

# Capítulo 5

## Infraestructura de TI y tecnologías emergentes

### OBJETIVOS DE APRENDIZAJE RESUMEN DEL CAPÍTULO

*Después de leer este capítulo, usted podrá responder a las siguientes preguntas:*

1. ¿Qué es la infraestructura de TI y cuáles son sus componentes?
2. ¿Cuáles son las etapas y los impulsores tecnológicos en la evolución de la infraestructura de TI?
3. ¿Cuáles son las tendencias actuales en las plataformas de hardware de computadora?
4. ¿Cuáles son las tendencias actuales en las plataformas de software?
5. ¿Cuáles son los desafíos de administrar la infraestructura de TI y las soluciones gerenciales?

- 5.1 **INFRAESTRUCTURA DE TI**  
Definición de la infraestructura de TI  
Evolución de la infraestructura de TI  
Impulsores tecnológicos en la evolución de la infraestructura
- 5.2 **COMPONENTES DE LA INFRAESTRUCTURA**  
Plataformas de hardware de computadora  
Plataformas de sistemas operativos  
Aplicaciones de software empresariales  
Administración y almacenamiento de datos  
Plataformas de redes/telecomunicaciones  
Plataformas de Internet  
Servicios de consultoría e integración de sistemas
- 5.3 **TENDENCIAS DE LAS PLATAFORMAS DE HARDWARE CONTEMPORÁNEAS**  
La plataforma digital móvil emergente  
Computación en malla  
Virtualización  
Computación en la nube  
Computación verde  
Computación autónoma  
Procesadores de alto rendimiento y ahorro de energía
- 5.4 **TENDENCIAS DE LAS PLATAFORMAS DE SOFTWARE CONTEMPORÁNEAS**  
Linux y el software de código fuente abierto  
Software para Web: Java y Ajax  
Los servicios Web y la arquitectura orientada a servicios  
Outsourcing de software y servicios en la nube
- 5.5 **ASPECTOS GERENCIALES**  
Cómo lidiar con el cambio de plataforma e infraestructura  
Gerencia y gobernanza  
Cómo realizar inversiones de infraestructura inteligentes
- 5.6 **PROYECTOS PRÁCTICOS SOBRE MIS**  
Problemas de decisión gerencial  
Mejora de la toma de decisiones: uso de una hoja de cálculo para evaluar las opciones de hardware y de software  
Mejora de la toma de decisiones: uso de la investigación Web para obtener el presupuesto de una conferencia de ventas

#### *Sesiones interactivas:*

Novedad táctil

¿Es buena la computación verde para las empresas?

#### MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

Cómo funcionan el hardware y software de computadora  
Acuerdos a nivel de servicio  
La iniciativa de software de código fuente abierto  
Comparación de las etapas en la evolución de la infraestructura de TI  
Computación en la nube

## BART SE AGILIZA CON UNA NUEVA INFRAESTRUCTURA DE TI

El Tránsito Rápido del Área de la Bahía (BART) es un sistema de tránsito público ferroviario pesado, que conecta a San Francisco con Oakland, con California y otras ciudades vecinas al este y al sur. BART ha proporcionado un transporte rápido y confiable por más de 35 años y ahora transporta a más de 346 000 pasajeros a diario a través de 104 millas de rieles y 43 estaciones. Ofrece una alternativa para los que conducen a través de puentes y carreteras, también ayuda a reducir el tiempo de recorrido y el número de autos en los caminos congestionados del Área de la Bahía. Es el quinto sistema de tránsito rápido más concurrido en Estados Unidos.

Hace poco BART se embarcó en un esfuerzo de modernización ambicioso para actualizar sus estaciones, desplegar nuevos autovagones y extender sus rutas. Este esfuerzo también abarcó la infraestructura de tecnología de la información de BART. Sus sistemas de información ya no eran de vanguardia, además de que estaban empezando a afectar la capacidad de proveer un buen servicio. Los avejentados sistemas de recursos financieros y humanos desarrollados de manera interna ya no podían proveer información con la suficiente rapidez como para tomar decisiones oportunas, además de que eran muy poco confiables para dar soporte a sus operaciones 24/7.

BART actualizó tanto su hardware como su software. Reemplazó las viejas aplicaciones mainframe heredadas con aplicaciones PeopleSoft Enterprise de Oracle que se ejecutan en servidores blade HP Integrity y el sistema operativo Oracle Enterprise Linux. Esta configuración provee más flexibilidad y espacio para crecer, ya que BART puede ejecutar el software PeopleSoft junto con nuevas aplicaciones que antes no podía.

BART quería crear una infraestructura de TI de alta disponibilidad mediante el uso de computación en malla en donde pudiera ajustar el poder de cómputo y la capacidad de almacenamiento lo más posible para satisfacer a la demanda actual. BART eligió ejecutar sus aplicaciones en un grupo de servidores a través de una arquitectura de malla. Varios entornos operativos comparten capacidad y recursos de cómputo que se pueden suministrar, distribuir y redistribuir según sea necesario a través de la malla.

En la mayoría de los centros de datos se implementa un servidor distinto para cada aplicación; cada uno utiliza por lo general sólo una fracción de su capacidad. BART usa la virtualización para ejecutar varias aplicaciones en el mismo servidor, con lo cual se incrementa el uso de la capacidad del servidor hasta en un 50 por ciento o más. Esto significa que se pueden usar menos servidores para realizar la misma cantidad de trabajo.

Con los servidores blade, si BART necesita más capacidad, puede agregar otro al sistema principal. El uso de la energía se minimiza puesto que BART no tienen que comprar capacidad de cómputo si no la necesita; además el diseño modular simplificado de los servidores blade minimiza el uso de espacio físico y energía.

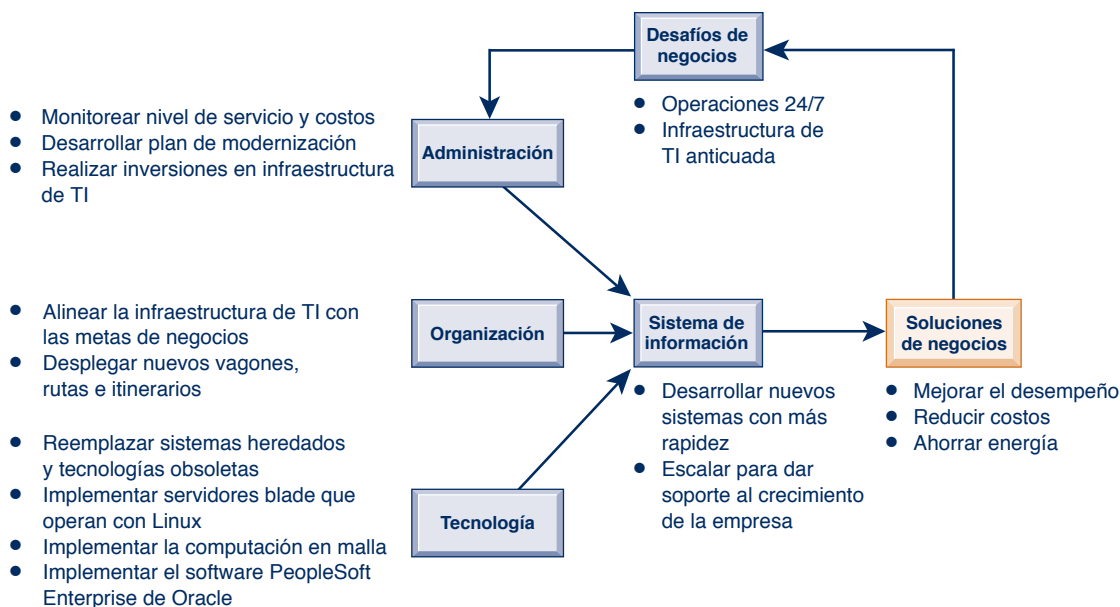
Al usar menos hardware y los recursos existentes con más eficiencia, el entorno en malla de BART ahorra costos en cuanto a energía y enfriamiento. Se espera que la consolidación de las aplicaciones en una capacidad de malla compartida de servidores reduzca el uso de energía en un valor aproximado al 20 por ciento.

**Fuentes:** David Baum, "Speeding into the Modern Age", *Profit*, febrero de 2010; [www.bart.gov](http://www.bart.gov), visitado el 5 de junio de 2010, y Steve Clouter, "The San Francisco Bay Area Rapid Transit Uses IBM Technology to Improve Safety and Reliability", *ARC Advisory Group*, 7 de octubre de 2009.

BART ha sido elogiado en muchas partes como un moderno sistema de tránsito rápido, pero sus operaciones y habilidad de crecer en donde sea necesario estaban obstaculizadas por una infraestructura de TI obsoleta. La gerencia de BART sintió que la mejor solución era invertir en nuevas tecnologías de hardware y software que fueran más efectivas en costo, eficaces y que ahorraran energía.

El diagrama de apertura del capítulo dirige la atención a los puntos importantes generados por este caso y este capítulo. La gerencia llegó a la conclusión de que para poder seguir proporcionando el nivel de servicio esperado por los residentes del Área de la Bahía, tenía que modernizar sus operaciones, entre ellas el hardware y software utilizados para operar la organización. Las inversiones en infraestructura de TI que realizó tenían que dar soporte a las metas de negocios de BART y contribuir a mejorar su desempeño. Entre otros objetivos estaban los de disminuir costos así como las metas "verdes" de reducir la energía y el consumo de materiales.

Al reemplazar su software heredado y sus computadoras con servidores blade en una malla y con software de negocios más moderno, BART pudo reducir los recursos de cómputo desperdiciados que no se utilizaban para el procesamiento, usarlos con más eficiencia y recortar tanto los costos como el consumo de energía. Las nuevas herramientas de software facilitan en gran medida el desarrollo de nuevas aplicaciones y servicios. La infraestructura de TI de BART es más fácil de administrar y es capaz de escalar para dar cabida a las cargas de procesamiento cada vez mayores, además de las nuevas oportunidades de negocios. Este caso muestra que las inversiones correctas en hardware y software no sólo mejoran el desempeño de negocios, sino que también pueden contribuir al logro de metas sociales importantes, como la conservación de energía y materiales.



## 5.1 INFRAESTRUCTURA DE TI

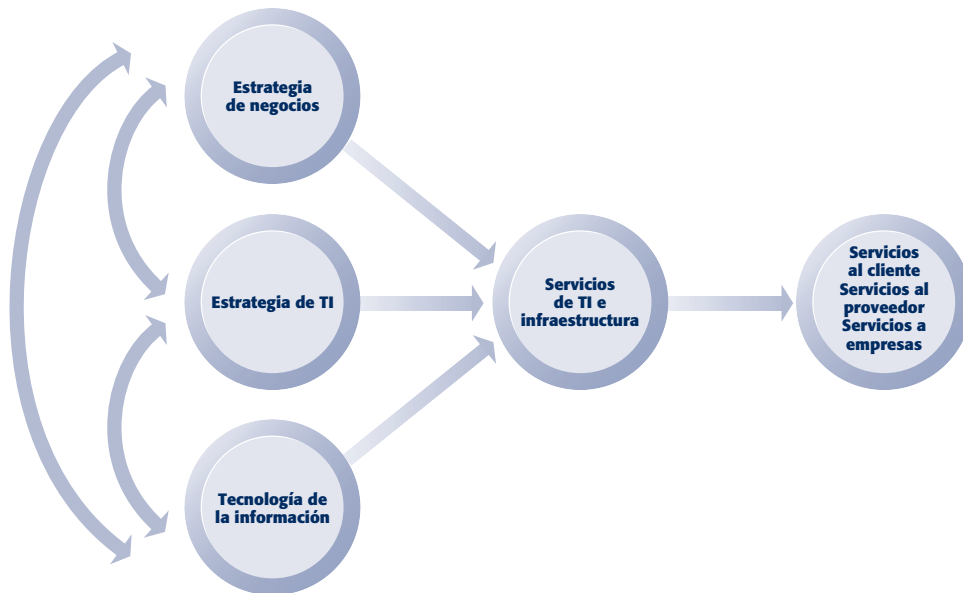
En el capítulo 1 definimos la *infraestructura de tecnología de la información (TI)* como los recursos de tecnología compartidos que proveen la plataforma de TI para las aplicaciones de sistemas de información específicas para la empresa. La infraestructura de TI incluye la inversión en hardware, software y servicios —como consultoría, educación y capacitación— que se comparten a través de toda la empresa o de unidades de negocios completas en ésta. La infraestructura de TI de una empresa provee la base para dar servicio a los clientes, trabajar con los distribuidores y gestionar los procesos de negocios internos (vea la figura 5-1).

Se estima que el negocio de proveer a las empresas de Estados Unidos infraestructura de TI (hardware y software) en 2010 fue una industria de \$1 billón si se incluyen las telecomunicaciones, el equipo de redes y los servicios de telecomunicaciones (Internet, teléfono y transmisión de datos). Esto no incluye a los servicios de consultoría de TI y procesos de negocios relacionados, lo cual agregaría otros \$800 mil millones. Las inversiones en infraestructura representan entre el 25 y 50 por ciento de los gastos en tecnología de la información en las empresas grandes, encabezadas por las de servicios financieros en las que la TI representa más de la mitad de toda la inversión de capital (Weill y colaboradores, 2002).

### DEFINICIÓN DE LA INFRAESTRUCTURA DE TI

La infraestructura de TI consiste en un conjunto de dispositivos físicos y aplicaciones de software requeridas para operar toda la empresa. Sin embargo, esta infraestructura también es un conjunto de servicios a nivel empresarial presupuestado por la gerencia, que abarca las capacidades tanto humanas como técnicas. Estos servicios abarcan:

**FIGURA 5-1 CONEXIÓN ENTRE LA EMPRESA, LA INFRAESTRUCTURA DE TI Y LAS CAPACIDADES DE NEGOCIOS**



Los servicios que una empresa es capaz de brindar a sus clientes, proveedores y empleados son una función directa de su infraestructura de TI, y lo ideal es que apoye la estrategia de negocios y sistemas de información de la empresa. Las nuevas tecnologías de la información tienen un poderoso impacto sobre las estrategias de negocios y de TI, así como en los servicios que se pueden proveer a los clientes.

- Plataformas computacionales que se utilizan para proveer servicios que conectan a los empleados, clientes y proveedores en un entorno digital coherente, entre ellos las grandes mainframes, las computadoras medianas, las computadoras de escritorio, las laptop y los dispositivos móviles portátiles.
- Servicios de telecomunicaciones que proporcionan conectividad de datos, voz y video a los empleados, clientes y proveedores.
- Servicios de gestión de datos que almacenan y gestionan los datos corporativos, además de proveer herramientas para analizarlos.
- Servicios de software de aplicación que ofrece herramientas a nivel empresarial, como la planificación de recursos empresariales, la administración de relaciones con el cliente, la gestión de la cadena de suministro y los sistemas de administración del conocimiento que comparten todas las unidades de negocios.
- Servicios de administración de instalaciones físicas que desarrollen y gestionen las instalaciones físicas requeridas para los servicios de cómputo, telecomunicaciones y administración de datos.
- Servicios de gestión de TI que planeen y desarrollen la infraestructura, se coordinen con las unidades de negocios para los servicios de TI, administren la contabilidad para los gastos de TI y proporcionen servicios de gestión de proyectos.
- Servicios de estándares de TI que proporcionen a la empresa y sus unidades de negocios, políticas que determinen qué tecnología de información se utilizará, cuándo y cómo.
- Servicios de educación de TI que provean capacitación en cuanto al uso del sistema para los empleados y que ofrezcan a los gerentes instrucción en cuanto a la forma de planear y gestionar las inversiones en TI.
- Servicios de investigación y desarrollo de TI que proporcionen a la empresa investigación sobre futuros proyectos e inversiones de TI que podrían ayudar a la empresa a sobresalir en el mercado.

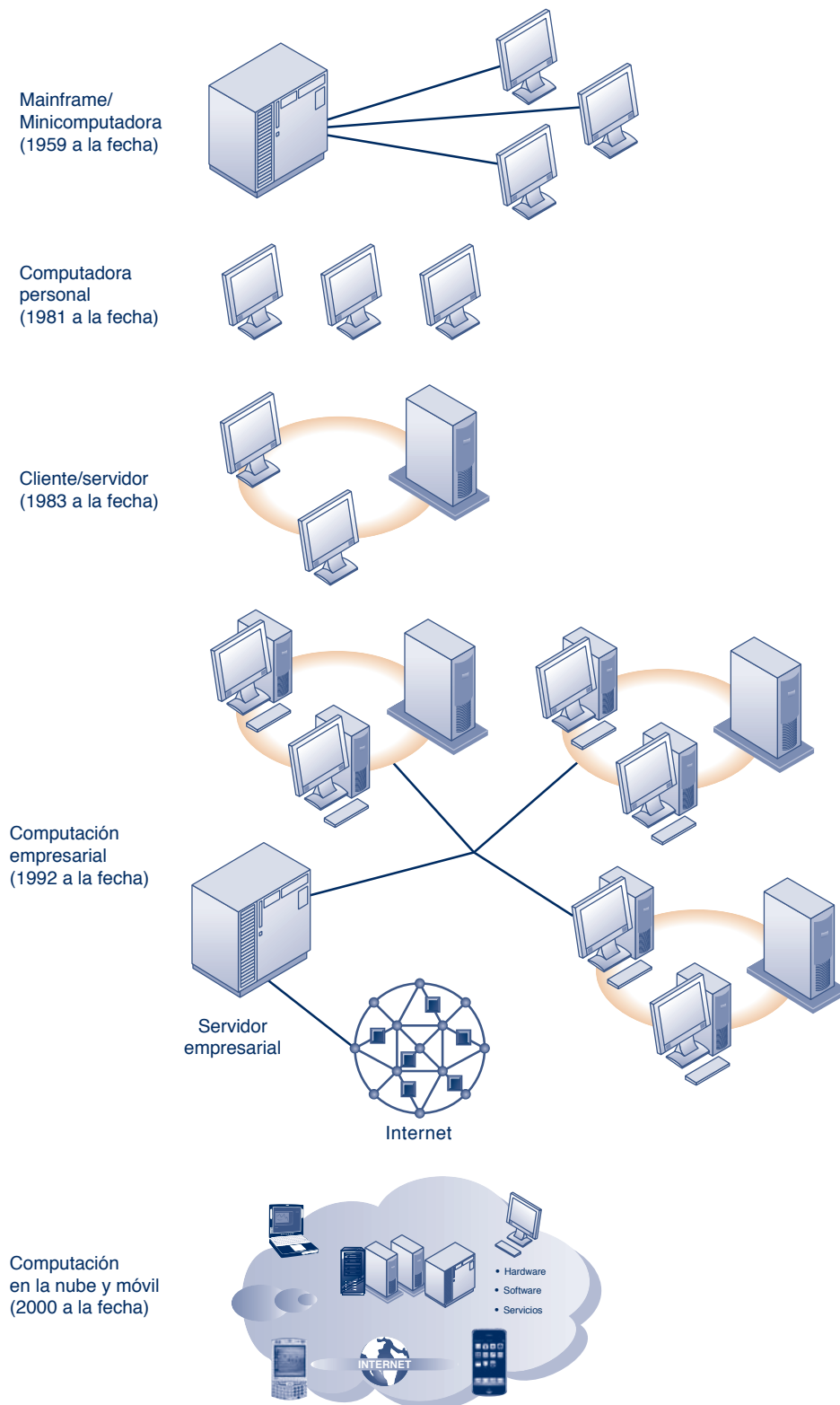
Esta perspectiva de “plataforma de servicios” facilita la comprensión del valor de negocios que proporcionan las inversiones de infraestructura. Por ejemplo, el verdadero valor comercial de una computadora personal con carga completa, que opera a 3 gigahertz y cuesta cerca de \$1 000, o de una conexión a Internet de alta velocidad, son cosas difíciles de entender sin saber quién las utilizará y cómo lo hará. Sin embargo, cuando analizamos los servicios que proporcionan estas herramientas, su valor se vuelve más aparente: la nueva PC hace posible que un empleado de alto costo que gana \$100 000 al año conecte todos los principales sistemas de la compañía con la red Internet pública. El servicio de Internet de alta velocidad ahorra a este empleado cerca de una hora al día del tiempo que tiene que esperar para recibir o enviar información a través de Internet. Sin esta PC y la conexión a Internet, el valor de este empleado para la empresa se podría recortar a la mitad.

## EVOLUCIÓN DE LA INFRAESTRUCTURA DE TI

La infraestructura de TI en las organizaciones actuales es el fruto de más de 50 años de evolución en las plataformas de computadora. Han transcurrido cinco etapas en esta evolución, cada una de las cuales representa una distinta configuración de poder de cómputo y elementos de la infraestructura (vea la figura 5-2). Las cinco eras son la computación con mainframes y minicomputadoras de propósito general, las microcomputadoras mejor conocidas como computadoras personales, las redes cliente/servidor, la computación empresarial y la computación en la nube y móvil.

Las tecnologías que caracterizan una era también se pueden usar en otro periodo de tiempo para otros fines. Por ejemplo, algunas compañías todavía utilizan sistemas mainframe tradicionales o usan computadoras mainframe como servidores masivos para dar soporte a sitios Web grandes y aplicaciones empresariales corporativas.

**FIGURA 5-2 ERAS EN LA EVOLUCIÓN DE LA INFRAESTRUCTURA DE TI**



En esta figura se ilustran las configuraciones típicas de computadoras que caracterizan cada una de las cinco eras de la evolución en la infraestructura de TI.

### Era de las mainframes y minicomputadoras de propósito general (1959 a la fecha)

La introducción de las máquinas transistorizadas IBM 1401 y 7090 en 1959 marcó el principio del uso comercial extendido de las computadoras **mainframe**. En 1965, la computadora mainframe llegó a su momento máximo con la introducción de la serie IBM 360. La cual fue la primera computadora comercial con un poderoso sistema operativo que podía proveer tiempo compartido, multitareas y memoria virtual en modelos más avanzados. IBM dominó el área de las computadoras mainframe desde este punto en adelante. Estas computadoras tenían el suficiente poder como para dar soporte a miles de terminales remotas en línea, conectadas a la mainframe centralizada mediante el uso de protocolos de comunicación y líneas de datos propietarios.

La era de la mainframe fue un periodo de computación con alto grado de centralización bajo el control de programadores y operadores de sistemas profesionales (por lo general en un centro de datos corporativo), en donde la mayoría de los elementos de la infraestructura los proveía un solo distribuidor, el fabricante del hardware y del software.

Este patrón empezó a cambiar con la llegada de las **minicomputadoras** producidas por Digital Equipment Corporation (DEC) en 1965. Las minicomputadoras DEC (PDP-11 y más adelante las máquinas VAX) ofrecían máquinas poderosas a precios mucho más bajos que las mainframes de IBM, lo que hizo posible la computación descentralizada, personalizada a las necesidades específicas de los departamentos individuales o las unidades de negocios en vez de compartir el tiempo en una sola y gigantesca mainframe. En años recientes, la minicomputadora evolucionó en una computadora o servidor de medio rango y forma parte de una red.

### Era de la computadora personal (1981 a la fecha)

Aunque las primeras computadoras que de verdad eran personales (PCs) aparecieron en la década de 1970 (la Xerox Alto, la MITS Altair 8800 y las Apple I y II, por mencionar algunas), sólo tenían distribución limitada para los entusiastas de las computadoras. La aparición de la IBM PC en 1981 se considera por lo general como el inicio de la era de la PC, ya que esta máquina fue la primera que se adoptó de manera extendida en las empresas estadounidenses. La computadora **Wintel PC** (sistema operativo Windows en una computadora con un microprocesador Intel), que en un principio utilizaba el sistema operativo DOS, un lenguaje de comandos basado en texto y posteriormente el sistema operativo Windows, se convirtió en la computadora personal de escritorio estándar. En la actualidad, el 95 por ciento de los 1.5 mil millones de computadoras estimadas en el mundo utilizan el estándar Wintel.

La proliferación de las PCs en la década de 1980 y a principios de la de 1990 desató un torrente de herramientas de software personales de productividad de escritorio (procesadores de palabras, hojas de cálculo, software de presentación electrónica y pequeños programas de gestión de datos) que fueron muy valiosos para los usuarios tanto domésticos como corporativos. Estas PCs eran sistemas independientes hasta que el software de sistema operativo de PC en la década de 1990 hizo posible enlazarlas en redes.

### Era cliente/servidor (1983 a la fecha)

En la **computación cliente/servidor**, las computadoras de escritorio o laptop conocidas como **clientes** se conectan en red a poderosas computadoras **servidores** que proveen a las computadoras clientes una variedad de servicios y herramientas. El trabajo de procesamiento de cómputo se divide entre estos dos tipos de máquinas. El cliente es el punto de entrada del usuario, mientras que el servidor por lo general procesa y almacena datos compartidos, sirve páginas Web o gestiona las actividades de la red. El término "servidor" se refiere tanto a la aplicación de software como a la computadora física en la que se ejecuta el software de red. El servidor podría ser una mainframe, pero en la actualidad las computadoras servidor son por lo general versiones más poderosas de computadoras personales, basadas en chips económicos y que a menudo utilizan varios procesadores en una sola caja de computadora.



La red cliente/servidor más simple consiste en una computadora cliente conectada en red a una servidor, en donde el procesamiento se divide entre los dos tipos de máquinas. A esto se le conoce como *arquitectura cliente/servidor de dos niveles*. Mientras que podemos encontrar las redes cliente/servidor simples en empresas pequeñas, la mayoría de las corporaciones tienen **arquitecturas cliente/servidor multinivel** (a menudo conocida como de **N-niveles**) más complejas, en donde el trabajo de toda la red se balancea a través de distintos niveles de servidores, dependiendo del tipo de servicio que se solicite (vea la figura 5-3).

Por ejemplo, en el primer nivel, un **servidor Web** sirve una página Web a un cliente en respuesta a una solicitud de servicio. El software del servidor Web es responsable de localizar y gestionar las páginas Web almacenadas. Si el cliente solicita acceso a un sistema corporativo (una lista de productos o información de precios, por ejemplo), la solicitud se pasa a un **servidor de aplicaciones**. El software del servidor de aplicaciones maneja todas las operaciones de las aplicaciones entre un usuario y los sistemas empresariales back-end de una organización. El servidor de aplicaciones puede residir en la misma computadora que el servidor Web, o en su propia computadora dedicada. Los capítulos 6 y 7 proporcionan más detalle sobre otras piezas de software que se utilizan en las arquitecturas cliente/servidor multinivel para el comercio y los negocios electrónicos.

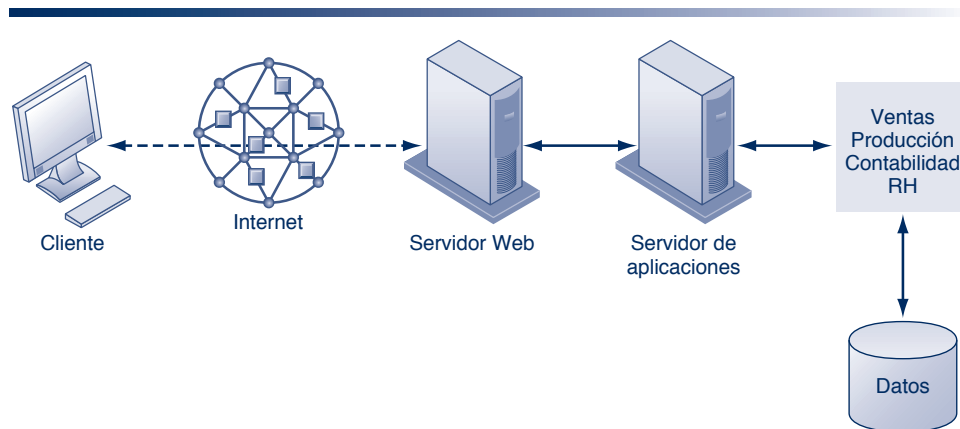
La computación cliente/servidor permite a las empresas distribuir el trabajo de cómputo entre una serie de máquinas más pequeñas y económicas que cuestan mucho menos que las minicomputadoras o los sistemas mainframe centralizados. El resultado es una explosión en el poder de cómputo y las aplicaciones en toda la empresa.

Novell NetWare fue la tecnología líder para las redes cliente/servidor al principio de la era cliente/servidor. En la actualidad, Microsoft es el líder del mercado con sus sistemas operativos **Windows** (Windows Server, Windows 7, Windows Vista y Windows XP).

### Era de la computación empresarial (1992 a la fecha)

A principios de la década de 1990, las empresas recurrieron a estándares de redes y herramientas de software que pudieran integrar redes y aplicaciones dispares esparcidas por toda la empresa en una infraestructura a nivel empresarial. Cuando Internet se desarrolló para convertirse en un entorno de comunicaciones de confianza después de 1995, las empresas de negocios empezaron a utilizar en serio el estándar de redes *Protocolo de control de transmisión/Protocolo Internet (TCP/IP)* para

**FIGURA 5-3** UNA RED CLIENTE/SERVIDOR MULTINIVEL (N-NIVELES)



En una red cliente/servidor multinivel, las solicitudes de servicio de los clientes se manejan mediante distintos niveles de servidores.



enlazar sus redes dispares. En el capítulo 7 analizaremos el estándar TCP/IP con detalle.

La infraestructura de TI resultante enlaza distintas piezas de hardware de computadora y redes más pequeñas en una sola red a nivel empresarial, de modo que la información pueda fluir con libertad por toda la organización, y también entre la empresa y otras organizaciones. Puede enlazar distintos tipos de hardware de computadora, entre ellos mainframes, servidores, PCs, teléfonos móviles y otros dispositivos portátiles; además cuenta con infraestructuras públicas como el sistema telefónico, Internet y los servicios de redes públicas. La infraestructura empresarial también requiere software para enlazar aplicaciones dispares y permitir que los datos fluyan con libertad entre distintas partes de la empresa, como las aplicaciones empresariales (vea los capítulos 2 y 9) y los servicios Web (que analizaremos en la sección 5.4).

### **Era de la computación en la nube y móvil (2000 a la fecha)**

El poder cada vez mayor del ancho de banda de Internet ha impulsado el avance del modelo cliente/servidor, hacia lo que se conoce como el “Modelo de computación en la nube”. La **computación en la nube** se refiere a un modelo de cómputo que provee acceso a una reserva compartida de recursos computacionales (computadoras, almacenamiento, aplicaciones y servicios) a través de una red, que con frecuencia viene siendo Internet. Se puede acceder a estas “nubes” de recursos computacionales según sea necesario, desde cualquier dispositivo conectado y cualquier ubicación. En la actualidad, la computación en la nube es la forma de computación que crece con mayor rapidez, en donde se espera que los ingresos globales lleguen a cerca de \$89 mil millones en 2011 y a casi \$149 mil millones para 2014, de acuerdo con los consultores de tecnología de Gartner Inc. (Cheng y Borzo, 2010; Veverka, 2010).

Hay miles, o incluso cientos de miles de computadoras ubicadas en centros de datos en la nube, y podemos acceder a ellas mediante computadoras de escritorio, laptops, netbooks, centros de entretenimiento, dispositivos móviles y otras máquinas cliente enlazadas a Internet, en donde una parte cada vez mayor de la computación personal y corporativa está cambiando a las plataformas móviles. IBM, HP, Dell y Amazon operan enormes centros de computación en la nube escalables que proveen poder de cómputo, almacenamiento de datos y conexiones a Internet de alta velocidad para empresas que desean mantener sus infraestructuras de TI en forma remota. Las empresas de software como Google, Microsoft, SAP, Oracle y Salesforce.com venden aplicaciones de software como servicios que se ofrecen a través de Internet.

En la sección 5.3 analizaremos la computación en la nube con más detalle. Las Trayectorias de aprendizaje proporcionan una tabla sobre las etapas en la evolución de la infraestructura de TI, en la cual se compara cada era en las dimensiones de infraestructura presentadas.

## **IMPULSORES TECNOLÓGICOS EN LA EVOLUCIÓN DE LA INFRAESTRUCTURA**

Los cambios en la infraestructura de TI que acabamos de describir, son el resultado de los desarrollos en el procesamiento de las computadoras, los chips de memoria, los dispositivos de almacenamiento, el hardware y software de telecomunicaciones y redes, el diseño de software, lo cual ha incrementado de manera exponencial el poder de cómputo, a la vez que ha reducido los costos a una gran velocidad. Ahora veamos los desarrollos más importantes.

### **La ley de Moore y el poder de los microprocesadores**

En 1965, Gordon Moore, director de los Laboratorios de investigación y desarrollo de Fairchild Semiconductor, uno de los primeros fabricantes de circuitos integrados, escribió en la revista *Electronics* que desde la introducción del primer chip microprocesador en 1959, el número de componentes en un chip con los menores costos de fabricación por componente (por lo general, transistores) se había duplicado cada año. Esta asevera-

ción se convirtió en la base de la **ley de Moore**. Más adelante, Moore redujo la tasa de crecimiento al doble cada dos años.

Tiempo después, esta ley se interpretaría de varias formas. Hay por lo menos tres variaciones de ella, ninguna de las cuales fue planteada por Moore: (1) el poder de los microprocesadores se duplica cada 18 meses; (2) el de cómputo cada 18 meses, y (3) el precio de los componentes de cómputo se reduce a la mitad cada 18 meses.

La figura 5-4 ilustra la relación entre el número de transistores en un microprocesador y los millones de instrucciones por segundo (MIPS), una medida común del poder de un procesador. La figura 5-5 muestra la disminución exponencial en el costo de los transistores y el aumento en el poder de cómputo. Por ejemplo, en 2011 un procesador Intel Xeon de ocho núcleos contenía 2 300 millones de transistores.

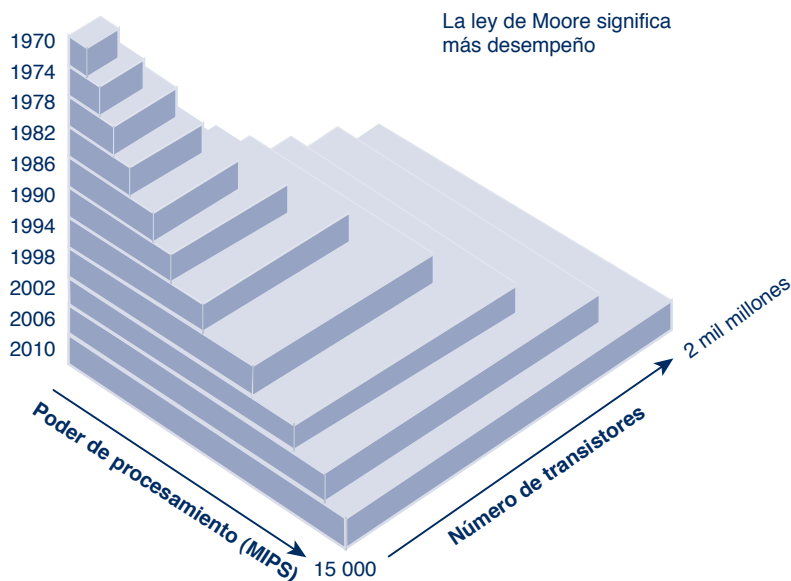
Es probable que continúe el crecimiento exponencial en el número de transistores y el poder de los procesadores, aunado a una reducción cada vez más rápida en los costos de los componentes de cómputo. Los fabricantes de chips siguen miniaturizando componentes. Los transistores de la actualidad ya no deberían compararse con el tamaño de un cabello humano, sino con el de un virus.

Mediante el uso de la nanotecnología, los fabricantes de chips pueden incluso reducir el tamaño de los transistores hasta la anchura de varios átomos. La **nanotecnología** usa átomos y moléculas individuales para crear chips de computadora y otros dispositivos que son miles de veces más pequeños de lo que las tecnologías actuales permiten. Los fabricantes están tratando de desarrollar un proceso de manufactura que pueda producir procesadores de nanotubos de manera económica (figura 5-6). IBM recién empezó a fabricar microprocesadores en un entorno de producción que utiliza esta tecnología.

### Ley del almacenamiento digital masivo

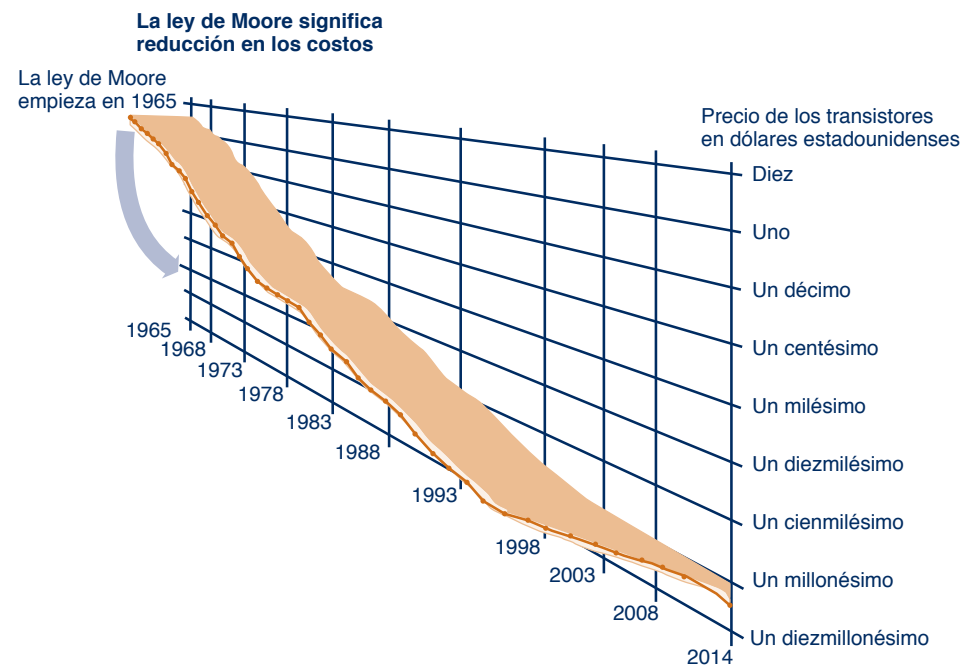
La ley del almacenamiento digital masivo es un segundo impulsor de tecnología de la infraestructura de TI. El mundo produce hasta 5 exabytes de información única al año (un exabyte equivale a mil millones de gigabytes, o  $10^{18}$  bytes). En términos generales, la cantidad de información digital se duplica cada año (Lyman y Varian, 2003). Por fortuna, el costo de almacenar información digital se está reduciendo a una tasa exponen-

**FIGURA 5-4 LA LEY DE MOORE Y EL DESEMPEÑO DEL MICROPROCESADOR**



Al empaquetar más de 2 mil millones de transistores en un diminuto microprocesador se ha incrementado de manera exponencial el poder de procesamiento. Éste se incrementó a más de 500 000 MIPS (millones de instrucciones por segundo).

Fuentes: Intel, 2010; estimación de los autores.

**FIGURA 5-5 DISMINUCIÓN EN EL COSTO DE LOS CHIPS**

Al empaquetar más transistores en menos espacio, el costo de los transistores se reduce de manera dramática, así como el costo de los productos en los que se utilizan.

*Fuente:* Intel, 2010; estimaciones de los autores.

**FIGURA 5-6 EJEMPLOS DE NANOTUBOS**

Los nanotubos son tubos diminutos cerca de 10 000 veces más delgados que un cabello humano. Consisten en hojas enrolladas de hexágonos de carbono y tienen los usos potenciales como minúsculos cables o en dispositivos electrónicos ultrapequeños; además son conductores muy poderosos de corriente eléctrica.

cial del 100 por ciento cada año. La figura 5-7 muestra que el número de kilobytes que se pueden almacenar en medios magnéticos por \$1 desde 1950 a la fecha se duplicó cada 15 meses aproximadamente.

### La ley de Metcalfe y la economía de red

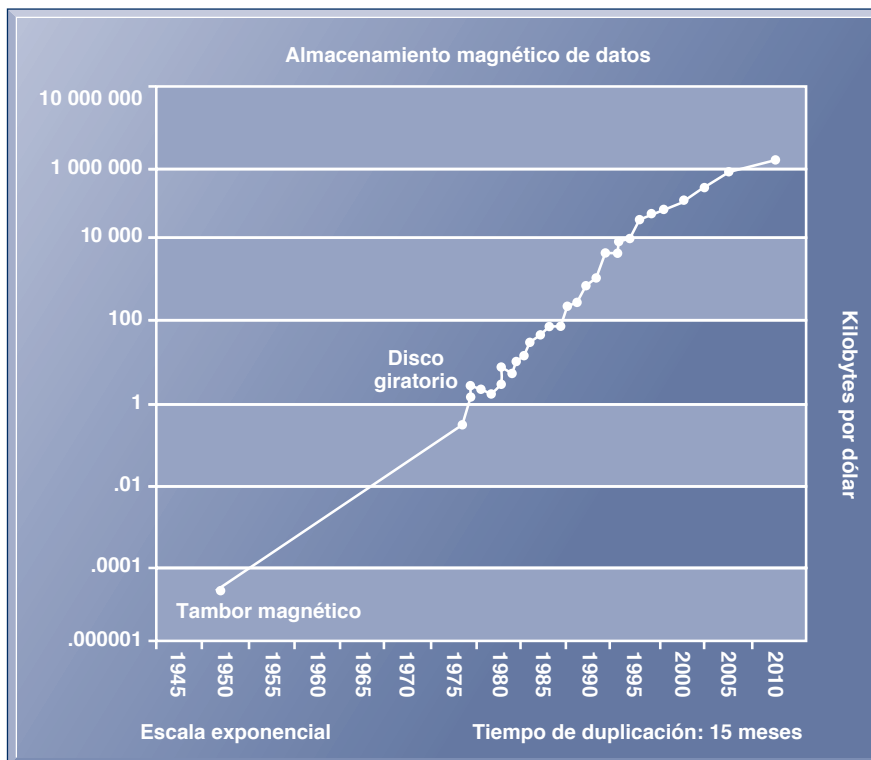
La ley de Moore y la ley del almacenamiento masivo nos ayudan a comprender por qué ahora los recursos de cómputo están disponibles con tanta facilidad. Pero, ¿por qué desean las personas más poder de cómputo y de almacenamiento? La economía de las redes y el crecimiento de Internet ofrecen algunas respuestas.

Robert Metcalfe (inventor de la tecnología de red de área local Ethernet) afirmó en 1970 que el valor o poder de una red aumenta en forma exponencial como una función del número de miembros en la red. Metcalfe y otros señalan los *rendimientos crecientes con respecto a la escala* que reciben los miembros de la red, a medida que cada vez más personas se unen a ésta. Conforme aumenta el número de miembros en una red de manera lineal, el valor de todo el sistema crece en forma exponencial y continúa haciéndolo indefinidamente, según aumentan sus miembros. La demanda de tecnología de la información funciona con base en el valor social y comercial de las redes digitales, que multiplican con rapidez los enlaces actuales y potenciales entre los miembros de la red.

### Reducción en los costos de las comunicaciones e Internet

Un cuarto elemento impulsor de la tecnología que transforma la infraestructura de TI es la rápida reducción en los costos de la comunicación y el crecimiento exponencial

**FIGURA 5-7 EL COSTO DE ALMACENAR DATOS DISMINUYE DE MANERA EXPONENCIAL 1950-2010**



Desde que se utilizó el primer dispositivo de almacenamiento magnético en 1955, el costo de almacenar un kilobyte de dato se ha reducido de manera exponencial, a la vez que se duplica la cantidad de almacenamiento digital por cada dólar gastado cada 15 meses en promedio.

Fuentes: Kurzweil 2003; estimaciones de los autores.

en el tamaño de Internet. Se estima que en la actualidad 1.8 mil millones de personas en todo el mundo tienen acceso a Internet (Internet World Stats, 2010). La figura 5-8 ilustra la reducción exponencial en el costo de comunicarse tanto a través de Internet como de las redes telefónicas (que cada vez dependen más de Internet). A medida que disminuyen los costos de comunicación y llegan a una cifra muy pequeña que se acerca a 0, aumenta en forma explosiva el uso de las herramientas de comunicaciones y computación.

Para aprovechar el valor de negocios asociado con Internet, las empresas deben expandir en forma considerable sus conexiones, que involucran a la conectividad inalámbrica, al poder de sus redes cliente/servidor, a los clientes de escritorio y a los dispositivos de cómputo móviles. Todo indica que estas tendencias continuarán.

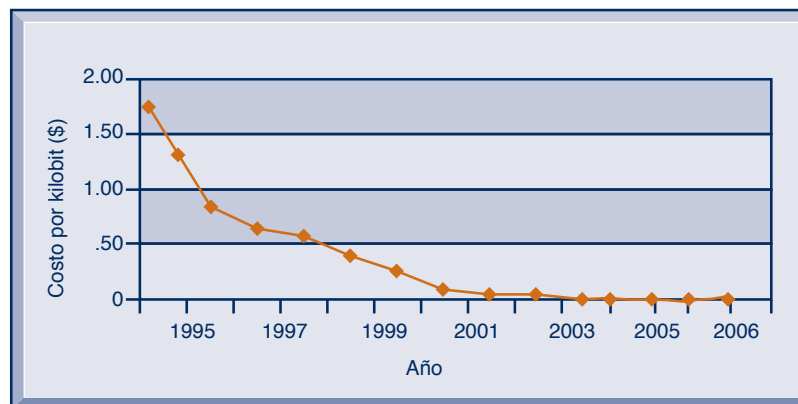
### Estándares y efectos de la red

Tanto la actual infraestructura empresarial como la computación en Internet serían imposibles —ahora y en el futuro— sin acuerdos en los que los fabricantes y los consumidores aceptaran de manera extendida los **estándares de tecnología**. Los cuales son especificaciones que establecen la compatibilidad de los productos y la habilidad de comunicarse en una red (Stango, 2004).

Los estándares de tecnología desencadenan poderosas economías de escala y provocan reducciones en los precios, a medida que los fabricantes se enfocan en producir los productos con base en un solo estándar. Sin estas economías de escala, la computación de cualquier tipo sería mucho más costosa de lo actual. La tabla 5-1 describe los estándares importantes que han dado forma a la infraestructura de TI.

A partir de la década de 1990, las corporaciones empezaron a avanzar hacia la computación y las plataformas de comunicaciones estándar. La Wintel PC con el sistema operativo Windows y las aplicaciones de productividad de escritorio Microsoft Office se convirtieron en la plataforma de computación estándar para clientes de escritorio y móviles. La adopción extendida de Unix como el sistema operativo servidor empresarial preferido hizo posible el reemplazo de las infraestructuras de mainframes propietarias y costosas. En las telecomunicaciones, el estándar Ethernet permitió conectar las PCs en pequeñas redes de área local (LANs; vea el capítulo 7), y el estándar TCP/IP posibilitó la conexión de estas LANs en redes a nivel empresarial, que a su vez se conectaron a Internet.

**FIGURA 5-8 REDUCCIONES EXPONENCIALES EN LOS COSTOS DE LAS COMUNICACIONES EN INTERNET**



El crecimiento en la población de Internet se debe a la rápida reducción en los costos de conexión y comunicación en general de la misma. El costo por kilobit de acceso a Internet se redujo de manera exponencial desde 1995. La línea de suscriptor digital (DSL) y los módems de cable ahora ofrecen un kilobit de comunicación por un precio al menudeo de cerca de 2 centavos.

*Fuente:* Autores.

**TABLA 5-1 VARIOS ESTÁNDARES IMPORTANTES EN LA COMPUTACIÓN**

ESTÁNDAR	SIGNIFICADO
Código estándar estadounidense para el intercambio de información (ASCII) (1958)	Hizo posible que las computadoras de distintos fabricantes intercambiaran datos; se utilizó más adelante como el lenguaje universal para enlazar los dispositivos de entrada y salida como teclados y ratones a las computadoras. El Instituto Nacional Estadounidense de Estándares lo adoptó en 1963.
Lenguaje común orientado a negocios (COBOL) (1959)	Un lenguaje de software fácil de usar que expandió de manera considerable la habilidad de los programadores de escribir programas relacionados con negocios y redujo el costo del software. Fue patrocinado por el Departamento de Defensa en 1959.
Unix (1959 a 1975)	Un poderoso sistema operativo portable multitareas y multiusuario, que en un principio se desarrolló en Bell Labs (1969) y más tarde se liberó para que otros lo utilizaran (1975). Opera sobre una amplia variedad de computadoras de distintos fabricantes. Adoptado por Sun, IBM, HP y otros en la década de 1980, se convirtió en el sistema operativo más utilizado a nivel empresarial.
Protocolo de control de transmisión/Protocolo Internet (TCP/IP) (1974)	Suite de protocolos de comunicaciones y un esquema de direccionamiento común que permiten conectar millones de computadoras en una red global gigante (Internet). Más adelante se utilizó como la suite de protocolos de red predeterminada para las redes de área local y las intranets. Se desarrolló a principios de la década de 1970 para el Departamento de Defensa de Estados Unidos.
Ethernet (1973)	Un estándar de red para conectar computadoras de escritorio en redes de área local que permitió la adopción extendida de la computación cliente/servidor y las redes de área local; además estimuló la adopción de las computadoras personales.
Computadora personal IBM/Microsoft/Intel (1981)	El diseño Wintel estándar para la computación de escritorio personal, basada en los procesadores Intel estándar y en otros dispositivos estándar, Microsoft DOS y más adelante el software Windows. El surgimiento de este producto estándar de bajo costo estableció la base para un periodo de 25 años de crecimiento explosivo en el área de la computación, por todas las organizaciones en todo el mundo. En la actualidad, más de 1 mil millones de PCs están detrás de las actividades comerciales y gubernamentales a diario.
World Wide Web (1989 a 1993)	Los estándares para almacenar, recuperar, dar formato a la información y mostrarla como una red mundial de páginas electrónicas que incorporan texto, gráficos, audio y video permiten la creación de un almacén global de miles de millones de páginas Web.

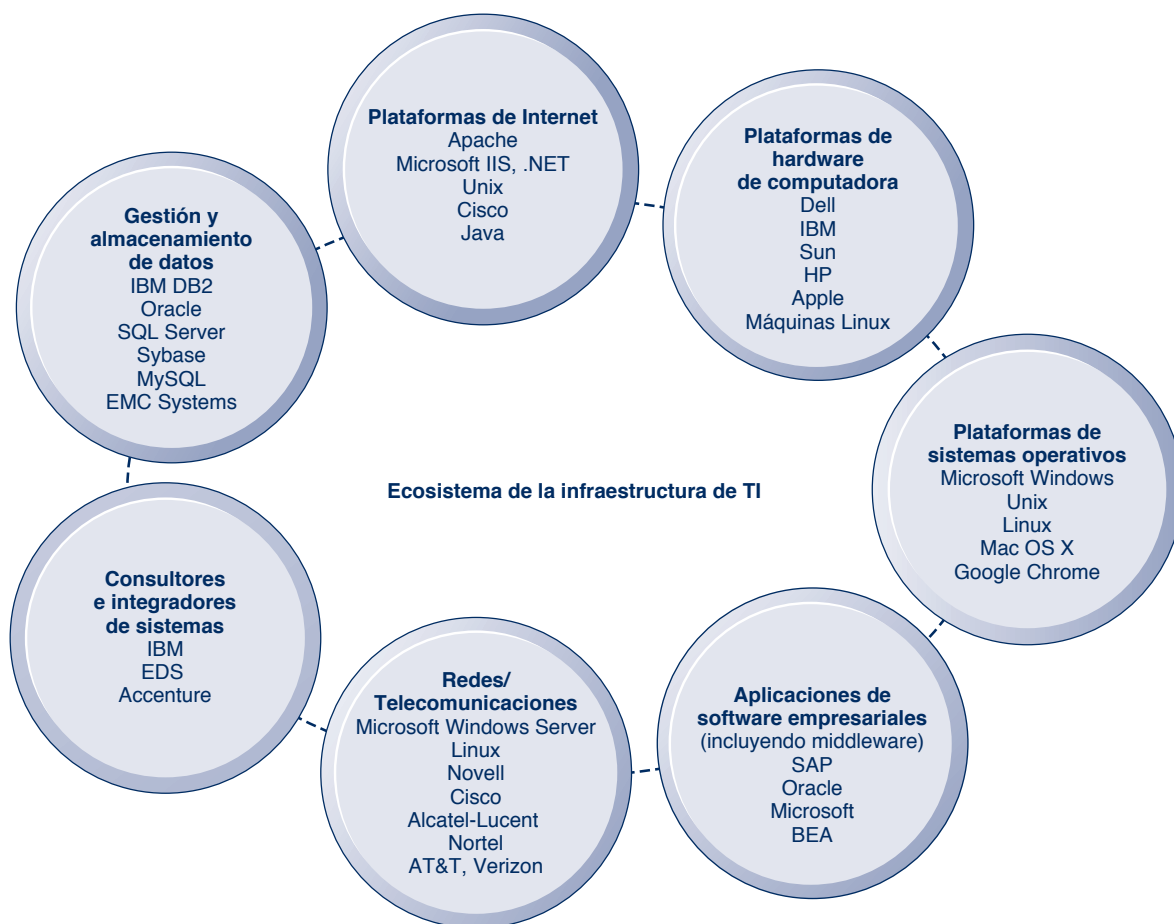
## 5.2 COMPONENTES DE LA INFRAESTRUCTURA

En la actualidad, la infraestructura de TI está compuesta de siete componentes principales. La figura 5-9 ilustra estos componentes y los principales distribuidores dentro de cada categoría. Estos componentes constituyen inversiones que se deben coordinar entre sí para proveer a la empresa una infraestructura coherente.

En el pasado, los distribuidores de tecnología que suministraban estos componentes competían entre sí con frecuencia, y ofrecían a las empresas compradoras una mezcla de soluciones parciales incompatibles y propietarias. Sin embargo, las empresas distribuidoras se han visto cada vez más obligadas por los clientes grandes a cooperar en sociedades estratégicas unas con otras. Por ejemplo, un proveedor de hardware y software como IBM coopera con todos los principales proveedores de software empresarial, tiene relaciones estratégicas con integradores de sistemas y promete trabajar con los productos de bases de datos que sus empresas clientes deseen usar (aun y cuando vende su propio software de gestión de bases de datos llamado DB2).

### PLATAFORMAS DE HARDWARE DE COMPUTADORA

En 2010, las empresas estadounidenses tenían planeado invertir cerca de \$109 mil millones en hardware de computadora. Que involucraba a máquinas cliente (PC de escritorio, dispositivos de computación móvil como netbook y laptop, pero no dispositivos iPhone ni BlackBerry) como máquinas servidor. En su mayoría, las máquinas

**FIGURA 5-9 EL ECOSISTEMA DE LA INFRAESTRUCTURA DE TI**

Hay siete componentes principales que se deben coordinar para proveer a la empresa una infraestructura de TI efectiva. Aquí se muestra una lista de las principales y de los proveedores para cada componente.

cliente usan microprocesadores Intel o AMD. En 2010 había un estimado de vender alrededor de 90 millones de PCs a clientes en Estados Unidos (400 millones en todo el mundo) (Gartner, 2010).

El mercado de los servidores utiliza en su mayoría procesadores Intel o AMD en forma de servidores blade en estantes, pero también incluye microprocesadores Sun SPARC y chips IBM POWER diseñados de manera especial para uso en servidores. Los **servidores blade**, que analizamos en el caso de apertura del capítulo, son computadoras ultradelgadas que consisten de un tablero de circuitos con procesadores, memoria y conexiones de red que se almacenan en estantes. Ocupan menos espacio que los servidores tradicionales en gabinete. El almacenamiento secundario se puede proporcionar mediante un disco duro en cada servidor blade o a través de unidades externas de almacenamiento masivo.

El mercado para el hardware de computadora se enfoca cada vez más en las principales empresas como IBM, HP, Dell y Sun Microsystems (adquirida por Oracle), y en tres productores de chips: Intel, AMD e IBM. La industria se decidió en forma colectiva por Intel como el procesador estándar, aunque hay importantes excepciones en el mercado de servidores para las máquinas Unix y Linux, que podrían usar procesadores Sun o IBM Unix.



Las mainframes no han desaparecido. En realidad su mercado ha crecido de manera estable durante la última década, aunque el número de proveedores se redujo a uno: IBM. Además, este proveedor readaptó sus sistemas mainframe para poder utilizarlos como servidores gigantes en redes empresariales masivas y sitios Web corporativos. Un solo mainframe de IBM puede ejecutar hasta 17 000 instancias de software Linux o Windows para servidor y es capaz de reemplazar a miles de servidores blade más pequeños (en la sección 5.3 hablaremos sobre la virtualización).

## PLATAFORMAS DE SISTEMAS OPERATIVOS

En 2010, Microsoft Windows se apoderó de cerca del 75 por ciento del mercado de sistemas operativos de servidor, en donde el 25 por ciento de los servidores corporativos utilizaron alguna forma del sistema operativo **Unix** o de **Linux**, un pariente de Unix de código fuente abierto, económico y robusto. Microsoft Windows Server es capaz de proveer un sistema operativo y servicios de red a nivel empresarial, y llama la atención de las organizaciones que buscan infraestructuras de TI basadas en Windows (IDC, 2010).

Unix y Linux son escalables, confiables y mucho menos costosos que los sistemas operativos de mainframe. También se pueden ejecutar en muchos tipos distintos de procesadores. Los principales proveedores de sistemas operativos Unix son IBM, HP y Sun, cada uno con versiones ligeramente distintas e incompatibles en ciertos aspectos.

A nivel cliente, el 90 por ciento de las PCs usan alguna forma de **sistema operativo** Microsoft Windows (como Windows 7, Windows Vista o Windows XP) para administrar los recursos y actividades de la computadora. Sin embargo, ahora hay una variedad mucho mayor de sistemas operativos que en el pasado, con nuevos sistemas operativos para la computación en dispositivos digitales móviles portátiles o computadoras conectadas a la nube.

El sistema **Chrome OS** de Google provee un sistema operativo ligero para la computación en la nube mediante el uso de netbooks. Los programas no se almacenan en la PC del usuario, sino que se utilizan a través de Internet y se accede a éstos por medio del navegador Web Chrome. Los datos de los usuarios residen en servidores esparcidos por Internet. Microsoft introdujo el sistema operativo *Windows Azure* para sus servicios y plataforma en la nube. **Android** es un sistema operativo móvil desarrollado por Android, Inc. (empresa que compró Google), y más tarde pasó a manos de la Alianza para los dispositivos móviles abiertos (Open Handset Alliance) como una plataforma para dispositivos móviles flexible y actualizable.

El software de sistema operativo cliente convencional está diseñado con base en el ratón y teclado, pero cada vez se vuelve más natural e intuitivo gracias al uso de la tecnología táctil. *iPhone OS*, el sistema operativo para los dispositivos Apple iPad, iPhone y iPod Touch cuya popularidad es fenomenal, tiene una interfaz **multitáctil** en la que los usuarios usan sus dedos para manipular objetos en la pantalla. La Sesión interactiva sobre tecnología explora las implicaciones de usar la tecnología multitáctil para interactuar con la computadora.

## APLICACIONES DE SOFTWARE EMPRESARIALES

Además del software para las aplicaciones utilizadas por grupos específicos o unidades de negocios, las empresas estadounidenses invirtieron cerca de \$165 mil millones en el año 2010 en software para aplicaciones empresariales que se tratan como componentes de la infraestructura de TI. En el capítulo 2 introdujimos los diversos tipos de aplicaciones empresariales; el capítulo 9 provee un análisis más detallado de cada uno de ellos.

Los proveedores más importantes de software de aplicaciones empresariales son SAP y Oracle (que adquirió PeopleSoft). En esta categoría también se incluye el software middleware que proveen los distribuidores tales como BEA, para obtener una integración a nivel empresarial mediante la vinculación de los sistemas de aplicaciones existentes de la empresa. Microsoft intenta entrar a los extremos inferiores de este mercado al enfocarse en las empresas pequeñas y de tamaño mediano que aún no han implementado aplicaciones empresariales.

## SESIÓN INTERACTIVA: TECNOLOGÍA

### NOVEDAD TÁCTIL

Cuando Steve Jobs demostró por primera vez “el pellizco” —el gesto de dos dedos para realizar acercamientos y alejamientos en las fotos y las páginas Web en el iPhone, no sólo sacudió la industria de los teléfonos móviles— todo el mundo digital se enteró. Las características multitáctiles del Apple iPhone dramatizaron nuevas formas de usar el tacto para interactuar con el software y los dispositivos.

Las interfaces táctiles no son nuevas. La gente las utiliza todos los días para recibir dinero de los cajeros automáticos o para registrarse en los vuelos en los quioscos de los aeropuertos. Los investigadores académicos y comerciales han estado trabajando en la tecnología multitáctil durante años. Lo que hizo Apple fue convertir la interfaz multitáctil en algo más emocionante y relevante, y la popularizó como lo hizo en la década de 1980 con el ratón y la interfaz gráfica de usuario (también se habían inventado en otra parte).

Las interfaces multitáctiles pueden llegar a ser más versátiles que las unitáctiles, ya que nos permiten usar uno o más dedos para realizar gestos especiales que manipulan listas u objetos en una pantalla sin necesidad de mover un ratón, oprimir botones, girar ruedas o pulsar teclas. Realizan distintas acciones dependiendo de cuántos dedos detecten y cuáles gestos realice el usuario. Los gestos multitáctiles son más fáciles de recordar que los comandos, ya que se basan en movimientos humanos arraigados que no se necesitan aprender, dicen los científicos.

La pantalla y el software multitáctiles del iPhone le permiten controlar todo con sólo usar sus dedos. Un panel debajo de la cubierta de cristal de la pantalla detecta el tacto mediante el uso de campos eléctricos. Después transmite esa información a una pantalla LCD debajo de éste. El software especial reconoce los múltiples puntos táctiles simultáneos (a diferencia de la pantalla unitáctil, que sólo reconoce un punto táctil). Usted se puede desplazar con rapidez hacia atrás y hacia delante a través de una serie de páginas Web o fotografías al “deslizar” o colocar tres dedos en la pantalla y moverlos con rapidez hacia los lados. Al pellizcar la imagen, puede encoger o expandir una foto.

Apple ha realizado un esfuerzo conjunto por ofrecer las características de la tecnología multitáctil en todas sus categorías de productos, pero muchas otras compañías de tecnología para el consumidor han adoptado la esta tecnología para algunos de sus productos. Synaptics, proveedor líder de almohadillas táctiles (touchpads) para fabricantes de laptops que compiten con Apple, ha anunciado que piensa incorporar varias características de la tecnología multitáctil en sus almohadillas táctiles.

El sistema operativo Windows 7 de Microsoft cuenta con características multitáctiles: al usar Windows 7 en una PC con pantalla táctil, es posible navegar por periódicos

en línea, hojear por los álbumes fotográficos y revolver tanto archivos como carpetas con sólo usar sus dedos. Para realizar un acercamiento sobre un objeto en la pantalla de una PC compatible con la tecnología multitáctil, puede colocar dos dedos en la pantalla y separarlos. Para hacer clic con el botón derecho sobre un archivo, hay que tocarlo con un dedo y golpear la pantalla con otro.

Varias PCs con Microsoft Windows tienen pantallas táctiles; unas cuantas laptops con Windows emulan algunas de las características multitáctiles de las computadoras y dispositivos portátiles Apple. La computadora Surface de Microsoft opera con Windows 7 y permite a sus clientes de negocios usar la tecnología multitáctil en una pantalla sobre una mesa. Los clientes de hoteles, casinos y tiendas al detalle podrán usar gestos multitáctiles con varios dedos para desplazarse alrededor de objetos digitales como fotografías, jugar y navegar a través de opciones de productos. La PC tipo tableta Dell Latitude XT utiliza la tecnología multitáctil, que es útil para las personas que no pueden manejar un ratón y desean la funcionalidad de una PC tradicional. En cambio, pueden usar un dedo o una plumilla. El sistema operativo Android para teléfonos inteligentes tiene soporte nativo para la interfaz multitáctil, y los teléfonos móviles como HTC Desire, Nexus One y Motorola Droid tienen esta capacidad.

Ahora Hewlett-Packard (HP) tiene computadoras laptops y de escritorio que usan tecnología táctil. Su computadora TouchSmart le permite usar dos dedos a la vez para manipular imágenes en la pantalla o hacer gestos en ella para designar comandos específicos sin usar punteros o barras de desplazamiento. Para mover un objeto, lo toca con un dedo y lo arrastra a su nueva ubicación. Al deslizar su dedo con suavidad hacia arriba o abajo, o incluso hacia los lados, se desplaza la pantalla.

La computadora TouchSmart hace posible que los usuarios domésticos se involucren en un nuevo tipo de computación casual: poner música mientras preparan la comida, buscar rápidamente indicaciones antes de salir de la casa o dejar memos escritos en video o audio para los miembros de la familia. Tanto los consumidores como las empresas han encontrado otros usos también. De acuerdo con Alan Reed, vicepresidente de HP y director general del departamento de Equipos empresariales de escritorio (Business Desktops), “Hay un potencial sin explotar en cuanto a la tecnología táctil en el mercado empresarial para involucrar a los usuarios de una manera que nunca se ha hecho antes”.

El Aeropuerto O'Hare de Chicago integró un grupo de PCs TouchSmart en quioscos para que los turistas exploren Chicago, en donde los visitantes pueden dar un vistazo en un Centro de visitantes virtual. Las computadoras TouchSmart ayudaron a un estudiante autista a hablar y comunicarse con otros por primera vez en los

14 años de su existencia. Sin usar el teclado y el ratón inalámbricos de la PC TouchSmart, los usuarios pueden sostener charlas en video con los trabajadores remotos a través de una cámara Web y micrófono integrados, acceder al correo electrónico e Internet, y administrar sus contactos, elementos de calendario y fotografías.

Las PCs con capacidad táctil también pueden atraer la atención de las escuelas primarias que busquen una computadora fácil de usar para los estudiantes de los primeros grados, o un dispositivo de información tipo quiosco que se pueda montar en la pared para los padres y visitantes. Los clientes podrían usar el tacto para colocar pedidos con un vendedor, realizar llamadas de servicio virtuales en video, o enseñar o usar las redes sociales para las empresas.

Es demasiado pronto para saber si la nueva interfaz multitáctil podrá ser tan popular como la interfaz grá-

fica de usuario controlada por un ratón. Aunque poner los dedos en la pantalla es la definición más reciente de “genial” en el mercado de los teléfonos celulares, aún no ha surgido una “aplicación revolucionaria” para la interfaz táctil en la PC. Sin embargo, ya es evidente que la tecnología táctil tiene verdaderas ventajas en los dispositivos en donde no es posible o conveniente usar un ratón, o cuando la interfaz de menús y carpetas muy antigua, es demasiado torpe.

**Fuentes:** Claire Cain Miller, “To Win Over Today’s Users, Gadgets Have to be Touchable”, *The New York Times*, 1 de septiembre de 2010; Katherine Boehret, “Apple Adds Touches to Its Mac Desktops”, *The Wall Street Journal*, 4 de agosto de 2010; Ashlee Vance, “Tech Industry Catches Its Breath”, *The New York Times*, 17 de febrero de 2010; Kathy Sandler, “The Future of Touch”, *The Wall Street Journal*, 2 de junio de 2009; Suzanne Robitaille, “Multitouch to the Rescue?” Suite101.com, 22 de enero de 2009, y Eric Lai, “HP Aims TouchSmart Desktop PC at Businesses”, *Computerworld*, 1 de agosto de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

## MIS EN ACCIÓN

1. ¿Qué problemas resuelve la tecnología multitáctil?
2. ¿Cuáles son las ventajas y desventajas de una interfaz multitáctil? ¿Qué tan útil es? Explique.
3. Describa tres aplicaciones empresariales que se beneficiarían de una interfaz multitáctil.
4. ¿Con qué aspectos de administración, organización y tecnología habría que lidiar si usted o su empresa estuvieran considerando sistemas y computadoras con interfaces multitáctil?

1. Describa lo que haría de manera distinta en su PC si tuviera capacidades multitáctiles. ¿Cuánta diferencia haría la tecnología multitáctil en cuanto a la forma en que usted utiliza su computadora?

## ADMINISTRACIÓN Y ALMACENAMIENTO DE DATOS

El software de gestión de bases de datos empresariales es responsable de organizar y administrar la información de la empresa, de modo que sea posible acceder a ella y utilizarla en forma eficiente. El capítulo 6 describe este software con detalle. Los principales proveedores de software de bases de datos son IBM (DB2), Oracle, Microsoft (SQL Server) y Sybase (Adaptive Server Enterprise), quienes proveen más del 90 por ciento del mercado de software de bases de datos en Estados Unidos. MySQL es un producto de bases de datos relacionales de código fuente abierto de Linux, que ahora pertenece a Oracle Corporation.

El mercado de almacenamiento físico de datos está dominado por EMC Corporation para los sistemas de gran escala, y un pequeño número de fabricantes de discos duros para PC encabezados por Seagate, Maxtor y Western Digital.

Se estima que la información digital aumenta a razón de 1.2 zettabytes al año. Todos los tweets, blogs, videos, correos electrónicos y mensajes publicados en Facebook, así como los datos corporativos tradicionales, equivalían en 2011 a varios miles de Bibliotecas del Congreso (EMC Corporation, 2010).

Debido a la cantidad de nueva información digital que aumenta vertiginosamente en el mundo, el mercado para los dispositivos de almacenamiento de datos digitales ha estado creciendo a más del 15 por ciento anual durante los últimos cinco años.

Además de las tradicionales matrices de discos y bibliotecas de cintas, las empresas grandes están recurriendo a las tecnologías de almacenamiento basadas en red. Las **redes de área de almacenamiento (SAN)** conectan varios dispositivos en una red separada de alta velocidad, dedicada al almacenamiento. La SAN crea una gran reserva central de almacenamiento disponible para que varios servidores accedan a ella y la compartan.

## PLATAFORMAS DE REDES/TELECOMUNICACIONES

Las empresas estadounidenses invirtieron \$100 mil millones al año en hardware de redes y telecomunicaciones, y la enorme cantidad de \$700 mil millones en servicios de red (que en su mayoría consistían en cargos de las compañías de telecomunicaciones y telefónicas por las líneas de voz y el acceso a Internet, lo cual no incluimos en este análisis). El capítulo 7 está dedicado a una descripción detallada del entorno de redes empresariales, abarcando Internet. Windows Server se utiliza de manera predominante como sistema operativo de red de área local, seguido de Linux y Unix. La mayor parte de las redes de área amplia empresariales extensas utilizan alguna variante de Unix. La mayoría de las redes de área local, así como las redes empresariales de área amplia, utilizan la suite de protocolos TCP/IP como estándar (vea el capítulo 7).

Los proveedores de hardware de red más importantes son Cisco, Alcatel-Lucent, Nortel y Juniper Networks. Por lo general, las compañías de servicios de telecomunicaciones/telefónicos que ofrecen conectividad de voz y datos, redes de área amplia, servicios inalámbricos y acceso a Internet son las que proveen las plataformas de telecomunicaciones. Entre los principales distribuidores de servicios de telecomunicaciones se encuentran AT&T y Verizon (vea el caso de apertura del capítulo 3). Este mercado se está disparando con nuevos proveedores de servicios inalámbricos celulares, Internet de alta velocidad y telefonía por Internet.

## PLATAFORMAS DE INTERNET

Las plataformas de Internet se traslapan y deben estar relacionadas con la infraestructura de redes general de la empresa, además de sus plataformas de hardware y software. Las empresas estadounidenses invirtieron cerca de \$40 mil millones al año en infraestructura relacionada con Internet. Estos gastos fueron de hardware, software y servicios administrativos para dar soporte al sitio Web de una empresa, que involucra servicios de hospedaje Web, enrutadores y cableado o equipo inalámbrico. Un **servicio de hospedaje Web** mantiene un servidor Web grande o una serie de servidores, además de proporcionar espacio a los suscriptores que pagan una cuota por mantener sus sitios Web.

La revolución de Internet creó una verdadera explosión en las computadoras tipo servidor, en donde muchas empresas poseen una colección de pequeños servidores para llevar a cabo sus operaciones en Internet. Desde entonces se produjo una presión constante para la consolidación de los servidores, para lo cual se reduce el número de computadoras servidores al incrementar el tamaño y poder de cada una. El mercado de los servidores de hardware de Internet cada vez se concentra más en las manos de IBM, Dell y HP/Compaq, puesto que los precios se han reducido en forma dramática.

Las principales herramientas y suites de desarrollo de aplicaciones de software Web las proveen Microsoft (Microsoft Expression Web, SharePoint Designer y la familia Microsoft .NET de herramientas de desarrollo); Oracle-Sun (Java de Sun es la herramienta más utilizada para desarrollar aplicaciones Web interactivas, tanto del lado servidor como del lado cliente), y una variedad de desarrolladores de software independientes, como Adobe (Flash y herramientas de texto como Acrobat) y Real Media (software de medios). En el capítulo 7 se describen con mayor detalle los componentes de la plataforma de Internet para empresas.



## SERVICIOS DE CONSULTORÍA E INTEGRACIÓN DE SISTEMAS

En la actualidad, ni siquiera una gran empresa tiene el personal, las habilidades, el presupuesto o la experiencia necesarios para implementar y mantener toda su infraestructura de TI. Para implementar una nueva infraestructura se requieren (como se indica en los capítulos 3 y 14) cambios considerables en los procesos y procedimientos de negocios, capacitación y educación, e integración de software. Las empresas líderes en consultoría que proveen esta experiencia son: Accenture, IBM Global Services, HP Enterprise Services, Infosys y Wipro Technologies.

Integración de software significa asegurar que la nueva infraestructura funcione con los sistemas anteriores de la empresa, conocidos como sistemas heredados, y también significa asegurar que los nuevos elementos de la infraestructura puedan trabajar en conjunto. Por lo general los **sistemas heredados** son sistemas de procesamiento de transacciones antiguos, creados para computadoras mainframe que se siguen utilizando para evitar el alto costo de reemplazarlos o rediseñarlos. El costo de reemplazar estos sistemas es prohibitivo y por lo general no es necesario si los antiguos se pueden integrar en una infraestructura contemporánea.

### 5.3 TENDENCIAS DE LAS PLATAFORMAS DE HARDWARE CONTEMPORÁNEAS

El explosivo poder de la tecnología de hardware de computadora y de redes ha cambiado drásticamente la forma en que las empresas organizan su poder de cómputo, al imponer una mayor parte de este poder en las redes y los dispositivos portátiles móviles. Ahora vamos a analizar siete tendencias de hardware: la plataforma digital móvil emergente, la computación en malla, la virtualización, la computación en la nube, la computación verde, los procesadores de alto rendimiento/ahorro de energía y la computación autónoma.

## LA PLATAFORMA DIGITAL MÓVIL EMERGENTE

En el capítulo 1 señalamos que han surgido nuevas plataformas de computación digital móviles como alternativas a las PCs y computadoras más grandes. Los teléfonos celulares y los inteligentes como BlackBerry y iPhone se han apropiado de muchas funciones de las computadoras portátiles, como la transmisión de datos, la navegación por Web, la transmisión de mensajes instantáneos y de correo electrónico, la visualización de contenido digital y el intercambio de datos con sistemas corporativos internos. La nueva plataforma móvil también incluye pequeñas subnotebooks ligeras y de bajo costo conocidas como **netbooks**, optimizadas para la comunicación inalámbrica y el acceso a Internet, con funciones de cómputo básicas tales como procesamiento de palabras; computadoras tipo tableta como el iPad, y lectores digitales de libros electrónicos como el Kindle de Amazon, con ciertas capacidades de acceso a Web.

En unos cuantos años, los teléfonos inteligentes, las netbooks y las computadoras tipo tableta serán los principales medios para acceder a Internet; cada vez más funciones de la computación empresarial pasarán de las PCs y los equipos de escritorio a estos dispositivos móviles. Por ejemplo, los ejecutivos de nivel superior en General Motors utilizan aplicaciones para teléfonos inteligentes que muestran los detalles sobre la información de ventas de vehículos, el desempeño financiero, la métrica de fabricación y el estado administrativo de los proyectos. En la empresa fabricante de dispositivos médicos de nombre Astra Tech, los representantes de ventas utilizan sus teléfonos inteligentes para acceder a las aplicaciones de administración de relaciones con el cliente (CRM) y los datos de las ventas en Salesforce.com, para verificar los datos sobre los productos vendidos y devueltos, así como las tendencias de ingresos en general antes de reunirse con los clientes.

## COMPUTACIÓN EN MALLA

La **computación en malla** se refiere al proceso de conectar computadoras separadas por límites geográficos en una sola red para crear una supercomputadora virtual, al combinar el poder computacional de todas las computadoras en la malla. La computación en malla se beneficia del hecho de que la mayoría de las computadoras utilizan sus unidades centrales de procesamiento en promedio sólo el 25 por ciento del tiempo para el trabajo que se les asigna, por lo cual estos recursos inactivos quedan disponibles para otras tareas de procesamiento. La computación en malla era imposible hasta que las conexiones de Internet de alta velocidad permitieron a las empresas conectar las máquinas remotas de una manera económica y desplazar enormes cantidades de datos.

La computación en malla requiere programas de software para controlar y asignar los recursos en la malla. El software cliente se comunica con una aplicación de software servidor. El cual divide los datos y el código de la aplicación en trozos que a su vez se reparten a las máquinas de la malla. Las máquinas cliente realizan sus tareas tradicionales mientras ejecutan aplicaciones de la malla en segundo plano.

El caso de negocios para usar computación en malla implica ahorros en el costo, velocidad en los cálculos y agilidad, como se indica en el caso de apertura del capítulo. Este caso muestra que, al ejecutar sus aplicaciones en servidores agrupados en una malla, BART eliminó los recursos de computadora que no se usaban, empleó los recursos existentes con más eficiencia y redujo tanto los costos como el consumo de energía.

## VIRTUALIZACIÓN

La **virtualización** es el proceso de presentar un conjunto de recursos de cómputo (como el poder de cómputo o el almacenamiento de datos) de modo que se pueda acceder a todos ellos en formas que no estén restringidas por la configuración física o la ubicación geográfica. La virtualización permite a un solo recurso físico (como un servidor o un dispositivo de almacenamiento) aparecer ante el usuario como varios recursos lógicos. Por ejemplo, un servidor o mainframe se puede configurar para ejecutar muchas instancias de un sistema operativo, de modo que actúe como muchas máquinas diferentes. La virtualización también permite que varios recursos físicos (como dispositivos de almacenamiento o servidores) aparezcan como un solo recurso lógico, como sería el caso con las redes de área de almacenamiento o la computación en malla. La virtualización hace posible que una compañía maneje su procesamiento y almacenamiento computacional mediante el uso de los recursos de cómputo alojados en ubicaciones remotas. VMware es el distribuidor líder en software de virtualización para servidores Windows y Linux. Microsoft ofrece su propio producto Virtual Server y tiene herramientas de virtualización integradas en la versión más reciente de Windows Server.

### Beneficios de la virtualización para las empresas

Al proveer la habilidad de alojar varios sistemas en una sola máquina física, la virtualización ayuda a las organizaciones a incrementar las tasas de uso del equipo, con lo cual conservan espacio en su centro de datos y usan menos energía. La mayoría de los servidores operan sólo a un 15 o 20 por ciento de su capacidad, por lo que la virtualización puede impulsar las tasas de uso hasta un 70 por ciento o más. Cuanto más grandes sean las tasas de uso, menores serán los componentes requeridos para procesar la misma cantidad de trabajo, como se ilustra mediante la experiencia de BART con la virtualización en el caso de apertura del capítulo.

Además de reducir los gastos en hardware y energía, la virtualización permite a las empresas ejecutar sus aplicaciones heredadas en versiones antiguas de un sistema operativo en el mismo servidor que las aplicaciones más recientes. La virtualización también facilita la centralización y consolidación de la administración del hardware. Ahora es posible para las compañías e individuos realizar todo su trabajo computacional mediante una infraestructura de TI virtualizada, como en el caso de la computación en la nube. Pasemos a continuación a este tema.

## COMPUTACIÓN EN LA NUBE

Al principio de este capítulo presentamos la computación en la nube, en donde las empresas y los individuos obtienen procesamiento computacional, almacenamiento, software y otros servicios como una reserva de recursos virtualizados a través de una red, principalmente Internet. Estos recursos se ponen a disposición de los usuarios con base en sus necesidades, sin importar su ubicación física o la de los mismos usuarios. El Instituto nacional estadounidense de estándares y tecnología (NIST) define la computación en la nube como algo que contiene las siguientes características esenciales (Mell y Grance, 2009):

- **Autoservicio bajo demanda:** los individuos pueden obtener herramientas computacionales, como tiempo del servidor o almacenamiento de red por su propia cuenta.
- **Acceso ubicuo a la red:** los individuos pueden usar dispositivos de red e Internet estándar, incluyendo las plataformas móviles, para acceder a los recursos de la nube.
- **Agrupamiento de recursos independiente de la ubicación:** los recursos de cómputo se agrupan para dar servicio a varios usuarios; los distintos recursos virtuales se asignan en forma dinámica de acuerdo con la demanda de los usuarios. Por lo general el usuario no sabe en dónde se encuentran los recursos de cómputo.
- **Elasticidad rápida:** los recursos de cómputo se pueden suministrar, incrementar o reducir con rapidez para satisfacer la demanda cambiante de los usuarios.
- **Servicio medido:** los cargos por los recursos de la nube se basan en la cantidad de recursos utilizados.

La computación en la nube consiste en tres tipos distintos de servicios:

- **Infraestructura en la nube como un servicio:** los clientes utilizan el procesamiento, el almacenamiento, la conexión en red y otros recursos de cómputo de los proveedores de servicio en la nube para operar sus sistemas de información. Por ejemplo, Amazon utiliza la capacidad libre de su infraestructura de TI para proveer un entorno en la nube con una amplia base para vender servicios de infraestructura de TI. Entre estos servicios están el servicio de almacenamiento simple (S3) para almacenar los datos de sus clientes y el servicio en la Nube de cómputo elástica (EC2) para ejecutar sus aplicaciones. Los usuarios pagan sólo por la cantidad de cómputo y capacidad de almacenamiento que utilizan.
- **Plataforma en la nube como un servicio:** los clientes usan la infraestructura y las herramientas de programación hospedadas por el proveedor de servicios para desarrollar sus propias aplicaciones. Por ejemplo, IBM ofrece el servicio de desarrollo y prueba de aplicaciones de negocios inteligentes para desarrollar y probar software en el entorno IBM Cloud. Otro ejemplo es el sitio Force.com de Salesforce.com, que describimos en el caso de estudio al final del capítulo, el cual permite a los desarrolladores crear aplicaciones que se alojen en sus servidores como un servicio.
- **Software en la nube como un servicio:** los clientes usan el software que el distribuidor aloja en su hardware y ofrece a través de una red. Algunos de los principales ejemplos son Google Apps, que provee aplicaciones empresariales comunes en línea y Salesforce.com, que también renta sistemas CRM y servicios de software relacionados a través de Internet. Ambos cobran a los usuarios una cuota anual de suscripción, aunque Google Apps también cuenta con una versión gratuita con funcionalidad reducida. Los usuarios acceden a estas aplicaciones desde un navegador Web; los datos y el software se mantienen en los servidores remotos de los proveedores.

Una nube puede ser privada o pública. Una **nube pública** se mantiene a través un proveedor de servicios externo, como Amazon Web Services; se puede acceder a ella por medio de Internet y está disponible para el público en general. Una **nube privada** es una red propietaria o un centro de datos propietario que enlaza servidores, almacenamiento, redes, datos y aplicaciones como un conjunto de servicios virtualizados que los usuarios comparten dentro de una compañía. Al igual que las nubes públicas, las nubes privadas pueden asignar almacenamiento, poder de cómputo u



otros recursos de manera transparente para proveer recursos de cómputo según sean necesarios. Es probable que las instituciones financieras y los proveedores de servicios médicos graviten hacia las nubes, ya que estas organizaciones manejan muchos datos financieros y personales delicados. En el capítulo 8 analizaremos los aspectos de seguridad de las nubes.

Como las organizaciones que utilizan computación en la nube por lo general no son propietarias de la infraestructura, no tienen que realizar grandes inversiones en su propio hardware y software. En cambio, compran sus servicios de cómputo a los proveedores remotos y pagan sólo por la cantidad de poder de cómputo que utilizan en realidad (**computación utilitaria**), o se les cobra una suscripción mensual o anual. El término **computación bajo demanda** también se utiliza para describir dichos servicios.

Por ejemplo, Envoy Media Group, una empresa de marketing directo que ofrece campañas de medios muy especializadas a través de varios canales como TV, radio e Internet, aloja toda su presencia Web en Azimuth Web Services. La estructura de precios tipo "pague a medida que consuma" permite a la compañía agregar servidores con rapidez y sin problemas en donde se requieran, sin necesidad de invertir grandes sumas en hardware. La computación en la nube redujo los costos cerca de un 20 por ciento, debido a que Envoy ya no tenía que dar mantenimiento a su propio hardware ni requería personal de TI.

Sin embargo, la computación en la nube tiene ciertas desventajas. A menos que los usuarios tomen las precauciones necesarias para almacenar sus datos en forma local, la responsabilidad del almacenamiento y control de los datos está en las manos del proveedor. Algunas compañías se preocupan en cuanto a los riesgos de seguridad que surgen al confiar sus datos y sistemas críticos a un distribuidor externo que también trabaja con otras compañías. También hay dudas en cuanto a la confiabilidad del sistema. Las empresas esperan que sus sistemas estén disponibles 24/7 y no desean sufrir ninguna pérdida de capacidad de negocios en caso de que fallen sus infraestructuras de TI. Cuando la nube de Amazon dejó de funcionar en diciembre de 2009, los suscriptores en la costa este de Estados Unidos no pudieron utilizar sus sistemas por varias horas. Otra limitación de la computación en la nube es la posibilidad de que los usuarios se hagan dependientes del proveedor de este servicio.

Existen algunos que creen que la computación en la nube representa un cambio radical en cuanto a la forma en que las corporaciones realizarán sus actividades de cómputo, a medida que la computación de negocios se desplace de los centros de datos privados hacia los servicios de la nube (Carr, 2008). Esto sigue siendo cuestión de debate. La computación en la nube es más atractiva a corto plazo para las empresas pequeñas y de tamaño mediano que carecen de los recursos para comprar y poseer su propio hardware y software. No obstante, las corporaciones extensas tienen enormes inversiones en sistemas propietarios complejos que dan soporte a los procesos únicos de negocios, algunos de los cuales les proporcionan ventajas estratégicas. Para ellas, el escenario más probable es un modelo de computación híbrido en donde las empresas usan su propia infraestructura para sus actividades básicas más esenciales y adoptan la computación en la nube pública para sistemas menos críticos o para obtener una capacidad de procesamiento adicional durante los periodos de negocios pico. La computación en la nube desplazará en forma gradual a las empresas, desde tener una capacidad de infraestructura fija hasta llegar a una infraestructura más flexible, en donde una parte de esta infraestructura pertenezca a la empresa y la otra se rente a los centros de cómputo gigantes que pertenezcan a los distribuidores de hardware de computadora.

## COMPUTACIÓN VERDE

Al frenar la proliferación de hardware y el consumo de energía, la virtualización se ha convertido en una de las principales tecnologías para promover la computación verde. La **computación verde**, o **TI verde**, se refiere a las prácticas y tecnologías para diseñar, fabricar, usar y disponer de computadoras, servidores y dispositivos asociados, como

monitores, impresoras, dispositivos de almacenamiento, sistemas de redes y comunicaciones para minimizar el impacto sobre el entorno.

Reducir el consumo de poder de cómputo ha sido una prioridad “verde” muy alta. A medida que las compañías implementan cientos o miles de servidores, muchas invierten casi la misma cantidad en electricidad para energizar y enfriar sus sistemas que en hardware. La Agencia de Protección Ambiental de Estados Unidos estima que los centros de datos utilizarán más del 2 por ciento de toda la energía eléctrica de ese país para el año 2011. Se cree que la tecnología de la información contribuirá con cerca del 2 por ciento de los gases de invernadero del mundo. La reducción del consumo de energía en los centros de datos se ha convertido tanto en un asunto serio como en un desafío ambiental. La Sesión interactiva sobre organizaciones examina este problema.

## COMPUTACIÓN AUTONÓMICA

Con los sistemas extensos que abarcan muchos miles de dispositivos en red, los sistemas de computadora se han vuelto tan complejos en la actualidad que algunos expertos piensan que será imposible administrarlos en el futuro. Una metodología para lidiar con este problema es emplear la computación autónoma. La **computación autónoma** es un esfuerzo a nivel industrial por desarrollar sistemas que se puedan configurar, optimizar, ajustar, arreglarse por sí solos cuando se descompongan y protegerse de los intrusos externos y de la autodestrucción.

Podemos vislumbrar unas cuantas de estas capacidades en los sistemas de escritorio. Por ejemplo, el software de protección antivirus y de firewall puede detectar virus en las computadoras, vencerlos de manera automática y alertar a los operadores. Estos programas se pueden actualizar de manera automática según sea necesario, al conectarse a un servicio de protección de virus en línea tal como McAfee. IBM y otros distribuidores están empezando a integrar herramientas autónomas a sus productos para los sistemas grandes.

## PROCESADORES DE ALTO RENDIMIENTO Y AHORRO DE ENERGÍA

Otra forma de reducir los requerimientos de energía y la expansión descontrolada del hardware es mediante el uso de procesadores más eficientes y ahorradores de energía. Ahora los microprocesadores contemporáneos cuentan con varios núcleos de procesadores (que llevan a cabo la lectura y ejecución de las instrucciones de computadora) en un solo chip. Un **procesador multinúcleo** es un circuito integrado al que se conectan dos o más núcleos de procesadores para mejorar el desempeño, reducir el consumo de energía y procesar varias tareas simultáneas con más eficiencia. Esta tecnología permite que dos o más motores de procesamiento con requerimientos de energía y disipación de calor reducidos realicen tareas con más rapidez que un chip que requiere de muchos recursos y que sólo contiene un núcleo de procesamiento. En la actualidad es común encontrar procesadores de doble núcleo (dual-core) y cuádruple núcleo (quad-core) en las PCs y servidores con procesadores de 8, 10, 12 y 16 núcleos.

Intel y otros fabricantes de chips han desarrollado también microprocesadores que minimizan el consumo de energía. El bajo consumo de energía es esencial para prolongar la vida de la batería en los teléfonos inteligentes, las computadoras Netbook y otros dispositivos digitales móviles. Ahora es común encontrar microprocesadores con alta eficiencia en el uso de energía, como ARM, el procesador A4 de Apple y el Atom de Intel en las computadoras Netbook, reproductores de medios digitales y teléfonos inteligentes. El procesador A4 que se utilizó en la versión más reciente de los dispositivos iPhone y iPad consume entre 500 y 800 miliwatts de energía, entre 1/50 y 1/30 parte del consumo de energía de un procesador de doble núcleo en una laptop.

## SESIÓN INTERACTIVA: ORGANIZACIONES

### ¿ES BUENA LA COMPUTACIÓN VERDE PARA LAS EMPRESAS?

Las salas de computadoras se están calentando tanto que es muy difícil administrarlas. Las tareas que requieren muchos datos, como el video bajo demanda, la descarga de música, el intercambio de fotos y el mantenimiento de sitios Web necesitan máquinas que consumen cada vez más energía. Los costos de energía y enfriamiento para los centros de datos se han disparado a más del 800 por ciento desde 1996, y se pronostica que los centros de datos empresariales en Estados Unidos invertirán dos veces más en costos de energía que en hardware durante los siguientes cinco años.

El calor que se genera de las salas llenas de servidores está provocando que el equipo falle. Algunas organizaciones invierten más dinero para mantener sus centros de datos fríos que en rentar la propiedad en sí. Es un ciclo vicioso, ya que las compañías deben pagar para energizar sus servidores, y después para mantenerlos fríos y funcionando. Para enfriar un servidor se requiere casi la misma cantidad de kilowatts de energía que para operarlo. Todo este consumo de energía adicional tiene un impacto negativo sobre el entorno, además de los costos de operación corporativos.

Algunas de las empresas más prominentes del mundo están haciendo frente a sus problemas de consumo de energía con un ojo puesto en el tema de cómo salvar el entorno y el otro en cómo ahorrar dólares. Google y Microsoft están construyendo centros de datos que aprovechan la energía hidroeléctrica. Hewlett-Packard trabaja en una serie de tecnologías para reducir el impacto ecológico de los centros de datos en un 75 por ciento y, con nuevos servicios y software, medir el uso de energía y las emisiones de carbono. Redujo sus costos de energía entre un 20 y 25 por ciento por medio de la consolidación de los servidores y centros de datos.

El centro de datos de Microsoft en San Antonio implementa sensores que miden casi todo el consumo de energía, recicla el agua que se utiliza en el enfriamiento y usa software de gestión de energía desarrollado en forma interna. Microsoft también está tratando de fomentar las prácticas de software para ahorrar energía al cobrar a las unidades de negocios la cantidad de energía que consumen en la captura de datos, en vez del espacio que ocupan en el piso.

Ninguna de estas compañías puede afirmar que sus esfuerzos salvarán al mundo, pero lo que sí demuestran es que reconocen un problema cada vez mayor, junto con el comienzo de la era de la computación verde. Y como la tecnología y los procesos de estas empresas son más eficientes que los de otras compañías, usar sus servicios de software en línea en vez del software interno también puede contar como una inversión verde.

Por lo general las PCs permanecen encendidas más del doble del tiempo del que en realidad se utilizan. De

acuerdo con un informe de la Alianza para Ahorrar Energía (Alliance to Save Energy), una compañía con 10 000 escritorios con computadoras personales invertirá más de \$165 000 al año en facturas de electricidad si estas máquinas se dejan encendidas toda la noche. El grupo estima que esta práctica está desperdiciando alrededor de \$1.7 mil millones cada año, tan sólo en Estados Unidos.

Aunque muchas compañías establecen opciones pre-determinadas de administración de energía en las PCs, cerca del 70 por ciento de los empleados desactivan estas opciones. El software de administración de energía de PC de BigFix, 1E NightWatchman y Verdiem bloquea las opciones de energía y enciende las PCs de manera automática justo antes de que lleguen los empleados a trabajar en la mañana.

Las escuelas públicas del condado de Miami-Dade recortaron el tiempo que sus PCs estaban encendidas de 21 a 10.3 horas al día, mediante el uso de BigFix para controlar de manera central las opciones de energía de sus PCs. City University de Nueva York adoptó el software Surveyor de Verdiem para apagar sus 20 000 PCs cuando están inactivas durante la noche. Surveyor ha recortado un 10 por ciento de las facturas de energía de CUNY, con lo cual ha creado un ahorro anual aproximado de \$320 000.

La virtualización es una herramienta muy efectiva para una computación verde rentable, ya que reduce el número de servidores y recursos de almacenamiento en la infraestructura de TI de la empresa. El condado de Fulton en Georgia, que provee servicios para 988 000 ciudadanos, escudriña el uso de la energía al comprar nueva tecnología de la información. Utiliza el software de virtualización VMWare y una nueva plataforma de servidor blade Fujitsu para consolidar los servidores heredados de poco uso, de modo que una máquina desempeñe el trabajo que anteriormente realizaban ocho, con lo cual se ahorraron \$44 000 al año en costos de energía. Estos esfuerzos también crearon una infraestructura de TI más actualizada.

Los expertos señalan que es importante para las compañías medir su uso de energía y llevar un inventario y el registro de sus activos de tecnología de la información, tanto antes como después de empezar con sus iniciativas de ecología. Normalmente, la métrica que utilizan tanto Microsoft como otras empresas involucra la efectividad en el uso de la energía, la eficiencia de la infraestructura de los centros de datos y la eficacia de los datos promedio.

No siempre es necesario comprar nuevas tecnologías para lograr metas "verdes". Las organizaciones pueden obtener eficiencias considerables al administrar mejor los recursos de cómputo con los que ya cuentan.

En un principio, la aseguradora de servicios médicos Highmark quería aumentar el uso de su CPU en un 10 por ciento y reducir a la vez el uso de energía en un 5 por ciento, hasta alcanzar el 10 por ciento en un momento dado. Cuando la compañía realizó un inventario de todos sus activos de tecnología de la información, descubrió que su personal de sistemas de información dependía de servidores “muertos” que no desempeñaban ninguna función, pero seguían consumiendo energía. Por desgracia, muchos departamentos de sistemas de información aún no implementan sus recursos de tecnología de una manera eficiente, ni utilizan herramientas de medición ecológicas.

Tal vez también se necesiten programas para educar a los empleados en cuanto a la conservación de energía.

Además de usar herramientas de monitoreo de energía, Honda Motor Corporation capacita a los administradores de su centro de datos para usar la energía con más eficiencia. Por ejemplo, les enseñó a retirar con rapidez el equipo comisionado que no estaba en uso y a utilizar las herramientas administrativas para asegurar que los servidores se estén optimizando.

**Fuentes:** Kathleen Lao, “The Green Issue”, *Computerworld Canada*, abril de 2010; Matthew Sarrell, “Greening Your Data Center: The Real Deal”, *eWeek*, 15 de enero de 2010; Robert L. Mitchell, “Data Center Density Hits the Wall”, *Computerworld*, 21 de enero de 2010; Jim Carlton, “The PC Goes on an Energy Diet”, *The Wall Street Journal*, 8 de septiembre de 2009, y Ronan Kavanagh, “IT Virtualization Helps to Go Green”, *Information Management Magazine*, marzo de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

1. ¿Qué problemas de negocios y sociales provoca el consumo de energía en los centros de datos?
2. ¿Qué soluciones hay disponibles para estos problemas? ¿Cuáles son amigables para el entorno?
3. ¿Cuáles son los beneficios de negocios y los costos de estas soluciones?
4. ¿Es conveniente para todas las empresas migrar a la computación verde? ¿Por qué sí o por qué no?

## MIS EN ACCIÓN

Realice una búsqueda en Internet sobre la frase “computación verde” y luego responda a las siguientes preguntas:

1. ¿Quiénes son algunos de los líderes del movimiento de computación verde? ¿Qué corporaciones van a la cabeza? ¿Qué organizaciones ambientales desempeñan un papel importante?
2. ¿Cuáles son las tendencias más recientes en la computación verde? ¿Qué tipo de impacto están teniendo?
3. ¿Qué pueden hacer los individuos para contribuir al movimiento de la computación verde? ¿Vale la pena el movimiento?

## 5.4 TENDENCIAS DE LAS PLATAFORMAS DE SOFTWARE CONTEMPORÁNEAS

Hay cuatro temas importantes en la evolución de las plataformas de software contemporáneas:

- Linux y el software de código fuente abierto
- Java y Ajax
- Los servicios Web y la arquitectura orientada a servicios
- Outsourcing de software y servicios de la nube

### LINUX Y EL SOFTWARE DE CÓDIGO FUENTE ABIERTO

El **software de código abierto** es software producido por una comunidad de varios cientos de miles de programadores en todo el mundo. De acuerdo con la principal asociación profesional de código abierto, OpenSource.org, el software de código abierto es gratis y los usuarios pueden modificarlo. Las obras derivadas del trabajo original también deben ser gratuitas, además de que el usuario puede redistribuir el software sin necesidad de licencias adicionales. Por definición, el software de código abierto no está restringido a ningún sistema operativo o tecnología de hardware específico, aunque en



la actualidad la mayor parte del software de código abierto se basa en un sistema operativo Linux o Unix.

El movimiento de código abierto ha estado en evolución durante más de 30 años y ha demostrado que puede producir software de alta calidad, aceptable en el entorno comercial. Entre las herramientas populares de software de código abierto se encuentran el sistema operativo Linux, el servidor Web HTTP Apache, el navegador Web Mozilla Firefox y la suite de productividad de escritorio Open Office de Oracle. Las herramientas de código abierto se utilizan en netbooks como alternativas económicas de Microsoft Office. Los principales distribuidores de hardware y software, como IBM, HP, Dell, Oracle y SAP, ahora ofrecen versiones de sus productos compatibles con Linux. En las Trayectorias de aprendizaje de este capítulo encontrará más información sobre la definición de código abierto de la iniciativa de código abierto y sobre la historia del software de código abierto.

## Linux

Tal vez el software de código abierto más popular sea Linux, un sistema operativo relacionado con Unix. Linux fue creado por el programador finlandés Linus Torvalds, quien lo publicó por primera vez en Internet en agosto de 1991. Las aplicaciones de Linux están incrustadas en teléfonos celulares, teléfonos inteligentes, netbooks y productos electrónicos para el consumidor. Linux está disponible en versiones gratuitas que se pueden descargar de Internet, o en versiones comerciales de bajo costo que incluyen herramientas y soporte de distribuidores como Red Hat.

Aunque Linux no se utiliza en muchos sistemas de escritorio, es una fuerza importante en las redes de área local, los servidores Web y el trabajo de cómputo de alto desempeño, con más del 20 por ciento del mercado de sistemas operativos para servidores. IBM, HP, Intel, Dell y Oracle-Sun han hecho de Linux una parte central de los servicios y productos que ofrecen a las corporaciones.

El surgimiento del software de código abierto, en especial Linux y las aplicaciones que soporta, tiene profundas implicaciones para las plataformas de software corporativas: reducción en costo, confiabilidad y resistencia, e integración, ya que Linux funciona en todas las principales plataformas de hardware, tanto en mainframes como en servidores y clientes.

## SOFTWARE PARA WEB: JAVA Y AJAX

**Java** es un lenguaje de programación orientado a objetos independiente del sistema operativo e independiente del procesador, que se ha convertido en el principal entorno interactivo para Web. Java fue creado por James Gosling y el Equipo Green en Sun Microsystems, en 1992. El 13 de noviembre de 2006, Sun liberó gran parte de Java como software de código abierto bajo los términos de la licencia pública general (GPL) de GNU, y completó el proceso el 8 de mayo de 2007.

La plataforma de Java ha migrado a los teléfonos celulares, teléfonos inteligentes, automóviles, reproductores de música, máquinas de juegos y por último, a los decodificadores en los sistemas de televisión por cable para ofrecer contenido interactivo y servicios de pago por evento. El software de Java está diseñado para ejecutarse en cualquier computadora o dispositivo de cómputo, sin importar el microprocesador o sistema operativo específico que utilice el dispositivo. Para cada uno de los entornos en los que se utiliza Java, Sun creó una máquina virtual de Java (JVM) que interpreta el código programación de Java para ese equipo específico. De esta forma, el código se escribe una vez y se puede utilizar en cualquier máquina para la que exista una máquina virtual de Java.

Los desarrolladores de Java pueden crear pequeños programas en forma de applets, que se incrustan en las páginas Web y se descargan para ejecutarlos en un navegador Web. Un **navegador Web** es una herramienta de software fácil de usar con una interfaz gráfica de usuario para mostrar páginas Web y acceder tanto a Web como a otros recursos en Internet. Los navegadores Microsoft Internet Explorer, Mozilla Firefox y Google Chrome son algunos ejemplos. A nivel empresarial, Java se utiliza para aplicaciones de comercio electrónico y negocios electrónicos más complejos que requieren

comunicación con los sistemas de procesamiento de transacciones del back-end de una organización.

Ajax

¿Alguna vez, debido a un error ha tenido que volver a llenar un formulario de pedidos Web tras una larga espera por una nueva página del formulario? ¿O ha visitado un sitio de mapas y ha tenido que esperar un buen tiempo a que se cargue una nueva página después de haber hecho un clic sobre la flecha Norte? **Ajax** (JavaScript asíncrono y XML) es otra técnica de desarrollo Web para crear aplicaciones Web interactivas que evita toda esta inconveniencia.

Ajax permite que un cliente y un servidor intercambien pequeñas piezas de datos tras bambalinas, de modo que no haya que volver a cargar toda una página Web cada vez que el usuario solicite una modificación. De esta forma, si usted hace clic en la flecha Norte en un sitio de mapas, como Google Maps, el servidor descarga sólo esa parte de la aplicación que cambia sin necesidad de esperar un mapa totalmente nuevo. También puede manipular mapas en aplicaciones de éstos y moverlos en cualquier dirección sin necesidad de que se vuelva a cargar toda la página completa. Ajax usa programas de JavaScript que se descargan en su equipo cliente para mantener una conversación casi continua con el servidor que utiliza, con lo cual la experiencia del usuario es más fluida y uniforme.

LOS SERVICIOS WEB Y LA ARQUITECTURA ORIENTADA A SERVICIOS

Los **servicios Web** se refieren a un conjunto de componentes de software con acoplamiento débil, que intercambian información entre sí mediante el uso de estándares y lenguajes de comunicación Web universales. Pueden intercambiar información entre dos sistemas distintos, sin importar los sistemas operativos o lenguajes de programación en los que se basen esos sistemas. Se pueden utilizar para crear aplicaciones basadas en Web con estándares abiertos que vinculen sistemas de dos organizaciones distintas, y también se pueden usar para crear aplicaciones que vinculen sistemas dispares dentro de una sola compañía. Los servicios Web no están atados a ningún sistema operativo o lenguaje de programación específico; además, distintas aplicaciones los pueden utilizar para comunicarse entre sí de una manera estándar, sin necesidad de codificación personalizada que consuma mucho tiempo.

La tecnología base para los servicios Web es **XML**, que significa **lenguaje de marcado extensible**. Este lenguaje fue desarrollado en 1996 por el Consorcio World Wide Web (W3C, la organización internacional que supervisa el desarrollo de Web) como lenguaje de marcado más poderoso y flexible que el de hipertexto (HTML) para las páginas Web. El **lenguaje de marcado de hipertexto (HTML)** es un lenguaje de descripción de páginas para especificar cómo se deben colocar el texto, los gráficos, el video y el sonido en un documento de página Web. Mientras que el HTML se limita a describir cómo se deben presentar los datos en forma de páginas Web, XML puede realizar la presentación, comunicación y almacenamiento de datos. En XML, un número no es tan sólo una cifra; la etiqueta de XML especifica si ésta representa un precio, una fecha o un código postal. La tabla 5-2 ilustra algunas instrucciones de XML de ejemplo.

TABLA 5-2 EJEMPLOS DE XML

ESPAÑOL COMÚN	XML
Subcompacto	<TIPOAUTOMOVIL="Subcompacto">
4 pasajeros	<PASAJERO UNIDAD="PAS">4</PASAJERO>
\$16 800	<PRECIO MONEDA="USD">\$16 800</PRECIO>

Al etiquetar elementos seleccionados del contenido de documentos con base en su significado, XML hace posible que las computadoras manipulen e interpreten sus datos de manera automática y realicen operaciones sobre éstos sin necesidad de intervención humana. Los navegadores Web y los programas de computadora, como el software de procesamiento de pedidos o de planificación de recursos empresariales (ERP), pueden seguir reglas programadas para aplicar y desplegar los datos. XML provee un formato estándar para el intercambio de datos, lo cual permite a los servicios Web pasar datos de un proceso a otro.

Los servicios Web se comunican por medio de mensajes de XML a través de protocolos Web estándar. SOAP, que significa *Protocolo de Acceso Simple a Objetos*, es un conjunto de reglas para estructurar mensajes que permite a las aplicaciones pasarse datos e instrucciones entre sí. WSDL significa *Lenguaje de Descripción de Servicios Web*; es un marco de trabajo común para describir las tareas realizadas por un servicio Web junto con los comandos y datos que aceptará, de modo que otras aplicaciones puedan usarlo. UDDI, que significa *Descripción, Descubrimiento e Integración Universal*, permite listar un servicio Web en un directorio de servicios Web de modo que se pueda localizar con facilidad. Las empresas descubren y localizan los servicios Web a través de este directorio en forma muy similar a como lo harían los servicios en las páginas amarillas de un directorio telefónico. Mediante el uso de estos protocolos, una aplicación de software se puede conectar con libertad a otras sin necesidad de utilizar programación personalizada para cada aplicación diferente con la que desee comunicarse. Todos comparten los mismos estándares.

La colección de servicios Web que se utilizan para construir los sistemas de software de una empresa constituye lo que se conoce como una **Arquitectura Orientada al Servicio (SOA)**: un conjunto de servicios autocontenidos que se comunican entre sí para crear una aplicación de software funcional. Las tareas de negocios se realizan mediante la ejecución de una serie de estos servicios. Los desarrolladores de software reutilizan estos servicios en otras combinaciones para ensamblar otras aplicaciones, según sea necesario.

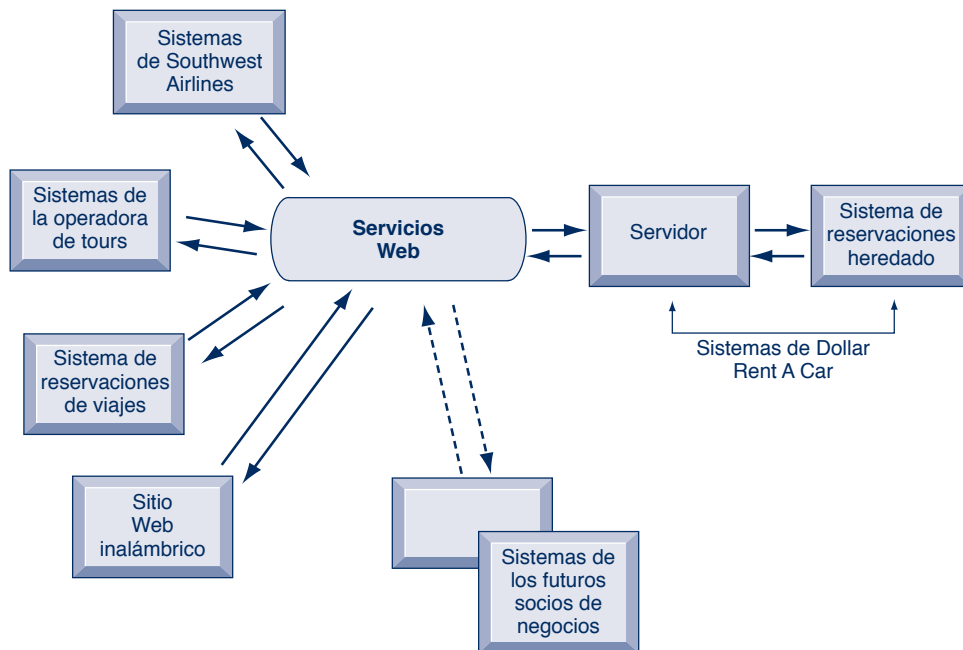
Casi todos los principales distribuidores de software proveen herramientas y plataformas completas para crear e integrar aplicaciones de software mediante el uso de servicios Web. IBM incluye herramientas de servicios Web en su plataforma de software de negocio electrónico WebSphere, y Microsoft incorporó herramientas de servicios Web en su plataforma Microsoft .NET.

Los sistemas de Dollar Rent A Car utilizan servicios Web para su sistema de reservaciones en línea con el sitio Web de Southwest Airlines. Aunque los sistemas de ambas compañías se basan en distintas plataformas de tecnología, una persona que reserve un vuelo en Southwest.com puede reservar un auto de Dollar sin tener que salir del sitio Web de la aerolínea. En vez de luchar por lograr que el sistema de reservaciones comparta datos con los sistemas de información de Southwest, Dollar utilizó la tecnología de servicios Web de Microsoft .NET como intermediario. Las reservaciones de Southwest se traducen en protocolos de servicios Web, que a su vez se traducen en formatos que las computadoras de Dollar puedan entender.

Otras compañías de renta de autos ya habían enlazado con anterioridad sus sistemas de información con los sitios Web de aerolíneas. Sin embargo, sin los servicios Web, había que construir cada una de estas conexiones a la vez. Los servicios Web proveen una manera estándar para que todas las computadoras de Dollar "hablen" con los sistemas de información de otras compañías sin tener que construir vínculos especiales con cada uno de ellos. Ahora Dollar está expandiendo su uso de los servicios Web para enlazarse de manera directa con los sistemas de una pequeña operadora de tours y un sistema grande de reservaciones de viajes, así como un sitio Web inalámbrico para teléfonos celulares y teléfonos inteligentes. No tiene que escribir nuevo código de software para los sistemas de información de cada nuevo socio ni para cada nuevo dispositivo inalámbrico (vea la figura 5-10).



**FIGURA 5-10 CÓMO UTILIZA DOLLAR RENT A CAR LOS SERVICIOS WEB**



Mediante el uso de servicios Web, Dollar Rent A Car provee una capa intermedia estándar de software para "hablar" con los sistemas de información de otras compañías. Dollar Rent A Car puede usar este conjunto de servicios Web para enlazarse con los sistemas de información de otras compañías sin tener que construir un enlace separado con cada uno de los sistemas de la empresa.

## OUTSOURCING DE SOFTWARE Y SERVICIOS EN LA NUBE

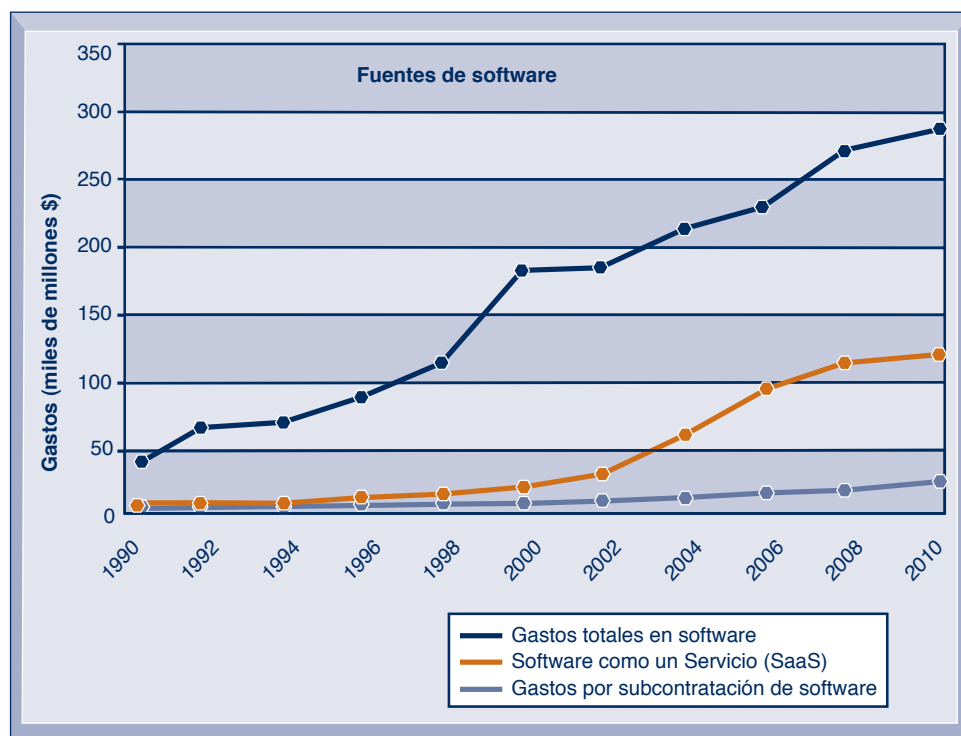
En la actualidad, muchas empresas continúan operando sistemas heredados que siguen cumpliendo con una necesidad de negocios y que serían muy costosos de reemplazar. No obstante, estas empresas compran o rentan la mayoría de sus nuevas aplicaciones de software a fuentes externas. La figura 5-11 ilustra el rápido crecimiento en las fuentes externas de software para las empresas en Estados Unidos.

Existen tres fuentes externas para el software: paquetes de software de un distribuidor de software comercial, subcontratar (outsourcing) el desarrollo de aplicaciones personalizadas con un distribuidor externo, y los servicios y herramientas de software basados en la nube.

### Paquetes de software y software empresarial

Ya describimos los paquetes de software para aplicaciones empresariales como uno de los principales tipos de componentes de software en las infraestructuras de TI contemporáneas. Un **paquete de software** es un conjunto de programas listo para usarse y disponible en forma comercial, que elimina la necesidad de que una empresa escriba sus propios programas para ciertas funciones, como el procesamiento de la nómina o el manejo de pedidos.

Los distribuidores de software de aplicaciones empresariales como SAP y Oracle-PeopleSoft han desarrollado poderosos paquetes que pueden dar servicio a los procesos de negocios primarios de una empresa a nivel mundial, desde los almacenes de datos, la administración de relaciones con el cliente, la administración de la cadena de suministro y las finanzas, hasta recursos humanos. Estos sistemas de software empresariales a gran escala proveen un solo sistema de software integrado a nivel mundial para las empresas, a un costo mucho menor del que pagarían si lo desarrollaran por su cuenta. En el capítulo 9 analizaremos los sistemas empresariales con detalle.

**FIGURA 5-11 FUENTES CAMBIANTES DEL SOFTWARE PARA EMPRESAS**

En 2010, las empresas estadounidenses invirtieron poco más de \$291 mil millones en software. Cerca del 40 por ciento de esa cantidad (\$116 mil millones) se originó fuera de la empresa, ya sea a través de los distribuidores de software empresarial o mediante proveedores de servicios de aplicaciones individuales que rentan o venden módulos de software. Otro 10 por ciento (\$29 mil millones) se obtuvo a través de los distribuidores de SaaS como un servicio en línea basado en la nube.

Fuentes: BEA National Income and Product Accounts, 2010; Gartner Group, 2010; estimaciones de los autores.

## Outsourcing de software

El **outsourcing** de software permite que una empresa contrate el desarrollo de software personalizado o el mantenimiento de los programas heredados existentes con empresas externas, que por lo común operan en el extranjero, en áreas del mundo con sueldos bajos. De acuerdo con los analistas de la industria, los ingresos aproximados por outsourcing desde el extranjero en 2010 en Estados Unidos fueron de \$50 mil millones, y los ingresos por outsourcing desde el interior de \$106 mil millones (Lohr, 2009). En este caso, la mayor cantidad de gastos se paga a las empresas internas en Estados Unidos, que proveen middleware, servicios de integración y demás soporte de software que se requiere por lo común para operar sistemas empresariales más grandes.

Por ejemplo, en marzo de 2008, Royal Dutch Shell PLC, el tercer productor petrolero más grande del mundo, firmó un contrato de outsourcing de cinco años por \$4 mil millones con T-Systems International GmbH, AT&T y Electronic Data Systems (EDS). En el acuerdo se asignó a AT&T la responsabilidad de redes y telecomunicaciones, a T-Systems el hospedaje y almacenamiento, y a EDS los servicios de cómputo para el usuario final y la integración de los servicios de la infraestructura. Al subcontratar estas tareas, Shell pudo reducir costos y enfocarse en sistemas que mejoren su posición competitiva en el mercado de petróleo y gas.

Los principales servicios que ofrecen las empresas de outsourcing en el extranjero se han sido mantenimiento a nivel inferior, captura de datos y operaciones de call centers. Sin embargo, con el creciente aumento en sofisticación y experiencia de las empresas en el extranjero, en especial en India, cada vez se llevan a cabo más actividades de desarrollo de nuevos programas en el extranjero. En el capítulo 13 analizaremos el outsourcing de software en el extranjero con mayor detalle.

## Servicios y herramientas de software basadas en la nube

En el pasado, el software como Microsoft Word o Adobe Illustrator venía en una caja y se diseñaba para operar en una sola máquina. En la actualidad, es más probable que descargue el software del sitio Web del distribuidor, o que lo utilice como un servicio que se ofrece a través de Internet.

El software basado en la nube y los datos que utiliza se alojan en poderosos servidores dentro de centros de datos masivos, y se puede acceder a éste mediante una conexión a Internet y un navegador Web estándar. Además de las herramientas gratuitas o de bajo costo para individuos y pequeñas empresas que proveen Google o Yahoo!, también hay software empresarial y otras funciones complejas de negocios disponibles como servicios de los principales distribuidores de software comercial. En vez de comprar e instalar programas de software, las compañías suscriptoras rentan las mismas funciones de estos servicios, en donde los usuarios pagan ya sea con base en una suscripción, o por cada transacción. Hoy en día, a los servicios para ofrecer y proveer acceso al software de manera remota como un servicio basado en Web se les conoce como **Software como un Servicio (SaaS)**. Un popular ejemplo es el de Salesforce.com, que describimos en el caso de estudio al final del capítulo, y que provee servicios de software bajo demanda para la administración de relaciones con el cliente.

Para poder administrar su relación con un subcontratista (outsourcer) o proveedor de servicio de tecnología, las empresas necesitan un contrato que incluya un **Acuerdo de Nivel de Servicio (SLA)**. El SLA es un contrato formal entre los clientes y sus proveedores de servicios, en el cual se definen las responsabilidades específicas del proveedor de servicios y el nivel de servicio que espera el cliente. Por lo general, los SLA especifican la naturaleza y el nivel de servicios proporcionados, criterios para la medición del desempeño, opciones de soporte, provisiones de seguridad y recuperación de desastres, propiedad, actualizaciones de hardware y software, soporte al cliente, facturación, condiciones para terminar el acuerdo. Hay una Trayectoria de aprendizaje sobre este tema.

## Mashups y apps

El software que utiliza para sus tareas personales y de negocios puede consistir de grandes programas autocontenidos, o tal vez esté compuesto de componentes intercambiables que se integran sin problemas con otras aplicaciones en Internet. Los usuarios individuales y empresas completas combinan al gusto estos componentes de software para crear sus propias aplicaciones personalizadas y compartir información con otros. Las aplicaciones de software resultantes se denominan **mashups**. La idea es tomar distintas fuentes y producir una nueva obra que sea “mayor que” la suma de sus partes. Si alguna vez ha personalizado su perfil de Facebook o su blog con la capacidad de mostrar videos o presentaciones con diapositivas, ha realizado un mashup.

Los mashups Web combinan las capacidades de dos o más aplicaciones en línea para crear un tipo de híbrido que provee más valor para el cliente que las fuentes originales por sí solas. Por ejemplo, EveryBlock Chicago combina a Google Maps con los datos criminales para la ciudad de Chicago. Los usuarios pueden buscar por ubicación, zona policiaca o tipo de crimen, y los resultados se despliegan como puntos en un mapa de Google Maps, codificados por colores. Amazon utiliza las tecnologías de mashups para agregar descripciones de productos con los sitios de socios y perfiles de usuarios.

Las **apps** son pequeñas piezas de software que se ejecutan en Internet, en su computadora o en su teléfono celular, y por lo general se ofrecen a través de Internet. Google se refiere a sus servicios en línea como apps, que comprende la suite de herramientas de productividad de escritorio Google Apps. Sin embargo, al hablar de apps en la actualidad, la mayor parte de la atención se dirige a las apps que se han desarrollado para la plataforma digital móvil. Son estas apps las que convierten a los teléfonos inteligentes y otros dispositivos móviles portátiles en herramientas de cómputo de propósito general.

La mayoría son para las plataformas de sistemas operativos iPhone, Android y BlackBerry. Muchas son gratuitas o se pueden comprar por un pequeño costo, mucho

menor que el del software convencional. En la actualidad ya existen más de 250 000 apps para la plataforma iPhone y iPad de Apple, y cerca de 80 000 que se ejecutan en teléfonos inteligentes que utilizan el sistema operativo Android de Google. El éxito de estas plataformas móviles depende en gran parte de la cantidad y calidad de las apps que ofrecen. Las apps atan al cliente a una plataforma de hardware específica: a medida que el usuario agrega cada vez más apps a su teléfono móvil, aumenta el costo de cambiar a una plataforma móvil competidora.

En este momento, las apps que se descargan con más frecuencia son: juegos (65%), seguidos de las noticias y el clima (56%), mapas/navegación (55%), redes sociales (54%), música (46%) y video/películas (25%). Sin embargo, también hay apps serias para usuarios de negocios con las que pueden crear y editar documentos, conectarse a sistemas corporativos, programar reuniones y participar en ellas, rastrear envíos, dictar mensajes de voz (vea la Sesión interactiva sobre administración en el capítulo 1). También hay una enorme cantidad de apps de comercio electrónico para investigar y comprar bienes y servicios en línea.

## 5.5 ASPECTOS GERENCIALES

Al crear y administrar una infraestructura de TI coherente se producen varios desafíos: lidiar con el cambio de plataforma y tecnología (que implica la computación en la nube y móvil), administración y gobernanza, y realizar inversiones inteligentes en infraestructura.

### CÓMO LIDIAR CON EL CAMBIO DE PLATAFORMA E INFRAESTRUCTURA

Conforme las empresas crecen, con frecuencia dejan atrás su infraestructura. A medida que las empresas se reducen, pueden quedarse con la infraestructura excesiva que compraron en épocas más productivas. ¿Cómo puede permanecer flexible una empresa cuando la mayoría de las inversiones en infraestructura de TI son compras y licencias con costos fijos? ¿Con qué efectividad puede escalar la infraestructura? La **escalabilidad** se refiere a la habilidad de una computadora, producto o sistema de expandirse para dar servicio a un mayor número de usuarios sin fallar. Tanto las nuevas aplicaciones, las fusiones y adquisiciones, como los cambios en el volumen de negocios generan un impacto en la carga de trabajo, por lo que se deben tener en cuenta al planificar la capacidad de hardware.

Las empresas que utilicen plataformas de computación móvil y de computación en la nube requerirán nuevas políticas y procedimientos para administrar estas plataformas. Tendrán que realizar un inventario de todos sus dispositivos móviles que se utilicen para actividades de negocios y deberán desarrollar tanto políticas como herramientas para rastrear, actualizar y asegurar esos dispositivos, además de controlar los datos y aplicaciones que se ejecutan en ellos. Las empresas que utilicen la computación en la nube y la tecnología SaaS tendrán que crear nuevos acuerdos contractuales con los distribuidores remotos para asegurarse de que el hardware y el software para las aplicaciones críticas siempre estén disponibles cuando se necesiten y que cumplan con los estándares corporativos en cuanto a la seguridad de la información. Es responsabilidad de la gerencia de negocios determinar los niveles aceptables de tiempo de respuesta de las computadoras y la disponibilidad de los sistemas de misión crítica de la empresa para mantener el nivel de desempeño de negocios esperado.

### GERENCIA Y GOBERNANZA

Un aspecto siempre presente entre los gerentes de sistemas de información y los directores generales (CEO) ha sido la cuestión acerca de quién debe controlar y administrar la infraestructura de TI de la empresa. En el capítulo 2 se introdujo el concepto de gobernanza de TI y se describieron algunos aspectos con los que lidia. Otras cues-

ciones importantes sobre la gobernanza de TI son: ¿Deberían los departamentos y las divisiones tener la responsabilidad de tomar sus propias decisiones sobre tecnología de la información, o habría que controlar y gestionar la infraestructura de TI de manera centralizada? ¿Cuál es la relación entre la administración centralizada de los sistemas de información y la administración de los sistemas de información de las unidades de negocios? ¿Cómo se pueden asignar los costos de infraestructura entre las unidades de negocios? Cada organización tendrá que obtener las respuestas con base en sus propias necesidades.

## CÓMO REALIZAR INVERSIONES DE INFRAESTRUCTURA INTELIGENTES

La infraestructura de TI es una importante inversión para la empresa. Si se invierte demasiado en infraestructura, no se aprovecha y constituye un rezago en el desempeño financiero de la empresa. Si se invierte poco, no se podrán ofrecer los servicios de negocios importantes y los competidores de la empresa (que invirtieron la cantidad correcta) superaran a la empresa con la inversión insuficiente. ¿Cuánto tiene que invertir la empresa en infraestructura? Esta pregunta no es fácil de responder.

Una pregunta relacionada es si una empresa debe comprar y mantener sus propios componentes de infraestructura de TI, o si es mejor que los rente de proveedores externos, entre ellos los que ofrecen servicios en la nube. A la decisión entre comprar sus propios activos de TI o rentarlos a proveedores externos se le conoce por lo general como la decisión entre *rentar y comprar*.

Tal vez la computación en la nube sea una manera de bajo costo para aumentar la escalabilidad y flexibilidad, pero las empresas deberían evaluar esta opción con cuidado en vista de los requerimientos de seguridad, además del impacto sobre los procesos de negocios y los flujos de trabajo. En ciertos casos, el costo de rentar software resulta ser mayor que el de comprar y mantener una aplicación en forma interna. Aún así, puede haber beneficios en cuanto al uso de SaaS si la compañía se puede enfocar en los aspectos de negocios básicos en vez de los desafíos tecnológicos.

### Costo total de propiedad de los activos de tecnología

El costo actual de poseer recursos de tecnología incluye el costo original de adquirir e instalar el hardware y software, así como los costos administrativos continuos para las actualizaciones de hardware y software, mantenimiento, soporte técnico, capacitación e incluso los costos de servicios públicos y bienes raíces para operar y alojar la tecnología. Podemos usar el modelo de **Costo Total de Propiedad (TCO)** para analizar estos costos directos e indirectos, para ayudar a las empresas a determinar el costo actual de las implementaciones de tecnología específicas. La tabla 5-3 describe los componentes más importantes del TCO que debemos considerar en un análisis de TCO.

Si se consideran todos estos componentes del costo, el TCO para una PC podría ser de hasta tres veces el precio de compra original del equipo. Aunque el precio de compra de un dispositivo inalámbrico para un empleado corporativo podría ser de varios cientos de dólares, el TCO para cada dispositivo es mucho mayor, y puede variar entre \$1 000 y \$3 000, de acuerdo con las estimaciones de varios consultores. Las ganancias en cuanto a productividad y eficiencia al equipar a los empleados con dispositivos de cómputo móviles se deben balancear en comparación con el aumento en los costos debido a la integración de estos dispositivos a la infraestructura de TI de la empresa, además del soporte técnico que se puede llegar a proporcionar. Otros componentes del costo son las cuotas por el tiempo inalámbrico, la capacitación de los usuarios finales, el soporte técnico y el software para aplicaciones especiales. Los costos son mayores si los dispositivos móviles ejecutan muchas aplicaciones distintas o necesitan integrarse a sistemas de back-end, como las aplicaciones empresariales.

Los costos de adquisición de hardware y software sólo representan cerca del 20 por ciento del TCO, por lo que los gerentes deben poner mucha atención en los costos administrativos para comprender el costo total del hardware y software de la empresa. Es posible reducir algunos de estos costos administrativos por medio de una mejor labor

**TABLA 5-3    COMPONENTES DEL COSTO EN EL MODELO DE VALOR TOTAL DE PROPIEDAD (TCO)**

COMPONENTE DE INFRAESTRUCTURA	COMPONENTES DEL COSTO
Adquisición de hardware	Precio de compra del equipo de hardware de computadora, que comprende computadoras, terminales, almacenamiento e impresoras.
Adquisición de software	Compra de licencia o software para cada usuario.
Instalación	Costo para instalar computadoras y software.
Capacitación	Costo para proveer capacitación a los especialistas en sistemas de información y los usuarios finales.
Soporte	Costo para proveer soporte técnico continuo, departamentos de soporte, etcétera.
Mantenimiento	Costo por actualizar el hardware y software.
Infraestructura	Costo por adquirir, mantener y dar soporte a la infraestructura relacionada, como las redes y el equipo especializado (así como las unidades de respaldo de almacenamiento).
Tiempo inactivo	Costo de pérdida de productividad si las fallas de hardware o software provocan que el sistema no esté disponible para el procesamiento y las tareas de los usuarios.
Espacio y energía	Costos de bienes raíces y servicios públicos para alojar y proveer energía para la tecnología.

gerencial. Muchas empresas grandes se quedan con hardware y software redundante e incompatible, debido a que permitieron que sus departamentos y divisiones realizaran sus propias compras de tecnología.

Además de cambiar a los servicios en la nube, estas empresas podrían reducir su TCO por medio de una mayor centralización y estandarización de sus recursos de hardware y software. Las compañías podrían reducir el tamaño del personal de sistemas de información requerido para dar soporte a su infraestructura, si la empresa minimiza el número de modelos de computadora y piezas de software distintos que se permite usar a los empleados. En una infraestructura centralizada, los sistemas se pueden administrar desde una ubicación central y el diagnóstico de problemas se puede realizar desde esa ubicación.

**Modelo de fuerzas competitivas para la inversión en infraestructura de TI**

La figura 5-12 ilustra un modelo de fuerzas competitivas que puede usar para lidiar con la pregunta sobre qué tanto debe gastar su empresa en infraestructura.

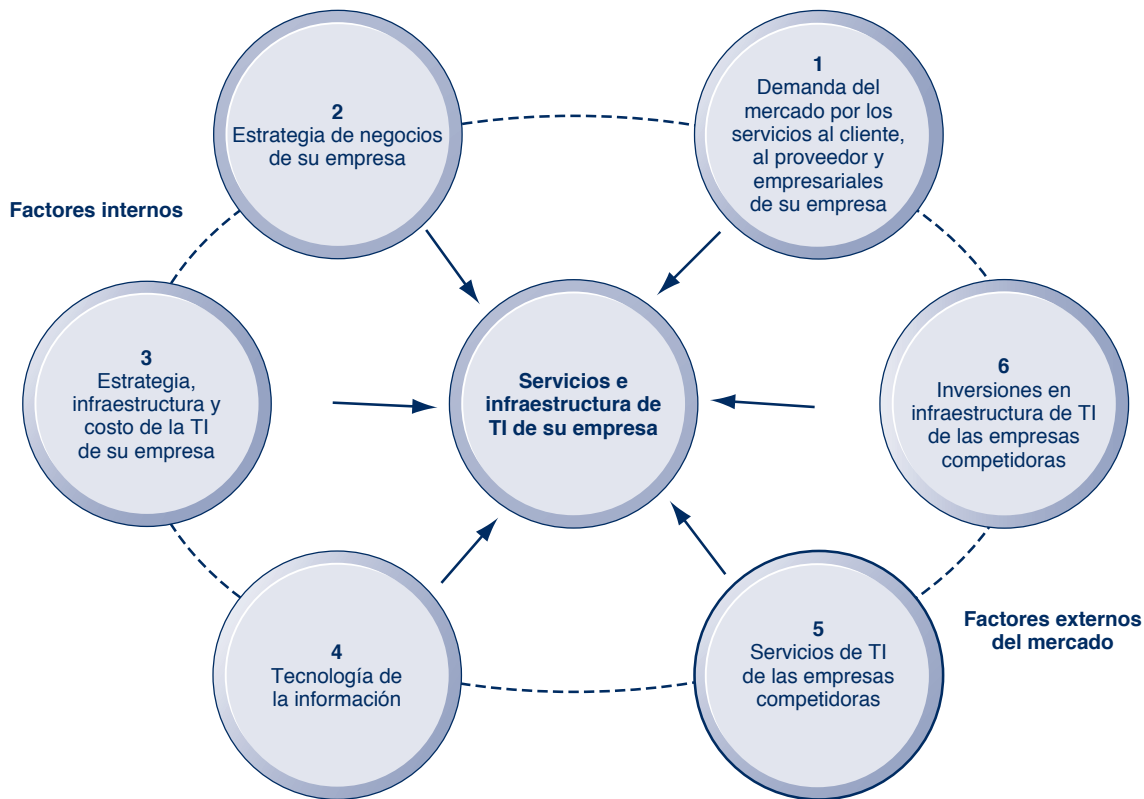
**Demanda en el mercado por los servicios de su empresa.** Haga un inventario de los servicios que provee en la actualidad a los clientes, proveedores y empleados. Realice una encuesta de cada grupo o cree equipos de enfoque para averiguar si los servicios que ofrece en la actualidad satisfacen las necesidades de cada uno. Por ejemplo, ¿se quejan los clientes de una respuesta lenta a sus consultas sobre precio y disponibilidad? ¿Se quejan los empleados sobre la dificultad de averiguar la información correcta para sus trabajos? ¿Se quejan los proveedores sobre las dificultades de descubrir sus requerimientos de producción?

**Estrategia de negocios de su empresa.** Analice la estrategia de negocios de su empresa en cinco años y trate de evaluar qué nuevos servicios y capacidades se requerirán para lograr las metas estratégicas.

**Estrategia, infraestructura y costo de TI de su empresa.** Examine los planes de tecnología de la información de su empresa para los próximos cinco años y evalúe su grado de alineación con los planes de negocios de ella. Determine los costos totales de la infraestructura de TI. Tal vez sea conveniente que realice un análisis de TCO. Si su empresa no tiene estrategia de TI, necesitará idear una que tome en cuenta el plan estratégico de cinco años de su empresa.

**Evaluación de la tecnología de la información.** ¿Está su empresa detrás de la curva de tecnología o a la vanguardia de ésta? Hay que evitar ambas situaciones. Por lo general no es conveniente invertir recursos en tecnologías avanzadas que aún

**FIGURA 5-12** MODELO DE FUERZAS COMPETITIVAS PARA LA INFRAESTRUCTURA DE TI



Hay seis factores que puede utilizar para responder a la pregunta: "¿Qué tanto debe invertir nuestra empresa en infraestructura de TI?"

son experimentales, a menudo son costosas y algunas veces poco confiables. Es conveniente que invierta en tecnologías para las cuales se hayan establecido estándares y los distribuidores de TI compitan en costo, no en diseño, y que haya también varios proveedores. Sin embargo, tampoco es conveniente dejar de invertir en nuevas tecnologías o permitir que los competidores desarrollen nuevos modelos de negocios y capacidades con base en las nuevas tecnologías.

**Servicios de las empresas competidoras.** Trate de evaluar los servicios de tecnología que ofrecen los competidores a los clientes, proveedores y empleados. Establezca medidas cuantitativas y cualitativas para compararlas con las de su empresa. Si los niveles de servicio de su empresa quedan cortos, su compañía se encuentra en desventaja competitiva. Busque formas en que su empresa pueda sobresalir en los niveles de servicio.

**Inversiones en infraestructura de TI de las empresas competidoras.** Mida sus gastos de infraestructura de TI con los de sus competidores. Muchas compañías hacen públicos sus gastos innovadores sobre TI. Si las empresas competidoras tratan de mantener secretos sus gastos en TI, tal vez pueda encontrar información sobre inversiones de TI en los informes anuales del formulario 10-K del SEC que las compañías públicas ofrecen al gobierno federal cuando esos gastos generan un impacto sobre los resultados financieros de una empresa.

No es necesario que su empresa invierta la misma cantidad que sus competidores, o una cantidad mayor. Tal vez haya descubierto formas mucho menos costosas de proveer servicios, y esto puede producir una ventaja en el costo. Por el contrario, tal vez su empresa gaste mucho menos que los competidores y esté experimentando el correspondiente mal desempeño, además de perder participación en el mercado.



5.6

PROYECTOS PRÁCTICOS SOBRE MIS

Los proyectos en esta sección le proporcionan experiencia práctica en el desarrollo de soluciones para administrar infraestructuras de TI y realizar outsourcing de TI, mediante el uso de software de hojas de cálculo para evaluar sistemas de escritorio alternativos y usar la investigación Web para generar el presupuesto de una conferencia de ventas.

Problemas de decisión gerencial

1. El Centro Médico de la Universidad de Pittsburgh (UPMC) se basa en sus sistemas de información para operar 19 hospitales, una red de sitios médicos adicionales y empresas tanto internacionales como comerciales. La demanda de servidores adicionales y tecnología de almacenamiento aumentaba a razón del 20 por ciento anual. El UPMC establecía un servidor separado para cada aplicación, y sus servidores al igual que otras computadoras ejecutaban varios sistemas operativos distintos, entre éstos varias versiones de Unix y Windows. El UPMC tuvo que administrar las tecnologías de muchos distribuidores distintos, como HP, Sun Microsystems, Microsoft e IBM. Evalúe el impacto de esta situación sobre el desempeño de negocios. ¿Qué factores y decisiones gerenciales se deben tener en cuenta al desarrollar una solución a este problema?
2. Qantas Airways, la principal aerolínea de Australia, se enfrenta a presiones relacionadas con los costos debido al aumento en los precios de combustible y a la reducción en los niveles de tráfico global de la aerolínea. Para permanecer competitiva, la empresa debe encontrar formas de mantener bajos los costos y proveer al mismo tiempo un alto nivel de servicio al cliente. Qantas tenía un centro de datos con 30 años de antigüedad. La gerencia tuvo que decidir entre reemplazar su infraestructura de TI con tecnología más reciente o subcontractar esta labor. ¿Debe subcontractar Qantas a un distribuidor de computación en la nube? ¿Qué factores debe tener en cuenta la gerencia de Qantas al decidir si van o no a subcontractar? Si Qantas decide subcontractar, mencione y describa los puntos que se deben tratar en un acuerdo de nivel de servicio.

Mejora de la toma de decisiones: uso de una hoja de cálculo para evaluar las opciones de hardware y de software

Habilidades de software: fórmulas de hojas de cálculo  
Habilidades de negocios: calcular los precios de la tecnología

En este ejercicio utilizará software de hojas de cálculo para calcular el costo de los sistemas de escritorio, las impresoras y el software.

Le han asignado la tarea de obtener información sobre los precios del hardware y software para una oficina de 30 personas. Use Internet para obtener el precio de 30 sistemas de escritorio PC (monitores, computadoras y teclados) fabricados por Lenovo, Dell y HP/Compaq según los listados en sus propios sitios Web corporativos (para los fines de este ejercicio, ignore el hecho de que los sistemas de escritorio por lo general incluyen paquetes de software precargados). Obtenga además los precios sobre 15 impresoras de escritorio fabricadas por HP, Canon y Dell. Cada sistema de escritorio debe satisfacer las especificaciones mínimas que se muestran en la siguiente tabla:

ESPECIFICACIONES MÍNIMAS DE LOS EQUIPOS DE ESCRITORIO	
Velocidad del procesador	3 GHz
Unidad de disco duro	350 GB
RAM	3 GB
Unidad de DVD-ROM	16 x
Monitor (medida diagonal)	18 pulgadas

Además, cada impresora de escritorio debe cumplir con las especificaciones mínimas que se muestran en la siguiente tabla:

## ESPECIFICACIONES MÍNIMAS DE LAS IMPRESORAS MONOCROMÁTICAS

Velocidad de impresión (blanco y negro)	20 páginas por minuto
Resolución de impresión	600 × 600
¿Lista para trabajo en red?	Si
Precio máximo/unidad	\$700

Después de obtener precios sobre los sistemas de escritorio y las impresoras, consiga los precios de 30 copias de las versiones más recientes de los paquetes de productividad de escritorio Microsoft Office, Lotus SmartSuite y Oracle OpenOffice, y de 30 copias de Windows 7 Professional. Los paquetes de las suites de software de aplicación vienen en varias versiones, por lo que debe asegurarse que cada uno contenga programas para procesamiento de palabras, hojas de cálculo, bases de datos y presentaciones.

Prepare una hoja de cálculo en la que muestre los resultados de sus investigaciones en cuanto a los sistemas de escritorio, las impresoras y el software. Use su software de hojas de cálculo para determinar la combinación de sistema de escritorio, impresora y software que ofrezca tanto el mejor desempeño como el mejor precio por trabajador. Como dos trabajadores van a compartir una impresora (15 impresoras/30 sistemas), suponga sólo la mitad del costo de una por trabajador en la hoja de cálculo. Suponga que su compañía desea la garantía y el servicio de contrato estándar que ofrece el fabricante de cada producto.

## Mejora de la toma de decisiones: uso de la investigación Web para obtener el presupuesto de una conferencia de ventas

Habilidades de software: software basado en Internet

Habilidades de negocios: investigación de costos de transporte y hospedaje

La compañía Foremost Composite Materials planea una conferencia de ventas de dos días para el 15 y 16 de octubre, empezando con una recepción la tarde del 14 de octubre. La conferencia consiste en reuniones de todo el día a las que debe asistir toda la fuerza de ventas, que incluye a 125 representantes de ventas con sus 16 gerentes. Cada representante de ventas requiere su propia sala, y la compañía necesita dos salas de reuniones comunes, una lo bastante grande como para alojar a toda la fuerza de ventas más los visitantes (200 en total) y la otra para alojar a la mitad de la fuerza. La gerencia estableció un presupuesto de \$120 000 para las rentas de las salas de los representantes. El hotel también debe ofrecer servicios como retroproyectores y proyectores de computadora, así como instalaciones de centro de negocios y banquetes. También debe tener instalaciones para que los representantes de la compañía puedan trabajar en sus cuartos y recrearse en una alberca o gimnasio. A la compañía le gustaría llevar a cabo la conferencia ya sea en Miami o en Marco Island, Florida.

Asimismo, a Foremost por lo general le gusta realizar dichas reuniones en hoteles propiedad de Hilton o Marriott. Use los sitios Web de Hilton y Marriott para seleccionar un hotel en cualquiera de estas ciudades que permita a la compañía llevar a cabo su conferencia de ventas dentro de su presupuesto.

Visite las páginas de inicio de ambos sitios y realice búsquedas para encontrar un hotel que cumpla con los requerimientos de la conferencia de ventas de Foremost. Una vez que haya seleccionado el hotel, localice vuelos que lleguen al mediodía del día anterior a la conferencia, ya que los asistentes tendrán que registrar su entrada un día antes y asistir a la recepción en la tarde anterior a la conferencia. Sus asistentes llegarán desde Los Ángeles (54), San Francisco (32), Seattle (22), Chicago (19) y Pittsburgh (14). Determine los costos de cada boleto de avión desde estas ciudades. Cuando termine, cree un presupuesto para la conferencia. El presupuesto debe incluir el costo de cada boleto de avión, el costo de los cuartos y \$60 por asistente al día para los alimentos.

- ¿Cuál fue su presupuesto final?
- ¿Cuál seleccionó como el mejor hotel para la conferencia de ventas y por qué?

## MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

Las siguientes Trayectorias de aprendizaje proporcionan contenido relevante a los temas que se cubrieron en este capítulo:

1. Cómo funcionan el hardware y software de computadora
2. Acuerdos de nivel de servicio
3. La iniciativa de software de código fuente abierto
4. Comparación de las etapas en la evolución de la infraestructura de TI
5. Computación en la nube

## Resumen de repaso

### 1. *¿Qué es la infraestructura de TI y cuáles son sus componentes?*

La infraestructura de TI constituye los recursos de tecnología compartidos que proveen la plataforma para las aplicaciones de sistemas de información específicas de la empresa. Consta de hardware, software y servicios que se comparten a través de toda la empresa. Entre los principales componentes de infraestructura de TI se encuentran las plataformas de hardware de computadora, las de sistemas operativos, las de software empresarial, las de redes y telecomunicaciones, el software de administración de bases de datos, las plataformas de Internet, los servicios de consultoría y los integradores de sistemas.

### 2. *¿Cuáles son las etapas y los impulsores tecnológicos en la evolución de la infraestructura de TI?*

Las cinco etapas en la evolución de la infraestructura de TI son: la era de las mainframes, la era de la computadora personal, la cliente/servidor, la de la computación empresarial, y la de computación móvil y en la nube. La ley de Moore trata sobre el incremento exponencial en el poder de procesamiento y la reducción en el costo de la tecnología de computadora; además establece que cada 18 meses se duplica el poder de los microprocesadores y se reduce el precio de la computación a la mitad. La ley del almacenamiento digital masivo trata sobre la reducción exponencial en el costo por almacenar la información; establece que el número de kilobytes de datos que se pueden almacenar en medios magnéticos por \$1 se duplica alrededor de cada 15 meses. La ley de Metcalfe muestra que el valor para los participantes en una red aumenta en forma exponencial a medida que ésta recibe más miembros. Además, el componente que controla el aumento explosivo en el uso de las computadoras es el rápido decremento en los costos de la comunicación y el hecho de que cada vez hay más acuerdos en la industria de la tecnología para usar estándares de computación y comunicaciones.

### 3. *¿Cuáles son las tendencias actuales en las plataformas de hardware de computadora?*

Cada vez más actividades de cómputo se realizan en una plataforma digital móvil. La computación en malla implica conectar computadoras remotas, separadas por límites geográficos, en una sola red para crear una malla computacional que combine el poder de cómputo de todos los ordenadores en la red. La virtualización organiza los recursos de computación de modo que su uso no se restrinja debido a la configuración física o ubicación geográfica. En la computación en la nube, las empresas y los individuos obtienen poder de cómputo y software como servicios a través de una red, incluyendo Internet, en vez de tener que comprar e instalar el hardware y software en sus propias computadoras. Un procesador multinúcleo es un microprocesador al que se conectan dos o más núcleos de procesamiento para mejorar su desempeño. La computación verde abarca prácticas y tecnologías para producir, usar y desechar el hardware de tecnología de la información para minimizar el impacto negativo sobre el entorno. En la computación autónoma, los sistemas computacionales tienen la capacidad de configurarse y repararse por sí solos. Los procesadores que ahorran energía reducen de manera drástica el consumo de ésta en los dispositivos móviles y digitales.

### 4. *¿Cuáles son las tendencias actuales en las plataformas de software?*

El software de código abierto se produce y mantiene gracias a una comunidad global de programadores; con frecuencia se puede descargar sin costo. Linux es un poderoso y flexible sistema operativo de código fuente que se puede ejecutar en varias plataformas de hardware, además de que es muy utilizado para operar servidores Web. Java es un lenguaje de programación independiente del sistema operativo y del

hardware, que en la actualidad es el principal entorno de programación interactiva para Web. Los servicios Web son componentes de software con acoplamiento débil, basados en estándares Web abiertos que trabajan con cualquier software de aplicación y sistema operativo. También se pueden utilizar como componentes de aplicaciones basadas en Web que enlazan los sistemas de dos organizaciones distintas o sistemas dispares de una sola compañía. Las empresas compran sus nuevas aplicaciones de software a fuentes externas, entre ellos los paquetes de software, mediante la subcontratación del desarrollo de aplicaciones personalizadas con un distribuidor externo (que puede estar en el extranjero), o mediante la renta de servicios de software en línea (SaaS). Los mashups combinan dos servicios de software distintos para crear nuevas aplicaciones y servicios de software. Las apps son pequeñas piezas de software que se ejecutan en Internet, en una computadora o en un teléfono móvil, y por lo general se ofrecen a través de Internet.

5. *¿Cuáles son los desafíos de administrar la infraestructura de TI y las soluciones gerenciales?*

Los principales desafíos implican el hecho de lidiar con el cambio en la plataforma, con la infraestructura, la gestión y la gobernanza de la infraestructura, así como con la realización de inversiones inteligentes en infraestructura. Los lineamientos de solución incluyen: utilizar un modelo de fuerzas competitivas para determinar cuánto invertir en infraestructura de TI y en dónde realizar inversiones estratégicas de infraestructura, además de establecer el costo total de propiedad (TCO) de los activos de tecnología de la información. El costo total de poseer los recursos de tecnología no sólo involucra al costo original del hardware y software de computadora, sino también a los costos de las actualizaciones de hardware y software, mantenimiento, soporte técnico y capacitación.

## Términos clave

*Acuerdo de Nivel de Servicio (SLA)*, 193

*Ajax*, 189

*Android*, 177

*Apps*, 193

*Arquitectura cliente/servidor multinivel (N-niveles)*, 169

*Arquitectura Orientada al Servicio (SOA)*, 190

*Cientes*, 168

*Computación autónoma*, 185

*Computación bajo demanda*, 184

*Computación cliente/servidor*, 168

*Computación en la nube*, 170

*Computación en malla*, 182

*Computación utilitaria*, 184

*Computación verde*, 184

*Costo total de propiedad (TCO)*, 195

*Chrome OS*, 177

*Escalabilidad*, 194

*Estándares de tecnología*, 174

*Java*, 188

*Lenguaje de marcado de hipertexto (HTML)*, 189

*Lenguaje de marcado extensible (XML)*, 189

*Ley de Moore*, 171

*Linux*, 177

*Mainframe*, 168

*Mashup*, 193

*Minicomputadoras*, 168

*Multitáctil*, 177

*Nanotecnología*, 171

*Navegador Web*, 188

*Netbook*, 181

*Nube privada*, 183

*Nube pública*, 183

*Outsourcing*, 192

*Paquete de software*, 191

*Procesador multinúcleo*, 185

*Red de área de almacenamiento (SAN)*, 180

*SaaS (Software como un Servicio)*, 193

*Servicio de hospedaje Web*, 180

*Servicios Web*, 189

*Servidor*, 168

*Servidor de aplicaciones*, 169

*Servidor Web*, 169

*Servidores blade*, 176

*Sistema operativo*, 177

*Sistemas heredados*, 181

*Software de código abierto*, 187

*Unix*, 177

*Virtualización*, 182

*Windows*, 169

*Wintel PC*, 168

## Preguntas de repaso

1. ¿Qué es la infraestructura de TI y cuáles son sus componentes?
  - Defina la infraestructura de TI desde una perspectiva de tecnología y una perspectiva de servicios.
  - Mencione y describa los componentes de la infraestructura de TI que las empresas necesitan administrar.
2. ¿Cuáles son las etapas y los impulsores tecnológicos en la evolución de la infraestructura de TI?
  - Mencione cada una de las eras en la evolución de la infraestructura de TI y describa sus características distintivas.
  - Defina y describa lo siguiente: servidor Web, servidor de aplicación, arquitectura cliente/servidor multinivel.
  - Describa la ley de Moore y la ley del almacenamiento digital masivo.
  - Describa cómo es que la economía de red, la reducción en los costos de comunicación y los estándares de tecnología afectan a la infraestructura de TI.
3. ¿Cuáles son las tendencias actuales en las plataformas de hardware de computadora?
  - Describa la plataforma móvil en desarrollo, la computación en malla y la computación en la nube.
4. ¿Cuáles son las tendencias actuales en las plataformas de software?
  - Defina y describa los conceptos software de código abierto y Linux; explique además sus beneficios de negocios.
  - Defina Java y Ajax; explique también por qué son importantes.
  - Defina y describa los servicios Web y el papel que desempeña XML.
  - Mencione y describa las tres fuentes externas de software.
  - Defina y describa los mashups y las apps de software.
5. ¿Cuáles son los desafíos de administrar la infraestructura de TI y las soluciones gerenciales?
  - Mencione y describa los desafíos gerenciales impuestos por la infraestructura de TI.
  - Explique cómo el uso de un modelo de fuerzas competitivas y el cálculo del TCO de los activos de tecnología ayudan a las empresas a realizar buenas inversiones en infraestructura.

## Preguntas para debate

1. ¿Por qué el hecho de seleccionar el hardware y software de computadora para la organización es una decisión gerencial importante? ¿Qué aspectos de administración, organización y tecnología se deben tener en cuenta al seleccionar hardware y software de computadora?
2. ¿Deben las organizaciones usar proveedores de servicios de software para todas sus necesidades de software? ¿Por qué sí o por qué no? ¿Qué factores de administración, organización y tecnología hay que tener en cuenta al tomar esta decisión?
3. ¿Cuáles son las ventajas y desventajas de la computación en la nube?

## Colaboración y trabajo en equipo: evaluación de los sistemas operativos de servidor y los sistemas operativos móviles

Forme un grupo con tres o cuatro de sus compañeros de clases. Elija sistemas operativos de servidor o móviles para evaluarlos. Podría investigar y comparar las capacidades y costos de Linux y la versión más reciente del sistema operativo Windows o Unix. Como alternativa, podría comparar las capacidades del sistema operativo móvil Android con la versión más reciente del sistema

operativo iPhone (iOS). De ser posible, use Google Sites para publicar vínculos a páginas Web, anuncios de comunicación en equipo, asignaturas de trabajo; para lluvias de ideas; y para trabajar de manera colaborativa en los documentos del proyecto. Trate de usar Google Docs para desarrollar una presentación de sus hallazgos para la clase.



## Salesforce.com: los servicios en la nube pasan a la corriente dominante

### CASO DE ESTUDIO

**S**alesforce.com, una de las compañías de tecnología más revolucionaria de los últimos años, ha sacudido a la industria de software con su innovador modelo de negocios y su rotundo éxito. Salesforce ofrece soluciones de administración de relaciones con el cliente (CRM) y otras soluciones de software de aplicación como un servicio, que se renta a través de Internet, en contraste al software que se compra e instala en las máquinas en forma local.

La compañía fue fundada en 1999 por Marc Benioff, un ejecutivo de Oracle; desde entonces ha crecido y cuenta con más de 3 900 empleados, 82 400 clientes corporativos y 2.1 millones de suscriptores. Obtuvo \$1.3 mil millones en ingresos en 2009, gracias a lo cual se convirtió en una de las principales 50 compañías de software en el mundo. Salesforce atribuye su éxito a los diversos beneficios de su modelo de distribución de software bajo demanda.

El modelo bajo demanda elimina la necesidad de realizar inversiones iniciales de hardware y software en sistemas e implementaciones extensas en computadoras corporativas. Las suscripciones empiezan desde los \$9 por usuario al mes, para la versión con funcionalidad reducida de Group para equipos pequeños de ventas y marketing, con suscripciones mensuales para versiones más avanzadas adecuadas para empresas grandes, que empiezan desde los \$65 por usuario.

Por ejemplo, la tienda Haagen-Dasz con base en Minneapolis que posee Nestle Estados Unidos calculó que tendría que invertir \$65 000 por una base de datos diseñada a la medida que ayude a la gerencia a permanecer en contacto con las franquicias de menudeo de la compañía. Ésta sólo tuvo que pagar \$20 000 para establecer el servicio con Salesforce.com, además de un cobro mensual de \$125 por 20 usuarios para usar dispositivos portátiles inalámbricos o Web para supervisar en forma remota todas las franquicias de Haagen-Dasz por todo Estados Unidos.

Las implementaciones de Salesforce.com tardan cuando mucho tres meses, por lo general menos de un mes. Los suscriptores no tienen que comprar, escalar ni mantener ningún tipo de hardware. No hay que instalar sistemas operativos, servidores de bases de datos o servidores de aplicación, tampoco hay consultores ni personal, y no existen las costosas licencias y cuotas de mantenimiento. Se puede acceder al sistema a través de un navegador Web estándar, con ciertas funciones accesibles para los dispositivos portátiles móviles. Salesforce.com actualiza en forma continua su software tras bambalinas. Hay herramientas para personalizar ciertas características del software y dar soporte a los procesos de negocios únicos de una empresa. Los suscriptores pueden irse si los negocios dejan de prosperar o si llega un mejor sistema. Si despiden gente, pueden

recortar el número de suscripciones de Salesforce que deben comprar.

Salesforce se enfrenta a considerables desafíos a medida que continúa su crecimiento y refina sus actividades de negocios. El primer desafío proviene del aumento en la competencia, tanto por parte de los líderes tradicionales de la industria como los nuevos retadores que esperan repetir el éxito de Salesforce. Microsoft, SAP y Oracle han implementado versiones basadas en suscripciones de sus productos de CRM en respuesta a Salesforce. Los competidores más pequeños como NetSuite, Salesboom.com y RightNow también han realizado ciertas incursiones contra la participación en el mercado de Salesforce.

De todas formas, Salesforce todavía tiene mucho por hacer para alcanzar el tamaño y la participación en el mercado de sus competidores más poderosos. En 2007, la participación en el mercado de SAP era casi cuatro veces mayor que la de Salesforce, y la base de clientes de IBM contiene 9 000 compañías de software que ejecutan sus aplicaciones en su software, por lo que es más probable que opten por una solución que les ofrezca IBM en vez de optar por Salesforce.

Salesforce necesita demostrar de manera continua a sus clientes que tienen la confiabilidad y seguridad suficiente como para poder manejar sus datos y aplicaciones corporativas en forma remota. La compañía ha experimentado varias fallas en su servicio. Por ejemplo, el 6 de enero de 2009 falló un dispositivo básico de red y evitó que se procesaran los datos en Europa, Japón y Norteamérica durante 38 minutos. Se vieron afectadas cerca de 177 millones de transacciones. Si bien la mayoría de los clientes de Salesforce aceptan el hecho de que los servicios de TI que se ofrecen a través de la nube no van a estar disponibles el 100 por ciento del tiempo, algunos clientes y críticos aprovecharon la falla como una oportunidad para cuestionar la solidez de todo el concepto de la computación en la nube. En febrero de 2009 ocurrió una falla similar, la cual afectó a toda Europa junto con Norteamérica unas cuantas horas después.

Hasta ahora, Salesforce sólo ha experimentado una fuga de seguridad. En noviembre de 2007, un empleado de Salesforce fue engañado para que divulgara su contraseña corporativa, con lo cual quedó expuesta la lista de clientes de Salesforce. Los clientes de esta empresa fueron bombardeados con intentos de fraude y piratería informática muy especializados que no parecían ser estafas. Aunque este incidente provocó una alerta roja, muchos clientes informaron que la forma en que Salesforce manejó la situación había sido satisfactoria. Los principales clientes de Salesforce a menudo envían auditores para revisar su seguridad.

Otro desafío para Salesforce es la expansión de su modelo de negocios hacia otras áreas. En la actualidad, los principales usuarios de Salesforce pertenecen al personal de ventas que necesita mantener el registro de los prospectos y las listas de clientes. Una forma en que la compañía trata de proveer funcionalidad adicional es mediante una sociedad con Google, en específico con Google Apps. Salesforce desea combinar sus servicios con Gmail, Google Docs, Google Talk y Google Calendar para permitir que sus clientes puedan realizar más tareas a través de Web. Tanto Salesforce como Google esperan que su iniciativa de Salesforce.com para Google Apps impulse el futuro crecimiento del software bajo demanda.

Salesforce también se asoció con Apple para distribuir sus aplicaciones de modo que se puedan usar en el iPhone. La compañía espera poder entrar en el extenso mercado de usuarios del iPhone, al promover la habilidad de usar las aplicaciones de Salesforce en cualquier momento y en cualquier parte. Además, Salesforce introdujo una herramienta de desarrollo para integrarse con la red social de Facebook y permitir a los clientes crear aplicaciones que hagan llamadas a funciones en el sitio de Facebook (a principios de 2010, Salesforce introdujo su propia aplicación de redes sociales llamada Chatter, que permite a los empleados crear perfiles y realizar actualizaciones de estado que aparezcan en las fuentes de noticias de los colegas, algo similar a Facebook y Twitter).

Para poder incrementar sus ingresos a los niveles que esperan en un momento dado los observadores de la industria y Wall Street, Salesforce cambiará su enfoque de vender una suite de aplicaciones de software al de proveer una "plataforma" de computación en la nube más amplia, en la que muchas compañías de software ofrezcan aplicaciones. Como lo mencionó el CEO Marc Benioff, durante la última década "nos enfocamos en el software como un servicio... En la siguiente década, Salesforce.com se enfocará de verdad en la plataforma como un servicio".

La compañía ha intensificado sus esfuerzos por proveer ofrecimientos de computación en la nube a sus clientes. El nuevo sitio Web Salesforce.com enfatiza más la computación en la nube, al agrupar los productos en tres tipos de nube: la nube de ventas (sales cloud), la nube de servicio (service cloud) y la nube personalizada (custom cloud). Las nubes de ventas y de servicio consisten en aplicaciones destinadas a mejorar las ventas y el servicio al cliente respectivamente, y la Nube personalizada es otro nombre para la plataforma de desarrollo de aplicaciones Force.com, en donde los clientes pueden desarrollar sus propias aplicaciones para usarlas dentro de la red más amplia de Salesforce.

Force.com provee un conjunto de herramientas de desarrollo y servicios de TI que permiten a los usuarios personalizar sus aplicaciones de administración de relaciones con el cliente de Salesforce, o crear aplicaciones totalmente nuevas y ejecutarlas "en la nube", en la infraestructura del centro de datos de Salesforce.

La compañía abrió Force.com a otros desarrolladores independientes de software y mostró una lista de sus programas en su AppExchange.

Mediante el uso de AppExchange, las empresas pequeñas pueden entrar al mundo en línea y descargar con facilidad más de 950 aplicaciones de software, algunas de las cuales son complementos para Salesforce.com y otras que no están relacionadas, incluso en funciones que no tratan directamente con el cliente, como recursos humanos. Force.com Sites, basada en el entorno de desarrollo Forces.com, permite a los usuarios desarrollar páginas Web y registrar nombres de dominio. Los precios se basan en el tráfico del sitio.

La infraestructura en la nube de Salesforce tiene dos centros de datos en Estados Unidos y un tercero en Singapur; se planea contar con otros en Europa y Japón en un futuro. Asimismo, Salesforce se asoció con Amazon para permitir a los clientes de Force.com incursionar en los servicios de computación en la nube de Amazon (nube de cómputo elástica y servicio de almacenamiento simple). Los servicios de Amazon se encargarían de las tareas de "computación en ráfaga de nubes" de las aplicaciones de Force.com que requieran un poder de procesamiento o de una capacidad de almacenamiento adicionales.

Un informe del Centro de Datos Internacional (IDC) estimó que la plataforma Force.com permite a los usuarios crear y ejecutar aplicaciones de negocios y sitios Web cinco veces más rápido y a la mitad del costo de las alternativas que no están basadas en nubes. Por ejemplo, RehabCare, un proveedor nacional de servicios médicos de rehabilitación, utilizó a Force.com para crear una aplicación de admisión de pacientes móvil que los médicos pudieran usar en su iPhone. El equipo de sistemas de información de RehabCare creó un prototipo de la aplicación en cuatro días, el cual se ejecuta en la plataforma Force.com. Se hubieran requerido seis meses para crear una aplicación móvil similar mediante el uso de las herramientas de desarrollo de Microsoft. En la actualidad, cerca de 400 médicos utilizan esa aplicación.

Author Solutions, una compañía de autopublicación con base en Bloomington, Minnesota, usa la plataforma Force.com para alojar las aplicaciones que controlan sus operaciones. Esta empresa reporta haber ahorrado hasta un 75 por ciento al no tener que dar mantenimiento ni administrar sus propias aplicaciones de centro de datos, comercio electrónico y flujo de trabajo, además de la habilidad de escalar a medida que su negocio se multiplica de manera explosiva. Las modificaciones en el flujo de trabajo, que alguna vez requirieron de 30 a 120 horas, ahora se realizan en una cuarta parte del tiempo. El costo y las horas que se necesitaban para agregar un nuevo producto, que solía requerir de 120 a 240 horas (con un costo entre \$6 000 y \$12 000), se redujo en un 75 por ciento. La nueva plataforma es capaz de manejar un 30 por ciento más de volumen de trabajo que los sistemas anteriores con el mismo número de empleados.



La pregunta es si la audiencia para las plataformas AppExchange y Force.com de Salesforce.com llegará a ser lo bastante grande como para poder ofrecer el nivel de crecimiento que Salesforce desea. Aún no está claro si la compañía generará los ingresos que necesita para ofrecer servicios de computación en la nube a la misma escala que Google o Amazon, y lograr que sus inversiones en la computación en la nube produzcan rendimientos.

Algunos analistas creen que tal vez la plataforma no sea atractiva para las necesidades de las compañías más grandes en cuanto a aplicaciones. Otro reto adicional es el de proveer una disponibilidad constante. Los suscriptores de Salesforce.com dependen de que el servicio esté disponible 24/7. Sin embargo, gracias a las fallas antes descritas, muchas compañías han reconsiderado su dependencia en cuanto al software como un servicio. Salesforce.com provee herramientas para asegurar a los clientes la confiabilidad de su sistema y también ofrece aplicaciones de PC que se enlazan con sus servicios, de modo que los usuarios puedan trabajar sin conexión.

Aun así, muchas compañías se rehúsan a subirse al vagón del SaaS y la computación en la nube. Lo que es más, todavía no está claro si el software ofrecido a través de Web costará menos a la larga. De acuerdo con el analista Rob DiSisto de los consultores de Gartner, tal vez sea más económico suscribirse a los servicios de software de Salesforce.com durante los primeros años, pero ¿qué ocurre después? ¿Aumentará el costo de actualizar y administrar el software bajo demanda más que las cuotas que pagan las compañías por poseer y hospedar su propio software?

**Fuentes:** "How Salesforce.com Brings Success to the Cloud", *IT BusinessEdge.com*, visitado el 10 de junio de 2010; Lauren McKay, "Salesforce.com Extends Chatter Across the Cloud", *CRM Magazine*, 14 de abril de 2010; Jeff Cogswell, "Salesforce.com Assembles an Array of Development Tools for Force.com", *eWeek*, 15 de febrero de 2010; Mary Hayes Weier, "Why Force.com Is Important to Cloud Computing", *Information Week*, 23 de noviembre de 2009; Jessi Hempel, "Salesforce Hits Stride", *CNN Money.com*, 2 de marzo de 2009; Clint Boulton, "Salesforce.com Network Device Failure Shuts Thousands Out of SaaS Apps", *eWeek*, 7 de enero de 2009; J. Nicholas Hoover, "Service Outages Force Cloud Adopters to Rethink Tactics", *Information Week*, 18/25 de agosto de 2008, y Charles Babcock, "Salesforce Ascends Beyond Software As Service", *Information Week*, 10 de noviembre de 2008.

## PREGUNTAS DEL CASO DE ESTUDIO

1. ¿Cómo utiliza Salesforce.com la computación en la nube?
2. ¿Cuáles son algunos de los desafíos a los que se enfrenta Salesforce a medida que continúa con su crecimiento? ¿Qué tan bien podrá cumplir con esos desafíos?
3. ¿Qué tipos de empresas se podrían beneficiar al cambiar a Salesforce y por qué?
4. ¿Qué factores tomaría en cuenta al decidir si debe usar Salesforce.com o no para su empresa?
5. ¿Podría una compañía operar todas sus actividades de negocios mediante el uso de Salesforce.com, Force.com y AppExchange? Explique su respuesta.

# Capítulo 6

## Fundamentos de inteligencia de negocios: bases de datos y administración de la información

### OBJETIVOS DE APRENDIZAJE

*Después de leer este capítulo, usted podrá responder a las siguientes preguntas:*

1. ¿Cuáles son los problemas de administrar los recursos de datos en un entorno de archivos tradicional y cómo se resuelven mediante un sistema de administración de bases de datos?
2. ¿Cuáles son las principales capacidades de los sistemas de administración de bases de datos (DBMS) y por qué es tan poderoso un DBMS?
3. ¿Cuáles son algunos principios importantes del diseño de bases de datos?
4. ¿Cuáles son las principales herramientas y tecnologías para acceder a la información de las bases de datos y mejorar tanto el desempeño de negocios como la toma de decisiones?
5. ¿Por qué son la política de información, la administración de datos y el aseguramiento de la calidad de los datos esenciales para administrar los recursos de datos de la empresa?

#### *Sesiones interactivas:*

¿Qué pueden aprender las empresas de la minería de texto?

Errores del buró de crédito: grandes problemas de la gente

### RESUMEN DEL CAPÍTULO

#### 6.1 ORGANIZACIÓN DE LOS DATOS EN UN ENTORNO DE ARCHIVOS TRADICIONAL

Términos y conceptos de organización de archivos  
Problemas con el entorno de archivos tradicional

#### 6.2 LA METODOLOGÍA DE LAS BASES DE DATOS PARA LA ADMINISTRACIÓN DE DATOS

Sistemas de administración de bases de datos  
Capacidades de los sistemas de administración de bases de datos  
Diseño de bases de datos

#### 6.3 USO DE BASES DE DATOS PARA MEJORAR EL DESEMPEÑO DE NEGOCIOS Y LA TOMA DE DECISIONES

Almacenes de datos  
Herramientas para la inteligencia de negocios: análisis de datos multidimensional y minería de datos  
Las bases de datos y Web

#### 6.4 ADMINISTRACIÓN DE LOS RECURSOS DE DATOS

Establecimiento de una política de información  
Aseguramiento de la calidad de los datos

#### 6.5 PROYECTOS PRÁCTICOS SOBRE MIS

Problemas de decisión gerencial  
Obtención de la excelencia operacional: creación de una base de datos relacional para la administración del inventario  
Mejora de la toma de decisiones: uso de las bases de datos en línea para buscar recursos de negocios en el extranjero

#### MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

Diseño de bases de datos, normalización y diagramas de entidad-relación  
Introducción a SQL  
Modelos de datos jerárquico y de red

## RR DONNELLEY TRATA DE DOMINAR SUS DATOS

Es probable que en estos momentos usted esté utilizando un producto de RR Donnelley. Esta empresa con base en Chicago es una gigantesca compañía de impresión y servicio comercial que provee servicios de impresión, formularios, etiquetas, correo directo y otros servicios. Quizás este libro de texto provenga de esas imprentas. La reciente expansión de la empresa se ha visto impulsada por una serie de adquisiciones, entre las que están, la imprenta comercial Moore Wallace en 2005 y la compañía de administración de la cadena de suministro e impresión llamada Banta, en enero de 2007. Los ingresos de RR Donnelley dieron un salto considerable, de \$2.4 mil millones en 2003 a más de \$9.8 mil millones en la actualidad.

Sin embargo, todo ese crecimiento generó desafíos en cuanto a la administración de la información. Cada compañía adquirida tenía sus propios sistemas, conjunto de datos de clientes, distribuidores y productos. Al provenir de tantas fuentes distintas, con frecuencia los datos eran inconsistentes, duplicados o incompletos. Por ejemplo, cada una de las diferentes unidades de la empresa podría tener un significado distinto para la entidad “cliente”. Una podría definir “cliente” como una ubicación específica de facturación, mientras que otra lo podría definir como la entidad matriz legal de una compañía. Donnelley tuvo que utilizar procesos manuales que consumían mucho tiempo para reconciliar los datos almacenados en varios sistemas, para poder obtener una imagen clara a nivel empresarial de cada uno de sus clientes, ya que podrían estar haciendo negocios con varias unidades de la compañía. Estas condiciones aumentaron las ineficiencias y los costos.

RR Donnelley había crecido tanto que ya no era práctico almacenar la información de todas sus unidades en un solo sistema. No obstante, Donnelley aún necesitaba un solo conjunto claro de datos que fuera preciso y consistente para toda la empresa. Para resolver este problema, RR Donnelley recurrió a la administración de datos maestros (MDM). El objetivo de la MDM es asegurar que una organización no utilice varias versiones de la misma pieza de datos en distintas partes de sus operaciones, para lo cual fusiona los registros dispares en un solo archivo maestro autenticado. Una vez implementado el archivo maestro, los empleados y las aplicaciones acceden a una sola vista consolidada de los datos de la compañía. En especial, es útil para las compañías como Donnelley que tienen problemas de integración de sus datos como resultado de las fusiones y adquisiciones.

La implementación de la MDM es un proceso de varios pasos que incluye el análisis de los procesos de negocios, la limpieza de los datos, la consolidación, reconciliación de los datos y la migración de datos hacia un archivo maestro de toda la información de la compañía. Las compañías deben identificar qué grupo es “propietario” de cada pieza de datos y responsable de resolver las definiciones inconsistentes de datos, además de otras discrepancias. Donnelley lanzó su programa MDM a finales de 2005 y empezó a crear un solo conjunto de identificadores para los datos de sus clientes y distribuidores. La compañía optó por un modelo de registro mediante el concentrador de datos (Data Hub) de Purisma, en el cual los datos del cliente aún residen en el sistema en donde se originan, pero se registran en un “concentrador” o “hub” maestro y se hace referencia cruzada a ellos, de modo que las aplicaciones puedan encontrarlos, y los que están en el sistema de origen no se tocan.

Casi un año después, Donnelley lanzó su almacén de datos maestro de clientes (Customer Master Data Store), el cual integra los datos provenientes de numerosos sistemas debido a las adquisiciones de Donnelley. Los datos obsoletos, incompletos o que tienen un formato incorrecto se corrigen o eliminan. Al tener un solo conjunto consistente a nivel empresarial de datos con definiciones y estándares comunes, la gerencia puede averiguar con facilidad qué tipo de negocios y qué tanta actividad comercial tiene con un cliente específico para identificar los mejores clientes y las oportunidades de ventas. Y cuando Donnelley adquiera una compañía, podrá ver con rapidez una lista de los clientes que se traslapen.

**Fuentes:** John McCormick, "Mastering Data at R.R. Donnelley", *Information Management Magazine*, marzo de 2009; [www.rdonnelley.com](http://www.rdonnelley.com), visitado el 10 de junio de 2010, y [www.purisma.com](http://www.purisma.com), visitado el 10 de junio de 2010.

La experiencia de RR Donnelley ilustra la importancia de la administración de datos para las empresas. Donnelley ha experimentado un crecimiento fenomenal, en su mayor parte debido a las adquisiciones, aunque su desempeño de negocios depende de lo que pueda o no hacer con sus datos. La forma en que las empresas almacenan, organizan y administran sus datos tiene un tremendo impacto sobre la efectividad organizacional.

El diagrama de apertura del capítulo dirige la atención a los puntos importantes generados por este caso y por este capítulo. La gerencia decidió que la compañía necesitaba centralizar la administración de sus datos. La información sobre los clientes, distribuidores, productos y demás entidades importantes se había almacenado en varios sistemas y archivos distintos, de donde no era fácil recuperarlos y analizarlos. A menudo eran redundantes e inconsistentes, lo cual limitaba su utilidad. La gerencia no podía obtener una vista a nivel empresarial de todos sus clientes en todas sus adquisiciones para comercializar sus productos y servicios, además de proveer un mejor servicio y soporte.

En el pasado, RR Donnelley había utilizado mucho los procesos manuales en papel para reconciliar sus datos inconsistentes y redundantes, y para administrar su información desde una perspectiva a nivel empresarial. Esta solución ya no era viable a medida que la organización crecía cada vez más. Una solución más apropiada era identificar, solidificar, limpiar y estandarizar los datos de los clientes junto con los demás tipos de datos en un solo registro de administración de datos maestro. Además de usar la tecnología apropiada, Donnelley tuvo que corregir y reorganizar los datos en un formato estándar, así como establecer reglas, responsabilidades y procedimientos para actualizar y utilizar los datos.

Un sistema de administración de datos maestro ayuda a RR Donnelley a impulsar la rentabilidad, al facilitar la identificación de clientes y las oportunidades de ventas. También mejora la eficiencia organizacional y la toma de decisiones, al tener disponibles datos más precisos y completos sobre los clientes, y al reducir el tiempo requerido para reconciliar los datos redundantes e inconsistentes.



## 6.1 ORGANIZACIÓN DE LOS DATOS EN UN ENTORNO DE ARCHIVOS TRADICIONAL

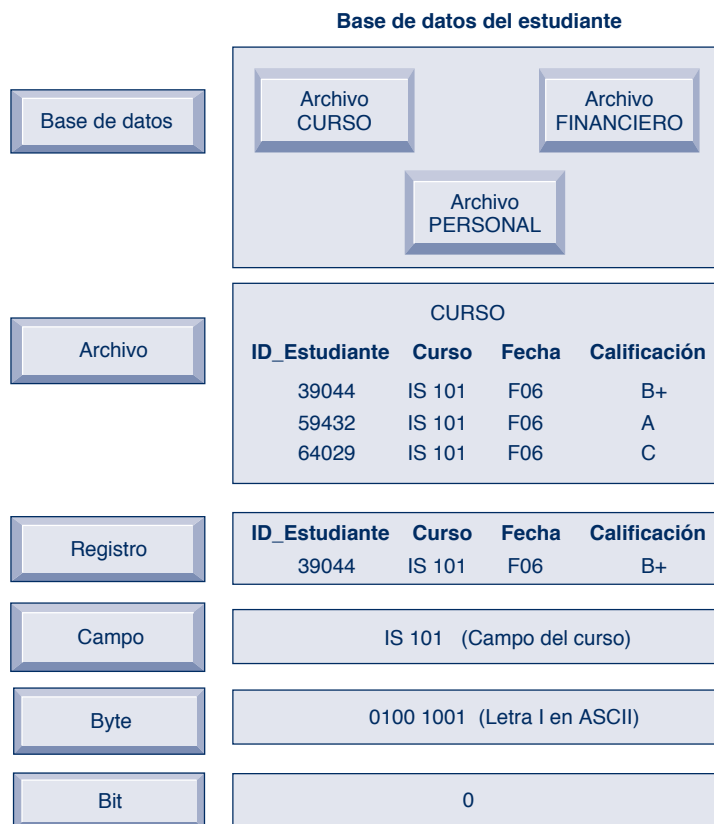
Un sistema de información efectivo provee a los usuarios información precisa, oportuna y relevante. La información precisa está libre de errores. La información es oportuna cuando está disponible para los encargados de tomar decisiones en el momento en que la necesitan. Así mismo, es relevante cuando es útil y apropiada tanto para los tipos de trabajos como para las decisiones que la requieren.

Tal vez le sorprenda saber que muchas empresas no tienen información oportuna, precisa o relevante debido a que los datos en sus sistemas de información han estado mal organizados y se les ha dado un mantenimiento inapropiado. Ésta es la razón por la que la administración de los datos es tan esencial. Para comprender el problema, veamos cómo es que los sistemas de información organizan los datos en archivos de computadora, junto con los métodos tradicionales de administración de archivos.

### TÉRMINOS Y CONCEPTOS DE ORGANIZACIÓN DE ARCHIVOS

Un sistema computacional organiza los datos en una jerarquía que empieza con bits y bytes, y progresa hasta llegar a los campos, registros, archivos y bases de datos (vea la figura 6-1). Un bit representa la unidad más pequeña de datos que una computadora pue-

**FIGURA 6-1 LA JERARQUÍA DE DATOS**



Un sistema computacional organiza los datos en una jerarquía, la cual empieza con el bit, que representa 0 o 1. Los bits se pueden agrupar para formar un byte que representa un carácter, número o símbolo. Los bytes se pueden agrupar para formar un campo, y los campos relacionados para constituir un registro. Los registros relacionados se pueden reunir para crear un archivo, y los archivos relacionados se pueden organizar en una base de datos.

de manejar. Un grupo de bits, denominado byte, representa a un solo carácter, que puede ser una letra, un número u otro símbolo. Un agrupamiento de caracteres en una palabra, un conjunto de palabras o un número completo (como el nombre o la edad de una persona) se denomina **campo**. Un grupo de campos relacionados, como el nombre del estudiante, el curso que va a tomar, la fecha y la calificación, representan un **registro**; un grupo de registros del mismo tipo se denomina **archivo**.

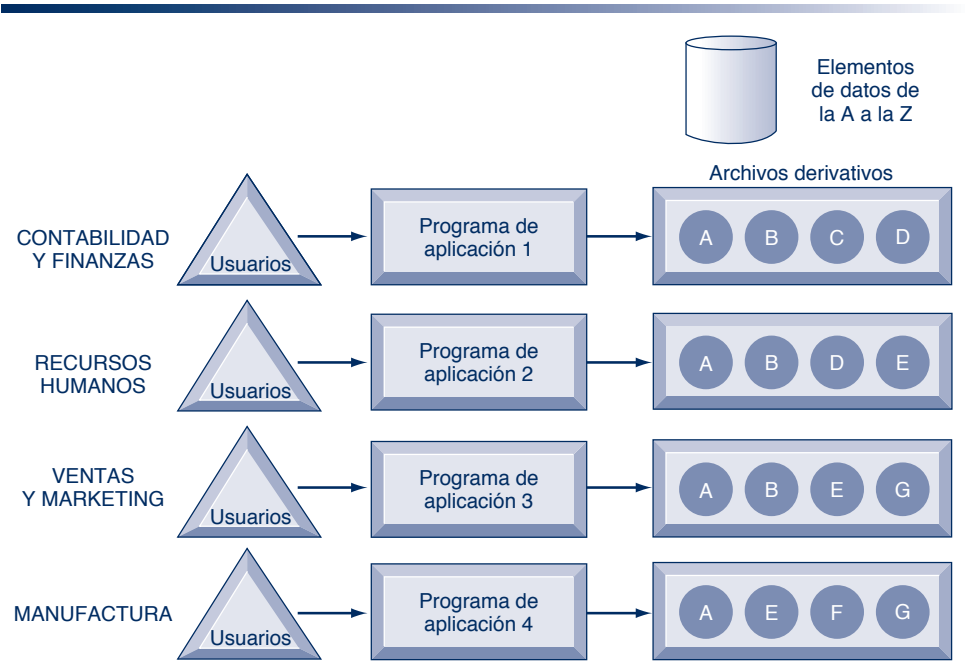
Por ejemplo, los registros en la figura 6-1 podrían constituir un archivo de cursos de estudiantes. Un grupo de archivos relacionados constituye una **base de datos**. El archivo de cursos de estudiantes que se ilustra en la figura 6-1 se podría agrupar con los archivos en los historiales personales de los estudiantes y sus antecedentes financieros, para crear una base de datos de estudiantes.

Un registro describe a una entidad. Una **entidad** es una persona, lugar, cosa o evento sobre el cual almacenamos y mantenemos información. Cada característica o cualidad que describe a una entidad específica se denomina **atributo**. Por ejemplo, ID\_Estudiante, Curso, Fecha y Calificaciones son atributos de la entidad CURSO. Los valores específicos que pueden tener estos atributos se encuentran en los campos del registro que describe a la entidad CURSO.

PROBLEMAS CON EL ENTORNO DE ARCHIVOS TRADICIONAL

En la mayoría de las organizaciones, los sistemas tendían a crecer de manera independiente sin un plan a nivel de toda la compañía. Contabilidad, finanzas, manufactura, recursos humanos, ventas y marketing han desarrollado sus propios sistemas y archivos de datos. La figura 6-2 ilustra la metodología normal para el procesamiento de la información.

FIGURA 6-2 PROCESAMIENTO DE ARCHIVOS TRADICIONAL



El uso de una metodología tradicional para el procesamiento de archivos impulsa a cada área funcional en una corporación a desarrollar aplicaciones especializadas. Cada aplicación requiere un archivo de datos único que probablemente sea un subconjunto del archivo maestro. Estos subconjuntos producen redundancia e inconsistencia en los datos, inflexibilidad en el procesamiento y desperdicio de los recursos de almacenamiento.



Desde luego que cada aplicación requería sus propios archivos y programa para operar. Por ejemplo, el área funcional de recursos humanos podría tener un archivo maestro de personal, uno de nómina, uno de seguros médicos, uno de pensiones, uno de listas de correos y así en lo sucesivo, hasta que existieran decenas, tal vez cientos, de archivos y programas. En la compañía en general, este proceso condujo a varios archivos maestros creados, mantenidos y operados por divisiones o departamentos separados. A medida que continúa este proceso durante cinco o 10 años, la organización se ve atestada de cientos de programas y aplicaciones que son muy difíciles de mantener y administrar. Los problemas resultantes son la redundancia e inconsistencia de los datos, la dependencia programa-datos, la inflexibilidad, la seguridad defectuosa de los datos y la incapacidad de compartir datos entre aplicaciones.

### Redundancia e inconsistencia de los datos

La **redundancia de los datos** es la presencia de datos duplicados en varios archivos, de modo que se almacenen los mismos datos en más de un lugar o ubicación. La redundancia ocurre cuando distintos grupos en una organización recolectan por separado la misma pieza de datos y la almacenan de manera independiente unos de otros. Desperdicia recursos de almacenamiento y también conduce a la **inconsistencia de los datos**, en donde el mismo atributo puede tener distintos valores. Por ejemplo, en las instancias de la entidad CURSO que se ilustran en la figura 6-1, la Fecha puede estar actualizada en algunos sistemas pero no en otros. El mismo atributo, ID\_Estudiante, también puede tener distintos nombres en los distintos sistemas en toda la organización. Por ejemplo, algunos sistemas podrían usar ID\_Estudiante y otros ID.

Asimismo se podría generar una confusión adicional al utilizar distintos sistemas de codificación para representar los valores de un atributo. Por ejemplo, los sistemas de ventas, inventario y manufactura de un vendedor minorista de ropa podrían usar distintos códigos para representar el tamaño de las prendas. Un sistema podría representar el tamaño como “extra grande”, mientras que otro podría usar el código “XL” para el mismo fin. La confusión resultante dificultaría a las compañías el proceso de crear sistemas de administración de relaciones con el cliente, de administración de la cadena de suministro o sistemas empresariales que integren datos provenientes de distintas fuentes.

### Dependencia programa-datos

La **dependencia programa-datos** se refiere al acoplamiento de los datos almacenados en archivos y los programas específicos requeridos para actualizar y dar mantenimiento a esos archivos, de tal forma que los cambios en los programas requieran cambios en los datos. Todo programa de computadora tradicional tiene que describir la ubicación y naturaleza de los datos con los que trabaja. En un entorno de archivos tradicional, cualquier cambio en un programa de software podría requerir un cambio en los datos a los que accede ese programa. Tal vez un programa se modifique de un código postal de cinco dígitos a nueve. Si el archivo de datos original se cambiara para usar códigos postales de nueve dígitos en vez de cinco, entonces otros programas que requirieran el código postal de cinco dígitos ya no funcionarían en forma apropiada. La implementación apropiada de dichos cambios podría costar millones de dólares.

### Falta de flexibilidad

Un sistema de archivos tradicional puede entregar informes programados de rutina después de cierto esfuerzo extenso de programación, pero no puede entregar informes ad hoc ni responder de manera oportuna a los requerimientos de información no anticipados. La información requerida por las solicitudes ad hoc está en alguna parte del sistema, pero tal vez sea demasiado costoso recuperarla. Tal vez varios programadores tengan que trabajar durante semanas para reunir los elementos de datos requeridos en nuevo archivo.

### Seguridad defectuosa

Como hay poco control o poca administración de los datos, el acceso a la información, así como su disseminación, pueden estar fuera de control. La gerencia tal vez no tenga forma de saber quién está accediendo a los datos de la organización, o incluso modificándolos.

### Falta de compartición y disponibilidad de los datos

Como las piezas de información en los distintos archivos y las diferentes partes de la organización no se pueden relacionar entre sí, es casi imposible compartir o acceder a la información de una manera oportuna. La información no puede fluir con libertad entre áreas funcionales o partes de la organización distintas. Si los usuarios encuentran valores desiguales de la misma pieza de información en dos sistemas diferentes, tal vez no quieran usar estos sistemas debido a que no pueden confiar en la precisión de sus datos.

## 6.2

### LA METODOLOGÍA DE LAS BASES DE DATOS PARA LA ADMINISTRACIÓN DE DATOS

La tecnología de las bases de datos resuelve muchos de los problemas de la organización de los archivos tradicionales. Una definición más rigurosa de una **base de datos** es la de una colección de datos organizados para dar servicio a muchas aplicaciones de manera eficiente, al centralizar los datos y controlar los que son redundantes. En vez de guardar los datos en archivos separados para cada aplicación, se almacenan de modo que los usuarios creen que están en una sola ubicación. Una sola base de datos da servicio a varias aplicaciones. Por ejemplo, en vez de que una corporación almacene los datos de los empleados en sistemas de información y archivos separados para personal, nómina y beneficios, podría crear una sola base de datos común de recursos humanos.

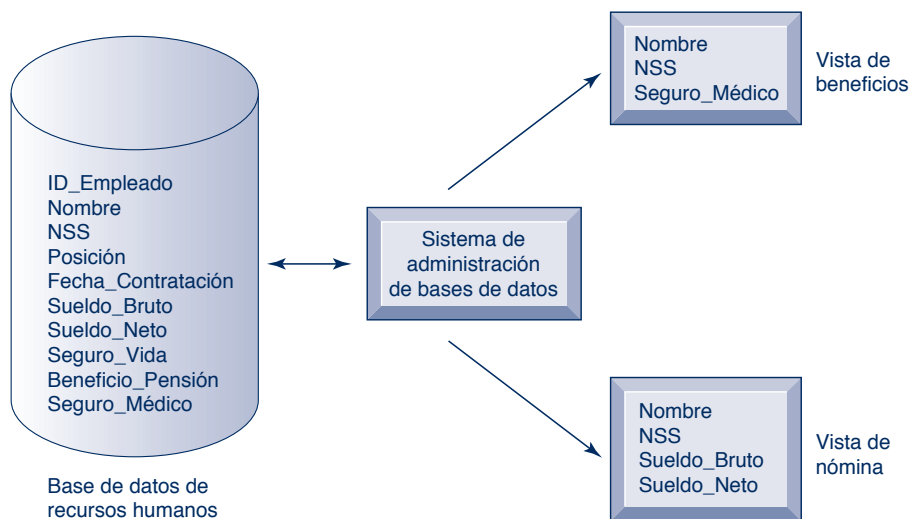
### SISTEMAS DE ADMINISTRACIÓN DE BASES DE DATOS

Un **Sistema de Administración de Bases de Datos (DBMS)** es software que permite a una organización centralizar los datos, administrarlos en forma eficiente y proveer acceso a los datos almacenados mediante programas de aplicación. El DBMS actúa como una interfaz entre los programas de aplicación y los archivos de datos físicos. Cuando el programa de aplicación solicita un elemento de datos, como el sueldo bruto, el DBMS lo busca en la base de datos y lo presenta al programa de aplicación. Si utilizara archivos de datos tradicionales, el programador tendría que especificar el tamaño y formato de cada elemento de datos utilizado en el programa y después decir a la computadora en dónde están ubicados.

El DBMS libera al programador o al usuario final de la tarea de comprender en dónde y cómo están almacenados los datos en realidad, al separar las vistas lógica y física de los datos. La *vista lógica* presenta los datos según la manera en que los perciben los usuarios finales o los especialistas de negocios, mientras que la *vista física* muestra la verdadera forma en que están organizados y estructurados los datos en los medios de almacenamiento físicos.

El software de administración de bases de datos se encarga de que la base de datos física esté disponible para las diferentes vistas lógicas requeridas por los usuarios. Por ejemplo, para la base de datos de recursos humanos que se ilustra en la figura 6-3, un especialista de negocios podría requerir una vista que consista en el nombre del empleado, número de seguro social y cobertura del seguro médico. El miembro de un departamento de nómina podría necesitar datos tales como el nombre del empleado, el número de seguro social, el sueldo bruto y neto. Los datos para todas estas vistas se

**FIGURA 6-3 BASE DE DATOS DE RECURSOS HUMANOS CON VARIAS VISTAS**



Una sola base de datos de recursos humanos provee muchas vistas distintas de los datos, dependiendo de los requerimientos de información del usuario. Aquí se ilustran dos posibles vistas, una de interés para un especialista de beneficios y otra de interés para un miembro del departamento de nómina de la compañía.

almacenan en una sola base de datos, en donde la organización puede administrarlos con más facilidad.

### Cómo resuelve un DBMS los problemas del entorno de archivos tradicionales

Un DBMS reduce la redundancia e inconsistencia de los datos al minimizar los archivos aislados en los que se repiten los mismos datos. Tal vez el DBMS no logre que la organización elimine la redundancia de datos en su totalidad, pero puede ayudar a controlarla. Incluso si la organización mantiene ciertos datos redundantes, el uso de un DBMS elimina la inconsistencia de los datos debido a que puede ayudar a la organización a asegurar que cada ocurrencia de datos redundantes tenga los mismos valores. El DBMS desacopla los programas y los datos, con lo cual estos últimos se pueden independizar. El acceso y la disponibilidad de la información serán mayores, a la vez que se reducirán los costos de desarrollo y mantenimiento de los programas debido a que los usuarios y programadores pueden realizar consultas ad hoc de la información en la base de datos. El DBMS permite a la organización administrar los datos, su uso y su seguridad en forma central.

### DBMS relacional

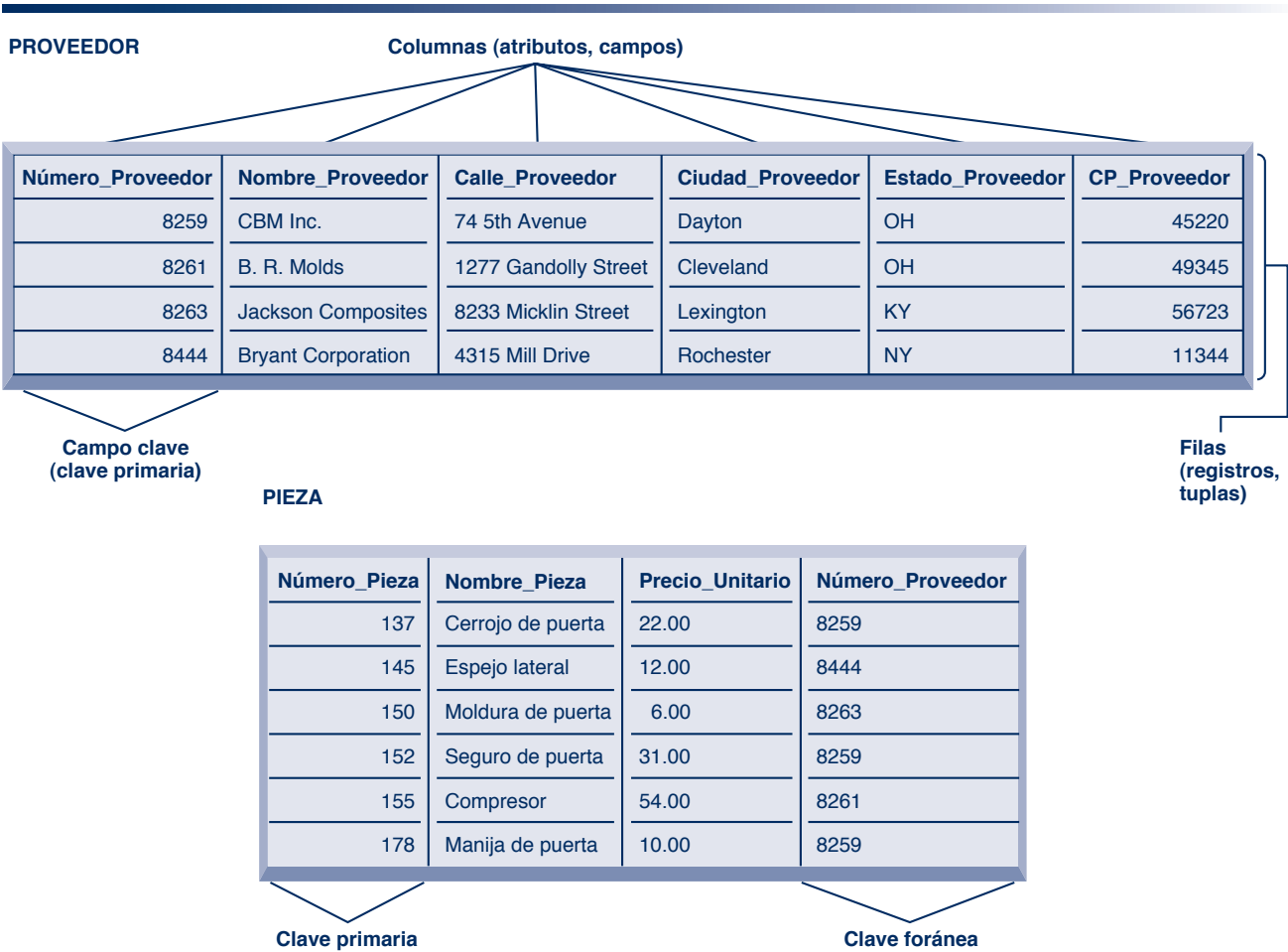
Los DBMS contemporáneos utilizan distintos modelos de bases de datos para llevar el registro de las entidades, atributos y relaciones. El tipo más popular de sistemas DBMS en la actualidad para las PCs, así como para computadoras más grandes y mainframes, es el **DBMS relacional**. Las bases de datos relacionales representan los datos como tablas bidimensionales (llamadas relaciones), a las cuales se puede hacer referencia como si fueran archivos. Cada tabla contiene datos sobre una entidad y sus atributos. Microsoft Access es un DBMS relacional para sistemas de escritorio, mientras que DB2, Oracle Database y Microsoft SQL Server son DBMS relacionales para las grandes mainframes y las computadoras de rango medio. MySQL es un popular DBMS de código fuente abierto; Oracle Database Lite es un DBMS para pequeños dispositivos de cómputo portátiles.

Veamos ahora cómo organiza una base de datos relacional la información sobre proveedores y piezas (vea la figura 6-4). La base de datos tiene una tabla separada para la entidad PROVEEDOR y una para la entidad PIEZA. Cada tabla consiste en una cuadrícula de columnas y filas de datos. Cada elemento individual de datos para cada entidad se almacena como un campo separado, y cada campo representa un atributo para esa entidad. Los campos en una base de datos relacionales también se llaman columnas. Para la entidad PROVEEDOR, el número de identificación de proveedor, nombre, calle, ciudad, estado y código postal se almacenan como campos separados dentro de la tabla PROVEEDOR y cada campo representa un atributo para la entidad PROVEEDOR.

La información real sobre un solo proveedor que reside en una tabla se denomina fila. Por lo general las filas se conocen como registros, o en términos muy técnicos, como **tuplas**. Los datos para la entidad PIEZA tienen su propia tabla separada.

El campo para Nombre\_Proveedor en la tabla PROVEEDOR identifica a cada registro en forma única, de modo que ese registro se pueda recuperar, actualizar u ordenar, y se denomina **campo clave**. Cada tabla en una base de datos relacional tiene un campo que se designa como su **clave primaria**. Este campo clave es el identificador único para toda la información en cualquier fila de la tabla y su clave primaria no puede estar duplicada. Numero\_Proveedor es la clave primaria para la tabla PROVEEDOR y

FIGURA 6-4 TABLAS DE BASES DE DATOS RELACIONALES



Una base de datos relacional organiza los datos en forma de tablas bidimensionales. Aquí se ilustran las tablas para las entidades PROVEEDOR y PIEZA, las cuales muestran cómo representan a cada entidad y sus atributos. Numero\_Proveedor es una clave primaria para la tabla PROVEEDOR y una clave foránea para la tabla PIEZA.

Numero\_Pieza es la clave primaria para la tabla PIEZA. Observe que Numero\_Proveedor aparece tanto en la tabla PROVEEDOR como en PIEZA. En la tabla PROVEEDOR, Numero\_Proveedor es la clave primaria. Cuando el campo Numero\_Proveedor aparece en la tabla PIEZA se denomina **clave foránea**, la cual es en esencia un campo de búsqueda para averiguar datos sobre el proveedor de una pieza específica.

## Operaciones de un DBMS relacional

Las tablas de bases de datos relacionales se pueden combinar con facilidad para ofrecer los datos requeridos por los usuarios, siempre y cuando dos tablas cualesquiera compartan un elemento de datos común. Suponga que queremos encontrar en esta base de datos los nombres de los proveedores que nos puedan suministrar el número de pieza 137 o el 150. Necesitaríamos información de dos tablas: la tabla PROVEEDOR y la tabla PIEZA. Observe que estos dos archivos tienen un elemento de datos compartido: Numero\_Proveedor.

En una base de datos relacional se utilizan tres operaciones básicas, como se muestra en la figura 6-5, para desarrollar conjuntos útiles de datos: seleccionar, unir y proyectar. La operación *seleccionar* crea un subconjunto que consiste en todos los registros del archivo que cumplan con criterios establecidos. En otras palabras, la selección crea un subconjunto de filas que cumplen con ciertos criterios. En nuestro ejemplo, queremos seleccionar registros (filas) de la tabla PIEZA en donde el Numero\_Pieza sea igual a 137 o 150. La operación *unir* combina tablas relacionales para proveer al usuario más información de la que está disponible en las tablas individuales. En nuestro ejemplo, queremos unir la tabla PIEZA, que ya está recortada (sólo se presentarán las piezas 137 o 150), con la tabla PROVEEDOR en una sola tabla nueva.

La operación *proyectar* crea un subconjunto que consiste de columnas en una tabla, con lo cual el usuario puede crear nuevas tablas que contengan sólo la información requerida. En nuestro ejemplo queremos extraer de la nueva tabla sólo las siguientes columnas: Numero\_Pieza, Nombre\_Pieza, Numero\_Proveedor y Nombre\_Proveedor.

## DBMS orientado a objetos

En la actualidad y en el futuro, muchas aplicaciones requerirán bases de datos que puedan almacenar y recuperar no sólo números y caracteres estructurados, sino también dibujos, imágenes, fotografías, voz y video en movimiento completo. Los DBMS diseñados para organizar datos estructurados en filas y columnas no se adaptan bien al manejo de aplicaciones basadas en gráficos o multimedia. Las bases de datos orientadas a objetos son más adecuadas para este propósito.

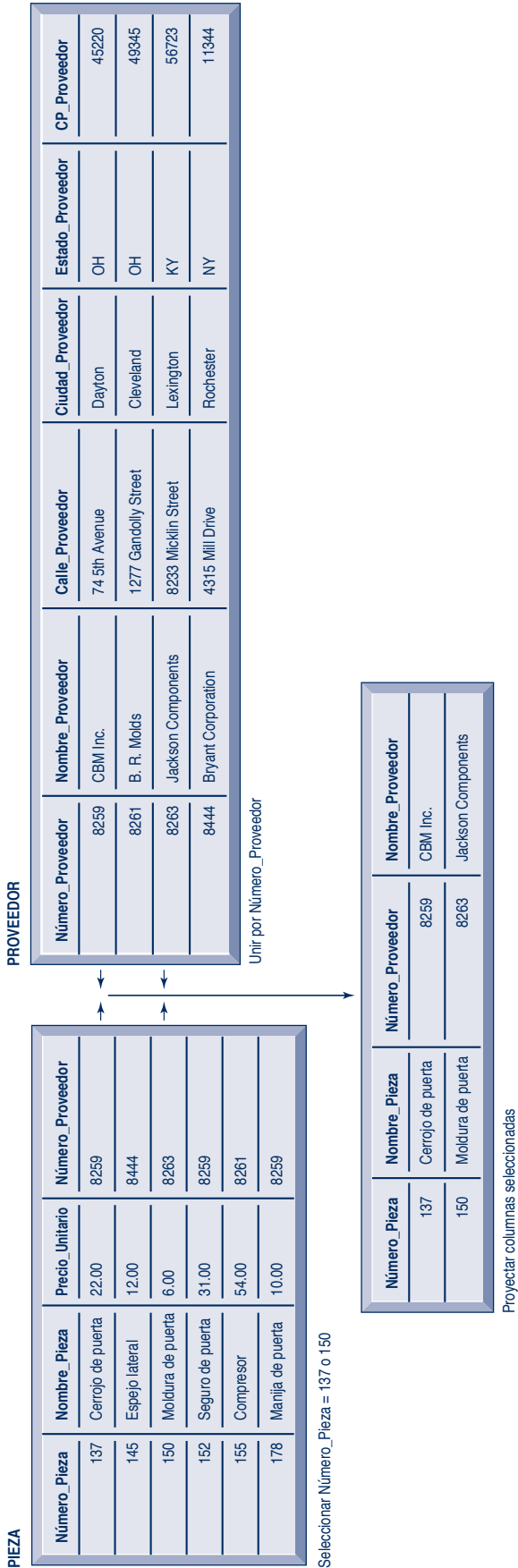
Un **DBMS orientado a objetos** almacena los datos y los procedimientos que actúan sobre esos datos como objetos que se pueden recuperar y compartir de manera automática. Los Sistemas de Administración de Bases de Datos Orientados a Objetos (OODBMS) están ganando popularidad debido a que se pueden utilizar para manejar los diversos componentes multimedia o los applets de Java que se utilizan en las aplicaciones Web, que por lo general integran piezas de información provenientes de una variedad de orígenes.

Aunque las bases de datos orientadas a objetos pueden almacenar tipos más complejos de información que los DBMS relacionales, son lentos en comparación con los DBMS relacionales para procesar grandes números de transacciones. Ahora hay sistemas **DBMS objeto-relacional** híbridos, que ofrecen las capacidades de los sistemas DBMS tanto orientados a objetos como relacionales.

## Bases de datos en la nube

Suponga que su compañía desea utilizar los servicios de computación en la nube. ¿Hay alguna forma de administrar los datos en la nube? La respuesta es un "sí" condicional. Los proveedores de computación en la nube ofrecen servicios de administración de bases de datos, pero por lo general estos servicios tienen menos funcionalidad que sus contrapartes dentro de las premisas de la empresa. Por el momento, la base de clientes primordial para la administración de datos basados en la nube consiste en

FIGURA 6-5 LAS TRES OPERACIONES BÁSICAS DE UN DBMS RELACIONAL



Las operaciones seleccionar, unir y proyectar permiten combinar datos de dos tablas distintas y mostrar sólo los atributos seleccionados.



empresas iniciales enfocadas en Web o negocios desde pequeños hasta medianos que buscan capacidades de bases de datos a un menor precio que el de un DBMS relacional estándar.

Amazon Web Services cuenta con una base de datos no relacional simple llamada SimpleDB y también con un servicio de bases de datos relacionales, el cual se basa en una implementación en línea de MySQL, el DBMS de código fuente abierto. Amazon Relational Database Service (Amazon RDS) ofrece el rango completo de capacidades de MySQL. El precio se basa en el uso (los costos varían desde 11 centavos por hora para una pequeña base de datos que utilice 1.7 GB de memoria del servidor, hasta \$3.10 por hora para una base de datos extensa que utilice 68 GB de memoria del servidor). También hay cargos por el volumen de datos almacenado, el número de solicitudes de entrada-salida, la cantidad de datos que se escriben en la base de datos y la cantidad que se leen de ella.

Además, Amazon Web Services ofrece a los clientes de Oracle la opción de obtener una licencia de Oracle Database 11g, Oracle Enterprise Manager y Oracle Fusion Middleware para ejecutarlos en la plataforma Amazon EC2 (nube de cómputo elástica).

Microsoft SQL Azure Database es un servicio de bases de datos relacionales basado en la nube y en el DBMS SQL Server de Microsoft. Ofrece un servicio de bases de datos con alta disponibilidad y escalable, hospedado por Microsoft en la nube. SQL Azure Database ayuda a reducir los costos al integrarse con las herramientas de software existentes y proveer simetría con las bases de datos tanto en las premisas de la empresa como en la nube.

TicketDirect, que vende boletos para conciertos, eventos deportivos, obras de teatro y películas en Australia y Nueva Zelanda, adoptó la plataforma de nube SQL Azure Database para poder mejorar la administración de las cargas pico del sistema durante los periodos con muchas ventas de boletos. Migró sus datos a la base de datos SQL Azure. Al cambiar a una solución en la nube, TicketDirect pudo escalar sus recursos de cómputo en respuesta a la demanda en tiempo real, al tiempo que mantuvo sus costos bajos.

## CAPACIDADES DE LOS SISTEMAS DE ADMINISTRACIÓN DE BASES DE DATOS

Un DBMS incluye capacidades y herramientas para organizar, administrar y acceder a los datos en la base de datos. Las más importantes son: su lenguaje de definición de datos, el diccionario de datos y el lenguaje de manipulación de datos.

Los DBMS tienen una capacidad de **definición de datos** para especificar la estructura del contenido de la base de datos. Podría usarse para crear tablas de bases de datos y definir las características de los campos en cada tabla. Esta información sobre la base de datos se puede documentar en un **diccionario de datos**, el cual es un archivo automatizado o manual que almacena las definiciones de los elementos de datos y sus características.

Microsoft Access cuenta con una herramienta rudimentaria de diccionario de datos, la cual muestra información sobre el nombre, la descripción, el tamaño, tipo, formato y otras propiedades de cada campo en una tabla (vea la figura 6-6). Los diccionarios de datos para las grandes bases de datos corporativas pueden capturar información adicional, como el uso, la propiedad (quién en la organización es responsable de dar mantenimiento a la información), autorización, seguridad y los individuos, funciones de negocios, programas e informes que utilizan cada elemento de datos.

### Consultas e informes

Un DBMS contiene herramientas para acceder a la información en las bases de datos y manipularla. La mayoría de los DBMS tienen un lenguaje especializado conocido como **lenguaje de manipulación de datos** el cual se utiliza para agregar, modificar, eliminar y recuperar los datos en la base. Este lenguaje contiene comandos que permiten a los usuarios finales y a los especialistas de programación extraer los datos de la base para satisfacer las solicitudes de información y desarrollar aplicaciones. El lenguaje de manipulación de datos más prominente en la actualidad es el **lenguaje de consulta estructurado**, o **SQL**. La figura 6-7 ilustra la consulta de SQL que produciría la nueva tabla

**FIGURA 6-6** **CARACTERÍSTICAS DEL DICCIONARIO DE DATOS  
DE MICROSOFT ACCESS**

**FIGURA 6-8 UNA CONSULTA EN ACCESS**

se construiría la misma consulta que la SQL para seleccionar piezas y proveedores, pero ahora mediante las herramientas para crear consultas de Microsoft.

Microsoft Access y otros sistemas DBMS tienen herramientas para generación de informes, de modo que se puedan mostrar los datos de interés en un formato más estructurado y elegante que el de las consultas. Crystal Reports es un popular generador de informes para los DBMS corporativos extensos, aunque también se puede utilizar con Access. Este último también cuenta con herramientas para desarrollar aplicaciones de sistemas de escritorio. Se incluyen herramientas para crear pantallas de captura de datos, para generar informes y desarrollar la lógica de procesamiento de transacciones.

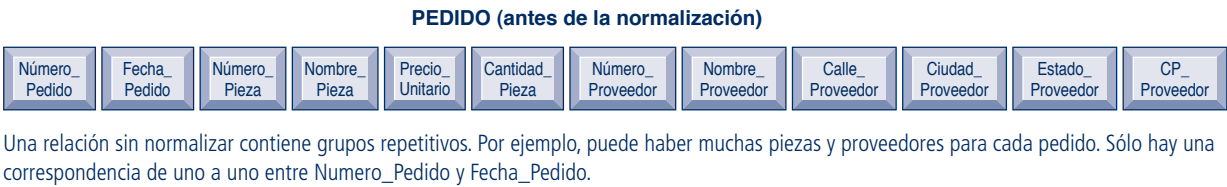
## DISEÑO DE BASES DE DATOS

Para crear una base de datos hay que comprender las relaciones entre la información, el tipo de datos que se mantendrán en la base, cómo se utilizarán y la forma en que tendrá que cambiar la organización para administrarlos desde una perspectiva a nivel de toda la compañía. La base de datos requiere tanto un diseño conceptual como uno físico. El diseño conceptual o lógico de la base de datos es un modelo abstracto de ésta desde una perspectiva de negocios, mientras que el diseño físico muestra la verdadera disposición de la base de datos en los dispositivos de almacenamiento de acceso directo.

### Diagramas de normalización y de entidad-relación

El diseño de bases de datos conceptual describe la forma en que se deben agrupar los elementos de datos en la base. El proceso de diseño identifica las relaciones entre los elementos de datos y la manera más eficiente de agruparlos en conjunto para satisfacer los requerimientos de información de la empresa. Este proceso también identifica a los elementos de datos redundantes y las agrupaciones de elementos de datos requeridas

FIGURA 6-9 UNA RELACIÓN SIN NORMALIZAR PARA PEDIDO



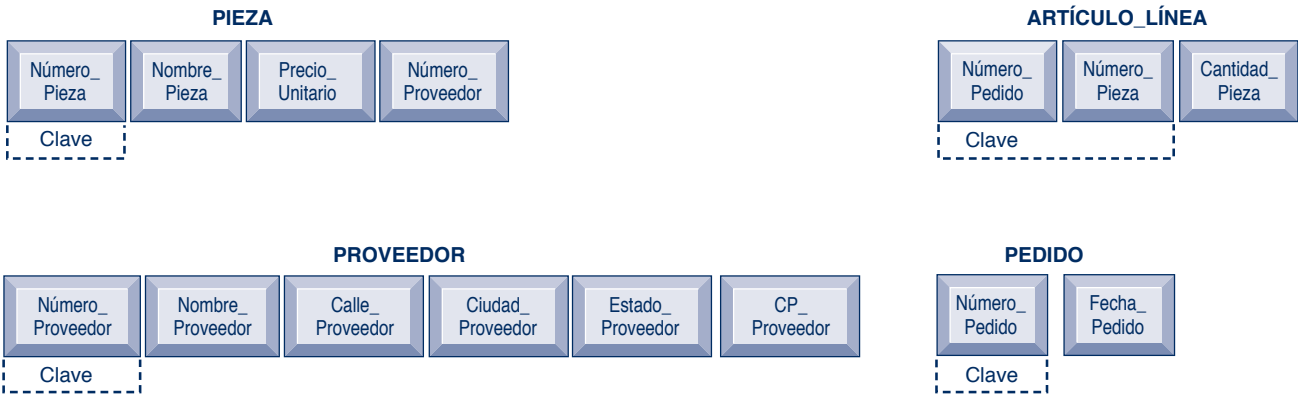
para ciertos programas de aplicaciones específicos. Los grupos de datos se organizan, refinan y optimizan hasta que emerge una vista lógica general de las relaciones entre todos los datos en la base.

Para usar un modelo de base de datos relacional en forma efectiva, hay que optimizar los agrupamientos complejos de datos para minimizar los elementos de datos redundantes y las incómodas relaciones de varios a varios. El proceso de crear estructuras de datos pequeñas y estables pero a la vez flexibles y adaptivas a partir de grupos complejos de datos se denomina **normalización**. Las figuras 6-9 y 6-10 ilustran este proceso.

En la empresa específica que se modela aquí, un pedido puede tener más de una pieza, pero cada una sólo es proporcionada por un proveedor. Si creamos una relación llamada PEDIDO con todos los campos que se incluyen aquí, tendríamos que repetir el nombre y la dirección del proveedor para cada pieza del pedido, aun y cuando éste sea de piezas de un solo proveedor. Esta relación contiene lo que se denomina grupos de datos repetitivos, ya que puede haber muchas piezas en un solo pedido para un proveedor dado. Una manera más eficiente de ordenar los datos es dividir PEDIDO en relaciones más pequeñas, cada una de las cuales describe a una sola entidad. Si avanzamos paso a paso y normalizamos la relación PEDIDO, obtendremos las relaciones que se ilustran en la figura 6-10. Para averiguar más sobre la normalización, los diagramas entidad-relación y el diseño de bases de datos, consulte las Trayectorias de aprendizaje de este capítulo.

Los sistemas de bases de datos relacionales tratan de cumplir reglas de **integridad referencial** para asegurar que las relaciones entre las tablas acopladas permanezcan consistentes. Cuando una tabla tiene una clave foránea que apunta a otra, no es posible agregar un registro a la tabla con la clave foránea a menos que haya uno correspondiente en la tabla vinculada. En la base de datos que examinamos antes en el

FIGURA 6-10 TABLAS NORMALIZADAS CREADAS A PARTIR DE PEDIDO



Después de la normalización, la relación original PEDIDO se divide en cuatro relaciones más pequeñas. La relación PEDIDO se queda con sólo dos atributos y la relación ARTICULO\_LINEA tiene una clave combinada, o concatenada, que consiste en Numero\_Pedido y Numero\_Pieza.

capítulo, la clave foránea Numero\_Proveedor vincula la tabla PIEZA con la tabla PROVEEDOR. No podemos agregar un nuevo registro a la tabla PIEZA para una pieza con el Numero\_Proveedor 8266 a menos que haya un registro correspondiente en la tabla PROVEEDOR para el Numero\_Proveedor 8266. También debemos eliminar el registro correspondiente en la tabla PIEZA si quitamos el registro en la tabla PROVEEDOR para el Numero\_Proveedor 8266. En otras palabras, ¡no debemos tener piezas de proveedores que no existen!

Los diseñadores de bases de datos documentan su modelo de datos con un **diagrama entidad-relación**, el cual se ilustra en la figura 6-11. Este diagrama muestra la relación entre las entidades PROVEEDOR, PIEZA, ARTICULO\_LINEA y PEDIDO. Los cuadros representan las entidades, y las líneas que conectan los cuadros, las relaciones. Una línea que conecta dos entidades que termina en dos marcas cortas designa una relación de uno a uno. Una línea que conecta dos entidades y termina con una pata de cuervo y una marca corta encima de ella indica una relación de uno a varios. La figura 6-11 muestra que un PEDIDO puede contener varios ARTICULO\_LINEA (es posible ordenar una PIEZA muchas veces y aparecer otras tantas como artículo de línea en un solo pedido). Cada PIEZA sólo puede tener un PROVEEDOR, pero muchos elementos PIEZA pueden ser proporcionados por el mismo PROVEEDOR.

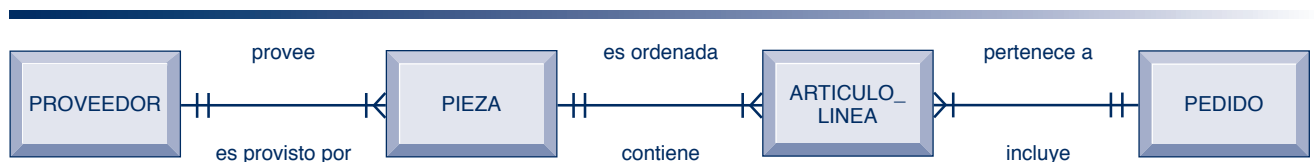
No podemos enfatizarlo lo suficiente: si el modelo de datos de la empresa no es el correcto, el sistema no podrá dar buen servicio a la empresa. Los sistemas de la compañía no serán tan efectivos como podrían serlo debido a que tendrán que trabajar con datos que tal vez sean imprecisos, incompletos o difíciles de recuperar. Comprender los datos de la organización y la forma en que se deben representar en una base de datos es tal vez la lección más importante que puede usted aprender de este curso.

Por ejemplo, Famous Footwear, una cadena de zapaterías con más de 800 sucursales en 49 estados, no pudo lograr su objetivo de tener “el estilo correcto de zapato en la tienda apropiada para venderse al precio adecuado”, ya que su base de datos no estaba diseñada en forma correcta para ajustar con rapidez el inventario de las tiendas. La compañía tenía una base de datos relacional Oracle operando en una computadora IBM AS/400 de medio rango, pero el objetivo primordial para el que se diseñó la base de datos era producir informes estándar para la gerencia, en vez de reaccionar a los cambios en el mercado. La gerencia no pudo obtener datos precisos sobre artículos específicos en el inventario en cada una de sus tiendas. Para solucionar este problema, la compañía tuvo que crear una nueva base de datos en donde se pudieran organizar mejor los datos de las ventas y del inventario para realizar análisis y administrar el inventario.

## 6.3 USO DE BASES DE DATOS PARA MEJORAR EL DESEMPEÑO DE NEGOCIOS Y LA TOMA DE DECISIONES

Las empresas utilizan sus bases de datos para llevar el registro de las transacciones básicas, como pagar a los proveedores, procesar pedidos, llevar el registro de los clientes y pagar a los empleados. Pero también se necesitan bases de datos para proveer

**FIGURA 6-11 UN DIAGRAMA ENTIDAD-RELACIÓN**



El diagrama muestra las relaciones entre las entidades PROVEEDOR, PIEZA, ARTICULO\_LINEA y PEDIDO que se podrían usar para modelar la base de datos de la figura 6-10.

información que ayude a la compañía a operar sus negocios con más eficiencia, y ayudar a los gerentes y empleados a tomar mejores decisiones. Si una compañía desea saber cuál producto es el más popular o quién es su cliente más rentable, la respuesta radica en los datos.

Por ejemplo, al analizar los datos de las compras de los clientes con tarjeta de crédito, la cadena de restaurantes Lousie's Trattoria de Los Ángeles descubrió que la calidad era más importante que el precio para la mayoría de sus clientes, que tenían educación universitaria y les gustaba el vino fino. Con base en esta información, la cadena introdujo platillos vegetarianos, más selecciones de mariscos y vinos más costosos, con lo cual se elevaron las ventas en más de un 10 por ciento.

En una compañía grande, con bases de datos o sistemas extensos para funciones separadas, como manufactura, ventas y contabilidad, se requieren capacidades y herramientas especiales para analizar enormes cantidades de datos y acceder a los datos de múltiples sistemas. Estas capacidades incluyen almacenes de datos, minería de datos y herramientas para acceder a las bases de datos internas a través de Web.

## ALMACENES DE DATOS

Suponga que desea información concisa y confiable sobre las operaciones, tendencias y cambios actuales a través de toda la compañía. Si trabajara en una empresa grande, podría ser difícil obtener esta información debido a que, con frecuencia, los datos se mantienen en sistemas separados, como en ventas, manufactura o contabilidad. Tal vez algunos de los datos que llegara a necesitar estuvieran en el sistema de ventas, mientras que otros podrían encontrarse en el sistema de manufactura. Muchos son sistemas antiguos heredados que usan tecnologías de administración de datos o sistemas de archivos obsoletos, en donde es difícil para los usuarios acceder a la información.

Tal vez tendría que invertir una cantidad exorbitante de tiempo para localizar y recopilar los datos que necesitara, o se vería obligado a tomar su decisión con base en un conocimiento incompleto. Y si deseara información sobre las tendencias, tal vez también tendría problemas para encontrar datos sobre los eventos anteriores, ya que en la mayoría de las empresas sólo sus datos actuales están disponibles de inmediato. Los almacenes de datos se encargan de estos problemas.

### ¿Qué es un almacén de datos?

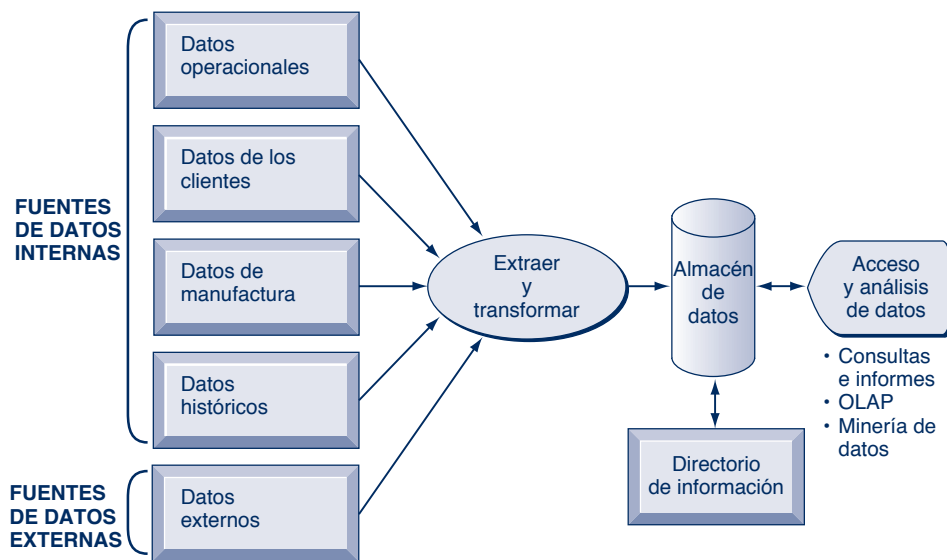
Un **almacén de datos** es una base de datos que almacena la información actual e histórica de interés potencial para los encargados de tomar decisiones en la compañía. Los datos se originan en muchos sistemas de transacciones operacionales básicos, como los sistemas de ventas, las cuentas de clientes, la manufactura, y pueden incluir datos de transacciones de sitios Web. El almacén de datos consolida y estandariza la información de distintas bases de datos operacionales, de modo que se pueda utilizar en toda la empresa para el análisis gerencial y la toma de decisiones.

La figura 6-12 ilustra cómo funciona un almacén de datos. Éste pone los datos a disposición de cualquiera que los necesite, pero no se pueden alterar. Un sistema de almacén de datos también provee un rango de herramientas de consulta ad hoc y estandarizadas, herramientas analíticas y facilidades de informes gráficos. Muchas empresas usan portales de intranets para que la información del almacén de datos esté disponible en toda la empresa.

Catalina Marketing, una empresa de marketing global para importantes compañías y minoristas de bienes empaquetados para el consumidor, opera un almacén de datos gigante que incluye tres años de historial de compras para 195 millones de miembros del programa de lealtad de clientes en Estados Unidos en supermercados, farmacias y otros minoristas. Es la base de datos de lealtad más grande del mundo. Los clientes de la tienda minorista de Catalina analizan esta base de datos de historiales de compras de los clientes para determinar las preferencias de compras de los clientes individuales. Cuando un comprador paga en la caja registradora de uno de los clientes minoristas de Catalina, la compra se analiza al instante junto con el historial de compra de ese cliente



**FIGURA 6-12 COMPONENTES DE UN ALMACÉN DE DATOS**



El almacén de datos extrae los datos actuales e históricos de varios sistemas operacionales dentro de la organización. Estos datos se combinan con los provenientes de fuentes externas y se reorganizan en una base de datos central, diseñada para realizar informes y análisis gerenciales. El directorio de información da a conocer a los usuarios los datos disponibles en el almacén.

en el almacén de datos, para determinar qué cupones recibirá el cliente al momento de pagar, junto con su recibo.

El Servicio de Recaudación de Impuestos (IRS) de Estados Unidos mantiene un almacén de datos de conformidad que consolida la información de los contribuyentes que se ha fragmentado entre varios sistemas heredados distintos, contiene los datos personales sobre contribuyentes y devoluciones fiscales archivadas. Estos sistemas se habían diseñado para procesar formularios de devolución de impuestos de manera eficiente, pero sus datos eran muy difíciles de consultar y analizar. El almacén de datos de conformidad integra los datos de los contribuyentes de muchas fuentes dispares en una estructura relacional, lo cual facilita en gran medida las consultas y el análisis. Con una imagen completa y exhaustiva de los contribuyentes, el almacén ayuda a los analistas y al personal del IRS a identificar las personas que tienen más probabilidades de hacer trampa en sus pagos de impuestos y a responder con rapidez a las consultas de los contribuyentes.

## Mercados de datos

A menudo las compañías crean almacenes de datos a nivel empresarial, en donde un almacén de datos central da servicio a toda la organización, o crean almacenes más pequeños y descentralizados, conocidos como mercados de datos. Un **mercado de datos** es un subconjunto de un almacén de datos, en el cual se coloca una porción con alto grado de enfoque en los datos de la organización en una base de datos separada para una población específica de usuarios. Por ejemplo, una compañía podría desarrollar mercados de datos sobre marketing y ventas para lidiar con la información de los clientes. Antes de implementar un almacén de datos a nivel empresarial, la librería Barnes & Noble mantenía una serie de mercados de datos: uno para los datos sobre los puntos de venta en las tiendas minoristas, otro para las ventas de las librerías universitarias y un tercero para las ventas en línea. Por lo general, un mercado de datos se enfoca en un solo tema o línea de negocios, por lo que es común que se construya con más rapidez y a un menor costo que un almacén de datos a nivel empresarial.

## HERRAMIENTAS PARA LA INTELIGENCIA DE NEGOCIOS: ANÁLISIS DE DATOS MULTIDIMENSIONAL Y MINERÍA DE DATOS

Una vez que los datos en línea se capturan y organizan en almacenes y mercados de datos, están disponibles para su posterior análisis mediante el uso de las herramientas para inteligencia de negocios, de las que hablamos brevemente en el capítulo 2. Las herramientas de inteligencia de negocios permiten a los usuarios analizar datos para ver nuevos patrones, relaciones y perspectivas que son útiles para guiar la toma de decisiones.

Las principales herramientas para la inteligencia de negocios incluyen el software para consultas e informes de bases de datos, herramientas para el análisis de datos multidimensional (procesamiento analítico en línea), y herramientas para la minería de datos. En esta sección le presentaremos estas herramientas; veremos más detalles sobre la ciencia del análisis de inteligencia de negocios y las aplicaciones al examinar la toma de decisiones en el capítulo 12.

### Procesamiento analítico en línea (OLAP)

Suponga que su compañía vende cuatro productos distintos: tuercas, pernos, arandelas y tornillos en las regiones Este, Oeste y Central. Si desea hacer una pregunta bastante directa, como cuántas arandelas se vendieron durante el trimestre pasado, podría encontrar la respuesta con facilidad al consultar su base de datos de ventas. Pero, ¿qué pasaría si quisiera saber cuántas arandelas se vendieron en cada una de sus regiones de ventas, para comparar los resultados actuales con las ventas proyectadas?

Para obtener la respuesta, necesitaría el **Procesamiento Analítico en Línea (OLAP)**. OLAP soporta el análisis de datos multidimensional, el cual permite a los usuarios ver los mismos datos de distintas formas mediante el uso de varias dimensiones. Cada aspecto de información —producto, precios, costo, región o periodo de tiempo— representa una dimensión distinta. Así, un gerente de productos podría usar una herramienta de análisis de datos multidimensional para saber cuántas arandelas se vendieron en el Este en junio, cómo se compara esa cifra con la del mes anterior y con la de junio del año anterior, y cómo se compara con el pronóstico de ventas. OLAP permite a los usuarios obtener respuestas en línea a las preguntas ad hoc tales como éstas en un periodo de tiempo bastante corto, incluso cuando los datos se almacenan en bases de datos muy grandes, como las cifras de ventas de varios años.

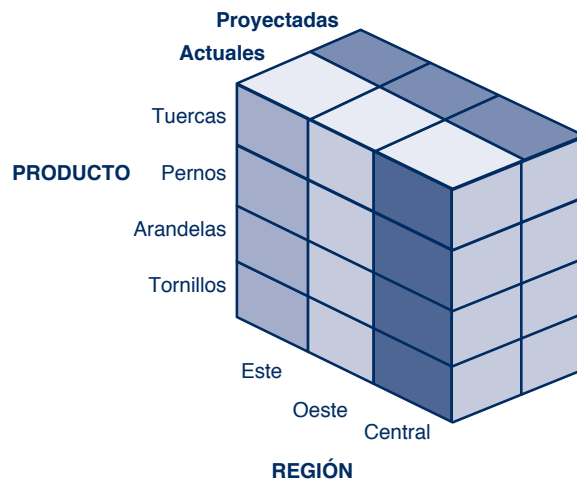
La figura 6-13 muestra un modelo multidimensional que podría crearse para representar productos, regiones, ventas reales y ventas proyectadas. Una matriz de ventas actuales se puede apilar encima de una matriz de ventas proyectadas para formar un cubo con seis caras. Si gira el cubo 90 grados en un sentido, la cara que se muestre será la de producto contra ventas actuales y proyectadas, si lo gira 90 grados de nuevo, verá la cara de región contra ventas actuales y proyectadas, si lo gira 180 grados a partir de la vista original, verá las ventas proyectadas y producto contra región. Se pueden anidar cubos dentro de otros cubos para crear vistas complejas de datos. Una compañía podría utilizar una base de datos multidimensional especializada o una herramienta que cree vistas multidimensionales de datos en las bases de datos relacionales.

### Minería de datos

Las consultas en las bases de datos tradicionales responden a preguntas como: “¿Cuántas unidades del producto número 403 se enviaron en febrero de 2010?” El OLAP (análisis multidimensional) soporta solicitudes mucho más complejas de información, como: “Comparar las ventas del producto 403 relativas con el plan por trimestre y la región de ventas durante los últimos dos años”. Con OLAP y el análisis de datos orientados a consultas, los usuarios necesitan tener una buena idea sobre la información que están buscando.

La **minería de datos** está más orientada al descubrimiento, ya que provee perspectivas hacia los datos corporativos que no se pueden obtener mediante OLAP, al encontrar patrones y relaciones ocultas en las bases de datos grandes e inferir reglas a partir

**FIGURA 6-13** MODELO DE DATOS MULTIDIMENSIONAL



La vista que se muestra es la de producto contra región. Si gira el cubo 90 grados, la cara mostrará la vista de producto contra las ventas actuales y proyectadas, si lo gira 90 grados otra vez, verá la vista de región contra ventas actuales y proyectadas. Es posible obtener otras vistas.

de estos patrones y relaciones, para predecir el comportamiento a futuro. Los patrones y reglas se utilizan para guiar la toma de decisiones y pronosticar el efecto de esas decisiones. Los tipos de información que se pueden obtener de la minería de datos son: asociaciones, secuencias, clasificaciones, agrupamientos y pronósticos.

- Las *asociaciones* son ocurrencias vinculadas a un solo evento. Por ejemplo, un estudio de los patrones de compra en supermercados podría revelar que, cuando se compran frituras de maíz, el 65 por ciento del tiempo se compra un refresco de cola, pero cuando hay una promoción, el 85 por ciento se compra un refresco de cola. Esta información ayuda a los gerentes a tomar mejores decisiones debido a que descubren la rentabilidad de una promoción.
- En las *secuencias*, los eventos se vinculan en el transcurso del tiempo. Por ejemplo, podríamos descubrir que si se compra una casa, el 65 por ciento del tiempo se compra un nuevo refrigerador dentro de las siguientes dos semanas, y el 45 por ciento se compra un horno dentro del mes posterior a la compra de la casa.
- La *clasificación* reconoce los patrones que describen el grupo al que pertenece un elemento, para lo cual se examinan los elementos existentes que hayan sido clasificados y se infiere un conjunto de reglas. Por ejemplo, las empresas como las compañías de tarjetas de crédito o las telefónicas se preocupan por la pérdida de clientes estables. La clasificación ayuda a descubrir las características de los clientes con probabilidades de dejar de serlo y puede proveer un modelo para ayudar a los gerentes a predecir quiénes son esos clientes, de modo que puedan idear campañas especiales para retenerlos.
- El *agrupamiento* funciona de una manera similar a la clasificación cuando aún no se han definido grupos. Una herramienta de minería de datos puede descubrir distintas agrupaciones dentro de los datos, como el hecho de encontrar grupos de afinidad para tarjetas bancarias o particionar una base de datos en grupos de clientes con base en la demografía y los tipos de inversiones personales.
- Aunque estas aplicaciones implican predicciones, el *pronóstico* utiliza las predicciones de una manera distinta. Se basa en una serie de valores existentes para pronosticar cuáles serán los otros valores. Por ejemplo, el pronóstico podría encontrar patrones en los datos para ayudar a los gerentes a estimar el futuro valor de variables continuas, como las cifras de ventas.

Estos sistemas realizan análisis de alto nivel de los patrones o tendencias, pero también pueden profundizar para proveer más detalles cuando sean necesarios. Existen

aplicaciones de minería de datos para todas las áreas funcionales de negocios, y también para el trabajo gubernamental y científico. Un uso popular de la minería de datos es el de proveer análisis detallados de los patrones en los datos de los consumidores para las campañas de marketing de uno a uno, o para identificar los clientes rentables.

Por ejemplo, Harrah's Entertainment, la segunda compañía de apuestas más grande en su industria, utiliza la minería de datos para identificar a sus clientes más rentables y generar más ingresos gracias a ellos. La compañía analiza en forma continua los datos sobre sus clientes que se recopilan cuando las personas juegan en las máquinas tragamonedas o utilizan los casinos y hoteles de Harrah's. El departamento de marketing de Harrah's utiliza esta información para crear un perfil de apuestas detallado, con base en el valor continuo de un cliente específico para la compañía. Por ejemplo, la minería de datos permite a Harrah's conocer la experiencia de juego favorita de un cliente regular en uno de sus casinos en los barcos de la región del Medio Oeste, junto con las preferencias de esa persona en cuanto al alojamiento, los restaurantes y el entretenimiento. Esta información guía las decisiones gerenciales sobre cómo cultivar los clientes más rentables y animarlos a que gasten más, y también sobre cómo atraer más clientes con un alto potencial de generación de ingresos. La inteligencia de negocios mejoró tanto las ganancias de Harrah's que se convirtió en la pieza central de la estrategia de negocios de la empresa.

El **análisis predictivo** utiliza las técnicas de minería de datos, los datos históricos y las suposiciones sobre las condiciones futuras para predecir los resultados de los eventos, como la probabilidad de que un cliente responda a una oferta o que compre un producto específico. Por ejemplo, la división estadounidense de The Body Shop International plc utilizó el análisis predictivo con su base de datos de clientes de catálogo, Web y de las tiendas minoristas para identificar a los clientes que tenían mayores probabilidades de realizar compras por catálogo. Esa información ayudó a la compañía a crear una lista de correo más precisa y dirigida para sus catálogos, con lo cual se pudo mejorar la tasa de respuesta en cuanto al envío de catálogos por correo y los ingresos por las ventas a través de este medio.

## Minería de datos y minería Web

La principal función de las herramientas de inteligencia de negocios es lidiar con los datos que se han estructurado en bases de datos y archivos. Sin embargo, se cree que los datos no estructurados, que en su mayoría están organizados en forma de archivos de texto, representan más del 80 por ciento de la información útil de una organización. El correo electrónico, los memorándums, las transcripciones de los call centers, las respuestas a las encuestas, los casos legales, las descripciones de patentes y los informes de servicio son todos elementos valiosos para encontrar patrones y tendencias que ayuden a los empleados a tomar mejores decisiones de negocios. En la actualidad hay herramientas de **minería de texto** disponibles para ayudar a las empresas a analizar estos datos. Estas herramientas pueden extraer elementos clave de los conjuntos de datos extensos no estructurados, descubrir patrones y relaciones, así como sintetizar la información. Las empresas podrían recurrir a la minería de texto para analizar las transcripciones de los call centers de servicio al cliente para identificar las principales cuestiones de servicio y reparación.

La minería de texto es una tecnología relativamente nueva, pero la verdadera novedad es la cantidad de formas en que los consumidores generan datos no estructurados y los usos que dan las empresas a esos datos. La Sesión interactiva sobre tecnología explora algunas de las aplicaciones de negocios de la minería de texto.

La Web es otra fuente extensa de información valiosa, y parte de ésta se puede explorar en busca de patrones, tendencias y perspectivas en relación con el comportamiento de los clientes. El descubrimiento y análisis de los patrones útiles y la información proveniente de World Wide Web se denominan **minería Web**. Las empresas podrían recurrir a la minería Web para que les ayude a comprender el comportamiento de los clientes, evaluar la efectividad de un sitio Web específico o cuantificar el éxito de una campaña de marketing. Por ejemplo, los comerciantes utilizan los servicios Google Trends y Google Insights for Search, que rastrean la popularidad de varias palabras y frases utilizadas en las consultas de búsqueda de Google para saber en qué están interesadas las personas y qué les gusta comprar.

## SESIÓN INTERACTIVA: TECNOLOGÍA

### ¿QUÉ PUEDEN APRENDER LAS EMPRESAS DE LA MINERÍA DE TEXTO?

La minería de texto es el descubrimiento de patrones y relaciones a partir de grandes conjuntos de datos no estructurados; el tipo de datos que generamos en los correos electrónicos, las conversaciones telefónicas, lo que publicamos en los blogs, las encuestas en línea para los clientes y los tweets. La plataforma digital móvil ha amplificado la explosión en la información digital, en donde cientos de millones de personas llaman, envían mensajes de texto, buscan, usan “apps” (aplicaciones), compran bienes y escriben miles de millones de correos electrónicos mientras van de un lado a otro.

En la actualidad los consumidores son más que simples compradores: tienen más formas de colaborar, compartir información e influir en las opiniones de sus amigos y colegas; además, los datos que crean al hacerlo tienen un valor considerable para las empresas. A diferencia de los datos estructurados, que se generan a partir de eventos como completar una transacción de compra, los datos sin estructura no tienen una forma definida. Sin embargo, los gerentes creen que dichos datos pueden ofrecer perspectivas únicas en cuanto al comportamiento y las actitudes de los clientes que eran mucho más difíciles de terminar hace unos cuantos años.

Por ejemplo, en 2007 JetBlue experimentó niveles sin precedente de quejas de los clientes a raíz de una tormenta de hielo en febrero que provocó muchas cancelaciones de vuelos por todos lados y aviones varados en las pistas del Aeropuerto Kennedy. La aerolínea recibió 15 000 correos electrónicos al día de los clientes durante la tormenta y justo después de ella, mucho más de su volumen diario habitual de 400. Tan grande fue el volumen a comparación de lo usual, que JetBlue simplemente no podía leer todo lo que sus clientes decían.

Por fortuna, la compañía recién había contratado a Attensity, un distribuidor líder de software de análisis de texto, y pudo usar el software para analizar todo el correo que recibió durante dos días. De acuerdo con el analista de investigación de JetBlue llamado Bryan Jeppsen, el software Attensity Analyze for Voice of the Customer (VoC) permitió a JetBlue extraer con rapidez los sentimientos de los clientes, sus preferencias y las solicitudes que no pudo averiguar de ninguna otra forma. Esta herramienta utiliza una tecnología propietaria para identificar de manera automática hechos, opiniones, solicitudes, tendencias y puntos problemáticos a partir del texto no estructurado de las respuestas a las encuestas, notas de servicio, mensajes de correo electrónico, foros Web, mensajes publicados en blogs, artículos de noticias y otras comunicaciones de los clientes. La tecnología es capaz de identificar con precisión y de manera automática las muchas “voces” distintas que utilizan los clientes para expresar su opinión (como una voz negativa, positiva o condicional), la cual ayuda a las organizaciones a señalar los eventos y relaciones clave, como la intención de comprar, de salirse,

o los “deseos” de los clientes. Puede revelar cuestiones sobre productos y servicios específicos, reacciones a los esfuerzos de marketing y de relaciones públicas, e incluso señales de compra.

El software de Attensity integrado con las demás herramientas de análisis de clientes de JetBlue, como la métrica de Net Promoter de Satmetrix, que clasifica a los clientes en grupos que generan retroalimentación positiva, negativa o ningún tipo de retroalimentación sobre la compañía. Al usar el análisis de texto de Attensity en conjunto con estas herramientas, JetBlue desarrolló una declaración de derechos de los clientes que lidiaba con los principales problemas que tenían los clientes con la compañía.

Las cadenas hoteleras como Gaylord Hotels y Choice Hotels utilizan software de minería de texto para cosechar opiniones de las miles de encuestas de satisfacción del cliente que proporcionan sus huéspedes. Gaylord Hotels utiliza la solución de análisis de texto de Clarabridge que se ofrece a través de Internet como un servicio de software hospedado para recopilar y analizar la retroalimentación de los clientes proveniente de las encuestas, el correo electrónico, la mensajería instantánea, los call centers dotados de personal, y los foros en línea asociados con las experiencias de los huéspedes y los planificadores de reuniones en los centros de convenciones de la compañía. El software Clarabridge examina las encuestas de los clientes de la cadena hotelera y recopila los comentarios tanto positivos como negativos, para después organizarlos en una variedad de categorías y revelar opiniones menos obvias. Por ejemplo, los huéspedes se quejaron más sobre otros asuntos que sobre los cuartos ruidosos, pero las quejas de los cuartos ruidosos se correlacionaron con más frecuencia con las encuestas que indicaban una indisposición a regresar al hotel.

El análisis de las encuestas de los clientes solía tomar semanas, pero ahora sólo es cuestión de días gracias al software Clarabridge. Los gerentes de locaciones y los ejecutivos corporativos también han utilizado los hallazgos de la minería de texto para influir en las decisiones sobre mejoras en las empresas.

Wendy's International adoptó el software Clarabridge para analizar los cerca de 500 000 mensajes que recolecta cada año de su foro de retroalimentaciones basado en Web, las notas del call center, los mensajes de correo electrónico, las encuestas en los recibos y los medios sociales. El equipo de satisfacción al cliente de la cadena había utilizado antes hojas de cálculo y búsquedas de palabras clave para repasar los comentarios de los clientes, una metodología manual muy lenta. La gerencia de Wendy's estaba en busca de una mejor herramienta para agilizar el análisis, detectar los problemas emergentes y señalar las áreas problemáticas de la empresa a nivel de tienda, regional o corporativo.



La tecnología de Clarabridge permite a Wendy's rastrear las experiencias de los clientes hasta el nivel de tienda en cuestión de minutos. Esta información oportuna ayuda a los gerentes de tiendas, regionales y corporativos a detectar y lidiar con los problemas relacionados con la calidad de los alimentos, la limpieza y la velocidad del servicio.

El software de análisis de texto tuvo auge primero con las agencias gubernamentales y las compañías de mayor tamaño con departamentos de sistemas de información que tenían los medios para usar de manera apropiada el complicado software, pero ahora Clarabridge ofrece una versión de su producto orientada hacia las pequeñas empresas. La tecnología ya ha tenido auge con las agencias policiales, las interfaces de las herramientas de búsqueda y las "plataformas de escucha" como Nielsen Online. Las plataformas de escucha son herramientas de minería de texto que se enfocan en la administración

de marcas para permitir a las empresas determinar cómo se sienten los clientes en cuanto a su marca y tomar acciones para responder al sentimiento negativo.

El análisis de datos estructurados no se hará obsoleto debido al análisis de texto, pero a las compañías que pueden usar ambos métodos para desarrollar una imagen más clara de las posturas de sus clientes les será más fácil establecer su marca y deducir las perspectivas que mejorarán la rentabilidad.

**Fuentes:** Doug Henschen, "Wendy's Taps Text Analytics to Mine Customer Feedback", *Information Week*, 23 de marzo de 2010; David Stodder, "How Text Analytics Drive Customer Insight", *Information Week*, 1 de febrero de 2010; Nancy David Kho, "Customer Experience and Sentiment Analysis", *KMWorld*, 1 de febrero de 2010; Siobhan Gorman, "Details of Einstein Cyber-Shield Disclosed by White House", *The Wall Street Journal*, 2 de marzo de 2010; [www.attensity.com](http://www.attensity.com), visitado el 16 de junio de 2010, y [www.clarabridge.com](http://www.clarabridge.com), visitado el 17 de junio de 2010.

## PREGUNTAS DEL CASO DE ESTUDIO

1. ¿Qué retos presenta para las empresas el aumento en los datos no estructurados?
2. ¿Cómo mejora la minería de texto el proceso de toma de decisiones?
3. ¿Qué tipos de compañías tienen más probabilidad de beneficiarse del software de minería de texto? Explique su respuesta.
4. ¿En qué formas podría la minería de texto conducir potencialmente a la erosión de la privacidad de la información personal? Explique.

## MIS EN ACCIÓN

Visite un sitio Web como QVC.com o TripAdvisor.com, en donde se detallen los productos o servicios que tienen reseñas de los clientes. Elija un producto, hotel u otro servicio que tenga al menos 15 reseñas de clientes y léalas, tanto las positivas como las negativas. ¿Cómo podría la minería de contenido Web ayudar a que la compañía mejore o comercialice de una mejor manera los productos o servicios que ofrece? ¿Qué piezas de información se deberían resaltar?

La minería Web busca patrones en los datos a través de la minería de contenido, la minería de estructura y la minería de uso. La minería de contenido Web es el proceso de extraer conocimiento del contenido de páginas Web, lo cual puede incluir datos de texto, imágenes, audio y video. La minería de estructura Web extrae información útil de los vínculos incrustados en documentos Web. Por ejemplo, los vínculos que apuntan a un documento indican su popularidad, mientras que los que salen de un documento indican la riqueza, o tal vez la variedad de temas cubiertos en él. La minería de uso Web examina los datos de interacción de los usuarios registrados por un servidor Web cada vez que se reciben solicitudes relacionadas con los recursos de un sitio Web. Los datos de uso registran el comportamiento del usuario cuando navega o realiza transacciones en el sitio Web y recolecta los datos en un registro del servidor. Al analizar esos datos, las compañías pueden determinar el valor de ciertos clientes específicos, las estrategias de marketing cruzado entre los diversos productos y la efectividad de las campañas promocionales.

## LAS BASES DE DATOS Y WEB

¿Alguna vez ha tratado de usar la Web para realizar un pedido o ver un catálogo de productos? Si su respuesta es positiva, es probable que haya usado un sitio Web vinculado a una base de datos corporativa interna. Ahora muchas compañías utilizan Web para poner parte de la información en sus bases de datos internas a disposición de los clientes y los socios de negocios.



Suponga por ejemplo que un cliente con un navegador Web desea buscar información de precios en la base de datos en línea de un vendedor minorista. La figura 6-14 ilustra la forma en que ese cliente podría acceder a la base de datos interna del vendedor a través de Web. El usuario accede al sitio Web del vendedor a través de Internet mediante el software de navegador Web en su PC cliente. El software de navegador Web del usuario solicita información a la base de datos de la organización, mediante comandos de HTML para comunicarse con el servidor Web.

Como muchas bases de datos de procesamiento en segundo plano (back-end) no pueden interpretar comandos escritos en HTML, el servidor Web pasa estas solicitudes de datos al software que traduce los comandos de HTML en SQL, de modo que el DBMS que trabaja con la base de datos pueda procesarlos. En un entorno cliente/servidor, el DBMS reside en una computadora dedicada llamada **servidor de bases de datos**. El DBMS recibe las solicitudes de SQL y provee los datos requeridos. El middleware transforma la información de la base de datos interna y la devuelve al servidor Web para que la ofrezca en forma de una página Web al usuario.

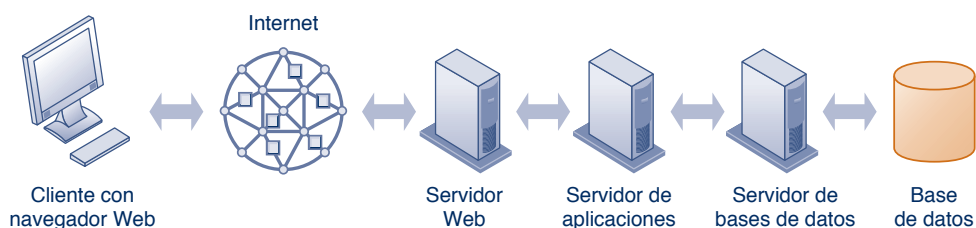
La figura 6-14 muestra que el middleware que trabaja entre el servidor Web y el DBMS es un servidor de aplicaciones que se ejecuta en su propia computadora dedicada (vea el capítulo 5). El software del servidor de aplicaciones maneja todas las operaciones de la aplicación, entre ellas el procesamiento de las transacciones y el acceso a los datos, entre las computadoras basadas en navegador y las aplicaciones o bases de datos de negocios de procesamiento en segundo plano (back-end) de una compañía. El servidor de aplicaciones recibe las solicitudes del servidor Web, ejecuta la lógica de negocios para procesar las transacciones con base en esas solicitudes y provee conectividad a los sistemas o bases de datos de procesamiento en segundo plano de la organización. De manera alternativa, el software para manejar estas operaciones podría ser un programa personalizado o una secuencia de comandos CGI: un programa compacto que utiliza la especificación *Interfaz de puerta de enlace común (CGI)* para procesar datos en un servidor Web.

Hay varias ventajas en cuanto al uso de Web para acceder a las bases de datos internas de una organización. En primer lugar, el software de navegador Web es mucho más fácil de usar que las herramientas de consulta propietarias. En segundo lugar, la interfaz Web requiere pocos o ningún cambio en la base de datos interna. Es mucho menos costoso agregar una interfaz Web frente a un sistema heredado que rediseñar y reconstruir el sistema para mejorar el acceso de los usuarios.

El acceso a las bases de datos corporativas por medio de Web está creando nuevas eficiencias, oportunidades y modelos de negocios. ThomasNet.com provee un directorio en línea actualizado de más de 600 000 proveedores de productos industriales, como químicos, metales, plásticos, goma y equipo automotriz. Antes conocida como Thomas Register, la compañía solía enviar enormes catálogos en papel con esta información y ahora la provee a los usuarios en línea a través de su sitio Web, gracias a lo cual se ha convertido en una compañía más pequeña y eficaz.

Otras compañías han creado empresas totalmente nuevas con base en el acceso a bases de datos extensas a través de Web. Un ejemplo de esto es el sitio de redes sociales MySpace, que ayuda a los usuarios a permanecer conectados entre sí o conocer nuevas

**FIGURA 6-14 VINCULACIÓN DE BASES DE DATOS INTERNAS A WEB**



Los usuarios acceden a la base de datos interna de una organización a través de Web, por medio de sus PCs de escritorio y el software de navegador Web.

personas. MySpace incluye música, comedia, videos y “perfiles” con información suministrada por 122 millones de usuarios sobre su edad, ciudad natal, preferencias en sus citas, estado civil e intereses. Mantiene una base de datos masiva para alojar y administrar todo su contenido. Facebook utiliza una base de datos similar.

## 6.4 ADMINISTRACIÓN DE LOS RECURSOS DE DATOS

El establecimiento de una base de datos es sólo el principio. Para poder asegurar que los datos para su empresa sigan siendo precisos, confiables y estén disponibles de inmediato para aquellos que los necesiten, necesitará políticas y procedimientos especiales para la administración de datos.

### ESTABLECIMIENTO DE UNA POLÍTICA DE INFORMACIÓN

Toda empresa, ya sea grande o pequeña, necesita una política de información. Los datos de su empresa son un recurso importante, por lo que no es conveniente que las personas hagan lo que quieran con ellos. Necesita tener reglas sobre la forma en que se van a organizar y mantener los datos, y quién tiene permitido verlos o modificarlos.

Una **política de información** es la que especifica las reglas de la organización para compartir, diseminar, adquirir, estandarizar, clasificar e inventariar la información. La política de información establece procedimientos y rendiciones de cuentas específicos, identifica qué usuarios y unidades organizacionales pueden compartir información, en dónde distribuirla y quién es responsable de actualizarla y mantenerla. Por ejemplo, una política de información típica especificaría que sólo los miembros selectos del departamento de nómina y recursos humanos tendrían el derecho de modificar y ver los datos confidenciales de los empleados, como el salario o número de seguro social de un empleado, y que estos departamentos son responsables de asegurar que los datos de cada empleado sean precisos.

Si usted está en una empresa pequeña, los propietarios o gerentes son los que establecerían e implementarían la política de información. En una organización grande, administrar y planificar la información como un recurso corporativo requiere con frecuencia de una función de administración de datos formal. La **administración de datos** es responsable de las políticas y procedimientos específicos a través de los cuales se pueden administrar los datos como un recurso organizacional. Estas responsabilidades abarcan el desarrollo de la política de información, la planificación de los datos, la supervisión del diseño lógico de la base de datos, y el desarrollo del diccionario de datos, así como el proceso de monitorear la forma en que los especialistas de sistemas de información y los grupos de usuarios finales utilizan los datos.

Tal vez escuche que se utiliza el término **gobernanza de datos** para describir muchas de estas actividades. La gobernanza de datos es promovida por IBM y se encarga de las políticas y procedimientos para administrar la disponibilidad, utilidad, integridad y seguridad de los datos empleados en una empresa, con un énfasis especial en promover la privacidad, seguridad, calidad de los datos y el cumplimiento con las regulaciones gubernamentales.

Una organización grande también debe tener un grupo de diseño y administración de bases de datos dentro de la división de sistemas de información corporativos que sea responsable de definir y organizar la estructura y el contenido de la base de datos, y de darle mantenimiento. En una estrecha cooperación con los usuarios, el grupo de diseño establece la base de datos física, las relaciones lógicas entre los elementos, las reglas de acceso y los procedimientos de seguridad. Las funciones que desempeña se denominan **administración de la base de datos**.

### ASEGURAMIENTO DE LA CALIDAD DE LOS DATOS

Una base de datos y una política de información bien diseñadas son un gran avance en cuanto a asegurar que la empresa tenga la información que necesita. Sin embargo, hay

que llevar a cabo ciertas acciones adicionales para asegurar que los datos en las bases de datos organizacionales sean precisos y permanezcan confiables.

¿Qué ocurriría si el número telefónico o el saldo de la cuenta de un cliente fueran incorrectos? ¿Cuál sería el impacto si la base de datos tuviera el precio incorrecto para el producto que usted vendió, o si su sistema de ventas y de inventario mostraran distintos precios para el mismo producto? Los datos imprecisos, inoportunos o inconsistentes con otras fuentes de información conducen a decisiones incorrectas, llamadas a revisión de los productos y pérdidas financieras. Los datos imprecisos en las bases de datos de justicia criminal y seguridad nacional podrían incluso someterlo a una vigilancia o detención innecesaria, como se describe en el caso de estudio al final del capítulo.

De acuerdo con Forrester Research, se devolvió el 20 por ciento de las entregas de paquetes de correo y comerciales en Estados Unidos debido a datos incorrectos en los nombres o las direcciones. Gartner Inc. informó que más del 25 por ciento de los datos críticos en las extensas bases de datos de las compañías Fortune 1000 son imprecisos o incompletos, incluyendo los códigos erróneos de productos y sus descripciones, las descripciones incorrectas en el inventario, los datos financieros erróneos, la información incorrecta de los proveedores y los datos erróneos de los empleados (Gartner, 2007).

Piense en todos los momentos que ha recibido varias piezas de la misma publicidad directa por correo el mismo día. Es muy probable que esto sea el resultado de que su nombre se repita varias veces en una base de datos. Tal vez lo hayan escrito mal o haya utilizado la inicial de su segundo nombre en una ocasión y en otra no, o quizás en un principio la información se capturó en un formulario en papel y no se digitalizó de manera apropiada para introducirlo al sistema. Debido a estas inconsistencias, ¡la base de datos lo consideraría como si fueran distintas personas! Nosotros a menudo recibimos correo redundante dirigido a Laudon, Lavdon, Lauden o Landon.

Si una base de datos está diseñada en forma apropiada y hay estándares de datos establecidos a nivel empresarial, los elementos de datos duplicados o inconsistentes deben reducirse al mínimo. Sin embargo, la mayoría de los problemas de calidad de los datos, como los nombres mal escritos, los números transpuestos y los códigos incorrectos o faltantes, se derivan de los errores durante la captura de los datos. La incidencia de dichos errores aumenta a medida que las compañías pasan sus negocios a Web y permiten que los clientes y proveedores introduzcan datos en sus sitios Web para actualizar de manera directa los sistemas internos.

Antes de implementar una nueva base de datos, las organizaciones necesitan identificar y corregir sus datos incorrectos y establecer mejores rutinas para editar los datos una vez que su base esté en operación. Con frecuencia, el análisis de la calidad de los datos empieza con una **auditoría de calidad de los datos**, la cual es una encuesta estructurada de la precisión y el nivel de su integridad en un sistema de información. Las auditorías de calidad de los datos se pueden realizar mediante la inspección de los archivos de datos completos, la inspección de muestras provenientes de los archivos de datos, o mediante encuestas a los usuarios finales sobre sus percepciones en cuanto a la calidad de los datos.

La **limpieza de datos**, conocida también en inglés como *data scrubbing*, consiste en actividades para detectar y corregir datos en una base que sean incorrectos, incompletos, que tengan un formato inapropiado o que sean redundantes. La limpieza de datos no sólo corrige los errores, sino que también impone la consistencia entre los distintos conjuntos de datos que se originan en sistemas de información separados. El software de limpieza de datos especializado está disponible para inspeccionar los archivos de datos de manera automática, corregir errores en los datos e integrarlos en un formato consistente a nivel de toda la compañía.

Los problemas de calidad de los datos no son sólo problemas de negocios, también representan serios problemas para los individuos, en cuanto a que afectan su condición financiera e incluso sus empleos. La Sesión interactiva sobre organización describe algunos de estos impactos, ya que detalla los problemas de calidad de los datos que se encuentran en las compañías que recolectan e informan sobre los datos de crédito de los consumidores. Cuando lea este caso analice los factores de administración, organización y tecnología detrás de este problema, y si las soluciones existentes son adecuadas o no.

## SESIÓN INTERACTIVA: ORGANIZACIONES

### ERRORES DEL BURÓ DE CRÉDITO: GRANDES PROBLEMAS DE LA GENTE

Acaba de encontrar el auto de sus sueños. Cuenta con un buen trabajo y suficiente dinero para el enganche. Todo lo que necesita es un préstamo por \$14 000. Tiene unas cuantas facturas de tarjetas de crédito, que paga con diligencia cada mes. Pero cuando solicita el préstamo, se lo rechazan. Cuando pregunta por qué, le dicen que tiene un préstamo vencido de un banco del cual nunca había escuchado antes. Acaba de convertirse en una de las millones de víctimas de los datos imprecisos u obsoletos en los sistemas de información de los burós de crédito.

La mayoría de los datos en los historiales de crédito de los consumidores en Estados Unidos se recolectan y mantienen a través de tres agencias de informes crediticios nacionales: Experian, Equifax y TransUnion. Estas organizaciones recolectan datos de varias fuentes para crear un expediente detallado de los hábitos de préstamos y pagos de un individuo. Esta información ayuda a los prestamistas a evaluar la capacidad crediticia de una persona, la capacidad de pagar un préstamo y puede afectar en la tasa de intereses y otros términos de un préstamo, como el hecho de si se puede otorgar o no un préstamo. Incluso puede afectar en la probabilidad de encontrar o mantener un empleo: por lo menos una tercera parte de los empleadores verifican los informes crediticios al tomar decisiones de contratación, despido o promoción.

Los burós de crédito en Estados Unidos recolectan información personal y datos financieros de una variedad de fuentes, entre ellos acreedores, prestamistas, empresas de servicios públicos, agencias de recolección de deudas y las cortes. Estos datos se agregan y almacenan en bases de datos masivas, cuyo mantenimiento está a cargo de los burós de crédito. A su vez, éstos venden la información a otras empresas para que evalúen los créditos.

Los burós de crédito afirman que saben qué tarjetas de crédito están en la cartera de cada cliente, cuánto deben de hipoteca y si la factura eléctrica se paga o no a tiempo. No obstante, si llega la información incorrecta a sus sistemas, ya sea por medio del robo de identidad o por los errores transmitidos por los acreedores, ¡tenga cuidado! Desenmarañar el enredo puede ser casi imposible.

Los burós comprenden la importancia de proporcionar información precisa tanto a los acreedores como a los consumidores. Pero también reconocen que sus propios sistemas son responsables de muchos errores en los informes crediticios. Algunos de estos errores ocurren debido a los procedimientos para asociar los préstamos con los informes crediticios individuales.

El volumen total de la información que se transmite de los acreedores a los burós de crédito incrementa la probabilidad de cometer errores. Por ejemplo,

Experian actualiza 30 millones de reportes de crédito a diario y alrededor de 2 mil millones de reportes de crédito al mes. Asocia la información de identificación personal en una solicitud o cuenta de crédito con la información de identificación personal en el archivo de crédito de un consumidor. La información de identificación personal contiene elementos como el nombre (primer nombre, apellido e inicial del segundo nombre), la dirección completa actual y el código postal, la dirección completa anterior y el código postal, y el número de seguro social. La nueva información de crédito pasa al archivo de crédito del consumidor que tenga la mejor coincidencia.

Los burós de crédito raras veces reciben información que coincida en todos los campos de los archivos de crédito, por lo que tienen que determinar cuánta variación permitir para poder seguirla considerando como coincidencia. Los datos imperfectos conducen a coincidencias no perfectas. Un consumidor podría proveer información incompleta o imprecisa en una solicitud de crédito. Un acreedor podría enviar información incompleta o imprecisa a los burós de crédito. Si la persona incorrecta coincide mejor que cualquier otra, los datos podrían por desgracia pasar a la cuenta incorrecta.

Tal vez el consumidor no escribió con claridad en la solicitud de la cuenta. Las variaciones en los nombres de las distintas cuentas de crédito también pueden producir coincidencias imperfectas. Considere como ejemplo el nombre Edward Jeffrey Johnson. Una cuenta podría decir Edward Jeffrey Johnson. Otra podría decir Ed Johnson. Otra más podría decir Edward J. Johnson. Suponga que los dos últimos dígitos del número de seguro social de Edward se transponen: hay más probabilidad de errores en la coincidencia.

Si el nombre o el número de seguro social en la cuenta de otra persona coinciden de manera parcial con los datos en su archivo, la computadora podría agregar los datos de esa persona a su registro. De igual forma, su registro podría corromperse si los trabajadores en las empresas que suministran datos fiscales y de bancarrota provenientes de los registros gubernamentales y de las cortes transponen de manera accidental un dígito o leen mal un documento.

Los burós de crédito afirman que es imposible para ellos monitorear la precisión de las 3.5 mil millones de piezas de información sobre las cuentas de crédito que reciben cada mes. Deben lidiar de manera continua con las reclamaciones falaces de los consumidores que falsifican información de las entidades crediticias o utilizan compañías sospechosas de reparación de crédito que desafían toda la información negativa en un informe de crédito, sin importar su validez. Para separar el bien del mal, los burós de crédito utilizan un sistema automatizado llamado e-OSCAR (solución electrónica en línea

para informes completos y precisos) para reenviar las disputas de los clientes a las entidades crediticias y que éstas las verifiquen.

Si su informe crediticio indica un error, los burós por lo general no se contactan de manera directa con la entidad crediticia para corregir la información. Para ahorrar dinero, los burós envían las protestas de los consumidores junto con la evidencia a un centro de procesamiento de datos operado por un contratista independiente. Estos contratistas sintetizan con rapidez cada queja con un breve comentario y un código de dos dígitos basado en un menú de 26 opciones. Por ejemplo, el código A3 indica que “pertenece a otro individuo con un nombre similar”. Estos resúmenes son a menudo demasiado breves como para incluir los antecedentes que necesitan los bancos para comprender una queja.

Aunque este sistema corrige muchos errores (los datos se actualizan o corrigen en el 72 por ciento de las disputas), los consumidores tienen pocas opciones si el sistema falla. A los consumidores que presentan una segunda disputa sin proveer nueva información se les podría rechazar por ser “frívola”. Si el consumidor trata de ponerse en contacto con la entidad crediticia que cometió el error por su cuenta, los bancos no tienen obligación de investigar la disputa: a menos que la envíe un buró de crédito.

**Fuentes:** Dennis McCafferty, “Bad Credit Could Cost You a Job”, *Baseline*, 7 de junio de 2010; Kristen McNamara, “Bad Credit Derails Job Seekers”, *The Wall Street Journal*, 16 de marzo de 2010; Anne Kadet, Lucy Lazarony, “Your Name Can Mess Up Your Credit Report”, *Bankrate.com*, visitado el 1 de julio de 2009; “Credit Report Fix a Headache”, *Atlanta Journal-Constitution*, 14 de junio de 2009, y “Why Credit Bureaus Can't Get It Right”, *Smart Money*, marzo de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

1. Evalúe el impacto comercial de los problemas de la calidad de los datos de los burós de crédito para éstos, para los prestamistas y para los individuos.
2. ¿Se generan problemas éticos debido a los problemas en la calidad de los datos de los burós de crédito? Explique su respuesta.
3. Analice los factores de administración, organización y tecnología responsables de los problemas en la calidad de los datos de los burós de crédito.
4. ¿Qué se puede hacer para resolver estos problemas?

## MIS EN ACCIÓN

Vaya al sitio Web de Experian ([www.experian.com](http://www.experian.com)) explórelo; ponga especial atención en sus servicios para empresas y negocios pequeños. Después responda las siguientes preguntas:

1. Mencione y describa cinco servicios para negocios y explique cómo utiliza cada uno los datos de los consumidores. Describa los tipos de negocios que utilizarían estos servicios.
2. Explique cómo se ve afectado cada uno de estos servicios por los datos imprecisos de los consumidores.



6.5
PROYECTOS PRÁCTICOS SOBRE MIS

Los proyectos en esta sección le proporcionan experiencia práctica para analizar los problemas de calidad de los datos, establecer estándares de datos a nivel de toda la compañía, crear una base de datos para administrar el inventario y utilizar Web para buscar recursos de negocios foráneos en las bases de datos en línea.

Problemas de decisión gerencial

- Emerson Process Management, proveedor global de instrumentos y servicios de medición, análisis y monitoreo con base en Austin Texas, tenía un nuevo almacén de datos diseñado para analizar la actividad de los clientes y mejorar tanto el servicio como el proceso de marketing que estaba lleno de datos imprecisos y redundantes. Los datos en el almacén provenían de muchos sistemas de procesamiento de transacciones en Europa, Asia y otras ubicaciones alrededor del mundo. El equipo que diseñó el almacén supuso que los grupos de ventas en todas estas áreas introducirían los nombres y direcciones de los clientes de la misma forma, sin importar su ubicación. De hecho, las diferencias culturales combinadas con las complicaciones que se provocaban al absorber las compañías que Emerson había adquirido, condujeron a varias formas de introducir datos de cotizaciones, facturación, envíos y demás datos relacionados. Evalúe el impacto de negocios potencial de estos problemas de calidad de los datos. ¿Qué decisiones y acciones hay que tomar para llegar a una solución?
- Su compañía proveedora industrial desea crear un almacén de datos en donde la gerencia pueda obtener una vista amplia a nivel corporativo de la información sobre las ventas críticas, para identificar los productos que se venden mejor en áreas geográficas específicas, los clientes clave y las tendencias de ventas. La información de sus ventas y productos se almacena en varios sistemas distintos: un sistema de ventas divisional que opera en un servidor Unix y uno corporativo de ventas que opera en una mainframe IBM. A usted le gustaría crear un solo formato estándar que consolide esos datos de ambos sistemas. Se ha propuesto el siguiente formato.

ID_PRODUCTO	DESCRIPCION_PRODUCTO	COSTO_POR_UNIDAD	UNIDADES_VENDIDAS	REGION_VENTAS	DIVISION	ID_CLIENTE

Los siguientes son archivos de ejemplo de los dos sistemas que proveerían la información para el almacén de datos:

SISTEMA CORPORATIVO DE VENTAS

ID_PRODUCTO	DESCRIPCION_PRODUCTO	COSTO_UNITARIO	UNIDADES_VENDIDAS	TERRITORIO_VENTAS	DIVISION
60231	Cojinete, 4"	5.28	900 245	Noreste	Piezas
85773	Unidad de montaje SS	12.45	992 111	Medio Oeste	Piezas

SISTEMA DE VENTAS DE LA DIVISIÓN DE PIEZAS MECÁNICAS

NUM_PROD	DESCRIPCION_PRODUCTO	COSTO_POR_UNIDAD	UNIDADES_VENDIDAS	REGION_VENTAS	ID_CLIENTE
60231	Cojinete de acero de 4"	5.28	900 245	N.E.	Anderson
85773	Unidad de montaje SS	12.45	992 111	M.O.	Kelly Industries



- ¿Qué problemas de negocios se crean al no tener estos datos en un solo formato estándar?
- ¿Qué tan fácil sería crear una base de datos con un solo formato estándar que pudiera almacenar los datos de ambos sistemas? Identifique los problemas con los que habría que lidiar.
- ¿Quiénes deben resolver los problemas, los especialistas de bases de datos o los gerentes generales de la empresa? Explique.
- ¿Quién debe tener la autoridad de finalizar un solo formato a nivel de toda la compañía para esta información en el almacén de datos?

### **Obtención de la excelencia operacional: creación de una base de datos relacional para la administración del inventario**

---

Habilidades de software: diseño, consultas e informes de bases de datos

Habilidades de negocios: administración del inventario

Hoy en día las empresas dependen de las bases de datos para que les provean información confiable sobre los artículos en el inventario, sus costos y los que necesitan reabastecerse. En este ejercicio utilizará software de bases de datos para diseñar una base con la que se pueda administrar el inventario de una pequeña empresa.

La Tienda de Bicicletas de Sylvester, ubicada en San Francisco, California, vende bicicletas para camino regular, de montaña, híbridas, para paseo y para niños. En la actualidad, Sylvester compra bicicletas a tres proveedores pero planea agregar nuevos proveedores en un futuro cercano. Este negocio de rápido crecimiento necesita un sistema de bases de datos para administrar la información.

En un principio, la base de datos debe alojar información sobre proveedores y productos. Además, contener dos tablas: una de proveedores y una de productos. El nivel de reabastecimiento se refiere al número de artículos en el inventario que desencadena una decisión para pedir más artículos y evitar un desabastecimiento (en otras palabras, si el número de unidades de un artículo específico en el inventario disminuye a una cantidad inferior al nivel de reabastecimiento, hay que reabastecer el artículo). El usuario debe ser capaz de realizar varias consultas y producir diversos informes gerenciales con base en los datos que contienen las dos tablas.

Use la información que se incluye en las tablas en MyMISLab para crear una base de datos relacional simple que se pueda usar en la tienda de Sylvester. Una vez que cree la base de datos, realice las siguientes actividades:

- Prepare un informe que identifique las cinco bicicletas más costosas. El informe debe mostrar la lista de bicicletas en orden descendente, de la más costosa hasta la menos costosa, la cantidad en existencia de cada una y el porcentaje de ganancia en cada una de ellas.
- Prepare un informe que muestre una lista de cada proveedor, sus productos, las cantidades en existencia y los niveles de reabastecimiento asociados. El informe se debe ordenar en forma alfabética por proveedor. Dentro de cada categoría de proveedor hay que colocar los productos en orden alfabético.
- Prepare un informe que muestre una lista sólo de las bicicletas que tengan un nivel bajo de existencia y necesiten reabastecerse. El informe debe proveer información a los proveedores para los artículos identificados.
- Escriba una descripción breve de cómo se podría mejorar la base de datos para una administración más eficiente de la empresa. ¿Qué tablas o campos se deberían agregar? ¿Qué informes adicionales serían útiles?

## Mejora de la toma de decisiones: uso de las bases de datos en línea para buscar recursos de negocios en el extranjero

---

Habilidades de software: bases de datos en línea

Habilidades de negocios: investigación de los servicios para operaciones en el extranjero

Los usuarios de Internet tienen acceso a muchos miles de bases de datos habilitadas para Web con información sobre servicios y productos en locaciones distantes. Este proyecto desarrolla habilidades en cuanto a cómo realizar búsquedas en estas bases de datos en línea.

Suponga que su compañía está ubicada en Greensboro, Carolina del Norte, y que fabrica muebles de oficina de diversos tipos. Hace poco adquirió varios nuevos clientes en Australia, y un estudio que comisionó indica que, si tuviera presencia ahí, podría incrementar de manera considerable sus ventas. Lo que es más, su estudio indica que obtendría más ganancias si empezara a fabricar muchos de sus productos en forma local (en Australia). En primer lugar, necesita abrir una oficina en Melbourne para establecer una presencia, y después empezar a importar de Estados Unidos. Después puede comenzar a producir en forma local.

Pronto viajará al área para planear el proceso de abrir una oficina, por lo que desea reunirse con organizaciones que le puedan ayudar con su operación. Tendrá que contactarse con personas u organizaciones que ofrezcan muchos de los servicios necesarios para que usted abra su oficina, como abogados, contadores, expertos en importación-exportación, equipo y soporte de telecomunicaciones, e incluso capacitadores que le puedan ayudar a preparar a sus futuros empleados a trabajar para usted. Empiece por buscar la recomendación del Departamento de Comercio de Estados Unidos acerca de cómo hacer negocios en Australia. Después pruebe las siguientes bases de datos en línea para localizar compañías con las que le gustaría reunirse durante su próximo viaje: el registro australiano de empresas ([abr.business.gov.au/](http://abr.business.gov.au/)), Australia Trade Noe ([australiatradenow.com/](http://australiatradenow.com/)) y el directorio nacional de empresas de Australia ([www.nationwide.com.au](http://www.nationwide.com.au)). Si es necesario, también podría probar los motores de búsqueda como Yahoo y Google. Después realice las siguientes actividades:

- Muestre una lista de compañías con las que quisiera ponerse en contacto para entrevistarlas en su viaje y determinar si le pueden ayudar con estas y otras funciones que piense que son vitales para establecer su oficina.
- Clasifique las bases de datos que utilizó en cuanto a la precisión en el nombre, integridad, facilidad de uso y utilidad en general.
- ¿Qué le indica este ejercicio acerca del diseño de las bases de datos?

## MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

---

Las siguientes Trayectorias de aprendizaje proporcionan contenido relevante a los temas que se cubrieron en este capítulo:

1. Diseño de bases de datos, normalización y diagramas entidad-relación
2. Introducción a SQL
3. Modelos de datos jerárquico y de red

## Resumen de repaso

1. *¿Cuáles son los problemas de administrar los recursos de datos en un entorno de archivos tradicional y cómo se resuelven mediante un sistema de administración de bases de datos?*

Las técnicas tradicionales de administración de archivos dificultan a las organizaciones el proceso de llevar el registro de todas las piezas de datos que utilizan de una manera sistemática, y de organizarlos de modo que se pueda tener un fácil acceso a ellos. Se permitió a las distintas áreas y grupos funcionales desarrollar sus propios archivos en forma independiente. Con el tiempo, este entorno tradicional de administración de archivos crea problemas como la redundancia e inconsistencia de los datos, la dependencia programa-datos, inflexibilidad, mala seguridad, falta de compartición y disponibilidad de éstos. Un sistema de administración de bases de datos (DBMS) resuelve estos problemas mediante software que permite su centralización y administración, de modo que las empresas tengan una sola fuente consistente para todas sus necesidades de datos. El uso de un DBMS minimiza la cantidad de archivos redundantes e inconsistentes.

2. *¿Cuáles son las principales capacidades de los sistemas de administración de bases de datos (DBMS) y por qué es tan poderoso un DBMS?*

Las principales capacidades de un DBMS son: capacidad de definición de datos, capacidad de diccionario de datos y lenguaje de manipulación de datos. La capacidad de definición de datos especifica la estructura y el contenido de la base de datos. El diccionario de datos es un archivo automatizado o manual que almacena información sobre los datos en la base, entre estos, nombres, definiciones, formatos y descripciones de los elementos de datos. El lenguaje de manipulación de datos (como SQL) es un lenguaje especializado para acceder a los datos y manipularlos en la base.

La base de datos relacional es el método primario para organizar y dar mantenimiento a los datos en la actualidad en los sistemas de información, ya que es muy flexible y accesible. Organiza los datos en tablas bidimensionales conocidas como relaciones con filas y columnas. Cada tabla contiene información acerca de una entidad y sus atributos. Cada fila representa un registro y cada columna representa un atributo o campo. Cada tabla contiene también un campo clave para identificar en forma única cada registro para recuperarlo o manipularlo. Las tablas de las bases de datos relacionales se pueden combinar con facilidad para ofrecer los datos que requieren los usuarios, siempre y cuando dos tablas cualesquiera compartan un elemento de datos común.

3. *¿Cuáles son algunos principios importantes del diseño de bases de datos?*

Para diseñar una base de datos se requieren un diseño lógico y uno físico. El diseño lógico modela la base de datos desde una perspectiva de negocios. El modelo de datos de la organización debe reflejar sus procesos de negocios clave y los requerimientos para la toma de decisiones. El proceso de crear estructuras de datos pequeñas, estables, flexibles y adaptativas a partir de grupos complejos de datos al momento de diseñar una base de datos relacional se denomina normalización. Una base de datos relacional bien diseñada no debe tener relaciones de varios a varios, y todos los atributos para una entidad específica sólo se aplican a esa entidad. Esta base de datos trata de imponer las reglas de integridad referencial para asegurar que las relaciones entre tablas acopladas permanezcan consistentes. Un diagrama entidad-relación describe en forma gráfica la relación entre las entidades (tablas) en una base de datos relacional.

4. *¿Cuáles son las principales herramientas y tecnologías para acceder a la información de las bases de datos y mejorar tanto el desempeño de negocios como la toma de decisiones?*

Hay poderosas herramientas disponibles para analizar y acceder a la información en las bases de datos. Un almacén de datos consolida los datos actuales e históricos de muchos sistemas operacionales distintos en una base central diseñada para generar informes y realizar análisis. Los almacenes de datos soportan el análisis de datos multidimensional, también conocido como procesamiento analítico en línea (OLAP). El OLAP representa las relaciones entre los datos como una estructura multidimensional, que se puede visualizar en forma de cubos de datos y cubos dentro de cubos de datos, con lo cual se permite un análisis más sofisticado. La minería de datos analiza grandes reservas de datos, incluyendo el contenido de los almacenes de datos, para encontrar patrones y reglas que se puedan utilizar para predecir el comportamiento en un futuro y guiar la toma de decisiones. Las herramientas de minería de datos ayudan a las empresas a analizar extensos conjuntos de datos no estructurados que consisten en texto. Las herramientas de minería de datos se enfocan en el análisis de patrones e información útiles provenientes de World Wide Web; examinan la estructura de los sitios Web y las actividades de los usuarios de esos sitios Web, así como el contenido de las páginas Web. Las bases de datos convencionales se pueden vincular mediante middleware a Web o a una interfaz Web para facilitar el acceso de un usuario a los datos internos de la organización.

5. *¿Por qué son la política de información, la administración de datos y el aseguramiento de la calidad de los datos esenciales para administrar los recursos de datos de la empresa?*

Para desarrollar un entorno de bases de datos se requieren políticas y procedimientos que ayuden a administrar los datos organizacionales, así como un buen modelo de datos y una tecnología de bases de datos eficiente. Una política de información formal gobierna el mantenimiento, la distribución y el uso de la información en la organización. En las grandes corporaciones, una función de administración de datos formal es responsable de la política de la información, así como de la planificación de los datos, el desarrollo del diccionario de datos y el monitoreo del uso de los datos en la empresa.

Los datos imprecisos, incompletos o inconsistentes crean serios problemas operacionales y financieros para las empresas, ya que pueden crear imprecisiones en los precios de los productos, las cuentas de los clientes y los datos del inventario, además de que conducen a decisiones imprecisas sobre las acciones que debe tomar la empresa. Las empresas deben realizar acciones especiales para asegurarse de tener un alto nivel de calidad en la información. Estas acciones incluyen el uso de estándares de datos a nivel empresarial, bases de datos diseñadas para minimizar los datos inconsistentes y redundantes, auditorías de calidad de los datos y software de limpieza de datos.

## Términos clave

*Administración de la base de datos*, 230

*Administración de datos*, 230

*Almacén de datos*, 222

*Análisis predictivo*, 226

*Archivo*, 210

*Atributo*, 210

*Auditoría de calidad de los datos*, 231

*Base de datos*, 210

*Base de datos (definición rigurosa)*, 212

*Campo*, 210

*Campo clave*, 214

*Clave foránea*, 215

*Clave primaria*, 214

*DBMS objeto-relacional*, 215

*DBMS orientado a objetos*, 215

*DBMS relacional*, 213

*Definición de datos*, 217

*Dependencia programa-datos*, 211

*Diagrama entidad-relación*, 221

*Diccionario de datos*, 217

*Entidad*, 210

*Gobernanza de datos*, 230

*Inconsistencia de los datos*, 211

*Integridad referencial*, 220

*Lenguaje de consulta estructurado (SQL)*, 217

*Lenguaje de manipulación de datos*, 217

*Limpieza de datos*, 231

*Mercado de datos*, 223

*Minería de datos*, 224

*Minería de texto*, 226

*Minería Web*, 226

*Normalización*, 219

*Política de información*, 230

*Procesamiento Analítico en Línea (OLAP)*, 224

*Redundancia de los datos*, 211

*Registro*, 214

*Servidor de bases de datos*, 229

*Sistema de Administración de Bases de Datos (DBMS)*, 212

*Tupla*, 214

## Preguntas de repaso

1. ¿Cuáles son los problemas de administrar los recursos de datos en un entorno de archivos tradicional y cómo se resuelven mediante un sistema de administración de bases de datos?
  - Mencione y describa cada uno de los componentes en la jerarquía de datos.
  - Defina y explique el significado de entidades, atributos y campos clave.
  - Mencione y describa los problemas del entorno tradicional de archivos.
  - Defina una base de datos y un sistema de administración de bases de datos; describa cómo resuelve los problemas de un entorno tradicional de archivos.
2. ¿Cuáles son las principales capacidades de los sistemas de administración de bases de datos (DBMS) y por qué es tan poderoso un DBMS?
  - Nombre y describa con brevedad las capacidades de un DBMS.
  - Defina un DBMS relacional y explique cómo organiza los datos.
  - Mencione y describa las tres operaciones de un DBMS relacional.
3. ¿Cuáles son algunos principios importantes del diseño de bases de datos?
  - Defina y describa la normalización y la integridad referencial; explique cómo contribuyen a una base de datos relacional bien diseñada.
  - Defina y describa un diagrama entidad-relación; explique su función en el diseño de bases de datos.
4. ¿Cuáles son las principales herramientas y tecnologías para acceder a la información de las bases de datos y mejorar tanto el desempeño de negocios como la toma de decisiones?
  - Defina un almacén de datos; explique cómo funciona y cómo beneficia a las organizaciones.
  - Defina inteligencia de negocios y explique cómo se relaciona con la tecnología de bases de datos.
  - Describa las capacidades del procesamiento analítico en línea (OLAP).
  - Defina minería de datos; describa cómo difiere de OLAP y los tipos de información que proporciona.
  - Explique cómo difieren la minería de texto y la minería Web de la minería de datos convencional.
  - Describa cómo pueden los usuarios acceder a la información de las bases de datos internas de una compañía por medio de Web.
5. ¿Por qué son la política de información, la administración de datos y el aseguramiento de la calidad de los datos esenciales para administrar los recursos de datos de la empresa?
  - Describa los roles de la política de la información y la administración de datos en cuanto a la administración de la información.
  - Explique por qué son esenciales las auditorías de calidad de los datos y su limpieza.

## Preguntas de debate

1. Se ha dicho que no es necesario el software de administración de bases de datos para crear un entorno de bases de datos. De su opinión al respecto.
2. ¿En qué grado deben estar involucrados los usuarios finales en la selección de un sistema de administración de bases de datos y del diseño de la base de datos?
3. ¿Cuáles son las consecuencias de que una organización no tenga una política de información?

## Colaboración y trabajo en equipo: identificación de las entidades y atributos en una base de datos en línea

Con su equipo de tres o cuatro estudiantes, seleccione una base de datos en línea para explorar, como AOL Music, iGo.com o Internet Movie Database (IMDb). Explore uno de estos sitios Web para ver qué información proporciona. Después haga una lista de las entidades y atributos que la compañía operadora del sitio Web debe registrar en sus bases de datos. Haga un diagrama

de la relación entre las entidades que identifique. Si es posible, use Google Sites para publicar vínculos a páginas Web, anuncios de comunicación en equipo y asignaturas de trabajo; para lluvias de ideas, y para trabajar de manera colaborativa en los documentos del proyecto. Intentar usar Google Docs para desarrollar una presentación de sus hallazgos para la clase.



## Los problemas de la base de datos de vigilancia de terroristas continúan

### CASO DE ESTUDIO

Después de los ataques del 9-11, se estableció el Centro de Detección de Terroristas (TSC) del FBI para consolidar la información sobre los terroristas sospechosos de varias agencias gubernamentales en una sola lista para mejorar la comunicación entre las agencias. En ese entonces se creó una base de datos de terroristas sospechosos conocida como la lista de vigilancia de terroristas. Varias agencias gubernamentales de Estados Unidos habían estado manteniendo listas separadas y carecían de un proceso consistente para compartir información relevante.

Los registros en la base de datos TSC contienen información confidencial pero no clasificada sobre las identidades de los terroristas, como el nombre y la fecha de nacimiento, que se pueden compartir con otras agencias de detección. La información clasificada sobre las personas en la lista de vigilancia se mantiene en otras bases de datos de agencias policiales y de la agencia de inteligencia. Los registros de la base de datos de la lista de vigilancia se proveen a través de dos fuentes: el Centro Nacional Antiterrorista (NCTC) administrado por la oficina del director de inteligencia nacional provee información de identificación sobre individuos que tienen lazos con el terrorismo internacional. El FBI provee información de identificación sobre los individuos que tienen lazos con el terrorismo puramente nacional.

Estas agencias recolectan y mantienen información de los terroristas y nominan individuos para incluirlos en la lista de vigilancia consolidada del TSC. Tienen que seguir estrictos procedimientos establecidos por el jefe de la agencia correspondiente y deben ser aprobados por el ministro de justicia de Estados Unidos. El personal del TSC debe revisar cada registro enviado antes de agregarlo a la base de datos. Un individuo permanecerá en la lista de vigilancia hasta que el departamento o agencia correspondiente que nominó a esa persona para la lista determine que ésta se debe quitar de ella y eliminar de la base de datos.

La base de datos de la lista de vigilancia del TSC se actualiza a diario con nuevas nominaciones, modificaciones a los registros existentes y eliminaciones. Desde su creación, la lista creció de manera explosiva hasta llegar a 400 000 personas, registradas como 1.1 millones de nombres y alias, y sigue creciendo a una proporción de 200 000 registros por año. La información en la lista se distribuye a un amplio rango de sistemas de agencias gubernamentales para usarse en los esfuerzos por impedir o detectar los movimientos de los terroristas conocidos o presuntos.

Las agencias que reciben la lista son: FBI, CIA, Agencia de Seguridad Nacional (NSA), Administración de Seguridad en el Transporte (TSA), Departamento de Seguridad Nacional, Departamento de Estado, Aduanas y Protección Fronteriza, Servicio Secreto, Servicio de

Alguaciles Federales de Estados Unidos y la Casa Blanca. Las aerolíneas utilizan los datos suministrados por el sistema TSA en sus listas NoFly y Selectee para investigar previamente a los pasajeros, mientras que el Sistema de Aduanas y Protección Fronteriza de Estados Unidos utiliza los datos de la lista de vigilancia para ayudar a investigar a los viajeros que entran al país. El sistema del Departamento de Estado investiga a los que solicitan visas para entrar a Estados Unidos y a los residentes de que solicitan pasaportes, mientras que las agencias policiales estatales y locales usan el sistema del FBI para que les ayude con los arrestos, detenciones y otras actividades de justicia criminal. Cada una de estas agencias recibe el subconjunto de datos en la lista de vigilancia pertinente a su misión específica.

Cuando una persona hace una reservación en una aerolínea, llega a un puerto de entrada, solicita una visa para Estados Unidos o es detenido por la policía estatal o local dentro de este país, la agencia de investigación de primera línea o la aerolínea realizan una búsqueda basada en el nombre del individuo para compararlo con los registros de la base de datos de la lista de vigilancia de terroristas. Cuando el sistema computarizado para relacionar los nombres genera una "ocurrencia" (una coincidencia potencial de un nombre) con un registro de la lista de vigilancia, la aerolínea o agencia revisarán cada coincidencia potencial. Las coincidencias que sean claramente positivas o las exactas que no sean concluyentes (inciertas o difíciles de verificar) se envían al centro de inteligencia o de operaciones de la agencia de investigación aplicable, y también al TSC para un análisis más detallado. A su vez, el TSC revisa sus bases de datos y otras fuentes, como las bases de datos clasificadas que mantienen el NCTC y el FBI para confirmar si el individuo es una coincidencia positiva, negativa o inconclusa para el registro de la lista de vigilancia. El TSC crea un informe diario en el que sintetiza todas las coincidencias positivas con la lista de vigilancia y las distribuye a las diversas agencias federales.

El proceso de consolidar la información de distintas agencias ha sido lento y minucioso, ya que se requiere integrar por lo menos 12 bases de datos distintas. Dos años después de que se llevó a cabo el proceso de integración, se habían procesado 10 de las 12 bases de datos. Las dos restantes (el Sistema de Identificación Biométrica Automático del Servicio de Inmigración y Control de Aduanas de Estados Unidos, y el Sistema Automático Integrado de Identificación de Huellas Dactilares de Estados Unidos) son bases de datos de huellas dactilares. Aún queda más trabajo por realizar para optimizar la utilidad de la lista.

Los informes de la oficina de auditoría general y la oficina del inspector general aseguran que la lista con-



tiene imprecisiones y que las políticas departamentales del gobierno para nominar y quitar personas de la lista no son uniformes. También se ha generado una protesta pública debido al tamaño de la lista y los incidentes tan publicitados de personas que sin duda no son terroristas y descubren que se encuentran en la lista.

Para que la lista sea efectiva contra los terroristas, es necesario proteger con cuidado la información sobre el proceso de inclusión en ella. Los criterios específicos de inclusión no son del conocimiento público. Sin embargo, sabemos que para llenar sus listas de vigilancia, las agencias gubernamentales realizan rastreos amplios de información recopilada sobre los viajeros, en donde utilizan palabras mal escritas y variaciones alternativas de los nombres de los terroristas sospechosos. Esto a menudo provoca que se ingresen personas que no pertenecen a las listas de vigilancia, conocidas como "falsos positivos". También ocasiona que algunas personas aparezcan varias veces en la lista con sus nombres escritos de distintas formas.

Aunque estos criterios de selección pueden ser efectivos para rastrear tantos terroristas potenciales como sea posible, también provocan muchas más entradas erróneas en la lista de las que se generarían si el proceso requiriera información mucho más detallada para agregar nuevas entradas. Algunos ejemplos notables de 'falsos positivos' son; Michael Hicks, niño explorador de Nueva Jersey de ocho años, a quien detenían con frecuencia en el aeropuerto para una investigación adicional, y el fallecido senador Ted Kennedy, quien sufrió varios retrasos en el pasado debido a que su nombre se asemeja a un alias que alguna vez utilizó un presunto terrorista. Al igual que Kennedy, tal vez se haya agregado a Hicks debido a que su nombre es igual o similar al de otro presunto terrorista.

Estos incidentes cuestionan la calidad y la precisión de los datos en la lista de vigilancia de terroristas consolidada del TSC. En junio de 2005, un informe de la oficina del inspector general del Departamento de Justicia encontró cuentas de registros inconsistentes, registros duplicados y registros que carecían de campos de datos o tenían fuentes dudosas para sus datos. Aunque después el TSC mejoró sus esfuerzos por identificar y corregir los registros incompletos o imprecisos en la lista de vigilancia, el inspector general observó en septiembre de 2007 que la administración de la lista de vigilancia por parte del TSC aún mostraba ciertas debilidades.

Dada la opción entre una lista que detecte a todos los terroristas potenciales a costa de rastrear de manera innecesaria a algunos inocentes, y entre una lista que no pueda identificar a muchos terroristas por hacer el esfuerzo de evitar rastrear a los inocentes, muchos elegirían la lista que reconoce a todos los terroristas a pesar de las desventajas. Sin embargo, para empeorar las cosas para aquellos que ya sufren de la inconveniencia de haber sido incluidos de manera errónea en la lista, en la actualidad no hay un proceso simple y rápido de rectificación para los inocentes que esperan ser removidos de la lista.

El número de solicitudes para quitar personas de la lista de vigilancia sigue en aumento, con más de 24 000 solicitudes registradas (una cifra aproximada de 2 000 al mes), y sólo el 54 por ciento de ellas resueltas. El tiempo promedio para procesar una solicitud en 2008 era de 40 días, lo cual no era (ni lo es en la actualidad) lo bastante rápido como para estar a la par con el número de solicitudes entrantes para quitar personas de la lista. Como resultado, los viajeros que cumplían con la ley y se encontraban de manera inexplicable en la lista de vigilancia no son quitados con facilidad de ella.

En febrero de 2007, el Departamento de Seguridad Nacional instituyó su programa de solicitud de rectificación para viajeros (TRIP) para ayudar a que las personas que se agregaron por equivocación a las listas de vigilancia de terroristas se puedan quitar por sí solas, para así evitar los procesos adicionales de investigación y cuestionamiento. La madre de John Anderson afirmó que a pesar de sus mejores esfuerzos, no pudo quitar a su hijo de las listas de vigilancia. Según se informa, el senador Kennedy sólo pudo quitarse de la lista al llevar personalmente el asunto a Tom Ridge, que en ese entonces era director del Departamento de Seguridad Nacional.

Los oficiales de seguridad dicen que los errores como el que provocó que Anderson y Kennedy se incluyeran en las listas de vigilancia de pasajeros prohibidos (no-fly) y consolidada ocurren debido a la coincidencia de datos imperfectos en los sistemas de reservación de las aerolíneas con los datos imperfectos en las listas de vigilancia. Muchas aerolíneas no incluyen género, segundo nombre o fecha de nacimiento en sus registros de reservaciones, lo cual incrementa la probabilidad de falsas coincidencias.

Una manera de mejorar la detección y de ayudar a reducir el número de personas marcadas de manera errónea para una investigación adicional sería utilizar un sistema más sofisticado que involucre datos más personales sobre los individuos en la lista. La TSA está desarrollando un sistema así, conocido como "Vuelo Seguro" (Secure Flight), pero se ha retrasado en forma continua debido a las cuestiones de privacidad relacionadas con la sensibilidad y seguridad de los datos que recolectaría. Otros programas y listas de vigilancia similares, como los intentos de la NSA de recopilar información sobre presuntos terroristas, han provocado críticas por violaciones potenciales a la privacidad.

Además, la lista de vigilancia ha provocado críticas debido a su potencial de promover los perfiles y la discriminación racial. Algunos alegan que fueron incluidos por virtud de su raza y descendencia étnica, como David Fathi, un abogado para la ACLU de descendencia iraní, y Asif Iqbal, un ciudadano estadounidense de descendencia pakistaní con el mismo nombre que un detenido en Guantánamo. Los críticos abiertos de la política foránea de Estados Unidos, como algunos oficiales electos y profesores universitarios, también se han encontrado dentro de la lista.

Un informe liberado en mayo de 2009 por Glenn A. Fine, inspector general del Departamento de Justicia,

encontró que el FBI había mantenido de manera incorrecta casi 24 000 personas en su propia lista de vigilancia que suministra datos a la lista de vigilancia de terroristas, con base en información obsoleta o irrelevante. Después de examinar casi 69 000 casos de la lista del FBI, el informe descubrió que el 35 por ciento de esas personas permanecían en la lista a pesar de una justificación inadecuada. Lo más preocupante aún es que la lista no contenía los nombres de las personas que deberían de haber sido incluidas debido a sus lazos con el terrorismo.

Los oficiales del FBI afirman que la agencia ha realizado mejoras, incluyendo una mejor capacitación y un procesamiento más rápido de los casos, además de requerir que los supervisores de las oficinas regionales revisen la precisión e integridad de las nominaciones a la lista de vigilancia. No obstante, esta lista de vigilancia y las otras siguen siendo herramientas imperfectas. A principios de 2008, se reveló que 20 terroristas conocidos no estaban incluidos de manera correcta en la lista de vigilancia consolidada (lo que no queda claro es si estos individuos pudieron entrar a Estados Unidos como consecuencia).

Umar Farouk Abdulmutallab, el nigeriano que no pudo detonar explosivos plásticos en el vuelo de Northwest Airlines de Amsterdam a Detroit durante el día de Navidad de 2009, no aparecía dentro de la lista de pasajeros prohibidos. Aunque el padre de Abdulmutallab había

reportado que estaba preocupado por la radicalización de su hijo al Departamento de Estado de Estados Unidos, éste no revocó la visa de Abdulmutallab debido a que su nombre estaba mal escrito en la base de datos de visas, por lo que se le permitió entrar a Estados Unidos. Faisal Shahzad, el bombardero del auto en Times Square, fue aprehendido el 3 de mayo de 2010, sólo unos momentos antes de que su vuelo de la aerolínea Emirates hacia Dubai y Pakistán despegara. La aerolínea no había verificado una actualización de último minuto a la lista de pasajeros prohibidos en donde se había agregado el nombre de Shahzad.

**Fuentes:** Scott Shane, "Lapses Allowed Suspect to Board Plane", *The New York Times*, 4 de mayo de 2010; Mike McIntire, "Ensnared by Error on Growing U.S. Watch List", *The New York Times*, 6 de abril de 2010; Eric Lipton, Eric Schmitt y Mark Mazzetti, "Review of Jet Bomb Pilot Shows More Missed Clues", *The New York Times*, 18 de enero de 2010; Lizette Alvarez, "Meet Mikey, 8: U.S. Has Him on Watch List", *The New York Times*, 14 de enero de 2010; Eric Lichtblau, "Justice Dept. Finds Flaws in F.B.I. Terror List", *The New York Times*, 7 de mayo de 2009; Bob Egelko, "Watch-list Name Confusion Causes Hardship", *San Francisco Chronicle*, 20 de marzo de 2008; "Reports Cite Lack of Uniform Policy for Terrorist Watch List", *The Washington Post*, 18 de marzo de 2008; Siobhan Gorman, "NSA's Domestic Spying Grows as Agency Sweeps Up Data", *The Wall Street Journal*, 10 de marzo de 2008; Ellen Nakashima y Scott McCartney, "When Your Name is Mud at the Airport", *The Wall Street Journal*, 29 de enero de 2008.

## PREGUNTAS DEL CASO DE ESTUDIO

1. ¿Qué conceptos en este capítulo se ilustran en este caso?
2. ¿Por qué se creó la lista de vigilancia de terroristas consolidada? ¿Cuáles son los beneficios de la lista?
3. Describa algunas de las debilidades de la lista de vigilancia. ¿Qué factores de administración, organización y tecnología son responsables de estas debilidades?
4. ¿Qué tan efectivo es el sistema de las listas de vigilancia descrito en este caso de estudio? Explique su respuesta.
5. Si fuera responsable de la administración de la base de datos de la lista de vigilancia del TSC, ¿qué acciones tomaría para corregir algunas de estas debilidades?
6. ¿Cree usted que la lista de vigilancia de terroristas representa una amenaza considerable para la privacidad o los derechos constitucionales de los individuos? ¿Por qué sí o por qué no?

# Capítulo 7

## Telecomunicaciones, Internet y tecnología inalámbrica

### OBJETIVOS DE APRENDIZAJE

*Después de leer este capítulo, usted podrá responder a las siguientes preguntas:*

1. ¿Cuáles son los principales componentes de las redes de telecomunicaciones y las tecnologías de red clave?
2. ¿Cuáles son los principales medios de transmisión de telecomunicaciones y de tipos de redes?
3. ¿Cómo funcionan Internet y su tecnología, y cómo dan soporte a la comunicación y el negocio electrónico?
4. ¿Cuáles son las principales tecnologías y estándares para redes inalámbricas, comunicación y acceso a Internet?
5. ¿Por qué son valiosas las redes de sensores inalámbricas y de identificación por radio frecuencia (RFID) para las empresas?

#### *Sesiones interactivas:*

La batalla sobre la neutralidad de la red

Monitoreo de los empleados en las redes: ¿falta de ética o buenos negocios?

### RESUMEN DEL CAPÍTULO

#### 7.1 LAS TELECOMUNICACIONES Y REDES EN EL MUNDO DE NEGOCIOS ACTUAL

Tendencias de redes y comunicación  
¿Qué es una red de computadoras?  
Tecnologías de redes digitales clave

#### 7.2 REDES DE COMUNICACIONES

Comparación entre señales digitales y analógicas  
Tipos de redes  
Medios de transmisión físicos

#### 7.3 INTERNET GLOBAL

¿Qué es Internet?  
Direccionamiento y arquitectura de Internet  
Servicios de Internet y herramientas de comunicación  
Web

#### 7.4 LA REVOLUCIÓN INALÁMBRICA

Sistemas celulares  
Redes inalámbricas de computadoras y acceso a Internet  
Redes de sensores inalámbricas y RFID

#### 7.5 PROYECTOS PRÁCTICOS SOBRE MIS

Problemas de decisión gerencial  
Mejora de la toma de decisiones: uso del software de hojas de cálculo para evaluar los servicios inalámbricos  
Obtención de la excelencia operacional: uso de los motores de búsqueda Web para la investigación de negocios

#### MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

Servicio de cómputo y comunicaciones proporcionados por los distribuidores de comunicaciones comerciales

Servicios y tecnologías de red de banda ancha

Generaciones de sistemas celulares

WAP y I-Mode: estándares celulares inalámbricos para el acceso Web

Aplicaciones inalámbricas para administrar las relaciones con el cliente, la cadena de suministro y el servicio médico

Web 2.0

## HYUNDAI HEAVY INDUSTRIES CREA UN ASTILLERO INALÁMBRICO

• Qué se siente ser el constructor de buques más grande del mundo? Pregunte a Hyundai Heavy Industries (HHI), cuyas oficinas generales están en Ulsan, Corea del Sur, y produce el 10 por ciento de los barcos en el mundo. HHI construye buques cisterna, buques de carga a granel, cargueros, de transporte de gas y elabora productos químicos, motores de barcos, plataformas de petróleo y gas en mar abierto, así como tuberías submarinas.

Sin duda, coordinar y optimizar la producción de tantos productos distintos es una tarea abrumadora. La compañía ya ha invertido casi \$50 millones en software de planificación de fábricas para ayudar a administrar este esfuerzo. Sin embargo, la "fábrica" de HHI abarca 11 kilómetros cuadrados (4.2 millas cuadradas) y se extiende por tierra y mar, consta de nueve diques secos, de los cuales el mayor abarca más de siete campos de fútbol americano y en él se pueden construir cuatro navíos al mismo tiempo. Más de 12 000 trabajadores construyen hasta 30 navíos a la vez y utilizan millones de piezas que varían en tamaño, desde pequeños remaches hasta edificios de cinco pisos.

Este entorno de producción demostró ser demasiado grande y complejo como para poder rastrear con facilidad el movimiento de piezas e inventario en tiempo real, al momento en que ocurrían estos eventos. Sin datos que se actualicen al instante, las eficiencias del software de planificación de recursos empresariales son muy limitadas. Para empeorar las cosas, la reciente crisis económica afectó mucho a HHI, ya que el comercio mundial y la navegación se desplomaron. Los pedidos para nuevos barcos en 2009 disminuyeron hasta 7.9 millones de toneladas brutas compensadas (CGT, una medida del tamaño de un navío), en comparación con los 150 millones de CGT del año anterior. En este entorno económico, Hyundai Heavy buscaba nuevas formas de reducir los gastos y optimizar la producción.

La solución de HHI fue una red inalámbrica de alta velocidad que abarcaba todo el astillero, creada por KT Corp., la empresa de telecomunicaciones más grande en Corea del Sur. Esta red puede transmitir datos a una velocidad de 4 megabits por segundo, casi cuatro veces más rápido que el típico módem por cable que ofrece servicio de Internet de alta velocidad en los hogares estadounidenses. La compañía utiliza sensores de radio para rastrear el movimiento de las piezas a medida que pasan del taller de fabricación a un costado del dique seco, y después a un barco en construcción. Los trabajadores en el barco utilizan computadoras notebook o teléfonos móviles portátiles para acceder a los planos y entablar conversaciones en video de dos vías con los diseñadores del barco en la oficina, a más de una milla de distancia.

En el pasado, los trabajadores que se encontraban dentro de un navío bajo tierra o debajo del nivel del mar tenían que trepar a la superficie para usar un teléfono o radio de comunicación cuando tenían que hablar con alguien respecto a un problema. La nueva red inalámbrica está conectada a las líneas eléctricas en el barco, que transportan datos digitales a los transmisores inalámbricos Wi-Fi colocados alrededor del casco durante la construcción. Los teléfonos de Internet, las cámaras Web y las PC de los trabajadores están vinculados con el sistema Wi-Fi, por lo que pueden usar el servicio VoIP de Skype para llamar a sus compañeros en la superficie. Los diseñadores en un edificio de oficinas a una milla de distancia del sitio de construcción utilizan las cámaras Web para investigar los problemas.

En los caminos de los astilleros, 30 camiones de transporte con receptores conectados a la red inalámbrica actualizan su posición cada 20 segundos y la envían a una sala de control. Esto ayuda a los despachadores a asociar la ubicación de los camiones de transporte con los pedidos de pie-

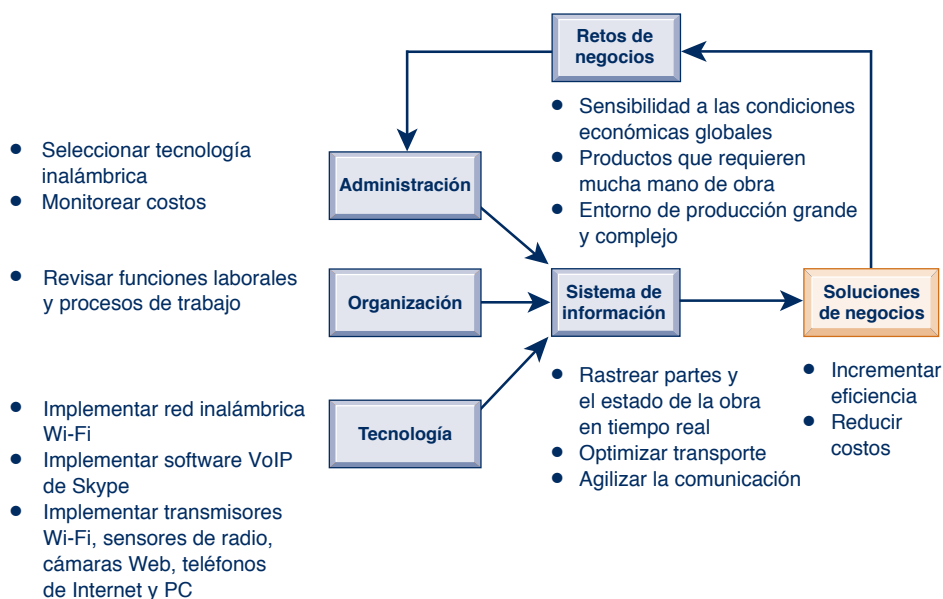
zas, con lo cual se acortan los viajes que realiza cada camión. Todos los movimientos del día se terminan a las 6 P.M. en lugar de las 8 P.M. Al aumentar la eficiencia en las operaciones y reducir los costos de mano de obra, se espera que la tecnología inalámbrica ahorre a Hyundai Heavy \$40 millones al año.

**Fuentes:** Evan Ramstad, "High-Speed Wireless Transforms a Shipyard", *The Wall Street Journal*, 15 de marzo de 2010, y "Hyundai Heavy Plans Wireless Shipyard", *The Korea Herald*, 30 de marzo de 2010.

La experiencia de Hyundai Heavy Industries ilustra algunas de las poderosas herramientas y oportunidades que ofrece la tecnología de redes contemporánea. La compañía utilizó la tecnología de redes inalámbricas para conectar a los diseñadores, peones, barcos en construcción y los vehículos de transporte para acelerar la comunicación y la coordinación, además de reducir el tiempo, la distancia o el número de pasos requeridos para realizar una tarea.

El diagrama de apertura del capítulo dirige la atención hacia los puntos importantes generados por este caso y este capítulo. Hyundai Heavy Industries produce barcos y otros productos que requieren de mucha mano de obra y son sensibles a los cambios en las condiciones económicas globales. Su entorno de producción es grande y complejo; además es muy difícil de coordinar y de administrar. La compañía necesita mantener los costos de operación en el nivel más bajo posible. El astillero de HHI se extiende a través de una inmensa área, por lo que era en extremo difícil monitorear y coordinar los distintos proyectos y equipos de trabajo.

La gerencia decidió que la tecnología inalámbrica ofrecía una solución e hizo los arreglos para implementar una red inalámbrica a través de todo el astillero. La red también vincula el astillero con los diseñadores en la oficina de HHI a una milla de distancia. La red facilitó de manera considerable el rastreo de las piezas y las actividades de producción, además de la optimización de los movimientos de los camiones de transporte. HHI tuvo que rediseñar su proceso de producción y otros procesos de trabajo para aprovechar la nueva tecnología.



## 7.1

LAS TELECOMUNICACIONES Y REDES  
EN EL MUNDO DE NEGOCIOS ACTUAL

Si opera una empresa o trabaja en una, no puede hacerlo sin las redes. Necesita una manera rápida de comunicarse con sus clientes, proveedores y empleados. Todavía en 1990, las empresas utilizaban el sistema postal o el telefónico con voz o fax para la comunicación. No obstante, en la actualidad, usted y sus empleados utilizan computadoras y correo electrónico, Internet, teléfonos celulares y computadoras móviles conectadas a redes inalámbricas para este fin. Ahora las redes e Internet son casi un sinónimo de hacer negocios.

## TENDENCIAS DE REDES Y COMUNICACIÓN

En el pasado las empresas utilizaban dos tipos fundamentalmente distintos de redes: las redes telefónicas y las redes de computadora. En un principio, las redes telefónicas manejaban la comunicación por voz y las redes de computadoras se encargaban del tráfico de datos. Las compañías telefónicas fabricaron las redes telefónicas durante el siglo xx mediante el uso de tecnologías de transmisión de voz (hardware y software), y estas compañías casi siempre operaban como monopolios regulados en todo el mundo. Las compañías de computadoras fabricaron las redes computacionales con el objetivo original de transmitir datos entre los ordenadores en distintas ubicaciones.

Gracias a la continua desregulación de las telecomunicaciones y a la innovación en la tecnología de la información, las redes telefónicas y computacionales están convergiendo en una sola red digital que utiliza estándares basados en Internet y equipo compartidos. En la actualidad, los proveedores de telecomunicaciones como AT&T y Verizon ofrecen servicios de transmisión de datos, acceso a Internet, servicio de teléfono celular y programación de televisión, así como servicio de voz (vea el caso de apertura del capítulo 3). Las compañías de cable, como Cablevisión y Comcast, ahora ofrecen servicio de voz y acceso a Internet. Las redes de computadoras se han expandido para incluir servicios de teléfono por Internet y video limitado. Todas estas comunicaciones de voz, video y datos se basan cada vez más en la tecnología de Internet.

Las redes de comunicaciones tanto de voz como de datos también se han vuelto más poderosas (veloces), más portables (pequeñas y móviles) y menos costosas. Por ejemplo, la velocidad de conexión a Internet típica en el año 2000 era de 56 kilobits por segundo, pero en la actualidad más del 60 por ciento de los usuarios de Internet en Estados Unidos tienen conexiones de **banda ancha** de alta velocidad que ofrecen las compañías de telefonía y TV por cable, las cuales operan entre 1 y 15 millones de bits por segundo. El costo de este servicio ha disminuido en forma exponencial, de 25 centavos por kilobit en el año 2000 a una pequeña fracción de un centavo en la actualidad.

Cada vez se utilizan más las plataformas inalámbricas de banda ancha para llevar a cabo la comunicación de voz y datos, así como el acceso a Internet, los teléfonos celulares, los dispositivos portátiles móviles y las PC en las redes inalámbricas. En unos cuantos años, más de la mitad de los usuarios de Internet en Estados Unidos utilizarán teléfonos inteligentes y computadoras netbook móviles para acceder a Internet. En 2010, 84 millones de estadounidenses accedieron a Internet por medio de dispositivos móviles, y se espera que este número se duplique para el año 2014 (eMarketer, 2010).

## ¿QUÉ ES UNA RED DE COMPUTADORAS?

Si tuviera que conectar las computadoras de dos o más empleados para que trabajaran juntas en la misma oficina, necesitaría una red de computadoras. ¿Qué es en sí una red? En su forma más simple, una red consiste de dos o más computadoras conectadas entre sí. La figura 7-1 ilustra los principales componentes de hardware,



software y transmisión que se utilizan en una red simple: una computadora cliente y una computadora servidor dedicada, interfaces de red, un medio de conexión, software de sistema operativo de red, y un concentrador (hub) o un conmutador (switch).

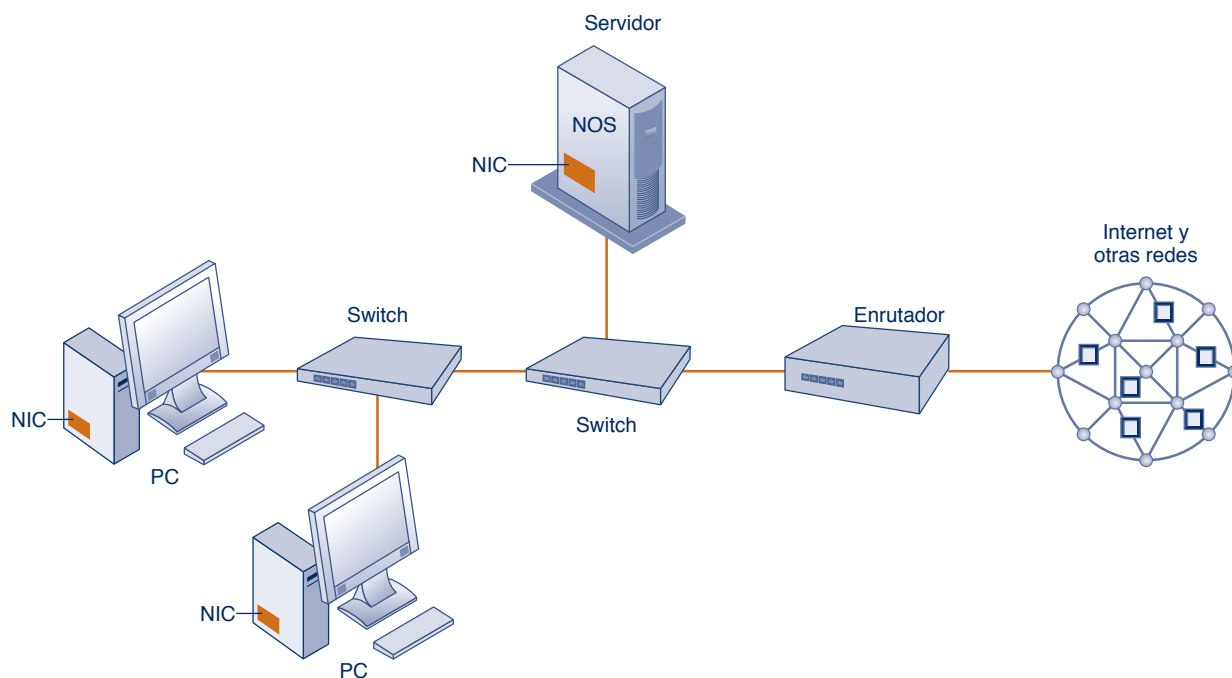
Cada computadora en la red contiene un dispositivo de interfaz de red llamado **tarjeta de interfaz de red (NIC)**. La mayoría de las computadoras personales en la actualidad tienen integrada esta tarjeta en la tarjeta madre. El medio de conexión para vincular componentes de red puede ser un cable telefónico, uno coaxial o una señal de radio, en el caso de las redes de teléfonos celulares y de área local inalámbricas (redes Wi-Fi).

El **sistema operativo de red (NOS)** enruta y administra las comunicaciones en la red y coordina los recursos de ésta. Puede residir en cualquier computadora en la red, o principalmente en una computadora servidor dedicada para todas las aplicaciones en la red. Una computadora servidor es una computadora en una red que realiza importantes funciones de red para computadoras cliente, como servir páginas Web, almacenar datos y almacenar el sistema operativo de red (lo cual le permite controlar la red). Los paquetes de software servidor tal como Microsoft Windows Server, Linux y Novell Open Enterprise Server son los sistemas operativos de red más utilizados.

La mayoría de las redes también contienen un switch o un hub que actúa como un punto de conexión entre las computadoras. Los **hubs** son dispositivos muy simples que conectan componentes de red, para lo cual envían un paquete de datos a todos los demás dispositivos conectados. Un **switch** tiene mayor funcionalidad que un hub y puede tanto filtrar como reenviar datos a un destino especificado en la red.

¿Y qué hay si se desea comunicar con otra red, como Internet? Necesitaría un **enrutador**: un procesador de comunicaciones que se utiliza para enrutar paquetes de datos a través de distintas redes y asegurar que los datos enviados lleguen a la dirección correcta.

**FIGURA 7-1 COMPONENTES DE UNA RED DE COMPUTADORAS SIMPLE**



Aquí se ilustra una red de computadoras muy simple, la cual consiste en computadoras, un sistema operativo de red que reside en una computadora servidor dedicada, cable para conectar los dispositivos, tarjetas de interfaz de red (NICs), switches y un enrutador.

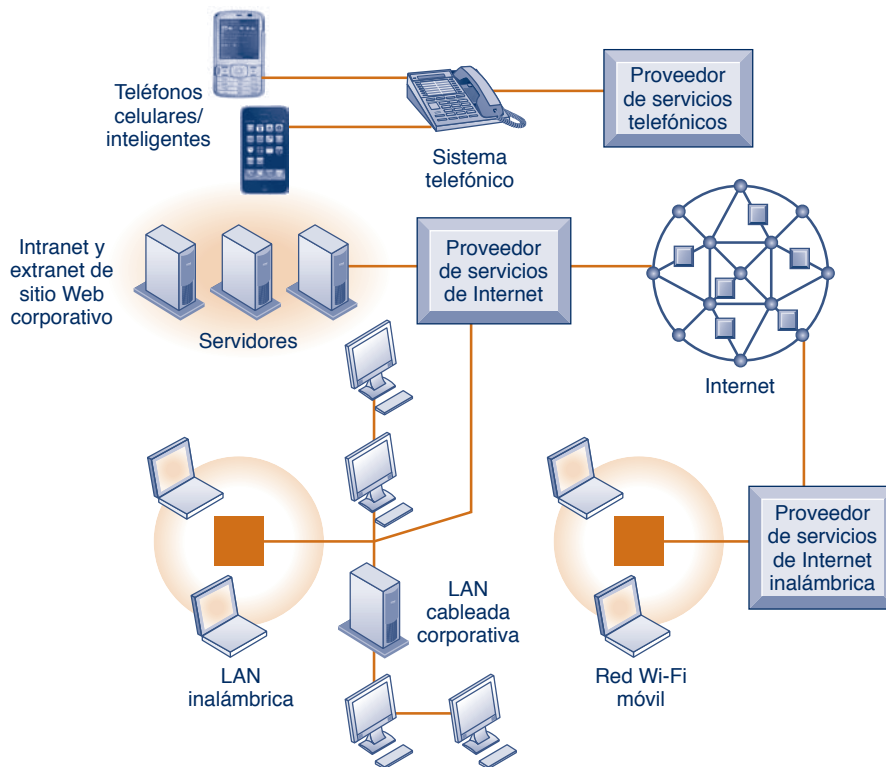
## Redes en compañías grandes

La red que acabamos de describir podría ser adecuada para una empresa pequeña. Pero, ¿qué hay sobre las grandes compañías con muchas ubicaciones distintas y miles de empleados? A medida que una empresa crece y se crean cientos de pequeñas redes de área local, estas redes se pueden enlazar en una infraestructura de red a nivel corporativo. La infraestructura de redes para una gran corporación consiste de una gran cantidad de estas pequeñas redes de área local vinculadas con otras redes de área local y con redes corporativas en toda la empresa. Varios servidores poderosos soportan un sitio Web corporativo, una intranet corporativa y tal vez una extranet. Algunos de estos servidores se vinculan a otras computadoras grandes que soportan sistemas de procesamiento en segundo plano (back-end).

La figura 7-2 provee una ilustración de estas redes de nivel corporativo más complejas y de mayor escala. Aquí puede ver que la infraestructura de red corporativa soporta una fuerza de ventas móvil que utiliza teléfonos celulares y teléfonos inteligentes, empleados móviles vinculados con el sitio Web de la compañía, redes internas de la compañía que utilizan redes de área local inalámbricas móviles (redes Wi-Fi) y un sistema de videoconferencias para apoyar a los gerentes en todo el mundo. Además de estas redes corporativas, la infraestructura de la empresa por lo general cuenta con una red telefónica separada que maneja la mayoría de los datos de voz. Muchas empresas se están deshaciendo de sus redes telefónicas tradicionales y utilizan teléfonos de Internet que operan en sus redes de datos existentes (lo cual describiremos después).

Como puede ver en esta figura, una infraestructura de red corporativa extensa utiliza una amplia variedad de tecnologías: desde el servicio telefónico ordinario y las redes de datos corporativas hasta el servicio de Internet, Internet inalámbrica y teléfonos celulares. Uno de los principales problemas a los que se enfrentan las corpora-

**FIGURA 7-2** INFRAESTRUCTURA DE RED CORPORATIVA



La infraestructura de red corporativa de la actualidad es una colección de muchas redes distintas: la red telefónica conmutada pública, Internet, redes de área local corporativas que vinculan grupos de trabajo, departamentos o pisos de oficinas.

ciones en la actualidad es cómo integrar todas las distintas redes de comunicaciones y canales en un sistema coherente que permita que la información fluya de una parte de la corporación a otra, y de un sistema a otro. A medida que cada vez más redes de comunicación se vuelvan digitales y basadas en tecnologías de Internet, será más fácil integrarlas.

## TECNOLOGÍAS DE REDES DIGITALES CLAVE

Las redes digitales contemporáneas e Internet se basan en tres tecnologías clave: computación cliente/servidor, el uso de la conmutación de paquetes y el desarrollo de estándares de comunicación con amplio uso (el más importante de los cuales es el Protocolo de Control de Transmisión/Protocolo Internet, o TCP/IP) para vincular redes y computadoras dispares.

### Computación cliente/servidor

En el capítulo 5 introducimos la computación cliente/servidor: un modelo de computación distribuida en el que parte del poder de procesamiento se encuentra dentro de pequeñas computadoras cliente económicas, y que reside literalmente en equipos de escritorio, laptops o en dispositivos portátiles. Estos poderosos clientes están vinculados entre sí mediante una red controlada por una computadora servidor de red. El servidor establece las reglas de comunicación para la red y provee a cada cliente una dirección, de modo que otros equipos puedan encontrarlos en la red.

La computación cliente/servidor ha reemplazado en gran parte a la computación centralizada de mainframes, en donde casi todo el procesamiento ocurre en una extensa computadora mainframe central. La computación cliente/servidor ha extendido la computación a departamentos, grupos de trabajo, pisos de fábricas y otras partes de las empresas a las que no se podía dar servicio mediante una arquitectura centralizada. Internet es la implementación más grande de la computación cliente/servidor.

### Conmutación de paquetes

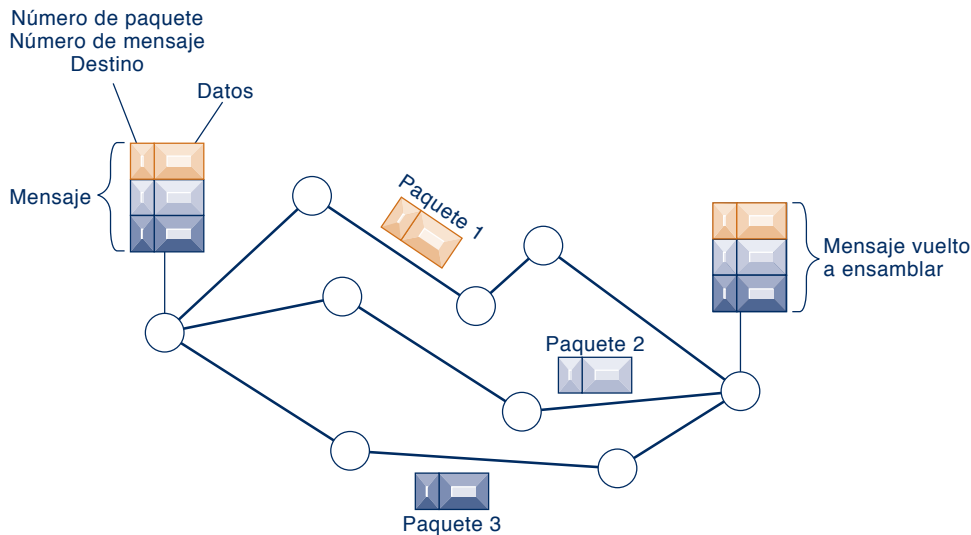
La **conmutación de paquetes** es un método para dividir mensajes digitales en parcelas llamadas paquetes, y éstos se envían por distintas rutas de comunicación a medida que se vuelven disponibles, para después reensamblarlos una vez que llegan a sus destinos (vea la figura 7-3). Antes del desarrollo de la conmutación de paquetes, para las redes de computadoras se rentaban circuitos telefónicos dedicados para comunicarse con otras computadoras en ubicaciones remotas. En las redes de conmutación de circuitos, como el sistema telefónico, se ensambla un circuito completo punto a punto y después se puede iniciar la comunicación. Estas técnicas dedicadas de conmutación de paquetes eran costosas y desperdiciaban la capacidad de comunicaciones disponible; el circuito se mantenía sin importar que se enviaran o no datos.

La conmutación de paquetes hace un uso mucho más eficiente de la capacidad de comunicaciones de una red. En las redes de conmutación de paquetes, los mensajes primero se descomponen en pequeños grupos fijos de datos conocidos como paquetes. Los cuales contienen información para dirigir el paquete a la dirección correcta y verificar los errores de transmisión junto con los datos. Los paquetes se transmiten a través de varios canales de comunicación mediante enrutadores; cada paquete viaja de manera independiente. Los paquetes de datos que provienen de un origen se enrutan a través de muchas rutas y redes antes de volver a ensamblarse en el mensaje original cuando llegan a sus destinos.

### TCP/IP y conectividad

En una red típica de telecomunicaciones, diversos componentes de hardware y software necesitan trabajar en conjunto para transmitir información. Los distintos compo-

**FIGURA 7-3 REDES DE CONMUTACIÓN DE PAQUETES Y COMUNICACIONES DE PAQUETES**



Los datos se agrupan en pequeños paquetes, los cuales se transmiten de manera independiente a través de varios canales de comunicación y se vuelven a ensamblar en su destino final.

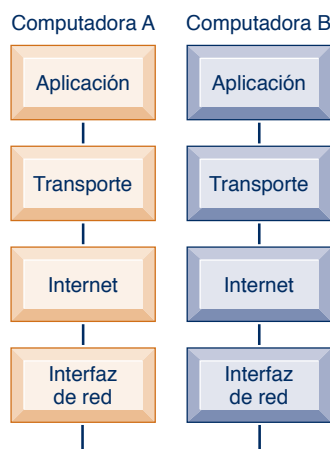
nentes en una red sólo se pueden comunicar si se adhieren a un conjunto común de reglas denominadas protocolos. Un **protocolo** es un conjunto de reglas y procedimientos que gobiernan la transmisión de información entre dos puntos en una red.

En el pasado, la gran diversidad de protocolos propietarios e incompatibles obligaba con frecuencia a las empresas de negocios a comprar equipo de cómputo y comunicaciones de un solo distribuidor. Sin embargo, en la actualidad, las redes corporativas utilizan cada vez más un único estándar común a nivel mundial, conocido como **Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP)**. Este protocolo se desarrolló a principios de la década de 1970 para apoyar los esfuerzos de la Agencia de Investigación de Proyectos Avanzados del Departamento de Defensa de Estados Unidos (DARPA) para ayudar a los científicos a transmitir datos entre distintos tipos de computadoras a través de largas distancias.

TCP/IP utiliza una suite de protocolos; TCP e IP son los principales. TCP se refiere al Protocolo de Control de Transmisión (TCP), el cual se encarga del movimiento de datos entre computadoras. TCP establece una conexión entre las computadoras, secuencia la transferencia de paquetes y confirma la recepción de los paquetes enviados. IP se refiere al Protocolo de Internet (IP), el cual es responsable de la entrega de paquetes y comprende los procesos de desensamblar y reensamblar los paquetes durante la transmisión. La figura 7-4 ilustra el modelo de referencia de cuatro capas del Departamento de Defensa para TCP/IP.

1. Capa de aplicación. La capa de aplicación permite a los programas de aplicaciones cliente acceder a las otras capas y define los protocolos que utilizan esas aplicaciones para intercambiar datos. Uno de estos protocolos de aplicación es el Protocolo de Transferencia de Hipertexto (HTTP), el cual se utiliza para transferir archivos de páginas Web.
2. Capa de transporte. La capa de transporte es responsable de proveer a la capa de aplicación los servicios de comunicación y de paquetes. Esta capa tiene TCP y otros protocolos.
3. Capa de Internet. La capa de Internet es responsable de direccionar, enrutar y empaquetar los paquetes de datos conocidos como datagramas IP. El Protocolo de Internet es uno de los protocolos utilizados en esta capa.

**FIGURA 7-4 EL MODELO DE REFERENCIA DEL PROTOCOLO DE CONTROL DE TRANSMISIÓN/PROTOCOLO DE INTERNET (TCP/IP)**



Esta figura ilustra las cuatro capas del modelo de referencia TCP/IP para las comunicaciones.

4. Capa de interfaz de red. En la parte inferior del modelo de referencia, la capa de Interfaz de red es responsable de colocar paquetes en el medio de red y recibirlos del mismo, que podría ser cualquier tecnología de red.

Dos computadoras que utilizan TCP/IP se pueden comunicar aunque estén basadas en distintas plataformas de hardware y software. Los datos que se envían de una computadora a la otra descienden por todas las cuatro capas, empezando por la capa de aplicación de la computadora emisora y pasando por la capa de Interfaz de red. Una vez que los datos llegan a la computadora huésped receptora, suben por las capas y se vuelven a ensamblar en un formato que la computadora receptora pueda utilizar. Si la computadora receptora encuentra un paquete dañado, pide a la computadora emisora que lo retransmita. Este proceso se invierte cuando la computadora receptora responde.

## 7.2 REDES DE COMUNICACIONES

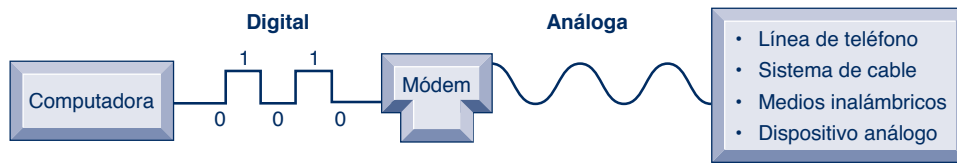
Ahora analicemos más de cerca las tecnologías de redes alternativas disponibles para las empresas.

### COMPARACIÓN ENTRE SEÑALES DIGITALES Y ANALÓGICAS

Hay dos formas de comunicar un mensaje en una red: ya sea mediante una señal analógica o una digital. Una *señal analógica* se representa mediante una forma de onda continua que pasa por un medio o canal de comunicación y se ha utilizado para la comunicación por voz. Los dispositivos analógicos más comunes son el auricular telefónico, el altavoz en su computadora o los audífonos de su iPod, cada uno de los cuales crea formas analógicas que su oído pueda escuchar.

Una *señal digital* es una forma de onda binaria discreta, en vez de una forma de onda continua. Las señales digitales comunican la información como cadenas de dos estados discretos: bits cero y bits uno, que se representan como pulsos eléctricos de encendido-apagado. Las computadoras usan señales digitales y requieren un módem para convertirlas en señales analógicas que se puedan enviar (o recibir) a través de líneas telefónicas, líneas de cable o medios inalámbricos que utilicen señales analógicas (vea la figura 7-5). La palabra **módem** es abreviación de modulador-demodulador. Los módems de

**FIGURA 7-5 FUNCIONES DEL MÓDEM**



Un módem es un dispositivo que transfiere señales digitales en forma analógica (y a la inversa) de manera que las computadoras puedan transmitir datos en redes analógicas como las de teléfono y de cable.

cable conectan su computadora a Internet mediante el uso de una red de cable. Los módems DSL conectan su computadora a Internet mediante el uso de una red de líneas de tierra de la compañía telefónica. Los módems inalámbricos realizan la misma función que los tradicionales; conectan su computadora a una red inalámbrica que podría ser una red telefónica celular o una red Wi-Fi. Sin los módems, las computadoras no se podrían comunicar entre sí mediante redes analógicas (como el sistema telefónico y las redes de cable).

## TIPOS DE REDES

Hay muchos tipos distintos de redes y varias formas de clasificarlas. Una manera de verlas es en términos de su alcance geográfico (vea la tabla 7-1).

### Redes de área local

Si trabaja en una empresa que utiliza redes, lo más probable es que se conecte con otros empleados y grupos a través de una red de área local. Una **red de área local (LAN)** está diseñada para conectar computadoras personales y otros dispositivos digitales dentro de un radio de media milla o 500 metros. Por lo general, las LAN conectan unas cuantas computadoras en una pequeña oficina, todas las computadoras en un edificio o todas en varios edificios en cercana proximidad. Las LAN también se utilizan para vincularse a redes de área amplia de larga distancia (WAN, que describiremos más adelante en esta sección) y a otras redes alrededor del mundo por medio de Internet.

Dé un vistazo a la figura 7-1, que puede servir como un modelo para una pequeña LAN en una oficina. Una computadora es un servidor de archivos de red dedicado, a través del cual los usuarios pueden acceder a los recursos de cómputo compartidos en la red, incluyendo programas de software y archivos de datos.

El servidor determina quién obtiene acceso a cuáles recursos y en qué secuencia. El enrutador conecta la LAN con otras redes, que podrían ser Internet u otra red corporativa, de modo que la LAN pueda intercambiar información con las redes externas. Los sistemas operativos de LAN más comunes son Windows, Linux y Novell. Cada uno de estos sistemas operativos de red soporta TCP/IP como su protocolo de redes predefinido.

**TABLA 7-1 TIPOS DE REDES**

TIPO	ÁREA
Red de área local (LAN)	Hasta 500 metros (media milla); una oficina o el piso de un edificio
Red de área de campus (CAN)	Hasta 1 000 metros (una milla); un campus universitario o edificio corporativo
Red de área metropolitana (MAN)	Una ciudad o área metropolitana
Red de área amplia (WAN)	Un área transcontinental o global



Ethernet es el estándar de LAN dominante a nivel de red física; especifica el medio físico para transportar las señales entre computadoras, las reglas de control del acceso y un conjunto estandarizado de bits que se utilizan para transportar datos a través del sistema. En un principio, Ethernet soportaba una tasa de transferencia de datos de 10 megabits por segundo (Mbps). Las versiones más recientes, como Fast Ethernet y Gigabit Ethernet, soportan tasas de transferencia de datos de 100 Mbps y 1 gigabit por segundo (Gbps), respectivamente; se utilizan en las conexiones troncales de red.

La LAN que se ilustra en la figura 7-1 utiliza una arquitectura cliente/servidor en donde el sistema operativo reside principalmente en un solo servidor de archivos, que provee una gran parte del control y los recursos para la red. Como alternativa, las redes LAN pueden usar una arquitectura de igual a igual. Una red de **igual a igual** trata de la misma forma a todos los procesadores y se utiliza en primera instancia en las redes pequeñas con 10 o menos usuarios. Las diversas computadoras en la red pueden intercambiar datos mediante el acceso directo; además de compartir dispositivos periféricos sin necesidad de pasar por un servidor separado.

En las LAN que utilizan la familia de sistemas operativos Windows Server, la arquitectura de igual a igual se denomina *modelo de red de grupos de trabajo*, en donde un pequeño grupo de computadoras pueden compartir recursos, como archivos, carpetas e impresoras a través de la red sin un servidor dedicado. En contraste, el *modelo de red de dominios* de Windows utiliza un servidor dedicado para administrar a las computadoras en la red.

Las LAN más grandes tienen muchos clientes y varios servidores, con servidores separados para servicios específicos, como ordenar y administrar tanto archivos como bases de datos (servidores de archivos o servidores de bases de datos), administrar impresoras (servidores de impresión), almacenar y administrar correo electrónico (servidores de correo), o almacenar y administrar páginas Web (servidores Web).

Algunas veces las LAN se describen en términos de la forma en que sus componentes se conectan entre sí, o su **topología**. Existen tres topologías importantes de LAN: estrella, bus y anillo (vea la figura 7-6).

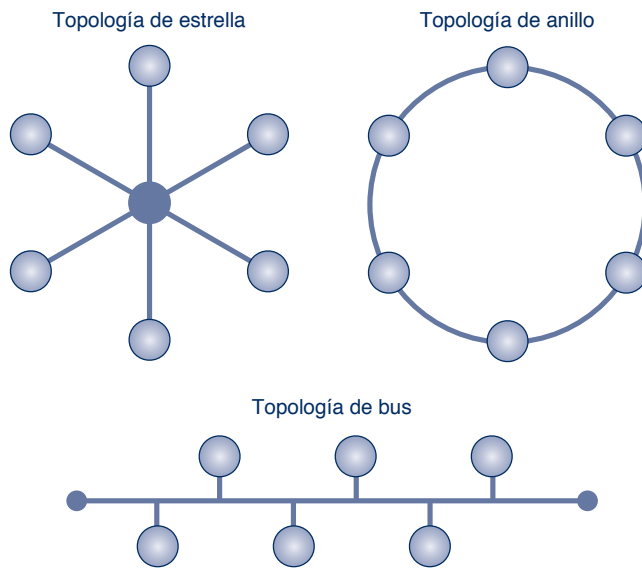
En una **topología de estrella**, todos los dispositivos en la red se conectan a un solo concentrador. La figura 7-6 ilustra una topología de estrella simple en la que todo el tráfico de red fluye a través del concentrador. En una *red de estrella extendida*, varias capas de concentradores se organizan en una jerarquía.

En una **topología de bus**, una estación transmite señales que viajan en ambas direcciones a lo largo de un solo segmento de transmisión. Todas las señales se difunden en ambas direcciones a toda la red. Todas las máquinas en la red reciben las mismas señales, y el software instalado en las computadoras cliente permite a cada cliente escuchar los mensajes dirigidos a él de manera específica. La topología de bus es la topología de Ethernet más común.

Una **topología de anillo** conecta a los componentes de la red en un lazo cerrado. Los mensajes pasan de una computadora a otra sólo en una dirección a través del lazo, y sólo una estación puede transmitir a la vez. La topología de anillo se encuentra principalmente en las LAN antiguas que utilizan software de red Token Ring.

## Redes metropolitanas y de área amplia

Las **redes de área amplia (WAN)** abarcan distancias geográficas amplias: regiones completas, estados, continentes o todo el globo terráqueo. La WAN más universal y poderosa es Internet. Las computadoras se conectan a una WAN por medio de redes públicas, como el sistema telefónico o los sistemas de cable privados, o por medio de líneas o satélites que se rentan. Una **red de área metropolitana (MAN)** abarca un área metropolitana, por lo general una ciudad y sus principales suburbios. Su alcance geográfico está entre una WAN y una LAN.

**FIGURA 7-6** TOPOLOGÍAS DE RED

Las tres topologías de red básicas son: estrella, bus y anillo.

## MEDIOS DE TRANSMISIÓN FÍSICOS

Las redes usan distintos tipos de medios de transmisión, entre ellos cable trenzado, cable coaxial, fibra óptica y medios para la transmisión inalámbrica. Cada uno tiene sus ventajas y desventajas. Es posible obtener un amplio rango de velocidades para cualquier medio dado, dependiendo de la configuración de software y hardware.

### Cable trenzado

El **cable trenzado** consiste en tiras de cable de cobre trenzadas en pares y es uno de los tipos más antiguos de medio de transmisión. Muchos de los sistemas telefónicos en los edificios tenían cables trenzados instalados para la comunicación analógica, pero se pueden usar también para la comunicación digital. Aunque es uno de los medios de transmisión físicos más antiguos, los cables trenzados que se utilizan en las redes LAN de la actualidad, como CAT5, pueden obtener velocidades de hasta 1 Gbps. El cableado de par trenzado se limita a un tendido máximo recomendado de 100 metros (328 pies).

### Cable coaxial

El **cable coaxial**, similar al que se utiliza para la televisión por cable, consiste en cable de cobre con aislamiento grueso, el cual puede transmitir un mayor volumen de datos que el cable trenzado. El cable se utilizó en las primeras LAN y se sigue usando en la actualidad para mayores tendidos (más de 100 metros) en edificios grandes. Puede alcanzar velocidades de hasta 1 Gbps.

### Fibra óptica y redes ópticas

El **cable de fibra óptica** consiste en tiras unidas de fibra de vidrio transparente, cada una del grosor de un cabello humano. Los datos se transforman en pulsos de luz, los cuales se envían a través del cable de fibra óptica mediante un dispositivo láser a velocidades que varían desde 500 kilobits hasta varios billones de bits por segundo en entornos experimentales. El cable de fibra óptica es mucho más veloz, ligero y durable que el medio de cable; además se adapta bien a los sistemas que requieren transferencias de grandes volúmenes de datos. Sin embargo, es más costoso que otros medios físicos de transmisión y más difícil de instalar.

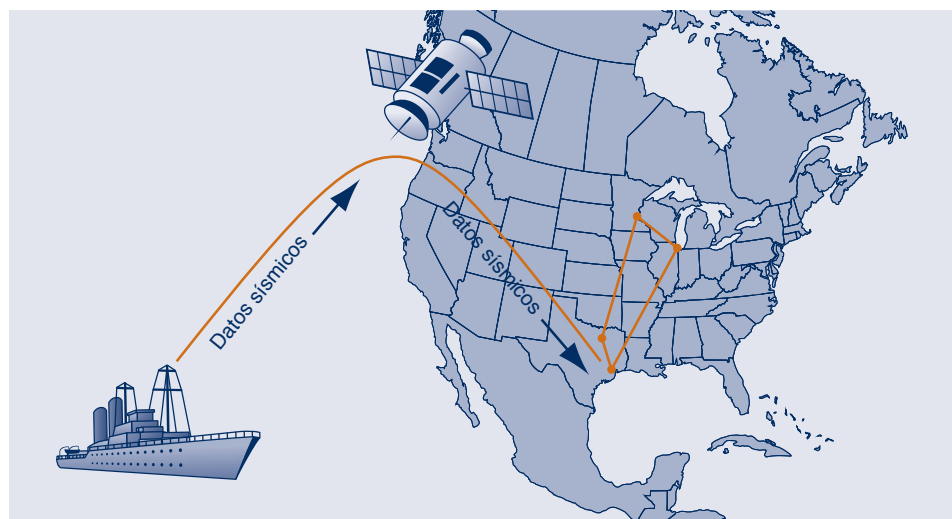
Hasta hace poco, el cable de fibra óptica se había utilizado sólo en la conexión troncal de red de alta velocidad, que maneja la mayor cantidad de tráfico. Ahora las compañías de teléfonos celulares como Verizon están empezando a llevar las líneas de fibra óptica al hogar para nuevos tipos de servicios, como el de Internet Fiber Optic Services (FiOS) de Verizon, que ofrece velocidades de descarga de hasta 50 Mbps.

### Medios de transmisión inalámbricos

La transmisión inalámbrica se basa en las señales de radio de varias frecuencias. Hay tres tipos de redes inalámbricas que utilizan las computadoras: de microondas, celular y Wi-Fi. Los sistemas de **microondas**, tanto terrestres como celestiales, transmiten señales de radio de alta frecuencia a través de la atmósfera y se utilizan mucho para la comunicación punto a punto de alto volumen y larga distancia. Las señales de microondas siguen una línea recta y no se doblan con la curvatura de la tierra. Por lo tanto, los sistemas de transmisión terrestres de larga distancia requieren que las estaciones de transmisión estén separadas por una distancia aproximada de 37 millas. También se pueden realizar transmisiones de larga distancia al usar los satélites de comunicación como estaciones repetidoras para las señales de microondas que se transmiten desde estaciones terrestres.

Los satélites de comunicación utilizan la transmisión por microondas; por lo general para transmitir en organizaciones extensas, dispersas en varias ubicaciones geográficas que sería difícil conectar en red mediante el uso de medios de cables o microondas terrestres, así como para el servicio de Internet en el hogar, en especial en las áreas rurales. Por ejemplo, la compañía de energía global BP p.l.c. usa satélites para la transferencia en tiempo real de los datos de exploración de los campos petroleros que se recopilan de las búsquedas en el fondo del océano. Mediante el uso de satélites geosíncronicos, los barcos de exploración transfieren esos datos a los centros de cómputo centrales en Estados Unidos para que los utilicen los investigadores en Houston, Tulsa y los suburbios de Chicago. La figura 7-7 ilustra cómo funciona este sistema. Los satélites también se utilizan para servicio de televisión e Internet en el hogar. Los dos principales proveedores de Internet por satélite (Dish Network y DirectTV) tienen cerca de 30 millones de suscriptores; cerca del 17 por ciento de todos los hogares en Estados Unidos acceden a Internet mediante el uso de servicios de satélite (eMarketer, 2010).

**FIGURA 7-7 SISTEMA DE TRANSMISIÓN POR SATÉLITE DE BP**



Los satélites de comunicación ayudan a BP a transferir los datos sísmicos entre los barcos de exploración petroleros y los centros de investigación en Estados Unidos.

Los sistemas celulares también utilizan ondas de radio y una variedad de protocolos distintos para comunicarse con antenas de radio (torres) colocadas dentro de áreas geográficas adyacentes, conocidas como celdas. Las comunicaciones que se transmiten de un **teléfono celular** a una celda local pasan de una antena a otra (de celda en celda) hasta que llegan a su destino final.

Las redes inalámbricas están suplantando a las redes fijas tradicionales para muchas aplicaciones; además están creando nuevas aplicaciones, servicios y modelos de negocios. En la sección 7.4 veremos una descripción detallada de las aplicaciones y los estándares de tecnología que dan fuerza a la “revolución inalámbrica”.

### Velocidad de transmisión

La cantidad total de información digital que se puede transmitir a través de cualquier medio de comunicación se mide en bits por segundo (bps). Se requiere un cambio de señal (o ciclo) para transmitir uno o varios bits; por lo tanto, la capacidad de transmisión de cada tipo de medio de telecomunicaciones es una función de su frecuencia. El número de ciclos por segundo que se pueden enviar a través del medio se mide en **hertz**: un hertz equivale a un ciclo por segundo.

El rango de frecuencias que se pueden acomodar en un canal de telecomunicaciones en particular se conoce como su **ancho de banda**. El ancho de banda es la diferencia entre las frecuencias más alta y más baja que se pueden acomodar en un solo canal. Cuanto más grande sea el rango de frecuencias, mayor será el ancho de banda y también la capacidad de transmisión del canal.

## 7.3 INTERNET GLOBAL

Todos utilizamos Internet, y muchos de nosotros no podemos vivir sin ella. Se ha convertido en una herramienta personal y de negocios indispensable. Pero, ¿qué es en sí Internet? ¿Cómo funciona y qué ofrece la tecnología de Internet a las empresas? Veamos las características más importantes.

### ¿QUÉ ES INTERNET?

Internet se ha convertido en el sistema de comunicación público más extenso en el mundo, que en la actualidad compite con el sistema telefónico global en cuanto a alcance y rango. También es la implementación más grande en el mundo de la computación cliente/servidor y de las interredes, ya que vincula a millones de redes individuales en todo el mundo. Esta red de redes global empezó a principios de la década de 1970 como una red del Departamento de Defensa de Estados Unidos para enlazar a científicos y profesores universitarios de todo el mundo.

La mayoría de los hogares y pequeñas empresas se conectan a Internet mediante una suscripción a un proveedor de servicios de Internet. Un **proveedor de servicios de Internet (ISP)** es una organización comercial con una conexión permanente a Internet que vende conexiones temporales a suscriptores minoristas. Algunos de los principales ISP son EarthLink, NetZero, AT&T y Time Warner. Los individuos también se conectan a Internet por medio de sus firmas de negocios, universidades o centros de investigación que tienen dominios de Internet designados.

Existe una variedad de servicios para las conexiones de Internet de los ISP. El método de conectarse a través de una línea telefónica tradicional y un módem, a una velocidad de 56.6 kilobits por segundo (Kbps), solía ser la forma más común de conexión en todo el mundo, pero ahora las conexiones de banda ancha son las que predominan. La línea de suscriptor digital (DSL), el cable, las conexiones a Internet vía satélite y las líneas T proveen estos servicios de banda ancha.

Las tecnologías de **línea de suscriptor digital (DSL)** operan a través de las líneas telefónicas existentes para transportar voz, datos y video a tasas de transmisión que varían desde 385 Kbps hasta llegar a 9 Mbps. Las **conexiones de Internet por cable** que ofrecen los distribuidores de televisión por cable utilizan líneas coaxiales de cable digital para ofrecer acceso a Internet de alta velocidad a los hogares y negocios. Pueden proveer acceso de alta velocidad a Internet de hasta 15 Mbps. En áreas en donde los servicios de DSL y de cable no están disponibles, es posible acceder a Internet vía satélite, aunque algunas conexiones tienen velocidades de envío más lentas que en otros servicios de banda ancha.

T1 y T3 son estándares telefónicos internacionales para la comunicación digital. Son líneas dedicadas rentadas, adecuadas para las empresas o agencias gubernamentales que requieren niveles de servicio garantizados de alta velocidad. Las **líneas T1** ofrecen una entrega garantizada a 1.54 Mbps, y las líneas T3 ofrecen una entrega a 45 Mbps. Internet no provee niveles de servicio garantizados similares, sino tan sólo el “mejor esfuerzo”.

## DIRECCIONAMIENTO Y ARQUITECTURA DE INTERNET

Internet se basa en la suite de protocolos de red TCP/IP que describimos en una sección anterior en este capítulo. A cada computadora en Internet se le asigna una **dirección de Protocolo de Internet (IP)** única, que en la actualidad es un número de 32 bits representado por cuatro cadenas de números, los cuales varían de 0 a 255 y se separan por puntos. Por ejemplo, la dirección IP de [www.microsoft.com](http://www.microsoft.com) es 207.46.250.119.

Cuando un usuario envía un mensaje a otro en Internet, primero se descompone en paquetes mediante el protocolo TCP. Cada paquete contiene su dirección de destino. Después los paquetes se envían del cliente al servidor de red, y de ahí a tantos servidores como sea necesario para que lleguen a una computadora específica con una dirección conocida. En la dirección de destino, los paquetes se vuelven a ensamblar para formar el mensaje original.

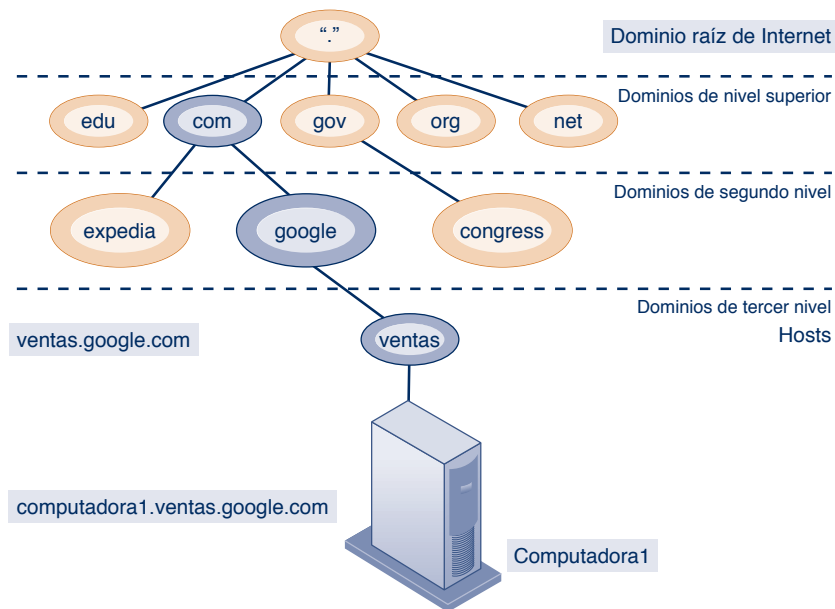
### El sistema de nombres de dominio

Como sería sumamente difícil para los usuarios de Internet recordar cadenas de 12 números, el **sistema de nombres de dominio (DNS)** convierte los nombres de dominio en direcciones IP. El **nombre de dominio** es el nombre en inglés o español que corresponde a la dirección IP numérica única de 32 bits para cada computadora conectada a Internet. Los servidores DNS mantienen una base de datos que contiene direcciones IP asociadas a sus correspondientes nombres de dominio. Para que una computadora tenga acceso a Internet, los usuarios sólo necesitan especificar su nombre de dominio.

DNS tiene una estructura jerárquica (vea la figura 7-8). En la parte superior de la jerarquía DNS se encuentra el dominio raíz. El dominio hijo de la raíz se denomina dominio de nivel superior y el dominio hijo de un dominio de nivel superior se denomina dominio de segundo nivel. Los dominios de nivel superior son nombres de dos o tres caracteres con los que de seguro usted está familiarizado por navegar en Web; por ejemplo, .com, .edu, .gov y los diversos códigos de países como .ca para Canadá o .it para Italia. Los dominios de segundo nivel tienen dos partes, las cuales designan un nombre de nivel superior y uno de segundo nivel —como [buy.com](http://buy.com), [nyu.edu](http://nyu.edu) o [amazon.ca](http://amazon.ca). Un nombre de host en la parte inferior de la jerarquía designa una computadora específica, ya sea en Internet o en una red privada.

Las extensiones de dominio más comunes que están disponibles en la actualidad y cuentan con aprobación oficial se muestran en la siguiente lista. Los países también tienen nombres de dominio como .uk, .au y .fr (Reino Unido, Australia y Francia, respectivamente); además hay una nueva clase de dominios “internacionalizados” de nivel superior que utilizan caracteres que no pertenecen al alfabeto en inglés o español tradicional (ICANN, 2010). En el futuro, esta lista se expandirá para incluir muchos tipos más de organizaciones e industrias.

**FIGURA 7-8 EL SISTEMA DE NOMBRES DE DOMINIO**



El sistema de nombres de dominio es un sistema jerárquico con un dominio raíz, dominios de nivel superior, dominios de segundo nivel y computadoras host en el tercer nivel.

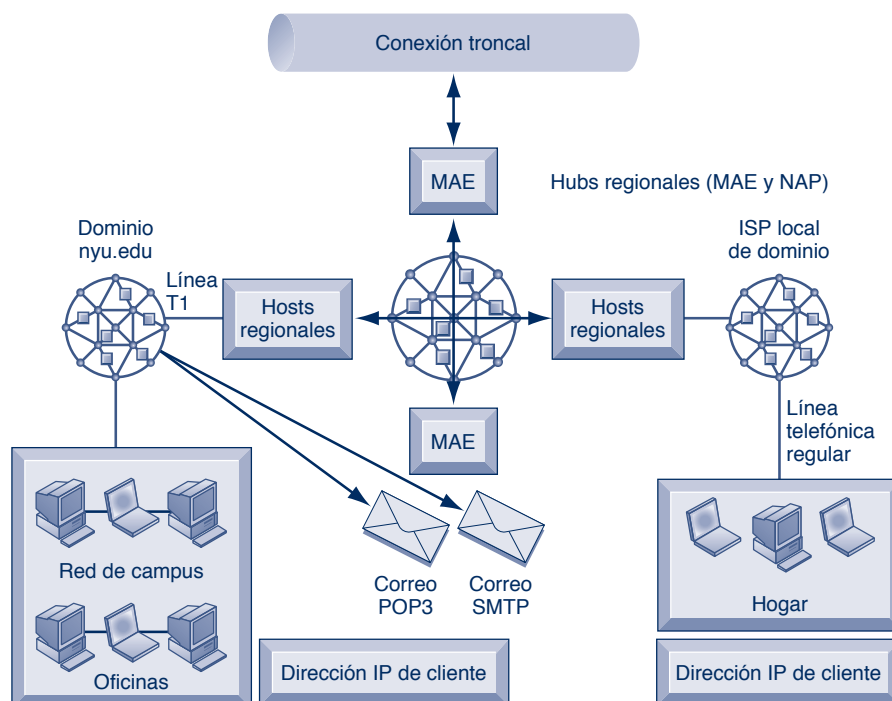
.com	Organizaciones/empresas comerciales
.edu	Instituciones educativas
.gov	Agencias gubernamentales de Estados Unidos
.mil	Milicia de Estados Unidos
.net	Computadoras de red
.org	Organizaciones y fundaciones sin fines de lucro
.biz	Firmas de negocios
.info	Proveedores de información

## Arquitectura y gobernanza de Internet

El tráfico de datos en Internet se transporta a través de redes troncales de alta velocidad transcontinentales, que por lo general operan en el rango de 45 Mbps a 2.5 Gbps en la actualidad (vea la figura 7-9). Casi todas estas líneas troncales pertenecen a las compañías telefónicas de larga distancia (denominadas *proveedores de servicios de red*) o a los gobiernos nacionales. Las líneas de conexión local pertenecen a las compañías telefónicas y de televisión por cable regionales en Estados Unidos, que conectan a Internet a los usuarios minoristas en los hogares y a empresas. Las redes regionales rentan el acceso a los ISP, las compañías privadas e instituciones gubernamentales.

Cada organización paga sus propias redes y servicios locales de conexión a Internet, de lo cual una parte se paga a los propietarios de las líneas troncales de larga distancia. Los usuarios individuales de Internet pagan a los ISP por usar su servicio; por lo general se trata de una cuota de suscripción fija, sin importar qué tanto o qué tan poco utilicen Internet. Ahora el debate está en si debe o no continuar este acuerdo, o si los que usan Internet con mucha frecuencia para descargar grandes archivos de video y música deben pagar más por el ancho de banda que consumen. La Sesión interactiva sobre organizaciones explora este tema, ya que examina los pros y los contras de la neutralidad de la red.



**FIGURA 7-9 ARQUITECTURA DE RED DE INTERNET**

La troncal de Internet se conecta a redes regionales, que a su vez proveen acceso a los proveedores de servicio de Internet, las grandes firmas y las instituciones gubernamentales. Los puntos de acceso a la red (NAP) y las centrales telefónicas de área metropolitana (MAE) son concentradores (hubs) en donde la troncal se cruza con las redes regionales y locales, y en donde los propietarios de las troncales se conectan entre sí.

Nadie es “dueño” de Internet, por lo cual no tiene una administración formal. Sin embargo, las políticas de Internet a nivel mundial se establecen a través de varias organizaciones profesionales y organismos gubernamentales, como lo son; el Consejo de Arquitectura de Internet (IAB), que ayuda a definir la estructura general de Internet; la Corporación de Internet para la Asignación de Nombres y Números (ICANN), que asigna direcciones IP, y el Consorcio World Wide Web (W3C), encargado de establecer el lenguaje de marcado de hipertexto y otros estándares de programación para Web.

Estas organizaciones influyen en las agencias gubernamentales, propietarios de redes, ISP y desarrolladores de software con el objetivo de mantener Internet en operación de la manera más eficiente posible. Internet también se debe conformar a las leyes de las naciones —estados soberanos en donde opera, así como a las infraestructuras técnicas que existen dentro de las naciones-estados—. Aunque en los primeros años de Internet y Web había muy poca interferencia legislativa o ejecutiva, esta situación está cambiando a medida que ésta desempeña un papel cada vez más importante en la distribución de la información y el conocimiento, incluso el contenido que algunos encuentran censurable.

### Internet en el futuro: IPv6 e Internet2

El diseño original de Internet no incluía la transmisión de cantidades masivas de datos y miles de millones de usuarios. Como muchas corporaciones y gobiernos han estado recibiendo extensos bloques de millones de direcciones IP para dar cabida a las fuerzas de trabajo actuales y futuras, y debido al crecimiento en sí de la población en Internet, el mundo se quedará sin direcciones IP disponibles si seguimos utilizando la conven-

ción de direccionamiento existente para 2012 o 2013. Ya se encuentra en desarrollo una nueva versión del esquema de direccionamiento IP conocido como *Protocolo de Internet versión 6 (IPv6)*, el cual contiene direcciones de 128 bits ( $2$  a la potencia de  $128$ ), o más de mil billones de direcciones únicas posibles.

**Internet2** y próxima generación de Internet (NGI) son consorcios que representan a 200 universidades, empresas privadas y agencias gubernamentales en Estados Unidos, que trabajan en una nueva versión robusta de Internet con ancho de banda alto. Han establecido varias redes troncales nuevas de alto rendimiento, con anchos de banda que alcanzan hasta 100 Gbps. Los grupos de investigación de Internet2 están desarrollando e implementando nuevas tecnologías para prácticas de enrutamiento más efectivas; distintos niveles de servicio, dependiendo del tipo y la importancia de los datos que se transmiten, y aplicaciones avanzadas para computación distribuida, laboratorios virtuales, bibliotecas digitales, aprendizaje distribuido y teleinmersión. Estas redes no sustituyen la red Internet pública, pero fungen como bancos de pruebas para la tecnología de punta que en un momento dado puede migrar a la red Internet pública.

## SERVICIOS DE INTERNET Y HERRAMIENTAS DE COMUNICACIÓN

Internet se basa en tecnología cliente/servidor. Los individuos que utilizan Internet controlan lo que hacen por medio de aplicaciones cliente en sus computadoras, como el software de navegador Web. Los datos, entre ellos los mensajes de correo electrónico y las páginas Web, se almacenan en servidores. Un cliente usa Internet para solicitar información de un servidor Web específico en una computadora distante, y el servidor envía la información solicitada de vuelta al cliente a través de Internet. Los capítulos 5 y 6 describen cómo funcionan los servidores Web con los servidores de aplicación y los servidores de bases de datos para acceder a la información desde las aplicaciones de sistemas de información internas de una organización y sus bases de datos asociadas. En la actualidad las plataformas cliente cuentan no sólo equipos PC y otras computadoras, sino también con teléfonos celulares, pequeños dispositivos digitales de bolsillo y otros dispositivos de información.

### Servicios de Internet

Una computadora cliente que se conecta a Internet tiene acceso a una variedad de servicios, como el correo electrónico, los grupos electrónicos de discusión, las salas de chat y la mensajería instantánea, **Telnet**, el **protocolo de transferencia de archivos (FTP)** y Web. La tabla 7-2 provee una breve descripción de estos servicios.

Cada servicio de Internet se implementa mediante uno o más programas de software. Todos los servicios se pueden ejecutar en una sola computadora servidor, o se

**TABLA 7-2 PRINCIPALES SERVICIOS DE INTERNET**

CAPACIDAD	FUNCIONES SOPORTADAS
Correo electrónico	Mensajería de persona a persona; compartición de documentos
Salas de chat y mensajería instantánea	Conversaciones interactivas
Grupos de noticias	Grupos de discusión en tableros de anuncios electrónicos
Telnet	Iniciar sesión en un sistema de computadora y trabajar en otro
Protocolo de transferencia de archivos (FTP)	Transferir archivos de una computadora a otra
World Wide Web	Recuperar y mostrar información, además de darle formato (incluidos texto, audio, gráficos y video) mediante el uso de vínculos de hipertexto

## SESIÓN INTERACTIVA: ORGANIZACIONES

### LA BATALLA SOBRE LA NEUTRALIDAD DE LA RED

¿Qué tipo de usuario de Internet es usted? ¿La utiliza en primera instancia para enviar y recibir un poco de correo electrónico y buscar números telefónicos? ¿O está en línea todo el día, viendo videos en YouTube, descargando archivos de música o participando en juegos masivos multijugador en línea? Si pertenece a este último tipo de usuario, entonces consume una gran cantidad de ancho de banda y cientos de millones de personas como usted podrían empezar a provocar que Internet se haga lenta. YouTube consumió en 2007 el mismo ancho de banda que el que consumieron todos los usuarios de Internet en 2000. Éste es uno de los argumentos que existen en la actualidad para cobrar a los usuarios de Internet con base en la cantidad de capacidad de transmisión que utilizan.

Si la demanda de los usuarios por Internet sobrepasa la capacidad de la red, tal vez Internet no se detendría de golpe pero los usuarios tendrían que lidiar con velocidades de descarga demasiado lentas y un rendimiento pobre de YouTube, Facebook y otros servicios que utilizan muchos datos (el uso frecuente de dispositivos iPhone en áreas urbanas tales como Nueva York y San Francisco ya ha degradado el servicio en la red inalámbrica de AT&T. Esta compañía informa que el 3 por ciento de su base de suscriptores es responsable del 40 por ciento de su tráfico de datos).

Otros investigadores tienen la creencia de que, a medida que aumenta el tráfico digital en Internet, incluso a una razón del 50 por ciento anual, la tecnología para manejar todo este tráfico está avanzando a un ritmo igual de rápido.

Además de estos aspectos técnicos, el debate en cuanto a medir el uso de Internet se centra alrededor del concepto de la neutralidad de la red. Este concepto representa la idea de que los proveedores de servicios de Internet deben permitir a los clientes el mismo acceso al contenido y las aplicaciones, sin importar el origen o naturaleza del contenido. En la actualidad, no hay duda de que Internet sea neutral: todo el tráfico en Internet se trata con igualdad, puesto que el primero en llegar es el primero en ser atendido por los propietarios de las conexiones troncales de Internet.

Sin embargo, las compañías de telecomunicaciones y de cable no están felices con este arreglo. Desean poder cobrar precios diferenciados con base en la cantidad de ancho de banda consumida por el contenido que se transmita a través de Internet. Estas compañías creen que los precios diferenciados son "la manera más justa" de financiar las inversiones necesarias en sus infraestructuras de red.

Los proveedores de servicios de Internet señalan el aumento en la piratería de los materiales protegidos por derechos de autor a través de Internet. Comcast, el segundo proveedor de servicios de Internet más grande en Estados Unidos, informó que la compartición ilegal de

archivos con material protegido por derechos de autor estaba consumiendo el 50 por ciento de su capacidad de red. En 2008, la compañía redujo la velocidad de transmisión de los archivos de BitTorrent, que se utilizan mucho para la piratería y la compartición ilegal de materiales con derechos de autor, incluyendo video. La Comisión Federal de Comunicaciones (FCC) dictaminó que Comcast tenía que dejar de reducir la velocidad del tráfico de igual a igual en nombre de la administración de la red. Después Comcast presentó una demanda legal para desafiar la autoridad de la FCC en cuanto a cumplir con la neutralidad de la red. En abril de 2010, una corte de apelaciones federal falló a favor de Comcast con el argumento de que la FCC no tenía autoridad para regular cómo debe administrar su red un proveedor de Internet.

Los defensores de la neutralidad de la red están presionando al Congreso para buscar formas de regular la industria y evitar que los proveedores de redes adopten prácticas similares a Comcast. Entre la extraña alianza de defensores de la neutralidad de la red están; a MoveOn.org, la Coalición Cristiana, la Asociación de bibliotecas estadounidenses, todos los principales grupos de consumidores, muchos bloggers y pequeñas empresas, y algunas compañías de Internet de gran tamaño, como Google y Amazon.

Los defensores de la neutralidad de la red argumentan que el riesgo de la censura aumenta cuando los operadores de red pueden bloquear o reducir en forma selectiva la velocidad del acceso a cierto contenido, como los videos de Hulu o el acceso a los servicios competidores de bajo costo, como Skype y Vonage. Ya existen muchos ejemplos de proveedores de Internet que restringen el acceso a materiales confidenciales (como el gobierno de Pakistán que bloquea el acceso a sitios anti-musulmanes y a YouTube en su totalidad, en respuesta al contenido que considera difamatorio para el Islam).

Los partidarios de la neutralidad de la red también argumentan que una Internet neutral alienta a todos a innovar sin permiso de las compañías de teléfono y de cable o de otras autoridades, y este campo de juego nivelado ha engendrado incontables empresas nuevas. La acción de permitir el flujo de la información sin restricciones es esencial para los mercados libres y la democracia, a medida que cada vez hay más comercios y sociedades que se conectan a Internet.

Los propietarios de las redes creen que la regulación para implementar la neutralidad de la red impedirá la competitividad de Estados Unidos al sofocar la innovación, frenar los gastos de capital para nuevas redes y contener la habilidad de sus redes en cuanto a lidiar con la explosión en la demanda de Internet y el tráfico inalámbrico. El servicio de Internet en Estados Unidos se encuentra detrás de muchas otras naciones en cuanto a velocidad en general, costo y calidad del servicio, lo cual agrega credibilidad a este argumento.

Y con suficientes opciones para acceder a Internet, la regulación no sería esencial para promover la neutralidad de la red. Los consumidores insatisfechos sólo tendrían que cambiar de proveedores que hagan cumplir la neutralidad de la red y permitan un uso ilimitado de Internet.

Puesto que se derrocó la resolución de Comcast, los esfuerzos de la FCC por apoyar la neutralidad de la red han quedado en modo de espera al tiempo que se busca algún medio de regular el servicio de Internet de banda ancha dentro de las restricciones de la ley y las resoluciones de los juzgados en la actualidad. Una propuesta es reclasificar la transmisión de Internet de banda ancha como un servicio de telecomunicaciones, de modo que la FCC pudiera aplicar las regulaciones para las redes telefónicas tradicionales, que tienen décadas de antigüedad.

En agosto de 2010, Verizon y Google emitieron la declaración de una política en la que proponen que los reguladores implementen la neutralidad de la red en las conexiones fijas, pero no en las redes inalámbricas,

que se están convirtiendo en la plataforma dominante de Internet. La propuesta fue un esfuerzo por definir algún tipo de punto medio que pudiera salvaguardar la neutralidad de la red y que al mismo tiempo proporcionara a las empresas de comunicaciones la flexibilidad que necesitan para administrar sus redes y generar ingresos a partir de éstas. Ninguno de los principales participantes en el debate sobre la neutralidad de la red mostraron su apoyo; ambos lados permanecen atrincherados.

**Fuentes:** Joe Nocera, "The Struggle for What We Already Have", *The New York Times*, 4 de septiembre de 2010; Claire Cain Miller, "Web Plan is Dividing Companies", *The New York Times*, 11 de agosto de 2010; Wayne Rash, "Net Neutrality Looks Dead in the Clutches of Congress", *eWeek*, 13 de junio de 2010; Amy Schatz y Spencer E. Ante, "FCC Web Rules Create Pushback", *The Wall Street Journal*, 6 de mayo de 2010; Amy Schatz, "New U.S. Push to Regulate Internet Access", *The Wall Street Journal*, 5 de mayo de 2010, y Joanie Wexler, "Net Neutrality: Can We Find Common Ground?", *Network World*, 1 de abril de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

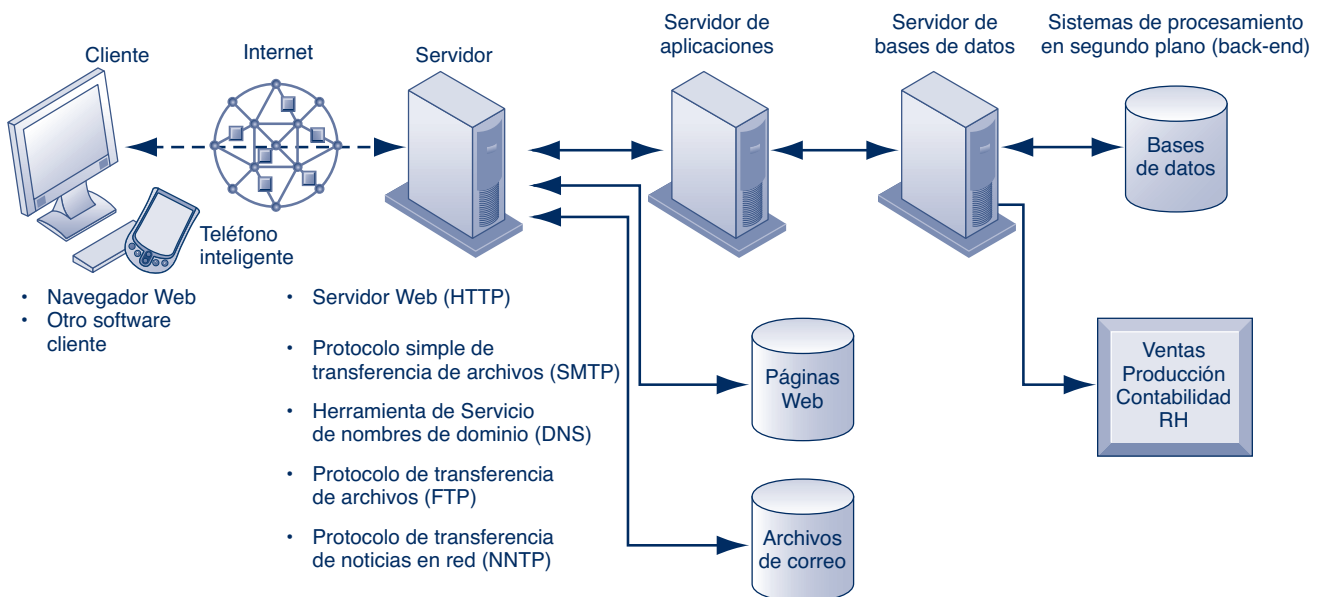
## MIS EN ACCIÓN

1. ¿Qué es la neutralidad de la red? ¿Por qué operó Internet bajo la neutralidad de la red hasta este punto en el tiempo?
2. ¿Quién está a favor de la neutralidad de la red? ¿Quién se opone? ¿Por qué?
3. ¿Cuál sería el impacto sobre los usuarios individuales, empresas y gobiernos si los proveedores de Internet cambiaran a un modelo de servicio en niveles?
4. ¿Está usted a favor de la legislación que haga cumplir la neutralidad de la red? ¿Por qué sí o por qué no?

1. Visite el sitio Web de la Coalición para la apertura de Internet (Open Internet Coalition) y seleccione cinco organizaciones miembros. Después visite el sitio Web de cada una de estas organizaciones o navegue por Web para encontrar más información sobre cada una de ellas. Escriba un breve ensayo en el que explique por qué cada organización está a favor de la neutralidad de la red.
2. Calcule cuánto ancho de banda consume al usar Internet a diario. ¿Cuántos correos electrónicos envía a diario y cuál es el tamaño de cada uno (su programa de correo electrónico puede mostrar el tamaño de los archivos)? ¿Cuántos clips de video y de música descarga a diario y cuál es el tamaño de cada uno? Si ve YouTube con frecuencia, navegue en Web para averiguar el tamaño de un archivo típico de YouTube. Sume la cantidad de archivos de correo electrónico, audio y video que transmite o recibe en un día ordinario.

pueden asignar distintos servicios a distintas máquinas. La figura 7-10 ilustra una manera en que se pueden distribuir estos servicios en una arquitectura cliente/servidor multinivel.

El **correo electrónico** permite intercambiar mensajes de una computadora a otra, con capacidades para dirigir mensajes a varios recipientes, reenviar mensajes y adjuntar documentos de texto o archivos multimedia a los mensajes. Aunque algunas organizaciones operan sus propios sistemas de correo electrónico internos, en la actualidad la mayoría del correo electrónico se envía a través de Internet. Los costos del correo electrónico son mucho menores que los equivalentes de transmisión de voz, del servicio postal o de entrega de un día a otro, por lo cual Internet se convierte en un medio de comunicaciones muy económico y veloz. La mayoría de los mensajes de correo electrónico llegan a cualquier parte del mundo en cuestión de segundos.

**FIGURA 7-10 COMPUTACIÓN CLIENTE/SERVIDOR EN INTERNET**

Las computadoras cliente que ejecutan software de navegador Web y otros tipos de software pueden acceder a una selección de servicios en servidores a través de Internet. Estos servicios pueden ejecutarse todos en un solo servidor o en varios servidores especializados.

Casi el 90 por ciento de los lugares de trabajo en Estados Unidos tienen empleados que se comunican de manera interactiva mediante herramientas de **chat** o de mensajería instantánea. Las salas de chat permiten que dos o más personas conectadas de manera simultánea a Internet sostengan conversaciones interactivas en vivo. Ahora los sistemas de chat soportan charlas de voz y video, así como conversaciones escritas. Muchas empresas minoristas en línea ofrecen servicios de chat en sus sitios Web para atraer visitantes, fomentar las compras repetidas y mejorar el servicio al cliente.

La **mensajería instantánea** es un tipo de servicio de chat que permite a los participantes crear sus propios canales privados. El sistema de mensajería instantánea alerta al usuario cada vez que alguien en su lista privada está en línea, de modo que pueda iniciar una sesión de chat con otros individuos. Algunos de los sistemas de mensajería instantánea para los consumidores son Yahoo! Messenger, Google Talk y Windows Live Messenger. Las compañías que se preocupan por la seguridad utilizan sistemas de mensajería instantánea propietarios tales como Lotus Sametime.

Los grupos de noticias son grupos de discusión a nivel mundial que se publican en tableros de anuncios electrónicos en Internet, en donde las personas comparten información e ideas sobre un tema definido, como la radiología o las bandas de rock. Cualquiera puede publicar mensajes en estos tableros de anuncios para que otros los lean. Existen muchos miles de grupos que hablan sobre casi cualquier tema concebible.

Se supone que el uso que dan los empleados al correo electrónico, la mensajería instantánea e Internet debe incrementar la productividad de los trabajadores, pero la Sesión interactiva complementaria sobre administración muestra que tal vez éste no sea siempre el caso. Ahora muchos gerentes de compañías tienen la creencia de que necesitan monitorear e incluso regular la actividad en línea de sus empleados. Pero, ¿es esto ético? Aunque hay algunas sólidas razones de negocios por las que las compañías necesitan monitorear el correo electrónico y las actividades Web de sus empleados, ¿qué significa esto para la privacidad del empleado?

## Voz sobre IP

Internet también se ha convertido en una plataforma popular para la transmisión de voz y las redes corporativas. La tecnología de **Voz sobre IP (VoIP)** transmite información de voz en forma digital mediante el uso de la conmutación de paquetes, con lo cual se



evitan los costos que cobran las redes telefónicas locales y de larga distancia (vea la figura 7-11). Las llamadas que de manera ordinaria se transmitirían a través de las redes telefónicas públicas viajan a través de la red corporativa con base en el Protocolo de Internet, o la red Internet pública. Se pueden hacer y recibir llamadas de voz con una computadora equipada con un micrófono y altavoces, o mediante un teléfono habilitado para VoIP.

Las firmas de cable como Time Warner y Cablevisión ofrecen el servicio de VoIP junto con sus ofertas de Internet de alta velocidad y cable. Skype ofrece el servicio de VoIP gratuito a nivel mundial mediante el uso de una red de igual a igual, y Google cuenta con su propio servicio gratuito de VoIP.

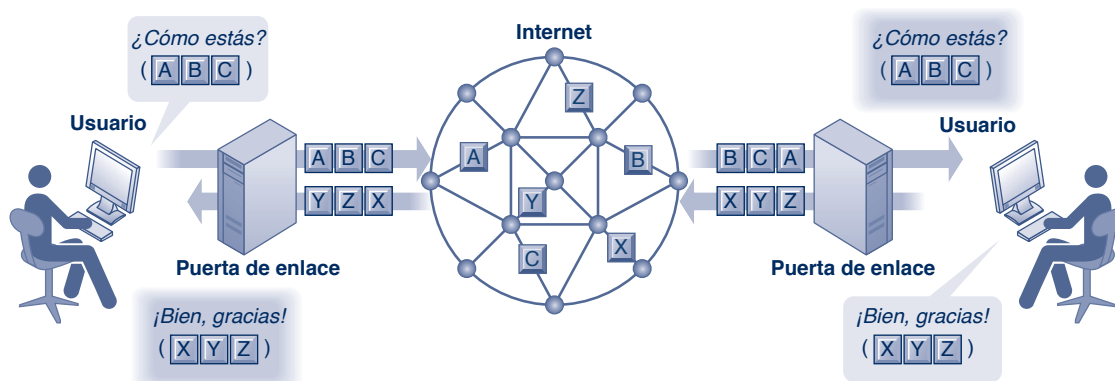
Aunque se requieren inversiones iniciales para un sistema de telefonía IP, la tecnología VoIP puede reducir los costos de comunicación y administración de la red de un 20 a 30 por ciento. Por ejemplo, VoIP ahorra a Virgin Entertainment Group \$700 000 al año en las facturas de larga distancia. Además de reducir los costos de larga distancia y de eliminar las cuotas mensuales para líneas privadas, una red IP provee una sola infraestructura de voz-datos tanto para los servicios de telecomunicaciones como de cómputo. Las compañías ya no tienen que mantener redes separadas ni proveer servicios de soporte y personal para cada tipo distinto de red.

Otra ventaja de VoIP es la flexibilidad. A diferencia de la red telefónica tradicional, se pueden agregar teléfonos o cambiarlos a distintas oficinas sin tener que volver a cablear o configurar la red. Con VoIP, se puede establecer una llamada de conferencia con una operación simple de arrastrar y colocar en la pantalla de computadora para seleccionar los nombres de los participantes. El correo de voz y el correo electrónico se pueden combinar en un solo directorio.

## Comunicaciones unificadas

En el pasado, cada una de las redes de la empresa para datos fijos e inalámbricos, comunicaciones de voz y videoconferencias operaban de manera independiente unas de otras y el departamento de sistemas de información tenía que administrarlas por separado. Sin embargo, en la actualidad las firmas pueden mezclar los distintos modos de comunicación en un solo servicio accesible de manera universal, mediante el uso de la tecnología de las comunicaciones. Las **comunicaciones unificadas** integran canales dispares para comunicaciones de voz, comunicaciones de datos, mensajería instantánea, correo electrónico y conferencias electrónicas en una sola experiencia, en donde los usuarios pueden alternar entre los distintos modos de comunicación sin ningún problema. La tecnología de presencia muestra si una persona está disponible para recibir una llamada. Las compañías tendrán que examinar cómo se alterarán los

**FIGURA 7-11** CÓMO FUNCIONA LA VOZ SOBRE IP



Una llamada de telefonía de VoIP digitaliza y descompone un mensaje de voz en paquetes de datos que pueden viajar a lo largo de distintas rutas antes de volver a ensamblarlos en el destino final. Un procesador más cercano al destino de la llamada, conocido como puerta de enlace, acomoda los paquetes en el orden apropiado y los dirige al número telefónico del receptor o la dirección IP de la computadora receptora.



## SESIÓN INTERACTIVA: ADMINISTRACIÓN

### MONITOREO DE LOS EMPLEADOS EN LAS REDES: ¿FALTA DE ÉTICA O BUENOS NEGOCIOS?

Al estar en su trabajo, ¿cuántos minutos (u horas) pasó en Facebook hoy? ¿Envío correo electrónico personal o visitó algunos sitios Web de deportes? Si es así, no está usted solo. De acuerdo con un estudio de Nucleus Research, el 77 por ciento de los trabajadores con cuentas de Facebook las utilizan durante horas de trabajo. Un estudio de IDC Research muestra que hasta un 40 por ciento de las actividades de navegación en Internet que ocurre durante horas de trabajo es personal, mientras que otros informan que hasta un 90 por ciento de los empleados reciben o envían correo electrónico personal en su trabajo.

Este comportamiento crea graves problemas de negocios. Al revisar el correo electrónico, responder a los mensajes instantáneos y ver a hurtadillas un video breve de YouTube se crea una serie de interrupciones continuas que desvían la atención del empleado de las tareas laborales que se supone debe estar realizando. De acuerdo con Basex, una compañía de investigación de negocios de la ciudad de Nueva York, estas distracciones ocupan hasta 28 por ciento del día de un trabajador promedio en Estados Unidos y provocan la pérdida de \$650 mil millones en productividad cada año.

Muchas compañías han empezado a monitorear el uso que hacen sus empleados del correo electrónico, los blogs e Internet, algunas veces sin su conocimiento. Una reciente encuesta de la Asociación de Administración Estadounidense (AMA) de 340 compañías en Estados Unidos de todos los tamaños encontró que el 66 por ciento de estas compañías monitorean los mensajes de correo electrónico de los empleados y las conexiones Web. Aunque las compañías estadounidenses tienen el derecho legal de monitorear la actividad de Internet y del correo electrónico de los empleados mientras éstos trabajan, ¿acaso es este monitoreo falta de ética o tan sólo son buenos negocios?

Los gerentes se preocupan por la pérdida de tiempo y la productividad de los empleados cuando éstos se enfocan en asuntos personales en vez de asuntos de la compañía. Si pasan demasiado tiempo con sus asuntos personales, ya sea en Internet o no, esto puede significar ingresos perdidos. Algunos empleados pueden incluso estar cobrando a sus clientes por el tiempo que invierten en sus intereses personales en línea, lo que significa que les están cobrando en exceso.

Si el tráfico personal en las redes de computadoras es demasiado alto, también puede obstruir la red de la compañía e impedir que se realice el trabajo legítimo de ésta. Schemmer Associates, una firma de arquitectura en Omaha, Nebraska y el Hospital Potomac en Wooridge, Virginia, descubrieron que los recursos de cómputo se limitaban debido a la carencia de ancho de banda puesto que los empleados utilizaban las

conexiones corporativas a Internet para ver y descargar archivos de video.

Cuando los empleados utilizan el correo electrónico o navegan por Web (hasta en las redes sociales) en las instalaciones de su empleador o con su equipo, cualquier cosa que hagan, incluso algo ilegal, lleva el nombre de la compañía. Por lo tanto, se puede rastrear y responsabilizar al empleador. Los directivos en muchas firmas temen que el material relacionado con actos racistas, que contenga sexo explícito u otro tipo de material potencialmente ofensivo al que accedan sus empleados, o con el que éstos comercien, pueda resultar en publicidad adversa e incluso en demandas legales para la firma. Aun si la compañía no resulta responsable, el hecho de responder a las demandas podría costarle decenas de miles de dólares.

Las compañías también temen a la fuga de información confidencial y de secretos comerciales a través del correo electrónico o los blogs. Una encuesta reciente realizada por la Asociación de Administración Estadounidense y el instituto ePolicy descubrió que el 14 por ciento de los empleados encuestados admitieron que habían enviado correos electrónicos de la compañía confidenciales o potencialmente embarazosos a personas externas.

Las compañías en Estados Unidos tienen el derecho legal de monitorear qué están haciendo los empleados con el equipo de la compañía durante horas de trabajo. La pregunta es si la vigilancia electrónica constituye o no una herramienta apropiada para mantener un lugar de trabajo eficiente y positivo. Algunas firmas tratan de prohibir todas las actividades comerciales en las redes corporativas: cero tolerancia. Otras bloquean el acceso a los empleados a sitios Web o sitios sociales específicos, o limitan el tiempo personal en Web.

Por ejemplo, la empresa Enterprise Rent-A-Car bloquea el acceso a los empleados a ciertos sitios sociales y monitorea la actividad en Web relacionada con las publicaciones en línea de los empleados sobre la compañía. Ajax Boiler en Santa Ana, California, usa software de SpectorSoft Corporation que registra todos los sitios Web que visitan los empleados, el tiempo invertido en cada sitio y todos los correos electrónicos enviados. Flushing Financial Corporation instaló software que evita que los empleados envíen correo electrónico a direcciones específicas y explora los adjuntos de correo electrónico en busca de información confidencial. Schemmer Associates usa OpenDNS para clasificar y filtrar el contenido Web además de bloquear el video no deseado.

Algunas firmas han despedido empleados que han sobrepasado los límites. Un tercio de las compañías encuestadas en el estudio de la AMA había despedido

trabajadores por hacer un mal uso de Internet en el trabajo. De los gerentes que despidieron empleados por mal utilizar Internet, el 64 por ciento lo hizo debido a que el correo electrónico de los empleados contenía lenguaje inapropiado u ofensivo, y más del 25 por ciento despidió a los trabajadores por un uso personal excesivo del correo electrónico.

Ninguna solución es libre de problemas, pero muchos consultores creen que las compañías deberían escribir políticas corporativas sobre el uso del correo electrónico y de Internet para los empleados. Las políticas deberían incluir directrices explícitas que declaren, por posición o nivel, bajo qué circunstancias pueden los empleados usar las instalaciones de la compañía para el correo electrónico, los blogs o la navegación Web. Las políticas también deberían informar a los empleados si estas actividades están monitoreadas y explicarles por qué.

Ahora IBM cuenta con "lineamientos de cómputo social" que cubren la actividad de los empleados en sitios tales como Facebook y Twitter. Los lineamientos insinúan a los empleados a no revelar sus identidades, a recordar que son personalmente responsables por lo

que publican y a abstenerse de debatir sobre temas controversiales que no estén relacionados con la función que desempeñan en IBM.

Las reglas se deben personalizar a las necesidades específicas de cada empresa y a las culturas organizacionales. Por ejemplo, aunque algunas compañías pueden excluir a todos los empleados de visitar sitios que tengan material sexual explícito, tal vez los empleados de firmas legales u hospitales requieran acceso a esos sitios. Las firmas de inversiones necesitarán permitir a muchos de sus empleados el acceso a otros sitios de inversiones. Una compañía que dependa de la comparación extendida de información, de la innovación y la independencia podría llegar a descubrir que el monitoreo crea más problemas de los que resuelve.

**Fuentes:** Joan Goodchild, "Not Safe for Work: What's Acceptable for Office Computer Use", *CIO Australia*, 17 de junio de 2010; Sarah E. Needleman, "Monitoring the Monitors", *The Wall Street Journal*, 16 de agosto de 2010; Michelle Conline y Douglas MacMillan, "Web 2.0: Managing Corporate Reputations", *Business Week*, 20 de mayo de 2009; James Wong, "Drafting Trouble-Free Social Media Policies", *Law.com*, 15 de junio de 2009, y Maggie Jackson, "May We Have Your Attention, Please?", *Business Week*, 23 de junio de 2008.

## PREGUNTAS DEL CASO DE ESTUDIO

## MIS EN ACCIÓN

1. ¿Deberían los gerentes monitorear la forma en que los empleados usan el correo electrónico e Internet? ¿Por qué sí o por qué no?
2. Describa una política de uso efectivo del correo electrónico y de Web para una compañía.
3. ¿Deben los gerentes informar a los empleados que se está monitoreando su comportamiento Web? ¿O deberían monitorearlos en secreto? ¿Por qué sí o por qué no?

Explore el sitio Web del software para monitorear empleados en línea tal como Websense, Barracuda Networks, MessageLabs o SpectorSoft, y responda a las siguientes preguntas:

1. ¿Qué actividades de los empleados rastrea este software? ¿Qué puede aprender un empleador sobre un empleado al usar este software?
2. ¿Cómo se pueden beneficiar las empresas al usar este software?
3. ¿Cómo se sentiría si su empleador usara este software en donde labora para monitorear lo que usted hace en el trabajo? Explique su respuesta.

flujos de trabajo y los procesos de negocios debido a esta tecnología para poder medir su valor.

CenterPoint Properties, una de las principales compañías de bienes raíces industriales del área de Chicago, usó la tecnología de comunicaciones unificadas en la creación de sitios Web colaborativos para cada uno de sus tratos de bienes raíces. Cada sitio Web provee un solo punto para acceder a los datos estructurados y no estructurados. La tecnología de presencia integrada permite a los miembros de un equipo usar el correo electrónico, la mensajería instantánea, realizar llamadas o videoconferencias con un solo clic.

### Redes privadas virtuales

¿Qué pasaría si tuviera un grupo de marketing encargado de desarrollar nuevos productos y servicios para su firma con miembros esparcidos en todo el territorio de Estados Unidos? Sería conveniente que pudieran enviar y recibir correo electrónico entre sí y comunicarse con la oficina central sin ninguna probabilidad de que personas

externas pudieran interceptar las comunicaciones. En el pasado, una respuesta a este problema era trabajar con las grandes firmas de redes privadas que ofrecían redes seguras, privadas y dedicadas a los clientes. Sin embargo, ésta era una solución costosa, una mucho más económica es crear una red privada virtual dentro de la red Internet pública.

Una **red privada virtual (VPN)** es una red privada segura y cifrada que se ha configurado dentro de una red pública para aprovechar la economía de escala y las facilidades administrativas de las grandes redes, como Internet (vea la figura 7-12). Una VPN ofrece a su firma comunicaciones seguras y cifradas a un costo mucho menor que las mismas capacidades que ofrecen los proveedores tradicionales que no son de Internet, y que utilizan sus redes privadas para las comunicaciones seguras. Las VPN también proporcionan una infraestructura de red para combinar redes de voz y de datos.

Se utilizan varios protocolos competidores para proteger los datos que se transmiten a través de la red Internet pública, como el *Protocolo de Tunnelización Punto a Punto (PPTP)*. En un proceso conocido como *tunnelización*, los paquetes de datos se cifran y envuelven dentro de paquetes IP. Al agregar esta envoltura alrededor de un mensaje de red para ocultar su contenido, las firmas de negocios crean una conexión privada que viaja a través de la red Internet pública.

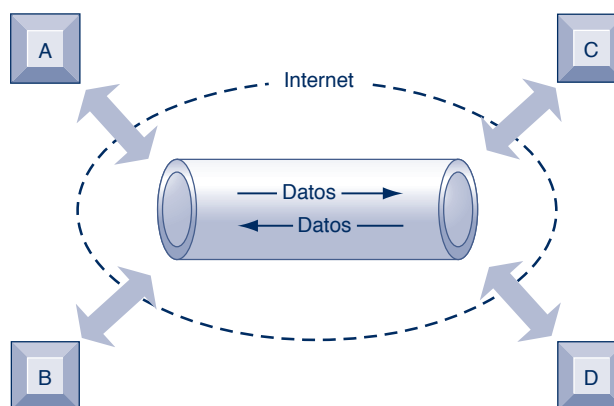
## WEB

Es probable que haya utilizado el servicio Web para descargar música, buscar información para un trabajo final o para obtener noticias y reportes del clima. Web es el servicio más popular de Internet. Es un sistema con estándares aceptados de manera universal para almacenar, recuperar, dar formato y mostrar información mediante el uso de una arquitectura cliente/servidor. Para dar formato a las páginas Web se utiliza el hipertexto con vínculos incrustados que conectan documentos entre sí, y que también vinculan páginas hacia otros objetos, como archivos de sonido, video o animación. Cuando usted hace clic en un gráfico y se reproduce un video, significa que ha hecho clic en un **hipervínculo**. Un **sitio Web** típico es una colección de páginas Web vinculadas a una página de inicio.

## Hipertexto

Las páginas Web se basan en un Lenguaje de Marcado de Hipertexto (HTML) estándar, el cual da formato a los documentos e incorpora vínculos dinámicos a otros documentos

**FIGURA 7-12 UNA RED PRIVADA VIRTUAL MEDIANTE EL USO DE INTERNET**



La VPN es una red privada de computadoras vinculadas mediante una conexión de "túnel" segura a través de Internet. Protege los datos que se transmiten a través de la red Internet pública al codificarlos y "envolverlos" dentro del Protocolo de Internet (IP). Al agregar una envoltura alrededor de un mensaje de red para ocultar su contenido, las organizaciones pueden crear una conexión privada que viaja a través de la red Internet pública.

e imágenes almacenadas en la misma computadora o en equipos remotos (vea el capítulo 5). Se puede acceder a las páginas Web por medio de Internet debido a que el software de navegador Web que opera en su computadora puede solicitar las páginas almacenadas en un servidor host de Internet mediante el **protocolo de transferencia de hipertexto (HTTP)**. HTTP es el estándar de comunicaciones que se utiliza para transferir páginas en Web. Por ejemplo, cuando usted escribe una dirección Web en su navegador, como `www.sec.gov`, su navegador envía una solicitud HTTP al servidor `sec.gov`, en la cual solicita la página inicial de `sec.gov`.

HTTP es el primer conjunto de letras al inicio de cada dirección Web, seguido del nombre de dominio que especifica la computadora servidor de la organización que almacena el documento. La mayoría de las compañías tienen un nombre de dominio que es igual o se relaciona mucho con su nombre corporativo oficial. La ruta de directorio y el nombre del documento son dos piezas más de información dentro de la dirección Web, que ayudan al navegador a rastrear la página solicitada. En conjunto, a la dirección se le conoce como **localizador uniforme de recursos (URL)**. Al escribirlo en un navegador, un URL indica al software navegador con exactitud en dónde debe buscar la información. Por ejemplo, en el URL `http://www.megacorp.com/contenido/caracteristicas/082610.html`, `http` nombra al protocolo que se utiliza para mostrar las páginas Web. `www.megacorp.com` es el nombre de dominio, `contenido/caracteristicas` es la ruta de directorio que identifica en qué parte del servidor Web del dominio está almacenada la página, y `082610.html` es tanto el nombre del documento como el del formato en el que se encuentra (es una página HTML).

## Servidores Web

Un servidor Web consiste en software para localizar y administrar páginas Web almacenadas. Localiza las páginas Web solicitadas por un usuario en la computadora en donde están almacenadas y las envía a la computadora del usuario. Por lo general, las aplicaciones de servidor se ejecutan en computadoras dedicadas, aunque en organizaciones pequeñas todas pueden residir en una sola computadora.

El servidor Web más común que se utiliza en la actualidad es el servidor Apache HTTP, que controla el 54 por ciento del mercado. Apache es un producto de código fuente abierto sin costo que se puede descargar de Internet. Microsoft Internet Information Services es el segundo servidor Web más utilizado, con 25 por ciento de participación en el mercado.

## Búsqueda de información en Web

Nadie sabe con certeza cuántas páginas Web hay en realidad. La Web superficial es la parte de Web que visitan los motores de búsqueda y sobre la cual se registra información. Por ejemplo, Google visitó cerca de 100 mil millones de páginas en 2010, y esto refleja una extensa porción de la población de páginas Web de acceso público. No obstante, hay una “Web profunda” que contiene una cantidad estimada de 900 mil millones de páginas adicionales, muchas de las cuales son propietarias (como las páginas de *The Wall Street Journal Online*, que no se pueden visitar sin un código de acceso) o que se almacenan en bases de datos corporativas protegidas.

**Motores de búsqueda** Sin duda, con tantas páginas Web el hecho de encontrar páginas específicas que nos puedan ayudar con nuestros asuntos, casi al instante, es un problema importante. La pregunta es, ¿cómo podemos encontrar esas pocas páginas que deseamos y necesitamos en realidad, entre los miles de millones de páginas Web indexadas? Los **motores de búsqueda** tratan de resolver el problema de encontrar información útil en Web casi al instante y, en definitiva, son la “aplicación asesina” de la era de Internet. Los motores de búsqueda actuales pueden filtrar archivos HTML, archivos de aplicaciones de Microsoft Office y archivos PDF, además de archivos de audio, video e imágenes. Hay cientos de motores de búsqueda distintos en el mundo, pero la gran mayoría de los resul-



tados de búsqueda se suministran a través de los tres principales proveedores: Google, Yahoo! y el motor de búsqueda Bing de Microsoft.

Los motores de búsqueda Web empezaron a principios de la década de 1990 como programas de software bastante simples que deambulaban por la Web naciente, visitando páginas y recopilando información sobre el contenido de cada página. Los primeros motores de búsqueda eran simples indexaciones de palabras clave de todas las páginas que visitaban, y dejaban al usuario listas de páginas que tal vez no eran en verdad relevantes para su búsqueda.

En 1994, los estudiantes David Filo y Jerry Yang de ciencias computacionales de la Universidad de Stanford crearon una lista seleccionada a mano de sus páginas Web favoritas y la llamaron “Otro oficioso oráculo jerárquico (Yet Another Hierarchical Official Oracle)”, o Yahoo!. En un principio no era un motor de búsqueda, sino más bien una selección editada de sitios Web organizados por categorías que los editores encontraban de utilidad, pero a partir de entonces desarrolló sus propias capacidades de motor de búsqueda.

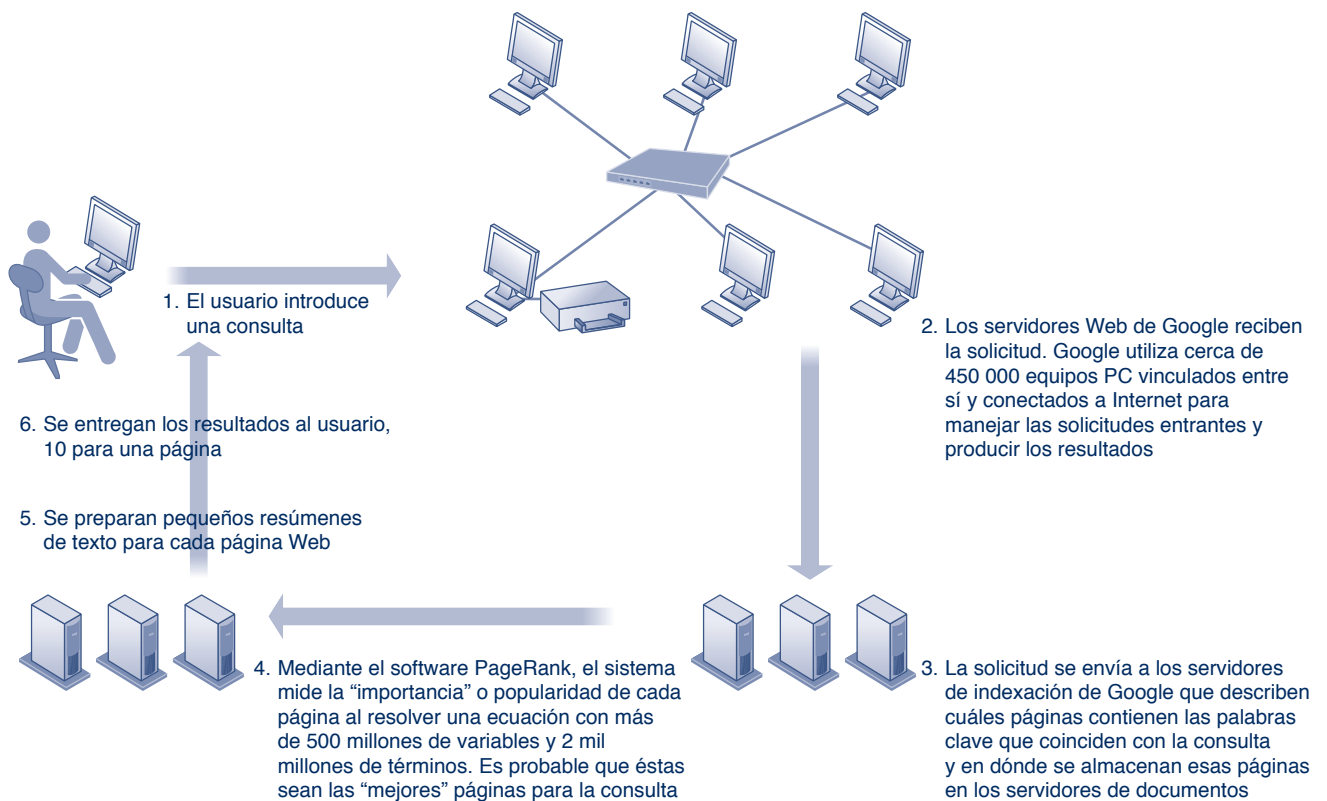
En 1998, Larry Page y Sergey Brin, otros dos estudiantes de ciencias computacionales en Stanford, liberaron su primera versión de Google. Este motor de búsqueda era distinto. No sólo indexaba las palabras de cada página Web, sino que también clasificaba los resultados de las búsquedas con base en la relevancia de cada página. Page patentó la idea de un sistema de clasificación de páginas (PageRank System), el cual en esencia mide la popularidad de una página Web al calcular el número de sitios que tienen vínculos hacia esa página, así como el número de vínculos que tiene a otras páginas. Brin contribuyó con un programa Web crawler único que indexaba no sólo las palabras clave en una página, sino también combinaciones de palabras (como los autores y los títulos de sus artículos). Estas dos ideas se convirtieron en la base del motor de búsqueda Google. La figura 7-13 ilustra cómo funciona Google.

Los sitios Web de motores de búsqueda son tan populares que muchas personas los utilizan como su página de inicio, la página en donde empiezan a navegar por Web (vea el capítulo 10). A pesar de su utilidad, nadie esperaba que los motores de búsqueda fueran grandes productores de dinero. Sin embargo, en la actualidad son la base para la forma de marketing y publicidad que crece con más rapidez, el marketing de motores de búsqueda.

Los motores de búsqueda se han convertido en importantes herramientas de compras al ofrecer lo que se conoce ahora como **marketing de motores de búsqueda**. Cuando los usuarios introducen un término de búsqueda en Google, Bing, Yahoo! o cualquiera de los otros sitios a los que dan servicio estos motores de búsqueda, reciben dos tipos de listados: vínculos patrocinados, en donde los anunciantes pagan por aparecer en el listado (por lo general en la parte superior de la página de resultados de búsqueda) y resultados de búsqueda “orgánicos” sin patrocinio. Además, los anunciantes pueden comprar pequeños cuadros de texto al lado de las páginas de resultados de búsqueda. Los anuncios patrocinados pagados son la forma con más rápido crecimiento de publicidad en Internet, además de que son nuevas y poderosas herramientas que relacionan con precisión los intereses de los consumidores con los mensajes de publicidad en el momento oportuno. El marketing de motores de búsqueda monetiza el valor del proceso de búsqueda. En 2010, el marketing de motores de búsqueda generó \$12.3 mil millones en ingresos, la mitad de toda la publicidad en línea (\$25.6 mil millones). El 97 por ciento de los ingresos anuales de Google de \$23.6 mil millones proviene del marketing de motores de búsqueda (eMarketer, 2010).

Puesto que el marketing de motores de búsqueda es tan efectivo, las compañías están empezando a optimizar sus sitios Web para que los motores de búsqueda puedan reconocerlos. Entre mejor optimizada esté la página, mayor clasificación obtendrá en los listados de resultados. La **optimización de motores de búsqueda (SEO)** es el proceso de mejorar la calidad y el volumen del tráfico Web hacia un sitio Web, para lo cual se emplea una serie de técnicas que ayudan a un sitio Web a obtener una mayor clasificación con los principales motores de búsqueda cuando se colocan ciertas palabras y frases clave en el campo de búsqueda. Una técnica es la de asegurarse que las palabras clave utilizadas en la descripción del sitio Web coincidan con las más probables que el cliente en potencia utilice como términos de búsqueda. Por ejemplo, es más factible que su sitio Web se encuentre entre los primeros lugares de los motores de búsqueda si

FIGURA 7-13 CÓMO TRABAJA GOOGLE



El motor de búsqueda de Google consulta el servicio Web en forma continua, indexa el contenido de cada página, calcula su popularidad y almacena las páginas de modo que pueda responder con rapidez a las solicitudes de un usuario para ver una página. Todo el proceso tarda cerca de medio segundo.

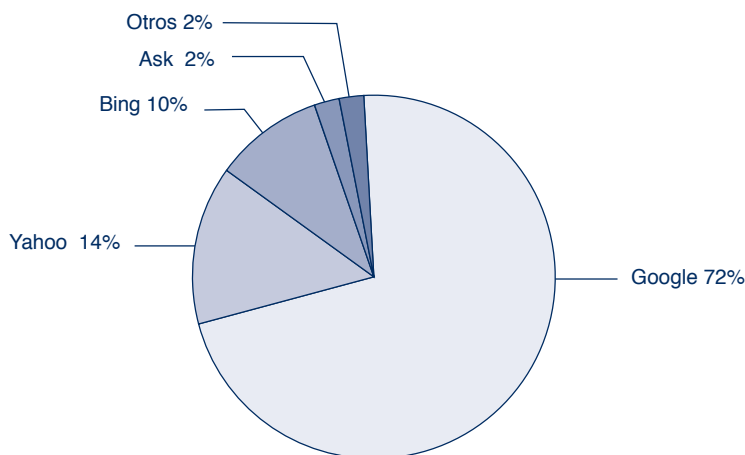
utiliza la palabra clave "iluminación" en vez de "lámparas", si la mayoría de los clientes potenciales están buscando "iluminación". También es conveniente vincular su sitio Web a todos los otros sitios que sea posible, ya que los motores de búsqueda evalúan dichos vínculos para determinar la popularidad de una página Web y la forma en que está vinculada al resto del contenido en Web. La suposición es que entre más vínculos haya para un sitio Web, más útil debe ser éste.

En 2010, cerca de 110 millones de personas en Estados Unidos utilizaron a diario un motor de búsqueda, con lo cual se produjeron más de 17 mil millones de búsquedas al mes. Hay cientos de motores de búsqueda, pero los tres principales (Google, Yahoo! y Bing) representan cerca del 90 por ciento de todas las búsquedas (vea la figura 7-14).

Aunque en un principio los motores de búsqueda se crearon para buscar documentos de texto, la explosión en cuanto al uso del video y las imágenes en línea ha generado una demanda de motores de búsqueda que puedan encontrar videos específicos con rapidez. Las palabras "baile", "amor", "música" y "chica" son muy populares en los títulos de videos de YouTube, por lo que al buscar con base en estas palabras clave se produce una avalancha de respuestas aun y cuando el contenido actual del video tal vez no tenga nada que ver con el término de la búsqueda. Es un desafío buscar videos debido a que las computadoras no son muy buenas o rápidas para reconocer imágenes digitales. Algunos motores de búsqueda han empezado a indexar guiones de películas, por lo que será posible buscar una película con base en el diálogo. Blinkx.com es un servicio popular de búsqueda de video y Google ha agregado herramientas de búsqueda de video.

**Bots de compras de agentes inteligentes** El capítulo 11 describe las herramientas de los agentes de software con inteligencia integrada, que pueden recopilar o filtrar información y realizar otras tareas para ayudar a los usuarios. Los **bots de com-**



**FIGURA 7-14 PRINCIPALES MOTORES DE BÚSQUEDA WEB DE ESTADOS UNIDOS**

Google es el motor de búsqueda más popular en Web, ya que maneja el 72 por ciento de todas las búsquedas Web.

Fuentes: Basado en datos de SeoConsultants.com, 28 de agosto de 2010.

**pras** usan software de agente inteligente para buscar en Internet la información sobre compras. Los bots de compras tales como MySimon o Google Product Search pueden ayudar a las personas interesadas en hacer una compra a filtrar y recuperar información sobre los productos de interés, evaluar los productos competidores de acuerdo con los criterios establecidos por los usuarios y negociar con los vendedores en cuanto al precio y los términos de entrega. Muchos de estos agentes de compras buscan en Web los precios y la disponibilidad de los productos especificados por el usuario y devuelven una lista de sitios que venden el artículo, junto con la información de los precios y un vínculo de compra.

## Web 2.0

Los sitios Web en la actualidad no sólo tienen contenido estático; también permiten a las personas colaborar y compartir información, además de crear nuevos servicios y contenido en línea. Estos servicios interactivos basados en Internet de segunda generación se conocen como **Web 2.0**. Si usted tiene fotos compartidas a través de Internet en Flickr u otro sitio de fotografías, si publicó un video en YouTube, creó un blog, usó Wikipedia o agregó un widget a su página de Facebook, ha utilizado algunos de estos servicios Web 2.0.

Web 2.0 tiene cuatro características distintivas: interactividad, control del usuario en tiempo real, participación social (compartición) y contenido generado por el usuario. Las tecnologías y servicios detrás de estas características incluyen la computación en la nube, los mashups y widgets de software, blogs, RSS, wikis y redes sociales.

Los mashups y widgets, que introdujimos en el capítulo 5, son servicios de software que permiten a los usuarios y desarrolladores de sistemas mezclar y asociar contenido o componentes de software para crear algo nuevo en su totalidad. Por ejemplo, el sitio para almacenar y compartir fotos Flickr de Yahoo combina fotografías con otra información sobre las imágenes que proveen los usuarios, además de las herramientas para que se pueda utilizar dentro de otros entornos de programación.

Estas aplicaciones de software se ejecutan en Web en vez de hacerlo en el escritorio. Con Web 2.0, el servicio Web no es sólo una colección de sitios de destino, sino un origen de datos y servicios que se pueden combinar para crear las aplicaciones que necesitan los usuarios. Las herramientas y servicios Web 2.0 han impulsado la creación de redes sociales y otras comunidades en línea, en donde las personas pueden interactuar entre sí según lo deseen.

Un **blog**, el término popular para un Weblog, es un sitio Web personal que por lo general contiene una serie de entradas cronológicas (de la más reciente a la más antigua) de su autor, además de vínculos a páginas Web relacionadas. El blog puede contener un *blogroll* (una colección de vínculos a otros blogs) y *trackbacks* (una lista de entradas en otros blogs que hacen referencia a un mensaje publicado en el primer blog). La mayoría de los blogs también permiten a los usuarios publicar comentarios en sus entradas. Por lo común, al acto de crear un blog se le conoce como “bloguear”. Los blogs pueden estar alojados en un sitio de terceros como Blogger.com, LiveJournal.com, TypePad.com y Xanga.com, o los blogueros potenciales pueden descargar software tal como Movable Type para crear un blog alojado en el ISP del usuario.

Las páginas de los blogs son por lo general variaciones de plantillas proporcionadas por el servicio o software de blogueo. Por lo tanto, millones de personas sin habilidades de HTML de ningún tipo pueden publicar sus propias páginas Web y compartir contenido con los demás. A la totalidad de los sitios Web relacionados con blogs se le conoce por lo común como **blogósfera**. Aunque los blogs se han convertido en herramientas de publicación personal populares, también tienen usos comerciales (vea los capítulos 9 y 10).

Si usted es un ávido lector de blogs, podría usar el servicio RSS para mantenerse actualizado con sus blogs favoritos sin tener que estar revisándolos de manera constante en búsqueda de actualizaciones. **RSS**, que significa resumen de sitios complejos o sindicación realmente simple, syndica el contenido de un sitio Web de modo que se pueda utilizar en otro entorno. La tecnología RSS extrae el contenido especificado de los sitios Web y lo transmite de manera automática a las computadoras de los usuarios, en donde se puede almacenar para que lo vean después.

Para recibir una transmisión de información RSS, necesita instalar software agregador o lector de noticias, el cual se puede descargar de Web (la mayoría de los navegadores Web actuales cuentan con herramientas para leer RSS). Como alternativa, puede establecer una cuenta con un sitio Web agregador. Usted indica al agregador que recolecte todas las actualizaciones de una página Web específica, o lista de páginas, o que recopile información sobre un tema dado mediante la realización de búsquedas Web a intervalos regulares. Una vez suscrito, usted recibe de manera automática nuevo contenido según se vaya publicando en el sitio Web especificado.

Varias empresas utilizan RSS de manera interna para distribuir información corporativa actualizada. Wells Fargo utiliza RSS para transmitir noticias que los empleados pueden personalizar para ver las noticias empresariales de mayor relevancia para sus empleos. Las transmisiones RSS son tan populares que las editoriales en línea están desarrollando formas de presentar publicidad junto con el contenido.

Los blogs permiten a los visitantes agregar comentarios al contenido original, pero no les permiten modificar el material original publicado. En contraste, los **wikis** son sitios Web colaborativos en donde los visitantes pueden agregar, eliminar o modificar contenido en el sitio, incluso las obras de autores anteriores. Wiki proviene de la palabra “rápido” en hawaiano.

Por lo general, el software de wiki cuenta con una plantilla que define la distribución y los elementos comunes para todas las páginas, muestra el código del programa editable por el usuario y después despliega el contenido en una página basada en HTML para que se muestre en un navegador Web. Cierta software de wiki sólo permite un formato básico del texto, mientras que otras herramientas permiten el uso de tablas, imágenes o incluso elementos interactivos, como encuestas o juegos. La mayoría de los wikis proveen herramientas para monitorear el trabajo de otros usuarios y corregir errores.

Como los wikis facilitan de manera considerable la compartición de la información, tienen muchos usos comerciales. Por ejemplo, los representantes de ventas de Motorola usan wikis para compartir la información de ventas. En vez de desarrollar una charla promocional para cada cliente, los representantes reutilizan la información publicada en el wiki. El Centro Nacional de Ciberseguridad del Departamento de Seguridad Nacional de Estados Unidos implementó un wiki para facilitar la colaboración entre las agencias federales sobre ciberseguridad. El NCSC y las otras agencias utilizan el wiki para compartir información en tiempo real sobre amenazas, ataques y respuestas, y también como depósito para la información técnica y de estándares.

Los sitios de **redes sociales** permiten a los usuarios crear comunidades de amigos y colegas profesionales. Por lo general, cada miembro crea un “perfil”, una página Web para publicar fotos, videos, archivos MP3 y texto, y después comparten estos perfiles con otros en el servicio que se identifican como sus “amigos” o contactos. Los sitios de redes sociales son muy interactivos, ofrecen al usuario un control en tiempo real, dependen del contenido generado por los usuarios y se basan en términos generales en la participación social y la compartición tanto de contenido como de opiniones. Los sitios de redes sociales más importantes son Facebook, MySpace (con 500 millones y 180 millones de miembros globales respectivamente en 2010), y LinkedIn (para los contactos profesionales).

Para muchos, los sitios de redes sociales son la aplicación que define a Web 2.0, además de que cambiarán de manera radical la forma en que las personas invierten su tiempo en línea; en la que se comunican y con quiénes lo hacen; cómo permanecen los hombres y mujeres de negocios en contacto con sus clientes, proveedores y empleados; cómo aprenden los proveedores de bienes y servicios sobre sus clientes, y cómo pueden llegar los anunciantes a los clientes potenciales. Los grandes sitios de redes sociales también se están convirtiendo en plataformas de desarrollo de aplicaciones en donde los miembros puedan crear y vender aplicaciones de software para otros miembros de la comunidad. Tan sólo Facebook tuvo más de 1 millón de desarrolladores que crearon cerca de 550 000 aplicaciones para juegos, compartir videos y comunicarse con amigos y familiares. En los capítulos 2 y 10 hablamos más sobre las aplicaciones de negocios de las redes sociales; además podrá encontrar discusiones sobre redes sociales en muchos otros capítulos del texto. También encontrará un análisis más detallado sobre Web 2.0 en nuestras Trayectorias de aprendizaje.

### **Web 3.0: el servicio Web del futuro**

Todos los días, casi 110 millones de estadounidenses introducen 500 millones de consultas en motores de búsqueda. ¿Cuántas consultas de entre estos 500 millones producen un resultado significativo (una respuesta útil en los primeros tres listados)? Sin duda, menos de la mitad. Google, Yahoo, Microsoft y Amazon están tratando de incrementar las probabilidades de que las personas encuentren respuestas significativas a las consultas en los motores de búsqueda. Sin embargo, con cerca de 100 mil millones de páginas Web indexadas, los medios disponibles para encontrar la información que de verdad se necesita son bastante primitivos, puesto que se basan en las palabras que se utilizan en las páginas y la popularidad relativa de la página entre las personas que utilizan esos mismos términos de búsqueda. En otras palabras, es al azar.

En mayor grado, el futuro de Web involucra a las técnicas de desarrollo para que las búsquedas en los 100 mil millones de páginas Web públicas sean más productivas y significativas para las personas ordinarias. Web 1.0 resolvió el problema de obtener acceso a la información. Web 2.0 resolvió el problema de compartir esa información con otros, y de crear nuevas experiencias Web. **Web 3.0** es la promesa de una Web futura en donde toda esta información digital y todos estos contactos se puedan entrelazar para formar una sola experiencia significativa.

Algunas veces a ésta se le conoce como **Web semántica**. La palabra “semántica” se refiere al significado. La mayoría del contenido de Web en la actualidad está diseñado para que los humanos lo lean y las computadoras lo desplieguen, no para que los programas de computadora lo analicen y manipulen. Los motores de búsqueda pueden descubrir cuándo aparece un término o palabra clave específico en un documento Web, pero en realidad no entienden su significado ni cómo se relaciona con el resto de la información en Web. Para comprobar esto, puede introducir dos búsquedas en Google. Primero escriba “Paris Hilton”. Después escriba “Hilton en París”. Como Google no entiende el inglés o español ordinario, no tiene idea de que en la segunda búsqueda a usted le interesa el Hotel Hilton en París. Como no puede comprender el significado de las páginas que ha indexado, el motor de búsqueda de Google devuelve las páginas más populares para las consultas en donde aparecen las palabras “Hilton” y “Paris” en las páginas.

La Web semántica, se describió por primera vez en un artículo de la revista *Scientific American* de 2001, ésta es un esfuerzo de colaboración encabezado por el Consorcio World Wide Web para agregar un nivel de significado encima del servicio Web existente para reducir la cantidad de participación humana en la búsqueda y el procesamiento de la información Web (Berners-Lee y colaboradores, 2001).

Las opiniones en cuanto al futuro del servicio Web varían, pero en general se enfocan en las formas para aumentar la “inteligencia” Web, en donde la comprensión de la información facilitada por las máquinas promueve una experiencia más intuitiva y efectiva para el usuario. Por ejemplo, digamos que desea preparar una fiesta con sus amigos del tenis en un restaurante local, el viernes en la noche después del trabajo. Pero hay un problema: usted había programado antes ir al cine con otro amigo. En un entorno de Web semántica 3.0, usted podría coordinar este cambio en los planes con los itinerarios de sus amigos tenistas y el itinerario de su amigo del cine para hacer una reservación en el restaurante, todo con un solo conjunto de comandos emitidos en forma de texto o voz en su teléfono inteligente. Justo ahora, esta capacidad está más allá de nuestro alcance.

La labor de hacer del servicio Web una experiencia más inteligente avanza con lentitud, en gran parte debido a que es difícil hacer que las máquinas, o hasta los programas de software, sean tan inteligentes como los humanos. Aunque hay otras opiniones sobre el servicio Web en el futuro. Algunos ven una Web en 3-D, en donde se puedan recorrer las páginas en un entorno tridimensional. Otros señalan la idea de un servicio Web dominante que controle todo desde las luces en su sala de estar hasta el espejo retrovisor de su auto, sin mencionar que administre su calendario y sus citas.

Otras tendencias complementarias que conducen hacia un servicio Web 3.0 en el futuro incluyen un uso más extenso de la computación en la nube y los modelos de negocios SaaS, la conectividad ubicua entre las plataformas móviles y los dispositivos de acceso a Internet, y el proceso de transformar el servicio Web de una red de contenido y aplicaciones separadas en un silo, a un conjunto más uniforme e interoperable. Es más probable que estas visiones más modestas del servicio Web 3.0 futuro se cumplan en un plazo cercano.

## 7.4 LA REVOLUCIÓN INALÁMBRICA

Si tiene un teléfono celular, ¿lo utiliza para tomar y enviar fotografías, enviar mensajes de texto o descargar clips de música? ¿Lleva su laptop a clases o a la librería para conectarse a Internet? Si es así, forma parte de la revolución inalámbrica. Los teléfonos celulares, las computadoras laptop y los pequeños dispositivos de bolsillo se han transformado en plataformas de cómputo portátiles que le permiten realizar algunas de las tareas de computación que solía realizar en su escritorio.

La comunicación inalámbrica ayuda a las empresas a permanecer con más facilidad en contacto con los clientes, proveedores y empleados, además de que provee arreglos más flexibles para organizar el trabajo. La tecnología inalámbrica también ha creado nuevos productos, servicios y canales de ventas, lo cual analizaremos en el capítulo 10.

Si requiere comunicación móvil y poder de cómputo o acceso remoto a sistemas corporativos, puede trabajar con una variedad de dispositivos inalámbricos, como teléfonos celulares, **teléfonos inteligentes (smartphones)** y computadoras personales con conexión inalámbrica. En nuestros análisis de la plataforma digital móvil en los capítulos 1 y 5 presentamos los teléfonos inteligentes. Además de transmitir voz, incluyen herramientas para correo electrónico, mensajería, acceso inalámbrico a Internet, fotografía digital y administración de la información personal. Las herramientas de los dispositivos iPhone y BlackBerry ilustran el grado al cual han evolucionado los teléfonos celulares para convertirse en pequeñas computadoras móviles.

## SISTEMAS CELULARES

El servicio celular digital utiliza varios estándares competidores. En Europa y en gran parte del resto del mundo fuera de Estados Unidos, el estándar es el sistema global de comunicaciones móviles (GSM). La fortaleza de GSM es la capacidad de roaming internacional. Hay sistemas de telefonía celular GSM en Estados Unidos, entre los que están T-Mobile y AT&T Wireless.

El principal estándar en Estados Unidos es el acceso múltiple por división de código (CDMA), sistema que utilizan Verizon y Sprint. El ejército desarrolló el CDMA durante la Segunda Guerra Mundial. Se transmite a través de varias frecuencias, ocupa el espectro completo y asigna de manera aleatoria usuarios a un rango de frecuencias a través del tiempo.

Las primeras generaciones de los sistemas celulares se diseñaron en primera instancia para la transmisión de voz y de datos limitados en forma de mensajes cortos. Ahora las compañías de comunicaciones inalámbricas ofrecen redes celulares más poderosas conocidas como redes de tercera generación o **redes 3G**, con velocidades de transmisión que varían desde los 144 Kbps para los usuarios móviles, por ejemplo en un auto, hasta 2 Mbps para los usuarios fijos. Esta capacidad de transmisión es suficiente para video, gráficos y otros medios complejos, además de la voz, con lo cual las redes 3G son adecuadas para el acceso a Internet de banda ancha. Muchos de los teléfonos celulares disponibles en la actualidad tienen capacidad de 3G.

Las redes celulares de alta velocidad se utilizan mucho en Japón, Corea del Sur, Taiwán, Hong Kong, Singapur y partes de la Europa moderna. En lugares en Estados Unidos sin cobertura 3G, las compañías de comunicaciones celulares han actualizado sus redes para soportar la transmisión a mayor velocidad, de modo que los teléfonos celulares se puedan utilizar para acceder a Web, descargar música y otros servicios de banda ancha. Las PC equipadas con una tarjeta especial pueden usar estos servicios celulares de banda ancha para el acceso inalámbrico a Internet en cualquier momento y en donde sea.

La siguiente evolución en la comunicación inalámbrica, conocida como **redes 4G**, se basa por completo en la conmutación de paquetes y es capaz de alcanzar una velocidad de transmisión de 100 Mbps (que puede llegar a 1 Gbps bajo condiciones óptimas), con una calidad de primera y mucha seguridad. Los servicios de voz, datos y video de flujo continuo de alta calidad estarán disponibles para los usuarios en cualquier parte y a cualquier hora. Las tecnologías actuales previas a 4G son la evolución a largo plazo (LTE) y WiMax móvil (en la siguiente sección analizaremos la tecnología WiMax). En las Trayectorias de aprendizaje de este capítulo encontrará más información sobre las generaciones celulares.

## REDES INALÁMBRICAS DE COMPUTADORAS Y ACCESO A INTERNET

Si tiene una computadora laptop, podría utilizarla para acceder a Internet al cambiarse de un cuarto a otro en su dormitorio, o de una mesa a otra en la biblioteca de su universidad. Una variedad de tecnologías proveen acceso inalámbrico de alta velocidad a Internet para las PC y otros dispositivos portátiles inalámbricos, así como para los teléfonos celulares. Estos nuevos servicios de alta velocidad tienen acceso extendido a Internet en muchas ubicaciones que no se podrían cubrir mediante los servicios tradicionales fijos de Internet.

### Bluetooth

**Bluetooth** es el nombre popular para el estándar de redes inalámbricas 802.15, que es útil para crear pequeñas **redes de área personal (PAN)**. Vincula hasta ocho dispositivos dentro de un área de 10 metros mediante el uso de comunicación basada en radio de baja energía, y puede transmitir hasta 722 Kbps en la banda de 2.4 GHz.

Los teléfonos celulares, localizadores, computadoras, impresoras y dispositivos de cómputo que utilizan Bluetooth se comunican entre sí, e incluso unos operan a otros sin necesidad de intervención directa por parte del usuario (vea la figura 7-15). Por ejemplo, una persona podría controlar una computadora notebook para enviar un archivo de documentos por vía inalámbrica a una impresora. Bluetooth conecta teclados y ratones inalámbricos a equipos PC, o teléfonos celulares a sus auriculares sin necesidad de cables. Bluetooth tiene requerimientos de baja energía, lo cual es apropiado para las computadoras portátiles operadas por batería, los teléfonos celulares o los PDA.

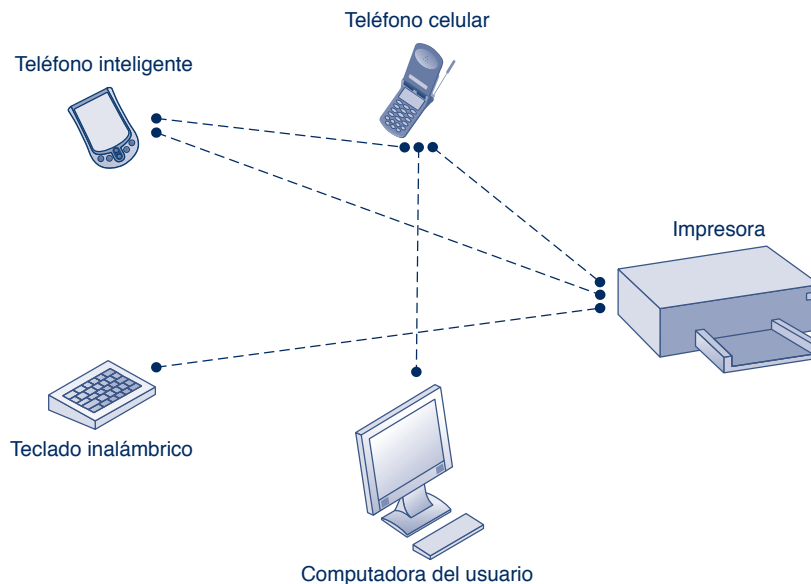
Aunque Bluetooth se presta en sí a las redes personales, también se puede usar en grandes corporaciones. Por ejemplo, los conductores de FedEx usan Bluetooth para transmitir los datos de entrega que capturan mediante sus computadoras PowerPad portátiles a los transmisores celulares, que reenvían los datos a las computadoras corporativas. Los conductores ya no necesitan invertir tiempo para acoplar sus unidades portátiles físicamente a los transmisores, por lo que Bluetooth ha ahorrado a FedEx \$20 millones al año.

### Wi-Fi y acceso inalámbrico a Internet

El conjunto de estándares 802.11 para redes LAN inalámbricas y acceso inalámbrico a Internet también se conoce como **Wi-Fi**. El primero de estos estándares que se adoptó con popularidad fue 802.11b, que puede transmitir hasta 11 Mbps en la banda de 2.4 GHz sin necesidad de licencia y tiene una distancia efectiva de 30 a 50 metros. El estándar 802.11g puede transmitir hasta 54 Mbps en el rango de 2.4 GHz. El estándar 802.11n es capaz de transmitir a cerca de 100 Mbps. Las computadoras PC y netbook de la actualidad tienen soporte integrado para Wi-Fi, al igual que los dispositivos iPhone, iPad y otros teléfonos inteligentes.

En casi todas las comunicaciones Wi-Fi, los dispositivos inalámbricos se comunican con una LAN fija mediante el uso de puntos de acceso. Un punto de acceso es una caja que consiste en un receptor/transmisor de radio y antenas con vínculos a una red fija, un enrutador o un concentrador (hub). Los puntos de acceso móviles como MiFi de Virgin Mobile usan la red celular existente para crear conexiones Wi-Fi.

**FIGURA 7-15 UNA RED BLUETOOTH (PAN)**



Bluetooth permite que una variedad de dispositivos, como teléfonos celulares, teléfonos inteligentes, teclados y ratones inalámbricos, equipos PC e impresoras, interactúen por vía inalámbrica entre sí dentro de una pequeña área de 30 pies (10 metros). Además de los vínculos mostrados, Bluetooth se puede utilizar para conectar en red dispositivos similares y enviar datos de una PC a otra, por ejemplo.



La figura 7-16 ilustra una LAN inalámbrica 802.11 que conecta un pequeño número de dispositivos móviles a una LAN fija más grande y a Internet. La mayoría de los dispositivos inalámbricos son máquinas cliente. Los servidores que las estaciones cliente móviles necesitan usar están en la LAN fija. El punto de acceso controla las estaciones inalámbricas y actúa como un puente entre la LAN fija principal y la LAN inalámbrica (un puente conecta dos LAN basadas en distintas tecnologías). El punto de acceso también controla las estaciones inalámbricas.

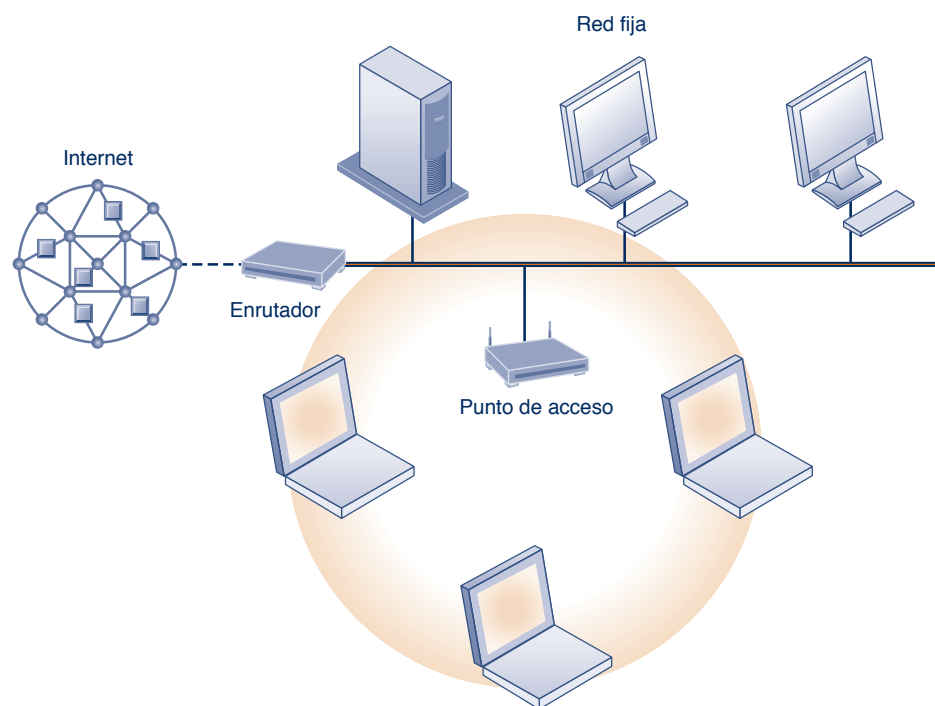
El uso más popular para Wi-Fi en la actualidad es para el servicio de Internet inalámbrico de alta velocidad. En esta instancia, el punto de acceso se enchufa en una conexión a Internet, la cual podría provenir de una línea de TV por cable o un servicio telefónico DSL. Las computadoras dentro del rango del punto de acceso lo utilizan para enlazarse de manera inalámbrica a Internet.

Por lo general, los **puntos activos** consisten en uno o más puntos de acceso que proveen acceso inalámbrico a Internet en un lugar público. Algunos puntos activos son gratuitos o no requieren software adicional para usarse; otros tal vez requieran activación y el establecimiento de una cuenta de usuario, para lo cual se proporciona un número de tarjeta de crédito a través de Web.

Las empresas de todos tamaños están usando redes Wi-Fi para proveer redes LAN inalámbricas de bajo costo y acceso a Internet. Los puntos activos Wi-Fi se pueden encontrar en hoteles, salas de aeropuertos, bibliotecas, cafés y campus universitarios para ofrecer acceso móvil a Internet. Dartmouth College es uno de muchos campus en donde los estudiantes ahora usan Wi-Fi para investigaciones, trabajos de los cursos y entretenimiento.

No obstante, la tecnología Wi-Fi impone varios desafíos. Uno de ellos corresponde a las características de seguridad de Wi-Fi, que hacen a estas redes inalámbricas vulnerables a los intrusos. En el capítulo 8 proveeremos más detalles sobre los aspectos de seguridad del estándar Wi-Fi.

**FIGURA 7-16 UNA LAN 802.11 INALÁMBRICA**



Las computadoras laptop móviles equipadas con tarjetas de interfaz de red se enlazan a la LAN fija al comunicarse con el punto de acceso. Este punto de acceso usa ondas de radio para transmitir las señales de la red fija a los adaptadores cliente, que convierten estas ondas de radio en datos que el dispositivo móvil pueda comprender. Después el adaptador cliente transmite los datos del dispositivo móvil de vuelta al punto de acceso, quien los reenvía a la red fija.

Otra desventaja de las redes Wi-Fi es la susceptibilidad a la interferencia de los sistemas cercanos que operan en el mismo espectro, como los teléfonos inalámbricos, los hornos de microondas u otras LAN inalámbricas. Sin embargo, las redes inalámbricas basadas en el estándar 802.11n son capaces de resolver este problema mediante el uso de varias antenas inalámbricas en conjunto para transmitir y recibir datos, y de una tecnología llamada *MIMO* (múltiple entrada múltiple salida) para coordinar las múltiples señales de radio simultáneas.

## WiMax

Una gran cantidad sorprendente de áreas en Estados Unidos y en todo el mundo no tienen acceso a Wi-Fi ni a la conectividad fija de banda ancha. El rango máximo de los sistemas Wi-Fi es de 300 pies desde la estación base, ya que es difícil para los grupos rurales que no tienen servicio de cable o DSL encontrar acceso inalámbrico a Internet.

El IEEE desarrolló una nueva familia de estándares conocida como WiMax para lidiar con estos problemas. **WiMax**, que significa interoperabilidad mundial para acceso por microondas, es el término popular para el estándar 802.16 del IEEE. Tiene un rango de acceso inalámbrico de hasta 31 millas y una velocidad de transmisión de hasta 75 Mbps.

Las antenas WiMax son lo bastante poderosas como para transmitir conexiones a Internet de alta velocidad a las antenas en los techos de los hogares y las empresas a millas de distancia. Los teléfonos celulares y las computadoras laptop con capacidad para WiMax están empezando a aparecer en el mercado. WiMax móvil es una de las tecnologías de red previas a 4G que vimos antes en este capítulo. Clearwire, que pertenece a Sprint-Nextel, utiliza la tecnología WiMax como base para las redes 4G que está implementando en el territorio de Estados Unidos.

## REDES DE SENSORES INALÁMBRICAS Y RFID

Las tecnologías móviles están creando nuevas eficiencias y formas de trabajar en toda la empresa. Además de los sistemas inalámbricos que acabamos de describir, los sistemas de identificación por radio frecuencia y las redes de sensores inalámbricas están teniendo un impacto importante.

### Identificación por radio frecuencia (RFID)

Los sistemas de **identificación por radio frecuencia (RFID)** ofrecen una tecnología poderosa para rastrear el movimiento de productos a través de la cadena de suministro. Los sistemas RFID usan diminutas etiquetas con microchips incrustados que contienen datos sobre un artículo y su ubicación para transmitir señales de radio a través de una distancia corta, a los lectores RFID. Después, los lectores RFID pasan los datos a través de una red a una computadora para su procesamiento. A diferencia de los códigos de barras, las etiquetas RFID no necesitan establecer contacto mediante una línea de visión para poder leerlas.

La etiqueta RFID se programa de manera electrónica con información que pueda identificar a un artículo en forma única, además de información adicional sobre el artículo, como su ubicación, en dónde y cuándo se fabricó, o su estado durante la producción. La etiqueta tiene incrustado un microchip para almacenar los datos. El resto de la etiqueta es una antena que transmite datos al lector.

La unidad lectora consiste en una antena y un transmisor de radio con una capacidad de decodificación, unidos a un dispositivo fijo o portátil. El lector emite ondas de radio en rangos que varían desde 1 pulgada hasta 100 pies, dependiendo de su salida de potencia, la frecuencia de radio empleada y las condiciones ambientales circundantes. Cuando una etiqueta RFID entra al rango del lector, se activa y empieza a enviar datos. El lector captura estos datos, los decodifica y los envía de vuelta a través de una red fija o inalámbrica a una computadora host para que los procese (vea la figura 7-17). Las etiquetas y las antenas RFID vienen en una variedad de formas y tamaños.

Las etiquetas RFID activas son operadas por una batería interna y por lo general permiten reescribir y modificar los datos. Las etiquetas activas pueden transmitir a través de cientos de pies, pero pueden llegar a costar varios dólares cada una. Los sistemas de caseta de cobro automatizados, tales como el sistema E-ZPass de Nueva York, utilizan etiquetas RFID activas.

Las etiquetas RFID pasivas no tienen su propia fuente de energía, por lo que obtienen su energía de operación a través de la energía de radiofrecuencia transmitida por el lector RFID. Son más pequeñas, más ligeras y menos costosas que las etiquetas activas, pero sólo tienen un rango de varios pies.

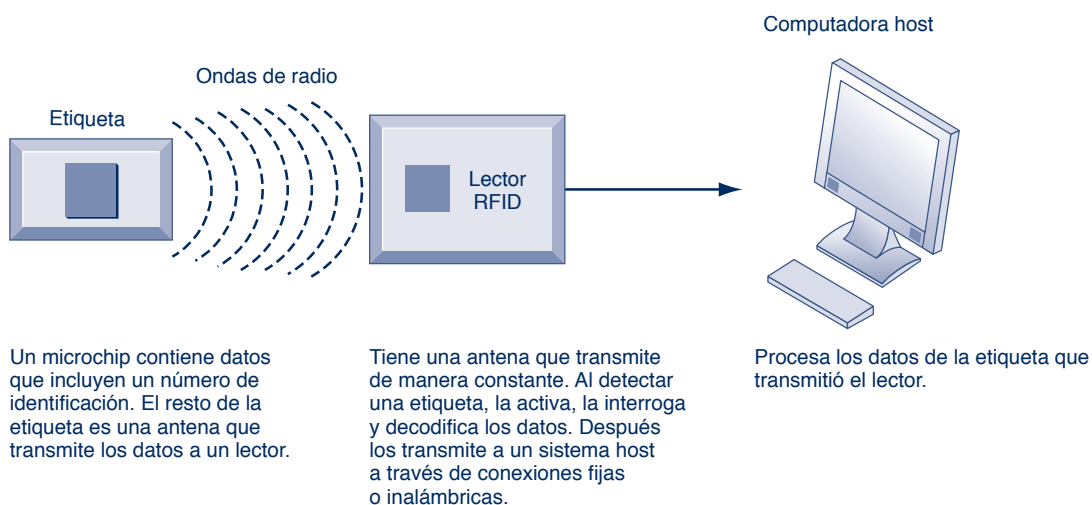
En el control de inventario y la administración de la cadena de suministro, los sistemas RFID capturan y administran información más detallada sobre los artículos en los almacenes o en producción que los sistemas de códigos de barras. Si se envía una gran cantidad de artículos en conjunto, los sistemas RFID rastrean cada palé, lote o incluso artículo unitario en el envío. Esta tecnología puede ayudar a las compañías como Walmart a mejorar las operaciones de recepción y almacenamiento, al mejorar su habilidad de “ver” con exactitud qué artículos están en existencia en los almacenes o en las repisas de las tiendas de menudeo.

Walmart ha instalado lectores RFID en los puertos de recepción de las tiendas para registrar la llegada de los palés y las cajas de productos que se envían con etiquetas RFID. El lector RFID lee las etiquetas una segunda vez, justo cuando las cajas se llevan al piso de ventas desde las áreas de almacenamiento de la bodega. El software combina los datos de ventas de los sistemas de punto de ventas de Walmart y los datos RFID relacionados con el número de cajas que se llevaron al piso de ventas. El programa determina qué artículos están a punto de agotarse y genera de manera automática una lista de artículos a recoger en el almacén para reabastecer los anaqueles de las tiendas antes de que se agoten. Esta información ayuda a Walmart a reducir los artículos sin existencias, a incrementar las ventas y a reducir aún más sus costos.

El costo de las etiquetas RFID solía ser demasiado alto como para usarlo de manera extendida, pero ahora es de menos de 10 centavos por etiqueta pasiva en Estados Unidos. A medida que el precio disminuye, la tecnología RFID está empezando a ser rentable para algunas aplicaciones.

Además de instalar lectores RFID y sistemas de etiquetado, las compañías tal vez necesiten actualizar su hardware y software para procesar las cantidades masivas de datos que producen los sistemas RFID: transacciones que podrían acumular decenas o cientos de terabytes de datos.

**FIGURA 7-17** CÓMO FUNCIONA LA TECNOLOGÍA RFID



RFID utiliza transmisores de radio que consumen poca energía para leer los datos almacenados en una etiqueta, a distancias que varían desde 1 pulgada hasta 100 pies. El lector captura los datos de la etiqueta y los envía a través de una red hacia una computadora host para que los procese.

Se utiliza cierto software para filtrar, agregar y evitar que los datos RFID sobrecarguen las redes empresariales y las aplicaciones de los sistemas. A menudo hay que rediseñar las aplicaciones para que acepten volúmenes más grandes de datos RFID generados de manera frecuente, y para compartir esos datos con otras aplicaciones. Los principales distribuidores de software empresarial, como SAP y Oracle-PeopleSoft, ofrecen ahora versiones listas para RFID de sus aplicaciones de administración de la cadena de suministro.

### Redes de sensores inalámbricas

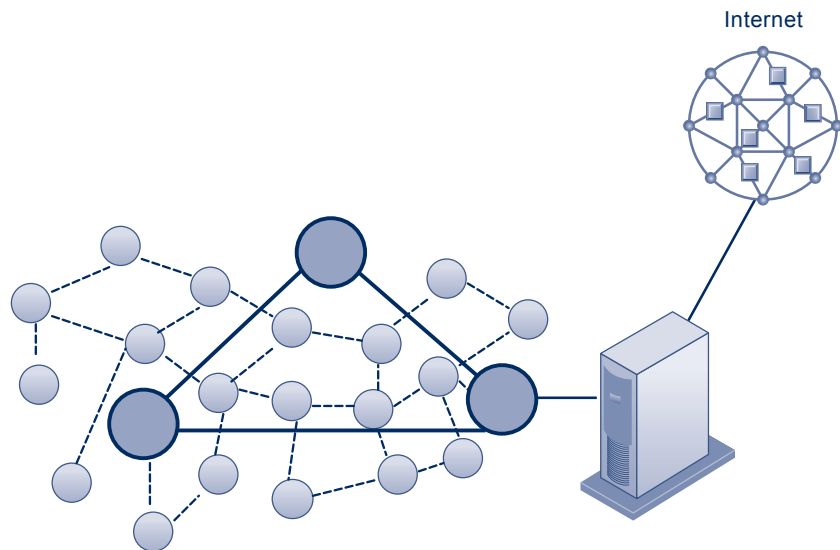
Si su compañía deseara tecnología de punta para monitorear la seguridad del edificio o detectar substancias peligrosas en el aire, podría implementar una red de sensores inalámbrica. Las **redes de sensores inalámbricas (WSN)** son redes de dispositivos inalámbricos interconectados, los cuales están incrustados en el entorno físico para proveer mediciones de muchos puntos a lo largo de espacios grandes. Estos dispositivos tienen integrados el procesamiento, el almacenamiento, los sensores de radiofrecuencia y las antenas. Están enlazados en una red interconectada que enruta los datos que capturan hacia una computadora para su análisis.

Estas redes pueden tener desde cientos hasta miles de nodos. Puesto que los dispositivos sensores inalámbricos se colocan en el campo durante años sin ningún tipo de mantenimiento ni intervención humana, deben tener requerimientos de muy poco consumo de energía y baterías capaces de durar años.

La figura 7-18 ilustra un tipo de red de sensores inalámbrica, con datos de los nodos individuales que fluyen a través de la red hacia un servidor con mayor poder de procesamiento. El servidor actúa como una puerta de enlace a una red basada en tecnología de Internet.

Las redes de sensores inalámbricas son valiosas en áreas como el monitoreo de los cambios ambientales, el monitoreo del tráfico o de la actividad militar, la protección de la propiedad, la operación y administración eficientes de maquinaria y vehículos, el establecimiento de perímetros de seguridad, el monitoreo de la administración de la cadena de suministro o la detección de material químico, biológico o radiológico.

**FIGURA 7-18 UNA RED DE SENSORES INALÁMBRICA**



Los círculos pequeños representan nodos de menor nivel y los círculos grandes representan nodos de alto nivel. Los nodos de menor nivel se reenvían datos entre sí o a nodos de mayor nivel, que transmiten los datos con más rapidez y agilizan el desempeño de la red.

## 7.5 PROYECTOS PRÁCTICOS SOBRE MIS

Los proyectos en esta sección le proporcionan experiencia práctica para evaluar y seleccionar la tecnología de comunicaciones, utilizar software de hojas de cálculo para mejorar la selección de los servicios de telecomunicaciones y utilizar los motores de búsqueda Web para la investigación de negocios.

### Problemas de decisión gerencial

1. Su compañía provee azulejos de piso cerámico para Home Depot, Lowe's y otras tiendas de mejoras para el hogar. A usted le han pedido que empiece a utilizar etiquetas de identificación por radiofrecuencia en cada caja de azulejos que envíe para ayudar a sus clientes a mejorar la administración de sus productos y los de otros proveedores en sus almacenes. Use el servicio Web para identificar el costo del hardware, software y los componentes de red de un sistema RFID adecuado para su compañía. ¿Qué factores hay que tener en cuenta? ¿Cuáles son las decisiones clave que se deben tomar para determinar si su empresa debe adoptar o no esta tecnología?
2. BestMed Medical Supplies Corporation vende productos médicos y quirúrgicos, además de equipo de más de 700 fabricantes distintos para hospitales, clínicas de salud y oficinas médicas. La compañía emplea 500 personas en siete ubicaciones distintas en estados de las regiones oeste y del medio oeste, como lo son gerentes de cuentas, representantes de servicio al cliente y soporte, y personal del almacén. Los empleados se comunican a través de los servicios tradicionales de telefonía de voz, de correo electrónico, mensajería instantánea y teléfonos celulares. La gerencia está preguntando si la compañía debería adoptar o no un sistema para unificar las comunicaciones. ¿Qué factores hay que tener en cuenta? ¿Cuáles son las decisiones clave que se deben tomar para determinar si hay que adoptar o no esta tecnología? Si es necesario, use el servicio Web para averiguar más sobre las comunicaciones unificadas y sus costos.

### Mejora de la toma de decisiones: uso del software de hojas de cálculo para evaluar los servicios inalámbricos

Habilidades de software: fórmulas de hojas de cálculo, aplicar formato

Habilidades de negocios: análisis de los servicios de telecomunicaciones y sus costos

En este proyecto usted utilizará el servicio Web para investigar sobre las alternativas de los servicios inalámbricos y utilizará software de hojas de cálculo para calcular los costos del servicio inalámbrico para una fuerza de ventas.

A usted le gustaría equipar su fuerza de ventas de 35 personas con base en Cincinnati, Ohio, con teléfonos móviles que tengan capacidades para transmitir voz, mensajería de texto, y para tomar y enviar fotografías. Use el servicio Web para seleccionar un proveedor de servicios inalámbricos que ofrezca servicio a nivel nacional, así como un buen servicio en el área cercana a su hogar. Examine las características de los teléfonos móviles que ofrece cada uno de estos distribuidores. Suponga que cada uno de los 35 vendedores tendrá que invertir tres horas al día durante el horario de oficina (8 a.m. a 6 p.m.) en comunicación móvil por voz, además de enviar 30 mensajes de texto al día y cinco fotos por semana. Utilice su software de hojas de cálculo para determinar el servicio inalámbrico y el teléfono que ofrezcan el mejor precio por usuario durante un periodo de dos años. Para los fines de este ejercicio no es necesario considerar los descuentos corporativos.

### Obtención de la excelencia operacional: uso de los motores de búsqueda Web para la investigación de negocios

Habilidades de software: herramientas de búsqueda Web

Habilidades de negocios: investigación de nuevas tecnologías

Este proyecto le ayudará a desarrollar sus habilidades de Internet para utilizar los motores de búsqueda Web en la investigación de negocios.

Desea saber más sobre el etanol como una alternativa de combustible para los vehículos de motor. Use los siguientes motores de búsqueda para obtener esa información: Yahoo!, Google y Bing. Si lo desea, pruebe también con otros motores de búsqueda. Compare el volumen y la calidad de la información que encuentra con cada herramienta de búsqueda. ¿Qué herramienta es más fácil de usar? ¿Cuál produjo los mejores resultados para su investigación? ¿Por qué?

## MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

---

Las siguientes Trayectorias de aprendizaje proveen contenido relevante a los temas que se cubrieron en este capítulo:

1. Servicio de cómputo y comunicaciones proporcionados por los distribuidores de comunicaciones comerciales
2. Servicios y tecnologías de red de banda ancha
3. Generaciones de sistemas celulares
4. WAP y I-Mode: estándares celulares inalámbricos para el acceso Web
5. Aplicaciones inalámbricas para administrar las relaciones con el cliente, la cadena de suministro y el servicio médico
6. Web 2.0



## Resumen de repaso

### 1. *¿Cuáles son los principales componentes de las redes de telecomunicaciones y las tecnologías de red clave?*

Una red simple consiste en dos o más computadoras conectadas. Los componentes básicos de red son las computadoras, las interfaces de red, un medio de conexión, el software de sistema operativo de red y un concentrador (hub) o un conmutador (switch). La infraestructura de red para una compañía grande abarca el sistema telefónico tradicional, la comunicación celular móvil, las redes de área local inalámbricas, los sistemas de videoconferencias, un sitio Web corporativo, intranets, extranets y una variedad de redes de área local y amplia, incluyendo Internet.

Se ha dado forma a las redes contemporáneas gracias al surgimiento de la computación cliente/servidor, el uso de la conmutación de paquetes y la adopción del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) como un estándar de comunicaciones universal para vincular redes y computadoras dispares, incluso Internet. Los protocolos proveen un conjunto común de reglas que permiten la comunicación entre los diversos componentes en una red de telecomunicaciones.

### 2. *¿Cuáles son los principales medios de transmisión de telecomunicaciones y los principales tipos de redes?*

Los principales medios físicos de transmisión son el cable telefónico de cobre trenzado, el cable de cobre coaxial, el cable de fibra óptica y la transmisión inalámbrica. El cable trenzado permite a las compañías usar el cableado existente de los sistemas telefónicos para la comunicación digital, aunque es relativamente lento. Los cables de fibra óptica y coaxial se utilizan para la transmisión de alto volumen, pero su instalación es costosa. Las microondas y los satélites de comunicaciones se utilizan para la comunicación inalámbrica a través de largas distancias.

Las redes de área local (LAN) conectan equipos PC y otros dispositivos digitales entre sí dentro de un radio de 500 metros, y en la actualidad se utilizan para muchas tareas de computación corporativas. Los componentes de red se pueden conectar entre sí mediante una topología de estrella, bus o anillo. Las redes de área amplia (WAN) abarcan distancias geográficas extensas, que varían desde unas cuantas millas hasta continentes enteros, y son redes privadas que se administran de manera independiente. Las redes de área metropolitana (MAN) abarcan una sola área urbana.

Las tecnologías de línea de suscriptor digital (DSL), las conexiones de Internet por cable y las líneas T1 se utilizan a menudo para conexiones de Internet de alta capacidad.

Las conexiones de Internet por cable proveen un acceso de alta velocidad a Web o a las intranets corporativas, a velocidades de hasta 10 Mbps. Una línea T1 soporta una tasa de transmisión de datos de 1.544 Mbps.

### 3. *¿Cómo funcionan Internet y la tecnología de Internet, y cómo dan soporte a la comunicación y el negocio electrónico?*

Internet es una red de redes a nivel mundial que utiliza el modelo de computación cliente/servidor y el modelo de referencia de red TCP/IP. A cada computadora en Internet se le asigna una dirección IP numérica única. El sistema de nombres de dominio (DNS) convierte las direcciones IP en nombres de dominio más amigables para los usuarios. Las políticas de Internet a nivel mundial se establecen a través de organizaciones y organismos gubernamentales, como el Consejo de Arquitectura de Internet (IAB) y el Consorcio World Wide Web (W3C).

Los principales servicios de Internet son el correo electrónico, los grupos de noticias, las salas de chat, la mensajería instantánea, Telnet, FTP y Web. Las páginas Web se basan en el lenguaje de marcado de hipertexto (HTML) y pueden mostrar texto, gráficos, video y audio. Los directorios de sitios Web, los motores de búsqueda y la tecnología RSS ayudan a los usuarios a localizar la información que necesitan en Web. RSS, los blogs, las redes sociales y los wikis son herramientas de Web 2.0.

Las firmas también están empezando a economizar mediante el uso de la tecnología VoIP para la transmisión de voz y mediante el uso de redes privadas virtuales (VPN) como alternativas de bajo costo para las redes WAN privadas.

### 4. *¿Cuáles son las principales tecnologías y estándares para redes inalámbricas, comunicación y acceso a Internet?*

Las redes celulares están evolucionando hacia una transmisión digital de conmutación de paquetes de alta velocidad con gran ancho de banda. Las redes 3G de banda ancha son capaces de transmitir datos a velocidades que varían desde 144 Kbps hasta más de 2 Mbps. Las redes 4G, capaces de obtener velocidades de transmisión de hasta 1 Gbps, se están empezando a extender.

Los principales estándares celulares son el acceso múltiple por división de código (CDMA), que se utiliza principalmente en Estados Unidos, y el sistema global de comunicaciones móviles (GSM), que viene siendo el estándar en Europa y en gran parte del resto del mundo.

Los estándares para las redes de computadoras inalámbricas son: Bluetooth (802.15) para las pequeñas redes de área personal (PAN), Wi-Fi (802.11) para las redes de área local (LAN) y WiMax (802.16) para las redes de área metropolitana (MAN).

5. *¿Por qué son valiosas las redes de sensores inalámbricas y de identificación por radiofrecuencia (RFID) para las empresas?*

Los sistemas de identificación por radiofrecuencia (RFID) proveen una poderosa tecnología para rastrear el movimiento de los productos mediante el uso de diminutas etiquetas con datos incrustados sobre un artículo y su ubicación. Los lectores RFID leen las señales de radio que transmiten estas etiquetas y pasan los datos a través de una red hacia una computadora para su procesamiento. Las redes de sensores inalámbricas (WSN) son redes de dispositivos inalámbricos de detección y transmisión interconectados, que se incrustan en el entorno físico para proveer medidas de muchos puntos a lo largo de grandes espacios.

## Términos clave

- Ancho de banda, 257
- Banda ancha, 247
- Blog, 273
- Blogósfera, 273
- Bluetooth, 276
- Bots de compras, 271
- Cable coaxial, 255
- Cable de fibra óptica, 255
- Cable trenzado, 255
- Comunicaciones unificadas, 265
- Conexiones de Internet por cable, 258
- Conmutación de paquetes, 250
- Correo electrónico, 263
- Chat, 264
- Dirección de Protocolo de Internet (IP), 258
- Enrutador, 248
- Hertz, 257
- Hubs, 248
- Identificación por radio frecuencia (RFID), 279
- Igual a igual, 254
- Internet2, 261
- Línea de suscriptor digital (DSL), 258
- Líneas T1, 258
- Localizador uniforme de recursos (URL), 269
- Marketing de motores de búsqueda, 270
- Mensajería instantánea, 264
- Microonda, 256
- Módem, 252
- Motores de búsqueda, 269
- Nombre de dominio, 258
- Optimización de motores de búsqueda (SEO), 270
- Protocolo, 251
- Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), 251
- Protocolo de transferencia de archivos (FTP), 261
- Protocolo de transferencia de hipertexto (HTTP), 269
- Proveedor de servicios de Internet (ISP), 257
- Puntos activos, 278
- Red de área local (LAN), 253
- Red de área metropolitana (MAN), 254
- Red privada virtual (VPN), 268
- Redes 3G, 276
- Redes 4G, 276
- Redes de área amplia (WAN), 254
- Redes de área personal (PAN), 276
- Redes de sensores inalámbricas (WSN), 281
- Redes sociales, 274
- RSS, 273
- Sistema de nombres de dominio (DNS), 258
- Sistema operativo de red (NOS), 248
- Sitio Web, 268
- Switch, 248
- Tarjeta de interfaz de red (NIC), 248
- Teléfono celular, 257
- Teléfonos inteligentes (smartphones), 276
- Telnet, 261
- Topología, 254
- Topología de anillo, 254
- Topología de bus, 254
- Topología de estrella, 254
- Voz sobre IP (VoIP), 264
- Web 2.0, 272
- Web 3.0, 274
- Web semántica, 274
- Wi-Fi, 277
- Wiki, 273
- WiMax, 279

## Preguntas de repaso

1. ¿Cuáles son los principales componentes de las redes de telecomunicaciones y las tecnologías de red clave?
  - Describa las características de una red simple y la infraestructura de red para una compañía grande.
  - Mencione y describa las principales tecnologías y tendencias que han dado forma a los sistemas de telecomunicaciones contemporáneos.
2. ¿Cuáles son los principales medios de transmisión de telecomunicaciones y los principales tipos de redes?
  - Mencione los distintos tipos de medios físicos de transmisión y compárelos en términos de velocidad y costo.
  - Defina una LAN y describa tanto sus componentes como las funciones de cada componente.
  - Mencione y describa las principales topologías de red.
3. ¿Cómo funcionan Internet y la tecnología de Internet, y cómo dan soporte a la comunicación y el negocio electrónico?
  - Defina Internet, describa cómo funciona y explique cómo provee un valor de negocios.
  - Explique cómo funcionan el sistema de nombres de dominio (DNS) y el sistema de direccionamiento IP.
- Liste y describa los principales servicios de Internet.
- Defina y describa la tecnología VoIP y las redes privadas virtuales; explique además cómo proveen valor para las empresas.
- Liste y describa las formas alternativas de localizar información en Web.
- Compare Web 2.0 y Web 3.0.
4. ¿Cuáles son las principales tecnologías y estándares para redes inalámbricas, comunicación y acceso a Internet?
  - Defina las redes Bluetooth, Wi-Fi, WiMax, 3G y 4G.
  - Describa las capacidades de cada una y para qué tipos de aplicaciones se adapta mejor.
5. ¿Por qué son valiosas las redes de sensores inalámbricas y de identificación por radio frecuencia (RFID) para las empresas?
  - Defina RFID, explique cómo funciona y describa cómo provee valor para las empresas.
  - Defina las redes WSN, explique cómo funcionan y describa los tipos de aplicaciones que las utilizan.

## Preguntas para debate

1. Se ha dicho que dentro de unos cuantos años, los teléfonos inteligentes se convertirán en el dispositivo digital individual más importante. Analice las implicaciones de esta declaración.
2. ¿Deben cambiar todas las principales compañías de ventas al menudeo y de manufactura a RFID? ¿Por qué sí o por qué no?
3. Compare la tecnología Wi-Fi y los sistemas celulares de alta velocidad para acceder a Internet. ¿Cuáles son las ventajas y desventajas de cada uno?

## Colaboración y trabajo en equipo: evaluación de teléfonos inteligentes

Forme un grupo con tres o cuatro de sus compañeros de clases. Compare las capacidades del iPhone de Apple con un teléfono inteligente de otro distribuidor que tenga características similares. Su análisis debe considerar el costo de compra de cada dispositivo, las redes inalámbricas en donde pueden operar, los costos de los planes de servicio y los teléfonos, y los servicios disponibles para cada dispositivo.

También debe considerar otras capacidades de cada dispositivo, como la habilidad de integrarse con las apli-

caciones corporativas o de PC existentes. ¿Qué dispositivo seleccionaría? ¿Qué criterios utilizaría para guiar su selección? Si es posible, use Google Sites para publicar vínculos a páginas Web, anuncios de comunicación en equipo y asignaturas de trabajo; para lluvias de ideas, y para trabajar de manera colaborativa en los documentos del proyecto. Intente usar Google Docs para desarrollar una presentación de sus hallazgos para la clase.

## La lucha de Google, Apple y Microsoft por acaparar la experiencia de usted en Internet

### CASO DE ESTUDIO

En lo que parece ser una pelea de comida estudiantil, los tres titanes de Internet (Google, Microsoft y Apple) se encuentran en una épica batalla por dominar la experiencia de usted, el usuario, en Internet. Lo que está en juego aquí es en dónde buscar, comprar, encontrar su música y videos, y qué dispositivo usará para hacer todo esto. El precio es un mercado de comercio electrónico proyectado de \$400 mil millones en 2015, en donde el principal dispositivo de acceso será un teléfono inteligente móvil o una computadora tipo tableta. Cada firma genera cantidades extraordinarias de efectivo con base en distintos modelos de negocios. Cada firma invierte miles de millones de dólares de efectivo de sobra en la pelea.

En esta pelea triangular, en un momento u otro, cada firma ha hecho amistad con una de las dos compañías sobrantes para combatir a la otra. Dos de ellas (Google y Apple) están determinadas en evitar que Microsoft expanda su dominio más allá de la PC de escritorio. Por lo tanto, Google y Apple son amigas, excepto cuando se trata de teléfonos móviles y apps, ya que cada una desea dominar el mercado de los dispositivos móviles. Tanto Apple como Microsoft tienen interés en impedir que Google se extienda más allá de su dominio en la búsqueda y la publicidad, lo cual, las hace amigas. No obstante, al tratarse del mercado móvil para dispositivos y apps, Apple y Microsoft son enemigas. Google y Microsoft son simples enemigas en una variedad de batallas. Google está tratando de debilitar el dominio de Microsoft sobre el software de PC, y Microsoft intenta entrar en el mercado de la publicidad en los motores de búsqueda con Bing.

En la actualidad, Internet (junto con los dispositivos de hardware y las aplicaciones de software) está pasando por una expansión importante. Los dispositivos móviles con funcionalidad avanzada y acceso ubicuo a Internet están ganando con rapidez a los equipos de cómputo de escritorio tradicionales en cuanto a ser la forma más popular de cómputo, con lo cual han cambiado las bases de competencia en toda la industria. La firma de investigación Gartner predice que para 2013, los teléfonos móviles sobrepasarán a los equipos PC como la forma en que la mayoría de las personas acceden a Internet. Hoy en día, los dispositivos móviles representan el 5 por ciento de todas las búsquedas que se realizan en Internet; en 2016 se espera que representen 23.5 por ciento de las búsquedas.

Estos dispositivos móviles de Internet son posibles gracias a una nube creciente de capacidad de cómputo disponible para cualquiera que tenga un teléfono inteligente y conectividad a Internet. ¿Quién necesita una PC cuando es posible escuchar música y ver videos 24/7 en uno de estos dispositivos móviles? Por ende, no es sorpresa que los titanes de la tecnología de hoy estén

peleando de una manera tan agresiva por el control de este valiente y nuevo mundo móvil.

Apple, Google y Microsoft ya están compitiendo de antemano en una variedad de campos. Google tiene una enorme ventaja en la publicidad, gracias a su dominio en la búsqueda por Internet. El servicio Bing alternativo ofrecido por Microsoft ha crecido para alcanzar cerca del 10 por ciento del mercado de los motores de búsqueda, y en esencia el resto pertenece a Google. Apple es líder en aplicaciones de software móviles gracias a la popularidad de la App Store para sus dispositivos iPhone. Google y Microsoft tienen ofrecimientos de apps menos populares en Web.

Microsoft sigue siendo líder en los sistemas operativos de PC y en el software de productividad de escritorio, pero ha fallado de manera miserable con el hardware y software de los teléfonos inteligentes, la computación móvil, las apps de software basadas en la nube, su portal de Internet e incluso sus máquinas y software para juegos. Todo esto contribuye en menos del 5 por ciento a los ingresos de Microsoft (el resto proviene de Windows, Office y el software de red). Aunque Windows sigue siendo el sistema operativo en el 95 por ciento de los 2 mil millones de equipos PC en el mundo, los sistemas operativos Android de Google e iOS de Apple son los participantes que dominan el mercado de la computación móvil. Estas compañías también compiten en la música, los navegadores de Internet, el video en línea y las redes sociales.

Tanto para Apple como para Google, el terreno de batalla más crítico es la computación móvil. Apple tiene varias ventajas que le servirán bien en la batalla por la supremacía móvil. No es coincidencia que desde el crecimiento explosivo de Internet en cuanto a tamaño y popularidad, también crecieron de igual forma los ingresos de la compañía, que sumaron un total de más de \$40 mil millones en 2009. Los dispositivos iMac, iPod e iPhone han contribuido en conjunto al enorme éxito de la compañía en la era de Internet, y ésta espera que el iPad siga la tendencia de rentabilidad establecida por estos productos. Apple cuenta con una base de usuarios leales que ha crecido de manera estable y es muy probable que compre los ofrecimientos de productos en el futuro. Apple espera que el iPad sea tan exitoso como el iPhone, que ya representa más del 30 por ciento de sus ingresos. Hasta ahora, el iPad parece estar a la altura de las expectativas.

Parte de la razón de la popularidad del iPhone de Apple, y del optimismo que rodea a los teléfonos equipados con Internet en general, ha sido el éxito de la App Store. Una vibrante selección de aplicaciones (apps) es lo que marca la diferencia entre los ofrecimientos de Apple y los de sus competidores, además de que le proporciona a la compañía una ventaja aprecia-

ble en este mercado. Apple ya ofrece cerca de 250 000 apps para sus dispositivos, y recibe 30 por ciento de todas las ventas de estas apps, que enriquecen de manera considerable la experiencia de usar un dispositivo móvil y, sin ellas, las predicciones del futuro de Internet móvil no serían tan brillantes. La compañía que cree el conjunto más atractivo de dispositivos y aplicaciones será la que obtenga una ventaja competitiva considerable sobre las compañías rivales. En estos momentos, esa compañía es Apple.

Sin embargo, el desarrollo de los teléfonos inteligentes e Internet móvil está aún en su infancia. Google ha actuado con rapidez para entrar en la batalla por la supremacía móvil mientras todavía puede 'ganar', pero en el proceso ha dañado de manera irreparable su relación con Apple, su antigua aliada. A medida que cada vez más personas cambian a la computación móvil como su método primario para acceder a Internet, Google sigue las miradas con agresividad. Esta compañía es tan fuerte como el tamaño de su red de publicidad. Con el inminente cambio hacia la computación móvil, no existe la certeza de que pueda mantener su posición dominante en los motores de búsqueda. Esta es la razón por la cual la compañía dominante de la búsqueda en línea empezó a desarrollar un sistema operativo móvil y su dispositivo Nexus One para participar en el mercado de los teléfonos inteligentes. Google espera controlar su propio destino en un mundo que cada vez se hace más móvil.

Los esfuerzos de Google por enfrentarse a Apple empezaron cuando adquirió Android, Inc., la compañía que desarrolló el sistema operativo móvil con el mismo nombre. La meta original de Google era contraatacar los intentos de Microsoft por entrar en el mercado de los dispositivos móviles, pero fracasó rotundamente. En su lugar, Apple y Research In Motion, fabricantes de la popular serie BlackBerry de teléfonos inteligentes, llenaron el vacío. Google continuó desarrollando Android y le agregó características que los ofrecimientos de Apple no tenían, como la habilidad de ejecutar varias apps a la vez. Después de una serie de prototipos poco atractivos en forma de bloque, ahora hay teléfonos equipados con Android que compiten en cuanto a funcionalidad y apariencia estética con el iPhone. Por ejemplo, el Motorola Droid recibió mucha publicidad, mediante el eslogan "Everything iDon't...Droid Does".

Google ha sido en especial agresiva con su entrada en el mercado de la computación móvil puesto que le preocupa la preferencia de Apple por los estándares propietarios 'cerrados' en sus teléfonos. A Google le gustaría que los teléfonos inteligentes tuvieran plataformas abiertas no propietarias en donde los usuarios pudieran vagar libremente por Web y obtener apps que funcionarían en muchos dispositivos distintos.

Apple tiene la creencia de que los dispositivos como los teléfonos inteligentes y las computadoras tipo tableta deben tener estándares propietarios y un control estricto, en donde los clientes usen aplicaciones en estos dispositivos que se hayan descargado de su App Store. Así, Apple tiene la última palabra acerca de si sus

usuarios móviles pueden acceder o no a los diversos servicios en Web, y eso abarca los servicios proporcionados por Google. Esta última no desea que Apple pueda bloquearla para evitar que provea sus servicios en los dispositivos iPhone o en cualquier otro teléfono inteligente. Un ejemplo notorio del deseo de Apple por eludir a Google ocurrió después de que esta última intentó colocar su programa de administración de correo de voz, Google Voice, en el iPhone. Apple citó problemas de privacidad para evadir el esfuerzo de Google.

Poco después, el CEO de Google Eric Schmidt dimitió de su puesto en el consejo de directores de Apple. Desde que Schmidt salió del consejo de Apple, las dos compañías se han enfrascado en una guerra declarada. Han estado peleando por adquisiciones destacadas, entre ellas la firma de publicidad móvil AdMob, sobre la cual estaban muy interesadas tanto Apple como Google. AdMob vende anuncios tipo pancarta que aparecen dentro de las aplicaciones móviles, y la compañía está a la vanguardia en cuanto al desarrollo de nuevos métodos de publicidad móvil. Apple estuvo cerca de cerrar un trato con la joven empresa cuando Google se adelantó y compró a AdMob por \$750 millones en acciones. Google no espera obtener ninguna cantidad similar en rendimiento gracias a este trato, pero estaba dispuesta a pagar una prima para interrumpir el esfuerzo de Apple por incursionar en el terreno de la publicidad móvil.

Sin inmutarse, Apple compró la principal empresa competidora Quattro Wireless por \$275 millones en enero de 2010. Después cerró el servicio en septiembre de ese año a favor de su propia plataforma de publicidad iAd. Esta plataforma permite que los desarrolladores de los programas en la tienda App Store de Apple para los dispositivos iPhone, iPad y iPod Touch incrusten anuncios en su software. Apple venderá los anuncios y dará a los desarrolladores de apps el 60 por ciento de los ingresos.

Apple ha estado más que dispuesta a utilizar tácticas de combate similares para entorpecer a la competencia. Por esta razón demandó a HTC, el fabricante taiwanés de teléfonos móviles equipados con Android, alegando una violación de patente. El CEO de Apple Steve Jobs ha atacado de manera consistente a Google en la prensa, en donde ha caracterizado a la compañía como bravucona y cuestiona sus éticas. Muchos analistas especulan que Apple tal vez intente vencer a Google al formar equipo con un socio que hubiera sido impensable hace unos cuantos años: Microsoft. Los nuevos informes sugieren que Apple está considerando llegar a un acuerdo con Microsoft para hacer de Bing su motor de búsqueda predeterminado, tanto en el iPhone como en el navegador Web de Apple. Esto sería un golpe para Google y una bendición para Microsoft, que recibiría el impulso tan necesario para su reciente servicio de búsqueda.

La lucha entre Apple y Google no importaría mucho si no hubiera tanto dinero potencial en juego. Miles de millones de dólares están colgando en el aire, y la mayor parte de ese dinero provendrá de la publicidad. Las ventas de apps son otro componente importante, en



especial para Apple. Esta compañía tiene la ventaja en cuanto a selección y calidad de las apps, pero aunque las ventas han sido ágiles, los desarrolladores se han quejado de que es muy difícil ganar dinero. Una cuarta parte de las 250 000 apps disponibles a principios de 2010 eran gratuitas, con lo cual no hay ganancias para los desarrolladores ni para Apple, pero lo cierto es que atraen consumidores al mercado de Apple, en donde se les pueden vender otras apps o servicios de entretenimiento.

Mientras tanto, Google se mueve con agresividad para apoyar a los fabricantes de teléfonos que ejecuten su sistema operativo Android y puedan acceder a sus servicios en línea. Apple depende de las ventas de sus dispositivos para mantener su rentabilidad. No ha tenido problemas con esto hasta ahora, pero Google sólo necesita esparcir sus redes de publicidad hacia estos dispositivos para obtener una ganancia. De hecho, algunos analistas especulan que Google prevé un futuro en el que los teléfonos móviles cuesten una fracción de lo que valen en la actualidad, o que incluso sean gratuitos, y que sólo se requieran los ingresos por publicidad generados por los dispositivos para obtener ganancias. Apple lucharía por permanecer competitiva en este entorno. Jobs ha mantenido cerrado el jardín de Apple por una simple razón: se necesita un dispositivo Apple para jugar ahí.

La lucha entre Microsoft, Apple y Google en realidad no tiene precedentes en la historia de las plataformas de cómputo. En ocasiones anteriores era por lo general una sola firma la que montaba la cima de una nueva tecnología para convertirse en el participante dominante. Como ejemplo tenemos el dominio de IBM sobre el mercado de las mainframes, el dominio de Digital Equipment sobre las minicomputadoras, el dominio de Microsoft sobre los sistemas operativos de PC y las aplicaciones de productividad, y el dominio de Cisco Systems sobre el mercado de enrutadores de Internet. En la lucha actual hay tres firmas que tratan de dominar la experiencia del cliente en Internet. Cada firma

aporta ciertas fortalezas y debilidades a la refriega. ¿Acaso “ganará” una sola firma, o sobrevivirán las tres a la lucha por la experiencia del consumidor en Internet? Es demasiado pronto para saber.

**Fuentes:** Jennifer LeClaire, “Quattro Wireless to be Closed as Apple Focuses on iAd”, *Top Tech News*, 20 de agosto de 2010; Yukari Iwatani Kane y Emily Steel, “Apple Fights Rival Google on New Turf”, *The Wall Street Journal*, 8 de abril de 2010; Brad Stone y Miguel Helft, “Apple’s Spat with Google is Getting Personal”, *The New York Times*, 12 de marzo de 2010; Peter Burrows, “Apple vs. Google”, *BusinessWeek*, 14 de enero de 2010; Holman W. Jenkins, Jr., “The Microsofting of Apple?”, *The Wall Street Journal*, 10 de febrero de 2010; Jessica E. Vascellaro y Ethan Smith, “Google and Microsoft Crank Up Rivalry”, *The Wall Street Journal*, 21 de octubre de 2009; Jessica E. Vascellaro y Don Clark, “Google Targets Microsoft’s Turf”, *The Wall Street Journal*, 9 de julio de 2009; Miguel Helft, “Google Set to Acquire AdMob for \$750 Million”, *The New York Times*, 10 de noviembre de 2009; Jessica E. Vascellaro, “Google Rolls Out New Tools as it Battles Rival”, *The Wall Street Journal*, 8 de diciembre de 2009, y Jessica E. Vascellaro y Yukari Iwatani Kane, “Apple, Google Rivalry Heats Up”, *The Wall Street Journal*, 10 de diciembre de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

1. Compare los modelos de negocios y las áreas de fortaleza de Apple, Google y Microsoft.
2. ¿Por qué es tan importante la computación móvil para estas tres firmas? Evalúe los ofrecimientos de cada firma en cuanto a la plataforma móvil.
3. ¿Cuál es la importancia de las aplicaciones y las tiendas de apps para el éxito o el fracaso de la computación móvil?
4. ¿Qué compañía y modelo de negocios cree usted que se impondrá en esta épica lucha? Explique su respuesta.
5. ¿Qué diferencia tendría para usted como gerente o consumidor individual el hecho de que Apple, Google o Microsoft dominaran la experiencia en Internet? Explique su respuesta.



# Capítulo 8

## Seguridad en los sistemas de información

### OBJETIVOS DE APRENDIZAJE

*Después de leer este capítulo, usted podrá responder a las siguientes preguntas:*

1. ¿Por qué son vulnerables los sistemas de información a la destrucción, el error y el abuso?
2. ¿Cuál es el valor de negocios de la seguridad y el control?
3. ¿Cuáles son los componentes de un marco de trabajo organizacional para la seguridad y el control?
4. ¿Cuáles son las herramientas y tecnologías más importantes para salvaguardar los recursos de información?

#### *Sesiones interactivas:*

Cuando el software antivirus inutiliza a sus computadoras  
¿Qué tan segura es la nube?

### RESUMEN DEL CAPÍTULO

- 8.1 VULNERABILIDAD Y ABUSO DE LOS SISTEMAS**  
Por qué son vulnerables los sistemas  
Software malicioso: virus, gusanos, caballos de Troya y spyware  
Los hackers y los delitos computacionales  
Amenazas internas: los empleados  
Vulnerabilidad del software
- 8.2 VALOR DE NEGOCIOS DE LA SEGURIDAD Y EL CONTROL**  
Requerimientos legales y regulatorios para la administración de registros digitales  
Evidencia electrónica y análisis forense de sistemas
- 8.3 ESTABLECIMIENTO DE UN MARCO DE TRABAJO PARA LA SEGURIDAD Y EL CONTROL**  
Controles de los sistemas de información  
Evaluación del riesgo  
Política de seguridad  
Planificación de recuperación de desastres y planificación de la continuidad de negocios  
La función de la auditoría
- 8.4 TECNOLOGÍAS Y HERRAMIENTAS PARA PROTEGER LOS RECURSOS DE INFORMACIÓN**  
Administración de la identidad y la autenticación  
Firewalls, sistemas de detección de intrusos y software antivirus  
Seguridad en las redes inalámbricas  
Cifrado e infraestructura de clave pública  
Aseguramiento de la disponibilidad del sistema  
Aspectos de seguridad para la computación en la nube y la plataforma digital móvil  
Aseguramiento de la calidad del software
- 8.5 PROYECTOS PRÁCTICOS SOBRE MIS**  
Problemas de decisión gerencial  
Mejora de la toma de decisiones: uso del software de hojas de cálculo para realizar una evaluación del riesgo de seguridad  
Mejora de la toma de decisiones: evaluación de los servicios de subcontratación (outsourcing) de la seguridad

#### MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

El fuerte crecimiento del mercado de empleos en seguridad de TI  
La Ley Sarbanes-Oxley  
Análisis forense de sistemas  
Controles generales y de aplicación para los sistemas de información  
Desafíos gerenciales de la seguridad y el control

## ¿ESTÁ USTED EN FACEBOOK? ¡TENGA CUIDADO!

Facebook es la red social en línea más grande del mundo; cada vez más personas la eligen como destino para enviar mensajes a los amigos, compartir fotos, videos, y recolectar “miradas” para la publicidad de negocios y la investigación de mercado. Pero ¡tenga cuidado! Es también un excelente lugar para perder su identidad o ser atacado por software malicioso.

¿Cómo podría pasar esto? Facebook tiene un equipo de seguridad que trabaja duro para contraatacar las amenazas en ese sitio. Utilizan tecnología de seguridad actualizada para proteger su sitio Web. No obstante, con 500 millones de usuarios, no pueden vigilar a todos ni todo. Además, Facebook representa un objetivo muy tentador tanto para las personas problemáticas como para los criminales.

Facebook cuenta con una enorme base de usuarios en todo el mundo, un sitio Web fácil de usar y una comunidad de usuarios vinculados a sus amigos. Es más probable que sus miembros confíen en los mensajes que reciben de los amigos, incluso aunque esta comunicación no sea legítima. Tal vez sea por estas razones que la investigación de la firma de seguridad Kaspersky Labs muestre que el software malicioso en los sitios de redes sociales tales como Facebook y MySpace tiene 10 veces más éxito al infectar a los usuarios que los ataques basados en correo electrónico. Lo que es más, la firma de seguridad de TI Sophos informó el 1 de febrero de 2010 que Facebook representa el riesgo más grande de todos los sitios de redes sociales.

He aquí algunos ejemplos de lo que puede salir mal:

De acuerdo con un informe en febrero de 2010 de la compañía de seguridad de Internet NetWitness, Facebook sirvió como el método primario de transmisión para un ataque de hackers de 18 meses de duración, en donde se engañó a sus usuarios para que revelaran sus contraseñas y descargaran un programa de antivirus falso que roba datos financieros. Un aviso por correo electrónico con apariencia legítima de Facebook pedía a los usuarios que proporcionaran información para ayudar a la red social a actualizar su sistema de inicio de sesión. Cuando el usuario hacía clic en el botón “actualizar” en el correo electrónico, era transportado a una pantalla de inicio de sesión de Facebook falsa, en donde aparecía el nombre del usuario y se pedía a esa persona que proporcionara su contraseña. Una vez que el usuario suministraba esa información, una “herramienta de actualización” instalaba el programa de software malintencionado tipo “caballo de Troya” llamado Zeus, diseñado para robar datos financieros y personales al rastrear de manera furtiva las pulsaciones de teclas de los usuarios al momento en que introducen información en sus computadoras. Los hackers, que lo más probable es que fuera un grupo criminal del este de Europa, robaron cerca de 68 000 credenciales de inicio de sesión de 2 400 compañías y agencias gubernamentales de banca en línea, sitios de redes sociales y correo electrónico.

El gusano Koobface se dirige a los usuarios de Facebook, Twitter y otros sitios Web de redes sociales que utilizan Microsoft Windows para recopilar información confidencial de las víctimas, como los números de tarjetas de crédito. Koobface se detectó por primera vez en diciembre de 2008. Se esparce al entregar mensajes falsos de Facebook a las personas que son “amigos” de un usuario de Facebook cuya computadora ya ha sido infectada. Al recibirlo, el mensaje dirige a quienes lo reciben a un sitio Web de terceros, en donde se les pide que descarguen lo que aparenta ser una actualización del reproductor Adobe Flash. Si descargan y ejecutan el archivo, Koobface puede infectar su sistema y utilizar la computadora para obras más maliciosas.

Durante la mayor parte de mayo de 2010, los miembros de Facebook y sus amigos fueron víctimas de una campaña de spam que trata de enviar por correo elec-

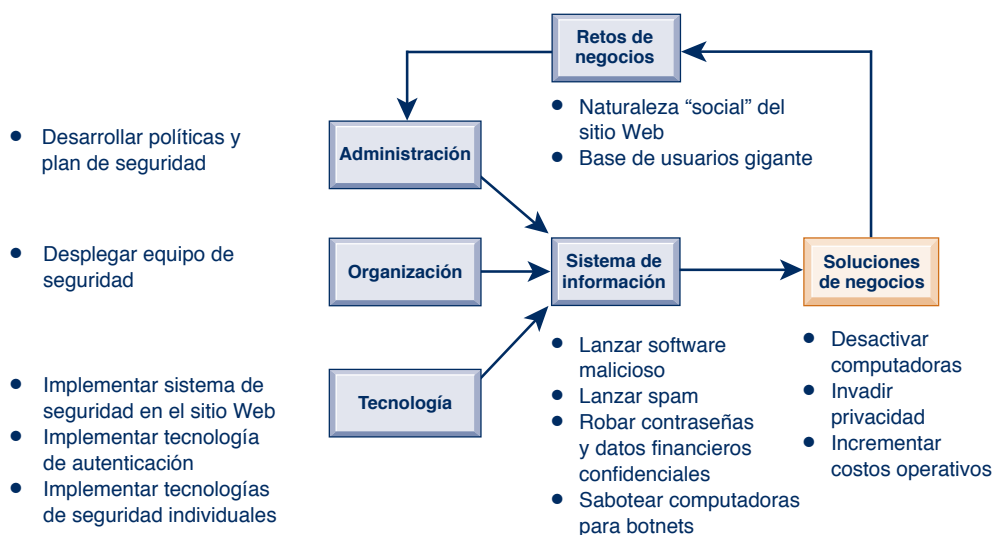
trónico anuncios no solicitados y robar las credenciales de inicio de sesión de los usuarios de Facebook. El ataque empieza con un mensaje que contiene un vínculo a una página Web falsa enviado por los usuarios infectados a todos sus amigos. El mensaje se dirige a cada amigo por su nombre e invita a esa persona a que haga clic en un vínculo al “video más gracioso de todos”. El vínculo transporta al usuario a un sitio Web falso que imita el formulario de inicio de sesión de Facebook. Cuando los usuarios tratan de iniciar sesión, la página los redirige a una página de aplicación de Facebook que instala software tipo adware ilícito, el cual bombardea sus computadoras con todo tipo de anuncios no deseados.

El proceso de recuperación de estos ataques requiere mucho tiempo y es costoso, en especial para las firmas de negocios. En un estudio realizado en septiembre de 2010 por Panda Security se descubrió que un tercio de las pequeñas y medianas empresas que se encuestaron habían sido afectadas por software malicioso proveniente de redes sociales, y más de una tercera parte de éstas sufrieron más de \$5 000 en pérdidas. Desde luego que, para las empresas grandes, las pérdidas debido a Facebook son mucho mayores.

**Fuentes:** Lance Whitney, “Social-Media Malware Hurting Small Businesses”, CNET News, 15 de septiembre de 2010; Raj Dash, “Report: Facebook Served as Primary Distribution Channel for Botnet Army”, all-facebook.com, 18 de febrero de 2010; Sam Diaz, “Report: Bad Guys Go Social: Facebook Tops Security Risk List”, ZDNet, 1 de febrero de 2010; Lucian Constantin, “Weekend Adware Scam Returns to Facebook”, Softpedia, 29 de mayo de 2010; Brad Stone, “Viruses that Leave Victims Red in the Facebook”, *The New York Times*, 14 de diciembre de 2009, y Brian Prince, “Social Networks 10 Times as Effective for Hackers, Malware”, *eWeek*, 13 de mayo de 2009.

Los problemas creados por el software malicioso en Facebook ilustran algunas de las razones por las que las empresas necesitan poner especial atención en la seguridad de los sistemas de información. Facebook ofrece abundantes beneficios tanto para individuos como para empresas. Sin embargo, desde el punto de vista de la seguridad, usar Facebook es una de las formas más fáciles de exponer un sistema computacional al software malicioso: su computadora, las computadoras de sus amigos e incluso las computadoras de las empresas que participan en esta red social.

El diagrama de apertura del capítulo dirige la atención a los puntos importantes generados por este caso y este capítulo. Aunque la gerencia de Facebook tiene una política de seguridad y un equipo de seguridad en acción, Facebook se ha visto plagado de muchos problemas de seguridad que afectan a individuos y empresas por igual. La naturaleza “social” de este sitio y el gran número de usuarios lo hacen en especial atractivo para que los criminales y hackers intenten robar información personal y financiera de valor, además de propagar software malicioso. Aun y cuando Facebook y sus usuarios implementan una tecnología de seguridad, de todas formas son vulnerables a los nuevos tipos de ataques de software malicioso y estafas criminales. Además de las pérdidas por el robo de datos financieros, las dificultades de erradicar el software malicioso o de reparar los daños provocados por el robo de identidad se añaden a los costos operacionales y hacen menos efectivos a los individuos y a las empresas.



## 8.1 VULNERABILIDAD Y ABUSO DE LOS SISTEMAS

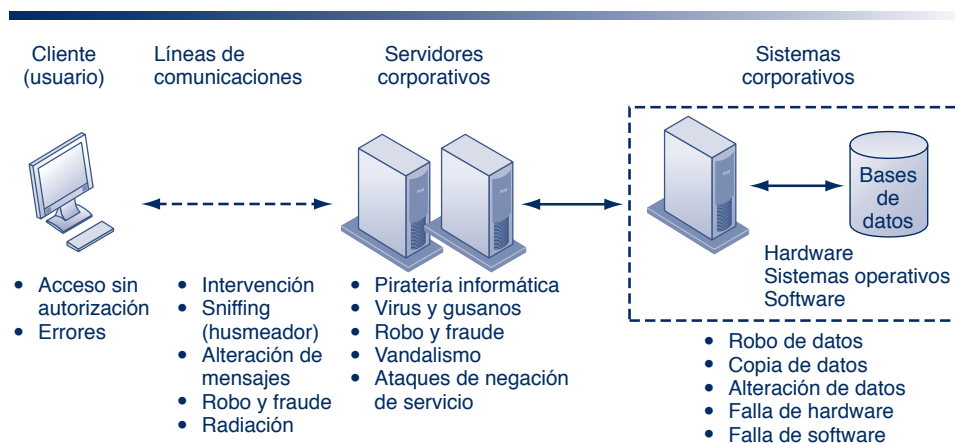
¿Puede imaginar lo que ocurriría si intentara conectarse a Internet sin un firewall o software antivirus? Su computadora quedaría deshabilitada en unos cuantos segundos, y podría tardar varios días en recuperarla. Si utilizara la computadora para operar su negocio, tal vez no podría venderles a sus clientes o colocar pedidos con sus proveedores mientras estuviera deshabilitada. Quizás descubra que su sistema computacional pudo haber sido penetrado por personas externas, que probablemente hayan robado o destruido información valiosa, como los datos de pago confidenciales de sus clientes. Si se destruyeran o divulgaran muchos datos, es posible que su negocio no pudiera volver a operar.

En resumen, si opera un negocio en la actualidad, la seguridad y el control tienen que ser una de sus prioridades más importantes. La **seguridad** se refiere a las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico a los sistemas de información. Los **controles** son métodos, políticas y procedimientos organizacionales que refuerzan la seguridad de los activos de la organización; la precisión y confiabilidad de sus registros, y la adherencia operacional a los estándares gerenciales.

### POR QUÉ SON VULNERABLES LOS SISTEMAS

Quando se almacenan grandes cantidades de datos en forma electrónica, son vulnerables a muchos más tipos de amenazas que cuando existían en forma manual. Los sistemas de información se interconectan en distintas ubicaciones a través de las redes de comunicaciones. El potencial de acceso sin autorización, abuso o fraude no se limita a una sola ubicación, sino que puede ocurrir en cualquier punto de acceso en la red. La figura 8-1 ilustra las amenazas más comunes contra los sistemas de información contemporáneos. Se pueden derivar de los factores técnicos, organizacionales y ambientales compuestos por malas decisiones gerenciales. En el entorno de computación cliente/servidor multinivel que se ilustra en esta figura, existen vulnerabilidades en cada capa y en las comunicaciones entre ellas. Los usuarios en la capa cliente pueden provocar daños al introducir errores o acceder a los sistemas sin autorización. Es posible acceder a los datos que fluyen a través de las redes, robar datos valiosos durante la transmisión

**FIGURA 8-1 DESAFÍOS Y VULNERABILIDADES DE SEGURIDAD CONTEMPORÁNEOS**



La arquitectura de una aplicación basada en Web tiene por lo general un cliente Web, un servidor y sistemas de información corporativos vinculados a bases de datos. Cada uno de estos componentes presenta desafíos y vulnerabilidades de seguridad. Las inundaciones, los incendios, las fallas de energía y otros problemas eléctricos pueden provocar interrupciones en cualquier punto en la red.

o alterar mensajes sin autorización. La radiación puede interrumpir una red en diversos puntos también. Los intrusos pueden lanzar ataques de negación de servicio o software malicioso para interrumpir la operación de los sitios Web. Aquellas personas capaces de penetrar en los sistemas corporativos pueden destruir o alterar los datos corporativos almacenados en bases de datos o archivos.

Los sistemas fallan si el hardware de computadora se descompone, no está configurado en forma apropiada o se daña debido al uso inapropiado o actos delictivos. Los errores en la programación, la instalación inapropiada o los cambios no autorizados hacen que el software de computadora falle. Las fallas de energía, inundaciones, incendios u otros desastres naturales también pueden perturbar los sistemas computacionales.

La asociación a nivel nacional o internacional con otra compañía impone una mayor vulnerabilidad si la información valiosa reside en redes y computadoras fuera del control de la organización. Sin un resguardo sólido, los datos valiosos se podrían perder, destruir o hasta caer en manos equivocadas y revelar importantes secretos comerciales o información que viole la privacidad personal.

A estas tribulaciones se agrega la popularidad de los dispositivos móviles de bolsillo para la computación de negocios. La portabilidad provoca que los teléfonos celulares, los teléfonos inteligentes y las computadoras tipo tableta sean fáciles de perder o robar. Los teléfonos inteligentes comparten las mismas debilidades de seguridad que otros dispositivos de Internet, y son vulnerables al software malicioso y a que extraños se infiltren en ellos. En 2009, los expertos de seguridad identificaron 30 fallas de seguridad en software y sistemas operativos de los teléfonos inteligentes fabricados por Apple, Nokia y Research In Motion, fabricante de los equipos BlackBerry.

Incluso las apps que se han desarrollado a la medida para los dispositivos móviles son capaces de convertirse en software mal intencionado. Por ejemplo, en diciembre de 2009 Google extrajo docenas de apps de banca móvil de su Android Market debido a que podían haberse actualizado para capturar las credenciales bancarias de los clientes. Los teléfonos inteligentes utilizados por los ejecutivos corporativos pueden contener datos confidenciales, como cifras de ventas, nombres de clientes, números telefónicos y direcciones de correo electrónico. Tal vez los intrusos tengan acceso a las redes corporativas internas por medio de estos dispositivos.

## **Vulnerabilidades de Internet**

Las redes públicas grandes, como Internet, son más vulnerables que las internas, ya que están abiertas para casi cualquiera. Internet es tan grande que, cuando ocurren abusos, pueden tener un impacto mucho muy amplio. Cuando Internet se vuelve parte de la red corporativa, los sistemas de información de la organización son aún más vulnerables a las acciones de personas externas.

Las computadoras que tienen conexión constante a Internet mediante módems de cable o líneas de suscriptor digitales (DSL) son más propensas a que se infiltren personas externas debido a que usan direcciones de Internet fijas, mediante las cuales se pueden identificar con facilidad (con el servicio de marcación telefónica, se asigna una dirección temporal de Internet a cada sesión). Una dirección fija en Internet crea un objetivo fijo para los hackers.

El servicio telefónico basado en la tecnología de Internet (vea el capítulo 7) es más vulnerable que la red de voz conmutada si no se opera a través de una red privada segura. La mayoría del tráfico de voz sobre IP (VoIP) a través de la red Internet pública no está cifrado, por lo que cualquiera con una red puede escuchar las conversaciones. Los hackers pueden interceptar conversaciones o apagar el servicio de voz al inundar los servidores que soportan VoIP con tráfico fantasma.

La vulnerabilidad también ha aumentado debido al extenso uso del correo electrónico, la mensajería instantánea (IM) y los programas de compartición de archivos de igual a igual. El correo electrónico puede contener adjuntos que sirven como trampolines para el software malicioso o el acceso sin autorización a los sistemas corporativos internos. Los empleados pueden usar mensajes de correo electrónico para transmitir valiosos secretos comerciales, datos financieros o información confidencial de los clientes a recipientes no autorizados. Las aplicaciones de mensajería instantánea populares para los consumidores no utilizan una capa segura para los mensajes de texto, por lo

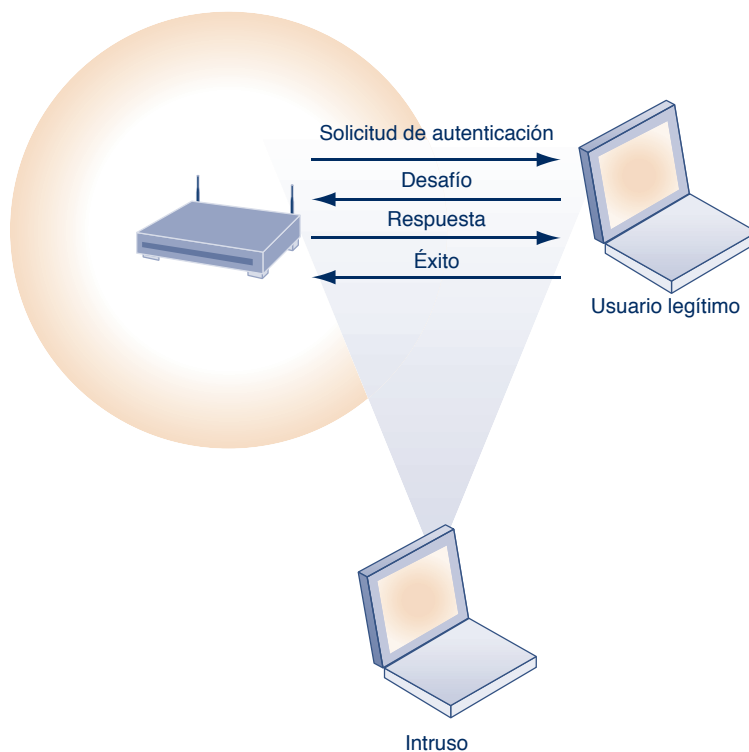
que personas externas pueden interceptarlos y leerlos durante la transmisión a través de la red Internet pública. La actividad de mensajería instantánea a través de Internet puede utilizarse en algunos casos como una puerta trasera hacia una red que de otra forma sería segura. En la compartición de archivos a través de redes de igual a igual (P2P), como las que se utilizan para compartir música ilegal, también se puede transmitir software malicioso o exponer la información en las computadoras individuales o corporativas a personas externas.

### Desafíos de seguridad inalámbrica

¿Es seguro iniciar sesión en una red inalámbrica en un aeropuerto, biblioteca u otra ubicación pública? Depende de qué tan alerta esté usted. Incluso la red inalámbrica en su hogar es vulnerable debido a que las bandas de radiofrecuencia son fáciles de explorar. Las redes Bluetooth y Wi-Fi son susceptibles a la piratería informática por parte de intrusos fisgones. Aunque el rango de las redes Wi-Fi es de sólo varios cientos de pies, se puede extender a un cuarto de milla mediante el uso de antenas externas. Intrusos externos equipados con laptops, tarjetas de red inalámbricas, antenas externas y software de piratería informática pueden infiltrarse con facilidad en las redes de área local (LAN) que utilizan el estándar 802.11. Los hackers utilizan estas herramientas para detectar redes no protegidas, monitorear el tráfico de red y, en algunos casos, obtener acceso a Internet o a redes corporativas.

La tecnología de transmisión Wi-Fi se diseñó para facilitar el proceso de las estaciones de encontrarse y escucharse entre sí. Los *identificadores de conjuntos de servicios* (SSID) que identifican los puntos de acceso en una red Wi-Fi se transmiten varias veces y los programas husmeadores de los intrusos pueden detectarlos con bastante facilidad (vea la figura 8-2). En muchos lugares las redes inalámbricas no tienen protecciones básicas contra la técnica de **war driving**, en la que los espías conducen

**FIGURA 8-2** DESAFÍOS DE SEGURIDAD DE WI-FI



Los intrusos pueden infiltrarse en muchas redes Wi-Fi con facilidad mediante el uso de programas husmeadores para obtener una dirección y acceder a los recursos de una red sin autorización.



cerca de edificios o se estacionan afuera de éstos y tratan de interceptar el tráfico de la red inalámbrica.

Un hacker puede emplear una herramienta de análisis de 802.11 para identificar el SSID (Windows XP, Vista y 7 tienen herramientas para detectar el SSID que se utiliza en una red y configurar de manera automática la NIC de radio dentro del dispositivo del usuario). Un intruso que se haya asociado con un punto de acceso mediante el uso del SSID correcto es capaz de acceder a otros recursos en la red, en donde usa el sistema operativo Windows para determinar qué otros usuarios están conectados a la red y accede a los discos duros de su computadora, de modo que puede abrir o copiar sus archivos.

Los intrusos también utilizan la información que han recopilado para establecer puntos de acceso falsos en un canal de radio diferente, en ubicaciones físicas cercanas a los usuarios para obligar a la NIC de radio de un usuario a asociarse con el punto de acceso falso. Una vez que ocurre esta asociación, los hackers que utilizan el punto de acceso falso pueden capturar los nombres y contraseñas de los usuarios desprevenidos.

El estándar de seguridad inicial desarrollado para Wi-Fi, conocido como privacidad equivalente al cableado (WEP), no es muy efectivo. WEP está integrado en todos los productos 802.11 estándar, pero su uso es opcional. Muchos usuarios se rehúsan a utilizar las características de seguridad de WEP y quedan desprotegidos. La especificación básica de WEP establece que un punto de acceso y todos sus usuarios deben compartir la misma contraseña cifrada de 40 bits, que los hackers pueden descifrar con facilidad a partir de una pequeña cantidad de tráfico. Ahora hay disponibles sistemas de cifrado y autenticación más sólidos, como el Acceso Wi-Fi protegido 2 (WPA2), pero los usuarios deben estar dispuestos a instalarlos.

## SOFTWARE MALICIOSO: VIRUS, GUSANOS, CABALLOS DE TROYA Y SPYWARE

Los programas de software malicioso se conocen como **malware** e incluyen una variedad de amenazas, como virus de computadora, gusanos y caballos de Troya. Un **virus de computadora** es un programa de software malintencionado que se une a otros programas de software o archivos de datos para poder ejecutarse, por lo general sin el conocimiento o permiso del usuario. La mayoría de los virus de computadora entregan una “carga útil”. La cual puede ser benigna en cierto sentido, como las instrucciones para mostrar un mensaje o imagen, o puede ser muy destructiva: tal vez destruya programas o datos, obstruya la memoria de la computadora, aplique formato al disco duro o haga que los programas se ejecuten de manera inapropiada. Por lo general los virus se esparcen de una computadora a otra cuando los humanos realizan una acción, como enviar un adjunto de correo electrónico o copiar un archivo infectado.

La mayoría de los ataques recientes provienen de **gusanos**: programas de computadora independientes que se copian a sí mismos de una computadora a otras computadoras a través de una red (a diferencia de los virus, pueden operar por su cuenta sin necesidad de unirse a otros archivos de programa de computadora y dependen menos del comportamiento humano para poder esparcirse de una computadora a otra. Esto explica por qué los gusanos de computadora se esparcen con mucha mayor rapidez que los virus). Los gusanos destruyen datos y programas; además pueden interrumpir o incluso detener la operación de las redes de computadoras.

Los gusanos y los virus se esparcen con frecuencia a través de Internet, de archivos o software descargado, de archivos adjuntos a las transmisiones de correo electrónico, y de mensajes de correo electrónico o de mensajería instantánea comprometidos. Los virus también han invadido los sistemas de información computarizados por medio de discos “infectados” o máquinas infectadas. En la actualidad los gusanos de correo electrónico son los más problemáticos.

El malware dirigido a los dispositivos móviles no es tan extenso como el que está dirigido a las computadoras, pero de todas formas se esparce mediante el correo electrónico, los mensajes de texto, Bluetooth y las descargas de archivos desde Web, por medio de redes Wi-Fi o celulares. Ahora hay más de 200 virus y gusanos dirigi-

dos a teléfonos celulares, como Cabir, Commwarrior, Frontal.A y Ikee.B. Frontal.A instala un archivo corrupto que provoca fallas en los teléfonos celulares y evita que el usuario pueda reiniciar su equipo, mientras que Ikee.B convierte los dispositivos iPhone liberados en dispositivos controlados por botnets. Los virus de dispositivos móviles imponen serias amenazas a la computación empresarial, debido a que ahora hay muchos dispositivos inalámbricos vinculados a los sistemas de información corporativos.

Las aplicaciones Web 2.0, como los sitios de blogs, wikis y redes sociales tales como Facebook y MySpace, han emergido como nuevos conductos para malware o spyware. Estas aplicaciones permiten a los usuarios publicar código de software como parte del contenido permisible, y dicho código se puede iniciar de manera automática tan pronto como se ve una página Web. El caso de estudio de apertura del capítulo describe otros canales para el malware dirigido a Facebook. En septiembre de 2010, unos hackers explotaron una falla de seguridad de Twitter para enviar a los usuarios a sitios pornográficos japoneses y generaron mensajes de manera automática desde otras cuentas (Coopes, 2010).

La tabla 8-1 describe las características de algunos de los gusanos y virus más dañinos que han aparecido hasta la fecha.

Durante la década pasada, los gusanos y virus han provocado miles de millones de dólares en daños a redes corporativas, sistemas de correo electrónico y datos. De acuerdo con la encuesta State of the Net 2010 de Consumer Reports, los consumidores estadouni-

**TABLA 8-1 EJEMPLOS DE CÓDIGO MALICIOSO**

NOMBRE	TIPO	DESCRIPCIÓN
Conficker (alias Downadup, Downup)	Gusano	Se detectó por primera vez en noviembre de 2008. Utiliza las fallas en el software Windows para tomar el control de las máquinas y vincularlas a una computadora virtual que se puede controlar de forma remota. Tiene más de 5 millones de computadoras bajo su control en todo el mundo. Es difícil de erradicar.
Storm	Gusano/ caballo de Troya	Se identificó por primera vez en enero de 2007. Se esparce a través del spam de correo electrónico con un adjunto falso. Infectó cerca de 10 millones de computadoras; provocó que se unieran a su red de computadoras zombis involucradas en actividades criminales.
Sasser.ftp	Gusano	Apareció por primera vez en mayo de 2004. Se esparció por Internet al atacar direcciones IP aleatorias. Hace que las computadoras fallen y se reinicien de manera continua, y que las computadoras infectadas busquen más víctimas. Afectó a millones de computadoras en todo el mundo; interrumpió los registros de los vuelos de British Airways, las operaciones de las estaciones guardacostas británicas, los hospitales de Hong Kong, las sucursales de correo de Taiwán y el Banco Westpac de Australia. Se estima que Sasser y sus variantes provocaron entre \$14.8 y \$18.6 mil millones en daños por todo el mundo.
MyDoom.A	Gusano	Apareció por primera vez el 26 de julio de 2004. Se esparce como un adjunto de correo electrónico. Envía correo electrónico a las direcciones que se obtienen de las máquinas infectadas, falsificando la dirección del emisor. En su momento cumbre este gusano redujo el rendimiento global de Internet en un 10 por ciento, y los tiempos de carga de las páginas Web hasta en un 50 por ciento. Se programó para dejar de esparcirse después de febrero 12 de 2004.
Sobig.F	Gusano	Se detectó por primera vez el 19 de agosto de 2003. Se esparce mediante adjuntos de correo electrónico y envía cantidades masivas de correo con información falsificada del emisor. Se desactivó por sí solo el 10 de septiembre de 2003, después de infectar a más de 1 millón de equipos PC y de provocar entre \$5 y \$10 mil millones en daños.
ILOVEYOU	Virus	Se detectó por primera vez el 3 de mayo de 2000. Es un virus de secuencia de comandos escrito en Visual Basic y se transmitió como adjunto en el correo electrónico con la línea ILOVEYOU en el asunto. Sobrescribe música, imágenes y otros archivos con una copia de sí mismo; se estima que provocó entre \$10 y \$15 mil millones en daños.
Melissa	Macrovirus/ gusano	Apareció por primera vez en marzo de 1999. Es una secuencia de macro de Word que envía por correo un archivo infectado de Word a las primeras 50 entradas en la libreta de direcciones de Microsoft Outlook. Infectó entre un 15 y 29 por ciento de todas las PC de negocios, provocando entre \$300 y \$600 millones en daños.

densos perdieron \$3.5 mil millones debido al malware y a las estafas en línea, y la mayoría de estas pérdidas provinieron del malware (Consumer Reports, 2010).

Un **caballo de Troya** es un programa de software que parece ser benigno, pero entonces hace algo distinto de lo esperado, como el virus troyano Zeus descrito en el caso de apertura del capítulo. El caballo de Troya en sí no es un virus, ya que no se reproduce, pero es con frecuencia un medio para que los virus u otro tipo de software malicioso entren en un sistema computacional. El término *caballo de Troya* se basa en el enorme caballo de madera utilizado por los griegos para engañar a los troyanos y que abrieran las puertas a su ciudad fortificada durante la *Guerra de Troya*. Una vez dentro de las paredes de la ciudad, los soldados griegos ocultos en el caballo salieron y tomaron la ciudad.

Hasta este momento, los ataques por inyección de SQL son la mayor amenaza de malware. Los **ataques de inyección de SQL** aprovechan las vulnerabilidades en el software de aplicación Web mal codificado para introducir código de programa malicioso en los sistemas y redes de una compañía. Estas vulnerabilidades ocurren cuando una aplicación Web no valida o filtra de manera apropiada los datos introducidos por un usuario en una página Web, que podría ocurrir al momento de pedir algo en línea. Un atacante utiliza este error de validación de la entrada para enviar una consulta SQL falsa a la base de datos subyacente y acceder a ésta, plantar código malicioso o acceder a otros sistemas en la red. Las aplicaciones Web extensas tienen cientos de lugares para introducir datos de los usuarios, cada uno de los cuales crea una oportunidad para un ataque por inyección de SQL.

Se cree que una gran cantidad de aplicaciones orientadas a Web tienen vulnerabilidades de inyección de SQL, por lo que hay herramientas disponibles para que los hackers verifiquen si determinadas aplicaciones Web tienen estas vulnerabilidades. Dichas herramientas pueden localizar un campo de entrada de datos en un formulario de una página Web, introducir datos en él y verificar la respuesta para ver si muestra vulnerabilidad a una inyección de SQL.

Algunos tipos de spyware también actúan como software malicioso. Estos pequeños programas se instalan a sí mismos de manera furtiva en las computadoras para monitorear la actividad de navegación Web de los usuarios y mostrarles anuncios. Se han documentado miles de formas de spyware.

A muchos usuarios el **spyware** les parece molesto y algunos críticos se preocupan en cuanto a que infringe la privacidad de los usuarios de computadora. Algunas formas de spyware son en especial nefastas. Los **keyloggers** registran cada pulsación de tecla en una computadora para robar números de serie de software, lanzar ataques por Internet, obtener acceso a cuentas de correo electrónico, conseguir contraseñas para los sistemas computacionales protegidos o descubrir información personal tal como los números de tarjetas de crédito. Otros programas de spyware restablecen las páginas de inicio de los navegadores Web, redirigen las solicitudes de búsqueda o reducen el rendimiento al ocupar demasiada memoria. El troyano Zeus descrito en el caso de apertura del capítulo utiliza un keylogger para robar información financiera.

## LOS HACKERS Y LOS DELITOS COMPUTACIONALES

Un **hacker** es un individuo que intenta obtener acceso sin autorización a un sistema computacional. Dentro de la comunidad de hackers, el término *cracker* se utiliza con frecuencia para denotar a un hacker con intención criminal, aunque en la prensa pública los términos hacker y cracker se utilizan sin distinción. Los hackers y los crackers obtienen acceso sin autorización al encontrar debilidades en las protecciones de seguridad empleadas por los sitios Web y los sistemas computacionales; a menudo aprovechan las diversas características de Internet que los convierten en sistemas abiertos fáciles de usar.

Las actividades de los hackers se han ampliado mucho más allá de la mera intrusión en los sistemas, para incluir el robo de bienes e información, así como daños en los sistemas y **cibervandalismo**: la interrupción, desfiguración o destrucción intencional de un sitio Web o sistema de información corporativo. Por ejemplo, los cibervándalos han

convertido muchos de los sitios de “grupos” de MySpace, que están dedicados a intereses tales como la fabricación de cerveza casera o el bienestar de los animales, en paredes de ciber-grafiti, llenas de comentarios y fotografías ofensivos.

## Spoofing y Sniffing

Con frecuencia, los hackers que intentan ocultar sus verdaderas identidades utilizan direcciones de correo falsas o se hacen pasar por alguien más. El **spoofing** también puede implicar el hecho de redirigir un vínculo Web a una dirección distinta de la que se tenía pensada, en donde el sitio se hace pasar por el destino esperado. Por ejemplo, si los hackers redirigen a los clientes a un sitio Web falso que se ve casi igual que el sitio verdadero, pueden recolectar y procesar pedidos para robar de manera efectiva la información de negocios así como la información confidencial de los clientes del sitio verdadero. En nuestro análisis de los delitos por computadora proveemos más detalles sobre otras formas de spoofing.

Un **husmeador (sniffer)** es un tipo de programa espía que monitorea la información que viaja a través de una red. Cuando se utilizan de manera legítima, los husmeadores ayudan a identificar los potenciales puntos problemáticos en las redes o la actividad criminal en las mismas, pero cuando se usan para fines criminales pueden ser dañinos y muy difíciles de detectar. Los husmeadores permiten a los hackers robar información propietaria de cualquier parte de una red, como mensajes de correo electrónico, archivos de la compañía e informes confidenciales.

## Ataques de negación de servicio

En un **ataque de negación de servicio (DoS)**, los hackers inundan un servidor de red o de Web con muchos miles de comunicaciones o solicitudes de servicios falsas para hacer que la red falle. La red recibe tantas solicitudes que no puede mantener el ritmo y, por lo tanto, no está disponible para dar servicio a las solicitudes legítimas. Un **ataque de negación de servicio distribuida (DDoS)** utiliza varias computadoras para saturar la red desde muchos puntos de lanzamiento.

Por ejemplo, durante las protestas por las elecciones iraníes de 2009, los activistas extranjeros que trataban de ayudar a la oposición se involucraron en ataques DDoS contra el gobierno de Irán. El sitio Web oficial del gobierno iraní ([ahmadinejad.ir](http://ahmadinejad.ir)) resultó inaccesible en varias ocasiones.

Aunque los ataques DoS no destruyen información ni acceden a las áreas restringidas de los sistemas de información de una compañía, a menudo provocan que un sitio Web se cierre, con lo cual es imposible para los usuarios legítimos acceder a éste. Para los sitios de comercio electrónico con mucha actividad, estos ataques son costosos; mientras el sitio permanezca cerrado, los clientes no pueden hacer compras. Los negocios pequeños y de tamaño medio son los más vulnerables, puesto que sus redes tienden a estar menos protegidas que las de las grandes corporaciones.

A menudo los perpetradores de los ataques DoS utilizan miles de equipos PC “zombis” infectados con software malicioso sin que sus propietarios tengan conocimiento, y se organizan en una **botnet**. Los hackers crean estas botnets al infectar las computadoras de otras personas con malware de bot que abre una puerta trasera por la cual un atacante puede dar instrucciones. Así, la computadora infectada se convierte en un esclavo, o zombi, que da servicio a una computadora maestra perteneciente a alguien más. Una vez que un hacker infecta suficientes computadoras, puede usar los recursos amasados de la botnet para lanzar ataques DDoS, campañas de phishing o enviar correo electrónico de “spam” no solicitado.

Se estima que la cantidad de computadoras que forman parte de botnets está entre 6 y 24 millones, con miles de botnets que operan en todo el mundo. El ataque más grande en 2010 fue el de la botnet Mariposa, que empezó en España y se esparció por todo el mundo. Mariposa había infectado y controlado cerca de 12.7 millones de computadoras en sus esfuerzos por robar números de tarjetas de crédito y contraseñas de banca en línea. Más de la mitad de las compañías Fortune 1000, 40 de los principales bancos y numerosas agencias gubernamentales se infectaron, y no lo sabían.

El caso de estudio al final del capítulo describe varias ondas de ataques DDoS dirigidos a varios sitios Web de agencias gubernamentales y otras organizaciones en Corea del Sur y Estados Unidos en julio de 2009. El atacante utilizó una botnet que controlaba cerca de 65 000 computadoras y pudo inhabilitar algunos de estos sitios durante varios días. La mayor parte de la botnet era originaria de China y Corea del Norte. Los ataques de las botnets que se creyó habían surgido de Rusia fueron responsables de incapacitar los sitios Web del gobierno de Estonia en abril de 2007, y del gobierno gregoriano en julio de 2008.

Delitos por computadora

La mayoría de las actividades de los hackers son delitos criminales; las vulnerabilidades de los sistemas que acabamos de describir los convierten en objetivos para otros tipos de **delitos por computadora** también. Por ejemplo, a principios de julio de 2009, agentes federales estadounidenses arrestaron a Sergey Aleynikov, un programador de computadora en la firma bancaria de inversión Goldman Sachs, por robar programas de computadora propietarios que se utilizaban para realizar comercios lucrativos rápidos en los mercados financieros. El software generaba muchos millones de dólares en ganancias cada año para Goldman y, en manos equivocadas, se podría haber usado para manipular mercados financieros en forma deshonesta. El delito por computadora se define en el Departamento de Justicia de Estados Unidos como “cualquier violación a la ley criminal que involucra el conocimiento de una tecnología de computadora para su perpetración, investigación o acusación”. La tabla 8-2 provee ejemplos de la computadora como blanco de delitos y como instrumento de delito.

Nadie conoce la magnitud del problema del delito por computadora: cuántos sistemas se invaden, cuántas personas participan en la práctica, o el total de daños económicos. De acuerdo con la encuesta del CSI sobre delitos por computadora y seguridad de 2009 realizada en 500 compañías, la pérdida anual promedio de los participantes debido al delito por computadora y los ataques de seguridad fue de cerca de \$234 000 (Instituto de Seguridad Computacional, 2009). Muchas compañías se niegan a informar los delitos por computadora debido a que puede haber empleados involucrados, o porque la compañía teme que al publicar su vulnerabilidad se dañará su reputación. Los tipos de delitos por computadora que provocan el mayor daño económico son los

TABLA 8-2 EJEMPLOS DE DELITOS POR COMPUTADORA

COMPUTADORAS COMO BLANCOS DE DELITOS

- Violar la confidencialidad de los datos computarizados protegidos
- Acceder a un sistema computacional sin autorización
- Acceder de manera intencional a una computadora protegida para cometer fraude
- Acceder de manera intencional una computadora protegida y causar daño, ya sea por negligencia o de forma deliberada
- Transmitir conscientemente un programa, código de programa o comando que provoque daños intencionales a una computadora protegida
- Amenazar con provocar daños a una computadora protegida

COMPUTADORAS COMO INSTRUMENTOS DE DELITOS

- Robo de secretos comerciales
- Copia sin autorización de software o propiedad intelectual protegida por derechos de autor, como artículos, libros, música y video
- Ideas para defraudar
- Uso del correo electrónico para amenazas o acoso
- Tratar de manera intencional de interceptar comunicaciones electrónicas
- Acceder de manera ilegal a las comunicaciones electrónicas almacenadas, como el correo electrónico y el correo de voz
- Transmitir o poseer pornografía infantil mediante el uso de una computadora

ataques DoS, la introducción de virus, el robo de servicios y la interrupción de los sistemas computacionales.

## Robo de identidad

Con el crecimiento de Internet y el comercio electrónico, el robo de identidad se ha vuelto muy problemático. El **robo de identidad** es un crimen en el que un impostor obtiene piezas clave de información personal, como números de identificación del seguro social, números de licencias de conducir o números de tarjetas de crédito, para hacerse pasar por alguien más. La información se puede utilizar para obtener crédito, mercancía o servicios a nombre de la víctima, o para proveer al ladrón credenciales falsas. De acuerdo con Javelin Strategy and Research, las pérdidas debido al robo de identidad se elevaron a \$54 mil millones en 2009, y más de 11 millones de adultos estadounidenses fueron víctimas de fraude de identidad (Javelin Strategy & Research, 2010).

El robo de identidad ha prosperado en Internet, en donde los archivos de tarjetas de crédito son uno de los principales objetivos de los hackers de sitios Web. Además, los sitios de comercio electrónico son maravillosas fuentes de información personal sobre los clientes: nombre, dirección y número telefónico. Armados con esta información, los criminales pueden asumir nuevas identidades y establecer nuevos créditos para sus propios fines.

Una táctica cada vez más popular es una forma de spoofing conocida como **phishing**, la cual implica el proceso de establecer sitios Web falsos o enviar tanto correo electrónico como mensajes de texto que se parezcan a los de las empresas legítimas, para pedir a los usuarios datos personales. El mensaje instruye a quienes lo reciben para que actualicen o confirmen los registros, para lo cual deben proveer números de seguro social, información bancaria y de tarjetas de crédito, además de otros datos confidenciales, ya sea respondiendo al mensaje de correo electrónico, introduciendo la información en un sitio Web falso o llamando a un número telefónico. EBay, PayPal, Amazon.com, Walmart y varios bancos se encuentran entre las compañías más afectadas por el spoofing.

Las nuevas tecnologías de phishing conocidas como Evil Twin o gemelos malvados y pharming son más difíciles de detectar. Los **gemelos malvados** son redes inalámbricas que pretenden ofrecer conexiones Wi-Fi de confianza a Internet, como las que se encuentran en las salas de los aeropuertos, hoteles o cafeterías. La red falsa se ve idéntica a una red pública legítima. Los estafadores tratan de capturar las contraseñas o los números de tarjetas de crédito de los usuarios que inician sesión en la red sin darse cuenta de ello.

El **pharming** redirige a los usuarios a una página Web falsa, aun y cuando el individuo escribe la dirección de la página Web correcta en su navegador. Esto es posible si los perpetradores del pharming obtienen acceso a la información de las direcciones de Internet que almacenan los proveedores de servicio de Internet para agilizar la navegación Web; las compañías ISP tienen software con fallas en sus servidores que permite a los estafadores infiltrarse y cambiar esas direcciones.

En el mayor caso de robo de identidad a la fecha, Alberto Gonzalez de Miami y dos co-conspiradores rusos penetraron en los sistemas corporativos de TJX Corporation, Hannaford Brothers, 7-Eleven y otros importantes vendedores minoristas, para robar más de 160 millones de números de tarjetas de crédito y débito entre 2005 y 2008. En un principio el grupo plantó programas “husmeadores” en las redes de computadoras de estas compañías, los cuales capturaron los datos de tarjetas tan pronto como éstos se transmitían entre los sistemas computacionales. Más adelante cambiaron a los ataques por inyección de SQL, que presentamos antes en este capítulo, para penetrar en las bases de datos corporativas. En marzo de 2010, Gonzalez fue sentenciado a 20 años en prisión. Tan sólo TJX invirtió más de \$200 millones para lidiar con el robo de sus datos, entre ellos los acuerdos legales.

El Congreso de Estados Unidos hizo frente a la amenaza de los delitos por computadora en 1986 con la Ley de Fraude y Abuso de Computadoras. Según esta ley, es ilegal acceder a un sistema computacional sin autorización. La mayoría de los estados tienen leyes similares, y las naciones en Europa cuentan con una legislación comparable. El Congreso también aprobó la Ley Nacional de Protección a la Infraestructura de Información en 1996 para convertir en delitos criminales la distribución de virus y los ataques de hackers que deshabilitan sitios Web. La legislación estadounidense, como la Ley de Intercepción de Comunicaciones (Wiretap), la Ley de Fraude por Telecomunicaciones



(Wire Fraud), la Ley de Espionaje Económico, la Ley de Privacidad de las Comunicaciones Electrónicas, la Ley de Amenazas y Acoso por Correo Electrónico y la Ley Contra la Pornografía Infantil, cubre los delitos por computadora que involucran la interceptación de comunicación electrónica, el uso de comunicación electrónica para defraudar, robar secretos comerciales, acceder de manera ilegal a las comunicaciones electrónicas almacenadas, usar el correo electrónico para amenazas o acoso, y transmitir o poseer pornografía infantil.

### **Fraude del clic**

Cuando usted hace clic en un anuncio mostrado por un motor de búsquedas, por lo general el anunciante paga una cuota por cada clic, que se supone dirige a los compradores potenciales a sus productos. El **fraude del clic** ocurre cuando un individuo o programa de computadora hace clic de manera fraudulenta en un anuncio en línea, sin intención de aprender más sobre el anunciante o de realizar una compra. El fraude del clic se ha convertido en un grave problema en Google y otros sitios Web que cuentan con publicidad en línea del tipo “pago por clic”.

Algunas compañías contratan terceros (por lo general de países con bajos sueldos) para hacer clic de manera fraudulenta en los anuncios del competidor para debilitarlos al aumentar sus costos de marketing. El fraude del clic también se puede perpetrar con programas de software que se encargan de hacer el clic; con frecuencia se utilizan botnets para este fin. Los motores de búsqueda como Google tratan de monitorear el fraude del clic, pero no han querido hacer públicos sus esfuerzos por lidiar con el problema.

### **Amenazas globales: ciberterrorismo y ciberguerra**

Las actividades cibercriminales que hemos descrito —lanzar malware, ataques de negación de servicios y sondas de phishing— no tienen fronteras. La firma de seguridad computacional Sophos informó que 42 por ciento del malware que identificaron a principios de 2010 se originó en Estados Unidos, mientras que el 11 por ciento provino de China y el 6 por ciento de Rusia (Sophos, 2010). La naturaleza global de Internet hace que sea posible para los cibercriminales operar (y hacer daño) en cualquier parte del mundo.

La preocupación creciente es que las vulnerabilidades de Internet o de otras redes hacen de las redes digitales blancos fáciles para los ataques digitales por parte de los terroristas, servicios de inteligencia extranjeros u otros grupos que buscan crear trastornos y daños extensos. Dichos ciberataques podrían estar dirigidos al software que opera las redes de energía eléctrica, los sistemas de control del tráfico aéreo o las redes de los principales bancos e instituciones financieras. Se cree que por lo menos 20 países (uno de ellos China) están desarrollando capacidades ofensivas y defensivas de ciberguerra. El caso de estudio al final del capítulo analiza este problema con mayor detalle.

## **AMENAZAS INTERNAS: LOS EMPLEADOS**

Nuestra tendencia es pensar que las amenazas de seguridad para una empresa se originan fuera de la organización. De hecho, los trabajadores internos de la compañía representan graves problemas de seguridad. Los empleados tienen acceso a la información privilegiada, y en la presencia de procedimientos de seguridad interna descuidados, con frecuencia son capaces de vagar por los sistemas de una organización sin dejar rastro.

Los estudios han encontrado que la falta de conocimiento de los usuarios es la principal causa de fugas de seguridad en las redes. Muchos empleados olvidan sus contraseñas para acceder a los sistemas computacionales o permiten que sus compañeros de trabajo las utilicen, lo cual compromete al sistema. Algunas veces los intrusos maliciosos que buscan acceder al sistema engañan a los empleados para que revelen sus contraseñas al pretender ser miembros legítimos de la compañía que necesitan información. A esta práctica se le denomina **ingeniería social**.

Tanto los usuarios finales como los especialistas en sistemas de información son también una principal fuente de los errores que se introducen a los sistemas de información. Los usuarios finales introducen errores al escribir datos incorrectos o al no seguir las instrucciones apropiadas para procesar los datos y utilizar el equipo de cómputo. Los especialistas de sistemas de información pueden crear errores de software mientras diseñan y desarrollan nuevo software o dan mantenimiento a los programas existentes.

## VULNERABILIDAD DEL SOFTWARE

Los errores de software representan una constante amenaza para los sistemas de información, ya que provocan pérdidas incontables en cuanto a la productividad. La complejidad y el tamaño cada vez mayores de los programas, aunados a las exigencias de una entrega oportuna en los mercados, han contribuido al incremento en las fallas o vulnerabilidades del software. Por ejemplo, un error de software relacionado con una base de datos evitó que millones de clientes minoristas y de pequeñas empresas de JP Morgan Chase accedieran a sus cuentas bancarias en línea durante dos días en septiembre de 2010 (Dash, 2010).

Un problema importante con el software es la presencia de **bugs** ocultos, o defectos de código del programa. Los estudios han demostrado que es casi imposible eliminar todos los bugs de programas grandes. La principal fuente de los bugs es la complejidad del código de toma de decisiones. Un programa relativamente pequeño de varios cientos de líneas contiene decenas de decisiones que conducen a cientos, o hasta miles de rutas. Los programas importantes dentro de la mayoría de las corporaciones son por lo general mucho más grandes, y contienen decenas de miles, o incluso millones de líneas de código, cada una multiplica las opciones y rutas de los programas más pequeños.

No se pueden obtener cero defectos en programas extensos. En sí, no es posible completar el proceso de prueba. Para probar por completo los programas que contienen miles de opciones y millones de rutas, se requerirían miles de años. Incluso con una prueba rigurosa, no sabríamos con seguridad si una pieza de software es confiable sino hasta que el producto lo demostrara por sí mismo después de utilizarlo para realizar muchas operaciones.

Las fallas en el software comercial no sólo impiden el desempeño, sino que también crean vulnerabilidades de seguridad que abren las redes a los intrusos. Cada año las firmas de seguridad identifican miles de vulnerabilidades en el software de Internet y PC. Por ejemplo, en 2009 Symantec identificó 384 vulnerabilidades de los navegadores: 169 en Firefox, 94 en Safari, 45 en Internet Explorer, 41 en Chrome y 25 en Opera. Algunas de estas vulnerabilidades eran críticas (Symantec, 2010).

Para corregir las fallas en el software una vez identificadas, el distribuidor del software crea pequeñas piezas de software llamadas **parches** para reparar las fallas sin perturbar la operación apropiada del software. Un ejemplo es el Service Pack 2 de Microsoft Windows Vista, liberado en abril de 2009, que incluye algunas mejoras de seguridad para contraatacar malware y hackers. Es responsabilidad de los usuarios del software rastrear estas vulnerabilidades, probar y aplicar todos los parches. A este proceso se le conoce como *administración de parches*.

Ya que, por lo general, la infraestructura de TI de una compañía está repleta de varias aplicaciones de negocios, instalaciones de sistemas operativos y otros servicios de sistemas, a menudo el proceso de mantener los parches en todos los dispositivos y servicios que utiliza una compañía consume mucho tiempo y es costoso. El malware se crea con tanta rapidez que las compañías tienen muy poco tiempo para responder entre el momento en que se anuncian una vulnerabilidad y un parche, y el momento en que aparece el software malicioso para explotar la vulnerabilidad.

La necesidad de responder con tanta rapidez al torrente de vulnerabilidades de seguridad crea inclusive defectos en el software destinado a combatirlas, hasta en los productos antivirus populares. Lo que ocurrió en la primavera de 2010 a McAfee, distribuidor líder de software antivirus comercial, es un ejemplo que analizamos en la Sesión interactiva sobre administración.

## SESIÓN INTERACTIVA: ADMINISTRACIÓN

### CUANDO EL SOFTWARE ANTIVIRUS INUTILIZA A SUS COMPUTADORAS

McAfee es una prominente compañía de software antivirus y seguridad computacional con base en Santa Clara, California. Su popular producto VirusScan (que ahora se conoce como AntiVirus Plus) es utilizado tanto por compañías como por clientes individuales en todo el mundo, y le generó ingresos por \$1.93 mil millones en 2009.

Esta verdadera compañía global, tiene cerca de 6 000 empleados en Norteamérica, Europa y Asia. VirusScan y otros productos de seguridad de McAfee se encargan de la seguridad en las terminales y redes, además de hacerse cargo del riesgo y de la conformidad con las normas. La compañía ha trabajado para compilar un extenso historial de buen servicio al cliente y de un sólido aseguramiento de la calidad.

A las 6 a.m., hora de verano del Pacífico (PDT) del 21 de abril de 2010, McAfee cometió un error garrafal que amenazó con destruir ese historial impecable y provocó la posible partida de cientos de valiosos clientes. McAfee liberó lo que debería haber sido una actualización de rutina para su producto insignia VirusScan, con la intención de lidiar con un nuevo y poderoso virus conocido como 'W32/wecorl.a'. Pero a cambio, la actualización de McAfee provocó que potencialmente cientos de miles de máquinas equipadas con McAfee que ejecutaban Windows XP fallaran y no pudieran reiniciarse. ¿Cómo podría McAfee, una compañía enfocada en salvar y preservar las computadoras, cometer una metida de pata que logró lo opuesto para una considerable porción de su base de clientes?

Esa era la pregunta que hacían los iracundos clientes de McAfee la mañana del 21 de abril, cuando sus computadoras quedaron afectadas o de plano no funcionaban. Las actualizaciones se dirigieron por error a un archivo crítico de Windows de nombre svchost.exe, que hospeda otros servicios utilizados por diversos programas en las PC. Por lo general hay más de una instancia del proceso en ejecución en cualquier momento dado, por lo que al eliminarlo se dejaría inutilizado cualquier sistema. Aunque muchos virus, como W32/wecorl.a, se disfrazan y utilizan el nombre svchost.exe para evitar ser detectados, McAfee nunca antes había tenido problemas con los virus que utilizaban esa técnica.

Para empeorar las cosas, sin svchost.exe las computadoras Windows no pueden iniciar de manera apropiada. Los usuarios de VirusScan aplicaron la actualización, intentaron reiniciar sus sistemas y no pudieron actuar mientras sus sistemas se salían de control, se reiniciaban en forma repetida, perdían su capacidad para conectarse en red y, lo peor de todo, su habilidad para detectar unidades USB, que es la única forma de corregir las computadoras afectadas. Las compañías que utilizaban McAfee y dependían mucho de las computadoras Windows XP lucharon por lidiar con el hecho de que la mayoría de sus máquinas fallaran de manera repentina.

Los furiosos administradores de red recurrieron a McAfee en busca de respuestas, pero en un principio la compañía estaba tan confundida como sus clientes en cuanto a cómo podía haber ocurrido una equivocación tan monumental. Pronto, McAfee determinó que la mayoría de las máquinas afectadas utilizaban el Service Pack 3 de Windows XP combinado con la versión 8.7 de McAfee VirusScan. También observaron que la opción "Explorar procesos al habilitar" de VirusScan, desactivada de manera predeterminada en la mayoría de las instalaciones de VirusScan, estaba activada en la mayoría de las computadoras afectadas.

McAfee realizó una investigación más detallada sobre su error y publicó una hoja de preguntas frecuentes (FAQ) en la que explicaron de una forma más completa por qué habían cometido un error tan grande y qué clientes se vieron afectados. Los dos puntos más prominentes de falla fueron los siguientes: en primer lugar, los usuarios debieron haber recibido una advertencia de que svchost.exe se iba a poner en cuarentena o a eliminar, en vez de desechar el archivo de manera automática. En segundo lugar, la prueba automatizada de aseguramiento de calidad de McAfee no detectó dicho error crítico, debido a lo que la compañía consideró como "cobertura inadecuada del producto y los sistemas operativos en los sistemas de prueba utilizados".

La única forma en que el personal de soporte técnico que trabajaba en las organizaciones podía corregir el problema era en forma manual, yendo de computadora en computadora. McAfee liberó una herramienta conocida como "Herramienta de remedio SuperDAT", la cual había que descargar a una máquina que no estuviera afectada, colocarla en una unidad flash y ejecutarla en el Modo seguro de Windows en las máquinas afectadas. Puesto que las máquinas afectadas carecían de acceso a la red, había que hacer esto en una computadora a la vez hasta reparar todas las máquinas. El número total de máquinas afectadas no se conoce, pero sin duda había decenas de miles de computadoras corporativas involucradas. No hace falta decir que los administradores de red y el personal de las divisiones de soporte técnico corporativo estaban furiosos.

Con respecto a las fallas en los procesos de aseguramiento de calidad de McAfee, la compañía explicó en las preguntas frecuentes que no habían incluido el Service Pack 3 de Windows XP con la versión 8.7 de VirusScan en la configuración de prueba de los sistemas operativos y las versiones del producto de McAfee. Esta explicación dejó estupefactos a muchos de los clientes de McAfee y a otros analistas de la industria, ya que el SP3 de XP es la configuración de PC de escritorio más utilizada. Por lo general, Vista y Windows 7 se incluyen en computadoras nuevas y raras veces se instalan en computadoras que tienen XP funcionando.

Otra razón por la que el problema se esparció con tanta rapidez sin detección fue la creciente demanda de actualizaciones de antivirus más frecuentes. La mayoría de las compañías despliegan sus actualizaciones con agresividad para asegurar que las máquinas pasen la menor cantidad de tiempo posibles expuestas a los nuevos virus. La actualización de McAfee afectó a un gran número de máquinas sin detección debido a que la mayor parte de las compañías confían en su proveedor de antivirus para que haga bien las cosas.

Por desgracia para McAfee, basta una equivocación o descuido para dañar de manera considerable la reputación de una compañía de antivirus. McAfee recibió duras críticas por su lenta respuesta a la crisis y por sus intentos iniciales de minimizar el impacto de este problema sobre sus clientes. La compañía emitió una declaración afirmando que sólo se vio afectada una

pequeña fracción de sus clientes, pero esto pronto resultó ser falso. Dos días después de liberar la actualización, el ejecutivo de McAfee Barry McPherson se disculpó por fin con sus clientes en el blog de la compañía. Poco después, el CEO David DeWalt grabó un video para sus clientes, que todavía está disponible a través del sitio Web de McAfee, en donde se disculpó y explicó el incidente.

**Fuentes:** Peter Svensson, "McAfee Antivirus Program Goes Berserk, Freezes PCs", *Associated Press*, 21 de abril de 2010; Gregg Keizer, "McAfee Apologizes for Crippling PCs with Bad Update", *Computerworld*, 23 de abril de 2010 y "McAfee Update Mess Explained", *Computerworld*, 22 de abril de 2010; Ed Bott, "McAfee Admits 'Inadequate' Quality Control Caused PC Meltdown", *ZDNet*, 22 de abril de 2010, y Barry McPherson, "An Update on False Positive Remediation", <http://siblog.mcafee.com/support/an-update-on-false-positive-remediation>, 22 de abril de 2010.

## PREGUNTAS DEL CASO DE ESTUDIO

## MIS EN ACCIÓN

1. ¿Qué factores de administración, organización y tecnología fueron responsables del problema de software de McAfee?
2. ¿Cuál fue el impacto de negocios de este problema de software, tanto para McAfee como para sus clientes?
3. Si fuera empleado empresarial de McAfee, ¿consideraría que la respuesta de la compañía al problema es aceptable? ¿Por qué sí o por qué no?
4. ¿Qué debería hacer McAfee en el futuro para evitar problemas similares?

Busque la disculpa en línea de Barry McPherson ("disculpa de Barry McPherson") y lea la reacción de los clientes. ¿Cree usted que la disculpa de McPherson ayudó o empeoró la situación? ¿Qué es un "remedio positivo falso"?

## 8.2 VALOR DE NEGOCIOS DE LA SEGURIDAD Y EL CONTROL

Muchas firmas se rehúsan a invertir mucho en seguridad debido a que no se relaciona de manera directa con los ingresos de ventas. Sin embargo, proteger los sistemas de información es algo tan imprescindible para la operación de la empresa que merece reconsiderarse.

Las compañías tienen activos de información muy valiosos por proteger. A menudo los sistemas alojan información confidencial sobre los impuestos de las personas, los activos financieros, los registros médicos y las revisiones del desempeño en el trabajo. También pueden contener información sobre operaciones corporativas; secretos de estado, planes de desarrollo de nuevos productos y estrategias de marketing. Los sistemas gubernamentales pueden almacenar información sobre sistemas de armamento, operaciones de inteligencia y objetivos militares. Estos activos de información tienen un tremendo valor, y las repercusiones pueden ser devastadoras si se pierden, destruyen o ponen en las manos equivocadas. Un estudio estimó que cuando se compromete la seguridad de una gran firma, la compañía pierde cerca del 2.1 por ciento de su valor del mercado en menos de dos días después de la fuga de seguridad, que se traduce en una pérdida promedio de \$1.65 mil millones en valor en el mercado bursátil por incidente (Cavusoglu, Mishra y Raghunathan, 2004).



Un control y seguridad inadecuados pueden provocar una responsabilidad legal grave. Los negocios deben proteger no sólo sus propios activos de información, sino también los de sus clientes, empleados y socios de negocios. Si no hicieran esto, las firmas podrían involucrarse en litigios costosos por exposición o robo de datos. Una organización puede ser considerada responsable de crear riesgos y daños innecesarios si no toma la acción protectora apropiada para evitar la pérdida de información confidencial, la corrupción de datos o la fuga de privacidad. Por ejemplo, La Comisión Federal de Comercio de Estados Unidos demandó a BJ's Wholesale Club por permitir que hackers accedieran a sus sistemas y robaran datos de tarjetas de crédito y débito para realizar compras fraudulentas. Los bancos que emitieron las tarjetas con los datos robados exigieron \$13 millones a BJ's como compensación por reembolsar a los tarjetahabientes las compras fraudulentas. Por ende, un marco de trabajo sólido de seguridad y control que proteja los activos de información de negocios puede producir un alto rendimiento sobre la inversión. Una seguridad y un control sólidos también incrementan la productividad de los empleados y reducen los costos de operación.

## REQUERIMIENTOS LEGALES Y REGULATORIOS PARA LA ADMINISTRACIÓN DE REGISTROS DIGITALES

Las recientes regulaciones gubernamentales de Estados Unidos están obligando a las compañías a considerar la seguridad y el control con más seriedad, al exigir que se protejan los datos contra el abuso, la exposición y el acceso sin autorización. Las firmas se enfrentan a nuevas obligaciones legales en cuanto a la retención, el almacenaje de registros electrónicos y la protección de la privacidad.

Si usted trabaja en la industria de servicios médicos, su firma tendrá que cumplir con la Ley de Responsabilidad y Portabilidad de los Seguros Médicos (HIPAA) de 1996. La **HIPAA** describe las reglas de seguridad y privacidad médica, además de los procedimientos para simplificar la administración de la facturación de servicios médicos y para automatizar la transferencia de datos sobre servicios médicos entre los proveedores de los servicios médicos, los contribuyentes y los planes. Requiere que los miembros de la industria de estos servicios retengan la información de los pacientes durante seis años y aseguren la confidencialidad de esos registros. Especifica estándares de privacidad, seguridad y transacciones electrónicas para los proveedores de servicios médicos que manejan la información de los pacientes; además establece penalizaciones por violar la privacidad médica, divulgar información sobre los registros de los pacientes por correo electrónico, o el acceso a la red sin autorización.

Si usted trabaja en una empresa que proporciona servicios financieros, su firma tendrá que cumplir con la Ley de Modernización de Servicios Financieros de 1999, mejor conocida como **Ley Gramm-Leach-Bliley** en honor de sus patrocinadores congresistas. Esta ley requiere que las instituciones financieras garanticen la seguridad y confidencialidad de los datos de los clientes. Los cuales se deben almacenar en un medio seguro y se deben implementar medidas de seguridad especiales para proteger dichos datos en los medios de almacenamiento y durante la transmisión.

Si usted trabaja en una compañía que cotiza en la bolsa, su compañía tendrá que cumplir con la Ley de Reforma de Contabilidad Pública de Compañías y Protección al Inversionista de 2002, mejor conocida como **Ley Sarbanes-Oxley** en honor a sus patrocinadores, el senador Paul Sarbanes de Maryland y el representante Michael Oxley de Ohio. Esta ley se diseñó para proteger a los inversionistas después de los escándalos financieros en Enron, WorldCom y otras compañías que cotizan en la bolsa. Impone una responsabilidad sobre las compañías y su gerencia para salvaguardar la precisión e integridad de la información financiera que se utiliza de manera interna y se libera en forma externa. Una de las Trayectorias de aprendizaje para este capítulo analiza la Ley Sarbanes-Oxley con detalle.

En esencia, Sarbanes-Oxley trata sobre asegurar que se implementen controles internos para gobernar la creación y documentación de la información en los estados financieros. Como se utilizan sistemas de información para generar, almacenar y transportar

dichos datos, la legislación requiere que las firmas consideren la seguridad de los sistemas de información y otros controles requeridos para asegurar la integridad, confidencialidad y precisión de sus datos. Cada aplicación de sistemas que trata con los datos críticos de los informes financieros requiere controles para asegurar que estos datos sean precisos. También son esenciales los controles para asegurar la red corporativa, para evitar el acceso sin autorización a los sistemas y datos, y para asegurar tanto la integridad como la disponibilidad de los datos en caso de desastre u otro tipo de interrupción del servicio.

## EVIDENCIA ELECTRÓNICA Y ANÁLISIS FORENSE DE SISTEMAS

La seguridad, el control y la administración de los registros digitales se han vuelto fundamentales para responder a las acciones legales. Gran parte de la evidencia actual para el fraude en la bolsa de valores, la malversación de fondos, el robo de secretos comerciales de la compañía, los delitos por computadora y muchos casos civiles se encuentra en formato digital. Además de la información de las páginas impresas o mecanografiadas, en la actualidad los casos legales dependen cada vez más de la evidencia que se representa en forma de datos digitales almacenados en discos flexibles portátiles, CD y discos duros de computadora, así como en correo electrónico, mensajes instantáneos y transacciones de correo electrónico a través de Internet. En la actualidad el correo electrónico es el tipo más común de evidencia electrónica.

En una acción legal, una empresa se ve obligada a responder a una solicitud de exhibición de pruebas para acceder a la información que se puede utilizar como evidencia, y la compañía debe por ley entregar esos datos. El costo de responder a una solicitud de exhibición de evidencia puede ser enorme si la compañía tiene problemas para ensamblar los datos, o si éstos están corrompidos o se destruyeron. Ahora los juzgados imponen serios castigos financieros y hasta penales por la destrucción inapropiada de documentos electrónicos.

Una política efectiva de retención de documentos electrónicos asegura que los documentos electrónicos, el correo electrónico y otros registros estén bien organizados, sean accesibles y no se retengan demasiado tiempo ni se descarten demasiado pronto. También refleja una conciencia en cuanto a cómo preservar la potencial evidencia para el **análisis forense de sistemas**, que viene siendo el proceso de recolectar, examinar, autenticar, preservar y analizar de manera científica los datos retenidos o recuperados de medios de almacenamiento de computadora, de tal forma que la información se pueda utilizar como evidencia en un juzgado. Se encarga de los siguientes problemas:

- Recuperar datos de las computadoras y preservar al mismo tiempo la integridad evidencial
- Almacenar y manejar con seguridad los datos electrónicos recuperados
- Encontrar información importante en un gran volumen de datos electrónicos
- Presentar la información a un juzgado

La evidencia electrónica puede residir en medios de almacenamiento de computadora, en forma de archivos de computadora y como *datos ambientales*, que no son visibles para el usuario promedio. Un ejemplo podría ser un archivo que se haya eliminado en un disco duro de PC. Los datos que un usuario tal vez haya borrado de un medio de almacenamiento de computadora se pueden recuperar por medio de varias técnicas. Los expertos de análisis forense de sistemas tratan de recuperar dichos datos ocultos para presentarlos como evidencia.

Sería conveniente que una firma tomara conciencia del análisis forense de sistemas para incorporarlo al proceso de planeación de contingencia. El CIO, los especialistas de seguridad, el personal de sistemas de información y los asesores legales corporativos deberían trabajar en conjunto para implementar un plan que se pueda ejecutar en caso de que surja una necesidad legal. En las Trayectorias de aprendizaje para este capítulo podrá averiguar más sobre el análisis forense de sistemas.



8.3

ESTABLECIMIENTO DE UN MARCO DE TRABAJO PARA LA SEGURIDAD Y EL CONTROL

Aún con las mejores herramientas de seguridad, sus sistemas de información no serán confiables y seguros a menos que sepa cómo y en dónde implementarlos. Necesitará saber en dónde está su compañía en riesgo y qué controles debe establecer para proteger sus sistemas de información. También tendrá que desarrollar una política de seguridad y planes para mantener su empresa en operación, en caso de que sus sistemas de información no estén funcionando.

CONTROLES DE LOS SISTEMAS DE INFORMACIÓN

Los controles de los sistemas de información pueden ser manuales y automatizados; consisten tanto de controles generales como de aplicación. Los **controles generales** gobiernan el diseño, la seguridad y el uso de los programas de computadora, además de la seguridad de los archivos de datos en general, a lo largo de toda la infraestructura de tecnología de la información de la organización. En conjunto, los controles generales se asignan a todas las aplicaciones computarizadas y consisten en una combinación de hardware, software y procedimientos manuales que crean un entorno de control en general.

Los controles generales cuentan con controles de software, controles de hardware físicos, controles de operaciones de computadora, controles de seguridad de datos, controles sobre la implementación de procesos de sistemas y controles administrativos. La tabla 8-3 describe las funciones de cada uno de estos controles.

Los **controles de aplicación** son controles específicos únicos para cada aplicación computarizada, como nómina o procesamiento de pedidos. Implican procedimientos tanto automatizados como manuales, los cuales aseguran que la aplicación procese de una forma completa y precisa sólo los datos autorizados. Los controles de aplicación se pueden clasificar como (1) controles de entrada, (2) controles de procesamiento y (3) controles de salida.

Los *controles de entrada* verifican la precisión e integridad de los datos cuando éstos entran al sistema. Hay controles de entrada específicos para autorización de la entrada, conversión de datos, edición de datos y manejo de errores. Los *controles de procesamiento* establecen que los datos sean completos y precisos durante la actualización. Los *controles de salida* aseguran que los resultados del procesamiento de

TABLA 8-3 CONTROLES GENERALES

TIPO DE CONTROL GENERAL	DESCRIPCIÓN
Controles de software	Monitorean el uso del software de sistemas y evitan el acceso no autorizado de los programas de software, el software de sistemas y los programas de computadora.
Controles de hardware	Aseguran que el hardware de computadora sea físicamente seguro y verifican las fallas del equipo. Las organizaciones que dependen mucho de sus computadoras también deben hacer provisiones para respaldos o una operación continua, de modo que puedan mantener un servicio constante.
Controles de operaciones de computadora	Supervisan el trabajo del departamento de computadoras para asegurar que los procedimientos programados se apliquen de manera consistente y correcta al almacenamiento y procesamiento de los datos. Implican controles sobre el establecimiento de trabajos de procesamiento de computadora y procedimientos de respaldo y recuperación para el procesamiento que termina en forma anormal.
Controles de seguridad de datos	Aseguran que los archivos de datos de negocios valiosos que se encuentren en disco o cinta no estén sujetos a un acceso sin autorización, no se modifiquen ni se destruyan mientras se encuentran en uso o almacenados.
Controles de implementación	Auditán el proceso de desarrollo de sistemas en varios puntos para asegurar que el proceso se controle y administre de manera apropiada.
Controles administrativos	Formalizan estándares, reglas, procedimientos y disciplinas de control para asegurar que los controles generales y de aplicación de la organización se ejecuten e implementen en forma apropiada.

computadora sean precisos, completos y se distribuyan de manera apropiada. En nuestras Trayectorias de aprendizaje aprenderá más sobre los controles de aplicación y generales.

## EVALUACIÓN DEL RIESGO

Antes de que su compañía consigne recursos a los controles de seguridad y sistemas de información, debe saber qué activos requieren protección y el grado de vulnerabilidad de éstos. Una evaluación del riesgo ayuda a responder estas preguntas y a determinar el conjunto más eficiente de controles para proteger activos.

Una **evaluación del riesgo** determina el nivel de riesgo para la firma si no se controla una actividad o proceso específico de manera apropiada. No todos los riesgos se pueden anticipar o medir, pero la mayoría de las empresas podrán adquirir cierta comprensión de los riesgos a los que se enfrentan. Los gerentes de información que trabajan con especialistas en sistemas de información deberían tratar de determinar el valor de los activos de información, los puntos de vulnerabilidad, la probable frecuencia de un problema y el potencial de daño. Por ejemplo, si es probable que un evento ocurra no más de una vez al año, con un máximo de una pérdida de \$1 000 para la organización, no es conveniente gastar \$20 000 en el diseño y mantenimiento de un control para protegerse contra ese evento. No obstante, si ese mismo evento podría ocurrir por lo menos una vez al día, con una pérdida potencial de más de \$300 000 al año, podría ser muy apropiado invertir \$100 000 en un control.

La tabla 8-4 ilustra los resultados de muestra de una evaluación del riesgo para un sistema de procesamiento de pedidos en línea que procesa 30 000 al día. La probabilidad de que cada riesgo ocurra durante un periodo de un año se expresa como un porcentaje. La siguiente columna muestra los niveles más alto y más bajo posibles de pérdidas que se podrían esperar cada vez que ocurriera el riesgo, además de una pérdida promedio que se calcula al sumar las cifras tanto mayor como menor y dividir el resultado entre dos. La pérdida anual esperada para cada riesgo se puede determinar al multiplicar la pérdida promedio por su probabilidad de ocurrencia.

Esta evaluación del riesgo muestra que la probabilidad de que ocurra una falla de energía eléctrica en un periodo de un año es del 30 por ciento. La pérdida de transacciones de pedidos mientras no hay energía podría variar de \$5 000 a \$200 000 (lo cual da un promedio de \$102 500) por cada ocurrencia, dependiendo de cuánto tiempo esté detenido el procesamiento. La probabilidad de que ocurra una malversación de fondos durante un periodo de un año es de cerca del 5 por ciento, con pérdidas potenciales que varían entre \$1 000 y \$50 000 (lo que da un promedio de \$25 500) por cada ocurrencia. La probabilidad de que ocurran errores de los usuarios durante un periodo de un año es del 98 por ciento, con pérdidas entre \$200 y \$40 000 (para un promedio de \$20 100) por cada ocurrencia.

Una vez que se hayan evaluado los riesgos, los desarrolladores del sistema se concentrarán en los puntos de control con la mayor vulnerabilidad y potencial de pérdida. En este caso, los controles se deberían enfocar en las formas para minimizar el riesgo de fallas de energía eléctrica y errores de los usuarios, ya que las pérdidas anuales anticipadas son mayores en estas áreas.

**TABLA 8-4 EVALUACIÓN DEL RIESGO PARA EL PROCESAMIENTO DE PEDIDOS EN LÍNEA**

RIESGO	PROBABILIDAD DE OCURRENCIA (%)	RANGO DE PÉRDIDAS/ PROMEDIO (\$)	PÉRDIDA ANUAL ESPERADA (\$)
Falla de energía eléctrica	30%	\$5 000–\$200 000 (\$102 500)	\$30 750
Malversación de fondos	5%	\$1 000–\$50 000 (\$25 500)	\$1 275
Error de los usuarios	98%	\$200–\$40 000 (\$20 100)	\$19 698

## POLÍTICA DE SEGURIDAD

Una vez que identifique los principales riesgos para sus sistemas, su compañía tendrá que desarrollar una política de seguridad para proteger sus activos. Una **política de seguridad** consiste de enunciados que clasifican los riesgos de información, identifican los objetivos de seguridad aceptables y también los mecanismos para lograr estos objetivos. ¿Cuáles son los activos de información más importantes de la firma? ¿Quién genera y controla esa información en la empresa? ¿Cuáles son las políticas de seguridad que se implementan para proteger esa información? ¿Qué nivel de riesgo está dispuesta la gerencia a aceptar para cada uno de estos activos? ¿Acaso está dispuesta a perder los datos crediticios de sus clientes una vez cada 10 años? ¿O creará un sistema de seguridad para datos de tarjetas de crédito que pueda soportar al desastre una vez cada 100 años? La gerencia debe estimar qué tanto costará lograr este nivel de riesgo aceptable.

La política de seguridad controla las políticas que determinan el uso aceptable de los recursos de información de la firma y qué miembros de la compañía tienen acceso a sus activos de información. Una **política de uso aceptable (AUP)** define los usos admisibles de los recursos de información y el equipo de cómputo de la firma, que incluye las computadoras laptop y de escritorio, los dispositivos inalámbricos e Internet. La política debe clarificar la política de la compañía con respecto a la privacidad, la responsabilidad de los usuarios y el uso personal tanto del equipo como de las redes de la compañía. Una buena AUP define las acciones inaceptables y aceptables para cada usuario, además de especificar las consecuencias si no se lleva a cabo. Por ejemplo, la política de seguridad en Unilever, la gigantesca compañía multinacional de productos para el consumidor, requiere que cada empleado equipado con una laptop o dispositivo móvil de bolsillo utilice un dispositivo especificado por la compañía y emplee una contraseña u otro método de identificación al iniciar sesión en la red corporativa.

La política de seguridad también comprende de provisiones para administrar la identidad. La **administración de identidad** consiste en los procesos de negocios y las herramientas de software para identificar a los usuarios válidos de un sistema, y para controlar su acceso a los recursos del mismo. Involucra las políticas para identificar y autorizar a distintas categorías de usuarios del sistema, especificar los sistemas o partes de los mismos a los que cada usuario puede acceder, además de los procesos y las tecnologías para autenticar usuarios y proteger sus identidades.

La figura 8-3 es un ejemplo de cómo podría un sistema de administración de identidad capturar las reglas de acceso para los distintos niveles de usuarios en la función de recursos humanos. Especifica las porciones de una base de datos de recursos humanos a las que puede acceder cada usuario, con base en la información requerida para realizar el trabajo de esa persona. La base de datos contiene información personal confidencial, como los salarios, beneficios e historiales médicos de los empleados.

Las reglas de acceso que se ilustran aquí son para dos conjuntos de usuarios. Uno de esos conjuntos consiste en todos los empleados que realizan funciones de oficina, como introducir datos de los empleados en el sistema. Todos los individuos con este tipo de perfil pueden actualizar el sistema, pero no pueden leer ni actualizar los campos delicados, como el salario, el historial médico o los datos sobre los ingresos. Otro perfil se aplica a un gerente de división, que no puede actualizar el sistema pero sí leer todos los campos de datos de los empleados de su división, entre ellos el historial médico y el salario. Más adelante en este capítulo proveeremos más detalles sobre las tecnologías para la autenticación de los usuarios.

## PLANIFICACIÓN DE RECUPERACIÓN DE DESASTRES Y PLANIFICACIÓN DE LA CONTINUIDAD DE NEGOCIOS

Si opera una empresa, necesita planificar los eventos, como los cortes en el suministro eléctrico, las inundaciones, los terremotos o los ataques terroristas que evitarán que sus sistemas de información y su empresa puedan operar. La **planificación de recupera-**

**FIGURA 8-3 REGLAS DE ACCESO PARA UN SISTEMA DE PERSONAL**

PERFIL DE SEGURIDAD 1	
Usuario: Empleado del depto. de personal	
Ubicación: División 1	
Códigos de identificación de empleado con este perfil:	00753, 27834, 37665, 44116
Restricciones de los campos de datos	Tipo de acceso
Todos los datos de los empleados sólo para la División 1	Leer y actualizar
<ul style="list-style-type: none"> <li>• Datos de historial médico</li> <li>• Salario</li> <li>• Ingresos pensionables</li> </ul>	Ninguno Ninguno Ninguno

PERFIL DE SEGURIDAD 2	
Usuario: Gerente de personal divisional	
Ubicación: División 1	
Códigos de identificación de empleado con este perfil:	27321
Restricciones de los campos de datos	Tipo de acceso
Todos los datos de los empleados sólo para la División 1	Sólo lectura

Estos dos ejemplos representan dos perfiles de seguridad o patrones de seguridad de datos que se podrían encontrar en un sistema de personal. Dependiendo de las reglas de acceso, un usuario tendría ciertas restricciones sobre el acceso a varios sistemas, ubicaciones o datos en una organización.

**ción de desastres** idea planes para restaurar los servicios de cómputo y comunicaciones después de haberse interrumpido. El principal enfoque de los planes de recuperación de desastres es en los aspectos técnicos involucrados en mantener los sistemas en funcionamiento, tales como qué archivos respaldar y el mantenimiento de los sistemas de cómputo de respaldo o los servicios de recuperación de desastres.

Por ejemplo, MasterCard mantiene un centro de cómputo duplicado en Kansas City, Missouri, que sirve como respaldo de emergencia para su centro de cómputo primario en St. Louis. En vez de construir sus propias instalaciones de respaldo, muchas firmas se contactan con compañías de recuperación de desastres, como Comdisco Disaster Recovery Services en Rosemont, Illinois, y SunGard Availability Services, que tiene sus oficinas generales en Wayne, Pennsylvania. Estas compañías de recuperación de desastres proveen sitios activos con computadoras de repuesto en ubicaciones alrededor del mundo, en donde las firmas suscriptoras pueden ejecutar sus aplicaciones críticas en caso de emergencia. Por ejemplo, Champion Technologies, que suministra productos químicos para utilizar en operaciones de petróleo y gas, puede cambiar sus sistemas empresariales de Houston a un sitio activo SunGard en Scottsdale, Arizona, en sólo dos horas.

La **planificación de continuidad de negocios** se enfoca en la forma en que la compañía puede restaurar las operaciones de negocios después de que ocurre un desastre. El plan de continuidad de negocios identifica los procesos de negocios críticos y determina los planes de acción para manejar las funciones de misión crítica en caso de que fallen los sistemas. Por ejemplo, el Deutsche Bank, que provee servicios de banca de inversiones y de administración de activos en 74 países distintos, tiene un plan bien desarrollado de continuidad de negocios que actualiza y refina en forma continua. Mantiene equipos de tiempo completo en Singapur, Hong Kong, Japón, India y Australia para coordinar planes que tratan con la pérdida de instalaciones, personal o sistemas

críticos, de modo que la compañía pueda seguir operando cuando ocurra un evento catastrófico. El plan de Deutsche Bank hace la diferencia entre los procesos que son críticos para la supervivencia de los negocios y aquellos que son críticos para el apoyo en las crisis, y se coordina con la planificación de recuperación de desastres para los centros de cómputo de la compañía.

Los gerentes de negocios y los especialistas en tecnología de la información necesitan trabajar juntos en ambos tipos de planes para determinar qué sistemas y procesos de negocios son más críticos para la compañía. Deben realizar un análisis de impacto comercial para identificar los sistemas más críticos de la firma, además del impacto que tendría una falla de los sistemas en la empresa. La gerencia debe determinar la máxima cantidad de tiempo que puede sobrevivir la empresa con sus sistemas inactivos y qué partes de la empresa se deben restaurar primero.

## LA FUNCIÓN DE LA AUDITORÍA

¿Cómo sabe la gerencia que la seguridad y los controles de los sistemas de información son efectivos? Para responder a esta pregunta, las organizaciones deben llevar a cabo auditorías exhaustivas y sistemáticas. Una **auditoría de MIS** examina el entorno de seguridad general de la firma, además de controlar el gobierno de los sistemas de información individuales. El auditor debe rastrear el flujo de transacciones de ejemplo a través del sistema y realizar pruebas, mediante el uso (si es apropiado) de software de auditoría automatizado. La auditoría de MIS también puede examinar la calidad de los datos.

Las auditorías de seguridad revisan las tecnologías, los procedimientos, la documentación, la capacitación y el personal. Una auditoría detallada puede incluso simular un ataque o desastre para evaluar la respuesta de la tecnología, el personal de sistemas de información y los empleados de la empresa.

La auditoría lista y clasifica todas las debilidades de control; además estima la probabilidad de su ocurrencia. Después evalúa el impacto financiero y organizacional de cada amenaza. La figura 8-4 es el listado de ejemplo de un auditor sobre las debilidades de control para un sistema de préstamos. Contiene una sección para notificar a la gerencia sobre dichas debilidades y para la respuesta de la gerencia. Se espera que la gerencia idee un plan para contrarrestar las debilidades considerables en los controles.

### 8.4

## TECNOLOGÍAS Y HERRAMIENTAS PARA PROTEGER LOS RECURSOS DE INFORMACIÓN

Las empresas cuentan con una variedad de tecnologías para proteger sus recursos de información, tales como herramientas para administrar las identidades de los usuarios, evitar el acceso no autorizado a los sistemas y datos, asegurar la disponibilidad del sistema y asegurar la calidad del software.

## ADMINISTRACIÓN DE LA IDENTIDAD Y LA AUTENTICACIÓN

Las compañías grandes y de tamaño mediano tienen infraestructuras de TI complejas y muchos sistemas distintos, cada uno con su propio conjunto de usuarios. El software de administración de identidad automatiza el proceso de llevar el registro de todos estos usuarios y sus privilegios de sistemas, ya que asigna a cada usuario una identidad digital única para acceder a cada sistema. También tiene herramientas para autenticar usuarios, proteger las identidades de los usuarios y controlar el acceso a los recursos del sistema.

Para obtener acceso a un sistema, es necesario que el usuario tenga autorización y esté autenticado. La **autenticación** se refiere a la habilidad de saber que una persona es

**FIGURA 8-4 LISTA DE EJEMPLO DE UN AUDITOR SOBRE LAS DEBILIDADES DE LOS CONTROLES**

Función: Préstamos Ubicación: Peoria, IL		Preparado por: J. Ericson Fecha: 16 de junio de 2011		Recibido por: T. Benson Fecha de revisión: 28 de junio de 2011	
Naturaleza de la debilidad y el impacto	Probabilidad de error/abuso		Notificación a la gerencia		
	Sí/ No	Justificación	Fecha del informe	Respuesta de la gerencia	
Contraseñas faltantes en cuentas de usuarios	Sí	Deja el sistema abierto a personas externas no autorizadas o atacantes	5/10/11	Eliminar cuentas sin contraseñas	
La red está configurada para permitir compartir ciertos archivos del sistema	Sí	Expone los archivos de sistema críticos a partes hostiles conectadas a la red	5/10/11	Asegurar que sólo los directorios requeridos estén compartidos y protegidos con contraseñas sólidas	
Los parches de software pueden actualizar los programas de producción sin la aprobación final del grupo de estándares y controles	No	Todos los programas de producción requieren la aprobación de la gerencia; el grupo de estándares y controles asigna dichos casos a un estado de producción temporal			

Este diagrama es una página de ejemplo de una lista de debilidades de control que un auditor podría encontrar en un sistema de préstamos de un banco comercial local. Este formulario ayuda a los auditores a registrar y evaluar las debilidades de control, además de mostrar los resultados de analizar esas debilidades con la gerencia, así como cualquier acción correctiva que realice la gerencia.

quien dice ser. La forma más común de establecer la autenticación es mediante el uso de **contraseñas** que sólo conocen los usuarios autorizados. Un usuario final utiliza una contraseña para iniciar sesión en un sistema computacional y también puede usar contraseñas para acceder a sistemas y archivos específicos. Sin embargo, es común que los usuarios olviden las contraseñas, las compartan o elijan contraseñas inadecuadas que sean fáciles de adivinar, lo cual compromete la seguridad. Los sistemas de contraseñas que son demasiado rigurosos entorpecen la productividad de los empleados. Cuando éstos deben cambiar contraseñas complejas con frecuencia, es común que tomen atajos tales como elegir contraseñas que sean fáciles de adivinar, o escribirlas en sus estaciones de trabajo, a simple vista. También es posible “husmear” las contraseñas si se transmiten a través de una red o se roban por medio de la ingeniería social.

Las nuevas tecnologías de autenticación, como los tokens, las tarjetas inteligentes y la autenticación biométrica, solucionan algunos de estos problemas. Un **token** es un dispositivo físico, similar a una tarjeta de identificación, que está diseñado para demostrar la identidad de un solo usuario. Los tokens son pequeños gadgets que por lo general se colocan en los llaveros y muestran códigos de contraseña que cambian con frecuencia. Una **tarjeta inteligente** es un dispositivo con un tamaño aproximado al de una tarjeta de crédito, que contiene un chip formateado con permiso de acceso y otros datos (las tarjetas inteligentes también se utilizan en los sistemas de pago electrónico). Un dispositivo lector interpreta los datos en la tarjeta inteligente y permite o niega el acceso.

La **autenticación biométrica** usa sistemas que leen e interpretan rasgos humanos individuales, como las huellas digitales, el iris de los ojos y las voces, para poder otorgar o negar el acceso. La autenticación biométrica se basa en la medición de un rasgo físico o del comportamiento que hace a cada individuo único. Compara las características únicas de una persona, como las huellas digitales el rostro o la imagen de la retina, con un



perfil almacenado de estas características para determinar si hay alguna diferencia entre las características y el perfil guardado. Si los dos perfiles coinciden, se otorga el acceso. Las tecnologías de reconocimiento de huellas digitales y rostros apenas se están empezando a utilizar para aplicaciones de seguridad; hay muchas PC tipo laptop equipadas con dispositivos de identificación de huellas digitales y varios modelos con cámaras Web integradas, además del software de reconocimiento de rostro.

## **FIREWALLS, SISTEMAS DE DETECCIÓN DE INTRUSOS Y SOFTWARE ANTIVIRUS**

Sin protección contra el malware y los intrusos, sería muy peligroso conectarse a Internet. Los firewalls, los sistemas de detección de intrusos y el software antivirus se han vuelto herramientas de negocios esenciales.

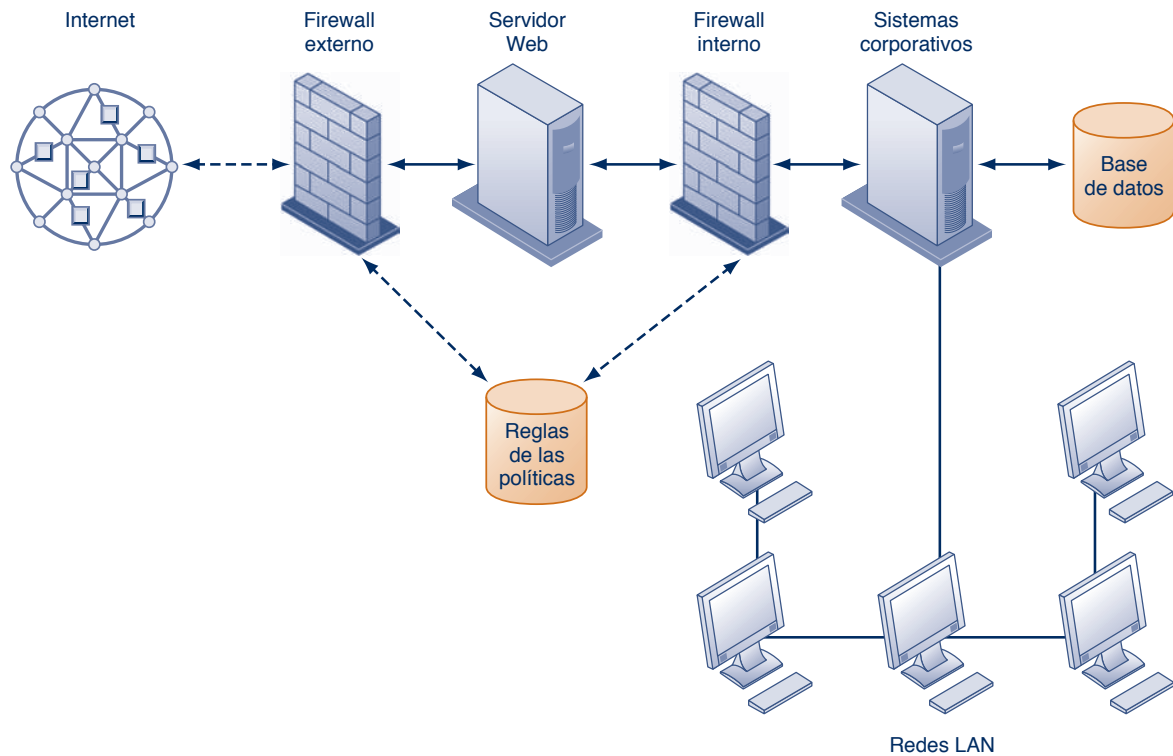
### **Firewalls**

Los **firewalls** evitan que los usuarios sin autorización accedan a redes privadas. Un firewall es una combinación de hardware y software que controla el flujo de tráfico de red entrante y saliente. Por lo general se colocan entre las redes internas privadas de la organización y las redes externas que no son de confianza como Internet, aunque también se pueden utilizar firewalls para proteger una parte de la red de una compañía del resto de la red (vea la figura 8-5).

El firewall actúa como un portero que examina las credenciales de cada usuario antes de otorgar el acceso a una red. Identifica nombres, direcciones IP, aplicaciones y otras características del tráfico entrante. Verifica esta información y la compara con las reglas de acceso que el administrador de red tiene programadas en el sistema. El firewall evita la comunicación sin autorización que entra a la red y sale de ella.

En organizaciones grandes, es común que el firewall resida en una computadora designada de forma especial y separada del resto de la red, de modo que ninguna solicitud entrante acceda de manera directa a los recursos de la red privada. Existen varias tecnologías de filtrado de firewall, como el filtrado de paquete estático, la inspección con estado, la Traducción de direcciones de red (NAT) y el filtrado de proxy de aplicación. Se utilizan con frecuencia en combinación para proveer protección de firewall.

**FIGURA 8-5 UN FIREWALL CORPORATIVO**



El firewall se coloca entre la red privada de la firma y la red Internet pública u otra red que no sea de confianza, para proteger contra el tráfico no autorizado.

El *filtrado de paquetes* examina ciertos campos en los encabezados de los paquetes de datos que van y vienen entre la red de confianza e Internet; se examinan paquetes individuales aislados. Esta tecnología de filtrado puede pasar por alto muchos tipos de ataques. La *inspección con estado* provee una seguridad adicional al determinar si los paquetes forman parte de un diálogo continuo entre un emisor y un receptor. Establece tablas de estado para rastrear la información a través de varios paquetes. Los paquetes se aceptan o rechazan con base en si forman o no parte de una conversación aprobada, o si tratan o no de establecer una conexión legítima.

La *traducción de direcciones de red* (NAT) puede proveer otra capa de protección cuando se emplean el filtrado de paquetes estáticos y la inspección con estado. NAT oculta las direcciones IP de la(s) computadora(s) host interna(s) de la organización para evitar que los programas husmeadores, que están fuera del firewall, las puedan descubrir y utilicen esa información para penetrar en los sistemas internos.

El *filtrado de proxy de aplicación* examina el contenido de los paquetes relacionado con aplicaciones. Un servidor proxy detiene los paquetes de datos que se originan fuera de la organización, los inspecciona y pasa un proxy al otro lado del firewall. Si un usuario que esté fuera de la compañía desea comunicarse con un usuario dentro de la organización, el usuario externo primero “habla” con la aplicación proxy y ésta se comunica con la computadora interna de la firma. De igual forma, un usuario de computadora dentro de la organización tiene que pasar por un proxy para hablar con las computadoras en el exterior.

Para crear un buen firewall, un administrador debe mantener reglas internas detalladas que identifiquen a las personas, aplicaciones o direcciones que se permiten o rechazan. Los firewalls pueden impedir, pero no prevenir por completo, que usuarios externos penetren la red, por lo cual se deben tener en cuenta como un elemento en un plan de seguridad general.

### Sistemas de detección de intrusos

Además de los firewalls, en la actualidad los distribuidores de seguridad comercial proveen herramientas de detección de intrusos y servicios para proteger contra el tráfico de red sospechoso y los intentos de acceder a los archivos y las bases de datos. Los **sistemas de detección de intrusos** contienen herramientas de monitoreo de tiempo completo que se colocan en los puntos más vulnerables, o “puntos activos” de las redes corporativas, para detectar y evadir a los intrusos de manera continua. El sistema genera una alarma si encuentra un evento sospechoso o anormal. El software de exploración busca patrones que indiquen métodos conocidos de ataques por computadora, como malas contraseñas, verifica que no se hayan eliminado o modificado archivos importantes, y envía advertencias de vandalismo o errores de administración de sistemas. El software de monitoreo examina los eventos a medida que ocurren para descubrir ataques de seguridad en progreso. La herramienta de detección de intrusos también se puede personalizar para desconectar una parte muy delicada de una red en caso de que reciba tráfico no autorizado.

### Software antivirus y antispyware

Los planes de tecnología defensivos tanto para individuos como para empresas deben contar con protección antivirus para cada computadora. El **software antivirus** está diseñado para revisar los sistemas computacionales y las unidades en busca de la presencia de virus de computadora. Por lo general, el software elimina el virus del área infectada. Sin embargo, la mayoría del software antivirus es efectivo sólo contra virus que ya se conocían a la hora de escribir el software. Para que siga siendo efectivo, hay que actualizar el software antivirus en forma continua. Hay productos antivirus disponibles para muchos tipos distintos de dispositivos móviles y de bolsillo además de los servidores, las estaciones de trabajo y las PC de escritorio.

Los principales distribuidores de software antivirus, como McAfee, Symantec y Trend Micro, han mejorado sus productos para incluir protección contra spyware. Las herramientas de software antispyware como Ad-Aware, Spybot S&D y Spyware Doctor son también de mucha utilidad.

### Sistemas de administración unificada de amenazas

Para ayudar a las empresas a reducir costos y mejorar la capacidad de administración, los distribuidores de seguridad han combinado varias herramientas de seguridad en un solo paquete, que ofrece firewalls, redes privadas virtuales, sistemas de detección de intrusos y software de filtrado de contenido Web y antispam. Estos productos de administración de seguridad completos se conocen como sistemas de **administración unificada de amenazas (UTM)**. Aunque en un principio estaban dirigidos a las empresas pequeñas y de tamaño mediano, hay productos UTM disponibles para redes de todos tamaños. Los principales distribuidores de UTM son Crossbeam, Fortinet y Check Point; los distribuidores de redes tales como Cisco Systems y Juniper Networks proveen ciertas capacidades de UTM en su equipo.

## SEGURIDAD EN LAS REDES INALÁMBRICAS

A pesar de sus fallas, WEP ofrece cierto margen de seguridad si los usuarios de Wi-Fi recuerdan activarla. Un primer paso sencillo para frustrar la intención de los hackers es asignar un nombre único al SSID de su red e instruir a su enrutador para que no lo transmita. Las corporaciones pueden mejorar aún más la seguridad Wi-Fi si utilizan WEP junto con la tecnología de redes privadas virtuales (VPN) para acceder a los datos corporativos internos.

En junio de 2004, el grupo industrial y comercial Alianza Wi-Fi finalizó la especificación 802.11i (también conocida como Acceso Wi-Fi protegido 2 o WPA2), la cual sustituye a WEP con estándares de seguridad más sólidos. En vez de las claves de cifrado estáticas que se utilizan en WEP, el nuevo estándar usa claves mucho más extensas que cambian de manera continua, lo cual dificulta aún más el que alguien pueda descifrar-

las. Además emplea un sistema de autenticación cifrado con un servidor de autenticación central, para asegurar que sólo los usuarios autorizados accedan a la red.

## CIFRADO E INFRAESTRUCTURA DE CLAVE PÚBLICA

Muchas empresas usan el cifrado para proteger la información digital que almacenan, transfieren por medios físicos o envían a través de Internet. El **cifrado** es el proceso de transformar texto o datos simples en texto cifrado que no pueda leer nadie más que el emisor y el receptor deseado. Para cifrar los datos se utiliza un código numérico secreto, conocido como clave de cifrado, que transforma los datos simples en texto cifrado. El receptor debe descifrar el mensaje.

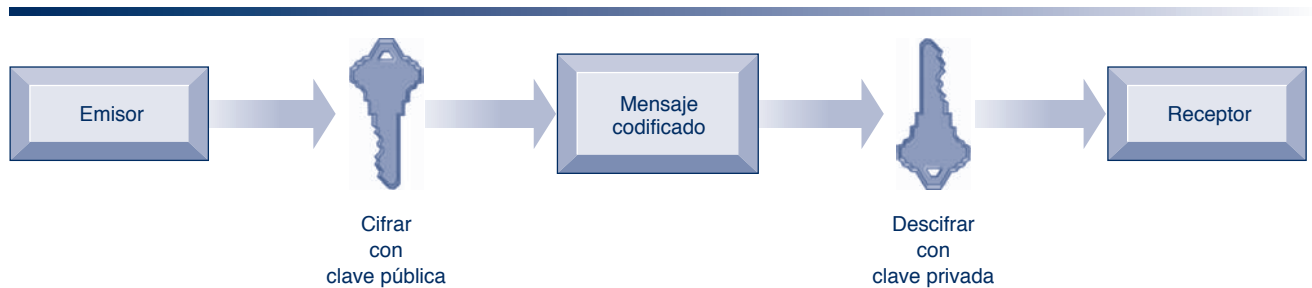
Los dos métodos para cifrar el tráfico de red en Web son SSL y S-HTTP. La **capa de sockets seguros (SSL)** y su sucesor, seguridad de la capa de transporte (TLS), permiten que las computadoras cliente y servidor manejen las actividades de cifrado y descifrado a medida que se comunican entre sí durante una sesión Web segura. El **protocolo de transferencia de hipertexto seguro (S-HTTP)** es otro protocolo que se utiliza para cifrar los datos que fluyen a través de Internet, pero se limita a mensajes individuales, mientras que SSL y TLS están diseñados para establecer una conexión segura entre dos computadoras.

La capacidad de generar sesiones seguras está integrada en el software navegador cliente de Internet y los servidores. El cliente y el servidor negocian qué clave y nivel de seguridad utilizar. Una vez que se establece una sesión segura entre el cliente y el servidor, todos los mensajes en esa sesión se cifran.

Existen dos métodos alternativos de cifrado: cifrado de clave simétrica y cifrado de clave pública. En el cifrado de clave simétrica, el emisor y el receptor establecen una sesión segura en Internet al crear una sola clave de cifrado y enviarla al receptor, de modo que tanto el emisor como el receptor compartan la misma clave. La solidez de la clave de cifrado se mide con base en su longitud de bits. En la actualidad, una clave común es de 128 bits de longitud (una cadena de 128 dígitos binarios).

El problema con todos los esquemas de cifrado simétrico es que la clave en sí se debe compartir de alguna forma entre los emisores y receptores, por lo cual queda expuesta a personas externas que tal vez puedan interceptarla y descifrarla. Una forma más segura de cifrado conocida como **cifrado de clave pública** utiliza dos claves: una compartida (o pública) y otra por completo privada, como se muestra en la figura 8-6. Las claves están relacionadas en sentido matemático, de modo que los datos cifrados con una clave se puedan descifrar sólo mediante la otra clave. Para enviar y recibir mensajes,

**FIGURA 8-6** CIFRADO DE CLAVE PÚBLICA



Un sistema de cifrado de clave pública se puede ver como una serie de claves públicas y privadas que bloquean los datos al transmitirlos y los desbloquean al recibirlos. El emisor localiza la clave pública del receptor en un directorio y la utiliza para cifrar un mensaje. El cual se envía en forma cifrada a través de Internet o de una red privada. Cuando llega el mensaje cifrado, el receptor usa su clave privada para descifrar los datos y leer el mensaje.

los comunicadores primero crean pares separados de claves privadas y públicas. La clave pública se conserva en un directorio y la privada se debe mantener secreta. El emisor cifra un mensaje con la clave pública del receptor. Al recibir el mensaje, el receptor usa su propia clave privada para descifrarlo.

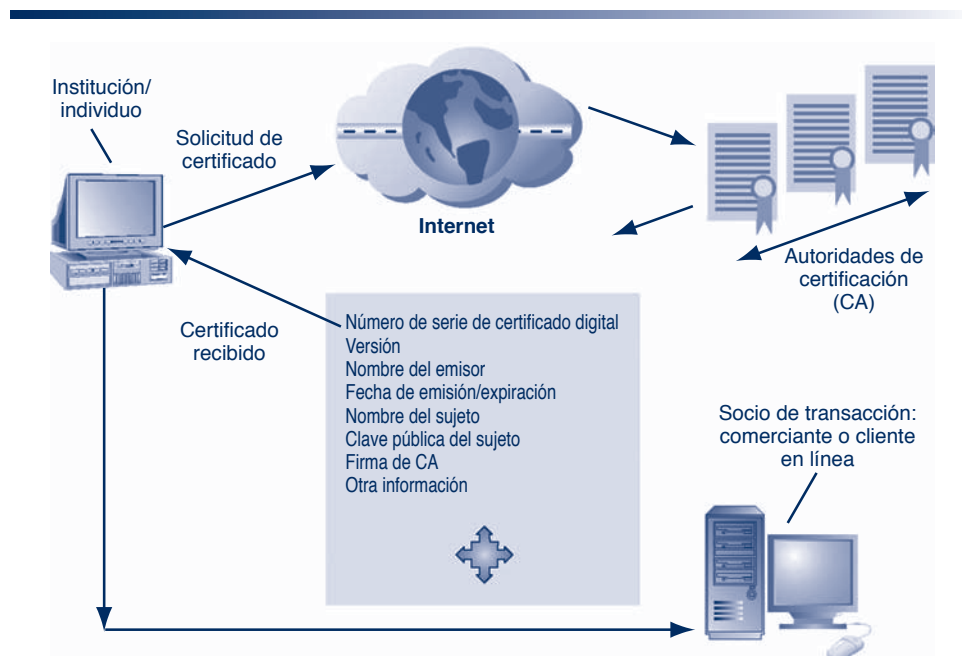
Los **certificados digitales** son archivos de datos que se utilizan para establecer la identidad de los usuarios y los activos electrónicos para proteger las transacciones en línea (vea la figura 8-7). Un sistema de certificados digitales utiliza una tercera parte de confianza, conocida como autoridad de certificado (CA, o autoridad de certificación), para validar la identidad de un usuario. Existen muchas CA en Estados Unidos y alrededor del mundo, como VeriSign, IdenTrust y KeyPost de Australia.

La CA verifica la identidad de un usuario del certificado digital desconectada de Internet. Esta información se coloca en un servidor de CA, el cual genera un certificado digital cifrado que contiene información de identificación del propietario y una copia de su clave pública. El certificado autentica que la clave pública pertenece al propietario designado. La CA hace que su propia clave esté disponible en forma pública, ya sea en papel o tal vez en Internet. El receptor de un mensaje cifrado utiliza la clave pública de la CA para decodificar el certificado digital adjunto al mensaje, verifica que lo haya emitido la CA y después obtiene la clave pública del emisor además de la información de identificación contenida en el certificado. Al usar esta información, el receptor puede enviar una respuesta cifrada. El sistema de certificados digitales permitiría, por ejemplo, que un usuario de tarjeta de crédito y un comerciante validaran que sus certificados digitales hayan sido emitidos por una tercera parte autorizada y de confianza, antes de intercambiar datos. La **infraestructura de clave pública (PKI)**, el uso de la criptografía de clave pública para trabajar con una CA, en la actualidad se utiliza mucho para el comercio electrónico.

## ASEGURAMIENTO DE LA DISPONIBILIDAD DEL SISTEMA

A medida que las compañías dependen cada vez más de las redes digitales para obtener ingresos y operaciones, necesitan realizar ciertos pasos adicionales para asegurar que sus sistemas y aplicaciones estén siempre disponibles. Las firmas como las que están en el ámbito de las industrias de servicios financieros y las aerolíneas, en donde las aplica-

**FIGURA 8-7 CERTIFICADOS DIGITALES**



Los certificados digitales ayudan a establecer la identidad de las personas o activos electrónicos. Protegen las transacciones en línea al proveer una comunicación en línea segura y cifrada.

ciones requieren el procesamiento de transacciones en línea, han usado desde hace varios años los sistemas computacionales tolerantes a fallas para asegurar una disponibilidad del 100 por ciento. En el **procesamiento de transacciones en línea**, la computadora procesa de inmediato las transacciones que se realizan en línea. Los cambios multitudinarios en las bases de datos, los informes y las solicitudes de información ocurren a cada instante.

Los **sistemas de computadora tolerantes a fallas** contienen componentes redundantes de hardware, software y suministro de energía que crean un entorno en donde se provee un servicio continuo sin interrupciones. Las computadoras tolerantes a fallas utilizan rutinas especiales de software o lógica de autocomprobación integrada en sus circuitos para detectar fallas de hardware y cambiar de manera automática a un dispositivo de respaldo. Las piezas de estas computadoras se pueden quitar y reparar sin interrupciones en el sistema computacional.

Hay que establecer la diferencia entre la tolerancia a fallas y la **computación de alta disponibilidad**. Tanto la tolerancia a fallas como la computación de alta disponibilidad tratan de minimizar el **tiempo de inactividad**: periodos de tiempo en los que un sistema no está en funcionamiento. Sin embargo, la computación de alta disponibilidad ayuda a las firmas a recuperarse con rapidez de un desastre en el sistema, mientras que la tolerancia a fallas promete tanto la disponibilidad continua como la eliminación del tiempo de recuperación.

Los entornos de computación de alta disponibilidad son un requerimiento mínimo para las firmas con mucho procesamiento de datos relacionados con el comercio electrónico, o para las firmas que dependen de las redes digitales para sus operaciones internas. La computación de alta disponibilidad requiere servidores de respaldo, la distribución del procesamiento entre varios servidores, almacenamiento de alta capacidad y planes convenientes de recuperación de desastres y continuidad de negocios. La plataforma computacional de la firma debe ser en extremo robusta, con capacidad de escalar el poder de procesamiento, el almacenamiento y el ancho de banda.

Los investigadores están explorando formas de hacer que los sistemas computacionales se recuperen aún con más rapidez cuando ocurran percances, algo que se conoce como **computación orientada a la recuperación**. Trabajo que consiste en diseñar sistemas que se recuperen con rapidez, además de la implementación de capacidades y herramientas para ayudar a los operadores a señalar los orígenes de las fallas en los sistemas con muchos componentes, para poder corregir sus errores con facilidad.

## Control del tráfico de red: inspección profunda de paquetes (DPI)

¿Alguna vez al intentar usar la red de su campus se encontró con que estaba muy lenta? Esto se puede deber a que sus compañeros estudiantes utilizan la red para descargar música o ver YouTube. Las aplicaciones que consumen ancho de banda, como los programas de procesamiento de archivos, el servicio telefónico por Internet y el video en línea, son capaces de obstruir y reducir la velocidad de las redes corporativas, lo cual degrada su desempeño. Por ejemplo, la Universidad Ball State en Muncie, Indiana, descubrió que su red estaba lenta debido a que una pequeña minoría de estudiantes utilizaba programas de compartición de archivos de igual a igual para descargar películas y música.

Una tecnología conocida como **inspección profunda de paquetes (DPI)** ayuda a resolver este problema. DPI examina los archivos de datos y ordena el material en línea de baja prioridad mientras asigna mayor prioridad a los archivos críticos para la empresa. Con base en las prioridades establecidas por los operadores de una red, decide si un paquete de datos específico puede continuar hacia su destino, o si hay que bloquearlo o retrasarlo mientras avanza el tráfico más importante. Mediante el uso de un sistema DPI de Allot Communications, la Universidad Ball State pudo tapar la cantidad de tráfico de compartición de archivos y asignarle una prioridad mucho menor. Por ende, el tráfico de red preferido de Ball State se agilizó.

## Subcontratación (outsourcing) de la seguridad

Muchas compañías, en especial las pequeñas empresas, carecen de los recursos o la experiencia para proveer un entorno de computación seguro de alta disponibilidad por su cuenta. Por fortuna, pueden subcontratar muchas funciones de seguridad con **proveedores de servicios de seguridad administrados (MSSP)**, quienes monitorean la actividad de



la red y realizan pruebas de vulnerabilidad, además de detección de intrusos. SecureWorks, BT Managed Security Solutions Group y Symantec son los principales proveedores de servicios MSSP.

## **ASPECTOS DE SEGURIDAD PARA LA COMPUTACIÓN EN LA NUBE Y LA PLATAFORMA DIGITAL MÓVIL**

Aunque la computación en la nube y la plataforma digital móvil emergente tienen el potencial de producir beneficios poderosos, imponen nuevos desafíos para la seguridad y confiabilidad de los sistemas. Ahora describiremos algunos de estos desafíos y cómo hay que lidiar con ellos.

### **Seguridad en la nube**

Cuando el procesamiento se lleva a cabo en la nube, la rendición de cuentas y la responsabilidad de proteger los datos confidenciales aún recae en la compañía que posee esos datos. Es imprescindible comprender cómo es que el proveedor de computación en la nube organiza sus servicios y administra los datos. La Sesión interactiva sobre tecnología muestra los detalles sobre algunos de los aspectos de seguridad en la nube con los que hay que tratar.

Los usuarios de nubes necesitan confirmar que, sin importar que sus datos se almacenen o transfieran, estarán protegidos a un nivel que cumpla con sus requerimientos corporativos. Deben estipular que el proveedor de la nube almacene y procese los datos en jurisdicciones específicas, de acuerdo con las reglas de privacidad de esas jurisdicciones. Los clientes de nubes deben averiguar cómo es que el proveedor de la nube segrega sus datos corporativos de los de otras compañías; además deben pedir una prueba de que los mecanismos de cifrado son sólidos. También es importante saber cómo responderá el proveedor de la nube si ocurre un desastre, si el proveedor podrá restaurar por completo sus datos y qué tanto tiempo tardaría. Los usuarios de nubes también deberían preguntar si los proveedores estarían dispuestos a someterse a auditorías y certificaciones de seguridad externas. Estos tipos de controles se pueden escribir en el acuerdo de nivel de servicio (SLA) antes de firmar con un proveedor de la nube.

### **Seguridad en las plataformas móviles**

Si los dispositivos móviles están realizando muchas de las funciones de las computadoras, necesitan estar protegidos de igual forma que las computadoras de escritorio y laptops contra malware, robo, pérdida accidental, acceso sin autorización y hackers. Los dispositivos móviles que acceden a los sistemas y datos corporativos requieren protección especial.

Las compañías se deben asegurar de que su política de seguridad corporativa contenga los dispositivos móviles, con detalles adicionales sobre cómo hay que dar soporte, proteger y utilizar los dispositivos móviles. Necesitarán herramientas para autorizar todos los dispositivos en uso; para mantener registros de inventario precisos de todos los dispositivos móviles, usuarios y aplicaciones; controlar las actualizaciones para las aplicaciones, y bloquear los dispositivos perdidos de manera que no puedan comprometer la seguridad. Las firmas deben desarrollar lineamientos que estipulen las plataformas móviles y las aplicaciones de software aprobadas, así como el software y los procedimientos requeridos para el acceso remoto a los sistemas corporativos. Las compañías tendrán que asegurar que todos los teléfonos inteligentes estén actualizados con los parches de seguridad más reciente y con software antivirus/antispam; además la comunicación se debe cifrar siempre que sea posible.

## **ASEGURAMIENTO DE LA CALIDAD DEL SOFTWARE**

Además de implementar una seguridad y controles efectivos, las organizaciones pueden mejorar la calidad y confiabilidad del sistema al emplear métrica de software y un proceso riguroso de prueba de software. La métrica de software consiste en las evaluaciones de los objetivos del sistema en forma de medidas cuantificadas. El uso continuo de la métrica permite al departamento de sistemas de información y a los usuarios

## SESIÓN INTERACTIVA: TECNOLOGÍA

### ¿QUÉ TAN SEGURA ES LA NUBE?

La firma Cowen and Co. de servicios financieros y de banca de inversión basada en Nueva York, ha transferido sus sistemas de ventas globales a sistemas en la nube a través de Salesforce.com. Hasta ahora, el CIO de Cowen, Daniel Flax, está complacido. El uso de los servicios en la nube ha ayudado a la compañía a reducir los costos directos de la tecnología, a disminuir el tiempo inactivo y a dar soporte a servicios adicionales. Sin embargo, Daniel está tratando de lidiar con los aspectos de seguridad en la nube. No cabe duda que la computación en la nube está algo nublada, y esta falta de transparencia es problemática para muchos.

Uno de los mayores riesgos de la computación en la nube es su alto grado de distribución. Las aplicaciones en la nube y los mashups de las aplicaciones residen en bibliotecas virtuales establecidas en extensos centros de datos remotos y granjas de servidores que proveen servicios comerciales y administración de datos para varios clientes corporativos. Para ahorrar dinero y mantener los costos bajos, los proveedores de computación en la nube distribuyen con frecuencia el trabajo a los centros de datos alrededor del mundo, en donde el trabajo se pueda realizar con la mayor eficiencia posible. Cuando usted utiliza la nube, tal vez no sepa con precisión en dónde están alojados sus datos, e ignore en qué país estén almacenados.

La naturaleza dispersa de la computación en la nube dificulta el rastreo de la actividad no autorizada. Casi todos los proveedores de la nube utilizan cifrado, como la capa de sockets seguros, para proteger los datos que manejan mientras los transmiten de un lado a otro. No obstante, si los datos se almacenan en dispositivos que también almacenan los datos de otras compañías, es importante asegurar que estos datos almacenados estén cifrados.

Indian Harvest Specialtifooods, una compañía basada en Bemidji, Minnesota, que distribuye arroz, granos y legumbres a restaurantes en todo el mundo, depende del proveedor de software de la nube NetSuite para asegurar que los datos que envía a la nube estén protegidos en forma total. Mike Mullin, director de TI de Indian Harvest, siente que al utilizar SSL (capa de sockets seguros) para cifrar los datos obtiene cierto nivel de confianza de que sus datos están seguros. También señala que su compañía y otros usuarios de los servicios en la nube deben poner atención en sus propias prácticas de seguridad, en especial los controles de acceso. "Su lado de la estructura es igual, o quizás más vulnerable que el lado del proveedor", recalca.

Una manera de lidiar con estos problemas es mediante el uso de un distribuidor de las nubes que sea una compañía que cotice en la bolsa de valores, que por ley debe divulgar la forma en que administra la información. Salesforce.com cumple con este requerimiento, con estrictos procesos y lineamientos para administrar sus centros de datos. "Sabemos que nuestros datos están en Estados

Unidos y tenemos un informe sobre los mismos centros de datos de los que estamos hablando", afirma Flax.

Otra alternativa es utilizar un proveedor de la nube que ofrezca a los suscriptores la opción de elegir en dónde deberán realizarse sus actividades de computación en la nube. Por ejemplo, Terremark Worldwide Inc. ofrece a su suscriptor Agora Games la opción de elegir en dónde ejecutar sus aplicaciones. Tiene instalaciones en Miami, pero está agregando otras ubicaciones. En el pasado, Agora no podía opinar en cuanto al lugar en el que Terremark hospedaba sus aplicaciones y datos.

Incluso aunque sus datos estén totalmente seguros en la nube, tal vez usted no pueda probarlo. Algunos proveedores de las nubes no cumplen con los requerimientos actuales de conformidad en relación con la seguridad, y algunos de estos proveedores, como Amazon, han asegurado que no tienen la intención de cumplir con esas reglas y no permitirán en sus sitios de trabajo el acceso a los auditores encargados de verificar la conformidad.

Existen leyes que restringen los lugares en donde las compañías pueden enviar y almacenar algunos tipos de información: información personal identificable en la Unión Europea (UE), el trabajo gubernamental en Estados Unidos o las aplicaciones que emplean ciertos algoritmos de cifrado. Las compañías que tienen que cumplir con estas regulaciones que involucran datos protegidos, ya sea en Estados Unidos o en la Unión Europea, no podrán usar proveedores de las nubes públicas.

Algunas de estas regulaciones exigen la prueba de que los sistemas se administren en forma segura, para lo cual tal vez se requiera la confirmación de una auditoría independiente. Es poco probable que los grandes proveedores permitan a los auditores de otra compañía inspeccionar sus centros de datos. Microsoft encontró una manera de lidiar con este problema, que puede ser de utilidad. La compañía redujo 26 tipos distintos de auditorías a una lista de 200 controles necesarios para cumplir con los estándares de conformidad que se aplicaron a los entornos y servicios de sus centros de datos. Microsoft no da acceso a cualquier cliente o auditor a sus centros de datos, pero su marco de trabajo de conformidad permite a los auditores elegir de un menú de pruebas y recibir los resultados.

Las compañías esperan que sus sistemas estén en funcionamiento 24/7, pero los proveedores de las nubes no siempre han sido capaces de ofrecer este nivel de servicio. Millones de clientes de Salesforce.com sufrieron un corte de energía de 38 minutos a principios de enero de 2009, y otros varios años antes. El corte en el suministro de energía en enero de 2009 bloqueó a más de 900 000 suscriptores que no podían acceder a sus aplicaciones y datos cruciales, necesarios para realizar transacciones de negocios con sus clientes. Más de 300 000 clientes que utilizaban la red en línea de Intuit de aplicaciones para pequeños negocios no pudieron acceder a estos servicios

durante dos días en junio de 2010, después de un corte en el suministro de energía.

Los acuerdos para servicios como EC2 de Amazon y Azure de Microsoft establecen que estas compañías no serán responsables de las pérdidas de datos, ni de multas u otros castigos legales cuando las compañías utilicen sus servicios. Ambos distribuidores ofrecen asesoría sobre cómo usar sus plataformas en la nube en forma segura, y tal vez aún puedan proteger mejor los datos que las propias instalaciones de algunas compañías.

Salesforce.com estuvo mejorando y rediseñando su infraestructura para asegurar un mejor servicio. La compañía invirtió \$50 millones en la tecnología Mirrorforce, un sistema de espejo que crea una base de datos duplicada en una ubicación separada y sincroniza

los datos de manera instantánea. Si una base de datos está deshabilitada, la otra se hace cargo. Salesforce.com agregó dos centros de datos en las costas este y oeste además de sus instalaciones en Silicon Valley. La compañía distribuyó procesamiento para sus clientes más grandes entre estos centros, para balancear la carga de su base de datos.

**Fuentes:** Seth Fineberg, "A Shadow on the Cloud", *Information Management*, agosto de 2010; Ellen Messmer, "Secrecy of Cloud Computing Providers Raises IT Security Risks", *IT World*, 13 de julio de 2010; John Edwards, "Cutting Through the Fog of Cloud Security", *Computerworld*, 23 de febrero de 2009; Wayne Rash, "Is Cloud Computing Secure? Prove IT", *eWeek*, 21 de septiembre de 2009; Robert Lemos, "Five Lessons from Microsoft on Cloud Security", *Computerworld*, 25 de agosto de 2009, y Mike Fratto, "Cloud Control", *Information Week*, 26 de enero de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

## MIS EN ACCIÓN

1. ¿Qué problemas de seguridad y control se describen en este caso?
2. ¿Qué factores de personas, organización y tecnología contribuyen a estos problemas?
3. ¿Qué tan segura es la computación en la nube? Explique su respuesta.
4. Si estuviera a cargo del departamento de sistemas de información de su compañía, ¿qué aspectos desearía aclarar con sus posibles distribuidores?
5. ¿Confiaría sus sistemas corporativos a un proveedor de computación en la nube? ¿Por qué sí o por qué no?

Vaya a [www.trust.salesforce.com](http://www.trust.salesforce.com) y después responda a las siguientes preguntas:

1. Escriba la palabra clave seguridad en el campo de búsqueda del sitio Web para encontrar información sobre las provisiones de seguridad de Salesforce.com. ¿Qué tan útiles son?
2. Ahora escriba mejores prácticas en el campo de búsqueda para encontrar información sobre las mejores prácticas de Salesforce.com y describa con base en esto qué es lo que pueden hacer las compañías suscriptores para reforzar la seguridad. ¿Qué tan útiles son estos lineamientos?
3. Si usted manejara una empresa, ¿se sentiría seguro en cuanto a usar el servicio bajo demanda de Salesforce.com? ¿Por qué sí o por qué no?

finales medir en conjunto el desempeño del sistema, e identificar los problemas a medida que ocurren. Algunos ejemplos de métrica de software son: el número de transacciones que se pueden procesar en una unidad de tiempo específica, el tiempo de respuesta en línea, la cantidad de cheques de nómina impresos en una hora y el número de errores conocidos por cada 100 líneas de código de programa. Para que la métrica tenga éxito, debe diseñarse con cuidado, ser formal y objetiva; además hay que utilizarla de manera consistente.

Un proceso de prueba oportuno, regular y exhaustivo contribuirá de manera considerable a la calidad del sistema. Muchos ven el proceso de prueba como una forma de demostrar que el trabajo que hicieron es correcto. De hecho, sabemos que todo el software de un tamaño considerable está plagado de errores, por lo que debemos realizar pruebas para descubrirlos.

Un buen proceso de prueba empieza antes de siquiera escribir un programa de software, mediante el uso de un *recorrido*: la revisión de una especificación o un documento de diseño realizada por un pequeño grupo de personas seleccionadas con sumo cuidado, con base en las habilidades necesarias para los objetivos específicos que se están evaluando. Una vez que los desarrolladores empiezan a escribir programas de software,

también es posible usar recorridos de código para revisar el código del programa. Sin embargo, para probar el código es necesario ejecutarlo en la computadora. Cuando se descubren errores, se encuentra el origen de los mismos y se elimina por medio de un proceso conocido como *depuración*. En el capítulo 13 encontrará más información sobre las diversas etapas de prueba requeridas para poner en funcionamiento un sistema de información. Además, nuestras Trayectorias de aprendizaje contienen descripciones de las metodologías para desarrollar programas de software que también contribuyan a la calidad del software.

## 8.5 PROYECTOS PRÁCTICOS SOBRE MIS

Los proyectos en esta sección le proporcionan experiencia práctica en el análisis de las vulnerabilidades de seguridad, el uso de software de hojas de cálculo para el análisis de riesgo y el uso de herramientas Web para investigar los servicios de subcontratación de la seguridad.

### Problemas de decisión gerencial

1. K2 Network opera sitios de juegos en línea utilizados por casi 16 millones de personas en más de 100 países. Los jugadores pueden entrar gratis a un juego, pero deben comprar “activos” digitales de K2, como espadas para luchar con dragones, si desean involucrarse mucho en el juego. Los juegos pueden alojar a millones de jugadores a la vez; personas de todo el mundo juegan al mismo tiempo. Prepare un análisis de seguridad para esta empresa basada en Internet. ¿Qué tipos de amenazas debe prever? ¿Cuál sería su impacto en el negocio? ¿Qué pasos puede tomar para evitar que se dañen sus sitios Web y sus operaciones continuas?
2. Una encuesta de la infraestructura de tecnología de la información de su firma ha producido las siguientes estadísticas de análisis de seguridad:

#### VULNERABILIDADES DE SEGURIDAD POR TIPO DE PLATAFORMA COMPUTACIONAL

PLATAFORMA	NÚMERO DE COMPUTADORAS	RIESGO ALTO	RIESGO MEDIO	RIESGO BAJO	TOTAL DE VULNERABILIDADES
Windows Server (aplicaciones corporativas)	1	11	37	19	
Windows 7 Enterprise (administradores de alto nivel)	3	56	242	87	
Linux (servicios de correo electrónico e impresión)	1	3	154	98	
Sun Solaris (Unix) (servidores Web y de comercio electrónico)	2	12	299	78	
Equipos de escritorio y laptops de los usuarios con Windows 7 Enterprise y herramientas de productividad de office que también se pueden enlazar a la red corporativa que ejecuta aplicaciones corporativas y la intranet	195	14	16	1 237	

Las vulnerabilidades de alto riesgo incluyen a los usuarios no autorizados que acceden a las aplicaciones, las contraseñas que se pueden adivinar, los nombres de usuarios que coinciden con la contraseña, las cuentas de usuario activas que no tienen contraseña y la existencia de programas no autorizados en los sistemas de aplicaciones.

Las vulnerabilidades de riesgo medio comprende la habilidad de los usuarios de apagar el sistema sin haber iniciado sesión, las configuraciones de contraseñas y protecto-



res de pantalla que no se establecieron para las PC, y las versiones obsoletas de software que siguen almacenadas en los discos duros.

Las vulnerabilidades de riesgo bajo implica la incapacidad de los usuarios de modificar sus contraseñas, las contraseñas de usuario que no se han modificado en forma periódica y las que eran más pequeñas del tamaño mínimo especificado por la compañía.

- Calcule el número total de vulnerabilidades para cada plataforma. ¿Cuál es el impacto potencial de los problemas de seguridad para cada plataforma computacional en la organización?
- Si sólo tiene un especialista en sistemas de información a cargo de la seguridad, ¿qué plataformas debería considerar en primer lugar al tratar de eliminar estas vulnerabilidades? ¿En segundo? ¿En tercero? ¿Al último? ¿Por qué?
- Identifique los tipos de problemas de control ilustrados por estas vulnerabilidades y explique las medidas a tomar para resolverlos.
- ¿Qué arriesga su firma al ignorar las vulnerabilidades de seguridad identificadas?

**Mejora de la toma de decisiones: uso del software de hojas de cálculo para realizar una evaluación del riesgo de seguridad**

Habilidades de software: fórmulas y gráficos de hojas de cálculo  
Habilidades de negocios: evaluación del riesgo

Este proyecto utiliza software de hojas de cálculo para calcular las pérdidas anuales anticipadas de varias amenazas de seguridad identificadas para una compañía pequeña.

Mercer Paints es una compañía de fabricación de pintura pequeña pero muy estimada, ubicada en Alabama. La compañía tiene una red en operación, la cual enlaza muchas de sus operaciones de negocios. Aunque la firma cree que su seguridad es adecuada, la reciente adición de un sitio Web se ha convertido en una invitación abierta a los hackers. La gerencia solicitó una evaluación del riesgo. Ésta identificó varios riesgos potenciales. En la siguiente tabla se resumen estos riesgos,, las probabilidades asociadas y las pérdidas promedio.

**EVALUACIÓN DEL RIESGO DE MERCER PAINTS**

RIESGO	PROBABILIDAD DE OCURRENCIA	PÉRDIDA PROMEDIO
Ataque por malware	60%	\$75 000
Pérdida de datos	12%	\$70 000
Malversación de fondos	3%	\$30 000
Errores de los usuarios	95%	\$25 000
Amenazas de los hackers	95%	\$90 000
Uso inapropiado por parte de los empleados	5%	\$5 000
Falla de energía eléctrica	15%	\$300 000

- Además de los potenciales riesgos que se listan, debe identificar al menos otras tres amenazas potenciales para Mercer Paints, asignar probabilidades y estimar un rango de pérdidas.
- Use software de hojas de cálculo y los datos de evaluación del riesgo para calcular la pérdida anual esperada de cada riesgo.
- Presente sus hallazgos en forma de un gráfico. ¿Qué puntos de control tienen la mayor vulnerabilidad? ¿Qué recomendaciones haría a Mercer Paints? Prepare un informe por escrito en el que sintetice sus hallazgos y recomendaciones.

## Mejora de la toma de decisiones: evaluación de los servicios de subcontratación (outsourcing) de la seguridad

---

Habilidades de software: navegador Web y software de presentación

Habilidades de negocios: evaluación de los servicios de subcontratación (outsourcing) de empresas

En la actualidad las empresas tienen la opción de subcontratar la función de seguridad o de mantener su propio personal interno para este propósito. Este proyecto le ayudará a desarrollar sus habilidades de Internet en cuanto a usar el servicio Web para investigar y evaluar los servicios de subcontratación de seguridad.

Como experto de sistemas de información en su firma, le han pedido que ayude a la gerencia a decidir si es mejor subcontratar seguridad o mantener la función de seguridad dentro de la firma. Use el servicio Web para buscar información que le ayude a decidir si es conveniente subcontratar la seguridad, localice servicios de subcontratación de seguridad.

- Presente un breve resumen de los argumentos a favor y en contra de subcontratar la seguridad computacional para su compañía.
- Seleccione dos firmas que ofrezcan servicios de subcontratación de seguridad computacional; compárelas junto con sus servicios.
- Prepare una presentación electrónica para la gerencia en donde sintetice sus hallazgos. Su presentación deberá defender su postura en cuanto a si su compañía debe subcontratar la seguridad computacional o no. Si cree que su compañía debe subcontratar, la presentación debe identificar qué servicio de subcontratación de seguridad hay que seleccionar y justificar su selección.

## MÓDULO DE TRAYECTORIAS DE APRENDIZAJE

---

Las siguientes Trayectorias de aprendizaje proporcionan contenido relevante a los temas que se cubrieron en este capítulo:

1. El fuerte crecimiento del mercado de empleos en seguridad de TI
2. La Ley Sarbanes Oxley
3. Análisis forense de sistemas
4. Controles generales y de aplicación para los sistemas de información
5. Desafíos gerenciales de la seguridad y el control



## Resumen de repaso

### 1. ¿Por qué son vulnerables los sistemas de información a la destrucción, el error y el abuso?

Los datos digitales son vulnerables a la destrucción, el mal uso, el error, el fraude y las fallas del hardware o software. Internet está diseñada para ser un sistema abierto, por lo que hace a los sistemas corporativos internos más vulnerables a las acciones de personas externas. Los hackers pueden desencadenar ataques de negación de servicio (DoS) o penetrar en las redes corporativas, provocando graves interrupciones en los sistemas. Los intrusos pueden penetrar las redes Wi-Fi con facilidad mediante el uso de programas husmeadores (sniffers) para obtener una dirección y acceder a los recursos de la red. Los virus y gusanos de computadora pueden deshabilitar sistemas y sitios Web. La naturaleza dispersa de la computación en la nube dificulta el rastreo de la actividad no autorizada o la aplicación de controles desde lejos. El software presenta problemas debido a que los errores o "bugs" de software pueden ser imposibles de eliminar, y además porque los hackers y el software malicioso pueden explotar sus vulnerabilidades. Los usuarios finales introducen errores con frecuencia.

### 2. ¿Cuál es el valor de negocios de la seguridad y el control?

La falta de una seguridad y un control sólidos puede hacer que las firmas que dependen de sistemas computacionales para sus funciones básicas de negocios pierdan ventas y productividad. Los activos de información, como los registros confidenciales de los empleados, los secretos comerciales o los planes de negocios, pierden gran parte de su valor si se revelan a personas externas o si exponen a la firma a una responsabilidad legal. Las nuevas leyes, como la HIPAA, la Ley Sarbanes-Oxley y la Ley Gramm-Leach-Bliley requieren que las compañías practiquen una estricta administración de los registros electrónicos y se adhieran a estrictos estándares de seguridad, privacidad y control. Las acciones legales que requieren evidencia electrónica y análisis forense de sistemas también requieren que las firmas pongan más atención a la seguridad y la administración de sus registros electrónicos.

### 3. ¿Cuáles son los componentes de un marco de trabajo organizacional para la seguridad y el control?

Las firmas necesitan establecer un buen conjunto de controles, tanto generales como de aplicación, para sus sistemas de información. Una evaluación del riesgo se encarga de valorar los activos de información, identifica los puntos de control y las debilidades del control, y determina el conjunto de controles más efectivo en costo. Las firmas también deben desarrollar una política de seguridad corporativa coherente y planes para continuar las operaciones de negocios en caso de desastre o interrupción. La política de seguridad implica políticas de uso aceptable y administración de identidad. La auditoría de MIS exhaustiva y sistemática ayuda a las organizaciones a determinar la efectividad de la seguridad y los controles para sus sistemas de información.

### 4. ¿Cuáles son las herramientas y tecnologías más importantes para salvaguardar los recursos de información?

Los firewalls evitan que los usuarios no autorizados accedan a una red privada cuando está enlazada a Internet. Los sistemas de detección de intrusos monitorean las redes privadas en busca de tráfico de red sospechoso o de intentos de acceder sin autorización a los sistemas corporativos. Se utilizan contraseñas, tokens, tarjetas inteligentes y autenticación biométrica para autenticar a los usuarios de los sistemas. El software antivirus verifica que los sistemas computacionales no estén infectados por virus y gusanos, y a menudo elimina el software malicioso, mientras que el software antispyware combate los programas intrusivos y dañinos. El cifrado, la codificación y encriptación de mensajes, es una tecnología muy utilizada para proteger las transmisiones electrónicas a través de redes desprotegidas. Los certificados digitales en combinación con el cifrado de clave pública proveen una protección más efectiva a las transacciones electrónicas, al autenticar la identidad de un usuario. Las compañías pueden usar sistemas computacionales tolerantes a fallas o crear entornos de computación de alta disponibilidad para asegurar que sus sistemas de información siempre estén disponibles. El uso de la métrica de software y las pruebas rigurosas de software ayuda a mejorar la calidad y confiabilidad del software.

## Términos clave

Administración de identidad, 310

Administración unificada de amenazas (UTM), 316

Análisis forense de sistemas, 307

Ataque de inyección de SQL, 298

Ataque de negación de servicio (DoS), 299

Ataque de negación de servicio distribuida (DDoS), 299

Auditoría de MIS, 312

Autenticación, 312

Autenticación biométrica, 313

Botnet, 299

Bugs, 303

Caballo de Troya, 298

Capa de sockets seguros (SSL), 317  
 Certificados digitales, 318  
 Cibervandalismo, 298  
 Cifrado de clave pública, 317  
 Cifrado, 317  
 Computación de alta disponibilidad, 319  
 Computación orientada a la recuperación, 319  
 Contraseña, 313  
 Controles, 293  
 Controles de aplicación, 308  
 Controles generales, 308  
 Delitos por computadora, 300  
 Evaluación del riesgo, 309  
 Firewall, 314  
 Fraude del clic, 202  
 Gemelos malvados, 301  
 Gusanos, 296  
 Hacker, 298  
 HIPAA, 306  
 Infraestructura de clave pública (PKI), 318  
 Ingeniería social, 302  
 Inspección profunda de paquetes (DPI), 319  
 Keyloggers, 298  
 Ley Gramm-Leach-Bliley, 306  
 Ley Sarbanes-Oxley, 306

Malware, 296  
 Parches, 303  
 Pharming, 301  
 Phishing, 301  
 Planificación de continuidad de negocios, 311  
 Planificación de recuperación de desastres, 310  
 Política de seguridad, 310  
 Política de uso aceptable (AUP), 310  
 Procesamiento de transacciones en línea, 319  
 Protocolo de transferencia de hipertexto seguro (S-HTTP), 317  
 Proveedores de servicios de seguridad administrados (MSSP), 319  
 Robo de identidad, 301  
 Seguridad, 293  
 Sistemas de computadora tolerantes a fallas, 319  
 Sistemas de detección de intrusos, 316  
 Husmeador (sniffer), 299  
 Software antivirus, 316  
 Spoofing, 299  
 Spyware, 298  
 Tarjeta inteligente, 313  
 Tiempo de inactividad, 319  
 Token, 313  
 Virus de computadora, 296  
 War driving, 295

## Preguntas de repaso

1. ¿Por qué son vulnerables los sistemas de información a la destrucción, el error y el abuso?
  - Mencione y describa las amenazas más comunes contra los sistemas de información contemporáneos.
  - Defina malware e indique la diferencia entre un virus, un gusano y un caballo de Troya.
  - Defina a un hacker y explique cómo es que los hackers crean problemas de seguridad y dañan sistemas.
  - Defina delitos por computadora. Mencione dos ejemplos de delitos en los que las computadoras sean el objetivo y dos ejemplos en donde se utilicen como instrumentos de delito.
  - Defina robo de identidad y phishing; explique además por qué el robo de identidad es un problema tan grande en la actualidad.
  - Describa los problemas de seguridad y confiabilidad de sistemas que crean los empleados.
  - Explique cómo es que los defectos del software afectan a la confiabilidad y seguridad de los sistemas.
2. ¿Cuál es el valor de negocios de la seguridad y el control?
  - Explique cómo la seguridad y el control proveen valor a los negocios.
3. ¿Cuáles son los componentes de un marco de trabajo organizacional para la seguridad y el control?
  - Describa la relación entre seguridad y control, los recientes requerimientos regulatorios del gobierno de Estados Unidos y el análisis forense de sistemas.
  - Defina los controles generales y describa cada tipo de control general.
  - Defina los controles de aplicación y describa cada tipo de control de aplicación.
  - Describa la función de la evaluación del riesgo y explique cómo se lleva a cabo para los sistemas de información.
  - Defina y describa lo siguiente: política de seguridad, política de uso aceptable y administración de identidad.
  - Explique cómo es que la auditoría de MIS promueve la seguridad y el control.
4. ¿Cuáles son las herramientas y tecnologías más importantes para salvaguardar los recursos de información?
  - Nombre y describa tres métodos de autenticación.
  - Describa las funciones de los firewalls, los sistemas de detección de intrusos y el software antivirus para promover la seguridad.

- Explique cómo es que el cifrado protege la información.
- Describa la función del cifrado y los certificados digitales en una infraestructura de clave pública.
- Indique la diferencia entre computación tolerante a fallas y computación de alta disponibilidad, y entre planificación de recuperación de desastres y planificación de continuidad de negocios.
- Identifique y describa los problemas de seguridad impuestos por la computación en la nube.
- Describa las medidas para mejorar la calidad y confiabilidad del software.

## Preguntas para debate

1. La seguridad no es tan sólo un aspecto de tecnología, es un aspecto de negocios. Debata sobre ello.
2. Si usted fuera a desarrollar un plan de continuidad de negocios para su compañía, ¿en dónde empezaría? ¿Qué aspectos de la empresa se tratarían en el plan?
3. Suponga que su empresa tiene un sitio Web de comercio electrónico en donde vende productos y acepta pagos con tarjeta de crédito. Debata sobre las principales amenazas de seguridad para este sitio Web y su potencial impacto. ¿Qué se puede hacer para minimizar estas amenazas?

## Colaboración y trabajo en equipo: evaluación de las herramientas de software de seguridad

Con un grupo de tres o cuatro estudiantes, use el servicio Web para investigar y evaluar los productos de seguridad de dos distribuidores competidores, como el software antivirus, los firewalls o el software antispyware. Para cada producto, describa sus capacidades, a qué tipos de negocios se adapta mejor y su costo tanto de compra como de instalación. ¿Cuál es el mejor producto? ¿Por

qué? Si es posible, use Google Sites para publicar vínculos a páginas Web, anuncios de comunicación en equipo y asignaturas de trabajo; para lluvias de ideas; y para trabajar de manera colaborativa en los documentos del proyecto. Trate de usar Google Docs para desarrollar una presentación de sus hallazgos para la clase.

## ¿Estamos listos para una ciberguerra?

### CASO DE ESTUDIO

Para la mayoría de nosotros, Internet es una herramienta que usamos para el correo electrónico, leer noticias, entretenimiento, socialización y compras. Sin embargo, para los expertos de seguridad computacional afiliados a las agencias gubernamentales y contratistas privados, así como sus contrapartes hackers de todo el mundo, Internet se ha convertido en un campo de batalla: una zona de guerra en donde la ciberguerra está siendo más frecuente y las tecnologías de los hackers se están volviendo más avanzadas. La ciberguerra impone un conjunto único y abrumador de desafíos para los expertos de seguridad, no sólo en cuanto a detectar y evitar las intrusiones, sino también en cuanto a rastrear los perpetradores y presentarlos ante la justicia.

La ciberguerra puede tomar muchas formas. A menudo, los hackers usan botnets, redes masivas de computadoras que controlan gracias al spyware y otros tipos de malware, para lanzar ataques DDoS a gran escala sobre sus servidores de blanco. Otros métodos permiten a los intrusos acceder a las computadoras seguras en forma remota y copiar o eliminar el correo electrónico y los archivos de la máquina, o incluso monitorear en forma remota a los usuarios de una máquina mediante el uso de software más sofisticado. Para los cibercriminales, el beneficio de la ciberguerra es que pueden competir con las superpotencias tradicionales por una fracción del costo de, por ejemplo, construir un arsenal nuclear. Como cada vez hay más infraestructura tecnológica moderna que depende de Internet para funcionar, los ciberguerreros no sufrirán escasez de objetivos a los que se puedan dirigir.

La ciberguerra también implica defenderse contra estos tipos de ataques. Éste es uno de los principales enfoques de las agencias de inteligencia de Estados Unidos. Aunque en la actualidad Estados Unidos se encuentra al frente de las tecnologías de ciberguerra, es poco probable que pueda mantener su dominio tecnológico debido al relativo bajo costo de las tecnologías necesarias para montar estos tipos de ataques.

De hecho, hackers de todo el mundo ya han empezado a tomar todo esto muy en serio. En julio de 2009, 27 agencias gubernamentales estadounidenses y de Corea del Sur, junto con otras organizaciones, sufrieron un ataque DDoS. Una cantidad aproximada de 65 000 computadoras que pertenecían a botnets extranjeras inundaron los sitios Web con solicitudes de acceso. Entre los sitios afectados estaban la Casa Blanca, la Tesorería, la Comisión Federal de Comercio, el Departamento de Defensa, el Servicio Secreto, la Bolsa de Valores de Nueva York y el Washington Post, además del Ministerio de Defensa Coreano, la Asamblea Nacional, la Casa Azul presidencial y varios sitios más.

Los ataques no eran sofisticados, sino esparcidos y prolongados, por lo que lograron reducir la velocidad de la mayoría de los sitios en Estados Unidos y obligaron a que varios sitios de Corea del Sur dejaran de funcionar. Se sospechaba que los grupos de Corea del Norte o a favor de ésta se encontraban detrás de los ataques, pero el gobierno de Pyongyang negó cualquier participación.

El único punto positivo de los ataques fue que sólo se vieron afectados los sitios Web de estas agencias. Sin embargo, otras intrusiones sugieren que los hackers ya tienen el potencial para realizar actos de ciberguerra mucho más dañinos. La Administración Federal de Aviación (FAA), que supervisa la actividad de las aerolíneas en Estados Unidos, ya ha sufrido ataques exitosos en sus sistemas, entre ellos uno en 2006 que apagó de manera parcial los sistemas de datos de tráfico aéreo en Alaska.

En 2007 y 2008, los espías de computadoras irrumpieron en el proyecto Joint Strike Fighter de \$300 millones del Pentágono. Los intrusos pudieron copiar y extraer varios terabytes de datos relacionados con el diseño y los sistemas electrónicos, con lo cual es posible facilitar la acción de defenderse contra el avión de combate cuando se llegue a producir. Los intrusos entraron por medio de las vulnerabilidades de dos o tres contratistas que trabajaban en el proyecto del avión de combate. Por fortuna, las computadoras que contienen la mayoría de los datos confidenciales no estaban conectadas a Internet, y por lo tanto eran inaccesibles para los intrusos. Los anteriores funcionarios de Estados Unidos dijeron que este ataque se había originado en China, y que este país había estado realizando un progreso continuo en cuanto al desarrollo de técnicas de guerra en línea. China rechazó estas afirmaciones e indicó que los medios estadounidenses estaban recurriendo a un pensamiento obsoleto como el de la Guerra Fría al culparlos, y que los hackers chinos no tenían la suficiente habilidad como para perpetrar un ataque de esa magnitud.

En diciembre de 2009, unos supuestos hackers robaron un archivo clasificado de diapositivas de PowerPoint en el que se detallaba la estrategia de Estados Unidos y Corea del Sur para pelear una guerra contra Corea del Norte. En Irak, los insurgentes interceptaron transmisiones del vehículo aéreo no tripulado Predator mediante el uso de software que habían descargado de Internet.

En abril de ese mismo año, unos ciberespías se infiltraron en la red eléctrica de Estados Unidos mediante el uso de los puntos débiles en donde las computadoras en la red se conectan a Internet, y dejaron a su paso programas de software cuyo propósito no está claro, pero que se supone podrían utilizarse para interrumpir el sistema. Los informes indicaron que los espías

empezaron desde las redes de computadoras en China y Rusia. De nuevo, ambas naciones negaron los cargos.

En respuesta a estas y otras intrusiones, el gobierno federal lanzó un programa llamado “ciudadano perfecto” para detectar los ciberataques a compañías privadas que operaban una infraestructura crítica. La Agencia de Seguridad Nacional (NSA) de Estados Unidos planea instalar sensores en las redes de computadora para la infraestructura crítica que se activen debido a actividades inusuales para indicar un inminente ciber-ataque. El enfoque inicial serán los sistemas de control de computadoras grandes y antiguos que desde un principio han estado enlazados a Internet, lo cual los hace más vulnerables al ciberataque. Es probable que la NSA empiece con los sistemas de control eléctrico, nuclear y de tráfico aéreo que pueden tener el mayor impacto sobre la seguridad nacional.

Al momento de escribir este libro, la mayoría de las agencias federales recibieron la aprobación por cumplir con los requerimientos de la Ley Federal de Administración de Seguridad de la Información, el conjunto más reciente de estándares aprobados y convertidos en ley. No obstante, a medida que las tecnologías de ciber guerra se desarrollan y se vuelven más avanzadas, es probable que los estándares impuestos por esta legislación no sean suficientes para poder defenderse contra los ataques.

En cada incidente de ciber guerra, los gobiernos de los países que se sospecha son responsables han negado de manera rotunda los cargos sin repercusiones. ¿Cómo podría ser esto posible? La razón principal es que rastrear identidades de atacantes específicos por el ciberespacio es algo casi imposible, lo cual facilita la acción de negar la responsabilidad.

La verdadera preocupación para los expertos en seguridad y los funcionarios de gobierno es un acto de ciber guerra contra un recurso crítico, como la red eléctrica, el sistema financiero o los sistemas de comunicaciones. Primero que nada, Estados Unidos no tiene una política clara sobre la forma en que debería responder el país a ese nivel de ciberataque. Aunque unos hackers tuvieron acceso a la red eléctrica, en realidad todavía no ha sido atacada. Un estudio de tres años sobre la ciberseguridad en Estados Unidos recomendó la creación de dicha política y que se hiciera pública. También sugirió que Estados Unidos debería tratar de encontrar puntos en común con otras naciones para unir fuerzas y evitar estos ataques.

En segundo lugar, es probable que los efectos de dicho ataque sean devastadores. Mike McConnell, el anterior director de inteligencia nacional, indicó que incluso si un solo banco estadounidense de gran tamaño sufriera un ataque exitoso, “tendría un impacto 10 veces mayor sobre la economía global” que los ataques al World Trade Center, y que “la habilidad de amenazar la reserva monetaria de Estados Unidos es el equivalente al arma nuclear moderna”. Dicho ataque tendría un efecto catastrófico sobre el sistema financiero de este país, y por ende, sobre la economía global.

Por último, muchos analistas de sistemas se preocupan debido a que la organización de la ciberseguridad en Estados Unidos es un desastre, ya que no hay un líder definido entre las agencias gubernamentales de este país. Varias agencias distintas, incluso el Pentágono y la NSA, tienen puesta su mira en cuanto a convertirse en la agencia líder en los esfuerzos continuos por combatir la ciber guerra. En junio de 2009, el secretario de Defensa Robert Gates ordenó la creación del primer comando designado para coordinar los esfuerzos de ciberseguridad del gobierno, conocido como Cybercom. Este comando se activó en mayo de 2010 con el objetivo de coordinar la operación y protección de las redes de computadoras militares y del Pentágono con la esperanza de resolver este enredo organizacional.

Al confrontar este problema ha surgido una pregunta crítica: ¿cuánto control para implementar la ciberseguridad se debería otorgar a las agencias espías estadounidenses, ya que tienen prohibido actuar en territorio estadounidense? Los ciberataques no tienen fronteras, por lo que hacer la diferencia entre territorio estadounidense y extranjero significa que se inhibirá de manera innecesaria la habilidad de las agencias nacionales para combatir el cibercrimen. Por ejemplo, si la NSA estuviera investigando el origen de un ciberataque en algunos sitios Web del gobierno y determinara que el ataque se originó desde servidores estadounidenses, bajo las leyes actuales no podría investigar más a fondo.

Algunos expertos creen que no hay una manera efectiva de que una agencia nacional realice operaciones de computadoras sin entrar a las redes prohibidas dentro de Estados Unidos, o incluso de realizar investigaciones en países que sean aliados estadounidenses. La NSA ya se ha enfrentado a una dura crítica por sus acciones de vigilancia después del 9-11, y esto tiene el potencial de generar problemas de privacidad similares. Para prevenir los ataques terroristas o la ciber guerra tal vez sea necesario examinar algunos mensajes de correo electrónico provenientes de otros países o dar a las agencias de inteligencia más acceso a las redes o a los proveedores de servicios de Internet. Existe la necesidad de un debate abierto en cuanto a lo que constituye una violación de la privacidad y lo que es aceptable durante el ‘tiempo de ciber guerra’, que en esencia viene siendo todo el tiempo. Tal vez haya que cambiar la ley para dar cabida a técnicas de ciberseguridad efectivas, pero lo que no queda claro es que se pueda hacer esto sin socavar algunos derechos de privacidad que consideramos esenciales.

En cuanto a estas medidas ofensivas, no está claro qué tan sólidas son las capacidades ofensivas de Estados Unidos para una ciber guerra. El gobierno protege mucho esta información, puesto que casi toda es clasificada. Aunque los antiguos funcionarios militares y de inteligencia indican que las capacidades de Estados Unidos de ciber guerra han aumentado de manera considerable en los últimos dos años. Y como el rastreo de los cibercriminales ha resultado ser tan difícil, tal vez la mejor defensa sea una ofensiva sólida.

**Fuentes:** "Cyber Task Force Passes Mission to Cyber Command", Defence Professionals, 8 de septiembre de 2010; Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies", *The Wall Street Journal*, 8 de julio de 2010 y "U.S. Hampered in Fighting Cyber Attacks, Report Says", *The Wall Street Journal*, 16 de junio de 2010; Siobhan Gorman, Yochi Dreazen y August Cole, "Drone Breach Stirs Calls to Fill Cyber Post", *The Wall Street Journal*, 21 de diciembre de 2009; Sean Gallagher, "New Threats Compel DOD to Rethink Cyber Strategy", *Defense Knowledge Technologies and Net-Enabled Warfare*, 22 de enero de 2010; Lance Whitney, Cyber Command Chief Details Threat to U.S.", *Military Tech*, 5 de agosto de 2010; Hoover, J. Nicholas, "Cybersecurity Balancing Act", *Information Week*, 27 de abril de 2009; David E. Sanger, John Markoff y Thom Shanker, "U.S. Steps Up Effort on Digital Defenses", *The New York Times*, 28 de abril de 2009; John Markoff, y Thom Shanker, "Panel Advises Clarifying U.S. Plans on Cyberwar", *The New York Times*, 30 de abril de 2009; Siobhan Gorman y Evan Ramstad, "Cyber Blitz Hits U.S., Korea", *The Wall Street Journal*, 9 de julio de 2009; Lolita C. Baldor, "White House Among Targets of Sweeping Cyber Attack", *Associated Press*, julio 8 de 2009; Choe Sang-Hun, "Cyberattacks Hit U.S. and South Korean Web Sites", *The New York Times*, 9 de julio de 2009; Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers", *The Wall Street Journal*, 7 de mayo de 2009; Thom Shanker, "New Military Command for Cyberspace", *The New York Times*, 24 de

junio de 2009; David E. Sanger y Thom Shanker, "Pentagon Plans New Arm to Wage Wars in Cyberspace", *The New York Times*, 29 de mayo de 2009; Siobhan Gorman, August Cole y Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project", *The Wall Street Journal*, 21 de abril de 2009; Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies", *The Wall Street Journal*, 8 de abril de 2009; "Has Power Grid Been Hacked? U.S. Won't Say", *Reuters*, 8 de abril de 2009; Markoff, John, "Vast Spy System Loots Computers in 103 Countries", *The New York Times*, 29 de marzo de 2009; Markoff, John, "Tracking Cyberspies Through the Web Wilderness", *The New York Times*, 12 de mayo de 2009.

## PREGUNTAS DEL CASO DE ESTUDIO

1. ¿Es la ciberguerra un problema grave? ¿Por qué sí o por qué no?
2. Evalúe los factores de administración, organización y tecnología que han creado este problema.
3. ¿Qué soluciones se han propuesto? ¿Cree usted que serán efectivas? ¿Por qué sí o por qué no?
4. ¿Hay otras soluciones para este problema que deban buscarse? ¿Cuáles son?