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

¿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-

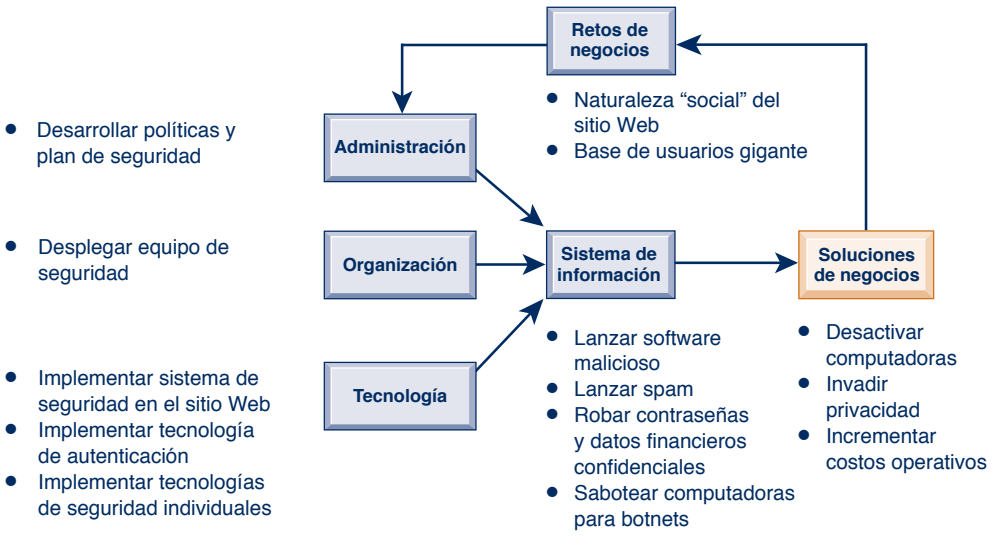
trónico anuncios no solicitados y robar las credenciales de inicio de sesión de los usuarios de Facebook. El ataque empieza con un mensaje que contiene un vínculo a una página Web falsa enviado por los usuarios infectados a todos sus amigos. El mensaje se dirige a cada amigo por su nombre e invita a 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", allfacebook.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

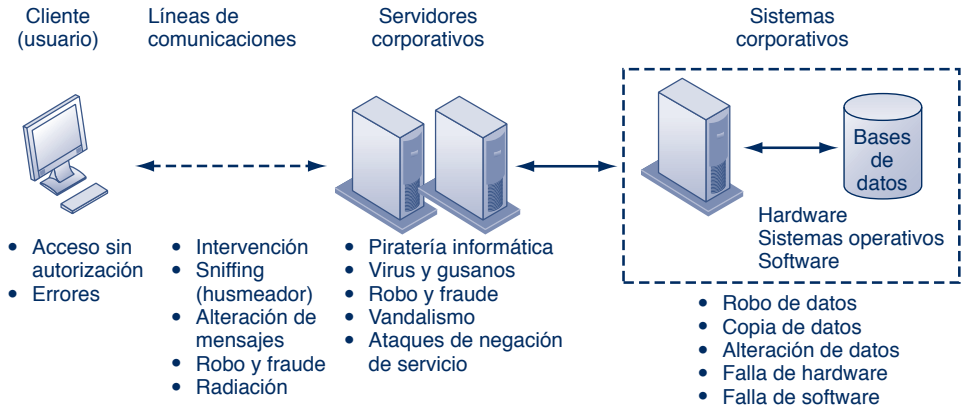
¿Puede imaginar lo que ocurriría si intentara conectarse a Internet sin un firewall o software antivirus? Su computadora quedaría deshabilitada en unos cuantos segundos, y podría tardar varios días en recuperarla. Si utilizara la computadora para operar su negocio, tal vez no podría venderles a sus clientes 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

Cuando 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

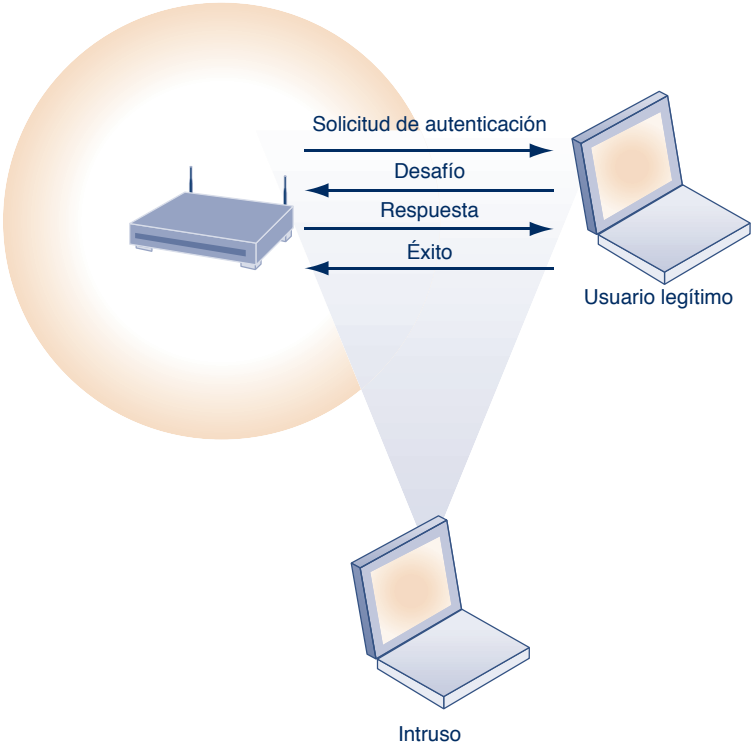
que personas externas pueden interceptarlos y leerlos durante la transmisión a través de la red Internet pública. La actividad de mensajería instantánea a través de Internet puede utilizarse en algunos casos como una puerta trasera hacia una red que de otra forma sería segura. En la compartición de archivos 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.

denses 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) 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 intercepción 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 MacAfee. Esta explicación dejó estupefactos a muchos de los clientes de McAffe 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 posible 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 iníciales 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 debito 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	Auditan 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 LINEA

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
• Datos de historial médico	Ninguno
• Salario	Ninguno
• Ingresos pensionables	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, Illionois, 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.

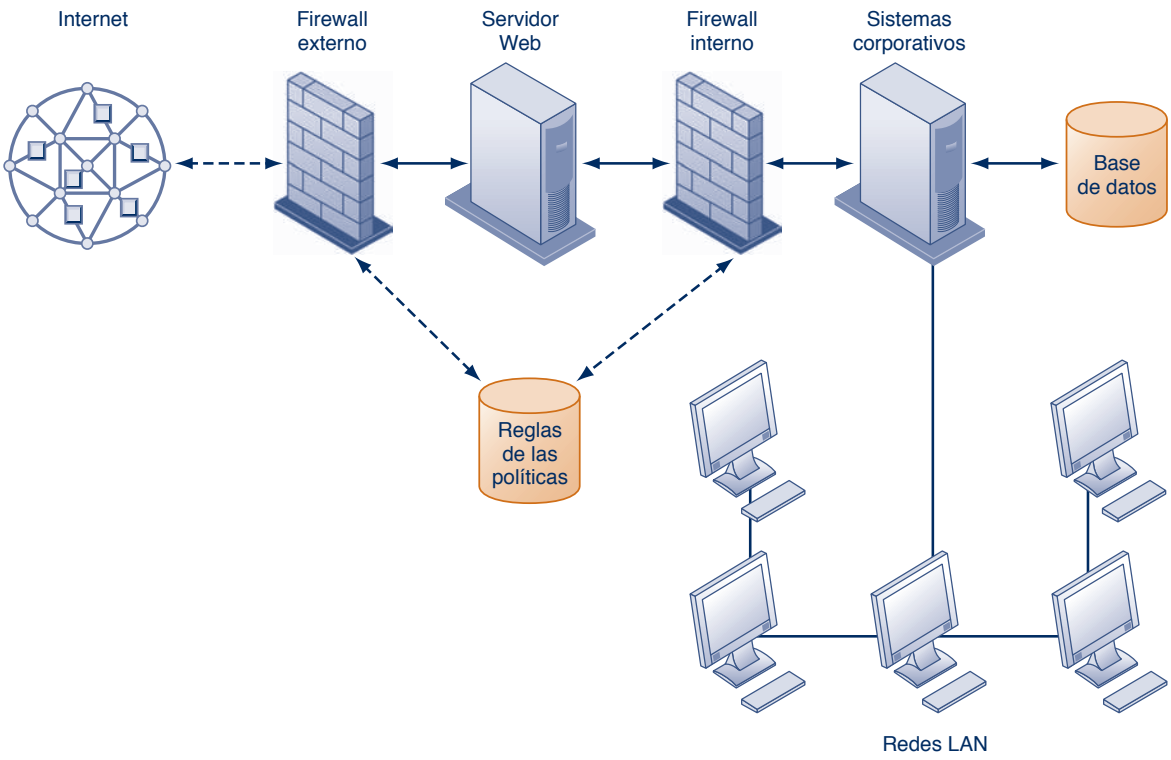
Firewalls

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, Fortinent 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.

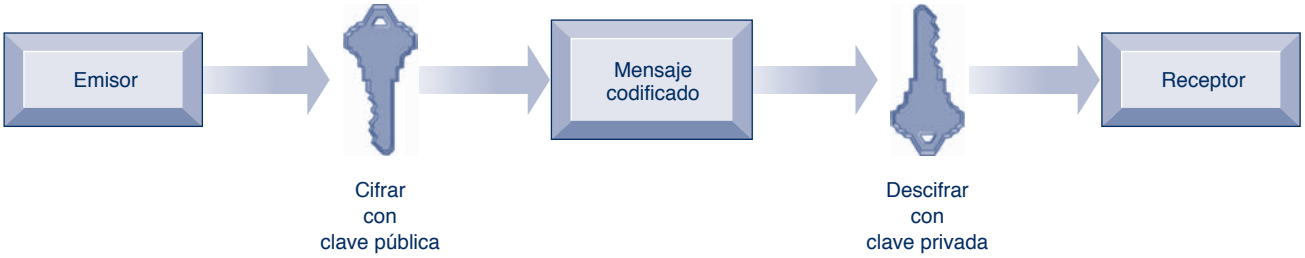
Los dos métodos para cifrar el tráfico de red en Web son SSL y S-HTTP. La **capa de sockets seguros (SSL)** y su sucesor, seguridad de la capa de transporte (TLS), permiten que las computadoras cliente y servidor manejen las actividades de cifrado y descifrado a medida que se comunican entre sí durante 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.

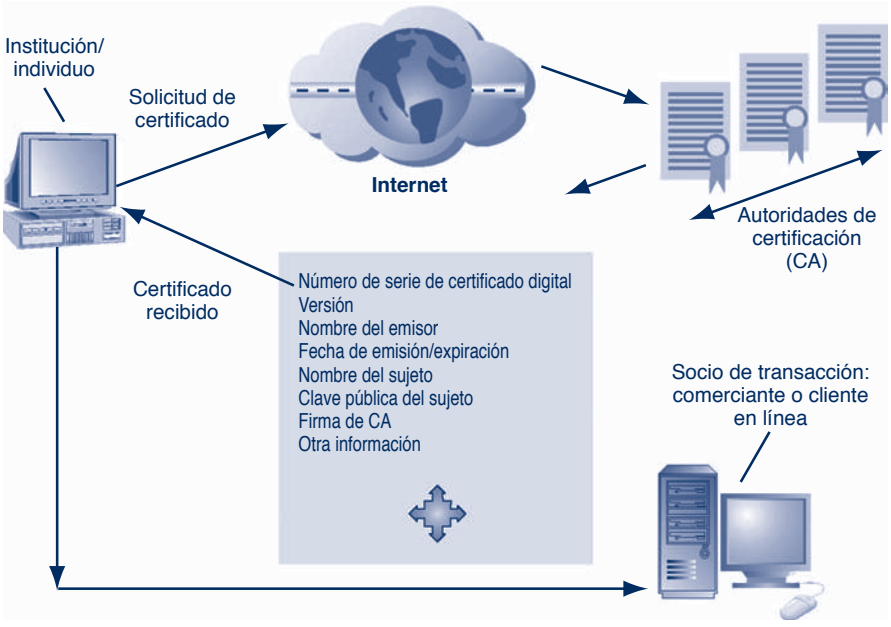
Los **certificados digitales** son archivos de datos que se utilizan para establecer la identidad de los usuarios y los activos electrónicos para proteger las transacciones en línea (vea la figura 8-7). Un sistema de certificados digitales utiliza una tercera parte de confianza, conocida como autoridad 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 Specialtifoods, 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.

Salesfoce.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

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?

MIS EN ACCIÓN

Vaya a 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, mientas 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

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.
   - Describa la relación entre seguridad y control, los recientes requerimientos regulatorios del gobierno de Estados Unidos y el análisis forense de sistemas.
3. ¿Cuáles son los componentes de un marco de trabajo organizacional para la seguridad y el control?
   - 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 ciberguerra 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 ciberguerra, 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 ciberguerra 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 ciberguerra. En junio de 2009, el secretario de Defensa Robert Gates ordenó la creación del primer comando designado para coordinar los esfuerzos de ciber-seguridad 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 ciberguerra tal vez sea necesario examinar algunos mensajes de correo electrónico provenientes de otros países o dar a las agencia 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 ciberguerra', que en esencia viene siendo todo el tiempo. Tal vez haya que cambiar la ley para dar cabida a técnicas de ciber-seguridad 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 ciberguerra. 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 ciberguerra 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?