clonar, con hacer clic sobre él, automáticamente encontrará la dirección MAC y completará el campo requerido en el formulario del panel de configuración del router.

PROTEGER MI RED

La primera línea de defensa que tenemos en nuestras casas contra los accesos no autorizados es la puerta de entrada cerrada con llave. De manera similar, el mismo concepto se utiliza en las redes, solo que en vez de una llave se utiliza una frase, una **contraseña**.

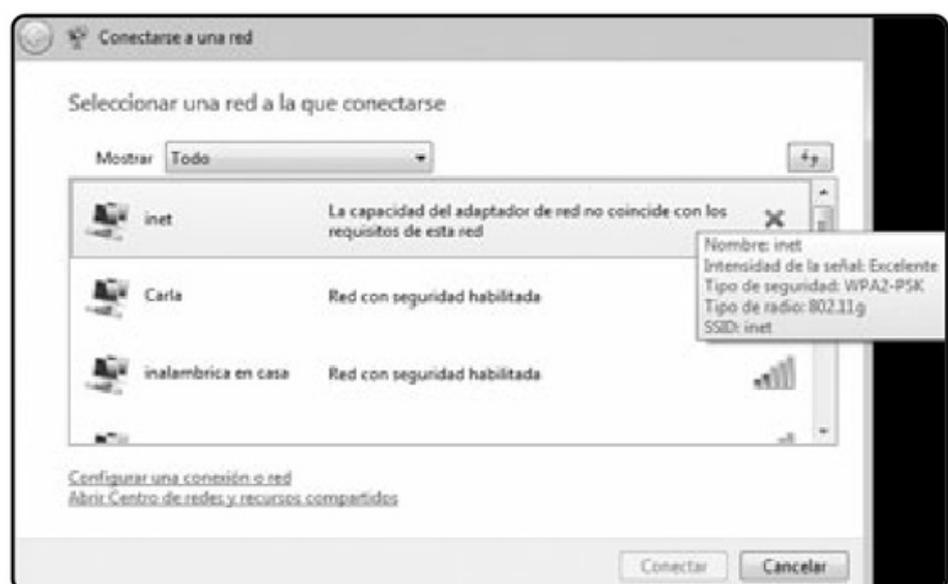
Para asegurar las redes inalámbricas, se han desarrollado un grupo de protocolos o **modos de seguridad** que permiten, al mismo tiempo, restringir el acceso a la red y proteger el tráfico de accesos no autorizados que circula por ella. El primer protocolo fue el **WEP** o **privacidad equivalente a la**

Para asegurar las redes inalámbricas se han desarrollado un grupo de protocolos o modos de seguridad

alámbrica (*Wired Equivalent Privacy*). El nombre indica que el sentido original de este protocolo era brindarles a las redes WiFi el nivel de seguridad que existía en las redes cableadas (**Figura 8**).

El protocolo WEP está muy extendido y prácticamente cada dispositivo WiFi lo soporta. Con el tiempo, se encontraron debilidades en sus algoritmos y se desarrollaron herramientas que permitían violar la seguridad de este protocolo en cuestión de minutos. La Alianza WiFi desarrolló, entonces, un nuevo protocolo, el **WPA** o **Acceso protegido a WiFi** (*WiFi Protected Access*). Los problemas de seguridad del

FIGURA 8.
Si el nivel de seguridad configurado en el router no es soportado por el controlador, veremos la indicación correspondiente.



WEP motivan que el WPA se base en una versión del protocolo 802.11i, que en ese momento no estaba concluido. Cuando fue concluido finalmente, para establecer una diferencia, se denominó **WPA2**, que no es más que la versión de WPA que implementa el protocolo 802.11i en su totalidad.

Windows Vista soporta los tres modos de seguridad que hemos mencionado hasta ahora. Como siempre, el más moderno es el que mayor nivel de seguridad brinda. WPA2 es más seguro que WPA que, a su vez, es más seguro que WEP. La decisión sobre cuál utilizar dependerá en gran medida del equipamiento que poseamos, en particular del software que utilizemos.

Podríamos tener en casa dispositivos que solo permitieran trabajar con WEP, otros que soportaran WPA, pero no WPA2. Para poder configurar un

modo de seguridad en la red WiFi, todos los equipos que vayamos a conectar a ella deben soportarlo.

Los protocolos que soportan un router o una tarjeta de red inalámbrica van a estar dados por la versión de software que utilicen. Es decir, dependerán de la versión del firmware, para el caso de los routers, y del driver, para la tarjeta de red. El propio ritmo de la tecnología hace que los equipos no sean soportados por mucho tiempo, ya que nuevos modelos surgen constantemente. Los viejos quedan descontinuados y ya no se publican actualizaciones para ellos. Siempre está la opción de comprarnos el último modelo, pero si ya teníamos uno, no vale la pena gastar dinero innecesariamente.

Para comprobar los modos de seguridad disponibles, revisamos la configuración del router (**Figura 9**).

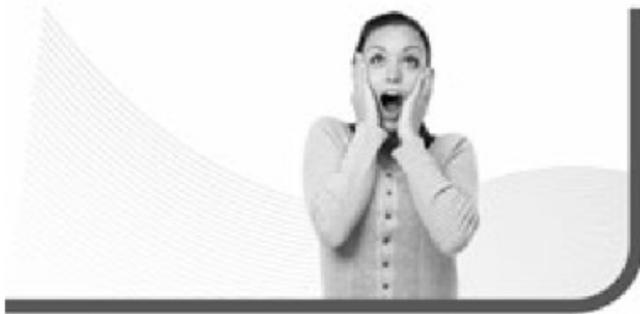


FIGURA 9.
El modo de seguridad seleccionado deberá estar soportado tanto por el router como por los equipos que se conecten a él.



ENCRIPCIÓN

Tanto WPA como WPA2 utilizan **algoritmos** para la encriptación. Los disponibles son el **AES** (estándar avanzado de encriptación o *Advanced Encryption Standard*) y el **TKIP** (protocolo de integridad con llave temporal o *Temporal Key Integrity Protocol*).



Cada modo de seguridad tiene parámetros de configuración adicionales

Esta información la encontramos en la pestaña **Wireless Security** (seguridad inalámbrica) en el ítem **Security Mode** (modo de seguridad). Allí seleccionamos el nivel más seguro que permitan los dispositivos que vamos a conectar a la red.

Cada modo de seguridad tiene parámetros de configuración adicionales. Si seleccionamos WEP, podemos utilizar encriptación de 64 ó 128 bits, que es la más segura, pero no todos los equipos la soportan.

También debemos teclear una **frase de contraseña** (*passphrase*) que el router utiliza para generar las **llaves** (*key*) de las que este protocolo se vale. En este caso, son las llaves las que se utilizan en la seguridad de la conexión, no la frase de contraseña como tal.

Si el modo seleccionado es **WPA Personal** (Figura 10) o **WPA2 Personal**, debemos elegir **WPA Algorithms** (algoritmo de cifrado) y teclear la **WPA Shared Key** (clave de seguridad o frase de contraseña compartida). La incorporación de algoritmos de seguridad es una mejora de estos modos con respecto a WEP (Figura 11).

BUSCAR REDES, CONECTARNOS A ELLAS

Desde la ventana **Administrar redes inalámbricas**, podemos seleccionar el botón **Agregar** para ejecutar el asistente **Conectarse manualmente a una red inalámbrica** (Figura 12).

La primera opción que aparece es **Agregar una red en el alcance de este equipo**. Al seleccionarla, veremos una ventana con todas las redes

FIGURA 10.
Aunque AES es el algoritmo más seguro, todavía no todos los equipos lo soportan.





FIGURA 11.
Para ayudarnos a evitar errores, podemos tildar la opción Unmask (mostrar caracteres), que nos permite ver lo que estamos escribiendo.

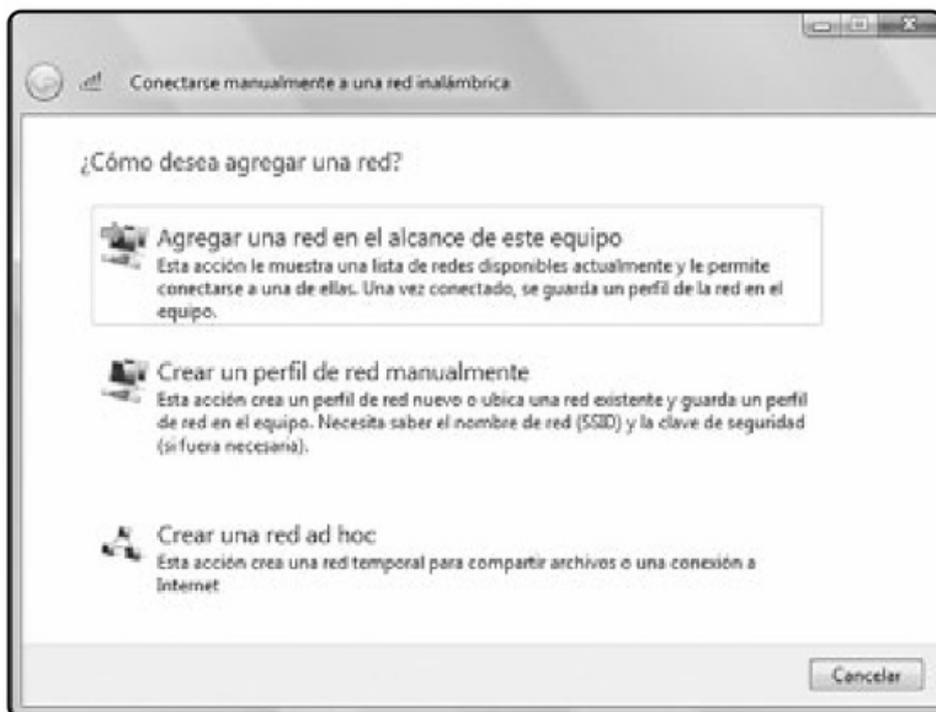


FIGURA 12.
El asistente de conexión a redes inalámbricas resulta muy cómodo de utilizar.



CONTRASEÑA DE CONFIGURACIÓN

No resulta especialmente complicado definir una contraseña y configurar la conexión del equipo a la red WiFi. En una red hogareña, es un procedimiento que tendremos que realizar dos o tres veces (cuatro, si un amigo trae su notebook).

inalámbricas que están a nuestro alcance. Seleccionamos nuestra red en el listado y hacemos clic en el botón **Conectar**. La siguiente ventana nos pedirá la **Clave o frase de contraseña de seguridad**, que fue la que definimos en el router cuando configuramos el modo de seguridad. Escribimos la contraseña y hacemos clic en el botón **Conectar**. Una vez establecida la conexión, aparecerá una última ventana donde podremos tildar dos opciones: **Guardar esta red** e **Iniciar esta conexión automáticamente**.

La segunda opción: **Crear un perfil de red manualmente** es la que se emplea en aquellas situaciones en las que se ha deshabilitado la difusión del **SSID**, y la red no aparece en los listados de redes. En este caso, completamos los campos y procedemos a conectarnos (**Figura 13**). Por último, podemos **Crear una red ad hoc**, que nos permite crear una red temporal entre equipos, sin un router (**Figura 14**).

MODIFICAR MIS REDES INALÁMBRICAS

En la ventana **Administrar redes inalámbricas** (**Figura 15**), veremos las redes que tenemos configuradas. De manera predeterminada, cada vez que nos conectamos a una red, Windows Vista guarda la conexión y, cada vez que la detecta, se conecta a ella automáticamente. Si en algún momento necesitamos modificar esta configuración, lo podemos hacer en esta ventana. Con un clic secundario sobre el icono de la red inalámbrica, veremos un menú contextual donde la primera opción es **Propiedades**. La seleccionamos con un clic y aparece la ventana **Propiedades de la red inalámbrica** de la red que hayamos seleccionado.

La ventana **Propiedades de la red inalámbrica** (**Figura 16**) tiene dos pestañas, la primera es **Conexión**, que contiene información general sobre la red. Ahí también podemos definir la forma en que

FIGURA 13.
La única forma de conectarnos a una red que haya deshabilitado la difusión del SSID es a través de una conexión manual.

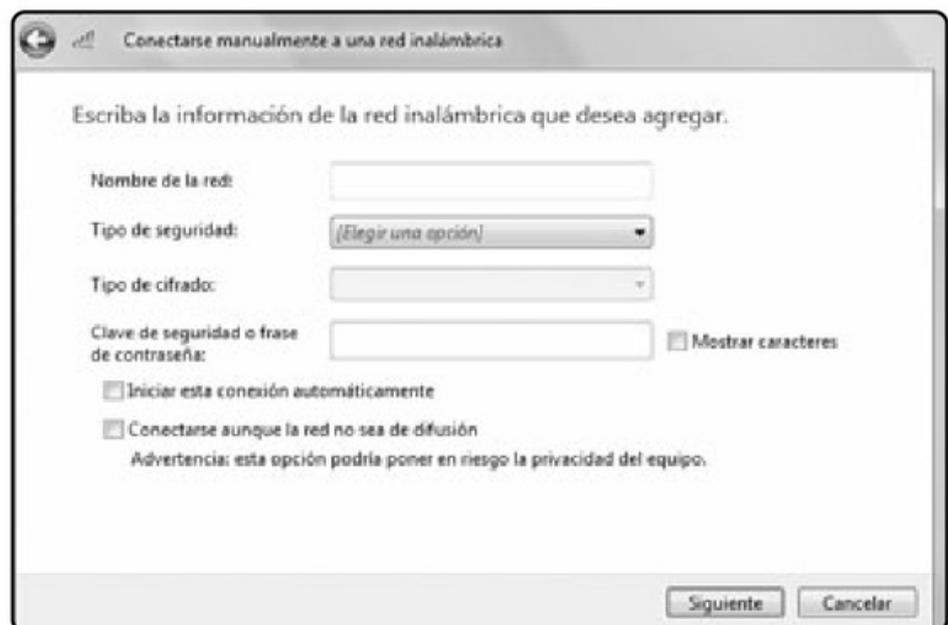




FIGURA 14.
Los enlaces de redes WiFi se identifican con líneas discontinuas en el Mapa de la red, para diferenciarlos de los cableados.

nos conectamos a ella. La primera opción: **Conectarse automáticamente cuando esta red esté dentro del alcance** nos evita tener que realizar los pasos de la conexión cada vez que encendemos la notebook dentro del alcance de nuestra red. Si estamos utilizando una red que no difunde el **SSID**, debemos tildar la casilla **Conectarse aunque la red no sea de difusión**. Cuando ya nos conectamos a una red, Windows Vista la almacena como **red preferida**. Si tenemos dos routers inalámbricos para cubrir un área mayor, es posible que en algún momento quedemos bajo el alcance de ambos.

Windows Vista los detectará y tratará de conectarse a cada uno alternativamente, y provocará interrupciones en la conexión. Para evitar esto, deberemos decidir cuál va a ser nuestra conexión favorita y, en la otra red, tendremos que tildar la opción **Conectarse a una**

En la ventana Administrar redes inalámbricas veremos las redes que tenemos configuradas



FIGURA 15.
A través del panel Administrar redes inalámbricas, podemos acceder a sus propiedades.

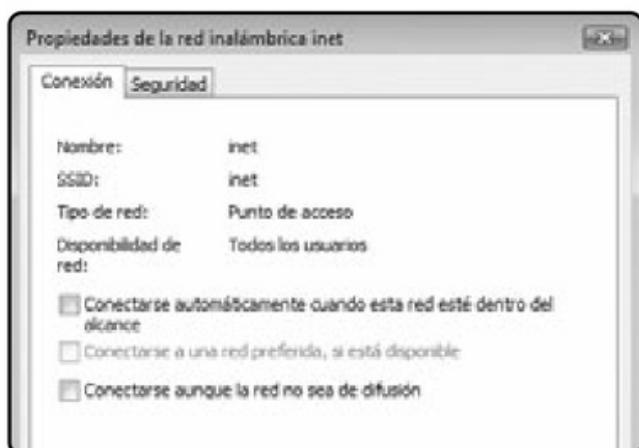


FIGURA 16. Windows Vista nos permite conectarnos automáticamente a las redes conocidas si estamos dentro de su alcance.

red preferida, si está disponible. De esta manera, Windows Vista chequea si hay alguna otra disponible antes de utilizar esta conexión y, solo si es la única existente, la establece.

La segunda pestaña es la que corresponde a **Seguridad (Figura 17)**. Aquí podemos modificar la configuración de seguridad, cambiar la contraseña, el tipo de seguridad, etcétera. De acuerdo con el **Tipo de seguridad** seleccionado, se muestran las opciones posibles. También veremos el **Tipo de cifrado** disponible para el controlador de nuestro equipo y la casilla de texto para escribir la **Clave de seguridad de red** que hayamos configurado en el router.

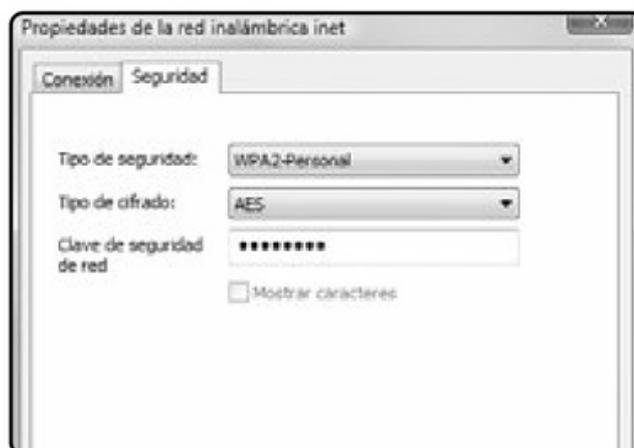


FIGURA 17. Debemos tener presente que el controlador de nuestra tarjeta de red WiFi determina los tipos de seguridad disponibles.

ARMAR UNA RED INALÁMBRICA SIN COMPRAR UN ROUTER

Imaginemos que estamos en una reunión de trabajo con nuestra notebook, nuestros colegas han llevado sus equipos, pero el salón de reuniones no tiene un punto de acceso inalámbrico.

En esos casos, podemos habilitar un modo de funcionamiento de las redes inalámbricas que permite conectar equipos entre sí, sin necesidad de contar con un punto central.

Este tipo de red se llama **ad hoc (Paso a paso 2)**. Existen servicios como el **Área de encuentro de**



CURIOSIDAD

Existen muchos aficionados al tema de las redes WiFi y todo el tiempo hacen experimentos. Uno de éstos llevó a la fabricación de una antena unidireccional con una lata de papas fritas de la marca **Pringles**, sobre la que se puede conseguir información en internet.



Si bien un router se puede configurar en modo ad hoc, lo más común es que lo encontremos funcionando en modo AP (Access Point)

Windows, que utilizan este tipo de redes, son muy útiles en casos particulares y redes temporales; sin embargo, carecen de las funcionalidades y prestaciones que brinda un router inalámbrico (**Figura 18**).

Si bien un router se puede configurar en modo ad hoc, lo más común es que lo encontremos funcionando en

modo **AP (Access Point)** o punto de acceso, que es el modo acostumbrado, donde actúa como nodo central.

En el **capítulo 6**, dedicado a Internet, aprenderemos todo sobre los navegadores y sus diferentes características. Además de nuestras opciones para la configuración de nuestra red a Internet.

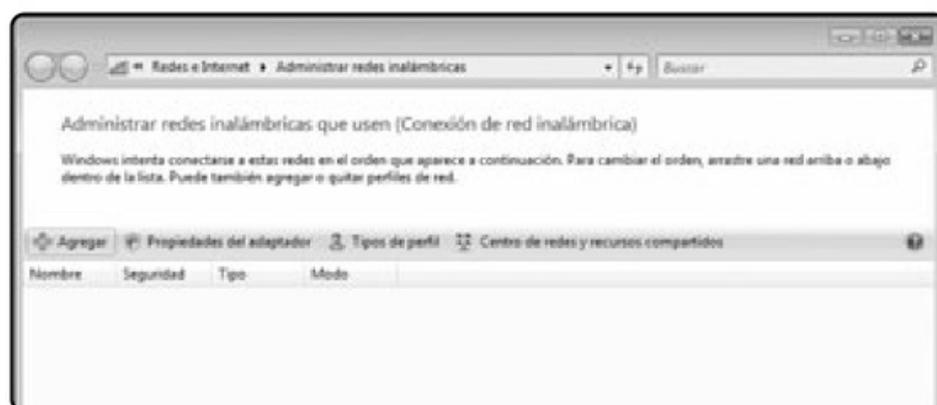


FIGURA 18.
Primero debemos conectarnos a una red antes de poder administrarla.



RESETEAR EL ROUTER

Si alguna vez llegamos al punto donde hemos hecho tantos cambios que ya no recordamos qué modificaciones hicimos, no debemos preocuparnos. Todo router inalámbrico cuenta con un botón de **Reset** al que se debe acceder con la ayuda de una aguja o alfiler.

PASO A PASO /2

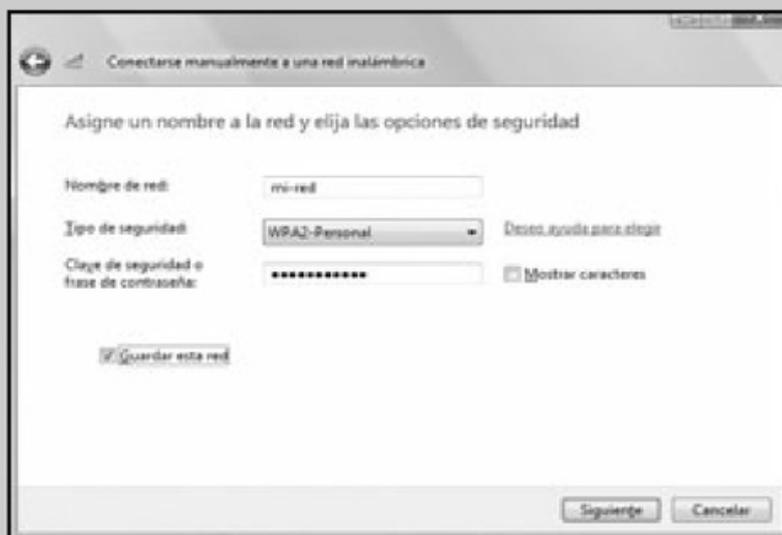
Configurar una red ad hoc

1



Luego de seleccionar la opción **Crear una red ad hoc** en la ventana **Conectarse manualmente a una red inalámbrica**, verá la primera pantalla del asistente, que le brindará algunos consejos.

2



Una vez que haya hecho clic en **Siguiente**, deberá colocar las opciones de configuración, que son similares a las que se configuran en el router para una red inalámbrica común.

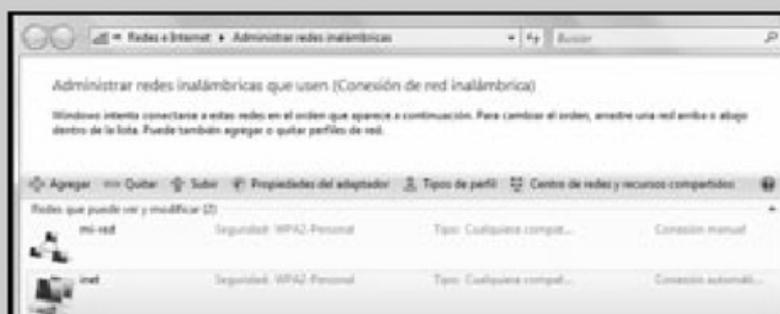
PASO A PASO /2 (cont.)

3



En la ventana siguiente, haga clic en **Activar la conexión compartida a Internet**, para que los otros equipos puedan conectarse a través de la red inalámbrica.

4



Luego de presionar **Cerrar**, habrá quedado configurada la red ad hoc, que podrá ver y modificar desde la ventana **Administrar redes inalámbricas**.

RESUMEN

En este capítulo, hemos analizado las redes WiFi. Estudiamos los diferentes tipos y, además, aprendimos a habilitar el filtraje por dirección MAC y a configurar una red ad hoc, entre otros procedimientos útiles.

Multiple choice

► **1** ¿Cuál es la dirección predeterminada del router?

- a- 192.168.1.1.
 - b- 192.168.1.10.
 - c- 1921.168.1.10.
 - d- 182.168.1.1.
-

► **2** La norma 802.11g tiene un alcance en metros en interiores, de alrededor de:

- a- 50m.
 - b- 32m.
 - c- 100m.
 - d- 38m.
-

► **3** El SSID se refiere a:

- a- El tipo de conexión que utiliza la red.
 - b- El nivel de seguridad de la red.
 - c- La contraseña de la red.
 - d- El nombre que identifica a la red.
-

► **4** Para averiguar la dirección MAC del equipo se utiliza el comando:

- a- Net stat.
 - b- Cmd.
 - c- Netmeeting.
 - d- Ipconfig.
-

► **5** El nivel de seguridad recomendable es:

- a- WEP.
 - b- WPA-Personal.
 - c- WPA-Enterprise.
 - d- WPA2.
-

► **6** ¿Cuál es el nombre que identifica a nuestra red?

- a- Wireless Network Mode.
 - b- Wireless Network Name.
 - c- Datos de autenticación.
 - d- Dirección IP del router.
-

Respuestas: 1-a, 2-d, 3-d, 4-d, 5-d, 6-b.

Capítulo 6

Internet



En este capítulo, conoceremos todo sobre Internet: los navegadores y sus diferentes características.

Internet

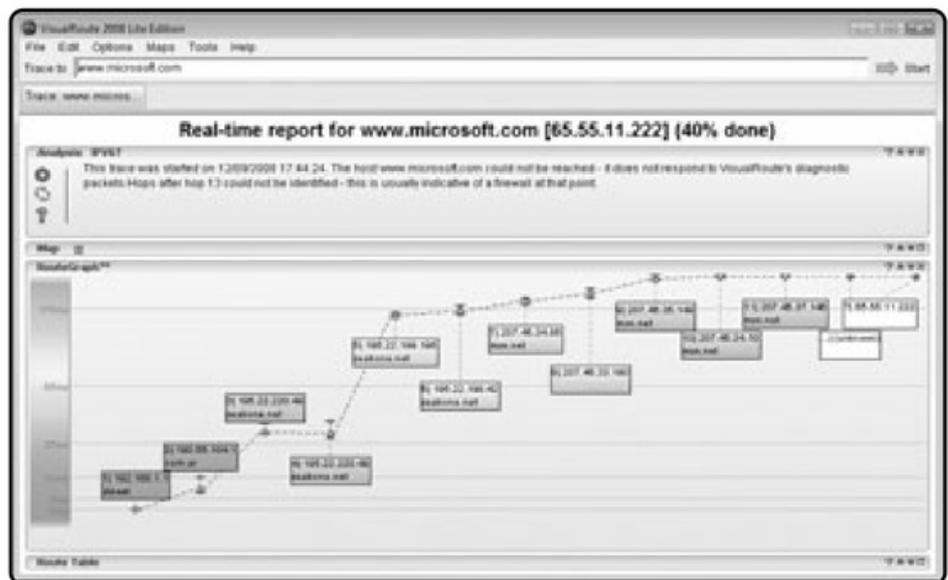
Cuando nos conectamos a Internet, tenemos conexión inmediata con todos los equipos que están conectados a ella en ese momento (**Figura 1**). Al ser una red internacional, queda clara la magnitud de la cantidad de equipos a los que podríamos tener acceso. Los detalles de cómo funciona Internet tomarían un libro entero. A nosotros nos basta con saber que, a partir de que tenemos una conexión a Internet, estamos conectados a ella.

De la misma manera en que necesitábamos un punto de red para conectar una PC a nuestra red,



vamos a necesitar un **punto de acceso** para acceder a Internet. Para eso existen entidades que se dedican a proveer este servicio.

FIGURA 1.
Si alguna vez nos preguntamos qué pasa cuando nos conectamos a un servidor, aplicaciones como VisualRoute nos permiten ver el recorrido que siguen los paquetes de datos cuando viajan por Internet.



COMIENZOS DE LA CONEXIÓN ENTRE REDES

Cuando comenzaron a conectarse entre sí redes dispersas geográficamente, el único medio de interconexión en ese momento eran los cables de las líneas telefónicas. Al conectar cables desde una central hasta la siguiente, se armaba un recorrido ininterrumpido.

Cuando nos conectamos a Internet, tenemos conexión inmediata con todos los equipos que están conectados a ella en ese momento

CONECTARSE A INTERNET DESDE CASA

Una vez más, la primera gran diferencia radica entre los accesos alámbricos y los inalámbricos. Nuevamente nos concentraremos en las conexiones alámbricas, que son las más extendidas.

En el momento en que Internet comenzó a adquirir popularidad, era común tener un teléfono en la casa. Ésta fue la vía seleccionada por los proveedores para ofrecer la conexión. A través de un dispositivo llamado **módem**, que se conectaba a la PC, podíamos conectarnos a un número telefónico y establecer una conexión a Internet (**Figuras 2 y 3**).

Con el tiempo, los usuarios empezaron a estar más tiempo conectados a Internet, y esto traía como



FIGURA 2. Los módems fueron muy populares en los inicios de Internet.

inconveniente que, mientras estábamos navegando por Internet, no podíamos recibir llamadas telefónicas. No pasó mucho tiempo antes de que los ingenieros encontraran la forma de enviar más de una señal por el mismo cable, lo que nos permitió estar conectados a Internet y poder hablar por teléfono al mismo tiempo.

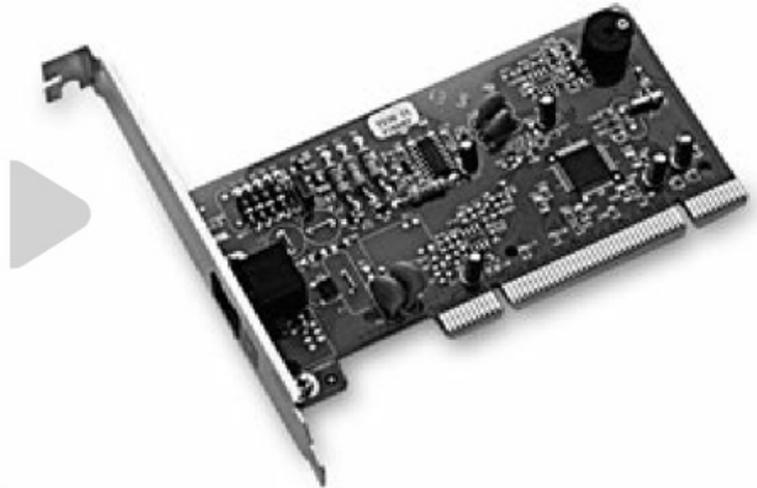
De esta manera, podíamos estar en casa revisando los e-mails de la oficina al tiempo que nuestra hija hablaba por teléfono con sus amigas. Como consecuencia, surgieron nuevas formas de conectarse a Internet con mayores velocidades, las llamadas **conexiones de banda ancha**.



CONCEPTO DE MÓDEM

La palabra módem está compuesta por la abreviatura de **modulador** y **demodulador**. Un módem realiza las dos funciones: toma una señal eléctrica y la modula en forma de señal, es decir los 0 y 1 emitidos por una PC, y es capaz de transformarlos en señales audibles.

FIGURA 3.
Los módems internos son placas que se conectan directamente al motherboard de la PC.



¿NECESITO PERMISOS PARA CONECTARME A INTERNET?

El agua es gratis, pero eso no quita que la empresa de agua nos cobre una cuota mensual por el servicio de traérsela hasta nuestra casa. Con Internet sucede algo similar, su uso es gratis, pero hay que pagar por la conexión. Un proveedor de acceso a Internet requiere mantener equipamiento que le permita establecer los enlaces a sus usuarios. Tiene que cubrir costos asociados a la operación del equipamiento y del personal que se encarga de manejarlo.

Estas empresas cobran por su servicio y controlan el acceso a sus recursos. En algunos casos, alguna entidad puede asumir estos gastos y permitir un acceso

que, si bien es libre de costo para el usuario, hay alguien que lo está pagando. Esto es común en redes Wi-Fi, donde una cafetería le ofrece el servicio a sus clientes o en un aeropuerto, donde lo habilitan como una comodidad para los pasajeros.

En la mayoría de los casos, el acceso a Internet desde nuestras casas será un servicio pago, y el proveedor se asegurará de que solo aquellos clientes que hayan contratado el servicio lo puedan utilizar. Si utilizamos una conexión de acceso telefónico, tendremos que tener un número de teléfono, un nombre de usuario y una contraseña (**Figura 4**).

FIGURA 4.
Los datos para utilizar una conexión de acceso telefónico gratuito a Internet se brindan en los sitios web de sus proveedores.



Para las conexiones de banda ancha, en algunos casos no hace falta nada, pero en otros sí tendremos un nombre de usuario y otra contraseña. A diferencia de las conexiones telefónicas, no va a hacer falta un número de teléfono porque no es necesario llamar, la conexión es permanente.

Las conexiones de banda ancha que requieren un nombre de usuario y contraseña utilizan, por lo general, el protocolo **PPPoE** que comentamos en el **Capítulo 3 (Figura 5)**.

Si contratamos el servicio con un cablemódem, es muy probable que no necesitemos ningún permiso ya que, al igual que la señal de TV que nos llega por el cable, la instalación del equipo corre por cuenta de la empresa, la que nos autoriza para acceder a Internet.

CONFIGURAR LA CONEXIÓN A INTERNET

Con el lanzamiento de Windows Vista, Microsoft ha puesto especial interés en facilitar el uso de las PC. Como el acceso a Internet es un procedimiento tan común en estos tiempos, contamos con un asistente que nos ayuda a configurar la conexión. Solo deberemos seleccionar el tipo de conexión que vamos a utilizar, y el asistente nos pedirá los datos que necesite (**Paso a paso 1**).

Una vez completada la información, Windows Vista creará la conexión. Si es una de tipo banda ancha, el enlace quedará establecido. Si es una de tipo acceso remoto (telefónico), creará la conexión y la dejará lista para el momento que necesitemos utilizarla y nos conectaremos por medio del dial-up.



FIGURA 5.
Cuando conectamos un router Wi-Fi a Internet, podemos configurarlo para que utilice PPPoE.



ORÍGENES DE INTERNET

A finales de los 80 y principios de los 90, el científico inglés **Sir Tim Berners-Lee**, que trabajaba para la **CERN** en Ginebra, Suiza, desarrolló una forma de crear documentos de texto entrelazados. Su invento, años después, dio lugar a Internet.

PASO A PASO /1

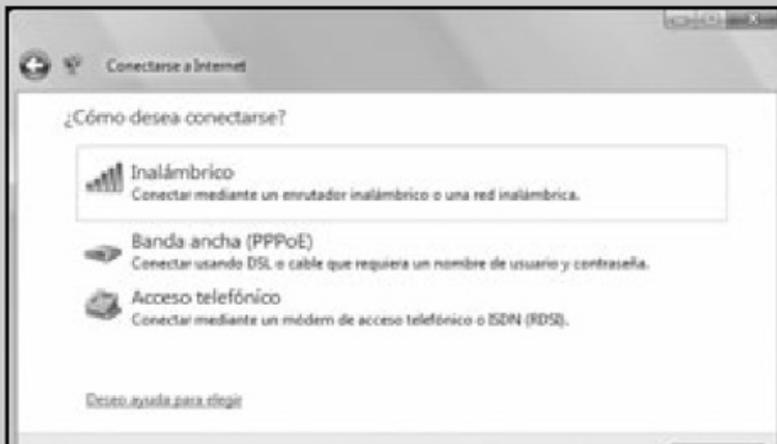
Configurar la conexión a Internet en Windows Vista

1



En el menú **Inicio**, haga clic en la opción **Conectar a** para ejecutar el asistente de conexión a redes. Luego en **Conectarse a Internet** y presione **Siguiente**.

2



El asistente le mostrará las opciones de conexión posibles, de acuerdo con la configuración de su PC. Si tiene un módem instalado, verá la opción **Acceso telefónico**, y así para el resto. La conexión de **Banda ancha** solo requiere la presencia de la tarjeta de red por lo que, al menos, esta opción deberá aparecerle en la ventana de este paso. Seleccione **Acceso telefónico**.

PASO A PASO /1 (cont.)

3

En la ventana **Configurar una conexión de acceso telefónico**, deberá completar el **Número de teléfono de marcado**, el **Nombre de usuario** y la **Contraseña**. Todos estos datos se los proporcionará el proveedor de acceso a Internet. Puede tildar la opción **Mostrar caracteres** para evitar errores de escritura de la contraseña y tildar la casilla de **Recordar esta contraseña** para evitar tener que escribirla en el futuro cuando utilice esta conexión. También puede asignarle un **Nombre de conexión** para diferenciarla de las de otros proveedores.

Cuando utilizamos un cablemódem, no es necesario el asistente. La conexión se establece con la tarjeta de red y toma la configuración TCP/IP automáticamente del cablemódem (**Figura 6**).

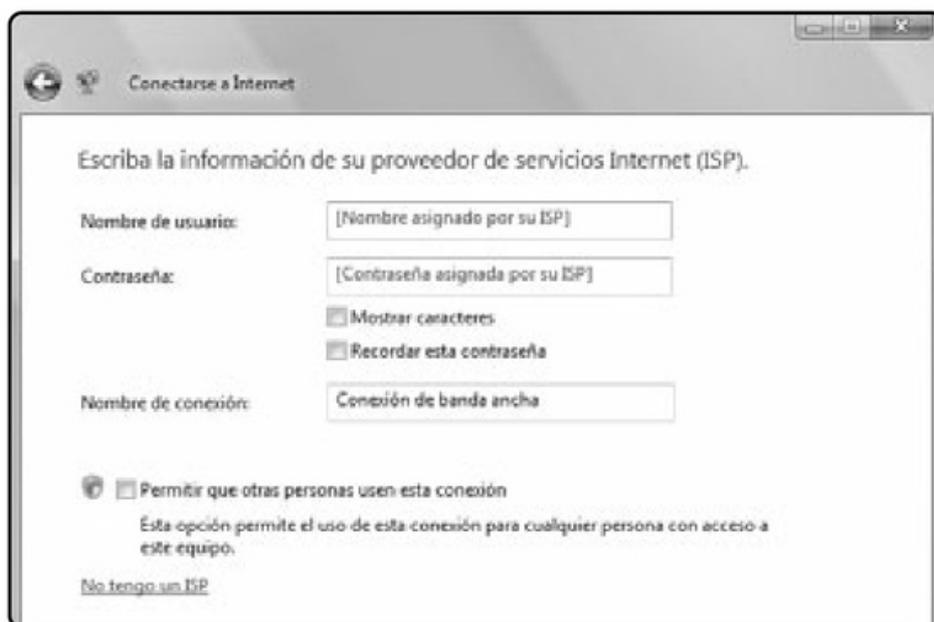
Algunos tipos de conexiones a Internet, como las de acceso telefónico, necesitan un nombre de usuario y una contraseña. En estos casos en los que se requiere

determinada autorización para establecer el enlace, Windows Vista muestra una casilla donde podemos **Permitir que otras personas usen esta conexión**. Si utilizamos una conexión para enlazar a la oficina por motivos de trabajo o tenemos una conexión a Internet con un número de horas limitado mensualmente, no nos gustaría que, por equivocación, algún miembro de la familia la utilice.



FIGURA 6.

Para las conexiones de banda ancha, solo necesitamos utilizar el asistente cuando se trata de una conexión PPPoE. Estas conexiones tienen las mismas opciones que las de acceso telefónico, pero no necesitan marcar un número de teléfono.



Dicha casilla deberá permanecer desmarcada para que no suceda esto. Si, por el contrario, nos conectamos a Internet a través de un proveedor sin restricciones de ningún tipo y queremos que cualquiera en la casa pueda conectarse, la dejamos tildada.

CONFIGURAR LA COMPUTADORA PARA TENER INTERNET

Los técnicos darán por concluido el proceso de instalación una vez que hayan establecido la conexión a Internet desde nuestra PC. Los servicios de banda ancha como los que emplean cablemódem no necesitan ninguna configuración especial en nuestra PC.

El cablemódem le asigna la dirección IP a la PC, en forma automática.

Para las conexiones por ADSL, en vez de un módem tradicional, se instala un router que incluye la funcionalidad del módem, pero que permite establecer la conexión PPPoE, y los datos del nombre de usuario y la contraseña se configuran en el router de forma directa.

Al igual que el cablemódem, conectamos un cable de red a la PC y la configuración TCP/IP se obtiene automáticamente (**Figura 7**).



UPnP

De la misma forma en que vimos que el sistema **PnP** (*Plug and Play*) de las tarjetas PCI nos ahorra el engorroso trabajo de configurarlas manualmente, en los routers **UPnP** va a permitirnos que las aplicaciones realicen sus configuraciones automáticamente.



FIGURA 7. En general, la configuración automática es todo lo que necesitamos definir para conectarnos a Internet.

COMPARTIR LA CONEXIÓN A INTERNET EN MI RED

Ya tenemos nuestra PC conectada a Internet, pero resulta que ahora necesitamos conectar otro equipo, ya sea una segunda PC que compramos o una

Para las conexiones por ADSL, en vez de un módem tradicional, se instala un router

notebook que nos trajimos de la oficina. El router ADSL o el cablemódem solo tienen una conexión Ethernet, ¿qué hacemos entonces?. Dejemos de lado la opción de contratar una segunda conexión a Internet (teóricamente, es una variante) y veamos qué otra alternativa tenemos.

Nuestro proveedor nos asigna una sola dirección IP, es decir, solo podemos tener un equipo conectado a Internet. Esto, en realidad, tampoco es un problema ya que, por una cuestión de seguridad, mientras menos equipos tengamos conectados a Internet, menos preocupaciones tendremos. Se trata entonces de buscar la manera de que, a través del único equipo que está conectado a Internet, podamos compartir esa conexión con el resto de los equipos de la red interna (**Figura 8**).



FIGURA 8. A través de su interfaz web, podemos consultar el estado de operación de nuestro cablemódem.



Para utilizar ICS necesitamos dos interfaces de red en la PC

Cuando la falta de direcciones IP empezó a surgir como un problema futuro, una de las soluciones que se desarrolló fue permitir el acceso a Internet a un grupo de PCs en una red interna a través de un único equipo conectado a Internet. De esta manera, con una sola dirección IP conectada a Internet, se garantizaba el acceso a todos los equipos en una red interna.

Esta técnica se conoce por el nombre de **NAT** (*Network Address Translation* o **traducción de direcciones de red**), y le permite al equipo conectado a Internet recibir conexiones de la red interna, enviarlas a Internet como si fueran propias, y devolverle la respuesta al equipo interno que hizo la solicitud.

Windows Vista incluye un servicio que implementa NAT, que se llama **Conexión compartida a Internet** o **ICS** (*Internet Connection Sharing*), por sus siglas en inglés. El **ICS** le permite a nuestra PC, si está conectada a Internet, compartir dicha conexión a través de una segunda interfaz de red. Pero **ICS** no es la única opción: los routers (incluidos los inalámbricos) incluyen soporte NAT, por lo que directamente proporcionan este servicio de manera predeterminada (**Figura 9**).

CONFIGURAR EL ACCESO A INTERNET DE LOS OTROS EQUIPOS

El primer paso sería compartir la conexión a Internet. Si disponemos de un router, podemos obviar el procedimiento del **Paso a paso 2, Compartir una conexión a Internet con ICS**, pero para los que no tenemos el router o el presupuesto para comprarlo, nos queda la opción de **ICS**.

FIGURA 9.
La configuración NAT de un router nos permite tener acceso a las aplicaciones que se ejecutan en la red interna.



Para utilizar **ICS** necesitamos dos interfaces de red en la PC: una conectada a Internet y la otra a la red interna (podría ser a otra PC si utilizamos un cable de red punto a punto). Los cablemódems suelen tener dos opciones para conectarse a la PC, como ya vimos, a través del puerto USB o de la tarjeta de red. En la actualidad, las PCs vienen con una tarjeta de red incorporada, por lo que si conectamos el cablemódem a la PC mediante el cable USB, la tarjeta de red de la PC quedará libre.

De esta manera, tendríamos la PC conectada a Internet por la conexión USB y podríamos compartirla a través de la tarjeta de red del equipo, que debemos conectar al switch de nuestra red local. Si conectamos la PC al cablemódem con la tarjeta de red, también podemos utilizar la computadora para compartir la

conexión a través de **ICS (Figura 10)** si le instalamos una segunda tarjeta de red, lo que resultará más conveniente en términos económicos ya que podemos invertir cerca de u\$s 7 en una nueva tarjeta, mientras que comprar un router estaría sobre los u\$s 70.

LAS OPCIONES DE INTERNET EN EL PANEL DE CONTROL

En **Panel de control/Redes e Internet**, encontramos tres secciones que ya conocimos: el **Centro de redes y recursos compartidos**, las **Opciones de Internet** y el **Firewall de Windows**. Al hacer clic sobre la primera o la tercera opción, se cargarán los paneles de configuración de las secciones mencionadas. En cambio, si seleccionamos **Opciones de Internet**, podremos ver la ventana **Propiedades de Internet**.



FIGURA 10.
Las PCs de la red interna recibirán la configuración de manera automática. Solo debemos restablecer el adaptador de red, que podemos hacerlo con un clic en Diagnosticar esta conexión.



¿POR QUÉ SE LLAMAN NAVEGADORES?

El efecto de conectarnos a un servidor web, y ahí hacer un clic en un enlace que nos lleva a otro servidor, y de allí a otro, es lo que se conoce como **navegar**. Por este motivo, las aplicaciones que se utilizan para acceder a la Web se llaman **navegadores**.

PASO A PASO /2

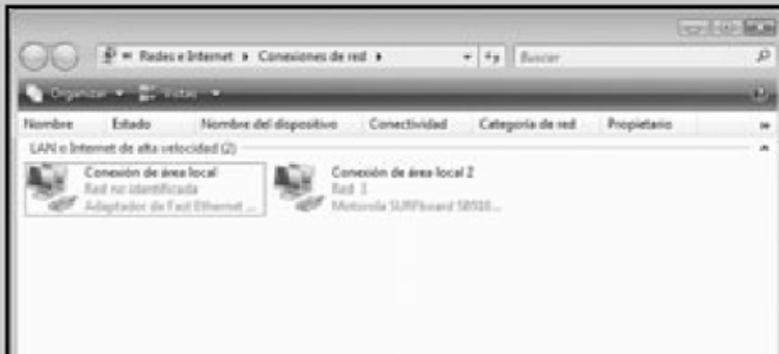
Compartir una conexión a Internet con ICS

1



En el **Centro de redes y recursos compartidos**, seleccione la tarea que aparece en el panel de la izquierda: **Administrar conexiones de red**.

2



En la ventana **Conexiones de red**, verá las conexiones de red configuradas en la PC. Deben existir al menos dos si quiere utilizar **ICS**.

3

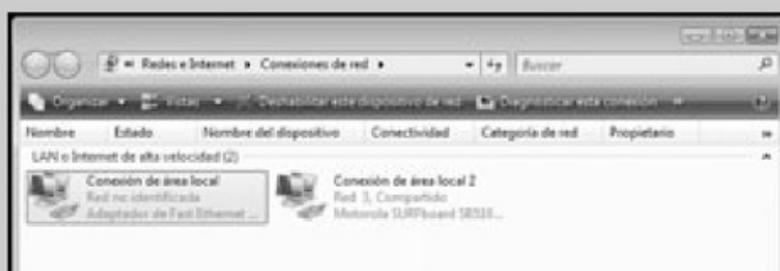
Sobre la conexión de red que está conectada a Internet haga clic secundario y, en el menú que aparece, seleccione **Propiedades**.

4

Haga clic en la pestaña **Uso compartido** y tildé la opción **Permitir que los usuarios de otras redes se conecten a través de la conexión a Internet de este equipo**.

PASO A PASO /2 (cont.)

5



Al finalizar el procedimiento debe presionar **Aceptar**, y la conexión a Internet se identificará como un enlace **Compartido**. El proceso finalizó con éxito.

Quienes llevamos algún tiempo trabajando con Windows notaremos cierta familiaridad con esta ventana (**Figura 11**): es la misma que aparece si buscamos las propiedades del navegador web de Windows, que forma parte integral del sistema operativo y, por esta razón, ambos comparten en una misma ventana opciones de configuración.

Las opciones se agrupan en pestañas. Algunas son específicas del navegador, y otras corresponden al tema de **Seguridad**. Estos casos los analizamos en los apartados siguientes. Relacionadas con el sistema operativo encontramos dos pestañas: **Conexiones** y **Programas**. En la primera, se establece cómo accede a Internet Windows Vista. Cualquier aplicación que intente utilizar Internet, lo hará a través de las conexiones aquí definidas. Si tenemos una red con banda ancha, no hace falta definir nada, pero si utilizamos un módem para conectarnos, el acceso telefónico creado se mostrará aquí.



FIGURA 11. Para configurar un acceso telefónico, debemos tener un módem instalado.



Definimos las aplicaciones que Windows Vista va a utilizar para realizar tareas comunes relacionadas con Internet

La opción **Configuración de LAN** nos permite definir algunas configuraciones que se utilizan principalmente en redes grandes que instalan **servidores** conectados a Internet.

Estos servidores, brindan el acceso a la Web a los navegadores de la red interna y cumplen una doble función: por un lado, guardan una copia de todas las páginas que se visitan de manera tal que, cuando un segundo usuario intenta acceder a la página que otro ya visitó, se le envía la copia almacenada en el servidor, con lo que la velocidad de navegación se incrementa; por otro lado, permiten establecer controles para el acceso a los sitios web.

La otra opción que afecta el sistema en general es la pestaña **Programas** (Figura 12). Allí definimos las aplicaciones que Windows Vista va a utilizar para realizar tareas comunes relacionadas con Internet.

Cada vez que aparece un enlace a una página web en un correo electrónico o en un documento de texto, al hacer clic sobre él, se carga el navegador predeterminado. Las restantes opciones se refieren a otras aplicaciones, como un editor de **HTML** (el lenguaje en el que se crean las páginas web), y la aplicación que estamos utilizando para trabajar con los correos electrónicos.

MICROSOFT INTERNET EXPLORER

Internet Explorer es el nombre que recibe una aplicación para navegar por la Web. Forma parte



FIGURA 12. Cuando empleamos otro navegador, resulta conveniente desactivar el chequeo que realiza IE para determinar si es el predeterminado.

del sistema operativo Windows desde su incorporación a Windows 95 y también se lo identifica por

sus siglas **IE** y **MSIE** (Microsoft Internet Explorer). En la **Guía Visual 1** conoceremos su interfaz.

GUÍA VISUAL /1

La interfaz de Internet Explorer 8



- 1 **Centro de favoritos:** carga la ventana donde podemos buscar los favoritos que hayan sido creados. Tenemos la posibilidad de organizarlos en carpetas para facilitar su recuperación.
- 2 **Atrás y Adelante:** para retornar a la página anterior que habíamos visitado y luego regresar a la actual. Si hacemos clic sobre la flecha, veremos el historial de las páginas visitadas en esa pestaña.
- 3 **Título de la página y nombre de la aplicación.**
- 4 **Barra de direcciones:** allí tecleamos la dirección del sitio web que queremos visitar.

GUÍA VISUAL /1 (cont.)

- 5 **Actualizar:** este botón carga de nuevo la página y actualiza su contenido.
- 6 **Detener:** este botón detiene la carga de la página.
- 7 **Búsqueda:** esta caja de texto nos permite realizar búsquedas sin necesidad de cargar la página de un navegador. Podemos cambiar la selección del buscador que se utiliza. De manera predefinida, se muestra el nombre del buscador que tenemos configurado.
Al escribir el término por buscar y presionar **Enter**, veremos el resultado en la pestaña actual. Si oprimimos **ALT+ENTER**, el resultado aparecerá en una nueva pestaña. El icono de la lupa sirve para ejecutar la búsqueda si hacemos un clic sobre él. La flecha nos permite seleccionar otro buscador como Yahoo o eBay, entre otros ejemplos.
- 8 **Otras opciones del menú:** en este caso, la ayuda solamente.
- 9 **Herramientas:** el menú para acceder a las opciones de la aplicación.
- 10 **Página:** nos muestra las opciones de la página.
- 11 **Imprimir:** a su lado aparece una flecha que nos permite acceder a las opciones de impresión.
- 12 **Sindicación de noticias:** nos podemos suscribir a un feed de noticias.
- 13 **Página principal:** es la página que se carga cuando abrimos la aplicación. Tenemos la posibilidad de definirla desde las opciones y puede ser un grupo de páginas o una página en blanco.
- 14 **Pestañas:** Internet Explorer 7 fue la versión que introdujo la navegación por pestañas. En vez de tener una nueva ventana por cada página web que visitamos, las va cargando en la misma ventana del navegador, pero en una pestaña diferente.
- 15 **Pestañas rápidas:** nos muestra un resumen de las pestañas abiertas.
- 16 **Agregar a Favoritos:** podemos agregar la página actual a los favoritos, en una carpeta actual o crear una nueva. También podemos realizar una entrada en los favoritos, que contenga todas las pestañas abiertas en ese momento.
- 17 **Barra de estado:** a la izquierda, vemos el enlace que se está cargando en ese momento. Luego, vemos la zona de seguridad que estamos utilizando. A su lado, el estado del **Modo protegido** y, a la derecha, podemos modificar el nivel de zoom con el que estamos visualizando la página activa.

De manera predeterminada, Windows Vista incluye la versión 7 de Internet Explorer, que incorpora mejoras significativas con respecto a las anteriores. Entre ellas, el uso de pestañas (**Figura 13**), un lector de noticias (RSS) y la posibilidad de aumentar o reducir el tamaño de la página que visualizamos (**CTRL++** para aumentarlo y **CTRL+-** para reducirlo).

En cuanto a la seguridad, esta versión incluye un **filtro de suplantación de identidad** (*phishing*), que nos protegerá de delincuentes informáticos.

La última versión de Internet Explorer es la 8, la cual incorpora un grupo de mejoras entre las que cabe citar la facilidad de uso, la seguridad y un cumplimiento

más estricto de los estándares web. También mejora el soporte de las **hojas de estilo (CSS)**, la sindicación de noticias (RSS) y las páginas dinámicas (**AJAX**). Por ahora, solo se encuentra disponible la versión de prueba que podemos descargar del sitio de Microsoft (**www.microsoft.com**), pero por el momento está disponible únicamente en inglés.

La última versión de Internet Explorer es la 8, la cual incorpora un grupo de mejoras



FIGURA 13.
Las pestañas rápidas nos permiten obtener una visión general de todas las páginas que tenemos abiertas en ese momento en el navegador.



RSS

RSS representa un grupo de protocolo de **sindicación de noticias** y tiene varias interpretaciones. Una de ellas es *Really Simple Syndication* o sindicación realmente simple. Lo emplean los sitios web de noticias y les permite crear un archivo resumen que se llama **feeds**.

Configurar Internet Explorer

Internet Explorer es una aplicación muy completa y, como tal, trae un gran número de funcionalidades que pueden ser configuradas acorde con nuestras necesidades. Gran parte de ellas se encuentra en el apartado de seguridad que veremos en el próximo capítulo, pero aquí nos ocuparemos de las más generales.

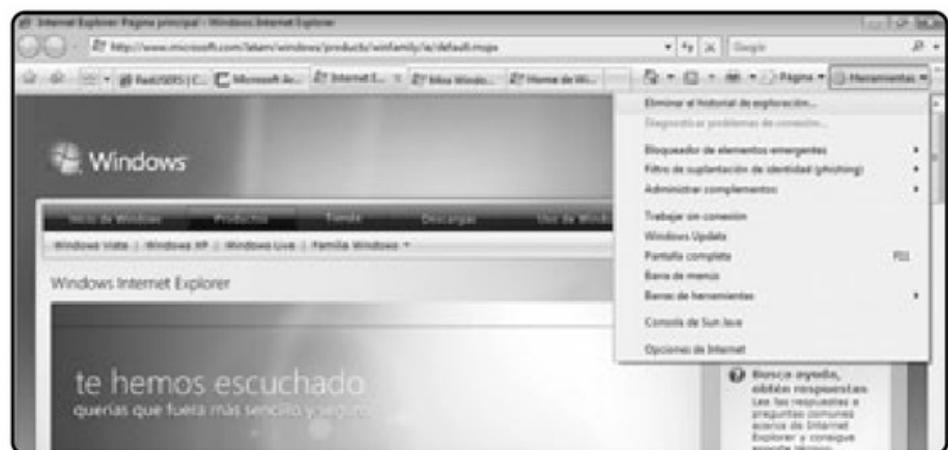
Como Internet Explorer forma parte del sistema operativo Windows, ambos comparten la configuración. Cuando estamos trabajando con IE, encontramos numerosas opciones directamente en el menú **Herramientas** (Figura 14), desde donde podemos configurar muchos parámetros a través de la entrada del menú **Opciones de Internet**. Esta ventana también podemos accederla a través del **Panel de control** en la opción de **Redes e Internet**.



Una de las primeras configuraciones que podemos realizar en nuestro navegador es definir qué página se va a cargar cada vez que abramos la aplicación (puede ser una página en blanco). Esto lo hacemos en la pestaña **General** de las **Opciones de Internet**, que podemos observar en la **Figura 15**.

En la medida en que navegemos, apreciaremos la inmensidad de la Web y notaremos que es demasiado

FIGURA 14.
El menú Herramientas es la vía para acceder a las opciones de configuración de IE.



REGULACIÓN DE INTERNET

Una de las preguntas más comunes de muchos usuarios es ¿quién gobierna Internet? No existe una entidad única que la regule, sino que hay un grupo de entidades que controlan determinados aspectos de su funcionamiento.



FIGURA 15. Podemos seleccionar una página específica para que cargue siempre que abrimos Internet Explorer.

fácil olvidar un sitio que encontramos la semana pasada. Por eso, Internet Explorer pone a nuestra disposición una herramienta para organizar nuestra navegación: el **Centro de favoritos (Figura 16)**,



FIGURA 16. El Centro de favoritos nos permite mantener un registro organizado y de fácil acceso a nuestros sitios web de interés.

al que podemos acceder con un clic en la estrella que aparece a la izquierda del nombre del menú o a través de la combinación de teclas **ALT+C**. El icono de la estrella con el signo + nos permite **Agregar a favoritos** la página que estamos visitando, **Importar y exportar** el listado que tenemos creado, así como **Organizar favoritos**, donde nos carga una ventana en la que podemos crear nuevas carpetas para clasificar nuestros enlaces preferidos.

Muchos sitios web obtienen ingresos a partir de la publicidad de sus páginas. No conformes con los avisos que nos presentan en ellas, algunos también crean ventanas que se cargan automáticamente. En la mayoría de los casos resultan muy molestas y, por esta razón, IE 7 incorpora la opción de evitarlas a través del **Bloqueador de elementos emergentes**, al que accedemos desde el menú **Herramientas**. Otra opción disponible de configuración es la de **Administrar complementos**, que son pequeñas aplicaciones que le proporcionan funcionalidad extra al navegador, ya sea visores para formatos de archivo específicos, como nuevas formas de utilizarlo o de aprovechar la Web (Figura 17).

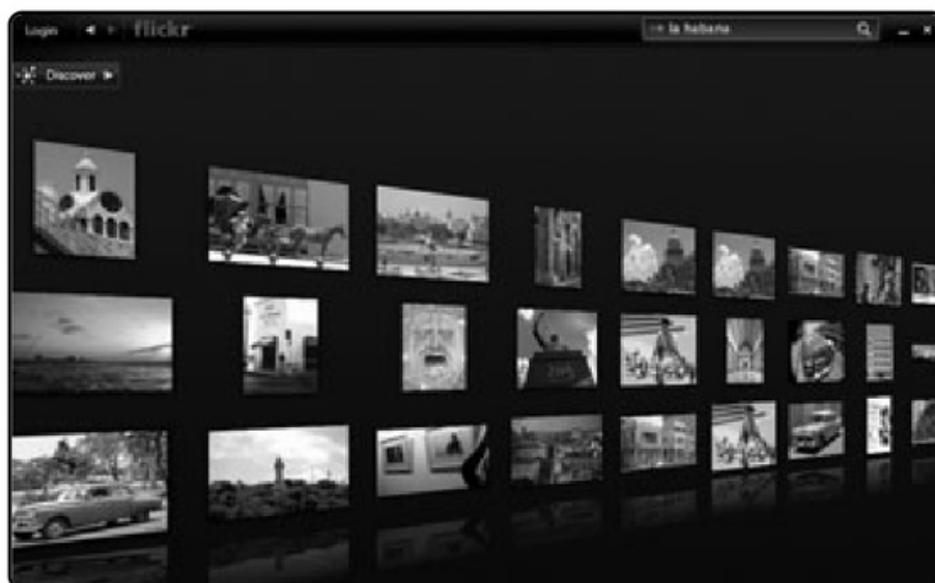


FIGURA 17.
Complementos como Cooliris están cambiando la forma en la que utilizamos la Web.

OTROS NAVEGADORES

El primer navegador popular fue **Netscape Navigator**. Con el crecimiento de Internet, Microsoft se dio cuenta de la importancia de los navegadores y creó Internet Explorer, al que incluyó en su sistema operativo Windows. Esto provocó la llamada **guerra de los navegadores**, de la cual resultó ganador IE ya que, gracias al apoyo destinado por Microsoft, llegó a convertirse en una aplicación con similares características a la de su competidor.



Actualmente, existen tres navegadores que representan una alternativa seria a IE. Uno de ellos es **Opera** (www.opera.com), que se caracterizó siempre por consumir menos recursos de la PC que el resto, al tiempo que popularizó un sinnúmero de funcionalidades que luego los demás imitaron, como por ejemplo, la **navegación basada en pestañas**.

En sus inicios, era una aplicación paga, pero después pasó a un modelo donde había una versión gratis con un espacio para anuncios. En la actualidad es un producto gratuito.

Muchos sitios web obtienen ingresos a partir de la publicidad de sus páginas



FIGURA 18.
Mozilla Thunderbird
 es una excelente
 alternativa para el cliente
 de correo de Windows.

Firefox (www.mozilla-europe.org/es) se ha convertido en el segundo navegador más utilizado en el mundo (detrás de IE), con una cuota de mercado que algunos reconocen del 20% (IE llegó a tener más del 90%). Surgió basado en Netscape Navigator y, al igual que Opera, también es un producto gratuito. Su última versión, Firefox 3, es un excelente programa, y su aparición se convirtió en un récord **Guinness** (el software más descargado en 24 horas) ya que más de 8 millones de personas decidieron instalarlo. Reduce considerablemente el consumo de recursos con respecto a sus versiones anteriores, incorpora las últimas tecnologías web y se encuentra

disponible para todos los sistemas operativos más empleados en la actualidad (**Figura 18**).

Safari (www.apple.com/es/safari) es el navegador que se incluye con el sistema operativo Mac OS X, pero que desde 2007 se encuentra disponible para Windows Vista. Su uso se incrementó con la popularidad de dispositivos como el iPhone, también producido por Apple. Es un navegador más fiel que el resto, a la hora de representar en pantalla las páginas web de acuerdo con cómo fueron diseñadas, lo cual no es de asombrar si tenemos en cuenta la orientación hacia el diseño que siempre ha tenido Apple (**Figura 19**).



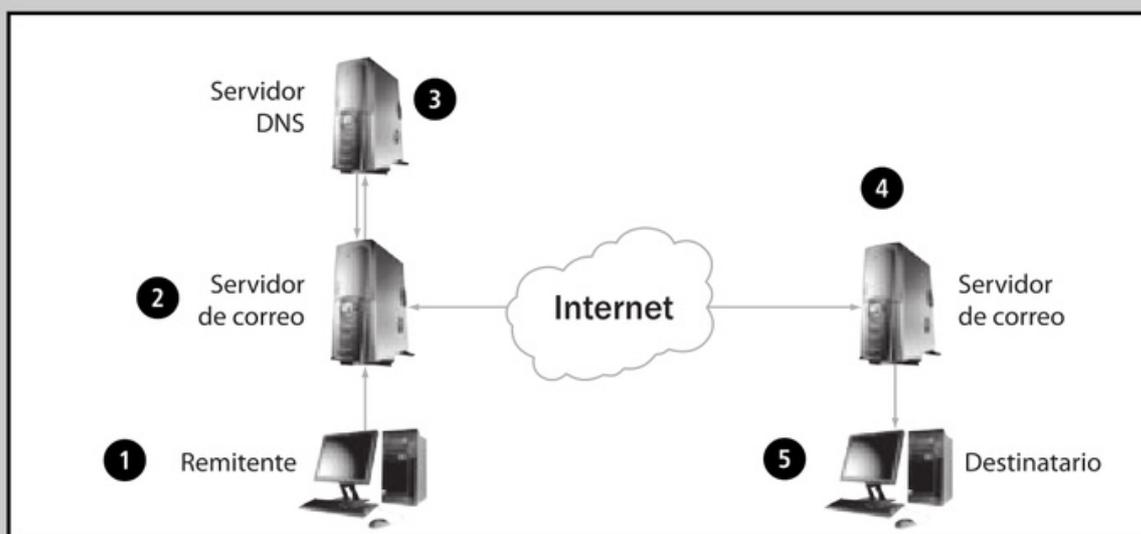
FIGURA 19.
Apple promueve Safari
 como el navegador
 más rápido de todos.

EL CORREO ELECTRÓNICO

El correo electrónico funciona de manera muy similar al correo tradicional. Los mensajes de este tipo van a tener uno o varios destinatarios, un asunto y un cuerpo de mensaje. Adicionalmente, podemos adjuntar archivos en el correo electrónico. En la **Guía Visual 2**, podemos observar su funcionamiento.



GUÍA VISUAL /2 Funcionamiento del correo electrónico



- 1** El remitente redacta el correo y lo envía a su servidor.
- 2** El servidor recibe el correo y chequea el remitente. Si pertenece al mismo servidor, lo entregará directamente en el buzón del usuario; si va dirigido a un usuario de otro servidor, le consultará a su servidor de DNS cuál es el servidor de correo para el dominio del remitente.
- 3** El servidor de DNS localiza cuál es el servidor remoto de correo y le devuelve esta información.
- 4** El servidor de correo contacta al servidor de correo remoto y le entrega el correo electrónico. Este correo se almacena en el buzón del usuario destinatario.
- 5** El usuario destinatario se conecta al servidor y descarga los correos que tiene en su buzón.

El correo electrónico funciona de manera muy similar al correo tradicional

Como todo servicio que funciona sobre Internet, el correo electrónico utiliza protocolos y funciona sobre TCP/IP. Uno de los protocolos que nos interesa en el caso del correo es el **SMTP** (*Simple Mail Transport Protocol* o **protocolo de transferencia simple de correo**), que se emplea para enviar correos.

Cada vez que enviamos un e-mail, se hace con este protocolo, sin importar si es de un cliente a un servidor o de un servidor a un cliente. Los e-mails se envían a direcciones de correo electrónico, cuyo formato es sencillo, por ejemplo: **maximo.gomez@redusers.com**.

Una dirección de correo electrónico se compone de dos partes separadas por el signo **arroba** (@). La primera (a la izquierda de la arroba) es el **nombre del buzón**, y la segunda es el **dominio** del destinatario.

Cada dominio tiene un servidor (o grupo de ellos) encargados de recibir los mensajes. Si el usuario no existe o la dirección es incorrecta, el servidor enviará un mensaje de error para notificarnos de esta situación. Cada servidor de correo tiene declarado el dominio que va a recibir y solo acepta los mensajes que vayan dirigidos a él. Se utiliza el **DNS** para identificar qué servidores son los que reciben la mensajería para cada dominio. Cuando el servidor recibe un mensaje para su dominio, revisa el nombre al que va dirigido y lo deposita en el buzón que corresponde.

WINDOWS MAIL

Es el cliente de correo incluido en Windows Vista (**Figura 20**), sucesor de **Outlook Express**. En la parte de la interfaz de la aplicación existen pocos cambios, la mayoría de ellos fue realizada en su funcionamiento interno.

Por ejemplo, **Windows Mail** almacena los mensajes en archivos individuales, mientras que Outlook Express los guarda dentro de un fichero único. Esto traía problemas cuando el contenido de los buzones comenzaba a crecer con el paso del tiempo.



FIGURA 20.
Windows Mail
incorpora una nueva
Barra de herramientas
a tono con la estética
de Windows Vista.

Otro cambio es que ahora todas las carpetas y correos asociados a una cuenta se almacenan en una misma carpeta del disco duro, donde también se encuentran los datos de configuración de ésta. Esto simplifica la tarea de copiar una cuenta a otra PC, ya que todo se reduce a copiar una carpeta.

OTROS CLIENTES DE CORREO PARA UTILIZAR

Windows Mail tiene la ventaja de que, cuando compramos una PC con Windows Vista, ya se encuentra disponible, pero las opciones que nos brinda son limitadas. Afortunadamente, tenemos a nuestra disposición un grupo de variantes.

Una alternativa a Windows Mail, también desarrollada por Microsoft, es **Windows Live Mail**, que podemos descargar sin costo desde su página web: <http://get.live.com/wlmail/overview>. Este cliente de correo fue desarrollado por el mismo equipo que hizo Windows Mail y es una aplicación que descargamos y ejecutamos en nuestra PC y que nada tiene que ver con el actual **Windows Live Home**, un servicio de webmail.

Expande a Windows Mail con nuevas funcionalidades, entre las que podemos destacar el soporte para cuentas de webmail y el mismo Windows Live Home, **Gmail** y **Yahoo! Mail**. También puede funcionar como un cliente RSS, tiene sincronización con **Windows Live Contacts** y nos permite almacenar las cuentas POP3 en carpetas separadas.



Windows Mail tiene la ventaja de que, cuando compramos una PC con Windows Vista, ya se encuentra disponible



CABLEMÓDEM

Los cabledemods son similares a los módems tradicionales en cuanto a su principio de funcionamiento, pero, en vez de utilizar las líneas telefónicas, se conectan por el mismo cable por donde nos llega el servicio de televisión por cable.

Aquellos que utilizan el paquete de MS Office pueden contar con **Outlook**, una aplicación que, además de ser cliente de correo, permite el trabajo colaborativo, ya que cuenta con calendario, gestor de contactos, tareas y notas.

Otro cliente que merece ser mencionado es **Mozilla Thunderbird**, desarrollado por la misma organización que está detrás de Firefox, pero son dos proyectos completamente separados.

Mozilla Thunderbird se encuentra disponible para distintos sistemas operativos, permite cambiar su apariencia a través del uso de temas y, al igual que los navegadores, es posible utilizar complementos que le incorporan nuevas funcionalidades (**Figura 21**).

Un párrafo especial merecen los webmails actuales. El desarrollo de las tecnologías web ha permitido crear

páginas que funcionan de manera similar a una aplicación que ejecutamos en nuestra PC. Ejemplos de estas interfaces son los webmails que ofrecen Windows Live Home (<http://home.live.com/>), Yahoo! Mail (www.yahoo.com) y Gmail (www.gmail.com). Cada día somos más los que decidimos no utilizar un cliente de correo a favor de un webmail. Esto tiene la ventaja de que, con un solo navegador web, podemos trabajar con nuestro correo desde cualquier PC en la que nos encontremos.

CHATEAR CON AMIGOS

El término **chatear** es un anglicismo que proviene de la palabra *chat*, que en español sería **conversación**, y se aplica a las conversaciones que se establecen a través de Internet en modo texto. Aunque la palabra no está reconocida por la Real Academia de la Lengua Española, la propia entidad acepta su uso en el habla cotidiana.



FIGURA 21.
Mozilla Thunderbird incluye un asistente para configurar las cuentas de correo de Gmail.

El primer servicio que permitió chatear fue el ya mencionado **IRC**, que era proporcionado por servidores a los cuales los usuarios se conectaban con aplicaciones llamadas **clientes IRC**. En cada servidor, existían distintas salas de chat divididas por temas. Todavía son bastante utilizados los servidores IRC como forma de intercambio entre usuarios afines a un mismo tema.

Allá por el lejano 1996 (parece una eternidad en el mundo de la informática), una empresa israelí llamada **Mirabilis** desarrolló un servicio de mensajería que difería de IRC, ya que permitía que cada usuario se conectara con una cuenta. El programa permitía agregar a otros usuarios y conocer si estaban conectados o desconectados. Y, lo más importante, permitía enviar mensajes a los contactos que, a diferencia de los que se envían por correo electrónico, llegaban al instante.

No era necesario ingresar en un salón de charlas, sino que permitía comunicarnos solo con nuestros amigos, conocer su estado en línea y conversar con ellos mediante mensajes de texto. Esto se conoce como **mensajería instantánea**, y el servicio era el famoso **ICQ**, que hoy en día ha sido reemplazado por otros similares como **Yahoo! messenger** que pertenece a Yahoo! (<http://messenger.yahoo.com>),



FIGURA 22. Windows Live Messenger es uno de los clientes más empleados para la mensajería instantánea.



DIFERENCIA ENTRE HARDWARE Y SOFTWARE

Un sistema de cómputo requiere un circuito electrónico y una lógica de procesamiento. En un inicio, todo se hacía con componentes físicos y mecánicos. Actualmente hay una separación entre la parte física y la lógica que dio lugar a los conceptos de hardware y software.

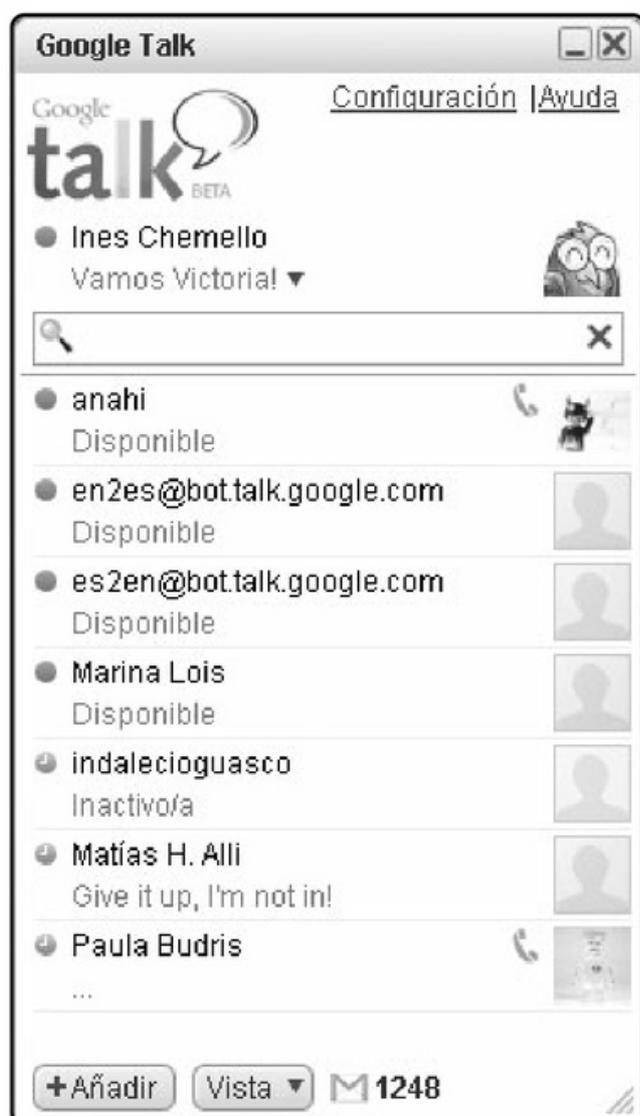


FIGURA 23. Gtalk es un programa integrado a Gmail de modo que solo funciona entre usuarios que tengan este correo electrónico.

Windows Live Messenger (antiguo **MSN Messenger**) de Microsoft (<http://messenger.live.com>) (Figura 22) y el más reciente **Google Talk** o Gtalk de Google (<http://google.com/talk/>). Todos estos servicios son gratuitos, por lo que solo necesitamos registrarnos en el sitio web y descargar el cliente —en algunos casos como Gtalk (Figura 23) o Yahoo! Messenger, el webmail incorpora el acceso a la mensajería instantánea—.

Aunque cada proveedor ofrece un cliente para utilizar su servicio, también existen aplicaciones que no dependen de un servicio. Algunos, como **Pidgin IM** (www.pidgin.im), nos permiten conectarnos con varias cuentas de distintos proveedores a la vez.



RESUMEN

En este capítulo, conocimos todo sobre Internet: los navegadores y sus diferentes características. También aprendimos sobre el correo electrónico: Windows Mail y otras opciones disponibles. Además, estudiamos el concepto de chat con sus alternativas.

Multiple choice

► **1** ¿Cuál de las siguientes no es un tipo de conexión de banda ancha?

- a- PPPoE.
 - b- ADSL.
 - c- Cablemódem.
 - d- Acceso telefónico.
-

► **2** ¿Cuál dispositivo nos permite compartir la conexión de Internet de la casa y oficina?

- a- Hub.
 - b- Switch.
 - c- Módem.
 - d- Router.
-

► **3** La última versión del navegador Internet Explorer es la:

- a- 6
 - b- 7
 - c- 8
 - d- 9
-

► **4** El más importante de los navegadores alternativos es:

- a- Apple Safari.
 - b- Google Chrome.
 - c- Opera.
 - d- Mozilla FireFox.
-

► **5** ¿Cuál de los siguientes no es un protocolo de correo electrónico?

- a- SMTP
 - b- POP3
 - c- IMAP
 - d- TCP/IP
-

► **6** ¿Qué aplicación permite la conexión con varias cuentas de distintos proveedores a la vez?

- a- Pidgin IM.
 - b- Windows Live Messenger.
 - c- ICQ.
 - d- ICQ.
-

Respuestas: 1-a, 2-d, 3-c, 4-d, 5-d, 6-a.

Capítulo 7

Seguridad



En este capítulo, aprenderemos a instalar un antivirus, mantener Windows actualizado y realizar backups.

Seguridad

El tema de la seguridad se ha convertido, hoy por hoy, en uno de los más importantes. Del modelo de una PC aislada sobre nuestro escritorio hemos pasado al de las computadoras conectas en redes globales.

En el pasado, Microsoft ha sido fuertemente criticado en este aspecto. De hecho, se realizaron estudios que dieron como resultado que, si conectábamos a Internet una PC solo con la instalación fresca de Windows XP, en apenas veinte minutos iba a ser atacada y comprometida. Por supuesto, esta situación fue corregida con la publicación de **Windows XP Service Pack 2**, que incluía un **Firewall**. Para su próximo sistema operativo, Microsoft ya había aprendido la lección, y Windows Vista presenta un impresionante listado de nuevas características en el aspecto de la seguridad. Algunas saltan a la vista, como es el caso del **Control de cuentas de usuario**, pero otras no son tan evidentes, como por ejemplo, el **Endurecimiento de Servicios de Windows**, que evita accesos no autorizados de aplicaciones, tanto a partes internas del sistema operativo como a través de la red a otros equipos.

El área de **Seguridad** del **Panel de Control** es el lugar donde Windows Vista concentra las opciones



del sistema relacionadas con este tema (**Figura 1**). Según la versión de Windows Vista que tengamos instalada, algunas opciones podrían no aparecer.

MANTENER WINDOWS ACTUALIZADO

Las aplicaciones —el sistema operativo puede ser considerado una de ellas— siempre han tenido errores. Unos son evidentes, otros tardan tiempo en ser detectados y algunos nunca salen a la luz. Por esta razón, los fabricantes de software publican **actualizaciones** para sus productos donde corrigen estos errores.

Inicialmente, los errores en las aplicaciones estaban relacionados con su operación y funcionamiento. Cada PC era de uso personal y un equipo aislado, solo lo utilizábamos nosotros, por lo que únicamente nos preocupaban los errores que surgían al realizar

FIREWALL

De nada sirve tener un firewall perfectamente configurado y seguro si instalamos un programa que tiene problemas de seguridad y permite que se comprometa el servidor. Hoy en día, toda red conectada a Internet debe contar con la protección de un firewall.



FIGURA 1.
El Panel de Control cuenta con una sección dedicada a Seguridad.

alguna operación específica. Cuando empezaron a utilizar la PC varios usuarios, comenzaron a aparecer una nueva gama de problemas, ya que la mala operación de un usuario podía afectar al resto.

El peligro se incrementa cuando conectamos nuestro equipo en red, ya que no hace falta tener acceso físico a nuestra PC para poder intentar acceder a ella. Un error ya no representa más una función que no podemos utilizar, sino la oportunidad para

un extraño de tener acceso a nuestros documentos. Por esta razón, los fabricantes de software monitorean, en forma constante, las nuevas fallas que surgen y publican actualizaciones en el menor tiempo posible para corregirlas (**Figura 2**).

En el caso de la seguridad, las actualizaciones se publican de inmediato, y Windows Vista cuenta con un mecanismo que nos posibilita acceder a ellas. La opción **Windows Update** del **Centro de seguridad**

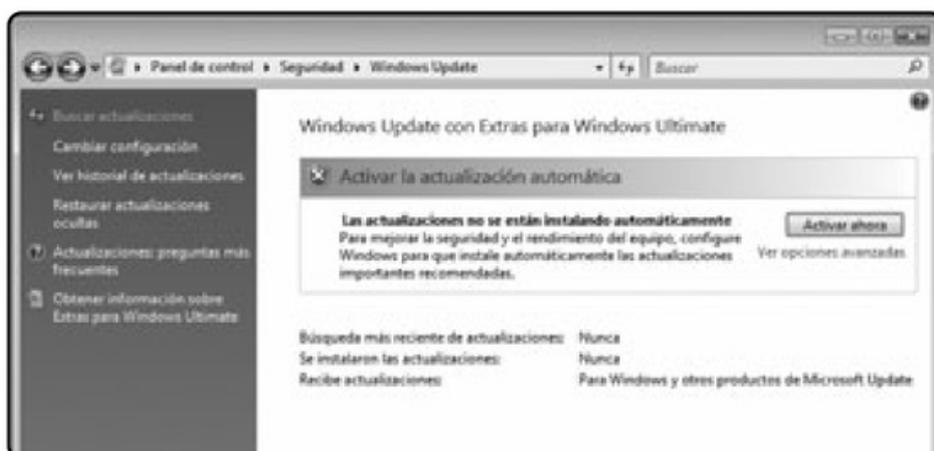


FIGURA 2.
Debemos evitar a toda costa que nuestro equipo tenga acceso a Internet si no instalamos antes las actualizaciones.

nos permite automatizar este proceso, que podemos configurar al hacer clic en **Ver opciones avanzadas**. En la nueva ventana (**Figura 3**) vamos a tener varias opciones: la primera es **Instalar actualizaciones automáticamente (recomendado)**, que solo debemos activar en aquellos equipos con acceso a Internet, ya que Windows Vista se conectará al sitio web de Microsoft para comprobar si existe alguna actualización disponible y, de ser así, la descargará a nuestra PC. También podemos definir el horario en que se realizará este chequeo y descargar las actualizaciones.

Debemos recordar que una actualización es un archivo que se descarga por Internet, con lo cual el acceso a la Web se ralentizará durante este período de tiempo. Al definir el horario, podemos asegurarnos de que Internet no comience a estar lenta justo cuando más apurados estamos navegando por la Web.

En ocasiones, podemos tener una razón para no instalar alguna aplicación. Ya sea porque es para un programa que no utilizamos o porque entra en conflicto con otro que ya tenemos instalado y pertenece a otro fabricante. Para esas situaciones podemos

seleccionar **Descargar actualizaciones, pero permitirme elegir si deseo instalarlas**. Cuando utilizamos el acceso telefónico, la velocidad es mucho menor que con las conexiones de banda ancha; por eso, no basta con decidir cuándo instalar la actualización, sino que es importante controlar en qué momento se descargará a nuestra PC. En esas circunstancias, es conveniente seleccionar **Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas**.

La última alternativa que tenemos es **No buscar actualizaciones (no recomendado)** que solo debemos utilizar en casos específicos que lo justifiquen, como en una PC aislada que nunca va a conectarse a la red. Aun en esa situación, deberíamos buscar otros medios para lograr que la PC pueda ser actualizada ya que, incluso cuando la seguridad no fuera una prioridad, habrá mejoras que afecten el rendimiento y el funcionamiento del sistema.

EL FIREWALL

Empecemos por hablar de arquitectura. Todos conocemos el peligro que representan los incendios, y por



En el caso de la seguridad, las actualizaciones se publican de inmediato, y Windows Vista cuenta con un mecanismo que nos posibilita acceder a ellas

eso los arquitectos incorporan soluciones en sus planos para minimizar los daños en caso de que ocurra un accidente de este tipo.

Entre las múltiples soluciones que existen, se encuentra la instalación de paredes que utilizan materiales especiales, no combustibles, en determinadas áreas de la construcción. Estas paredes se ubican de manera tal que sean capaces de detener el avance de las llamas ante un incendio en la casa o el edificio. Reciben el nombre de **cortafuegos** y, en inglés, se denominan **firewalls**.

Cuando la seguridad comenzó a ser tenida en cuenta en el mundo informático, una de las primeras soluciones fue, precisamente, utilizar el mismo concepto que los arquitectos. Las primeras redes eran locales, todos los equipos eran conocidos, pero con el tiempo las redes empezaron a conectarse entre sí, y ya no se tenía control sobre los equipos externos.

Por eso, los especialistas en temas de seguridad decidieron aplicar firewalls (pese a que es un anglicismo, se acepta el uso de la palabra en inglés). Cuando se iba a conectar una red interna a otra red

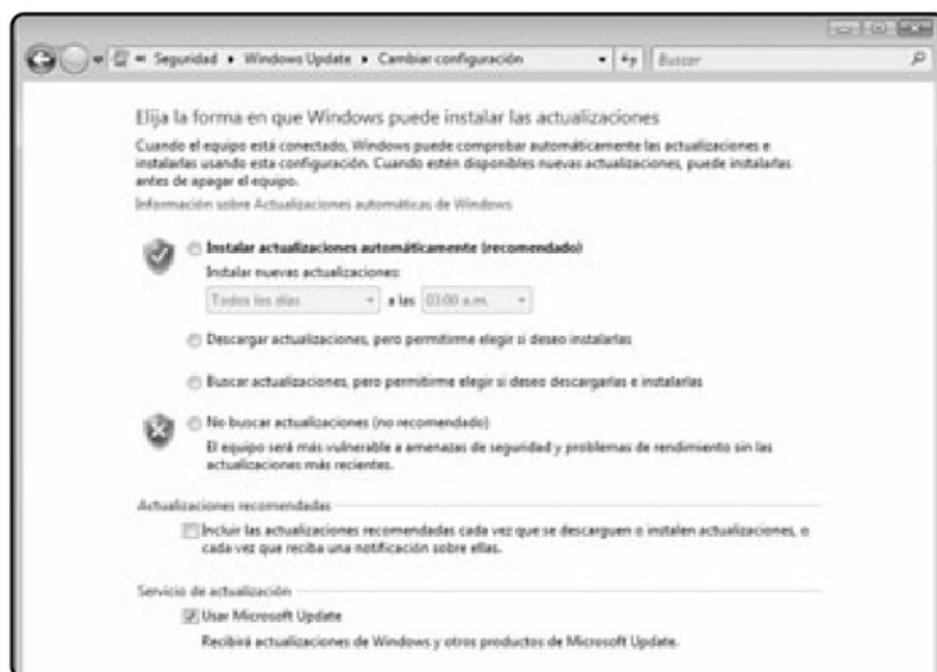


FIGURA 3.
Desde esta ventana, tendremos control total sobre la forma en que vamos a actualizar nuestro sistema.



CONVERTIR UN SERVIDOR EN UN FIREWALL

En el mercado, encontramos vendedores de software que ofrecen aplicaciones para convertir un servidor en un firewall, y existen sistemas operativos que incluyen todas las herramientas necesarias para ser configurados como firewalls.

o a otras redes, se hacía a través de un equipo que tenía la función de separar las dos redes y permitir únicamente el tráfico autorizado entre ellas.

La función básica de un firewall es **controlar el tráfico** que fluye a través de él. Además, los firewalls permiten **declarar reglas** para decidir qué tráfico puede pasar y cuál no. Como estamos hablando de redes conectadas a Internet, nos referimos al protocolo TCP/IP (**Figura 4**).

El protocolo TCP/IP utiliza el binomio de dirección IP y puerto para establecer las conexiones. Cuando visitamos un sitio web en Internet, nuestro navegador se conecta a la dirección IP de ese servidor y accede al puerto 80 (donde responde el servidor web). En ese momento, se establece una conexión entre dos puntos: nuestra PC en un extremo y el servidor web en el otro.

Como nosotros iniciamos la conexión, de nuestro lado el tráfico es **saliente**, mientras que para el servidor es **entrante**. El detalle para tener en cuenta aquí es esta clasificación: entrante y saliente. Esta diferencia es importante porque, cuando configuremos un



firewall en nuestro hogar para conectarnos a Internet, una de las primeras medidas por tomar va a ser, por lo general, **bloquear** todas las conexiones entrantes. A menos que tengamos un servidor en nuestra red al que nos deseemos conectar desde Internet, ésta será la primera resolución que implementaremos.

Por supuesto, toda regla tiene su excepción, y hay programas que necesitan conexiones desde Internet. Por eso, los firewalls nos permiten configurar los permisos que se van a aceptar y los que no. Estas definiciones, también llamadas reglas o **Excepciones**, van a posibilitar que el equipo identifique y permita el tráfico autorizado y deniegue el resto (**Figura 5**).

FIGURA 4.

Las empresas utilizan, con frecuencia, equipos contruidos y configurados para actuar como firewalls dedicados.





FIGURA 5.
Podemos convertir una vieja PC en un firewall dedicado con distribuciones como pfSense.

LAS COOKIES

Resulta curioso cómo algunas palabras resisten la traducción al español y se utilizan directamente en su versión original, en este caso tomándola del inglés.

Con esta palabra, diríamos que es justificado, uno puede tomar en serio algo como las **cookies**, pero ya si hablamos de "galletitas" (la traducción literal de cookie) cuesta más lograr que nos presten atención. Una **cookie** es un pedazo de información en la forma de un archivo de texto y, para entender de qué son, debemos remontarnos a sus orígenes.

Una cookie es un pedazo de información en la forma de un archivo de texto

La navegación web utiliza un protocolo llamado **HTTP** (*HyperText Transfer Protocol* o protocolo de transferencia de hipertextos) para establecer las conexiones entre los clientes y el servidor.



DESBLOQUEAR APLICACIÓN EN EL FIREWALL

Al desbloquear una aplicación en el firewall, le estamos dando permisos para establecer cualquier conexión que programe, por lo que si no confiamos en la aplicación, pero conocemos los puertos que utiliza, es mejor seleccionar la opción **Agregar puerto**.



FIGURA 6.
Los carritos de compra
fueron posibles
en un inicio gracias
a las cookies.

Cuando tecleamos la dirección de una página web, esta solicitud se dirige hasta el servidor web, que nos devuelve la página en cuestión.

Es un proceso de dos etapas: solicitamos algo al servidor y éste, a su vez, nos devuelve algo. Al mismo tiempo, podría haber otro usuario que estuviera llevando a cabo igual proceso. En lo que respecta al servidor, podría ser el mismo cliente, o dos distintos. La función del servidor se limita a recibir solicitudes y responderlas (**Figura 6**).

¿Qué pasa cuando queremos que exista relación entre la página anterior y la siguiente? Por ejemplo, cuando visitamos un sitio web que vende productos por Internet, se suele utilizar el llamado **carrito de compras**. Podemos navegar por el sitio, seleccionar los productos que nos interesan y adicionarlos al carrito. Solo con HTTP esto sería imposible: si en una página seleccionáramos un producto, cuando visitáramos la siguiente, el carrito quedaría vacío porque no tendría forma de saber qué habíamos elegido en la página anterior. ¿Y qué pasa si —el ejemplo anterior— había otra persona que estaba visitando el sitio al mismo tiempo? Los carritos de compra



**Cuando ingresamos
a la primera página,
el servidor nos envía
una cookie**

existen y funcionan, por ende, evidentemente, el problema fue resuelto: la solución fueron las cookies.

Supongamos que accedemos a un sitio que vende libros y revistas por Internet (por ejemplo, www.redusers.com). Cuando ingresamos a la primera página, el servidor nos envía una cookie. Luego, empezamos a navegar por el sitio y encontramos un libro que nos interesa; cuando hacemos clic para adicionarlo al carrito de compras, esta solicitud viaja hacia el servidor, pero esta vez acompañada de la cookie que nos envió el servidor al inicio. Esto se repite cada vez que adicionamos algo al carrito.

Gracias a la cookie, el servidor puede identificar a cada usuario que visita el sitio y conocer qué adicionó cada uno. Así, cuando iniciamos sesión en un servidor web, se nos asigna una cookie que nos identifica ante él para las solicitudes siguientes y nos ahorra tener que estar identificándonos todo el tiempo.

Sin embargo, las cookies han recibido muchas otras aplicaciones. Por ejemplo, también sirven para almacenar nuestras preferencias, el tamaño de las letras que seleccionamos para visualizar el sitio, la cantidad de resultados que deben mostrarse por página cuando hacemos una búsqueda, etcétera.

Por ese motivo, han sido fuente de controversia cuando las empresas de marketing no solo incluían sus publicidades en distintos sitios, sino que en cada uno ponían una cookie. De esta manera, podían llevar un registro de cada usuario que había visitado esos sitios, lo que se considera una invasión a la privacidad (**Figura 7**).

EL FILTRO DE SUPLANTACIÓN DE IDENTIDAD (PHISHING)

Antes de responder a esta pregunta, debemos tener claro a qué se refiere **phishing**. Si bien el término proviene del inglés, la palabra no existe



FIGURA 7.

A pesar de que no las vemos, las cookies están presentes en la conversación entre el servidor y nuestro navegador.

como tal, sino que es una forma modificada de *fishing*, que significa **pescar**, donde se cambia la f por la ph. Cuando salimos de pesca, colocamos carnada en el anzuelo, lo tiramos al agua y esperamos que algún pez pique.

Existen individuos que realizan una actividad similar en Internet con fines ilícitos, que representan una nueva amenaza. ¿Cómo operan? Se hacen pasar por sitios legítimos con el objetivo de obtener información privada. Por ejemplo, puede ser la clave con la que accedemos a un banco en línea, o el número de nuestra tarjeta de crédito.

Una de las formas más comunes de obtener información es mediante el envío de correos electrónicos, redactados de manera muy parecida a los que envía el negocio original. Supongamos que nos llega un correo de nuestro banco donde nos saluda afectuosamente y nos comunica que, por razones de seguridad, se ha implementado un nuevo sistema de acceso vía web que requiere que cambiemos nuestra contraseña por una nueva y más segura en el menor tiempo posible.

Puede ser ésa u otra acción, en cualquier caso, se nos pide que hagamos clic o visitemos alguna página web para ingresar algún dato nuestro.

Una de las formas más comunes de obtener información es mediante el envío de correos electrónicos

Es un hecho comprobado que un correo de este tipo va a ser asumido como real por un gran número de personas, quienes harán lo que se les solicite sin darse cuenta de que todo ha sido una **estafa**. De la misma manera, se utilizan sitios web que son réplicas perfectas del sitio original, con un dominio muy parecido. Ingresamos nuestros datos y podemos operar con nuestra cuenta como de costumbre.



BLOQUEO DE PROGRAMAS

Toda aplicación que intente conectarse a la red cuando el **Firewall de Windows** se encuentre activado sin tener creada una excepción, será bloqueada. La casilla **Notificarme cuando Firewall de Windows bloquee un nuevo programa** deberá estar activada.

En ese momento, el sitio falso capturó nuestros datos, los almacenó, y los utilizó para conectarse al sitio real y permitir que trabajáramos normalmente sin darnos cuenta de lo que acababa de suceder. Este tipo de estafa, donde alguien intenta hacerse pasar por otro, se conoce como **suplantación de la identidad**. Para lograrla, las personas que están detrás envían correos electrónicos, construyen sitios web y luego esperan a ver si algún usuario distraído cae en la trampa. De ahí la semejanza con la pesca, y el nombre.

Internet Explorer incluye una protección contra estas amenazas, el **Filtro de suplantación de identidad (phishing)**, un servicio compuesto por dos partes. La primera, le permite a nuestro navegador comparar cada sitio que visitamos con un grupo de características que suelen compartir estos sitios falsos. La segunda es que Microsoft tiene en línea servidores que se actualizan varias veces en una hora, con cada nuevo sitio falso que se detecta. Cuando visitamos un sitio sobre el cual el navegador tiene dudas respecto de su autenticidad, se consulta este servidor de Microsoft para conocer si está declarado como un sitio conocido de phishing (**Figura 8**).

SPYWARE

El mundo de la publicidad mueve millones de dólares en Internet, y existen empresas que intentan



FIGURA 8. La primera vez que utilizemos Internet Explorer para navegar por Internet, nos preguntará si deseamos activar el Filtro de suplantación de identidad (phishing).

obtener ingresos a cualquier precio. Las cookies les permitían a estas empresas llevar un registro de los sitios que visitaban los usuarios.

Sin embargo, los desarrolladores web encontraron otras variantes para no utilizarlas, y los navegadores empezaron a incluir protección contra el uso ilícito de las cookies. Pero éstas solo funcionaban en los servidores web que incluían publicidades de esas empresas. El usuario que no visitaba esos sitios quedaba



EXCEPCIONES DEL FIREWALL

Por lo general, las aplicaciones que requieren excepciones en el **Firewall de Windows** son aquellas que trabajan en **segundo plano** o son **servicios**, que se ejecutan sin interacción alguna por parte nuestra.

fuera de su alcance. Entonces apareció una variante: en vez de depender de la cookie de un sitio, era más efectivo instalar, no la cookie, sino un programa en la PC del usuario.

De esta manera, se controlaba todo su tráfico, independientemente de los sitios que visitara. Este programa, que se instala sin conocimiento del usuario y que **monitorea** toda su actividad, se llama **spyware**, una palabra que no tiene traducción literal al español, aunque en inglés *spy* significa **espía**.

El spyware agrupa una gama de aplicaciones que comparten el hecho de que su instalación se realiza sin conocimiento del usuario y que su actividad representa un peligro para él. Hay spyware que monitorean nuestra navegación y les reportan dicha información a las empresas que los crearon,

a fin de que puedan mostrarnos aquella publicidad que sea más relevante para nosotros.

También hay programas que directamente se encargan de mostrar la publicidad en la pantalla. Otros spyware envían información personal y privada. Incluso, son capaces de redireccionar los clics que hacemos en los enlaces de las empresas de la competencia hacia sus servidores (**Figura 9**).

WINDOWS DEFENDER

Windows Vista viene con un programa para protegernos del spyware, **Windows Defender**. Está basado en el **GIANT AntiSpyware**, un programa que Microsoft compró a fines de 2004 a la empresa que lo desarrolló, **GIANT Company Software, Inc.** La versión actual tiene muy poco que ver con las características de aquella original.

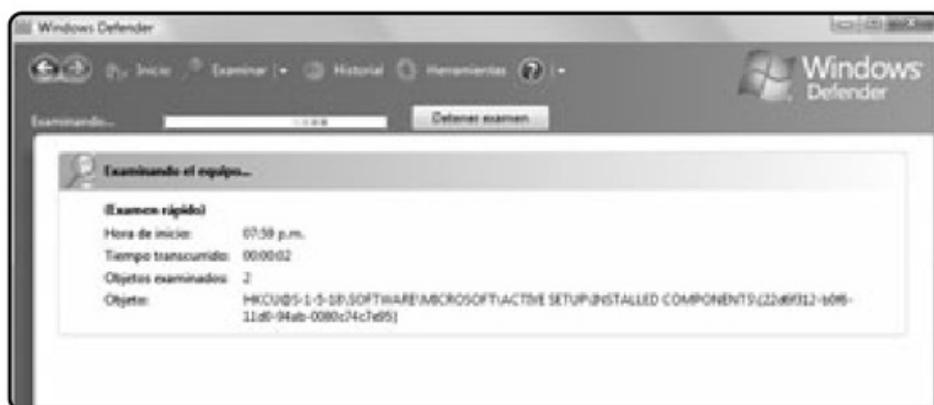


FIGURA 9.
Windows Vista
trae incorporado
un programa antispyware.



POSIBLE SPYWARE

Puede suceder que Windows Defender detecte un archivo como posible spyware pero no lo conozcamos, para nosotros es un archivo más del sistema que puede o no ser algo peligroso. Ante la duda, podemos poner ese archivo en **Cuarentena**.

Los spyware evolucionan constantemente, todo el tiempo buscan nuevas formas de evitar las protecciones que instalamos en las PCs. Los programas **antispyware** deben seguir el mismo ciclo de renovación para no quedarse atrás. Además, existen muchos tipos de spyware, por lo que un buen programa antispyware deberá ser capaz de detectar cualquiera de sus variantes (**Figura 10**).

Windows Defender es una aplicación dividida en dos: una parte funciona en segundo plano, como un servicio del sistema, y la otra es el panel de control al que accedemos a través del **Centro de seguridad de Windows**, con un clic sobre **Windows Defender** en la sección izquierda superior de la ventana. Entre las dos, se encargan de proveer al sistema operativo de tres características básicas. La primera es la detección y eliminación de software spyware que pudiera estar en nuestra PC o cualquier medio de almacenamiento de información que utilicemos para transferir datos.

Windows Defender revisa constantemente cualquier modificación que haya sido configurada

El programa revisa todos los archivos que tengamos almacenados y busca en ellos señales de que puedan ser una aplicación de spyware. Cuando Windows Defender detecte un spyware, nos consultará qué acción tomar: **Omitir**, para ignorar la amenaza por esta vez; **Cuarentena**, para dejarlo en cuarentena; **Eliminar**, para borrarlo; o **Permitir siempre**, para ignorarlo en sucesivos chequeos.

Gracias a la integración de Windows Defender con Internet Explorer y Windows Vista, esta herramienta es capaz de ofrecer protección en tiempo real. Esto quiere decir que, si conectamos una memoria USB



FIGURA 10.
Debemos revisar periódicamente nuestra PC para protegerla de los spyware.

a nuestra PC, Windows Defender detectaría si en ella se encuentra algún spyware que intente infectar la PC. Si estamos navegando por un sitio web que pretende descargar un spyware e instalarlo sin nuestro consentimiento, también será detectado por Windows Defender. Asimismo, es capaz de localizar actividad sospechosa en las aplicaciones.

Por ejemplo, los spyware tratan de modificar la configuración del sistema para que cada vez que encendamos el equipo, se activen; pueden cargarse en todo momento que iniciemos Internet Explorer. Éstos suelen ser indicios de spyware y, por eso, Windows

Defender revisa constantemente cualquier modificación que haya sido configurada, así como los programas que las realizaron (**Figura 11**).

ACERCA DE LOS VIRUS INFORMÁTICOS

Un **virus** informático es un programa que se introduce en nuestra PC y, al ejecutarse, es capaz de destruir toda o parte de la información que tengamos almacenada. El nombre virus proviene de la capacidad de estos programas, que al igual que sus semejantes del mundo de la biología, son capaces de reproducirse sin intervención externa.

FIGURA 11.
Windows Defender mantiene un registro de todas las acciones que realiza, en el Historial.



LA SEGURIDAD EN MICROSOFT

Microsoft ha sido duramente criticado por la inseguridad de Windows. Se dice que otros sistemas operativos como Mac OS X o las distribuciones de Linux son más seguros. A pesar de eso, el producto de Microsoft domina el 80% del mercado.

Los virus informáticos son bastante viejos, existían mucho antes de que apareciera Internet

Los spyware son molestos, nos espían, envían información nuestra a terceros, todo lo cual es muy preocupante. Los virus, en cambio, provocan consecuencias mucho más graves y directas: pueden **formatear** nuestro disco duro. Dada su facilidad de propagación, basta con que una PC sea infectada para que la información se encuentre en peligro.

Los virus informáticos son bastante viejos, existían mucho antes de que apareciera Internet. Como en toda tecnología (hay expertos que se dedican exclusivamente al tema), su tiempo de existencia se ve reflejado en su evolución. En la actualidad, los virus emplean técnicas para propagarse o no ser detectados que son dignas de admiración.

Recordemos que estamos hablando de aplicaciones compuestas por **código de programación**. Los primeros antivirus tenían una base de datos con fragmentos de código de virus conocidos.

Con esta información, revisaban los archivos de la PC en busca de coincidencias de código. Cuando las encontraban, estaban en presencia de un virus. Los creadores de virus se dieron cuenta de esto e idearon virus que eran capaces de **mutar** (el mundo virtual imita al real) e infectaban cada archivo con un nuevo código diferente del anterior (**Figura 12**).

EL ANTIVIRUS

Un virus necesita un medio para transmitirse. Si tomamos en cuenta que un virus informático es una aplicación, un software va a utilizar los mismos



FIGURA 12. El primer gusano (una categoría de virus) que inundó Internet fue escrito por Robert Morris, un estudiante de la Universidad de Cornell, como un ejercicio intelectual.



DETECTAR LA RED

Windows Vista es capaz de detectar la red en la cual se encuentra conectado el equipo, pero nosotros también lo podemos hacer. Para eso, necesitamos conocer la dirección IP y la **máscara de red**, que indica qué parte de la dirección IP identifica a la red.

medios que empleamos para transferir archivos. Un virus puede infectar una memoria USB que, a su vez, infecte los discos de todas las PCs a las que se conecte.

Existen virus que son capaces de transmitirse por la red al aprovechar vulnerabilidades de los sistemas operativos o las aplicaciones que se ejecutan sobre ellos. Por esta razón, para evitar los virus, debemos adoptar una serie de medidas que, en su conjunto, van a protegernos. La primera, por supuesto, sigue siendo instalar un programa **antivirus**.

Windows Vista no trae ninguno, pero, por suerte, contamos con suficientes alternativas al respecto, como veremos en el siguiente apartado (**Figura 13**).

Es buena idea tener siempre el antivirus activado, ya que necesitamos que la protección funcione en **tiempo real**. Los antivirus revisan automáticamente cada memoria USB que conectamos a la PC, cada CD-Rom o DVD-ROM que insertamos. Cuando accedemos por la red a una carpeta remota, cuando seleccionamos un archivo para abrirlo o copiarlo hacia

FIGURA 13.
El Centro de seguridad de Windows realiza chequeos, y nos alerta cuando detecta que no tenemos un antivirus instalado y nos encontramos desprotegidos.



A la hora de seleccionar un producto antivirus, tenemos un amplio grupo de alternativas. Algunos fabricantes de PC incluyen una versión de prueba



nuestra PC, el antivirus se encarga de revisarlo antes de realizar cualquier otra acción.

De todas maneras, debemos recordar que una de las mejores protecciones que tenemos contra los virus son los **respaldos**, también conocidos como **backups**. Hacer una copia de nuestra información periódicamente es un hábito que debemos incorporar para mantener nuestra PC a salvo.

Infectarnos con un virus puede ser solo cuestión de tiempo. Entonces, llegado el caso, se trata de minimizar al máximo los daños. Una copia reciente de la información no es la solución perfecta, pero se acerca a lo que podríamos soñar.

INSTALAR UN ANTIVIRUS EN LA PC

A la hora de seleccionar un producto antivirus tenemos un amplio grupo de alternativas. Algunos fabricantes de PC incluyen una versión de prueba, válida durante un período de tiempo determinado. Al cabo de ese tiempo, podemos decidir si compramos el producto o buscamos otro (**Figura 14**).

En la actualidad, es difícil encontrar un producto que sea solo antivirus, ya que estamos expuestos a muchos tipos de amenazas, y los virus son solo una. Pero tampoco podemos tener un programa antivirus, que se está ejecutando para protegernos, junto a otro antispyware, y la lista podría seguir creciendo (veremos más adelante otros riesgos).

Tantos programas que estuvieran procesándose al mismo tiempo para defender nuestra PC consumirían demasiados recursos y, al final, no podríamos utilizar la computadora para trabajar.

Los fabricantes de estos programas se dieron cuenta y tomaron la decisión de integrar en un solo producto el **paquete de protección** completa. La mayoría de los desarrolladores de antivirus, en la actualidad, ofrecen estos paquetes integradores (**suites**). Uno de los más conocidos es **Symantec Norton** (Norton fue adquirida por Symantec), que nos ofrece productos como **Symantec Norton Internet Security** y **Symantec Norton 360** (el segundo está más orientado al usuario hogareño,

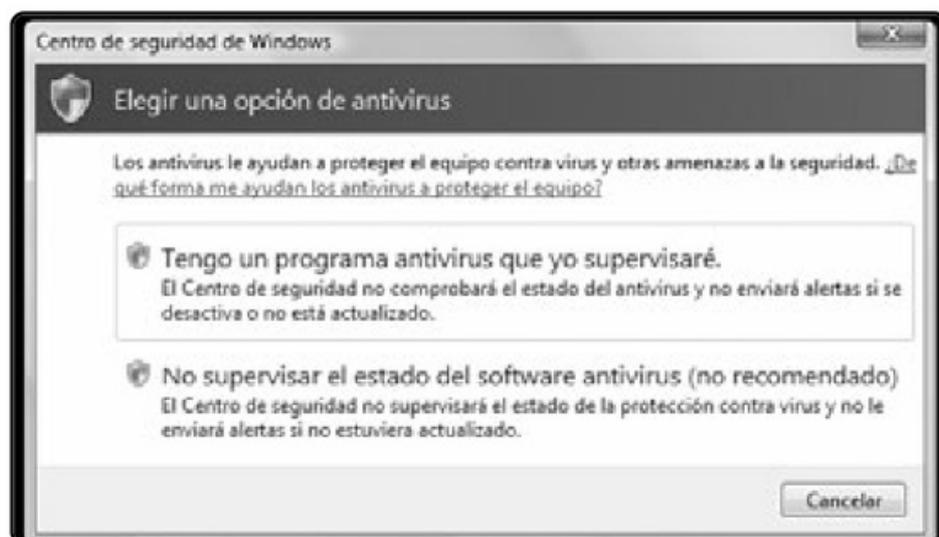


FIGURA 14.
Tenemos la opción de evitar las alertas enviadas por el Centro de seguridad de Windows cuando no tenemos instalado un software antivirus.

al contar con características como optimizar la PC, realizar copias de seguridad, etcétera).

Otras alternativas son **ESET NOD32 3.0 Antivirus System**, **Kaspersky Anti-Virus 2009** y **Panda Antivirus Pro 2009**, entre otros. Cada uno de estos fabricantes brinda varios productos diferenciados por la cantidad de características que integran. El precio refleja esta diferencia y nos permiten pagar por lo que estamos buscando exactamente.

Algunos llegan a ofrecer versiones gratis para uso personal en nuestro hogar. Brindan un nivel de protección similar a las versiones pagas y se diferencian en detalles. Por ejemplo, no tienen soporte técnico, o no integran todas las opciones del producto pago. Para el uso hogareño, sin embargo, la mayoría nos permitirá mantenernos protegidos y postergar el pago para cuando realmente necesitemos las prestaciones que ofrece la versión comercial.



Dentro de las alternativas gratis, los especialistas reconocen como las mejores opciones a: **Avira AntiVir Personal Edition Classic**, **AVG Anti-Virus Free Edition** y **avast! 4 Home Edition**. Decidimos instalar avast! (**Figura 15**), por sus buenas críticas y porque tiene una versión en español (**Paso a paso 1**).

Debemos descargarlo desde www.avast.com/esp/download-avast-home.html y seleccionar la versión en español. El fabricante nos pedirá registrarnos previamente (www.avast.com/eng/home-registration.php) y nos enviará a nuestra dirección de correo electrónico una clave de licencia válida para utilizar el producto durante un año.

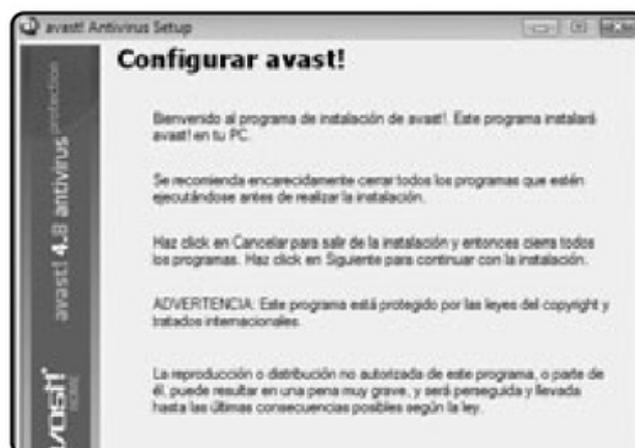


FIGURA 15. Cuando instalamos avast! Antivirus Setup, nos aparecerá una ventana para la configuración de la aplicación.



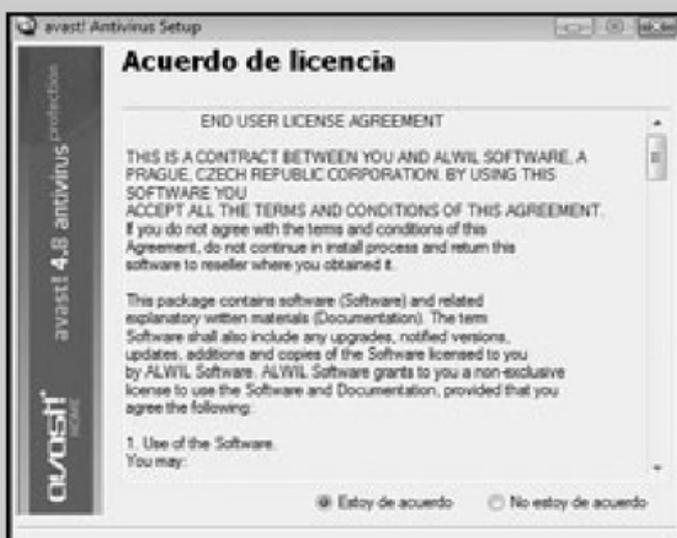
FIREWALL DE WINDOWS VISTA

Con Windows Vista, afortunadamente, tenemos la necesidad de un firewall satisfecha por el mismo sistema operativo ya que el **Firewall de Windows** que viene incorporado es suficiente para proteger nuestro sistema.

PASO A PASO /1

Instalar un antivirus

1



Una vez descargado y ejecutado el archivo, verá el asistente de instalación del programa.

En la pantalla de bienvenida, presione **Siguiente** para avanzar al próximo paso. Después de las notas, verá el **Acuerdo de licencia**. Tilde la casilla **Estoy de acuerdo** para continuar.

2



Acepte el **Destino** para instalar el programa y seleccione el tipo de **Configuración** por utilizar. La **Típica** debe servir en la mayoría de los casos. Puede seleccionar la opción **Personalizada**, si está seguro de que hay alguna función que no va a necesitar y no desea que se instale.

PASO A PASO /1 (cont.)

3



A continuación, el asistente le mostrará la **Información de la instalación** donde tendrá la oportunidad de chequear qué se va a instalar y dónde. Puede hacer clic en el botón **Atrás** para realizar alguna modificación.

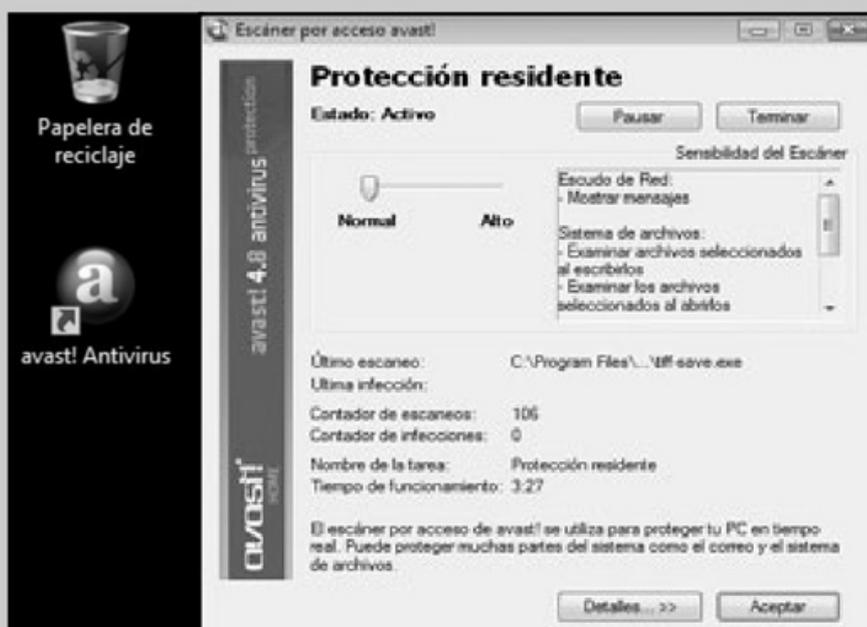
4



Una vez terminada la instalación, el asistente le dará dos opciones: **reiniciar** o **reiniciar más tarde** y advierte que, si no reinicia, algunos componentes no funcionarán correctamente.

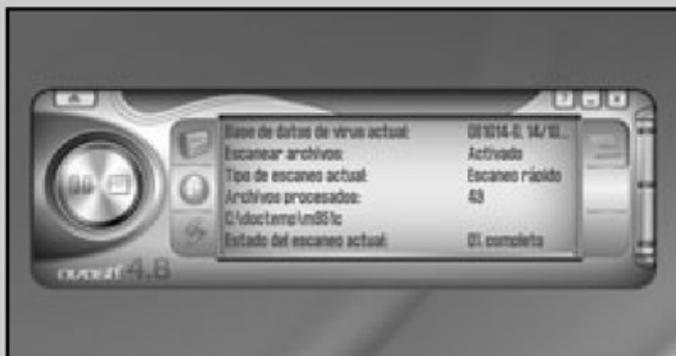
PASO A PASO /1 (cont.)

5



En el **Área de notificación**, verá ahora el icono del componente de protección en tiempo real avast!. Para modificar su configuración, haga doble clic sobre él, o clic derecho para acceder al menú contextual.

6



A través del menú **Inicio** o del icono en el **Escritorio**, puede ejecutar avast!. La interfaz es sencilla, se asemeja a la de un equipo de reproducción de video/DVD. Seleccione el área por examinar, con los botones que aparecen del lado derecho, y comience el escaneo con un clic en el botón **Comienzo**.

SPAM

Un correo **spam** es un correo no solicitado, que fue enviado masivamente. Se utiliza la palabra spam para identificar cuando hay algo que se ofrece insistentemente, todo el tiempo, sin que lo hayamos pedido.

El spam no es exclusivo del correo electrónico, de hecho, uno de los primeros spam fue a través de la red telegráfica, cuando ése era el medio de comunicación que existía. Por eso, también hay spam telefónico, a través de los mensajes de texto. La facilidad de comunicación que proporciona Internet permite el spam por mensajería instantánea, en los foros.

La palabra spam proviene de una marca registrada que comercializa carne enlatada. Al parecer, durante la segunda Guerra Mundial, el **SPAM** era uno de los pocos productos que no se encontraban regulados y por esa razón se podía conseguir en todos los lados (**Figura 16**).

El grupo de comediantes británicos **Monthy Python** creó un sketch para su programa televisivo **Monty Python's Flying Circus** basado en este hecho, que



tenía lugar en una cafetería donde todos los productos que se ofrecían tenían spam, lo llevaran o no.

El spam tiene un grupo de características que lo identifican. La primera es que se realiza de forma **masiva**. Por eso, un correo que alguien nos envió sin que se lo pidiéramos, si fue solo a nosotros, no es spam. Los que generan spam son llamados **spammers**, personas que buscan un beneficio económico a través del envío de estos mensajes. Para obtener ganancias, debe haber alguien que pague y, por esta razón, el tipo de spam más común es el comercial, mensajes que nos ofrecen un producto. Las matemáticas detrás del modelo de

FIGURA 16.
SPAM es una marca registrada de Hormel Foods Corporation, quien piden respetar el uso de la palabra en mayúsculas para su producto, al tiempo que permite el uso en minúsculas para identificar el spam electrónico.



Un correo spam es un correo no solicitado, que fue enviado masivamente

negocio son sencillas. Enviar un correo electrónico es algo muy barato en la actualidad y, si se envía el mismo correo a miles de usuarios, las posibilidades de tener un cliente interesado aumentan mucho más que si solo se lo enviara a un grupo de veinte personas.

Una pregunta que nos podríamos hacer en este punto sería: ¿cómo obtuvieron los spammers mi dirección de correo? Recordemos lo que mencionamos sobre spyware, sobre la importancia de respetar nuestra privacidad en Internet. Lo cierto es que la pueden obtener por muchas vías: por ejemplo, si un virus contagia la PC de un conocido y nosotros estamos en su libreta de contactos, es capaz de enviar nuestra dirección junto con toda la lista a un spammer. Hay individuos que se dedican a vender estos listados de direcciones de correo electrónico.

El problema para nosotros es que esos correos **consumen recursos** en los servidores, espacio en disco, procesamiento del correo, y ancho de banda para recibirlos. Algunos buzones pueden llegar a recibir

1000 mensajes diferentes de spam en un fin de semana (o incluso en menos tiempo), y es realmente molesto recibir algo que uno no ha solicitado.

Supongamos que, en una empresa, cada usuario recibe cien spams diarios y se tienen unos trescientos buzones en el servidor: estamos hablando de treinta mil mensajes diarios, que consumen tiempo para ser procesados, y ancho de banda para ser recibidos y devueltos. Todo esto, para la empresa, es gasto que no tiene forma de recuperar. Sumémosle el tiempo que un empleado ocupa en borrarlos de la bandeja de entrada. Los costos asociados al spam han llegado a ser lo suficientemente significativos como para que cada vez más países creen leyes que prohíben este tipo de actividad y la sancionen con fuertes multas.

Combatir el spam

Cuando combatimos los virus o el spyware, el antivirus o antispyware revisa el archivo y decide directamente si es o no una amenaza. Con los correos no es tan fácil, un e-mail que un usuario podría considerar spam, para otro podría ser interesante. Un conocido nuestro puede encontrar una noticia que quiera compartir con todos los integrantes de su libreta de contactos. Sin embargo, la misma persona puede empezar a bombardear a otras con mensajes sobre anuncios diversos buscando algún beneficio a través de ellos.



SIGNIFICADOS DE HARDWARE Y SOFTWARE

Las palabras hardware y software no tienen traducción sencilla al español y están aceptadas por la RAE. Ambas utilizan la terminación *ware*, que se utiliza para referirse a conjunto. Luego, si tomamos los prefijos, *hard* significa **duro**, mientras que *soft* quiere decir **suave**.

Por suerte (o desgracia, en realidad), al igual que sucede con los virus, hay patrones que se repiten. Existen servicios que ofrecen las bases de datos con estos patrones para que se instalen en los servidores de correo, los cuales aprovechan esta información para bloquearlos. Sin embargo, siempre hay correos que van a escapar a estos patrones. En esos casos, los servidores tienen programas que realizan un análisis de cada correo y le adjuntan un encabezado con un valor que representa la probabilidad de que sea un spam.

Para los usuarios, la principal arma contra el spam es el cliente de correo. Debemos aclarar que muchos productos antivirus incluyen protección **antispam** que, cuando descargamos nuestros mensajes del servidor, realizan un prechequeo y, si detectan que es un spam, evitan que llegue al programa de correo.

Los clientes de correo permiten protegernos contra el spam de distintas formas. En primer lugar, el correo que se sospecha que sea spam, se almacena en una carpeta aparte, lo que nos permite mantener la carpeta de entrada solo con los que nos interesan.

Hay varias razones por las cuales el correo no se borra directamente, sino que se almacena en esa carpeta aparte. La idea es que tengamos nuestra carpeta de

A nivel de usuario, nuestra principal arma contra el spam es el cliente de correo

entrada lo más limpia posible de spam y, periódicamente, revisemos la otra carpeta para comprobar que al filtro no se le haya escapado algún correo que no era spam.

El **filtro antispam** no es perfecto y, en ocasiones, puede que catalogue incorrectamente un correo (falso positivo). De esta manera, evitaríamos perderlo. O quizás el correo sí fue un envío masivo y no solicitado, pero descubrimos que nos interesa. Los filtros antispam permiten ser entrenados por el usuario, y definir reglas sobre lo que debe y no considerar spam.

La carpeta que almacena los posibles spam recibe distintos nombres de acuerdo con el cliente de correo que tengamos configurado. Algunos la llaman **Basura**, otros **Correo electrónico no deseado** y, en las versiones en inglés, se utiliza **Junk** o **Junk E-mail**, como podemos ver en la **Figura 17**.

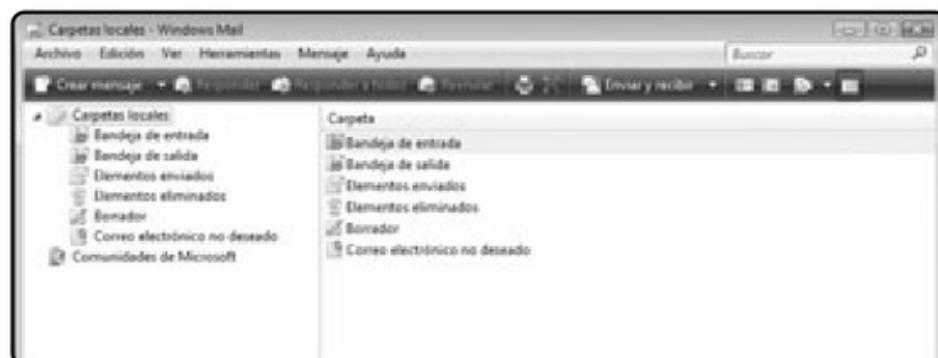


FIGURA 17. Windows Mail almacena los correos que identifica como spam en la carpeta Correo electrónico no deseado.

Backups

No hay nadie que se haya lamentado por hacer copias de respaldo y, sin embargo, somos muchos los que hemos agradecido tenerlas a mano.

Las causas que pueden provocar pérdida de información no son muchas: una mala operación nuestra (no lo neguemos), un virus, o un desperfecto del disco duro. También debemos tener cuidado cuando borramos archivos y carpetas: tenemos que hacerlo siempre con la **Papelera de reciclaje**, de manera que tengamos forma de recuperar lo que borramos sin darnos cuenta. Poseer protección antivirus activada y actualizada es otro aspecto que minimiza

en gran medida el riesgo de pérdida de información. Si utilizamos Windows Vista, es muy probable que nuestro disco duro no tenga más de un par de años de existencia, por lo que todavía va a durar un poco más.

Hay que tener en cuenta que los discos duros son impredecibles, tienen componentes mecánicos que giran a altas velocidades (el plato de un disco casero gira 7200 veces en un minuto). Por eso, una buena recomendación es grabar copias de los datos en CD-ROM o DV-DROM. Una memoria USB o un disco duro externo es otra buena opción. Por último, existen servicios de almacenamiento en línea que también podrían ser una variante interesante para considerar (**Figura 18**).

VirusTotal es un servicio de análisis de archivos sospechosos que permite detectar virus, gusanos, troyanos, y malware en general. [Más información...](#)

Análisis del archivo **ShellMgr.dll** recibido el 30.05.2008 00:30:09 (CET)
Estado actual: **análisis terminado**
Resultado: 0/32 (0.00%)

Motor antivirus	Versión	Última actualización	Resultado
AvastLab-V3	2008.5.29.0	2008-05-29	-
AvastV3	7.0.5.24	2008-05-29	-
AvastSecure	5.1.0.4	2008-05-29	-
Avast	4.8.1189-0	2008-05-29	-
AVG	7.5.0.358	2008-05-29	-
BitDefender	7.2	2008-05-30	-
ClamAV	0.90	2008-05-29	-
CleanAV	8.92.1	2008-05-29	-

FIGURA 18.
Si tenemos dudas respecto de un archivo específico, podemos verificar si contiene virus, en sitios web que ofrecen ese servicio.



RESUMEN

En este capítulo, dedicado a la seguridad de nuestro sistema informático, aprendimos a instalar un antivirus, mantener Windows actualizado y realizar backups. Además analizamos los conceptos de spam, virus, spyware, phishig, firewall, entre otros.

Multiple choice

► **1** ¿Por qué es importante tener el sistema operativo actualizado?

- a- Porque eso corregirá errores de seguridad.
 - b- Porque recibiremos actualizaciones para la interfaz de usuario.
 - c- Porque de otro modo expirará nuestra licencia.
 - d- Porque nuestro equipo correrá rápidamente.
-

► **2** El firewall de Windows:

- a- Nos protege frente ataques desde Internet.
 - b- Evita que los archivos salgan del equipo.
 - c- Quemará a quien toque nuestro equipo.
 - d- Reduce el rendimiento del equipo.
-

► **3** Para minimizar los riesgos de los ataques de phishing debemos:

- a- Dejar de utilizar el correo electrónico.
 - b- Darles nuestra dirección a amigos y familiares.
 - c- No abrir más correos adjuntos.
 - d- Utilizar un filtro de suplantación de identidad y prestar atención a los correos que abrimos.
-

► **4** La aplicación llamada Windows Defender nos protege contra:

- a- Los virus informáticos.
 - b- Los golpes que pueda sufrir el equipo.
 - c- Las intrusiones.
 - d- Adware y spyware.
-

► **5** Los virus necesitan protección del siguiente tipo:

- a- Especializada.
 - b- Crítica.
 - c- Constante.
 - d- Activa/en tiempo real.
-

► **6** Cuando un mensaje es filtrado erróneamente por el cliente de correo, debemos buscarlo en:

- a- La papelera de reciclaje.
 - b- El disco duro.
 - c- La carpeta Recibidos.
 - d- La carpeta Correo no deseado/Spam.
-

Respuestas: 1-a, 2-a, 3-d, 4-d, 5-d, 6-d.

Servicios al lector



Encontraremos información adicional relacionada con el contenido que servirá para complementar lo aprendido.

RedUSERS.com

▶ D

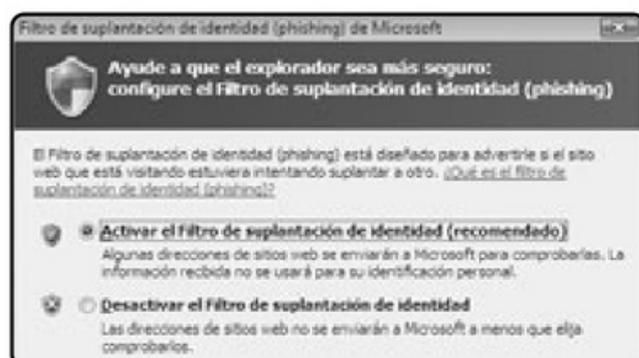
Descentralizadas	19
Dirección IP	60/61/62/163
DNS	62/142/143
Dirección MAC	106/107/108/109/110
Dirección física	106/109

▶ E

Estrella	139
EIA/TIA568	29
Escritorio remoto	72/84
Excepciones	154/159
Encriptación	111/112

▶ F

Fibra óptica	16/19/28
Firmware	111
Filtraje	106/107/108/109
Frase de contraseña	112/114
Firewall	131/150/152/153/154/155/158/159/166
Filtro de suplantación de identidad (phishing)	137/157/159



▶ G

Google Talk	147
Gusano	163

▶ H

Hub	25
Hotspots	105

▶ I

Intranet	20/21
Ipconfig	109
Invitado	80/81/86/87/88/89
Internet Explorer	134/135/136/137/139/140

▶ L

Linux	162
-------	-----

▶ N

NetBEUI	58/59
Niveles	13/14/17/27

▶ O

OSI	14/17
Organización Internacional para la Estandarización	14

8P8C	37
Opciones de Internet	131/138

► **P**

Par trenzado apantallado/ no apantallado	16
PC Card	101
PCI Express	101
Perfil	72/78/114
Pinza crimpeadora	35/36/37
Placa madre	49
POP3	63/144
PPPoE	62/64/125/128
Protocolo IP	60
Puerto Ethernet	25
Punto a punto	62/101/131
Punto central	101/116
Punto de acceso	64/116/117/122

► **R**

Roseta	34/37
Red de área local	43/59
Router inalámbrico	101/102/109/117

► **S**

STP	16/19
Switch	25/26/27/28/33/34/35
Spam	170/171/172
SSID	105/114/115
SMTP	143
Spyware	159/160/161/162/163/165

► **T**

TCP/IP	43/58/59/60/62/63
Téster	36/37
Tarjeta de red	28/29/36/37/38/39
Trabajo en Grupo	71

► **U**

UTP	15/16/19/26/27/28/29/33/36/37
Unix	21/58/84
Ubicación pública	46/48/50/69/70
Ubicación de red	46/48/49/70/91
UDP	60
Uso compartido de archivos	68/70/77/78/84/91
Uso compartido avanzado	84/85/86/88/90
UPnP	128
Uso compartido de impresoras	91

► **V**

VPN	65
Virus	162/163

► **W**

WAN	57/59
Windows Live Messenger	146/147
WEP	110/111/112
WPA	110/111/112
Windows Mail	143/144/172
Windows Defender	160/161/162
Windows Update	151

Sitios web recomendados

▶ **WINDOWS VISTA: AYUDA Y PROCEDIMIENTOS**
<http://windowshelp.microsoft.com/Windows/es-XL/>



En el sitio de Microsoft existe un espacio de ayuda dedicado exclusivamente a los usuarios de Windows Vista. Estas páginas nos brindan respuesta a prácticamente cualquier inquietud que tengamos respecto del trabajo con este sistema operativo.

▶ **MICROSOFT TECHNET**
<http://www.microsoft.com/latam/technet/seguridad/default.aspx>



Microsoft provee el sitio web **TechNet**, como un recurso para obtener información técnica sobre sus productos. Además, tiene una sección dedicada íntegramente al tema de la seguridad. Allí podemos encontrar los **Boletines de Seguridad** emitidos por Microsoft y las últimas **Alertas** realizadas, entre otras informaciones.

► **FORO DE WINDOWS VISTA**

<http://forums.microsoft.com/TechNetES/ShowForum.aspx?ForumID=633&SiteID=30>



Es un foro de Microsoft dedicado a los usuarios de Windows Vista. Como todo foro, nos permite registrarnos y formular las consultas que deseamos y serán respondidas por otros usuarios. Incluye una página de búsqueda que debemos utilizar en primera instancia por si nuestro problema ya fue planteado y resuelto anteriormente.

► **LINKSYS**

www-ar.linksys.com



La empresa Linksys es uno de los más importantes fabricantes de productos para redes inalámbricas. Si bien sus precios no son los más bajos, no son excesivos y están respaldados por la garantía de un excelente producto.

SPEEDTEST
www.speedtest.net



Los proveedores de acceso a Internet ofrecen herramientas en sus sitios web para comprobar la velocidad de acceso que tenemos, pero muchas veces, estas mediciones no reflejan el tráfico real cuando navegamos por Internet. Este es uno de los sitios en Internet y al estar fuera de la red de nuestro proveedor, nos brindará un dato más cercano a la velocidad que tenemos al navegar.

FIREFOX
www.mozilla-europe.org/es/firefox



En la actualidad no se puede hablar de Internet sin hablar de la Web. Y no se puede hablar de la Web sin hablar del Firefox. Un navegador que brinda una experiencia única de navegación, ayudado por un impresionante listado de complementos que cubren prácticamente cualquier necesidad que tengamos en nuestra interacción con Internet.

WINDOWS LIVE MAIL

<http://get.live.com/wlmail/overview>



Este cliente de correo es superior al que Windows Vista incorpora de manera predeterminada. De hecho fue desarrollado por el mismo equipo de programadores. Con nuevas funcionalidades y disponible para su descarga sin costo alguno, es sólo cuestión de tiempo antes de que reemplacemos a Windows Mail.

MOZILLA THUNDERBIRD

www.mozilla-europe.org/es/products/thunderbird/



Mozilla Thunderbird es un cliente de correo desarrollado por la misma fundación a cargo del navegador Firefox. Es un producto más completo que Windows Mail y al igual que Firefox, cuenta con un gran número de complementos que extienden su funcionalidad.

PANDA SECURITY

<http://www.pandasecurity.com/spain/homeusers/solutions/activescan/>



En ocasiones necesitamos asegurarnos de que una PC no tenga virus, pero no podemos instalarle un antivirus. Sitios como el fabricante de productos antivirus, **Panda Software**, nos ofrecen la oportunidad de realizar chequeos en nuestra PC sin instalar ningún programa.

AVAST!

www.avast.com/esp/download-avast-home.html



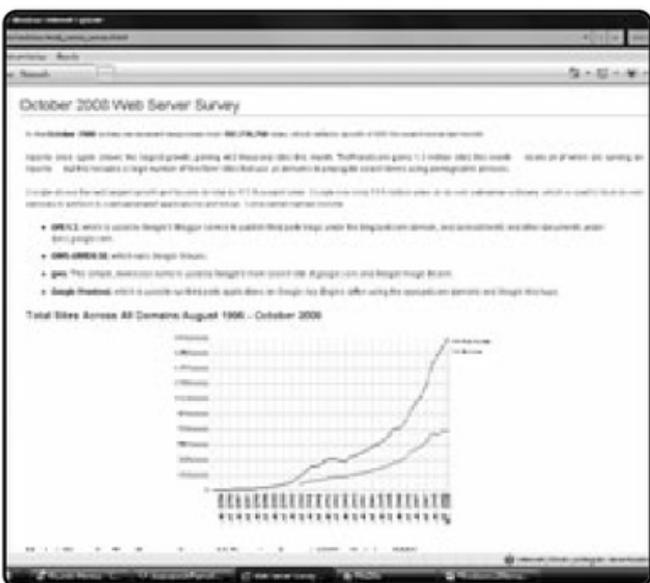
Uno de los componentes que no se incluyen en Windows Vista es el software antivirus. Avast! es una buena opción y para usar en nuestros hogares existe una versión gratis.

► **W3C WORLD WIDE WEB CONSORTIUM**
www.w3.org



Todo protocolo, todo estándar que se utilice en Internet, se encuentra regido por este consorcio internacional. Este es un sitio de referencia para todos aquéllos que nos dedicamos profesionalmente al trabajo con tecnologías de Internet.

► **NETCRAFT**
http://news.netcraft.com/archives/web_server_survey.html



Aunque este sitio se encuentra disponible sólo en inglés, es una excelente referencia sobre el desarrollo que sufre Internet. Mensualmente se publica un reporte que nos muestra el crecimiento que se ha producido en la cantidad de servidores conectados a Internet, entre otros datos de interés.

CLAVES PARA COMPRAR UN LIBRO DE COMPUTACIÓN

1 SOBRE EL AUTOR Y LA EDITORIAL

Revise que haya un cuadro "sobre el autor", en el que se informe sobre su experiencia en el tema. En cuanto a la editorial, es conveniente que sea especializada en computación.

2 PRESTE ATENCIÓN AL DISEÑO

Compruebe que el libro tenga guías visuales, explicaciones paso a paso, recuadros con información adicional y gran cantidad de pantallas. Su lectura será más ágil y atractiva que la de un libro de puro texto.

3 COMPARE PRECIOS

Suele haber grandes diferencias de precio entre libros del mismo tema; si no tiene el valor en tapa, pregunte y compare.

4 ¿TIENE VALORES AGREGADOS?

Desde un sitio exclusivo en la Red hasta un CD-ROM, desde un Servicio de Atención al Lector hasta la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, o la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No sólo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.

6 REVISE LA FECHA DE PUBLICACIÓN

Está en letra pequeña en las primeras páginas; si es un libro traducido, la que vale es la fecha de la edición original.



usershop.redusers.com

VISITE NUESTRO SITIO WEB

- » Vea información más detallada sobre cada libro de este catálogo.
- » Obtenga un capítulo gratuito para evaluar la posible compra de un ejemplar.
- » Conozca qué opinaron otros lectores.
- » Compre los libros sin moverse de su casa y con importantes descuentos.
- » Publique su comentario sobre el libro que leyó.
- » Manténgase informado acerca de las últimas novedades y los próximos lanzamientos.

TAMBIÉN PUEDE CONSEGUIR NUESTROS LIBROS EN KIOSCOS O PUESTOS DE PERIÓDICOS, LIBRERÍAS, CADENAS COMERCIALES, SUPERMERCADOS Y CASAS DE COMPUTACIÓN.



LLEGAMOS A TODO EL MUNDO VÍA »OCA * Y  **

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

 usershop.redusers.com //  usershop@redusers.com



Premiere + After Effects

Esta obra nos presenta un recorrido detallado por las aplicaciones audiovisuales de Adobe: Premiere Pro, After Effects y Soundbooth. Todas las técnicas de los profesionales, desde la captura de video hasta la creación de efectos, explicadas de forma teórica y práctica.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-9-3



Office 2010

En este libro aprenderemos a utilizar todas las aplicaciones de la suite, en su versión 2010. Además, su autora nos mostrará las novedades más importantes, desde los minigráficos de Excel hasta Office Web Apps, todo presentado en un libro único.

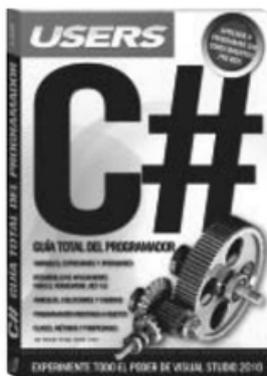
→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-26013-6-2



Excel Paso a Paso

En esta obra encontraremos una increíble selección de proyectos pensada para aprender mediante la práctica la forma de agilizar todas las tareas diarias. Todas las actividades son desarrolladas en procedimientos paso a paso de una manera didáctica y fácil de comprender.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-26013-4-8



C#

Este libro es un completo curso de programación con C# actualizado a la versión 4.0. Ideal tanto para quienes desean migrar a este potente lenguaje, como para quienes quieran aprender a programar desde cero en Visual Studio 2010.

→ COLECCIÓN: MANUALES USERS
→ 400 páginas / ISBN 978-987-26013-5-5



200 Respuestas Seguridad

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conseguir un equipo seguro. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-1-7



Funciones en Excel

Este libro es una guía práctica de uso y aplicación de todas las funciones de la planilla de cálculo de Microsoft. Desde las funciones de siempre hasta las más complejas, todas presentadas a través de ejemplos prácticos y reales.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-26013-0-0



¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Proyectos con Windows 7

En esta obra aprenderemos cómo aprovechar al máximo todas las ventajas que ofrece la PC. Desde cómo participar en las redes sociales hasta las formas de montar una oficina virtual, todo presentado en 120 proyectos únicos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-036-8



PHP 6

Este libro es un completo curso de programación de PHP en su versión 6.0. Un lenguaje que se destaca tanto por su versatilidad como por el respaldo de una amplia comunidad de desarrolladores, que lo convierten en un punto de partida ideal para quienes comienzan a programar.

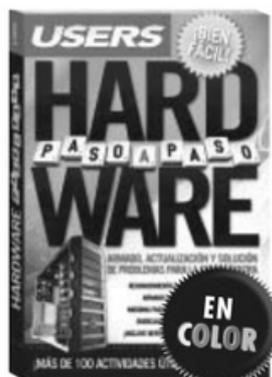
→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-039-9



200 Respuestas: Blogs

Esta obra es una completa guía que responde a las preguntas más frecuentes de la gente sobre la forma de publicación más poderosa de la Web 2.0. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-037-5



Hardware paso a paso

En este libro encontraremos una increíble selección de actividades que abarcan todos los aspectos del hardware. Desde la actualización de la PC hasta el overclocking de sus componentes, todo en una presentación nunca antes vista, realizada íntegramente con procedimientos paso a paso.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-034-4



200 Respuestas: Windows 7

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos conocer para dominar la última versión del sistema operativo de Microsoft. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-035-1



Office paso a paso

Este libro presenta una increíble colección de proyectos basados en la suite de oficina más usada en el mundo. Todas las actividades son desarrolladas con procedimientos paso a paso de una manera didáctica y fácil de comprender.

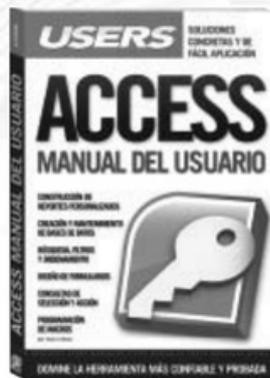
→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-030-6



101 Secretos de Hardware

Esta obra es la mejor guía visual y práctica sobre hardware del momento. En su interior encontraremos los consejos de los expertos sobre las nuevas tecnologías, las soluciones a los problemas más frecuentes, cómo hacer overclocking, modding, y muchos más trucos y secretos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-029-0



Access

Este manual nos introduce de lleno en el mundo de Access para aprender a crear y administrar bases de datos de forma profesional. Todos los secretos de una de las principales aplicaciones de Office, explicados de forma didáctica y sencilla.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-025-2



Redes Cisco

Este libro permitirá al lector adquirir todos los conocimientos necesarios para planificar, instalar y administrar redes de computadoras. Todas las tecnologías y servicios Cisco, desarrollados de manera visual y práctica en una obra única.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-024-5



Proyectos con Office

Esta obra nos enseña a usar las principales herramientas de Office a través de proyectos didácticos y útiles. En cada capítulo encontraremos la mejor manera de llevar adelante todas las actividades del hogar, la escuela y el trabajo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-023-8



Dreamweaver y Fireworks

Esta obra nos presenta las dos herramientas más poderosas para la creación de sitios web profesionales de la actualidad. A través de procedimientos paso a paso, nos muestra cómo armar un sitio real con Dreamweaver y Fireworks sin necesidad de conocimientos previos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-022-1



Excel revelado

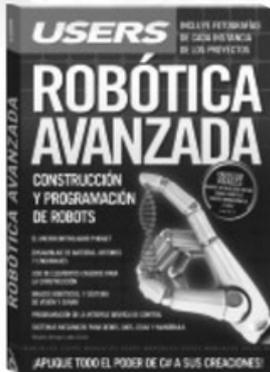
Este manual contiene una selección de más de 150 consultas de usuarios de Excel y todas las respuestas de Claudio Sánchez, un reconocido experto en la famosa planilla de cálculo. Todos los problemas encuentran su solución en esta obra imperdible.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-021-4



¡Léalo antes Gratis!

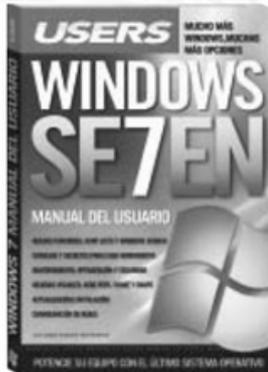
En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Robótica avanzada

Esta obra nos permitirá ingresar al fascinante mundo de la robótica. Desde el ensamblaje de las partes hasta su puesta en marcha, todo el proceso está expuesto de forma didáctica y sencilla para así crear nuestros propios robots avanzados.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-020-7



Windows 7

En este libro encontraremos las claves y los secretos destinados a optimizar el uso de nuestra PC tanto en el trabajo como en el hogar. Aprenderemos a llevar adelante una instalación exitosa y a utilizar todas las nuevas herramientas que incluye esta versión.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-015-3



De Windows a Linux

Esta obra nos introduce en el apasionante mundo del software libre a través de una completa guía de migración, que parte desde el sistema operativo más conocido: Windows. Aprenderemos cómo realizar gratuitamente aquellas tareas que antes hacíamos con software pago.

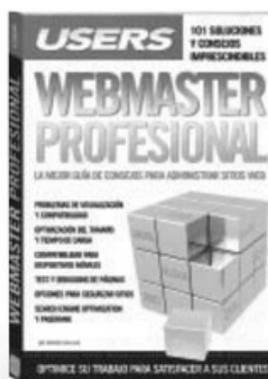
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-013-9



Producción y edición de video

Un libro ideal para quienes deseen realizar producciones audiovisuales con bajo presupuesto. Tanto estudiantes como profesionales encontrarán cómo adquirir las habilidades necesarias para obtener una salida laboral con una creciente demanda en el mercado.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-012-2



Webmaster Profesional

Esta obra explica cómo superar los problemas más frecuentes y complejos que enfrenta todo administrador de sitios web. Ideal para quienes necesiten conocer las tendencias actuales y las tecnologías en desarrollo que son materia obligada para dominar la Web 2.0.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-011-5



Silverlight

Este manual nos introduce en un nuevo nivel en el desarrollo de aplicaciones interactivas a través de Silverlight, la opción multiplataforma de Microsoft. Quien consiga dominarlo creará aplicaciones visualmente impresionantes, acordes a los tiempos de la incipiente Web 3.0.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-010-8



Flash Extremo

Este libro nos permitirá aprender a fondo Flash CS4 y ActionScript 3.0 para crear aplicaciones web y de escritorio. Una obra imperdible sobre uno de los recursos más empleados en la industria multimedia que nos permitirá estar a la vanguardia del desarrollo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-009-2



Hackers al descubierto

Esta obra presenta un panorama de las principales técnicas y herramientas utilizadas por los hackers, y de los conceptos necesarios para entender su manera de pensar, prevenir sus ataques y estar preparados ante las amenazas más frecuentes.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-008-5



Vista avanzado

Este manual es una pieza imprescindible para convertirnos en administradores expertos de este popular sistema operativo. En sus páginas haremos un recorrido por las herramientas fundamentales para tener máximo control sobre todo lo que sucede en nuestra PC.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-007-8



101 Secretos de Excel

Una obra absolutamente increíble, con los mejores 101 secretos para dominar el programa más importante de Office. En sus páginas encontraremos un material sin desperdicios que nos permitirá realizar las tareas más complejas de manera sencilla.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-005-4



Electrónica & microcontroladores PIC

Una obra ideal para quienes desean aprovechar al máximo las aplicaciones prácticas de los microcontroladores PIC y entender su funcionamiento. Un material con procedimientos paso a paso y guías visuales, para crear proyectos sin límites.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-002-3



Seguridad PC

Este libro contiene un material imprescindible para proteger nuestra información y privacidad. Aprenderemos cómo reconocer los síntomas de infección, las medidas de prevención a tomar, y finalmente, la manera de solucionar los problemas.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-004-7



¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Hardware desde cero

Este libro brinda las herramientas necesarias para entender de manera amena, simple y ordenada cómo funcionan el hardware y el software de la PC. Está destinado a usuarios que quieran independizarse de los especialistas necesarios para armar y actualizar un equipo.

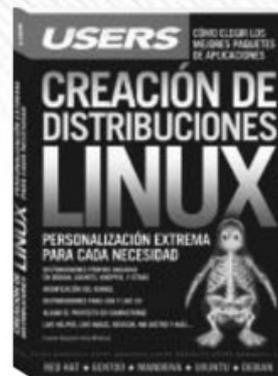
→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-001-6



200 Respuestas: Photoshop

Esta obra es una guía que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conocer y dominar Photoshop CS3. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-98-8



Creación de distribuciones Linux

En este libro recorreremos todas las alternativas para crear distribuciones personalizadas: desde las más sencillas y menos personalizables, hasta las más avanzadas, que nos permitirán modificar el corazón mismo del sistema, el kernel.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-1347-99-5



Métodos ágiles

Este libro presenta una alternativa competitiva a las formas tradicionales de desarrollo y los últimos avances en cuanto a la producción de software. Ideal para quienes sientan que las técnicas actuales les resultan insuficientes para alcanzar metas de tiempo y calidad.

→ COLECCIÓN: DESARROLLADORES
→ 336 páginas / ISBN 978-987-1347-97-1



SuperBlogger

Esta obra es una guía para sumarse a la revolución de los contenidos digitales. En sus páginas, aprenderemos a crear un blog, y profundizaremos en su diseño, administración, promoción y en las diversas maneras de obtener dinero gracias a Internet.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1347-96-4



UML

Este libro es la guía adecuada para iniciarse en el mundo del modelado. Conoceremos todos los constructores y elementos necesarios para comprender la construcción de modelos y razonarlos de manera que reflejen los comportamientos de los sistemas.

→ COLECCIÓN: DESARROLLADORES
→ 320 páginas / ISBN 978-987-1347-95-7

USERS PRESENTA...

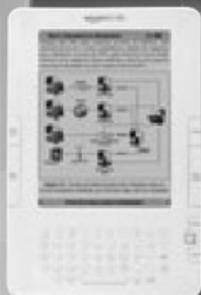
¡EL PRIMER EBOOK USERS!

Sí, ya podés leer Hackers al descubierto en tu PC, notebook, Amazon Kindle, iPad, en el celular...

CONSEGUILO
DESDE CUALQUIER
PARTE DEL MUNDO

A UN PRECIO
INCREÍBLE

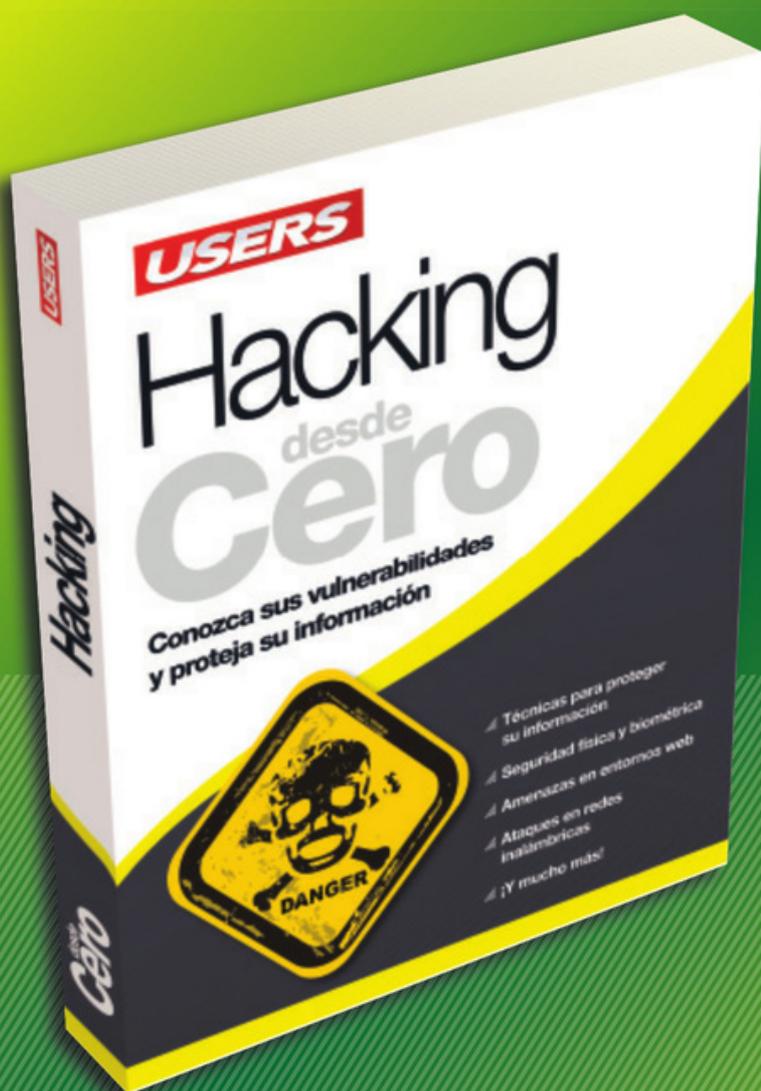
¿QUÉ ESTÁS
ESPERANDO?



¡LEELO
DONDE
QUIERAS!

INGRESA YA A [USERSHOP.REDUSERS.COM](http://usershop.redusers.com) Y ENTERATE MÁS

CONOZCA SUS VULNERABILIDADES Y PROTEJA SU INFORMACIÓN



En este libro encontraremos las principales técnicas y herramientas utilizadas por los hackers, explicadas en un lenguaje didáctico y sencillo. En sus páginas aprenderemos todo sobre las amenazas más frecuentes y sobre como defendernos ante los ataques.

» SEGURIDAD / HOME
» 192 PÁGINAS



SOBRE LA COLECCIÓN desde **Cero**

- » Aprendizaje práctico, divertido, rápido y sencillo.
- » Lenguaje simple y llano para una comprensión garantizada.
- » Consejos de los expertos para evitar problemas comunes.
- » Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS



LLEGAMOS A TODO EL MUNDO VÍA  * Y  **

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

 usershop.redusers.com //  usershop@redusers.com



Sobre la colección

- /// Aprendizaje práctico, divertido, rápido y sencillo
- /// Lenguaje simple y llano para una comprensión garantizada
- /// Consejos de los expertos para evitar problemas comunes
- /// Guías visuales y procedimientos paso a paso

Otros títulos de esta misma colección

Hardware / Office / Blogs /
Photoshop / Excel / Proyectos
Windows / Seguridad PC

Redes desde Cero



Las redes son una gran ventaja si sabemos cómo instalarlas, configurarlas y administrarlas. Este libro le enseñará cómo perder el miedo y animarse a realizar todas estas tareas de manera sencilla, evitando las complicaciones, pérdidas de tiempo y costos que un técnico puede requerir!

Dentro del libro encontrará

¿Qué es una red? | Redes en acción | Tipos de redes | Instalación de la red | Primeros pasos | Hubs vs. Switches | Armar un cable de red | Instalar un tarjeta de red | Configuración de la red | El protocolo TCP/IP | Windows y las redes | Grupos de trabajo | Compartir archivos e impresoras | Redes Wi-Fi | Establecer una conexión inalámbrica | Protección del router | Configurar la conexión a Internet | Seguridad en la red | Firewall | Protección de identidad

Networking from scratch



Networks have changed the way we work, play and communicate. This book will teach you how to use them, take advantage of all its secrets, and apply them to your everyday life with amazing results.

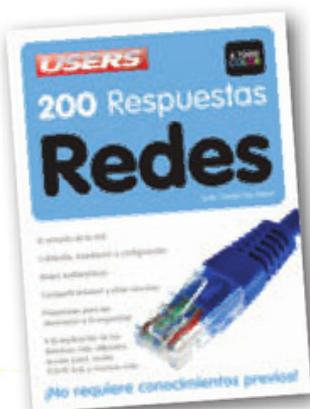
RedUSERS com

Nuestro sitio reúne a la mayor comunidad de tecnología en América Latina. Aquí podrá comunicarse con lectores, editores y autores, y acceder a noticias, foros y blogs constantemente actualizados.

Si desea más información sobre el libro:

Servicio de atención al lector usershop@redusers.com

El contenido de esta obra formó parte del libro 200 Respuestas Redes.



ISBN 978-987-1773-02-2



9 789871 773022 >