4

Objetivo general

Que el estudiante conozca y comprenda los conceptos y componentes de la seguridad física y lógica, tanto en computadoras personales, como en redes de cómputo.

Objetivos específicos

- Identificarás los componentes de la seguridad física y lógica en centros de cómputo.
- Identificarás las amenazas más comunes a las que están expuestas las PC y las redes de cómputo.
- Identificarás el funcionamiento y la prevención de un ataque de ingeniería social.

La seguridad física y lógica en redes

¿Qué sabes?

- ¿Conoces los elementos que se consideran para otorgar la certificación de la sustentabilidad operativa?
- ¿Qué es la ingeniería social?
- ¿Conoces el método de inyección SQL?
- ¿Conoces algún sistema de prevención de intrusiones?

Competencias a desarrollar

- El alumno identifica y describe cuáles son las amenazas físicas y lógicas a las que están expuestas las computadoras personales y las redes de cómputo.
- El alumno describe y entiende cómo se efectúan los principales ataques informáticos.

4.1 Introducción

Atender la seguridad tanto de una computadora personal, como de las computadoras conectadas a una red, es indispensable debido a que estos equipos de cómputo siempre están expuestos a dos tipos de riesgos: 1) riesgos de ataques físicos y 2) riesgos informáticos o lógicos. Como ejemplo del primer tipo de riesgo destaca la violación física a los espacios donde se encuentran las computadoras, los servidores o los respaldos de información; cuando sucede este tipo de violaciones, el atacante tiene a su disposición toda la información que requiera, incluso puede robar discos duros o dispositivos donde se tiene respaldada la información; sin embargo, este tipo de violaciones no siempre es hecha por un atacante humano, sino que en muchas ocasiones es la propia naturaleza la que, a través del medio ambiente, puede provocar daños, como sucede en caso de terremotos, lluvias intensas o incendios accidentales, que de llegar a los centros de cómputo de las empresas pueden causar daños irreversibles a las instalaciones y a la información, la cual, como se dijo en el capítulo 1 (Generalidades de la seguridad informática), es el segundo recurso más valioso que posee cualquier organización, después de los recursos humanos.

Por su parte, los riesgos informáticos o lógicos provienen de Internet o de cualquier otro tipo de red, pública o privada; consisten en alteraciones en el funcionamiento de cualquier tipo de software que contenga al menos una computadora de la red, desde la cual se puede dispersar o difundir no sólo a las computadoras de esa red, sino hacia otras redes. Los riesgos que provienen de Internet siempre son causados por personas con malas intenciones, aunque un mal funcionamiento de un sistema informático también puede deberse a un mal diseño o una mala programación de alguna parte del sistema.

Este capítulo describe con cierto detalle en qué consiste este tipo de riesgos y cómo se puede disminuir la probabilidad de que sucedan.

4.2 Riesgos físicos de los centros de cómputo y de las redes

Esta sección no trata tanto de conocer y comprender el funcionamiento de los dispositivos empleados para prevenir que fenómenos naturales, como terremotos, lluvias o fuego, puedan dañar las instalaciones. Aquí se enfatiza que las grandes empresas de todo el mundo tienen un sistema de respaldo de su información en tiempo real, con lo que se aseguran de que en verdad no se perderá ninguna información de la empresa.

Considérese lo que sucedería con la bolsa de valores de Nueva York, la más grande e importante a nivel mundial, si durante sólo unos pocos segundos se perdiera la información generada en un día normal de actividad. Ahora, supóngase que durante la perpetración de los atentados del 11 de septiembre de 2001 en Nueva York, uno de los objetivos hubiera sido destruir las instalaciones de la bolsa de valores, que se encuentran a unos 300 metros en línea recta del sitio donde se encontraban las Torres Gemelas del WTC (World Trade Center); de hecho, el ataque al WTC destruyó cientos de oficinas, computadoras, archivos, etcétera; no obstante, durante estos trágicos eventos no se perdió ni un bit de información, ya que todas las empresas tienen un almacén de datos, que capta on line toda la información que se va generando. Pero, dicho almacén de datos se ubica en lugares desconocidos y lejanos al sitio donde se encuentran las oficinas centrales, con una fachada que no aparenta ser la rama de una gran empresa, por lo que dicha instalación casi siempre está a salvo de las consecuencias de terremotos, inundaciones, fuego, etcétera, de manera que aunque se destruyó el WTC, la información de todas las empresas ubicadas en esos edificios estaba perfectamente resguardada.

Este hecho ofrece una idea acerca de por qué la información es tan valiosa para cualquier empresa u organización. Por tanto, en este capítulo se hace énfasis en que cualquiera que sea el tipo, tamaño y/o actividad de la empresa, siempre se deberá pensar en invertir en un resguardo de la información, de tal forma que haya una certeza total de que la información estará a salvo, sin importar los riesgos a los que está expuesta, naturales o intencionales.

En este contexto, en 1993 se creó el Uptime Institute, un conjunto de empresas cuyo interés se centra en los data center, sobre los cuales realizan investigaciones tecnológicas. Un data center se define como una instalación en cuyo interior hay todo lo relacionado con sistemas de cómputo, como telecomunicaciones y sistemas de almacenamiento para el respaldo de información, conexiones para la comunicación de datos redundantes, controles ambientales (aire acondicionado y extintores de fuego) y otros muy diversos dispositivos de seguridad.

El Uptime Institute es más conocido porque expide certificaciones de niveles (tier certifications, en inglés), a través de los estándares de niveles y las certificaciones para el centro de diseño de datos, aunque está enfocado en mejorar el desempeño, la eficiencia y la confiabilidad en la infraestructura que puede ser crítica para ciertos negocios, por medio de la innovación, la colaboración y la expedición de certificaciones independientes, a las personas y empresas que prestan servicios de tecnologías de información (TI). En la década de 1980, se vivió una enorme expansión de la industria de las microcomputadoras, las cuales aparecían en todas partes del mundo. Debido a esta rápida revolución de las computadoras personales, en esa época, en la mayoría de los casos no se tenía cuidado acerca de algunos de los requisitos operativos para su funcionamiento, pero cuando la tecnología de la información se volvió más compleja, las empresas también empezaron a cuidar más los recursos invertidos en estas tecnologías.

En aquellos años, el equipo para instalar redes se volvió poco costoso; sin embargo, con las computadoras en red y el uso de servidores surgió la necesidad de crear diseños jerárquicos para colocar a los servidores en sitios especiales dentro de los centros de cómputo. En ese momento se creó el término *data center* aplicado a estos sitios especiales como centros de cómputo o centros de procesamiento de datos.

En 2005, el American National Standards Institute (ANSI, por sus siglas en inglés), publicó el Estándar para la infraestructura de las telecomunicaciones en los data centers, que establece y define cuatro niveles (tiers, en inglés) para los data centers. De éstos, el data center nivel 1 es prácticamente un sitio para un servidor, que sigue una guía básica para la instalación de sistemas de

computadoras, mientras que el nivel 4 es el más exigente, ya que en éste se ha diseñado un host de los sistemas de computadoras de misión crítica, con subsistemas totalmente redundantes y zonas de seguridad por departamentos controladas con accesos de métodos biométricos.

Los niveles describen la disponibilidad de datos que pueden tomarse o consultarse del hardware de una instalación de cómputo. A mayor nivel, mayor confiabilidad en que los datos estarán disponibles cuando se necesiten. A continuación se exponen las características de cada uno de los cuatro niveles.

Nivel 1

1. Una sola trayectoria de distribución no redundante para dar servicio a la TI.
2. Componentes con capacidad no redundante.
3. Infraestructura básica del sitio con una disponibilidad esperada de 99.671 por ciento. Esto significa que de una disponibilidad anual total de 525 600 minutos, el sistema sólo puede no estar disponible 1 729.2 minutos.

Nivel 2

4. Excede, o al menos cumple, con todos los requisitos del nivel 1.
5. Infraestructura redundante del sitio con componentes de la capacidad con una disponibilidad esperada de 99.741 por ciento. Esto significa que de una disponibilidad anual total de 525 600 minutos, el sistema sólo puede no estar disponible 1 361.3 minutos

Nivel 3

6. Excede, o al menos cumple, con todos los requisitos del nivel 2.
7. Múltiples trayectorias de distribución independientes que sirven a los equipos de la TI.

8. Todos los equipos de la TI deben ser alimentados con fuentes de potencia dual y totalmente compatibles con la topología de una arquitectura de sitio.
9. Mantenimiento actualizado de la infraestructura del sitio con disponibilidad esperada de 99.982 por ciento. Esto significa que de una disponibilidad anual total de 525 600 minutos, el sistema sólo puede no estar disponible 94.608 minutos.

Nivel 4

10. Excede, o al menos cumple, con todos los requisitos del nivel 3.
11. Todo el equipo de control de temperatura ambiental tiene una alimentación independiente de potencia dual, incluyendo los sistemas de enfriadores, calentadores, ventilación y aire acondicionado.
12. Infraestructura del sitio tolerante a las fallas con almacenamiento de potencia eléctrica e instalaciones de distribución con disponibilidad esperada de 99.995 por ciento. Esto significa que de una disponibilidad anual total de 525 600 minutos, el sistema sólo puede no estar disponible 26.28 minutos.

La certificación por niveles sólo se aplica a la topología física de la infraestructura de los data center que afecta en forma directa a la operación de la sala de las computadoras.

Además de la certificación por niveles, el Uptime Institute también emite una certificación a la sustentabilidad operativa que se enfoca a la administración, la operación y el mantenimiento del sitio más que al diseño de su topología, al establecer las conductas y los riesgos que pueden impactar el desempeño a largo plazo del data center. Los tres elementos que considera para otorgar la certificación de la sustentabilidad operativa son los que se describen enseguida.

1. **Operación y administración:** incluye la presencia de apoyos externos, la calificación de estos apoyos y los programas de mantenimiento.
2. **Características del edificio donde se aloja el data center:** establece que tenga plantas de emergencia para cuando se interrumpa el abasto de energía eléctrica.
3. **Características del sitio donde se ubica el data center:** refiere a la protección contra inundaciones del data center, que cuente con buenas vías de comunicación, que el espacio interno sea suficiente, etcétera.

Sin embargo, el Uptime Institute no es el único que emite certificaciones. Otros modelos de clasificación también han sido emitidos por la AEC (Availability Environment Classification o Clasificación del Medioambiente Disponible), que pertenece al Hardvard Research Group y que establece niveles conocidos como AEC-0 al AEC-5.

Aunque éste es un aspecto muy importante de la seguridad y el bienestar físico de los trabajadores de las organizaciones, otro aspecto no menos importante es restringir el acceso de personas no autorizadas al lugar donde se encuentra la información almacenada, pues si un intruso tiene acceso a esos sitios, las consecuencias para la empresa o la organización podrían ser desastrosas. Para evitar este tipo de accesos, existen diversas figuras de control de ingreso, desde el policía que solicita una credencial de identificación y lleva un registro de los visitantes, hasta los dispositivos biométricos para permitir el acceso.

A continuación un ejemplo claro del control de acceso biométrico. Cualquier persona que ingrese en forma legal a Estados Unidos de América por cualquier medio, pasa por un control biométrico, que en este caso se trata de la huella digital del dedo índice de la mano derecha. Para el ingreso a territorio estadounidense no basta con un pasaporte en regla, y desde luego con una fotografía del interesado, sino que además se aplica el control biométrico.

Existen varios controles biométricos que se pueden implementar. El más usado es la huella digital, pero también existe la voz, que es una mezcla de características físicas y de comportamiento, y la identificación del iris del

ojo, los cuales se supone son infalsificables, esto es cierto; sin embargo, en el caso de dichos controles, puede surgir un problema porque las mediciones de estos parámetros (huella digital, voz o iris) tienen una tasa muy elevada de aciertos, pero no es del 100 por ciento. Debido a ello se han definido algunas tasas, como la tasa de falsa aceptación que significa el número de veces que se puede aceptar la identidad de una persona, cuando en realidad no es la persona a la cual pertenece cualquiera de los controles (huella, voz o iris), en tanto que la tasa de falso rechazo es la cantidad de veces que se presenta la persona a la cual pertenecen cualquiera de los controles, pero el sistema la rechaza porque no es capaz de comparar de manera correcta la lectura de los controles de la persona con los datos de los controles que tiene almacenados.

Ante esta situación, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el cual depende del Departamento de Comercio de Estados Unidos de América, se dedica, entre otras cosas, a desarrollar métodos de evaluación de sistemas y tecnologías para la identificación de personas por medio de imágenes digitalizadas, mediante el uso de una tecnología de reconocimiento facial.

Para desarrollar esta tecnología, en el NIST primero debieron preguntarse si esta tecnología sería mejor que las otras en cuanto a su desempeño por los niveles de calidad de diferentes videos e imágenes, si los resultados de esta prueba estarían correlacionados con otras pruebas de identificación, como el reconocimiento del iris, y algo que es muy importante, si esta tecnología sería capaz de mejorar los servicios públicos, si beneficiaría la aplicación de la ley y si se podría aplicar para aumentar la seguridad en hogares y organizaciones. Los principales servicios públicos en donde se utilizan los controles biométricos son del tipo de aceptar a extranjeros en aduanas por medio de esta prueba, o en la expedición de pasaportes o cualquier otra credencial de identificación personal.

De acuerdo con los reportes del NIST, esta tecnología ha incrementado la eficiencia y precisión de los sistemas de identificación humana en la aplicación de controles de acceso a sitios restringidos y para la localización de personas que están en constante observación por parte del gobierno estadounidense, como terroristas internacionales.

Para aceptar y poner en marcha una tecnología de este tipo, primero se mide su desempeño con respecto a varios niveles de calidad, para lo cual se realizan análisis de correlación con otras pruebas biométricas, entre las que se incluyen la evaluación del reconocimiento del iris y la certificación obligatoria de sistemas de reconocimiento facial.

Otra propuesta de prueba que ha llamado la atención es la identificación a través de la huella digital, pero no de un solo dedo, sino de los diez dedos de las manos. Sin embargo, la primera dificultad de esta prueba es que si se coloca la palma de cualquier mano hacia abajo, al menos el dedo pulgar, no queda en buena posición para que un dispositivo pueda leer la huella de los cinco dedos al mismo tiempo, por lo que esta prueba implica tomar cuatro lecturas de huellas, dos por cada mano. Un aspecto importante a considerar aquí es el tiempo y la resolución de la lectura dactilar; aun cuando esta prueba sea más segura que la lectura de la huella de un solo dedo, toma más tiempo. Además, sólo resulta efectiva y confiable si se consigue una alta precisión, pero si no se alcanza una certeza de 100 por ciento no se habrá avanzado mucho. Por tanto, si se requiere hacer la lectura de las dos manos a la vez, se necesita diseñar un dispositivo especial, lo cual implica una elevada inversión; además, también es necesario disminuir el tiempo en que la computadora realiza la identificación de las huellas.

El NIST considera que un buen sistema identificador de personas por medio de las diez huellas dactilares debe tomar como máximo 10 segundos. Dicho sistema debe ser capaz de formar un banco de datos a partir de huellas dactilares que ya se tienen en papel y de la huella en tinta, de manera que se requiere escanear todos esos millones de datos con alta calidad, para poder compararlos con la lectura que haga el identificador con las personas y la prueba presentes.

En este contexto, el gobierno de Estados Unidos de América no sólo piensa en la seguridad informática, sino también en los aspectos legales y las implicaciones que surgen de la identificación de cadáveres, identificación de intrusos a las empresas u hogares, la identificación de asesinos, etcétera, basados en las pruebas dactilares de las personas implicadas. Aun cuando la identificación dactilar conlleva muchas implicaciones legales a los sistemas de

justicia de todo el mundo, se espera que esta tecnología mejore las decisiones de los juicios legales, así como las investigaciones forenses.

Como en muchas ocasiones, una disciplina como la seguridad informática, se beneficia de las investigaciones que se realizan con otros fines, como sucede con la identificación dactilar; aunque no hay la menor duda de que la protección de información en las empresas y las organizaciones también requiere de una identificación con 100 por ciento de certeza de que se está dando acceso a la persona correcta.

4.3 La ingeniería social

La ingeniería social se define como una práctica, y en ocasiones como "un arte", para obtener información confidencial de la persona atacada, ya sea que se manipule a la persona o que se le engañe con sutileza para obtener la información deseada. El nombre asignado a esta actividad prácticamente insulta a la ingeniería pura, pues ésta se define como el uso de conocimientos y tecnología para promover la mejora en la vida de las personas; bajo esta premisa, a lo largo de la historia de la ingeniería se han desarrollado todo tipo de ingenierías: mecánica, eléctrica, química, petrolera, biomédica, financiera, etcétera, todas con el objetivo común de ayudar, desde su campo de conocimientos, a que el ser humano mejore algún aspecto de su vida cotidiana. Sin embargo, la ingeniería social está directamente enfocada a la manipulación o al engaño de personas ingenuas o de buena voluntad, para obtener información que al final sirve al atacante para cometer un fraude.

Desde luego, como es sabido, la palabra *ingeniero* proviene del vocablo en latín *ingenium*, o *ingenio* en español, así que si se considera que para engañar a una persona se requiere de mucho ingenio, esto es cierto, pero entonces sería más conveniente llamarla *engaño social*, *seducción social* o *manipulación social,* pero no ingeniería, debido a que esta disciplina siempre ha tenido fines elevados. Al margen de este nombre, la ingeniería social es utilizada por diversas personas, desde investigadores privados, individuos con malas intenciones o delincuentes informáticos, para obtener información directa o tener acceso

a bancos de información de cualquier tipo, que en el peor de los casos permite a los delincuentes llevar a cabo malas acciones.

En la actualidad, hay dos formas de practicar la ingeniería social. La primera es hablar de manera directa con la víctima, a fin de que sea ella misma quien proporcione información, mientras que la segunda consiste en hacerlo a través de Internet. En la primera, por lo común el atacante llama por teléfono a la víctima y se hace pasar por empleado de alguna empresa o por cualquier otra persona con quien la víctima pueda estar interesado en hablar y empieza a pedirle datos que le permitan ingresar a su sistema informático o de toda la empresa. En la segunda, se envía un "correo ciego", con el propósito de entablar un diálogo entre la víctima y el atacante. Entre los temas que, en general, propone el atacante destacan los que se relacionan a continuación.

1. Que su cuenta en determinado banco está bloqueada y de no contestar la llamada o el correo en pocos días, ésta será cancelada. En caso de que la víctima conteste, le informan que para solucionar el problema el banco requiere la contraseña de la cuenta.
2. Que representan a una institución de beneficencia, como la Cruz Roja, Unicef, etcétera, e invitan a la víctima a realizar una donación por una cantidad muy pequeña, para ello sólo debe proporcionar su número de tarjeta de crédito o de débito y la contraseña para hacer el cargo.
3. Que se trata de una persona extranjera que acaba de heredar una gran fortuna (varios millones de dólares o euros) y que requiere sacar ese dinero de su país, alegando ciertos problemas, y que el objetivo de su llamada o correo es pedirle a la víctima que lo ayude en esta acción, prestándole su cuenta bancaria para el depósito, a cambio éste promete darle de 10 a 20 por ciento de la suma total. Para tal acción, es obvio que quien engaña requiere obtener el número de la cuenta bancaria de la víctima y la contraseña.
4. Que el motivo del contacto con la víctima es comunicarle que Internet acostumbra realizar loterías mundiales a las personas que tienen una

cuenta de correo, ya sea de Yahoo, Hotmail, Gmail, etcétera, y que ella ha sido la ganadora de ese sorteo.

La forma de comunicarse con la víctima potencial está muy bien estudiada y si quien se comunica con ella es extranjero, por lo común los mensajes y todos los diálogos están perfectamente bien escritos, con nombre de la empresa, el nombre del remitente, el teléfono y los cargos que ostenta quien firma la carta, e incluso muchas veces incluyen logotipos de la empresa.

De acuerdo con el ingeniero social más famoso a nivel mundial, Kevin Mitnik, se puede engañar o manipular a una persona para obtener información privilegiada, atendiendo al ego de las personas, como se describe a continuación.

1. Si por hacer una donación monetaria a la Cruz Roja o Unicef me prometen que mi nombre va a aparecer en una lista de donadores voluntarios, entonces sí voy a donar dinero o "voy a dar dinero porque soy buena persona".
2. Si me avisan que me saque la lotería en Internet, "ya era tiempo de que la suerte se fijara en mí, seré rico sin esfuerzo".
3. "Voy a dar los datos que me pide un desconocido acerca de la empresa, para que todos vean que sí coopero con la organización".

Claro que cada una de estas acciones implica proporcionar un número de cuenta bancaria, contraseñas, datos de acceso a sistemas, etcétera. Incluso cuando el aviso por Internet es que la víctima se sacó la lotería en algún país de Europa, se pide dinero para enviar el cheque millonario a través de alguna reconocida empresa de mensajería. En este caso, quizá no se pida mucho dinero por enviar el cheque, por lo que la víctima accederá a enviarlo sin sospechar algún riesgo, pensando que prácticamente ya es millonaria; no obstante, si la víctima accede a pagar el dinero, enseguida le pedirán dinero extra por comisiones por la expedición del cheque y otros gastos menores; luego, vendrá la presión de tiempo, diciendo a la víctima que sólo tiene uno o dos días

para enviar el dinero, de lo contrario perderá todo lo que ha enviado, "porque así son las reglas de ese tipo de lotería", etcétera.

Como se puede deducir de los ejemplos anteriores, todo ingeniero social tiene muy estudiada la psique del ser humano y sabe muy bien cuáles son sus debilidades, a fin de aprovecharse de éstas. Por esa razón, se considera que el usuario de una computadora, ya sea desde su casa o su lugar de trabajo en una empresa, debe estar advertido acerca de los tipos de engaño a los que siempre está expuesto. En este mismo sentido, las empresas tienen la enorme tarea de capacitar a sus empleados y fijar reglas muy claras acerca de los protocolos que deben seguirse para cuando un extraño, o una persona "que parece pertenecer a la empresa", pida cierta información. El empleado debe saber distinguir y clasificar con plena consciencia toda aquella información que en manos de algún extraño resultaría fatal para la empresa, por lo que en caso de que ese tipo de información sea requerida por alguien, primero debe negar su entrega y luego notificar de inmediato a su jefe de área, acerca de quién y cuándo fueron solicitados esos datos, lo cual sólo se logra con una adecuada capacitación.

4.4 La seguridad lógica en las redes

Hoy día, existen múltiples formas de atacar a una computadora personal o a una red de computadoras, ya sea por medio de Internet o mediante ataques directos. A la seguridad (o inseguridad) de este tipo se le llama *seguridad lógica,* término que hace alusión a la lógica matemática y a la logística que priva en cualquier computadora. En esta sección sólo se presentan algunos de los ataques más comunes sobre computadoras que se tienen registrados, ya sea de manera individual o en red, por lo que la lista no es exhaustiva.

Suplantación de la dirección IP

Esta técnica consiste en suplantar una dirección IP de un paquete IP de la computadora que envía dicho paquete por la dirección IP de otra computadora, lo que le permite al atacante enviar paquetes de manera anónima. El uso de un

proxy podría dar la posibilidad de ocultar la dirección IP, con suplantación de IP, pero como los proxy sólo envían paquetes, aunque la dirección parezca que está oculta, es relativamente sencillo localizar a un atacante mediante el archivo de registro proxy. En cambio, un firewall no puede interceptar los paquetes que envía el atacante, ya que las reglas de filtrado de una firewall indican las direcciones IP que tienen autorización para comunicarse con las computadoras de, por ejemplo, una LAN, pero si la dirección IP de la computadora origen se ha suplantado, parecerá que el paquete ha sido enviado desde una computadora de la LAN y el firewall lo dejará pasar, pues como se dijo antes un firewall sólo rechaza paquetes con IP externos no autorizados.

En el formato de un datagrama, la suplantación de la dirección IP implica modificar el campo *Dirección IP origen*, para simular que el paquete proviene de otra dirección IP. Sin embargo, un paquete que se envía por Internet, que es la vía de ataque, normalmente utiliza un protocolo TCP (Protocolo del Control de Transferencia), por lo que el paquete enviado por el atacante parece confiable. Los datagramas IP agrupan paquetes TCP llamados segmentos, que tienen dentro de su formato un *número de acuse de recibo,* de modo que antes de aceptar un paquete, la computadora (o el servidor) receptor del datagrama, genera el número de acuse de recibo enviado por la computadora que envía el paquete, mientras la computadora que envía el paquete sólo espera la confirmación del receptor, que es el número de acuse, para que el paquete sea enviado y aceptado; es decir, este número es una confirmación tanto del envío como de la recepción del paquete. El efecto que causa la suplantación del IP es que invalida al equipo receptor, por lo que a dicho equipo sólo le queda esperar la información que contiene el acuse de recibo y el número de secuencia correcto; sin embargo, el atacante desconoce este número y tiene que enviarlo al servidor receptor para establecer la conexión sin levantar sospechas en el receptor. Este dato lo puede encontrar si observa el campo *opciones* que contiene el formato de *segmentos* que contienen los paquetes TCP (véase capítulo 3, Características de una PKI y de una PMI), para indicar al paquete la ruta de retorno segura, además de rastrear los puertos abiertos; con esto podrá enviar el acuse de recibo con el número de secuencia correcto.

Uso de rastreadores de red

Casi todos los protocolos de Internet no están cifrados, por lo que cuando se navega por una red sin utilizar un protocolo HTTPS (recuérdese que la S indica que se trata de un protocolo seguro) es posible interceptar la información que se envía o se recibe, como contraseñas o números de cuentas bancarias; esto lo logra un atacante con rastreadores de puertos.

Un analizador de red, o un atrapador de información de la red, como también se le conoce, permite supervisar toda la información que pasa a través de una tarjeta de red, sobre todo si esta tarjeta es inalámbrica. En un inicio, el analizador o rastreador de red se desarrolló para que los administradores de redes supervisaran el flujo de información que viaja por una red y pudieran detectar cualquier problema relacionado. Pero si un atacante pudiera tener acceso físico a la red, también sería capaz de analizar la información que viaja por la red y tomar la que necesite para sus intenciones; en redes inalámbricas incluso su trabajo se facilita, pues en éstas sólo necesita captar las señales que envía el router para poder analizar la información, lo que significa que ni siquiera requiere el contacto físico con la red.

Debido a que los analizadores de red son de uso cotidiano para los verdaderos administradores de redes, éstos también son accesibles y pueden ser utilizados por personas con malas intenciones; como contraparte, se desarrollaron los sistemas de detección de intrusos (IDS, por sus siglas en inglés; Intrusion Detection System), que son software de detección de accesos no autorizados a computadoras personales o redes.

Un IDS trabaja por medio de un analizador de paquetes, que es un software que captura las tramas de una red, y por trama debe entenderse que, de acuerdo con la topología de la red, es necesario el uso de cable coaxial, fibra óptica o par trenzado; es decir, cables que conectan físicamente a las computadoras de una red, por lo que es posible que una computadora capture un flujo de información que no está destinado a esa computadora. Este analizador de paquetes pone la tarjeta de red de manera que la capa de enlace de datos (véase modelo OSI en el capítulo 5, Firewalls como herramientas de seguridad) no elimine las tramas no destinadas a la dirección de *control*

de acceso al medio (MAC, por sus siglas en inglés; Media Access Control)[1]. Los analizadores de paquetes se pueden utilizar de diversas formas; por ejemplo, para monitorear redes, con el propósito de detectar y analizar fallas, o para determinar la estructura de un protocolo, con el fin de determinar cada componente, cómo funciona y cómo se diseñó. Con estas ventajas, un analizador de paquetes, desde luego, también puede ser utilizado por un atacante con fines maliciosos, como espiar correos electrónicos, robar contraseñas o apoderarse de cualquier otro tipo de información que sea de su interés. De esta forma, el analizador de paquetes supervisa todo el tráfico que viaja por la red.

Como parte de un IDS, un analizador de paquetes entre otras cosas, captura contraseñas sin cifrar y el nombre de usuario de la red, cualidad que puede ser utilizada por cualquier intruso, además de que también puede medir el tránsito de la red para descubrir dónde hay cuellos de botella[2], creación de registros de red, con lo cual los intrusos no pueden detectar que están siendo investigados, ya que su intrusión queda registrada para posteriores investigaciones de parte de un administrador de la red.

Cuando el tránsito de información no pasa por el analizador de paquetes, ese tránsito se compara con formas conocidas de ataques o de comportamientos sospechosos, como el escaneo de puertos[3], paquetes mal formados y otro tipo de ataques. La ventaja del IDS es que no sólo analiza el tipo de tránsito, sino que también revisa el contenido de la información y su comportamiento. Para realizar la comparación, un IDS normalmente tiene una base de datos de ataques conocidos.

Una excelente medida de seguridad contra un rastreador de red, sobre todo si es utilizado por un atacante, es usar un IDS integrado con un firewall, ya que si el IDS trabaja sólo no podría detener los ataques, excepto si trabaja

---

[1] La dirección MAC es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física y es única para cada dispositivo que pertenece a una red.

[2] *Cuello de botella* es un término que se utiliza en ingeniería industrial para determinar el o los factores que en un momento dado detienen el funcionamiento normal de una línea de producción.

[3] Un escáner de puertos o escaneo de puertos es la acción de analizar, por medio de un programa, el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado o protegido por un firewall.

con un Gateway (véase capítulo 5, Firewalls como herramientas de seguridad), el cual permite interconectar las computadoras de una red usando un protocolo de comunicaciones[4] y arquitecturas diferentes a todos los niveles de comunicación; o bien, si trabaja con un dispositivo de puerta de enlace que funcione como un firewall. De este modo, los paquetes deberán pasar forzosamente por estos filtros, y la mayoría de los paquetes maliciosos serán detectados antes de hacer daño a la red.

Cualquiera de las siguientes dos técnicas son utilizadas por un IDS para determinar que está sufriendo un ataque:

1. **Comparación de las características de un paquete que circula por la red con el perfil de un ataque conocido.** Sin embargo, la comparación toma tiempo, y en este tiempo de búsqueda el IDS no puede identificar que está siendo atacado.
2. **Encontrar anormalidades en el comportamiento normal de la red respecto al ancho de banda utilizado, protocolos, puertos y dispositivos interconectados normalmente.** Si el IDS detecta cualquier anormalidad mostrará una alerta.

Ataques a servidores de la Web

La dirección web o el localizador de recurso uniforme (URL, por sus siglas en inglés; Uniform Resource Locator) es un recurso con el que cuenta la Web para especificar su localización en una red de computadoras y poder tener acceso a esa localización. Se trata básicamente de la dirección que se utiliza para páginas web (HTTP), aunque también se utiliza para transferencia de archivos (ftp), correo electrónico (mailto), acceso a base de datos (JDBC) y algunas

[4] Un protocolo de comunicaciones es un sistema de reglas o el estándar que define la sintaxis, la semántica y la sincronización de la comunicación, que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre sí para transmitir información o datos por medio de cualquier tipo de variación de una magnitud física. El protocolo también contiene los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software o por una combinación de ambos.

otras aplicaciones. Los buscadores de la Web muestran una página web en el espacio de direcciones superior de la pantalla, que tiene la forma de http://. tecorizaba.edu/index.html, el cual indica un protocolo http, un nombre del huésped (tecorizaba.edu) y el nombre de un archivo (index.html).

La parte vulnerable de URL es el acceso a bases de datos con la tecnología de conectividad para bases de datos de Java (Java Standard Edition Platform) de Oracle, que es una tecnología de interface para programar aplicaciones, que define la forma en que un usuario puede accesar a una base de datos para solicitar y actualizar datos. Si el atacante logra accesar a la base de datos (orientada a bases de datos relacionales) de una computadora personal o al servidor de una red, podrá solicitar datos y actualizarlos, lo que significa robar información o modificarla para su beneficio. Sin embargo, con una conexión JDBC[5] es posible tener disponibles comandos de creación y ejecución, como *insert, update, delete* y *select*, o invocar procedimientos de almacenamiento.

Inyección SQL

El método de inyección SQL permite que un código intruso entre a una aplicación en el nivel de validación de las entradas, para realizar operaciones sobre una base de datos. El lenguaje estructurado para consulta (SQL, por sus siglas en inglés; Structured Query Language) es un lenguaje basado en el desarrollo de programas que especifican o declaran un conjunto de condiciones, proposiciones, afirmaciones, restricciones, ecuaciones o transformaciones que describen el problema y presentan la solución. Permite el manejo del álgebra y el cálculo relacional[6], lo cual admite consultar las bases de datos para recuperar información de manera sencilla y hacer cambios en la información que poseen las bases de datos.

[5] JDBC es un estándar Java API para poder accesar a bases de datos relacionales y a algunos almacenes de datos.

[6] El cálculo relacional es un lenguaje de consulta que describe la respuesta deseada sobre una base de datos, sin especificar cómo obtenerla, a diferencia del álgebra relacional que es de tipo procedimental o el cálculo relacional que es de tipo declarativo, aunque ambos métodos siempre logran los mismos resultados.

El origen de la vulnerabilidad radica en que no se verifican de manera correcta las variables utilizadas en un programa que contiene o genera un código SQL, esto es un error que sucede en cualquier lenguaje de programación que está incorporado a otro lenguaje, y por eso es posible incrustar un código intruso dentro del código SQL programado, con lo cual se altera el funcionamiento normal del programa, pues éste ya contiene un código adicional en la base de datos.

Cuando alguien, por lo común un hacker o un cracker, logra "agregar" ese código extra a la base de datos, lo hace para dañar o espiar la información de la base de datos, lo cual se logra más fácilmente cuando el programa se desarrolló con descuido o con ignorancia del problema, exponiendo a un riesgo la seguridad del sistema; por ejemplo, si al programar hay un simple olvido de anotar comillas en el programa, esto puede ser suficiente para volver vulnerable a ese programa, ya que una inyección de código SQL se aprovecha de la sintaxis en este lenguaje para introducir comandos de manera ilícita que permitan leer o modificar la base de datos, comprometiendo el contenido de la consulta original. Una vez que el intruso ha logrado entrar mediante la inyección o adición de este código, éste puede modificar valores en la base de datos en forma arbitraria, instalar cualquier tipo de malware, tener privilegios extras con el uso de las vulnerabilidades del sistema operativo o atacar usuarios de páginas web con inyecciones de código HTML o scripts.

Cuando se ejecuta un programa vulnerable es posible "agregar o inyectar" el nuevo código. Si esta acción se ejecuta en un sitio web, tiene lugar en el servidor huésped. Una inyección de código puede resultar en la pérdida o la corrupción de datos, falta de responsabilidad en acciones o denegación de acceso. Una inyección es capaz, incluso, de tomar control total de un nodo.

Pero el sistema se vuelve más vulnerable cuando en un programa se arma una sentencia SQL en forma descuidada en el intervalo de tiempo en que un programa de la computadora se ejecuta en un sistema operativo, que inicia al poner en la memoria principal el programa, por lo que el sistema operativo empieza a ejecutar sus instrucciones, y concluye al enviar al sistema operativo la indicación de terminación. Otro momento de vulnerabilidad se produce durante la fase de desarrollo, cuando el programador indica directamente

la sentencia que se debe ejecutar, pero lo hace de manera desprotegida. Cuando el programador va a hacer una consulta en la base de datos, y hace uso de los parámetros a ingresar por parte del usuario, es dentro de esos parámetros en que se puede "agregar o inyectar" un código adicional malintencionado. En el tiempo en que el programador hace la consulta, el código maligno, que ya forma parte de la base de datos, también se ejecuta y pone en práctica cualquiera de los comandos que se han señalado (*insert*, *update*, *delete* y *select*).

La inyección de encabezado HTTP es un área relativamente nueva para los ataques basados en la Web, que se produce cuando los encabezados del protocolo de transferencia de hipertexto (HTTP) se generan dinámicamente en función de la entrada del usuario. La inyección de cabeceras en las respuestas HTTP puede permitir la división de respuestas HTTP en la falsificación de solicitudes en un sitio de cruce de información (CSRF, por sus siglas en inglés; Cross Site Request Forgery) y los ataques de redireccionamiento maliciosos a través de la cabecera de ubicación del HTTP.

Existe otra forma de ataque mediante la inyección de comandos, por lo que es importante que los administradores de red conozcan que cualquier dato es factible de ser modificado, ya sea que vaya hacia un buscador o salga de éste, por lo que se recomienda que cada dato de entrada sea validado en el mismo servidor y que el usuario no pueda controlarlo. Esto significa que el administrador de la red deberá configurar el servidor para que haga una autenticación en el directorio de cada archivo que éste contenga.

Un atacante con cierta experiencia logra modificar los parámetros *accountnumber* y *debitamount*, con el fin de obtener un beneficio monetario de esta acción, ya que en general estos parámetros están asociados a cuentas y operaciones bancarias. Asimismo, también pueden ser modificados los parámetros de atributos que tienen datos únicos y que caracterizan el comportamiento de la página que se envía. En la actualidad, hay aplicaciones web para compartir contenidos que sólo permiten que el creador del contenido pueda modificar la información, ya que ésta verifica que el usuario que solicita acceso es el verdadero autor del contenido. Pero, si es un atacante quien solicita el acceso y le es negado, al modificar el parámetro mode readwrite, él podría obtener el permiso para entrar al contenido. Cualquier mecanismo de

validación que no sea suficientemente robusto, siempre será una debilidad del sistema que permita ataques maliciosos.

Correo spam

Se refiere a los correos que se reciben sin ser solicitados, en general de publicidad. También se les conoce como correos basura o mensajes basura. Su principal característica es que el remitente es anónimo. Desde su aparición, este tipo de correo se ha enviado a grupos de noticias, motores de búsqueda, redes sociales, foros y blogs. No obstante, en fechas recientes se utiliza con mucha mayor intensidad el correo electrónico y la telefonía móvil, a través de mensajes de texto, para el envío de spam.

La práctica del envío de correo spam se sustenta en las deficiencias de los protocolos de red, las cuales aprovecha muy bien. El protocolo de transferencia simple de correo (SMTP, por sus siglas en inglés; Simple Mail Transfer Protocol) es el protocolo que se utiliza para el intercambio de mensajes de correo electrónico entre computadoras y entre otros dispositivos, como los teléfonos móviles, la mayoría de los cuales ya cuentan con la aplicación de correo electrónico. El SMTP se define como el estándar oficial de Internet RFC 2821.

El protocolo es muy útil para enviar correos, pero tiene algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino, por lo que ha sido necesario asociar otros protocolos a SMTP, como el Protocolo de la Oficina de Correos (POP, por sus siglas en inglés; Post Office Protocol), que ya está en su versión 3, y que se utiliza para obtener los mensajes de correo electrónico almacenados en un servidor remoto; en el modelo OSI se le cataloga en la capa de aplicación.

Otro protocolo asociado a SMTP es el Protocolo de Acceso a Mensajes de Internet (IMAP, por sus siglas en inglés; Internet Message Access Protocol), que permite tener acceso a mensajes almacenados en un servidor de Internet; de este modo, por medio de IMAP se puede tener acceso al correo electrónico desde cualquier equipo que esté conectado a Internet. Tiene una ventaja sobre POP, ya que IMAP permite visualizar los mensajes de manera remota sin descargar los mensajes, como lo hace POP.

SMTP es un protocolo orientado a la conexión basado en texto, en el que un remitente de correo se comunica con un receptor de correo electrónico mediante la emisión de secuencias de comandos, proporcionando los datos necesarios de manera ordenada y confiable, normalmente un protocolo de control de transmisión de conexión (TCP). Una sesión SMTP consiste en comandos originados por un cliente SMTP (el agente de inicio, emisor o transmisor) y las respuestas correspondientes del SMTP del servidor (el agente de escucha o receptor), con el propósito de que la sesión se abra y se intercambien los parámetros de esta sesión. El intercambio de información de SMTP se compone de tres secuencias de comando.

1. MAIL. Comando para establecer la dirección de retorno, también conocido como Return-Path, remitente o sobre.
2. RCPT. Comando para establecer un destinatario del mensaje.
3. DATA. Comando para enviar el mensaje de texto. Éste es el contenido del mensaje, en lugar de su envoltura. Se compone de una cabecera de mensaje y el cuerpo del mensaje separado por una línea en blanco.

Un usuario de correo electrónico tiene en su configuración, la dirección IP de su servidor SMTP inicial, que está anotada como un nombre DNS, el cual, a nombre del usuario, puede enviar mensajes al exterior. Por tanto, los administradores de redes siempre deben tener disponibles los servidores para los usuarios, así como tomar las medidas pertinentes frente a cualquier amenaza. En la actualidad, para utilizar los servidores SMTP se requiere de una autenticación por parte de los usuarios antes de permitir el acceso. Mediante este procedimiento de autenticación, el servidor SMTP obtiene los servicios de un proveedor de servicios de Internet (ISP por sus siglas en inglés, Internet Service Provider).

Este proveedor puede estar organizado de diferentes formas, por ejemplo puede ser sólo para fines comerciales o con fines no benéficos o privados; en general, el servicio que ofrecen los proveedores incluye acceso y tránsito

en Internet, nombre de dominio, hosting en la Web, servicio de Usenet[7] y colocación. De esta forma, el SMTP no permite el acceso a usuarios que estén fuera de la red de un ISP. De hecho, sólo se permite el acceso a usuarios cuya dirección IP fue proporcionada por un ISP, lo que garantiza que todos los usuarios están con el mismo proveedor de Internet.

El problema es que el SMTP original no facilita los métodos de autenticación de los emisores de mensajes, por lo que, a pesar de las restricciones de acceso, el problema del spam sigue vigente; aunque Internet mail 2008 ha resuelto en parte el problema.

Una de las metodologías más aceptadas para evitar el spam es el Correo Identificado con Clave de Dominio (DKIM, por sus siglas en inglés; Domain Key Identified Mail), también llamado *identificador de correo electrónico.* Dicha metodología permite a una organización responsabilizarse del envío de mensajes, para que éstos puedan ser validados por el destinatario. Esta metodología surgió de la necesidad de autenticar mensajes debido a la falsificación de contenidos que usa un correo spam; el spammer (persona que envía el spam) puede falsear la cabecera de un mensaje para engañar al receptor para que acepte y lea el mensaje. El problema real del spam no consiste tanto recibir publicidad, sino que mucha pornografía es spam y puede llegar fácilmente a niños que tengan una cuenta de correo, y como la dirección de dominio es falsa, no hay forma de reclamar a alguien.

Para evitar todo tipo de spam, en especial el que causa algún tipo de daño, el DKIM utiliza el cifrado de clave pública (véase capítulo 5, Firewalls como herramientas de seguridad), lo que le permite al emisor firmar en forma electrónica los correos que envía a fin de que el destinatario pueda verificar el origen y confiar en que dichos correos son legítimos; es decir, que no está

---

[7] Usenet, establecido en 1980, es un sistema mundial para realizar foros de discusión, donde los usuarios pueden leer y enviar artículos o comentarios a los que se les llama colectivamente *noticias*.

Es el precursor de los *Foros de Internet* muy difundidos en la actualidad. Usenet es un híbrido entre el correo electrónico y los foros en la Web. Todas las contribuciones que hacen los participantes se almacenan secuencialmente en un servidor. El servicio se distribuye entre un gran número cambiante de servidores que almacenan y reenvían mensajes hacia otros servidores. El usuario individual puede leer los mensajes y enviarlos a un servidor local operado por un proveedor comercial de Usenet, que puede estar en una universidad, en un centro de trabajo o en la propia computadora, etcétera.

falsificada la dirección. Cualquier correo proveniente de estas organizaciones lleva una firma DKIM.

Otro tipo de tecnología para evitar el spam y otros correos dañinos es el Reporte y Conformidad de la Autenticación de Mensajes basada en el Dominio (DMARC, por sus siglas en inglés; Domain Based Message Authentication, Reporting and Conformance), que es un sistema de validación de correos capaz de detectar spoofing y spam por medio de un mecanismo que permite el envío y la recepción de correos electrónicos, al tiempo que verifica que el correo que se recibe de cierto dominio está autorizado por los administradores de ese dominio y que durante el tránsito de la información a través de la red no se han modificado los archivos adjuntos y el mensaje de dicho correo.

La tecnología se basa tanto en el DKMI, así como en la Estructura de la Política del Remitente (SPF, por sus siglas en inglés; Sender Policy Framework). La SPF es un mecanismo que permite verificar que cuando se recibe un correo, el dominio del correo viene de un host autorizado por los administradores del dominio.

La combinación y uso simultáneo de DKIM y SPF permite la especificación de los procedimientos para el manejo del correo que se está recibiendo, basado en los resultados de ambas tecnologías, lo que proporciona un reporte de las acciones realizadas bajo esas políticas. Una de estas políticas es que permite al dominio del remitente indicar que sus correos están protegidos por SPF y por DKIM, comunicando al receptor del correo lo que debe hacer si el correo enviado no aprueba los filtros de SPF ni de DKIM. Por lo común, lo que se aconseja al receptor del correo es eliminar el mensaje, con lo cual se elimina, o al menos limita, la amenaza de ser víctima de fraudes o a recibir mensajes dañinos. La política de DMARC también permite al receptor del correo enviar un reporte al remitente acerca de los mensajes que fueron aceptados o rechazados de acuerdo con la evaluación de autenticación que realizó la tecnología DMARC.

Otra tecnología que trabaja de manera conjunta con el protocolo SMTP para evitar correos dañinos son las Extensiones Multipropósito de Correo por Internet (MIME, por sus siglas en inglés; Multipurpose Internet Mail Extensions), una serie de especificaciones dirigidas al intercambio transparente de

todo tipo de archivos y mensajes a través de Internet. Hoy día, prácticamente todos los correos electrónicos escritos (no páginas web) que se envían por Internet se transmiten en formato MIME, a través del protocolo SMTP. Los tipos de contenido definidos por el estándar MIME también incluyen protocolos de red, como HTTP de la Web, el cual requiere que los datos sean transmitidos en un contexto de mensajes de correo electrónico, de manera que en la actualidad ningún programa se considera completo si no acepta MIME en sus diferentes tipos, como textos o formatos de archivo, ya sea un correo electrónico o un navegador de Internet.

A pesar del uso de MIME, el remitente de un correo spam puede controlar las direcciones que sí leen ese tipo de correos por medio de pequeñas imágenes, casi invisibles en una página web o en un mensaje de correo electrónico; a esta pequeña imagen se le llama baliza web o faro web, y puede ser tan pequeña como un pixel en formato GIF (Graphics Interchange Format o Formato de intercambio de gráficos) y de color transparente, la cual constituye una forma de spyware.

Como se puede ver, no existe una forma totalmente exitosa de evitar los correos spam, así que lo más simple es no responder a ese tipo de correos sospechosos, desactivar HTML del correo electrónico y denunciar el spam; además, algunos sistemas solicitan contraseñas de los remitentes, con lo cual éstos saben que no pueden utilizar con tanta facilidad ese correo para enviar los spam.

Ataques de secuencias de comandos

Scripting es una serie de instrucciones que se invocan en una computadora para que se ejecuten en un orden particular, por ejemplo, cuando en el link de un website se da un clic. A las vulnerabilidades XSS o CSS se les conoce como vulnerabilidades Cross Site Scripting (CSS). El CSS es un lenguaje de estilo, es decir, un lenguaje de computadora para expresar la presentación de documentos estructurados y diseñado para que sea visible la separación del contenido de un documento de la presentación de dicho documento, tanto en la distribución física de su contenido, como en los colores y en el tipo de letra. Junto con HTML y Java Script, CSS se ha convertido en una tecnología de referencia

para el diseño de sitios web, con el uso de interfaces para aplicaciones web y para aplicaciones de teléfonos móviles.

Las vulnerabilidades son un tipo de ataque muy peligroso debido a las múltiples aplicaciones que están disponibles en Internet; sin embargo, sólo los sitios web de contenido dinámico, que hasta hoy son la mayoría, pueden tener la vulnerabilidad CSS. Existen dos tipos de ataques CSS, el *reflejado* y el **almacenado**.

La vulnerabilidad *reflejada* tiene lugar cuando un usuario desconocido entra a una aplicación o sitio web. El ataque se efectúa a través de una serie de parámetros del URL (Uniform Resource Locator), los cuales se envían por el propio URL, mediante correos electrónicos, mensajes instantáneos, blogs, fórums o cualquier otro método que ofrezca esta posibilidad. Quien utiliza la computadora piensa que el usuario desconocido no dará un clic en una liga que parece que llevará a hacer algo dañino; sin embargo, donde ocurre el ataque reflejado es al utilizar Javascript, así que una vez que se ha abierto el correo o se ha visitado un sitio web es cuando se ejecuta el ataque, el cual normalmente tiene un código URL o un código hex, o algún otro método de codificación que hace que la URL parezca válida.

Por otro lado, la vulnerabilidad CSS *almacenada* tiene lugar cuando el atacante puede almacenar el ataque, el cual se recupera del almacén un poco después y se aplica sobre un usuario desconocido; el ataque se almacena de tal forma que sea posible ejecutarlo tiempo después. Para almacenar un método de ataque puede usarse una base de datos, un wiki o un blog. Así, cuando un usuario desconocido encuentra el ataque almacenado, éste se ejecuta. El método de almacenamiento presenta problemas de verificación incorrecta tanto para la validación de ingreso, como para la validación de salida de la base de datos. Incluso, puede suceder que se haya hecho un chequeo para validar el ingreso, pero si no se hizo el mismo procedimiento para la salida, el ataque también se producirá. Cabe resaltar que si se verifica y valida la salida de la base de datos, se pueden descubrir aspectos ocultos durante el proceso de validación de ingreso.

La vulnerabilidad CSS *almacenada* es más perjudicial que la reflejada. Pues el ataque *reflejado* constituye un ataque dinámico, en tanto que el ataque

almacenado sólo se almacena una vez, pero permanece vigente. Esto no significa que sólo se deban hacer pruebas del ataque *almacenado*, sino que lo más recomendable es verificar y comprobar si existe la posibilidad de sufrir cualquier tipo de ataque. Es importante destacar que hoy día ambos tipos son muy comunes, sobre todo en las aplicaciones.

Una variante del ataque CSS *almacenado* ocurre cuando se comparte una base de datos con otras aplicaciones, por tanto hay que tener cuidado cuando una nueva aplicación pueda almacenar este tipo de ataque y que la aplicación normal que utiliza el usuario usa el mismo contenido. Si el usuario no tiene forma, o no sabe, verificar que los datos almacenados por la nueva aplicación están validados, sólo debe recordar que en la aplicación que tiene, y con la cual no ha tenido problemas, debe validar la salida del mensaje. Si la aplicación no valida la salida, a pesar de que el usuario haya validado el ingreso, la nueva aplicación todavía tiene probabilidad de ser vulnerable. Se recomienda checar todos los métodos por los cuales se pueden almacenar y recuperar los datos. Se insiste en que no es suficiente validar el ingreso de datos, pues esto no significa que otro método o aplicación almacene datos malignos, los cuales van a emerger cuando se haga uso de la aplicación.

Aunque existen varios métodos de verificación para detectar este tipo de vulnerabilidad, este texto no intenta ser un manual operativo para detección de vulnerabilidades, por lo que aquí sólo se hace hincapié en que la validación es muy importante y que es mejor validar el ingreso cuando se está cargando una aplicación y ésta se va a almacenar, es decir, no hay que hacer la validación cuando la aplicación ya está cargada, además de que también es importante verificar la salida, es decir, cuando se utiliza la aplicación. La salida siempre debe estar correctamente codificada en html, pero si no es así, en vez de ejecutar el tag[8] ‹script›‹/script›, se debería codificar correctamente en html para evitar la vulnerabilidad.

[8] Tag, traducido como etiqueta, se refiere a un conjunto de letras o símbolos que se escriben antes y después de un texto o de datos para identificarlos, o con el fin de mostrar que esas letras o datos van a tener un tratamiento particular.

Análisis de puertos

Uno de los métodos que más utilizan los hackers es la búsqueda de puertos abiertos para la comunicación, acción que efectúan al enviar mensajes a los puertos del equipo con el propósito de localizar los puntos de vulnerabilidad, pero el análisis de los puertos no representa una puerta de acceso a un sistema remoto, por lo que en un inicio sólo se considera un intento de intrusión. En general, el estado de los puertos se considera como *abierto* o *cerrado*.

Se considera que un puerto está *abierto* si acepta paquetes UDO o conexiones TCP. El Protocolo de Datagrama de Usuario (UDP, por sus siglas en inglés; User Datagram Protocol) es un protocolo que actúa en la capa 4 de transporte del modelo OSI, que se basa en el intercambio de datagramas. UDP permite el envío de datagramas a través de la red, sin haber establecido una conexión previa, ya que el propio datagrama contiene suficiente información de direccionamiento en su encabezado; además, tampoco tiene confirmación ni control de flujo, ni se puede saber si se ha entregado de modo correcto, ya que no hay confirmación de entrega o recepción. En UPD, el nivel de transporte de datagramas no es confiable, pues sólo incluye la información necesaria para la comunicación extremo a extremo al paquete que envía al nivel inferior, por lo que principalmente se emplea en trabajos de control y en la transmisión de audio y video a través de la red. No introduce retardos para establecer la conexión y no realiza seguimiento de esos parámetros, por lo que un servidor dedicado a cierta aplicación puede soportar más usuarios activos cuando la aplicación corre sobre UDP en vez de sobre TCP.

Por su parte, el Protocolo de Control de Transporte (TCP, por sus siglas en inglés; Transport Control Protocol) es un protocolo fundamental en Internet, ya que proporciona un transporte confiable sobre grandes cantidades de información entre aplicaciones, liberando al programador de gestionar la confiabilidad de la conexión que gestiona el propio protocolo. Sin embargo, para lograr que el envío de información sea confiable, se tiene que incluir mucha información a los paquetes que se envían, lo que disminuye su eficiencia. Los paquetes que se envían tienen un tamaño máximo, de manera que si el protocolo incluye mucha información para ser enviado con toda confianza, dismi-

nuye la cantidad de información que proviene de la aplicación que contiene el paquete. Si es más importante la velocidad que la confiabilidad, se prefiere utilizar UDP, ya que al utilizar TCP lo que se asegura es que el paquete se va a recibir en el destino correcto, aunque quizá a menor velocidad, pues depende del tamaño del paquete.

Por un lado, están los hackers que saben que un puerto abierto representa una vulnerabilidad, así que lo primero que hacen es una prueba de intrusión para aprovechar los puertos abiertos, y por otro lado están los administradores de red que intentan utilizar todas las herramientas que tienen a la mano, como los firewall, para cerrar los puertos, pero con la consigna de que los usuarios de la red no pierdan acceso al servicio. Un puerto abierto es importante para los usuarios casuales de una red, pues son los que utilizan estos puertos de manera temporal, así que el dilema del administrador es proteger los puertos de intrusiones, pero a la vez mantener algunos abiertos para usuarios casuales o repentinos.

Un puerto cerrado resulta accesible y útil para determinar si un equipo está activo en determinada dirección IP y es parte de detección del sistema operativo. Un puerto se puede cerrar con un firewall, en cuyo caso se considera que están filtrados, que es lo que hace el firewall. El filtrado no sólo es efecto de la acción de un firewall dedicado, también puede filtrarse por las reglas de un router (enrutador) o por un firewall que tenga el propio equipo. Un puerto filtrado es una buena protección contra atacantes, pues proporcionan poca información, aunque lo más común es que un firewall sólo rechace las solicitudes de acceso, sin responder algún tipo de mensaje.

Para saber la condición de un puerto, es decir, para conocer si está abierto o cerrado, se utiliza un *analizador de puertos* o *escáner de puertos,* que es una máquina que tiene un programa y está conectada a una red de comunicaciones, lo que le permite detectar si un puerto está abierto, cerrado o protegido por un firewall; esta detección o análisis indica posibles vulnerabilidades a la seguridad, dependiendo de los puertos que están abiertos, además, también puede detectar el sistema operativo que se está ejecutando en una computadora, según los puertos que tenga abiertos. Con base en este punto de vista, y como muchas otras herramientas informáticas, un analizador de

puertos se desarrolló en un inicio para ser utilizado sólo por los administradores de redes, con el propósito de detectar posibles problemas de seguridad, no obstante hoy día también es utilizado por atacantes para detectar puntos de vulnerabilidad.

Aunque se conocen diversos y variados rastreadores de redes, tal vez el más conocido y utilizado es Nmap, que es un programa de código abierto, que originalmente fue creado para Linux, aunque en la actualidad es multiplataforma. Para evaluar la seguridad de sistemas informáticos y detectar servicios o servidores en una red, Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas. Por ejemplo, si se está utilizando un TCP, la computadora o servidor de origen envía un paquete SYN[9] a la computadora destino, la cual responde con un paquete SYN/ACK, que es la confirmación de que se ha hecho la conexión TCP.

El rastreador de puertos envía muchos paquetes SYN a la computadora que se está probando y observa la respuesta que indica el estado de los puertos en el destino; si la respuesta es SYN/ACK, el puerto está abierto y escuchando conexiones, si la respuesta es un paquete RST[10], el puerto está cerrado, pero si no regresa ninguna respuesta, entonces el puerto tiene un filtro de firewall.

Si se está utilizando un protocolo UDP, aunque no está orientado a la conexión ni tiene paquetes SYN, como el TCP, también es posible realizar un rastreo de puertos. Si se envía un paquete con el rastreador y el puerto no

[9] SYN es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión durante el procedimiento de establecimiento de tres fases (3 way handshake). Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo). Un ACK (del inglés acknowledgement —en español acuse de recibo—) es un mensaje que el destino de la comunicación envía al origen de ésta, con el fin de confirmar la recepción de un mensaje. Si dicho mensaje está protegido por un código detector de errores y el dispositivo de destino posee además capacidad para procesar dicha información, el ACK también puede informar si se ha recibido de forma íntegra y sin cambios.

[10] Es un dispositivo que puede tener conectados varios dispositivos en red, como computadoras, impresoras y servidores, para compartir y trasferir archivos y videos por la red. Gestiona a todos los dispositivos como un solo switch y ofrece seguridad hasta el nivel del puerto de ese único switch, lo cual evita la intrusión de usuarios no autorizados a toda la red.

está abierto, la respuesta es un mensaje ICMP[11], Port Unreachable (puerto no disponible). Si no hay respuesta al enviar el paquete, se infiere que el puerto está abierto, pero si en el puerto hay un filtro de firewall, se obtiene una respuesta errónea.

Secuestros informáticos

Son ataques informáticos que consisten en robar o apoderarse de algo, en general información. Existen muchos tipos de secuestros informáticos, pero tal vez el más popular de este tipo de secuestros sea el de la conexión TCP/IP, que hace perder la conectividad del servicio a una red de cómputo, con lo que el servicio se hace inaccesible a usuarios legítimos. El ataque se logra consumiendo la mayoría del ancho de banda de la red atacada o sobrecargando los recursos computacionales del sistema que es víctima del ataque, por ejemplo, inundando la red con spam. Si el atacante logra inyectar ciertos comandos para obstaculizar la conexión, también se puede lograr el mismo efecto de secuestro de la conexión.

El secuestro de una página web consiste en aprovechar un error de programación de la página, lo que le permite al atacante realizar modificaciones a la página, por ello a este ataque también se le conoce como *desconfiguración de página web.* Asimismo, también se puede secuestrar el dominio, donde el atacante modifica y redirecciona los servidores DNS (sistema de nombres de dominio), de manera que cuando los usuarios desean accesar a un dominio determinado, el DNS contesta con una dirección IP distinta y carga otra página web, que suele contener malware o publicidad maligna como pornografía. Para realizar este tipo de secuestro, el atacante recopila información del titular de un registro, inicia una sesión en la Web con esa información, donde el dominio está registrado, y modifica la IP auténtica de dicho dominio, para que el nuevo dominio se redirija a la página web dañina.

[11] El Protocolo de Mensajes de Control de Internet (ICMP, por sus siglas en inglés; *Internet Control Message Protocol*) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Se utiliza para enviar mensajes de error, indicando, por ejemplo, que un servicio determinado no está disponible o que un router o host no puede ser localizado.

De igual manera, también es posible secuestrar a los navegadores mediante el envío de *ventanas emergentes* o *pop-up,* los cuales modifican la página de inicio o la página de búsqueda predeterminada. Para lograrlo, se utiliza un malware que altera la configuración interna de los navegadores de Internet de una computadora, desde luego, modificaciones que se hacen sin el consentimiento del usuario. La ventana emergente se utiliza para mostrar publicidad; aunque también pueden aparecer en la pantalla de la computadora nuevas ventanas situadas detrás de la intrusa original, a esto se le llama pop-under. En ocasiones, los activan nuevas ventanas, lo que propicia desencadenar esta acción hasta el infinito. En la actualidad, muchos navegadores de Internet contienen los llamados *pop-up killers* que evitan la súbita aparición de este tipo de publicidad. Hay que recordar que en la programación de HTML se dice que una ventana sólo debe abrirse mediante un clic y que un solo clic no debe abrir más de una sola ventana, de modo que es relativamente sencillo darse cuenta si uno ha sido víctima de este tipo de intrusión.

Virus informáticos y seguridad

En el mundo actual, la mayoría de las personas ya no tienen archivos o notas en papel para guardar o anotar datos personales; por lo común, cualquier dato personal importante con seguridad está almacenado en una computadora personal, en un teléfono móvil o una tableta, con la característica que todos estos dispositivos se pueden conectar a Internet. Aunque en la vida cotidiana moderna el almacenamiento de datos es así, eso implica importantes riesgos, como que los archivos puedan ser borrados en su totalidad por un virus de cualquier dispositivo, que un virus modifique la información almacenada, que alguien robe esa información o que se utilice alguno de esos dispositivos para atacar a otras personas que tengan dispositivos similares, y esto desde luego puede suceder en computadoras personales y en redes empresariales. Estos ataques siempre suceden porque la computadora se infecta con un código maligno, llamado malware, que es cualquier código que pueda dañar una computadora. Este apartado describe algunos de los diferentes tipos de códigos dañinos, sus efectos y el nombre que se les ha dado.

Un virus informático es un software diseñado para causar daños de diferente tipo en una computadora o una red de computadoras, alterando el código del software original que tenía la computadora y haciendo que ésta trabaje de manera anormal. Algunos virus pueden causar tanto daño como incapacitar a un disco duro, haciendo que se pierda toda la información, o bloquear el funcionamiento de una red; los menos dañinos sólo provocan molestias en el funcionamiento de la computadora. El virus entra a la computadora sin que el usuario lo advierta y se aloja en la memoria RAM; a partir de ese momento toma el control de los servicios básicos del sistema operativo y de ahí se propaga para infectar a los archivos ejecutables. Posteriormente, el código del virus se *insert*a en el programa infectado y se graba en el disco duro, con lo cual se completa el ciclo de infección. Con el desarrollo de redes de cómputo de todo tipo, la propagación de virus se ha facilitado, siempre que no se tenga la protección adecuada.

Un virus puede infectar otras computadoras, ya sea que el usuario aceptó *insert*ar en su computadora una USB, un disco duro externo o cualquier otro dispositivo por medio del cual adquirió en forma directa el virus. La otra forma es que los virus están diseñados para propagarse a través de las redes, e Internet es la principal vía de contaminación, en cuyo caso se habla de gusanos.

Una vez infectado el sistema operativo, que es el blanco inmediato de la contaminación, la computadora se comporta de manera anormal; en muchas ocasiones este comportamiento permite identificar el tipo de virus y la forma de combatirlo. Existen diversos tipos de virus, ya que cada uno ejecuta su código de manera distinta. Los virus genéricos típicos son los siguientes:

1. **Gusano.** Se replica a sí mismo utilizando las partes del código del sistema operativo que son automáticas y que, desde luego, el usuario nunca puede ver.
2. **Troyano.** Es un virus que roba información, que puede alterar el funcionamiento del hardware y que, en ocasiones, permite que un usuario externo controle la computadora.

3. **Bombas de tiempo o bombas lógicas.** Sólo se activan si sucede determinada fecha o evento. El caso más recordado fue el virus del milenio, que se decía iba a activarse en cuanto las computadoras cambiaran la fecha del año 1999 a 2000; es decir, la activación del virus sucedería el 1 de enero de 2000 a las cero horas con un segundo.
4. **Hoax.** No son virus aunque pueden contenerlos. Son mensajes-cadenas que incitan a quien lee el mensaje a reenviar determinado número de copias. Por ejemplo: "Si reenvías este mensaje a diez personas sucederá un milagro en tu vida" o "Las personas que no han reenviado este mensaje al menos a 20 personas han sufrido un accidente, por tanto debes enviarlo", etcétera. En este tipo de infección se puede *insert*ar una bomba lógica, de manera que cuando el mensaje se haya reenviado, por ejemplo, 100 veces, se active un verdadero virus.
5. **Joke (broma o juego).** No es un virus, pero como su nombre lo indica es una broma molesta; por ejemplo, aparece repentinamente una ventana que dice "Apague de inmediato su computadora para evitar un virus que se ha detectado". Un usuario ingenuo apagará la computadora en cuanto vea la advertencia y así interrumpirá su trabajo muchas veces.

Existe otra clasificación de virus que describe cómo se alojan en la computadora o cómo actúan. A continuación se mencionan algunos ejemplos.

1. **Virus permanentes.** Se ocultan en la memoria RAM, por lo que es muy difícil eliminarlos y residen ahí durante mucho tiempo sin ser detectados. Pueden controlar todas las operaciones que realiza el sistema operativo e infectar todos los archivos sobre los cuales se realice una operación de abrir, cerrar, ejecutar, renombrar o copiar.
2. **Virus de acción directa.** Estos virus no permanecen en la memoria y sólo se activan al momento de ejecutar el archivo donde residen, pero es suficiente para iniciar su propagación a otros archivos cuando sucede cierta condición.

3. **Virus de superposición de caracteres.** Destruyen la información que se encuentra en los archivos infectados sobre escribiendo en los mismos, de manera que cuando se intenta leer dichos archivos aparecen líneas de escritura entrecortadas, por lo que es imposible leerlos, pues pierden todo su contenido.

4. **Virus de directorio.** Los archivos tienen identificada su ubicación, a la que invoca el sistema operativo para trabajar con ellos. Estos virus modifican las direcciones de los archivos en el disco duro, de manera que cuando se quiere ejecutar un programa infectado por este virus, el sistema operativo simplemente no puede encontrar el archivo, por lo que parecerá que ya se perdió. Al eliminar el virus, el archivo infectado vuelve a estar disponible.

5. **Virus cifrados.** Este tipo de virus es muy peligroso, ya que puede cifrarse a sí mismo, por lo que es casi imposible detectarlo. Cuando se utiliza el archivo donde está alojado, este mismo se desencripta y al terminar de utilizar el archivo se vuelve a cifrar.

6. **Virus de cifrado múltiple.** Son virus que cada vez que son activados, al utilizar el archivo que los aloja, se cifran con otra clave, debido a que están programados para cambiar el algoritmo de cifrado por sí mismos y de esa forma pueden generar muchas copias, lo que impide que sean identificados por el antivirus, por lo que resulta muy complicado eliminarlos.

7. **Virus de archivo.** Sólo infectan archivos ejecutables con extensiones .exe y .com. En este caso, al ejecutarse el programa infectado, el virus se activa.

8. **Virus spyware.** No son propiamente virus cuya función sea "espiar" información o archivos. Se le ha dado ese nombre a un software, cuya única función es mostrar publicidad no deseada por medio de ventanas que aparecen en forma repentina en la pantalla (pop-up), por lo que también se les conoce como adware (advertising ware o software de publicidad). Los virus spyware no sólo pueden generar los pop-up, sino que también pueden redirigir el buscador de la computadora a determinado sitio web, para que el usuario vea la publicidad que aparece ahí. Algunos de estos "virus" se activan con sólo teclear ciertas letras o números, aunque un uso

malicioso de este virus es el envío de pornografía por medio de pop-up o llevar en forma directa al buscador a estos sitios, con el peligro que un menor de edad tenga una computadora con este tipo de virus. La consecuencia inmediata de este tipo de infección es que la computadora se vuelve más lenta.

Se recomienda que si los menores de edad tienen disponible una computadora para su uso exclusivo, se revise con frecuencia si se presenta la aparición de pop-up o que sin ninguna instrucción especial la computadora se dirija a sitios web que no han sido solicitados, además de observar si aparecen nuevas barras de herramientas en el buscador o nuevos iconos en la base de la pantalla, que se teclea una letra o número en el buscador y no responde o hace otra cosa distinta o que repentinamente la computadora se hace más lenta sin motivo.

La computadora se puede infectar con un spyware dando un clic dentro de la ventana del pop-up, por tanto, evite hacerlo. También se puede infectar si en forma repentina aparecen en la pantalla cuadros de diálogo preguntando si se desea ejecutar determinado programa o realizar algún otro tipo de tarea; en esos casos, lo mejor es teclear CANCELAR. Una tercera forma de infección se produce a través del ofrecimiento de software libre de sitios poco confiables, y más aún de aquellos que ofrecen antispyware gratis. Si se ha detectado una infección de spyware, lo mejor es utilizar un spyware de una marca reconocida, aunque eso tenga un costo.

Actividad de aprendizaje

En equipo de dos o tres personas seleccionen un tipo de ataque de los mencionados, y con la ayuda de un video explíquenlo y den recomendaciones para evitarlo a los usuarios.

4.6 Medidas preventivas

Siempre resulta conveniente tener instalado en la computadora un buen antivirus que se adapte a nuestras necesidades personales; además, debido a que los atacantes desarrollan con mucha frecuencia nuevos virus, se hace necesario actualizar, con esa misma frecuencia, los antivirus. Los archivos adjuntos en los correos electrónicos en general son una fuente importante de virus, por lo que la recomendación es no abrir ningún archivo adjunto si no se sabe lo que contiene en realidad; es decir, sólo hay que abrir adjuntos de remitentes conocidos, pero si la decisión es abrir un archivo adjunto desconocido, lo más conveniente es hacer primero un escaneo con antivirus. Los adjuntos son un medio por el cual los atacantes realizan el spoofing, pero también un adjunto que proviene de una fuente conocida puede tener virus, pues quien lo envió pudo ignorar que estaba infectado.

Tampoco resulta conveniente abrir archivos adjuntos de sitios web en los que no se tenga confianza. En este caso, es mejor bajarlos, guardarlos en la computadora y, antes de abrirlos, someterlos a un escaneo de antivirus. Sin embargo, antes también se puede verificar que en la dirección URL aparezca la letra S, como HTTPS, y verificar que el sitio web cifra la información y tiene un certificado válido. Cuando se teclea una URL o se sigue una liga para acceder a un sitio web, el buscador revisa que la dirección del sitio web sea la misma que la de la dirección del certificado y reconoce que el certificado esté firmado por una autoridad competente.

Por lo común, cuando el buscador detecta que las direcciones del sitio web y del certificado no coinciden, presenta la opción de hacer un examen del certificado para que después de que éste se haya realizado se pueda aceptar o rechazar abrir el sitio. Lo que jamás hay que hacer es proporcionar información personal a un sitio web que la solicite para accesar, pero si por procedimiento es necesario proporcionar datos personales, por ejemplo cuando se hace una compra por Internet y se dan datos de la tarjeta de crédito y datos del domicilio para que envíen la mercancía, se recomienda verificar todos los puntos relacionados con la autenticidad del certificado, de que los datos están cifrados. Los tres puntos importantes de un certificado son quién emite el certificado,

para quién se emitió el certificado (persona física o persona moral) y la fecha de vencimiento. Si todo es correcto se tendrá más confianza en que el sitio es seguro; sin embargo, en realidad no hay una forma de asegurar que un sitio web es 100 por ciento confiable.

Por otro lado, si se compra un antivirus confiable y seguro, por lo común el proveedor del antivirus envía actualizaciones sin costo durante su vigencia y es conveniente tomar dichas actualizaciones, llamadas parches (patches en inglés), que son códigos adicionales que se van agregando al software original del antivirus para mejorar su desempeño, en el sentido de que tienen software reciente que puede atacar a los nuevos virus que aparecen día a día.

Antivirus pirata o falso

Algunos antivirus están diseñados como un malware (software malicioso) para robar información, sin despertar sospechas por parte del usuario, precisamente por aparentar que son antivirus auténticos. Una infección de antivirus también se puede manifestar por pop-up que aparecen en la pantalla. Cuando se ejecutan los pop-up, es muy difícil detenerlos y eliminarlos. Los atacantes distribuyen este malware mediante máquinas de búsqueda, correo electrónico, sitios de redes de ingeniería social y publicidad vía Internet, aprovechando cualquier debilidad que detecten en estos sitios. Un buen antivirus siempre eliminará este tipo de malware.

Actividad de aprendizaje

Anota al menos tres nombres de antivirus piratas o falsos. Comparte con tus compañeros.

¿Cómo funciona un antivirus?

Un antivirus en realidad es un software que escanea los archivos o toda la memoria de la computadora y compara lo que va encontrando contra ciertos patrones de comportamiento de definiciones de malware conocidos, que ya se incluyen en el software antivirus, con lo cual puede detectar la presencia de la mayoría de los malware. Como los atacantes generan a diario nuevo malware,

los desarrolladores de antivirus también desarrollan a diario el antivirus correspondiente, de manera que una buena protección para la computadora es actualizar con frecuencia el antivirus, siempre que sea de una empresa conocida.

En cuanto se instala un antivirus, la mayoría del software del antivirus se configura en forma automática para escanear en tiempo real directorios y archivos específicos, así como para realizar en forma periódica escaneos de toda la memoria de la computadora. Sin embargo, si el antivirus no se configura para que haga un escaneo de los nuevos archivos que se cargan o se leen en la computadora, entonces esta acción debe hacerse manualmente; de hecho, todo buen antivirus hace escaneos automáticos, tanto de la memoria como de todos los archivos nuevos que se guardan o que se leen. Cuando encuentran algo anormal durante los escaneos, algunos antivirus presentan una ventana de diálogo en la que se pregunta si el usuario desea que se elimine el archivo o simplemente se limpie, en tanto que otros antivirus realizan estos trabajos sin preguntar; si pueden eliminar el virus lo eliminan manteniendo el archivo y si no lo pueden eliminar, sólo eliminan el archivo.

Para controlar la entrada de virus a una red, siempre es necesario tomar medidas adicionales. En general, los virus se introducen mediante correo electrónico, páginas web y la conexión con cualquier dispositivo, como USB, disco duro externo o cualquier otro portátil, se recomienda mantener el máximo de recursos de la red únicamente en modo lectura, lo que impedirá que si una computadora se infecta, el virus pueda infectar a otras computadoras, además de mantener en el mínimo posible los permisos de cada usuario en la red. Otra práctica común es realizar escaneos completos de los servidores de la red en horarios nocturnos, para que a la mañana siguiente se tenga la certeza de que la red está libre de virus.

4.7 Sistema de prevención de intrusiones

A pesar de que existen filtros como el firewall, los antivirus y otra serie de medidas para evitar tener intrusiones indeseadas y muchas veces dañinas en las

computadoras personales o en las redes de computadoras, lo mejor siempre será prevenir tales situaciones. El sistema de prevención de intrusos (IPS, por sus siglas en inglés; Intruder Prevention System) es un software que controla el acceso de información en una red de cómputo, vigilando y detectando anormalidades en las vías por donde transita la información. El software está diseñado para tomar decisiones de control de acceso con base en el contenido de la información que viaja a través de la red, en vez de controlar las direcciones IP o los puertos, como normalmente lo hace un firewall (véase capítulo 5, Firewalls como herramientas de seguridad), aunque también puede actuar en una sola computadora para realizar las mismas actividades.

El software tiene una serie de reglas, a las que se les puede llamar *políticas de seguridad,* que le permiten tener la capacidad de decisión; de este modo, el software identifica e intenta detener cualquier actividad maliciosa, sin tener que avisar al usuario o al administrador de la red del peligro detectado, por tanto un IPS protege al equipo antes de que suceda la intrusión, en vez de eliminar o combatir al intruso que ya se ha alojado en la computadora, como lo hace un antivirus. Un IPS también es capaz de llevar un registro de todos los hechos detectados de actividades anormales o intentos de intrusión, generando un reporte para el usuario o para el administrador de la red. Un IPS puede clasificarse en cuatro tipos:

1. **Sistemas de Prevención de Intrusos Basados en una Red (NIPS, por sus siglas en inglés; Network-Based Intrusion Prevention System).** Monitorean redes internas (LAN) en búsqueda de información sospechosa que transita por la red, basando su análisis en el protocolo de comunicación de redes locales.
2. **Sistemas de Prevención de Intrusos Basados en Redes Inalámbricas (WIPS, por sus siglas en inglés; Wireless-based Intrusion prevention system).** Realizan lo mismo que los NIPS, pero con el uso de un protocolo de redes inalámbricas.
3. **Análisis del Comportamiento de la Red (NBA, por sus siglas en inglés; Network Behavior Analysis).** Analiza e identifica la información que tran-

sita por la red que puede representar una amenaza para el libre tránsito, como ataques de denegación del servicio o violaciones a las políticas de la red.

4. **Sistemas de Prevención de Intrusos Basados en el Host (HIPS, por sus siglas en inglés; Host-based Intruder Prevention System).** Consta de un software que monitorea a un solo host buscando cualquier actividad sospechosa.

La forma en la que funcionan los IPS presenta tres variantes.

1. Si la detección del probable intruso está basada en una firma, esta tiene la capacidad de reconocer el arreglo de una determinada cadena de bytes, por lo que al detectar una irregularidad emite una alerta; es decir, el software tiene una serie de patrones de bytes de referencia que compara contra las cadenas de bytes que va encontrando, de esa forma, encuentra irregularidades. Pero, si existe un intruso con una cadena de bytes desconocida para el IPS, simplemente no emitirá ninguna alerta, por lo que con este esquema de funcionamiento, es necesario actualizar continuamente la información de patrones que debe contener el software.
2. Una segunda variante en el funcionamiento de un IPS se basa en políticas de seguridad, las cuales fija el usuario, por lo común el administrador de la red. Por ejemplo, si la política declara que cualquier computadora de esa red sólo puede conectarse con determinado número de redes o usuarios previamente identificados, entonces todo aquello que no se encuentre dentro de esos parámetros autorizados, no podrá conectarse.
3. La tercera variante de funcionamiento se basa en que el IPS detecte anomalías. El IPS tiene ciertos patrones de comportamiento normal de tráfico por la red; por tanto, todo aquello que salga de ese patrón es reportado de inmediato por el IPS como una anomalía. El problema es que es muy difícil determinar con precisión los parámetros que identifican un comportamiento normal de tráfico. Existen dos formas para determinar el

patrón de un comportamiento normal; en el primero, se toman datos del comportamiento del tráfico de la red y con esas estadísticas se delinea el "comportamiento normal", así, cuando el comportamiento presenta una variación por fuera de esos límites, se genera la alerta. En la segunda forma, el administrador de la red, con base en su experiencia y antigüedad como administrador de la red, es quien fija los parámetros del "comportamiento normal". Por supuesto, este método no es muy confiable, sobre todo si el administrador de la red no tiene mucha experiencia y no es buen observador sobre ciertas características que presenta el tránsito de información a través de la red.

4.8 Forma de proceder de un hacker

Todos los problemas de intrusión que presentan tanto las computadoras personales, como las redes de cómputo, se deben a personas mal intencionadas llamadas hackers. Por tanto, si se conoce la forma de actuar y la lógica que por lo común siguen los hackers, quizá sea más fácil no combatirlos a ellos, pues siempre son anónimos, sino prevenir sus ataques o remediar más fácil y con mayor rapidez algunos daños que pudieran haber causado.

El primer paso que sigue un hacker, si la víctima seleccionada es una red privada de cómputo, es construir su propia base de datos acerca de la forma en como está organizada y la forma en la cual funciona dicha red, pues de esa manera le será más sencillo recopilar información, sobre todo aquella que poseen los servidores.

Si el hacker decide proceder de esta forma, primero observa el protocolo para administrar una red sencilla (SNMP, por sus siglas en inglés; Simple Network Management Protocol), que actúa como la capa de aplicación, en el nivel 7 del modelo OSI, con el cual puede examinar la tabla de ruteo en un dispositivo inseguro y la topología que tiene la red. Luego, con una consola de diagnóstico, también llamada traceroute (en UNIX), permite seguir el trayecto de los paquetes que vienen desde un punto de red (host), permitiendo estimar la distancia a la que se encuentran los extremos de la comunicación,

el número de redes intermedias y los ruteadores que puede haber conectados a un servidor.

Después, intenta accesar a un servidor DNS, con el fin de obtener la lista de direcciones IP. Como se dijo antes, un servidor DNS forma parte de una cadena que se forma al solicitar una página web con el navegador; el disco duro del servidor va almacenado todos los datos de las páginas consultadas, por lo que tiene el registro de cada dirección IP y el nombre de dominio asociado a esa IP.

Luego, podría utilizar un protocolo Name/Finger o el protocolo de información del usuario Finger, con los cuales es posible intercambiar información entre usuarios, ya que proporcionan reportes del estatus de un sistema de cómputo particular o de una determinada persona en sitios de la red. Por tanto, de ahí se pueden obtener nombres de login, teléfonos y otros datos, no sólo de personas sino también de servidores de redes.

Un hacker también puede utilizar el programa Ping, el cual es útil para comprobar el estatus de comunicación en redes, de un punto de red local (host) con uno o varios equipos remotos de una red IP, enviando paquetes con el Protocolo de Mensajes para el Control en Internet (ICMP, por sus siglas en inglés; Internet Control Message Protocol), pudiendo diagnosticar el estado, la velocidad y la calidad de una red de cómputo, además de poder localizar un servidor particular y determinar si es posible tener acceso, simplemente se hacen llamadas a la dirección de un servidor, para hacer una lista de los servidores que residen en una red.

Una vez que tiene la lista de servidores de determinada red, el hacker intentará conectarse a un puerto, especificando el tipo de servicio que tiene asignado ese servidor, con el fin de identificar los que se pueden conectar a Internet y cuáles pueden ser atacados. Para ello, cuenta con varias herramientas; por ejemplo, puede utilizar un Rastreador de Seguridad en Internet (ISS, por sus siglas en inglés; Internet Security Scanner) que es un programa que busca puntos vulnerables en la red con respecto a la seguridad o mediante la realización de un análisis de seguridad para auditar redes, que también se utiliza para localizar puntos vulnerables a la seguridad, pero lo hace en una subred o en un dominio. De hecho, estas herramientas las utiliza normalmente un

administrador de redes con el mismo objetivo, detectar puntos vulnerables a la seguridad de la red, a diferencia del hacker que las usa para atacar esos puntos.

Un hacker siempre tratará de ocultar su intrusión, así que para lograrlo instala paquetes de sondeo que contienen códigos binarios, con lo cual puede proteger su intrusión sin que alguien logre detectar la actividad que realiza. Dichos paquetes permiten extraer cuentas y contraseñas para los servicios de Telnet y del Protocolo de Transferencia de Archivos (FTP, por sus siglas en inglés; File Transfer Protocol), con lo cual el hacker ya tiene disponible una serie de opciones para perpetrar sus ataques. Luego, podrá intentar cualquiera de los tipos de ataques que ya se han mencionado en este capítulo, todo dependerá de las vulnerabilidades que haya encontrado y de su propia habilidad para realizar actividades maliciosas.

Comprueba tus saberes

1. Describe con tus propias palabras en qué consisten los niveles de certificación del Uptime Institute.

2. Describe con tus propias palabras las características de los niveles 1 a 4 de la certificación del Uptime Institute.

3. Menciona los tres elementos que se consideran para el otorgamiento de un certificado de sustentabilidad operativa.

4. Escribe el concepto de control biométrico.

5. Describe con tus propias palabras en qué consisten al menos tres tipos de los distintos controles biométricos que existen.

6. Escribe una definición de ingeniería social.

7. ¿En qué se basa la ingeniería social?

8. Describe con tus propias palabras el ataque informático de suplantación de la dirección IP.

9. ¿Cuál es el uso que tiene un rastreador de red?

10. Describe con tus propias palabras en qué consiste un ataque informático a los servidores de la Web.

11. ¿En qué consiste un ataque por inyección de SQL?

12. ¿Qué es el correo spam y qué daños ocasiona?

13. ¿Cómo se efectúa un ataque por secuencia de comandos?

14. ¿Cómo se realiza un análisis de puertos?

15. Describe con tus propias palabras en qué consiste un ataque informático a puertos.

16. ¿Qué son los secuestros informáticos?

17. ¿Cómo actúa un virus al infectar una computadora?

18. Menciona y describe con tus propias palabras al menos tres tipos genéricos de virus.

19. ¿Qué es un *spyware*?

20. Menciona y describe con tus propias palabras al menos tres medidas preventivas para evitar infecciones de virus en computadoras personales y redes de cómputo.

21. Describe con tus propias palabras cómo funciona un antivirus.

22. Menciona y describe con tus propias palabras al menos tres sistemas de prevención de intrusiones en redes de cómputo.

23. Menciona y describe con tus propias palabras los pasos que normalmente sigue un hacker con la intención de perpetrar un ataque informático a redes de cómputo.

Referencias electrónicas

1. http://www.monografias.com/trabajos75/seguridad-desarrollo-aplicaciones-web/seguridad-desarrollo-aplicaciones-web2.shtml
2. https://en.wikipedia.org/wiki/Java_Database_Connectivity
3. https://en.wikipedia.org/wiki/Application_programming_interface
4. https://es.wikipedia.org/wiki/SQL
5. https://es.wikipedia.org/wiki/Programaci%C3%B3n_declarativa
6. https://es.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions
7. https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
8. https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones
9. https://es.wikipedia.org/wiki/Puerta_de_enlace
10. https://es.wikipedia.org/wiki/Esc%C3%A1ner_de_puertos
11. https://es.wikipedia.org/wiki/Inyecci%C3%B3n_de_c%C3%B3digo
12. https://es.wikipedia.org/wiki/Inyecci%C3%B3n_de_encabezado_HTTP
13. https://es.wikipedia.org/wiki/Analizador_de_paquetes
14. http://cursohacker.es/ingenieria-social-informatica
15. http://www.nist.gov/mml/mmsd/security_technologies/dietbiom.cfm
16. https://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
17. https://es.wikipedia.org/wiki/Spam
18. https://es.wikipedia.org/wiki/Internet_Message_Access_Protocol
19. https://en.wikipedia.org/wiki/Usenet
20. https://en.wikipedia.org/wiki/Internet_service_provider
21. https://es.wikipedia.org/wiki/DomainKeys_Identified_Mail
22. https://en.wikipedia.org/wiki/DMARC

23. http://www.testingsecurity.com/how-to-test/injection-vulnerabilities/xss-injection

24. https://en.wikipedia.org/wiki/Markup_language

25. https://en.wikipedia.org/wiki/Style_sheet_language

26. https://en.wikipedia.org/wiki/Cascading_Style_Sheets

27. https://nmap.org/man/es/man-port-scanning-techniques.html

28. https://es.wikipedia.org/wiki/User_Datagram_Protocol

29. https://es.wikipedia.org/wiki/SYN

30. https://es.wikipedia.org/wiki/ACK

31. https://es.wikipedia.org/wiki/Hijacking

32. https://es.wikipedia.org/wiki/Ventana_emergente

33. https://www.us-cert.gov/ncas/tips/ST05-010

34. https://en.wikipedia.org/wiki/Finger_protocol

35. https://en.wikipedia.org/wiki/Uptime_Institute

CERT® Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections. RFC 1948 - Defending Against Sequence Number Attacks

5

Objetivo general

Que el estudiante entienda qué es un firewall, cómo funciona y para qué sirve.

Objetivos específicos

- Comprenderás el funcionamiento y las ventajas en la seguridad que proporciona un firewall.
- Conocerás el modelo OSI y comprenderás por qué es importante este modelo en el funcionamiento de un firewall.
- Identificarás los principales tipos de firewall de hardware y software, así como sus ventajas, desventajas y políticas de aplicación.

Firewalls como herramientas de seguridad

¿Qué sabes?

- ¿Cuántos tipos de ataques informáticos conoces?
- ¿En una conexión TCP se pueden aplicar algunos mecanismos de seguridad?
- ¿Conoces algunas limitaciones de los firewall?
- ¿Cómo se le conoce a un firewall con un nivel 7 de tránsito HTTP?

Competencias a desarrollar

- El estudiante comprende los problemas informáticos que resultan de conectarse a Internet.
- El estudiante define los tipos de firewall que existen.
- El estudiante selecciona un tipo de firewall, dependiendo del contexto informático en el que se encuentre.

5.1 Introducción

Casi todas las personas que poseen una computadora personal y sin duda todas las empresas, cualquiera que sea su giro o sector, se conectan cada día a Internet. Además, la mayoría de los negocios han instalado redes internas o externas de computadoras con el objetivo de optimizar el uso de sus recursos informáticos y, en general, de todas las TIC (Tecnologías Informáticas y de las Comunicaciones) que utilizan en sus instalaciones.

Cualquiera que sea el tipo de red que haya instalado una organización, al menos una de las computadoras de esa red, si no es que todas, se conectan a Internet como parte necesaria de su quehacer diario. Esta conexión es expuesta a riesgos informáticos, que en fechas recientes han surgido en Internet, por parte de personas mal intencionadas; riesgos que se han vuelto una amenaza constante para todo usuario de Internet. Dichos riesgos y amenazas pueden ocasionar desde algunas molestias pasajeras al usuario de la computadora, hasta daños muy severos, no sólo al equipo, sino a la seguridad de datos personales y empresariales, los cuales, en manos de gente con malas intenciones han derivado en robos de todo tipo, desde vaciar cuentas bancarias de los propietarios o usuarios de las computadoras, hasta el robo de secretos tecnológicos industriales y empresariales.

Hoy día, no existe una manera real de acabar con estos riesgos y amenazas, ya que lo único que podría aniquilarlos sería no utilizar Internet, lo cual en la actualidad es casi imposible. Entonces, lo que queda por hacer es disminuir este tipo amenazas.

Como se trató en capítulos anteriores, aquí también existe la "parte con buenas intenciones" y la parte "mal intencionada" de la informática. En este contexto, la "parte mal intencionada" hará todo lo posible por violar y acceder a computadoras personales o sistemas de redes informáticas para robar datos, espiar, hacer fraudes o enviar pornografía infantil o publicidad sin autorización del usuario de la computadora; mientras que "la parte buena" identificará la acción que pretende hacer "la parte mala" y tratará de prevenir dichos ataques con el diseño de antivirus, cifrado de datos o diseño de firewall, ya sea que se trate de hardware o de software.

En este capítulo se estudian los principales aspectos relacionados con un firewall, herramienta que si bien no proporciona una protección total a las redes o a las computadoras que trabajan en forma aislada, sí limita mucho el daño que suelen causar ciertos ataques informáticos.

5.2 Tipos de ataques informáticos

Spoofing

Aunque una computadora o una red tengan instalado un buen antivirus, éste puede no ser suficiente para evitar un spoofing de dirección IP. La palabra *spoofing* significa *copiar una película o un texto*, aunque en el caso específico de las redes de computación, incluyendo Internet, hace referencia a un paquete del IP o protocolo de Internet (protocolo básico para enviar datos por Internet o cualquier otro tipo de red), del que un intruso hace una copia falsa de la dirección IP para esconder la identidad de quien envía el mensaje y así poder entrar a otras computadoras o redes. El protocolo IP contiene una dirección fuente y una dirección destino expresadas en forma numérica del paquete que se envía. El atacante modifica los primeros números del protocolo, por lo que parece una dirección distinta a la del verdadero atacante; de esta manera, la máquina que recibe el paquete de información detecta que proviene de una máquina distinta y así la máquina receptora responde a la dirección falsa. De esa forma, el atacante prácticamente ha adivinado cómo comunicarse y tener el permiso del protocolo IP para entablar una comunicación, pero con una identidad falsa.

Si quien ejecuta un IP spoofing envía una enorme cantidad de información a la computadora cuya dirección IP ya conoce, se considera como un ataque para negar el servicio, pues al atacante no le interesa lo que la máquina atacada le responda. Es probable que la máquina elegida esté conectada pero no controlada, y que también sea elegida porque tiene un ancho de banda mayor, y rara vez va a cambiar su IP.

Cada nuevo ataque de spoofing lleva una diferente IP, de esa forma oculta el verdadero origen del ataque. Si, por ejemplo, hay un determinado número de computadoras conectadas mediante Internet para realizar un trabajo para el cual deba existir ese tipo de comunicación, éstas pueden sufrir un ataque de tipo spoofing; aunque el spoofing también se usa para enviar mensajes spam por correo, los cuales suelen ser muy molestos. En el caso de las computadoras que trabajan en equipo a través Internet, lo que sucede es que las máquinas participantes sólo enviarán respuestas a direcciones IP que quizá no existan.

Sin embargo, algunos tipos de spoofing logran vencer procesos de autenticación en redes, sólo basados en la dirección IP, por lo que el ataque es más efectivo si las computadoras conectadas a la red que sufre el ataque tienen relaciones de confianza mutua; así, el atacante podrá accesar a cualquier computadora de esa red y causar una serie de daños, ya que en ésta no se requiere de autenticación para tener acceso.

Otro tipo de ataque que no puede evitar un antivirus es el ataque a la ruta de direccionamiento o ruteo del origen. Como es sabido, para el envío de información una red de cómputo trabaja de dos formas distintas; la primera especifica la ruta que seguirá la información a través de la red, en tanto que la segunda utiliza un protocolo de ruteo sin origen, de manera que los routers en la red determinan la trayectoria de la información con base en el destino del paquete de información. Por tanto, se recomienda trazar la ruta a través de la red para prevenir congestionamiento en el tránsito de la información.

El punto importante aquí es que la dirección IP puede tener dos protocolos al inicio de la secuencia numérica: el "registro de ruta y origen estricto" (SSRR, por sus siglas en inglés) y el protocolo "registro de ruta y origen laxo" (LSRR, por sus siglas en inglés). Con respecto a la seguridad, en general los paquetes LSRR son bloqueados en Internet, ya que si no se bloquean, un protocolo LSRR puede permitir que un atacante realice un ataque de spoofing a su IP.

Como se mencionó antes, para prevenir éstos y otros ataques, ningún antivirus es suficiente, de ahí que lo más recomendable es contar con un firewall debidamente configurado; de lo contrario, un atacante cibernético bien preparado puede violar con facilidad la seguridad de cualquier tipo de red.

Ataque de negación del servicio

Un ataque dirigido hacia las redes privadas de cómputo o a una computadora que no está en red que por lo común proviene del exterior es conocido como "ataque de negación del servicio", mediante el cual el atacante impide al usuario legítimo tener acceso a la información y a los servicios de su computadora, lo que provoca que el usuario no tenga la posibilidad de accesar a su correo electrónico, sitios web, servicios en línea como bancos, líneas aéreas, etcétera.

El tipo más común de *ataque de negación* del servicio es cuando el atacante inunda una red con información. Durante este ataque, cuando el usuario llama por medio del buscador a un URL para determinado sitio web, en realidad está solicitando que el servidor de la computadora de ese sitio muestre la información solicitada en la pantalla del usuario. El servidor sólo puede procesar determinado número de solicitudes a la vez; si el atacante sobrecarga al servidor con muchas solicitudes, éste no podrá procesar la solicitud hecha por el usuario. Se le llama *negación del servicio* porque el usuario no consigue accesar al sitio que desea.

Al igual que sucede con las redes, el atacante utiliza mensajes spam por correo electrónico para efectuar un ataque similar en la cuenta de una persona. Ya sea que se trate de una cuenta de correo proporcionada por la empresa donde trabaja la persona o una cuenta gratuita, por ejemplo de Yahoo o Gmail, a cada una se le asigna una cuota específica que limita la cantidad de datos que puede tener en cualquier momento. Por tanto, cuando se envía una cantidad masiva de datos a través de los mensajes que recibe la cuenta, ésta llega al límite de la cuota asignada y, a partir de ese momento, es imposible recibir mensajes en forma legítima.

Pero además también existe el ataque llamado "negación distribuida del servicio", donde el atacante utiliza la computadora de una persona para atacar a otras computadoras, aprovechando las debilidades o vulnerabilidades que encuentra en los equipos; incluso, puede tomar el control de la computadora de un usuario cualquiera. Cuando el atacante ha tomado el control, fuerza a esa computadora a enviar cantidades masivas de información a sitios web o a enviar correo spam a direcciones de correo seleccionadas. Se llama ataque

distribuido porque el atacante utiliza muchas computadoras para lanzar un ataque de negación de servicio.

Como se puede deducir, resulta imposible evitar por completo este tipo de ataques, aunque siempre es posible tomar ciertas medidas para disminuir la probabilidad de que sucedan, sobre todo en las computadoras personales. Por ejemplo, siempre hay que instalar un buen antivirus, además de instalar y configurar de manera adecuada un firewall, de preferencia tanto de software como de hardware, si lo que quiere protegerse es una red, además de realizar prácticas seguras para distribuir la dirección personal de correo electrónico.

Sin embargo, hay que tener presente que no todas las interrupciones del servicio son resultado de este tipo de ataques y que pueden deberse a problemas técnicos con una red particular o a que ciertas partes de ésta se encuentran en mantenimiento. Pero, si el servicio de Internet o de algún sitio web es muy lento o al usuario le resulta imposible accesar a un sitio web en particular, recibe una enorme cantidad de correo spam o no puede tener acceso a los archivos de su propia computadora, entonces es muy probable que haya sido víctima de un ataque de negación del servicio.

Rootkit y botnet

Otro tipo de ataques muy comunes de los que se es víctima son los de *rootkit*, que es una pieza de software instalada y escondida en la computadora de un usuario sin que éste sepa de su existencia. El rootkit puede estar incluido en un paquete de software o haber sido instalado en forma personal por el atacante, aprovechando los puntos vulnerables de una computadora, sobre todo si el usuario "baja" información muy voluminosa de Internet. Un rootkit esconde actividades maliciosas, ya que una vez que está instalado, el atacante puede tener acceso a la información de la computadora, monitorear las actividades del propietario de la computadora, modificar programas y otras actividades sin que nadie lo note.

Además de los rootkit, los atacantes también hacen uso de *botnet*, un programa que se ejecuta de modo automático en la computadora, el cual tiene su origen en la palabra *bot*, que proviene de *robot*. Los *botnets* se refieren a computadoras que se controlan por una o más fuentes externas. Durante

el ataque con los botnet, el atacante toma el control de una computadora infectándola con un virus u otro intruso maligno, lo que le permite tener acceso a la computadora. Una vez que el atacante ha tomado el control de una computadora, ésta trabaja de manera normal, con lo cual al atacante se le facilitan ciertas operaciones, como la distribución de correos spam, infectar con virus a otras computadoras o realizar ataques de negación de servicio.

Estos ataques son muy difíciles de detectar, tanto el rootkit como el botnet, debido a que los atacantes suelen esconderse muy bien, por lo que pueden pasar inadvertidos para el usuario de la computadora, a menos de que éste busque ciertas actividades; incluso, un buen antivirus no puede detectar, y menos eliminar, estos programas malignos, los cuales son utilizados, entre otras cosas, para modificar información personal del propietario de la computadora, con el fin de dañarlo seriamente, sobre todo en sus cuentas bancarias. Si se considera que un atacante puede tomar el control de una computadora, también puede controlar muchas otras, lo que le permite cometer los mismos delitos (robar y alterar información) con muchos usuarios e incluso vigilar sus actividades en línea.

La mejor forma de evitar convertirse en víctima de alguno de estos tipos de ataque es tener buenos hábitos en lo que se refiere a seguridad informática, ya sea que se trate de una computadora personal o una red; en el caso específico de redes de cómputo, por política de las empresas (para mayor detalle véase capítulo 4, La seguridad física y lógica en redes), corresponde al administrador de la red mantener dichos hábitos. La instalación de un firewall previene esos riesgos de infección, bloqueando el tránsito de información maliciosa antes de que entre a la computadora y limitando la cantidad de información que se envía. También es importante utilizar buenos antivirus y mantenerlos actualizados, pues hay que recordar que los atacantes también actualizan sus virus para facilitar sus ataques.

Por desgracia, es muy difícil que un usuario detecte que ha sido atacado por un rootkit; y aunque logre detectarlo, es muy difícil que consiga eliminar dicha infección, pues una vez que el atacante ha logrado modificar algunos archivos en la computadora del usuario, la eliminación de estos archivos no basta para acabar con el problema y, de hecho, todas las versiones anteriores de ese

archivo serán sospechosas de haber sufrido un ataque similar. Una alternativa para solucionar el problema es formatear toda la computadora y reinstalar desde el sistema operativo con un software nuevo. Es tan difícil eliminar una infección de este tipo, que en ocasiones el rootkit se aloja en niveles muy profundos que no se eliminan formateando ni reinstalando el sistema operativo.

Phishing

Otra forma de ataque es el llamado *phishing* (también conocido como *fishing*). En términos informáticos significa más o menos lo mismo que pescar o pesca. En los ataques de phishing mediante el uso de correo electrónico o sitios web maliciosos, los atacantes solicitan información personal haciéndose pasar por una organización legal o altruista. Por ejemplo, si roban la identidad de una organización o empresa legal, presentan su sitio web en Internet con todos los logos de la empresa, como un banco o una institución financiera, y mediante mensajes de correo, por lo común alertan acerca de un supuesto problema que tiene una tarjeta de crédito o una cuenta de inversiones, por lo que para resolverlo piden datos personales de la persona, en específico password o NIP y, desde luego, el número de cuenta o tarjeta. Si el usuario atacado es ingenuo, con toda seguridad proporcionará los datos que se han solicitado, por lo que en poco tiempo sus cuentas estarán vacías o su tarjeta de crédito estará saturada de gastos hasta el límite.

También hay casos en los que el atacante se hace pasar por una organización altruista para solicitar donaciones de dinero, con el propósito de "ayudar a los damnificados de inundaciones, terremotos, epidemias, etcétera", y para facilitar el altruismo de la persona le hace saber que puede hacer las donaciones a través Internet, para lo cual evidentemente le solicita sus datos personales y de sus tarjetas de crédito o de inversión.

La mejor forma de prevenir estos ataques es sospechar de cualquier llamada telefónica de empresas conocidas pero que no tienen por qué llamar, así como no creer en correos electrónicos que informan acerca de un problema con cuentas o tarjetas de crédito, además de no proporcionar datos personales o de la empresa en la que se labora, a menos que se esté totalmente seguro de la identidad de la persona a quien se le proporcionan los datos o de la seguridad del sitio web visitado.

También es conveniente revisar el URL del sitio web. Los sitios maliciosos o falsos son idénticos a los sitios originales, pero una revisión rápida del URL podría evidenciar una letra distinta o un dominio distinto; por ejemplo, en vez de ser (.com) puede ser (.net). Si después de esto aún se tienen dudas acerca de la identidad del solicitante de datos, lo mejor es llamar directamente a la empresa vía telefónica y, si es posible, hacer una visita personal, pero nunca hay que llamar a los teléfonos que aparecen en el sitio sospechoso porque éstos también pueden ser falsos.

5.3 El modelo OSI

Antes de describir el funcionamiento de un firewall, es necesario conocer los aspectos elementales del funcionamiento del OSI (Open System Interconnection) o Modelo de Interconexión de Sistemas Abiertos (ISO/IEC 7498-1), creado en 1980 por la Organización Internacional de Normalización (ISO, por sus siglas en inglés), que se ha constituido como el marco de referencia para la definición de arquitecturas en la interconexión de sistemas de comunicaciones.

El OSI surge como una necesidad derivada del crecimiento desmedido y desordenado de las redes de computadoras en la década de 1980. En aquella época, cada fabricante diseñaba y construía su propia red, la cual sólo servía para la comunicación en redes de esa marca, por lo que cuando se intentaba la conexión en red con otras marcas, sencillamente las tecnologías no eran compatibles en muchos sentidos, empezando con los protocolos.

La ISO propuso estandarizar las tecnologías de red, y para lograrlo tomó como base a las empresas más avanzadas en esa tecnología de aquel tiempo. Los modelos que sirvieron como base fueron los de Digital Equipment Corporation, al SNA (Systems Network Architecture) y a los protocolos TCP/IP, con el propósito de poder encontrar un conjunto de reglas que pudieran aplicarse de manera general, a fin de que todo fabricante de redes de cómputo adoptara estas reglas, de este modo creó la compatibilidad entre todas las tecnologías.

Las investigaciones de la ISO dieron como resultado la identificación y definición de las diferentes etapas por las que pasan los datos que se transfieren de un dispositivo a otro en su viaje a través de una red. De este modo, se identificaron y definieron siete fases, a las que se llamó *capas* (*layer*, en inglés) y con éstas se definió una serie de protocolos, cada uno de los cuales (o varios) se utiliza en cada capa. La estandarización de las tecnologías de redes de cómputo generó una comunicación internacional entre las redes, sin importar el país del cual procede el fabricante o el idioma que hable; el ejemplo más representativo de la estandarización es, sin duda, Internet. En las tablas 5.1 y 5.2 se presentan unos esquemas del modelo OSI, tal como lo propuso la ISO.

Tabla 5.1 Capas host de acuerdo al modelo OSI

Capas host		
Unidad de datos	**Capa**	**Funciones**
Datos	**7. Nivel de aplicación** Servicios de red a aplicaciones	Un usuario no interactúa en forma directa con este nivel, sino más bien lo hace con programas que, a su vez, interactúan con dicho nivel. Define los protocolos que utilizan las aplicaciones para intercambiar datos, como el POP (Protocolo de Oficina Postal) y el SMTP (Protocolo de Transferencia Simple de Correo), ambos utilizados en el correo electrónico, administradores de bases de datos y servidores de archivos, como el FTP (Protocolo de Transferencia de Archivos) y otros. Cada vez que se crea una nueva aplicación, también se debe crear un nuevo protocolo para controlar el acceso a esa aplicación, por lo que cada día hay más aplicaciones y más protocolos.
Datos	**6. Nivel de presentación** Representación de los datos	Trabaja más con el contenido de la comunicación que con la forma en cómo se establece esa comunicación, por lo que los aspectos semánticos y sintácticos son abordados en los datos que se transmiten; con esto se encarga de representar la información para que ésta siempre llegue a su destino de forma reconocible, a pesar de que diferentes equipos pudieran tener distintas representaciones de los caracteres de los datos, es decir, actúa como traductor. También permite cifrar y comprimir datos.
Datos	**5. Nivel de sesión** Comunicación entre los dispositivos de la red	Esta capa tiene la capacidad de asegurar que cuando hay una sesión entre dos computadoras se lleven a cabo todas las operaciones previstas. Mantiene y controla el enlace establecido entre dos computadoras que transmiten datos entre sí.
Segmentos	**4. Nivel de transporte** Conexión extremo a extremo y fiabilidad de los datos	Transporta los datos que se encuentran dentro del paquete de la computadora de origen a la de destino, sin importar el medio (físico o inalámbrico) que se utilice. La unidad de datos de protocolo (PDU)[1] de esta capa, conocida como *segmento* o *datagrama*, depende de si corresponde a TCP, que es un protocolo orientado a conexión, o a UDP, que es un protocolo orientado sin conexión; trabaja con puertos lógicos y con la capa de red que forman los sockets IP: puerto.

[1] La Unidad de Datos de Protocolo (N-PDU) es la información intercambiada entre entidades pares; es decir, entre dos entidades pertenecientes a la misma capa, pero en dos sistemas diferentes que usan una conexión $N-1$.

Tabla 5.2 Capas de medios de acuerdo al modelo OSI

Capa de medios		
Unidad de datos	**Capa**	**Funciones**
Paquetes	**3. Nivel de red** Determinación de ruta y direccionamiento lógico	El objetivo de esta capa es que los datos lleguen del origen hasta su destino, sin importar si están conectados directamente. Este trabajo lo realizan los routers, identificando el enrutamiento que existe entre una o más redes. Las unidades de información se llaman "paquetes" y se clasifican en protocolos enrutables cuando viajan con los paquetes y protocolos de enrutamiento, los cuales permiten seleccionar la ruta. Aquí se realiza el direccionamiento lógico y se determina la ruta de los datos hasta su destino final. Los firewalls actúan principalmente sobre esta capa para descartar direcciones de máquinas.
Estructuras	**2. Nivel de enlace de datos** Direccionamiento físico MAC[2] y LLC[3]	Realiza el direccionamiento físico, el acceso al medio, la detección de errores, la distribución de tramas[4] y el control de flujo. Regula la forma de conexión entre computadoras. Determina el paso de tramas mediante el uso de los protocolos MAC[5] e IP, verificando su integridad y corrigiendo errores, por lo que es importante un excelente estado del medio físico de transmisión de datos con el medio de red que redirecciona las conexiones mediante un router.
Bits	**1. Nivel físico** Señal y transmisión binaria	Se encarga de la topología de red y de las conexiones globales de la computadora hacia la red. La conexión es tanto física, como la forma en que se transmite la información. Define el medio físico por el cual viajará la información. Define características materiales y eléctricas que se utilizarán para la transmisión de datos por medios físicos. Define las características funcionales de la interfaz. Transmite el flujo de bits a través del medio físico. Maneja señales eléctricas del medio de transmisión. Garantiza la conexión, aunque no su fiabilidad.

2 MAC, Control de Acceso al Medio (Media Access Control), en informática: subcapa inferior de la capa de enlace de datos.

3 LLC, Control de Enlace Lógico (Logical Link Control), en informática se refiere a la forma en que los datos son transferidos.

4 Trama es la unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes.

5 En redes informáticas y de telecomunicaciones, los protocolos MAC, Control de Acceso al Medio (Media Access Control), son un conjunto de algoritmos y métodos de comprobación encargados de regular el uso del medio físico por los distintos dispositivos que lo comparten. Una dirección MAC es la dirección hardware de un dispositivo conectado a una red.

Actividad de aprendizaje

En equipo de dos o tres personas creen un póster donde le muestren al público en general cuáles son los tipos de ataques informáticos y cómo pueden protegerse de ellos. Realicen una exposición con sus trabajos.

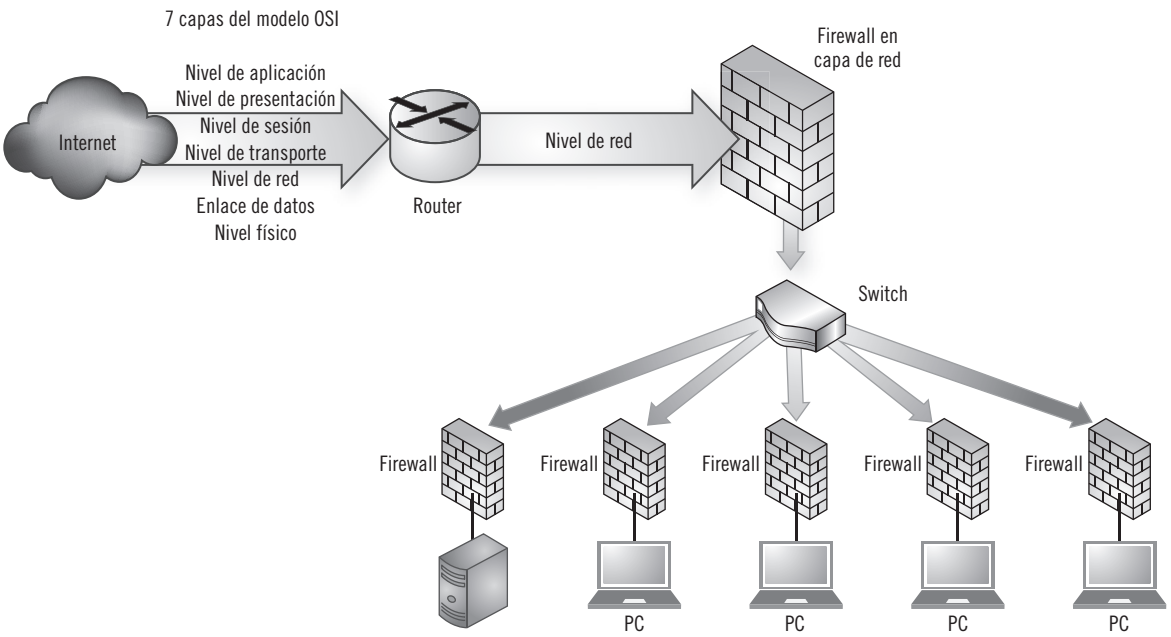
5.4 ¿Qué es un firewall y cómo funciona?

En informática, la palabra en inglés *firewall* se traduce al español como *cortafuego*, en analogía a una pared o un dispositivo que evita la propagación del fuego. Después de haber repasado brevemente los diferentes tipos de ataques a los que está expuesta cualquier computadora personal o red de cómputo conectada a Internet, parece adecuado llamarle así al dispositivo, físico (hardware) o lógico (software), o ambos trabajando de manera conjunta, que intenta detener los tipos de ataques informáticos expuestos en el apartado anterior.

La función de un firewall es proteger de ataques externos a computadoras personales o redes de computadoras, ya sea que esos ataques sean maliciosos, debido a que se haya introducido un software malicioso en la red, o simplemente porque haya un exceso de tráfico en la red. El firewall se puede configurar para bloquear datos provenientes de ciertos sitios o determinadas aplicaciones, a la vez que permite el paso de la información importante para la organización.

Los firewalls más sencillos, llamados de primera generación, básicamente se colocan en la tercera capa, que corresponde al nivel de red, del modelo OSI, donde se envían "paquetes" de información. Con base en este conocimiento es posible dibujar un esquema que muestre dónde está ubicado con exactitud el firewall más sencillo dentro de la enorme complejidad que implican los sistemas abiertos de interconexión con sus siete capas. La figura 5.1 muestra esta ubicación de forma esquematizada.

Como se dijo antes, el nivel de red o capa de red, proporciona la conectividad y elige una ruta entre dos sistemas conectados por medio de computadoras, que pudieran estar ubicados en redes geográficamente distintas. Su objetivo es conseguir que los datos lleguen del origen al destino fijado, aunque no tengan conexión directa, ya que puede asignar direcciones de red únicas, interconectar subredes distintas, enrutar paquetes y controlar la congestión de tránsito de mensajes, además de controlar errores.



› **Figura 5.1** Ubicación de un firewall en una LAN de primera generación.

Un firewall suele localizarse en el punto de unión entre dos redes. Por tanto, además de un firewall general, se recomienda que cada computadora tenga su propio firewall de software, pues de esta forma se evita, entre otras cosas, que se propague un spoofing de una subred a otra.

Cada firewall tiene sus propias reglas que debe cumplir; al hacerlo, la información entra y sale de la red. Además, el firewall también puede rechazar todos los paquetes que no cumplan con dichas reglas. Un firewall puede estar configurado para registrar todos los intentos de entrada y salida de una red, así como para guardar esos registros. Asimismo, también es capaz de filtrar paquetes en función de su origen, su destino y el número de puerto de acceso.

Para evitar el congestionamiento de tránsito, el firewall controla el número de conexiones que están activas en un mismo punto y bloquea aquellas que excedan cierto número de conexiones. Del mismo modo, también controla el tipo de aplicaciones que acceden a Internet, o bien, detecta los puertos en los que alguien está a la espera de una conexión para entrar, y que no debería estar ahí.

De igual modo, un firewall también es capaz de configurarse para cosas tan sencillas como administrar las solicitudes de acceso a ciertos servicios

Un *router*, también conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red, o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra; es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red) y que, por tanto, tienen prefijos de red distintos.

privados de la red. En resumen, una empresa u organización, dependiendo de su política de seguridad, puede configurar las reglas de operación del firewall para permitir una conexión, para rechazarla o para rechazar la solicitud de conexión, sin informar de dicho rechazo a aquella computadora que envió la solicitud de conexión.

Sin embargo, no es posible que un firewall proteja de todas las amenazas a las computadoras personales o redes, debido a que tiene ciertas limitantes que sólo le permiten la protección de aquellos ataques que pasan en forma directa por la capa de red, pero es totalmente vulnerable a los otros tipos de ataques, como el daño o robo de información proveniente de los propios empleados de la organización. Desde luego, es muy bueno tener un firewall bien configurado en los sitios que señala la figura 5.1, pero siempre hay que tener la estrategia de realizar una protección integral para la seguridad de la información por todos los frentes de ataque que existen (y que pudieran existir en un futuro), además de combatir los puntos débiles detectados.

5.5 Tipos de firewall

Nivel de aplicación de pasarela

Si se utilizan aplicaciones específicas, este tipo de firewall puede proporcionar mecanismos de seguridad. Por ejemplo, para Telnet (Telecommunication Network), que es un protocolo de red que permite utilizar la funcionalidad de administración remota, con la cual es posible realizar cierto tipo de acciones desde un equipo local y que éstas se ejecuten en un equipo remoto, como checar todas las computadores de una red desde una sola máquina, con el fin de identificar si hay problemas de intrusión o de cualquier otro tipo, el único requisito es que la computadora a la que se acceda debe tener un programa especial y reciba instrucciones que gestionen las conexiones. Así, Telnet es útil para arreglar ciertas fallas a distancia, consultar datos a distancia o como una variante de SSH (Secure Shell). Sin embargo, su mayor problema es la seguridad, ya que todos los datos personales, incluyendo las contraseñas, viajan por

la red como texto sin cifrar, por lo que la red queda expuesta a que cualquier intruso cometa actos ilícitos, como espiar, robar y hacer mal uso de esos datos personales. De hecho, se puede decir que SSH (véase capítulo 2, Criptografía) es una versión cifrada de Telnet.

Circuito a nivel pasarela

Cuando se utiliza una conexión TCP (Transfer Control Protocol) o de UDP (User Datagram Protocol) es posible aplicar algunos mecanismos de seguridad, lo que permite establecer una sesión entre una zona de mayor seguridad hacia una zona de menor seguridad, pues una vez que se ha iniciado la sesión, los paquetes fluyen entre las computadoras conectadas sin control.

Un firewall protege a una sola computadora o a toda una red interna contra intrusos provenientes de otras redes, ya que filtra paquetes de datos que son enviados por Internet. Un sistema firewall es un software que también puede contar con el apoyo de un hardware de red dedicada, que como muestra la figura 5.1, es el que ejecuta el filtro entre una computadora o una red local y una o más redes externas. Sólo se requiere que la computadora donde se instale el firewall tenga suficiente capacidad como para procesar el control de tránsito de los paquetes y que no se ejecute otro servicio más que el filtrado de paquetes en el servidor.

Recuérdese que el firewall más sencillo actúa sobre la tercera capa, capa de red, que es la encargada de la conectividad entre redes que tratan de comunicarse; es decir, actúa sobre la base del filtrado simple de paquetes llamado *stateless protocol,* o protocolo sin estado, que es un protocolo de conectividad que trata cada solicitud de conexión como una solicitud independiente no relacionada con solicitudes anteriores, de manera que para iniciar la conexión sólo basta una solicitud y una respuesta de las computadoras implicadas, ya sea que formen parte de una red o sean independientes, por lo que no se requiere que el servidor tenga el historial de quiénes han participado en comunicaciones en sesiones anteriores, aunque también existe el *protocolo de estado,* donde sí es necesario ese historial de comunicación. De hecho, el IP (Internet Protocol) y el HTTP (HyperText Transfer Protocol), que son fundamentales para Internet y para el uso de la WWW (World Wide Web, red

Un *datagrama* es un paquete de datos que constituye el mínimo bloque de información en una red de conmutación por datagramas, la cual es uno de los dos tipos de protocolo de comunicación por conmutación de paquetes usados para encaminar por rutas diversas dichas unidades de información entre nodos de una red, por lo que se dice que no está orientado a conexión. La alternativa a esta conmutación de paquetes es el circuito virtual, orientado a conexión. Los datagramas se componen de: una cabecera con información de control y los propios datos que se desean transmitir.

mundial), funcionan como protocolos sin estado. Y precisamente la forma en que funcionan estos dos protocolos se convierte en su ventaja y su desventaja; el stateless protocol es una ventaja porque simplifica el diseño del servidor, pues no se requiere un historial para que sucedan las conversaciones, pero también constituye una desventaja, ya que puede ser necesario el requerimiento de información adicional en cada nueva solicitud de conexión, en cuyo caso dicha información deberá ser interpretada por el servidor.

A la secuencia numérica del IP que va al principio se le llama encabezado; es lo primero que se analiza en cada paquete de datos que se envía desde una computadora de red interna y una computadora externa. El firewall analiza primero el IP de la computadora que envía los paquetes y luego el IP de la computadora que los recibe, así como la forma en que se envía el paquete. Por ejemplo, enviarlos con TCP (Transmission Control Protocol, Protocolo de Control de Transmisiones), le permite colocar los datagramas en el orden en el cual venían del IP, así como controlar el flujo de información, a fin de evitar congestionamientos. Además, también facilita que la información procedente de diferentes aplicaciones en la misma línea pueda circular de manera simultánea en la conexión. Por otra parte, enviarlos con UDP (User Datagram Protocol, protocolo de datagrama del usuario), facilita enviar datagramas a través de la red sin que se haya establecido una comunicación previa, ya que el datagrama proporciona suficiente información en su encabezado de IP para direccionar en forma correcta su destino.

Por último, el firewall también analiza el número de puerto, cuya numeración va del 0 al 1 023 (número asociado a un servicio o a una aplicación de red). Con los datos del tipo de protocolo y número de puerto se identifica el tipo de servicio que se utiliza.

La mayoría de los dispositivos de firewall se configuran para al menos filtrar comunicaciones de acuerdo con el puerto que se utiliza, por tanto la recomendación es bloquear todos los puertos que no son fundamentales para los fines que persigue la organización con respecto a seguridad.

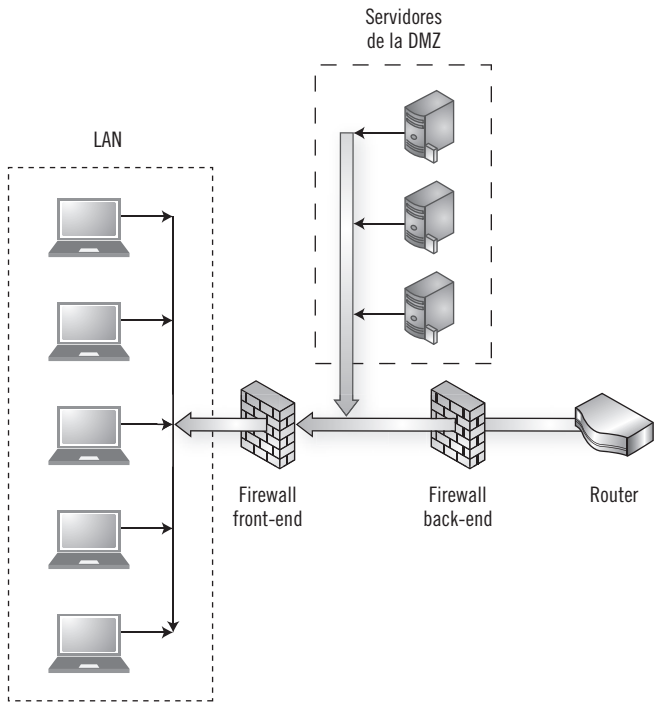
Si bien es cierto que una de las ventajas del uso del servicio FTP es que ofrece la máxima velocidad en la conexión, lo cual es muy útil cuando se envían archivos de gran tamaño, también es cierto que su principal desventaja

es que no hay mucha seguridad en la transmisión, pues los archivos deben enviarse en texto plano o claro (véase capítulo 2, Criptografía), es decir, sin cifrar, por lo que la transmisión es en extremo vulnerable al robo o a la modificación de información. Pero este problema se puede solucionar mediante el uso de aplicaciones como Secure Copy (SCP), que transfiere archivos en forma segura entre un host local y otro remoto, o SFTP (Secure File Transfer Protocol), ambos incluidos en el protocolo SSH (Secure Shell), el cual permite el envío de archivos cifrados (véase capítulo 2, Criptografía).

Zona desmilitarizada

Una red perimetral o *zona desmilitarizada* (DMZ, por sus siglas en inglés; Demilitarized Zone) constituye una zona segura ubicada entre la red interna de una organización y una red externa, que suele ser Internet. La zona desmilitarizada permite la conexión entre las dos redes, la interna y la externa a la DMZ, pero la conexión de la DMZ sólo se hace hacia la red externa; es decir, los host en la DMZ no se conectan con la red interna. De esta forma, los equipos (host) de la DMZ proporcionan servicio a la red externa, y lo hacen para proteger la red interna, ya que por su configuración cualquier intruso ataca primero a la DMZ, lo que le permitirá, si lograra pasar, conectarse y atacar a la red interna, lo cual es casi imposible pues el intruso entrará primero a la DMZ y de ésta será muy difícil que salga.

En general, en la DMZ se ubican los servidores, a los que sólo se tiene acceso desde afuera, como los servidores del correo electrónico, la Web y un DNS (Domain Name System, sistema de nombres de dominio), que es el sistema que maneja una nomenclatura jerárquica para conectarse a Internet o a una red privada. Como los servicios que se alojan en estos servidores son los únicos que se pueden conectar con la red interna de la organización, cualquier base de datos de la red interna está protegida en automático por la DMZ. Es importante destacar que tanto la DMZ como la red externa están controladas por un PAT (Port Address Translation, puerto de traducción de una dirección), que traduce las conexiones TCP y UDP hechas por un puerto desde una red externa a otra dirección y puerto de una red interna, permitiendo que una sola dirección IP sea utilizada por varias computadoras de la red interna al estar



› **Figura 5.2**
DMZ con front-end y back-end.

conectadas a Internet. Dentro de las opciones de configuración de los firewall está la creación de una DMZ, donde cada red se conecta a un puerto distinto de éste (véase figura 5.2).

Por tanto, si se instalan dos firewall, la configuración será mucho más segura, ya que esto ayuda a prevenir el acceso desde la red externa hacia la red interna. En este caso, para que la DMZ funcione se utilizan dos firewall; el primero recibe el nombre de front-end y sólo permite que pase la información del exterior a la DMZ, en tanto que el segundo firewall, denominado *back-end,* facilita que la información pase de la DMZ a la red interna.

Para computadoras personales

En el caso de un enrutador de uso doméstico, la DMZ host se refiere a la dirección IP que tiene una computadora para la que un enrutador deja todos los puertos abiertos, excepto aquellos que estén explícitamente definidos en la sección NAT del enrutador. Es configurable en varios enrutadores y se puede habilitar y deshabilitar.

Con ello se pretende superar algunas limitaciones para conectarse con determinados programas, aunque es un gran riesgo de seguridad que conviene tener bajo control con la instalación de un firewall o cortafuegos por software en el ordenador que tiene dicha IP en modo DMZ. Pero para evitar riesgos, lo mejor es no habilitar esta opción, usar las tablas NAT del enrutador y abrir sólo los puertos que son necesarios.

Actividad de aprendizaje

En el siguiente espacio, mediante un mapa mental conceptual, explica cada uno de los conceptos explicados de firewall.

5.6 Firewall de software y de hardware

Las amenazas para las computadoras que provienen de Internet, en especial los ataques de los hackers, pueden disminuir con el uso de un firewall de software, éste también resulta útil para pequeños negocios; aunque, si se utiliza un firewall de hardware, también se deberá tener un firewall de software. Si el negocio es pequeño, el firewall de software se instala en cada computadora en forma individual; lo mismo sucede si la organización es muy grande, pues también habrá la misma necesidad de instalar un firewall de software en cada computadora, pero adquirirlo y mantenerlo puede resultar muy costoso.

Un firewall de hardware puede adquirirse como un solo producto, conocido como router de banda ancha, y es muy importante que la computadora inicie con este tipo de router, sobre todo si tiene una conexión de banda ancha. Para su instalación, este tipo de router casi nunca requiere de una configuración especial, y tiene un mínimo de cuatro puertos para conectarse con otras computadoras. La función de un firewall de hardware es filtrar los paquetes, mediante un examen de los números iniciales del IP del paquete, con el propósito de determinar su origen y su destino; esta información se compara con un grupo predefinido de reglas de acceso, las cuales determinan cuál paquete pasa y cuál se rechaza.

Un firewall de hardware es una pequeña caja colocada entre un router y una computadora o una red de computadoras. Su funcionamiento se basa en un NAT (Network Address Translation —traducción de dirección de red—) que oculta la computadora del usuario de Internet o del NAT, así como de la inspección de paquetes de estado completo (Stateful packet inspection o SPI), para una mayor protección. Hay tres tipos básicos de firewall de hardware, los enrutadores (routers) cableados, los enrutadores (routers) inalámbricos y los Gateway de banda ancha.

Los *enrutadores cableados* deben conectarse mediante cable de red o PLC (Power Line Communications), que es la conexión por líneas eléctricas convencionales, es decir, es necesario conectar dos routers en LAN, pues si se quisiera conectarlos por WiFi, ambos tendrían que soportar WDS (Wireless Distribution System o Sistema de Distribución Inalámbrico); sin embargo, los

dos routers no soportan WDS, por lo que no hay más alternativa que conectarlos por cable de red Ethernet o con PLC.

Para que los enrutadores cableados funcionen es indispensable tener al menos un emisor-receptor y un receptor-emisor. Al utilizar la instalación eléctrica convencional (PLC) de una casa o una empresa, ésta no se verá afectada por la interferencia de las redes WiFi, que normalmente existen en cualquier hogar u oficina, lo cual equivale a un cable de red.

Por su parte, un *router inalámbrico* o *ruteador inalámbrico* es un dispositivo que realiza las funciones de un router, además de incluir las funciones de un punto de acceso inalámbrico. Se utiliza para proporcionar acceso a Internet o a una red informática. No se requiere un enlace por cable, ya que la conexión se realiza sin cables, a través de ondas de radio. Puede funcionar en una LAN cableada, en una LAN sólo-inalámbrica (WLAN) o en una red mixta cableada/inalámbrica, dependiendo del fabricante y el modelo.

Por último, un *Gateway de banda ancha* es el nodo que tiene la facultad de enviar paquetes a otras redes. Por definición, un Gateway es un router. De este modo, en una red TCP/IP, un nodo que puede ser un servidor, una estación de trabajo o cualquier otro dispositivo de red, tiene definida la ruta que deberá seguir en cada caso, la cual normalmente es el Gateway, que es el encargado de definir hacia dónde se envían los paquetes para determinada dirección IP, sin que haya una ruta específica previa.

Ya sea en casa o en pequeñas oficinas, la red local se puede conectar a Internet, la cual actuará como un Gateway por default para todos los dispositivos de red. La conexión se hace por un ruteador DLS (Digital Suscriber Line), que es un módem utilizado para conectar una computadora o un router a una línea telefónica y que proporciona el servicio DLS para conectarse a Internet; con frecuencia se le llama DLS de banda ancha. El módem se conecta a una sola computadora a través de un puerto Ethernet o un puerto de USB.

Sin embargo, en una empresa de mayor tamaño, donde puede haber muchos segmentos internos de red, si un dispositivo quiere comunicarse con una dirección de Internet, éste enviará por default el paquete de información al Gateway para su segmento de red. Éste, a su vez, pasará el paquete de información a una serie sucesiva de Gateway por default, antes de salir de la empresa.

Si esa es la posición y actuación que asume cada nodo del Gateway, se dice que se comporta como un servidor proxy y como un firewall.

El usuario que tiene conocimientos básicos de computación sólo tendrá que realizar pequeños ajustes a su equipo para que el firewall se instale sin problemas; sin embargo, para tener la certeza absoluta de que la instalación fue exitosa y el firewall trabaja como se espera se deberán consultar y aprender las operaciones y pruebas mínimas necesarias.

Si se utiliza un firewall de software es probable que se fuerce al usuario a tomar las decisiones de permitir o negar el acceso de cierta información proveniente de Internet, ya que el software sólo muestra una señal de alarma en la pantalla. Así que si un usuario no tiene mucha experiencia en cuestiones de seguridad, es probable que se sienta incómodo al tomar ese tipo de decisiones o que cometa un error al permitir el paso de paquetes, cuando en realidad debería haberlo negado.

Sin embargo, un firewall basado en hardware protege todas las computadoras de una red, por muy grande que ésta sea. Y lo más importante, es mucho más fácil mantener y administrar este tipo de firewall, que un firewall basado en software. Como un firewall de software sólo protege a una computadora, en forma individual, para tener una protección total en seguridad informática es más conveniente incluir una red privada virtual (VPN, por sus siglas en inglés; Virtual Private Network), que incluya antivirus, antispam, antispyware, filtro de contenido y cualquier otro dispositivo que aumente la seguridad.

Cuando una organización o empresa ya cuenta con firewall de hardware, se recomienda que cada usuario de la red instale firewall de software en su propia computadora, pues es muy útil cuando los empleados deben salir de la empresa por razones de trabajo y requieren tener la certeza de contar con seguridad informática en cualquier lugar donde se encuentren. Otra ventaja que presentan los firewall de software es que se pueden actualizar con facilidad, sólo basta descargar las actualizaciones desde el sitio web del proveedor.

5.7 Los firewall de software de última generación

Los firewall más avanzados realizan el trabajo de filtrado en otras capas del modelo OSI. Así, hay firewalls que actúan sobre la capa de aplicación, lo que permite detectar si un protocolo no deseado logró pasar por un puerto no estándar o si se está utilizando un protocolo que puede ser perjudicial para la seguridad. Este tipo de firewalls trabaja en la capa de aplicación, que es la capa 7 del modelo OSI, de forma que el filtrado de información se adapta a las características propias de los protocolos de este nivel; por ejemplo, si el tráfico proviene de un HTTP, se pueden realizar filtrados de acuerdo con la URL, a la cual se intenta tener acceso. Los protocolos de aplicación tienen ventajas y desventajas; por ejemplo, si se utiliza un FTP (File Transfer Protocol o Protocolo de Transferencia de Archivos), no bastará con tener un firewall de primera generación que sólo actúa sobre la tercera capa del modelo OSI; el servicio de FTP se ofrece a través de la capa de aplicación del modelo de capas TCP/IP, utilizando los puertos de red 20 y 21. Es un protocolo de la red que es utilizado, entre otras cosas, para permitir la transferencia de archivos entre sistemas conectados a una red, con base en una arquitectura cliente-servidor, lo cual significa poder enviar archivos desde una computadora que actúa como cliente, hasta un servidor que recibe los archivos, sin importar el sistema operativo de cada equipo. La computadora cliente o demandante pide al servidor realizar algún servicio. Algunas aplicaciones que utilizan el modelo cliente-servidor son el correo electrónico, un servidor de impresión y la World Wide Web (WWW).

Si se compara un firewall de filtrado de paquetes con uno de aplicación, sin duda el de aplicación es mucho más seguro porque cubre las siete capas del modelo de referencia OSI. Y aunque actúan de manera similar, el firewall de aplicación permite filtrar el contenido del paquete. Un buen ejemplo de firewall de aplicación es un servidor ISA (Internet Security Acceleration), el cual además ayuda en la organización de un firewall y en la conectividad de Internet. Un firewall se puede organizar para implementar una política de seguridad en las empresas u organizaciones, fijando reglas de uso para grupos

Una memoria caché puede copiar almacenes de datos que se utilizan con frecuencia cuando se corren ciertos programas, por lo que el acceso a esos datos se efectúa con mayor rapidez.

de usuarios, destinos, aplicaciones y criterios de contenido; además, también ofrece redundancia de hardware y equilibrio de cargas, lo que genera el uso eficiente de los recursos de la red.

Un servidor ISA (Internet Security Acceleration o Aceleración de la Seguridad en Internet) combina un firewall con un servidor caché de la Web que protege de accesos externos a una red al funcionar y compartir Internet de accesos externos. Por una parte, una LAN basada en un caché Web puede evitar el congestionamiento en redes, lo que rara vez se logra con una mejor tecnología de hardware o con un mayor ancho de banda.

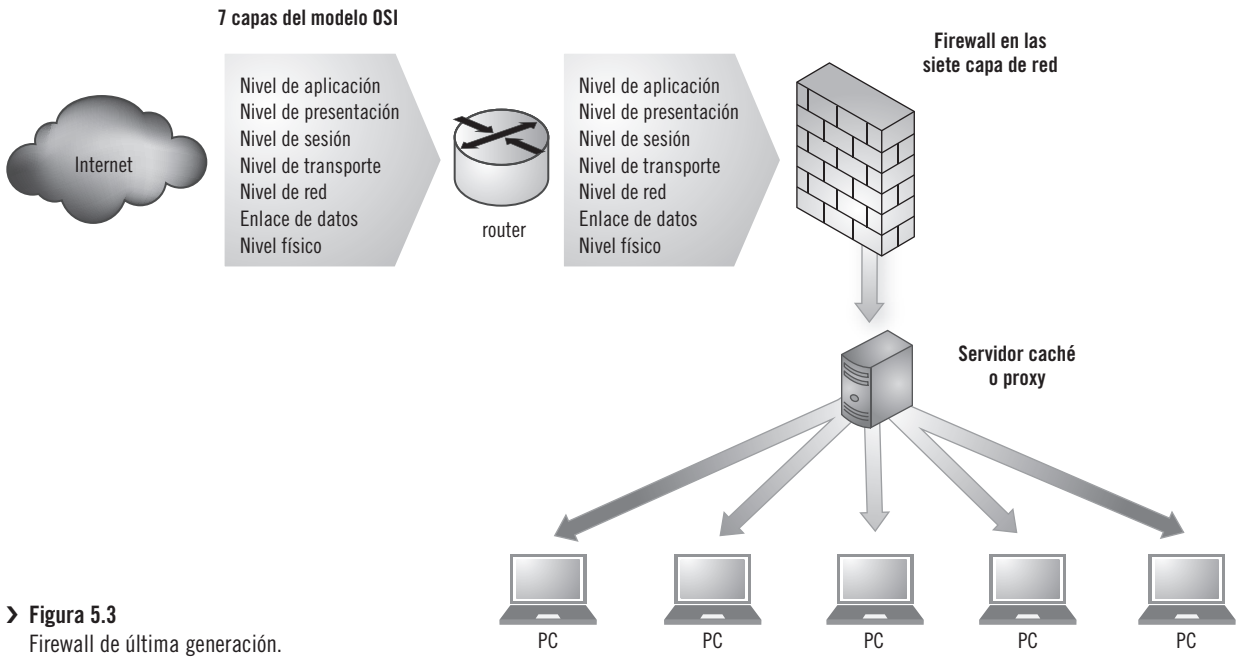
La función del firewall ISA de capas múltiples consiste en proteger los recursos que las empresas u organizaciones tienen en la red de accesos no autorizados, ataques de hackers y virus maliciosos, además de controlar el acceso de los clientes a Internet. Un ISA es en realidad un software conocido como caché Web que se aloja dentro de la LAN, por lo que todas las solicitudes relacionadas con contenidos en la Web se dirigen hacia este servidor, el cual, en cuanto recibe una solicitud, primero revisa su propia memoria caché para ver si tiene lo solicitado y si está actualizado, si es así, entonces entrega lo solicitado por el usuario, pero si no lo tiene, busca la fuente de la información, la encuentra y almacena una copia sobre su propio disco, al mismo tiempo que la entrega al usuario. El uso de este software siempre genera un acceso más rápido al contenido que se busca, en virtud de que almacena información utilizada con frecuencia; así, la próxima vez que el usuario requiera dicha información, el software la tomará de su memoria, reduciendo el uso del ancho de banda de la LAN. En otras versiones de un ISA, dirigidas a usuarios individuales o a negocios muy pequeños, el software actúa de la misma forma, sólo que la memoria caché que utiliza es la de la computadora y no la del servidor. Es importante aclarar aquí que la LAN, o red privada interna, está separada de Internet y que sólo hay una conexión física a Internet y otra conexión a la red interna. En este caso, la información se mueve a través del software del Servidor ISA, el cual transfiere la información de una conexión a otra.

A un firewall con un nivel 7 de tránsito HTTP se le conoce como *proxy*. Su importancia radica en que permite que las computadoras de una red tengan acceso a Internet en forma controlada. La mayoría de los servidores proxy

también son servidores caché, mientras que muchos servidores caché también son servidores proxy; no obstante, hay una diferencia sutil entre éstos.

Un proxy es un representante, o alguien que actúa a nombre de otra persona. En las TIC significa que un servidor proxy está conectado a Internet en representación de la computadora del usuario; de hecho, esa computadora no está conectada a Internet sino que es el servidor proxy el que está conectado, lo que le permite ocultar de manera eficaz las verdaderas direcciones de red. Por tanto, si los usuarios de una LAN no se conectan directamente a Internet, no necesitan un IP (Internet Protocol), lo cual es muy importante, ya que el servidor proxy, que es el único conectado a Internet, actúa como un firewall; así, todas las computadoras de esa red se encuentran exentas de los ataques vía Internet, lo que constituye una gran ventaja. El trabajo extra que hay que realizar es configurar todas las computadoras de esa red para que utilicen el servidor proxy.

Por otro lado, un servidor caché no necesita ser proxy. El servidor caché actúa como firewall y también distribuye la señal de Internet a las computadoras de esa red, pero sin los inconvenientes de configuración que presentan los servidores proxy (véase figura 5.3).



› Figura 5.3
Firewall de última generación.

Actividad de aprendizaje

En equipo de dos o tres personas realicen un listado de firewall de software de última generación. Comparen su listado con el de sus compañeros.

5.8 Limitaciones de los firewall

No hay que olvidar que un firewall de cualquier tipo es simplemente un filtro que atraviesa la información cuando transita a través de redes o de una computadora personal, por lo que las amenazas se mantienen vigentes si los ataques informáticos traspasan el firewall; esto es porque el filtrado de la información no es muy estricto, por ejemplo al utilizar puertos TCP abiertos, o porque la información no utiliza una red. Un firewall tampoco puede proteger de ataques internos a la organización o de las amenazas que provocan los usuarios descuidados o negligentes. Si un usuario interno lleva una USB contaminada con cualquier virus y la conecta a la red de la organización, el firewall no podrá detener la infección, ya que este tipo de ataques se controla sólo con potentes antivirus instalados en cada máquina. Por tanto, si no existe una buena configuración de los firewall y no se ha cuidado lo suficiente la seguridad de los servicios que se publican en Internet, éstos constituirán una seria amenaza contra la cual no hay mucho que hacer.

Un firewall sólo proporciona una seguridad parcial, por lo que es aconsejable tener otros elementos de seguridad, aunque sean redundantes, en caso de que llegue a fallar el firewall principal. Si un visitante mal intencionado observa que el firewall está bien configurado, buscará rutas alternas para perpetrar su ataque, y por eso la organización debe estar preparada. La mejor protección con firewall es instalar ambos tipos: el firewall de software y el firewall de hardware.

5.9 Políticas de los firewall

Al configurar un firewall existen dos políticas básicas, las cuales se basan en el tipo de seguridad que quiera adoptar la organización.

La primera es la **política restrictiva**, que rechaza el paso de cualquier información, excepto la que está explícitamente autorizada y que consiste en forma principal de servicios por Internet y de proveedores, por lo que es una política que en general adoptan los organismos gubernamentales y empresariales. Aquí se supone que el firewall puede obstruir todo el tráfico y que cada uno de los servicios o las aplicaciones que necesita la organización deberá ser analizado y aceptado, caso por caso. Parece claro que en esta política es más importante la seguridad que facilitar el acceso y uso de cierta información, por lo que en ocasiones los usuarios de la red se sienten muy limitados en el desempeño de su trabajo.

La segunda es la **política permisiva**, que autoriza el paso de todo tipo de información, excepto aquella para la cual el tránsito está negado. Toda la información que la organización considere que es potencialmente peligrosa se aísla y se analiza, en tanto que el resto pasa sin ser filtrada. Las organizaciones que normalmente adoptan esta política son las universidades, los centros de investigación y los servicios públicos con acceso a Internet. Esta política crea ambientes más flexibles, ya que se dispone de más servicios para los usuarios de la red. Contrario a la política anterior, aquí se privilegia la facilidad de uso sobre la seguridad de la red, aunque las amenazas no sólo provienen de Internet, por lo que es responsabilidad del administrador de la red incrementar la seguridad en todos los otros puntos de vulnerabilidad.

Hay que recordar que un firewall es sólo una parte de la estrategia de seguridad de toda la organización y lo primero que hay que conocer es qué es lo que se está protegiendo; no es lo mismo proteger los datos de una institución bancaria, que los datos clínicos de un hospital, las investigaciones realizadas en una universidad o las investigaciones tecnológicas que se desarrollan dentro de una empresa privada.

Para ayudar al buen funcionamiento de un firewall es útil implementar una serie de procedimientos:

1. Registrar los accesos de usuarios a los servicios privados de la red.
2. Registrar las aplicaciones del servidor.
3. Registrar todos los intentos de entrada y salida de la red.
4. Realizar un filtrado de protocolo, el cual permite aceptar (o rechazar) el tránsito de información en función del protocolo utilizado, ya que no es lo mismo utilizar un HTTP que un HTTPS (HyperText Transfer Protocol Secure), pues el segundo es una conexión segura.
5. Filtrar direcciones en función de origen, destino y número de puerto conectado.
6. Controlar el tipo de aplicaciones que pueden acceder a Internet.
7. Detectar puertos que están en espera de conexión y que no deberían estarlo.
8. Controlar el número de conexiones que se originan desde un mismo punto.

Con estas medidas, el firewall proveerá de una mejor seguridad a un solo equipo o a una red de computadoras.

5.10 ¿Cómo elegir el firewall más adecuado?

La decisión óptima en la elección de un firewall se basa en varios puntos. Primero, como se dijo antes, en el hecho de que existen firewall de hardware y firewall de software; y, segundo, del número de computadoras que protegerá el firewall.

Si sólo se va a proteger la computadora personal que hay en una casa, tal vez la mejor opción es un firewall de software, pues normalmente el firewall ya viene con todo el software de la computadora; siempre que sea software propietario, no se requiere gastar en hardware ni cableado adicional, aunque es probable que el paquete completo de software sea un poco más costoso.

Si se tiene una empresa muy pequeña, con una red de computadoras también muy pequeña, una buena opción puede ser un enrutador de hardware, los cuales tienen algunos puertos disponibles para conectarse a Internet. Este enrutador actúa como firewall para todas las computadoras conectadas. Pero, si la empresa es grande, entonces la mejor opción es un enrutador inalámbrico, al cual se pueden conectar tanto PC de escritorio como portátiles y hasta impresoras de la propia red. Sin embargo, el hecho de que el enrutador sea inalámbrico, lo hace vulnerable a que sus señales sean interceptadas por personas maliciosas fuera de la organización. Debido a que puede dar servicio a muchas computadoras y se ahorra el cableado, el costo de este enrutador suele ser un poco mayor.

Al final, el responsable de tomar las decisiones es el administrador de la red, quien debe asumir una posición definida respecto a la política del firewall, la cual debe estar alineada con la política general de seguridad informática de toda la organización y, desde luego, con el costo del firewall y los componentes adicionales (como cableado) o hardware adicional necesario.

Actividad de aprendizaje

En equipo elaboren un video donde expliquen con detalle cómo elegir el firewall más adecuado. Compartan su trabajo con el grupo.

Comprueba tus saberes

1. Explica con tus propias palabras qué es el OSI y menciona cuál fue la necesidad que motivó su desarrollo.

2. Describe las siete capas del modelo OSI.

3. Explica con tus propias palabras en qué consiste un ataque de spoofing.

4. Explica con tus propias palabras en qué consiste un ataque de "negación del servicio".

5. Describe qué es un rootkit.

6. Explica con tus propias palabras en qué consiste un ataque de botnet.

7. Explica con tus propias palabras qué es un ataque de phishing y cuáles son sus consecuencias.

8. Describe cuántos y cuáles son los tipos de firewall que se conocen.

9. ¿Qué características tiene un firewall de primera generación?

10. Describe en qué consiste un firewall de última generación y explica las diferencias con un firewall de primera generación.

11. ¿Qué es un router y para qué sirve?

12. Dentro del contexto de un firewall, explica con tus propias palabras qué es una zona desmilitarizada.

13. Explica con tus propias palabras los términos *front-end* y *back-end* en un firewall.

14. Describe las principales diferencias que existen entre un firewall de software y un firewall de hardware. Menciona las ventajas y las desventajas de ambos.

15. ¿Qué es un Gateway?

16. ¿Cuáles son las limitaciones de un firewall?

17. Explica con tus propias palabras en qué consisten las dos principales políticas que se pueden adoptar al instalar un firewall.

18. ¿Qué es un servidor proxy?

Referencias bibliográficas

1. Chapman, B. and Zwicky, E. *Building Internet Firewalls.* 2nd edition. O'reilly Media Publishers. 2000.
2. Stallings, W. *Network Security Essentials.* 1st ed. Ed Prentice-Hall. 2003.

Referencias electrónicas

1. http://www.ehowenespanol.com/gateway-vs-router-hechos_165191/
2. https://es.wikipedia.org/wiki/Modelo_OSI#Unidades_de_datos
3. https://www.us-cert.gov/ncas/tips/ST06-001
4. http://geekland.eu/que-es-y-para-que-sirve-un-firewall/
5. http://www.adslayuda.com/generico-terminologia.html
6. https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)
7. http://www.redeszone.net/redes/conectar-dos-routers-en-lan-mediante-cable-ethernet-o-plc/#sthash.bi0eVnw0.dpuf
8. https://en.wikipedia.org/wiki/Default_gateway

6

Objetivo general

Que el estudiante aprenda y sea capaz de aplicar métodos y planes para enfrentar las contingencias informáticas en una organización y que comprenda algunos de los conceptos y procedimientos utilizados por la informática forense.

Objetivos específicos

- Comprenderás la importancia del concepto de plan de contingencias en seguridad y las situaciones en las cuales es necesario aplicar dicho plan.
- Conocerás el concepto de Informática forense y los distintos métodos que existen para llevarla a cabo.

Las contingencias en seguridad informática e informática forense

¿Qué sabes?

- ¿Qué es un buen gobierno para las TIC?
- ¿Qué es un plan de contingencia informática?
- ¿Conoces algún riesgo físico interno en informática?
- ¿Por qué es importante un plan de previsión?
- ¿Conoces la norma ISO 27000?

Competencias a desarrollar

- El estudiante conoce en qué consiste un plan de contingencias informáticas.
- El estudiante describe el contenido de los tres subplanes que conforman un plan de contingencias informáticas.
- El estudiante comprende el concepto de informática forense y describe su procedimiento.

6.1 Introducción

En la mayoría de los textos académicos acerca de seguridad informática se trata el tema de las contingencias que pueden presentarse sobre los recursos informáticos que posee una empresa o una organización. Sin embargo, en la mayoría de estas obras se estudia al área de informática en forma aislada, y muy probablemente se piensa que los planes que se estructuran para las contingencias fueron elaborados en forma separada del contexto general de la planeación de la empresa.

Existe un concepto general llamado buen gobierno que se define como el conjunto de normas, prácticas, códigos de ética y elementos de conducta empresarial que fomentan la existencia de relaciones armónicas, ecuánimes y transparentes entre todos los miembros de una empresa u organización, ya sean accionistas, directores, administradores, proveedores, empleados y clientes; relaciones que deberán consolidarse con las autoridades civiles y la sociedad en general. Dentro de este mismo concepto, también se ha definido un buen gobierno para las TIC como un marco para tomar decisiones y establecer la asignación de responsabilidades, así como para fomentar el comportamiento deseado respecto al uso de las TIC.

Para saber el tipo de decisiones que se toman, lo primero es conocer el uso de la TI dentro de una empresa. Respecto a la arquitectura, se tiene una organización lógica de datos y aplicaciones que están basadas en políticas, relaciones y selecciones técnicas acerca del hardware y el software que se utilizará. Respecto a la infraestructura, se tienen servicios, centralizados, compartidos y coordinados, que sientan las bases para organizar el uso de la TI. En relación con el uso del dinero, hay que decidir cuánto y en qué invertir, con base en proyectos bien sustentados. Respecto a las necesidades, cada área plantea sus necesidades de TI y con base en ello se decide a quién se le da qué y cuánto.

De acuerdo con COBIT, dentro del marco del buen gobierno se establece que las TIC se componen de cuatro bloques; ahí mismo también se definen y establecen las actividades que deberá realizar cada uno de estos bloques.

1. **Planificación y organización.** Contempla el plan estratégico de la TI, la evaluación de riesgos y la administración de los proyectos derivados de los planes particulares.
2. **Adquisición e implementación.** Incluye la identificación de soluciones, la adquisición y el mantenimiento de la infraestructura tecnológica, el desarrollo y mantenimiento de los procedimientos.
3. **Entrega y soporte.** Se contempla el aseguramiento de la continuidad en el servicio, el mantenimiento de la seguridad de los sistemas, la identificación y distribución de costos.
4. **Monitoreo y evaluación.** Contiene la evaluación de los controles internos, la obtención de un aseguramiento independiente y la realización de auditorías independientes.

Luego, COBIT divide a las TIC en tres niveles, los cuales sólo se explican en el contexto de los aspectos que interesan para el desarrollo de este capítulo, aclarando que el cuerpo de COBIT es mucho más extenso en los puntos que contiene cada bloque y cada nivel:

- **Dominios**. Agrupación natural de procesos que corresponden a un dominio o a una responsabilidad organizacional.
- **Procesos.** Actividades normalmente secuenciales que tienen cotos de control.
- **Actividades.** Son las acciones requeridas para lograr un resultado medible. COBIT define 34 objetivos generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios.
- **Dominio de planeación y organización.** Incluye la estrategia que contempla una planeación estratégica en la que se establece misión, visión y objetivos de la empresa a corto y largo plazos, así como las tácticas. Esto es, se refiere a la identificación de la forma en que la TI puede contribuir al logro de los objetivos del negocio.

Por su parte, la evaluación de riesgos tiene como función asegurar el logro de los objetivos de la organización, para lo cual debe identificar, definir y actualizar el conocimiento de los diferentes riesgos y amenazas sobre la TI y el impacto que éstos tendrían sobre la empresa si llegaran a hacerse realidad. La evaluación de riesgos contempla las siguientes acciones:

- Establecer la forma en que deberán manejarse los riesgos de manera aceptable.
- Definir los umbrales de riesgo de cada tipo identificado.
- Medir los riesgos físicos internos, físicos externos y riesgos lógicos.
- Realizar una planeación de contingencias contra riesgos para asegurar que existan controles y medidas de seguridad a fin de disminuir, mitigar y, si es posible, eliminar algunos tipos de riesgos.
- Elaborar una política para enfrentar los riesgos, la cual incluya controles y sistemas de alerta, donde se incorpore la incertidumbre en la evaluación de los riesgos.
- Elaborar una serie de alternativas y elegir la mejor, con base en una serie de principios y políticas previamente establecidas.

Dominio de entrega y soporte

En este capítulo se hace referencia a la entrega de los servicios solicitados por todas las áreas de la empresa; debe incluir la capacitación en el uso de TI, así como la seguridad y la continuidad del negocio.

En lo que respecta al aseguramiento del servicio continuo, este dominio tiene como objetivo mantener disponible el servicio del área de informática (o de sistemas), con márgenes mínimos de interrupciones. Para lograrlo se hace un plan de continuidad del negocio que debe considerar la elaboración de un documento que incluya todos los procedimientos alternativos que deberán seguirse en caso de interrupción del servicio o daño severo a las instalaciones físicas de la empresa, suficientes para interrumpir la marcha normal del negocio. El plan de continuidad asegura que el servicio informático se reestablecerá lo más rápido posible o, incluso, permanecerá activo en forma continua.

En lo que se refiere a garantizar la seguridad de los sistemas, tiene como objetivo salvaguardar la información contra un uso no autorizado, como divulgación, modificación, daño o robo. Para evitar estos usos se instalan controles de acceso lógicos, lo que restringe el acceso de personal no autorizado a datos, sistemas y programas de la empresa. Esto se logra mediante controles de autorización, por autenticación de identidad y controles de acceso lógico, obedeciendo una serie de políticas preestablecidas, entre las que se considera incluso la suspensión de cuentas de usuario.

La seguridad de los sistemas también implica la administración de llaves criptográficas, lo que incluye la generación, distribución, certificación, almacenamiento y utilización de claves cifradas para asegurar sólo el acceso autorizado a los sistemas. Asimismo, la seguridad también implica prevención y detección de virus, a través de la instalación de medidas preventivas, de detección y correctivas y la instalación de firewall de hardware y de software.

COBIT también contempla la administración de problemas y la administración de datos. El objetivo de la administración de problemas es asegurar que los incidentes sean registrados y resueltos, y que sus causas sean investigadas a fin de que no vuelvan a presentarse. Por incidente se entiende el haber sufrido cualquier tipo de ataque, ya sea físico en las instalaciones o un ataque lógico en los sistemas. En tanto que la administración de datos tiene como objetivo asegurar que los datos permanezcan completos, precisos y válidos durante todos los procesos de entrada, actualización, procesamiento, salida y almacenamiento, lo cual se logra con el diseño de procesos, controles y formatos para cada etapa, a fin de minimizar errores y omisiones en el manejo de datos.

Por tanto, los documentos de donde se extraen inicialmente los datos, llamados documentos fuente, deberán estar completos, ser precisos y registrarse en forma adecuada. Los procesos, controles y formatos validarán los datos de entrada y así detectarán y corregirán los errores que aparezcan. De esta forma se asegura la integridad, autenticidad y confidencialidad de los datos almacenados.

Otro punto que considera COBIT es la administración de las instalaciones, cuyo objetivo es proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra riesgos físicos (fuego, polvo, calor excesivos,

etc.) o fallas humanas, lo cual se hace posible con la instalación de controles físicos y ambientales adecuados, que deben ser revisados con regularidad para un funcionamiento apropiado, mediante la definición de procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

Por último, de todos los aspectos que son de interés para este capítulo se cita el monitoreo de procesos, cuyo objetivo es asegurar el logro de los objetivos establecidos para los procesos de TI, éste se logra mediante la definición, por parte de la gerencia, de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte y la atención regular a los reportes emitidos. Para el logro satisfactorio de este objetivo, la dirección general de la empresa debe definir indicadores claves de desempeño *y/o* factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. Asimismo, también debe medir el grado de satisfacción de los clientes con respecto a los servicios de información proporcionados, a fin de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, mediante el monitoreo continuo de los indicadores de desempeño para observar el avance (o retroceso) de la organización hacia los objetivos propuestos.

Ésta constituye la base que da origen a los planes de contingencias informáticas, ya que de las cuatro grandes actividades del proceso administrativo que deben realizarse en toda organización (planeación, dirección, organización y control) se derivan las actividades específicas que van contenidas en un plan de contingencias. No se trata sólo de planear una actividad, sino también de dirigirla para que se instale y funcione de manera correcta en el momento necesario. De ahí la importancia de que cada una de las personas involucradas en el adecuado funcionamiento del plan de contingencia conozca lo que debe hacer, cómo lo debe hacer y cuándo lo debe hacer. Además, también hay que controlar su actividad; es decir, no se trata sólo de hacer el plan y dejarlo a un lado sin aplicación, sino de mantenerlo vigente, de tal forma que responda de inmediato a una contingencia y sea sujeto de una auditoría, a fin de corroborar que en cualquier momento se está preparado para responder a las contingencias.

En este mismo contexto, destaca la Norma ISO 31000:2009, la cual proporciona los principios generales para la administración del riesgo de cualquier tipo, sin importar la clase de industria o sector al cual pertenezca la empresa u organización y en la que se quiere adoptar dicha norma. Es importante aclarar que no hay certificación para esta norma, de manera que la empresa que la adopte, será exclusivamente porque es de su interés hacerlo por su propia seguridad, con el fin de protegerse de riesgos de cualquier tipo.

Esta norma ISO no pretende afirmar que todos los riesgos son iguales y deben administrarse de la misma forma. De acuerdo con la naturaleza de cada empresa u organización, cada cual deberá tener en cuenta sus necesidades específicas, su misión, visión, contexto económico y cultural en el cual se desenvuelve, los procesos de manufactura o servicios que desarrolla, los activos que posee y las prácticas que emplea en su manufactura de productos o prestación de servicios.

Además, dicha norma define al riesgo como el efecto de la incertidumbre sobre los objetivos que tiene la organización, los cuales pueden ser de tipos muy distintos; aunque, en general, se puede decir que el riesgo es obtener un resultado distinto al esperado. Así, un riesgo surge por la incertidumbre, que es la carencia de información, del conocimiento o del entendimiento de un hecho probable y sus consecuencias; por tanto, en lo que se refiere a los riesgos informáticos, esto obliga a tener información estadística de los riesgos ocurridos y de entender cada tipo de riesgo, así como de conocer las consecuencias que tendría para toda la empresa, y en especial para el área de informática, que tales riesgos llegaran a suceder. Administrar el riesgo significa, entonces, la realización de una serie de esfuerzos coordinados para disminuir las probabilidades de ocurrencia de las amenazas informáticas y físicas.

En este mismo contexto, hay una serie de beneficios en caso de que la empresa u organización decida administrar los riesgos informáticos, los cuales se describen a continuación.

- Aumentar la probabilidad de lograr objetivos, ya que ahora todos los datos de la dirección, de la administración y del control de logros de objetivos de la empresa, se encuentran almacenados de manera digital en la empresa,

pues el robo o la alteración de esos datos implica no poder monitorear la información si se está avanzando en la consecución de los objetivos.

- Si la empresa decide elaborar un plan de prevención de riesgos informáticos, aprenderá a prevenir riesgos y no a corregir consecuencias desastrosas.
- Estar acorde a las necesidades, a los requerimientos legales y a las normas internacionales. Hoy día, en México se han promulgado leyes de protección de la confidencialidad de la información de datos personales y políticas de privacidad, de manera que desde el punto de vista legal, las empresas están obligadas a mantener todos los datos de empresas y de sus clientes de manera segura.
- Derivado del punto anterior, si se demuestra a todos los interesados que la empresa tiene programas efectivos de prevención de riesgos informáticos, se mejorará la confianza de los accionistas, empleados y clientes.
- En muchas ocasiones se toman decisiones sobre seguridad o se elaboran planes de prevención con poco conocimiento sobre los riesgos informáticos. Un plan elaborado con bases ayudará a tomar mejores decisiones y mejorar la planeación en general.
- Sin duda, todas las empresas asignan ciertos recursos para el manejo de riesgos, sobre todo los informáticos, pero si las bases para disminuir o evitar este tipo de riesgos no son muy buenas, un plan bien elaborado ayudará a mejorar la asignación de recursos para el manejo de riesgos.
- Uno de los grandes errores de muchas empresas es decir "a nosotros nunca nos va a pasar". Por ello, cuando algo sucede, las pérdidas son muy costosas, de manera que un buen plan de prevención ayuda a prevenir pérdidas tanto de información como monetarias.
- Si se elabora un plan de prevención con la mejor información disponible, en el futuro se tendrán todos los elementos para reaccionar mejor ante una contingencia informática, que si no se tiene ningún plan.
- Si se copia un plan de otra empresa sólo porque en la otra empresa "ha dado buenos resultados", es posible que dicho plan trabaje y funcione de manera adecuada; sin embargo, las condiciones nunca serán las mismas en una empresa o en otra, por lo que es probable que la adopción de un plan ya hecho consuma recursos innecesarios o no considere algunas condiciones especiales que tiene la empresa; es decir, de entrada este plan ya

tendrá deficiencias. No hay nada como elaborar un plan a la medida de las necesidades de la empresa.

- Hay actividades que crean valor para la empresa, y la creación de valor implica realizar actividades que le otorguen una ventaja competitiva a la institución; es decir, la actividad que crea valor sólo la realiza dicha empresa, lo que puede llevar a convertirla en líder en su sector de mercado. Si una empresa cuenta con excelentes planes de contingencia informática, y nadie de la competencia tiene planes similares, se puede afirmar que tiene una ventaja competitiva en el mercado, ya que es casi seguro que sus actividades nunca se detendrán debido a esta causa. Por tanto, un plan de contingencia informática le agrega valor a la empresa.

Es con esta visión integral que se aborda el presente capítulo.

Actividad de aprendizaje

Formen equipos y, mediante una presentación electrónica, expliquen con detalle los cuatro bloques que componen a las TIC dentro del marco del buen gobierno. Expongan su trabajo frente al grupo.

6.2 El plan de contingencia informática

En lo que se refiere a seguridad informática, se puede hacer una *planeación idealizada* y una *planeación estratégica*. Lo que distingue a ambas planeaciones se observa en su nombre. La palabra estrategia proviene del vocablo griego *strategos*, que significa un general en el campo de batalla; por esta razón, cuando se habla de planeación estratégica se habla de hacer un plan para vencer a un enemigo, en tanto que en la planeación idealizada no hay enemigo, sólo se planea hacer algo de la mejor manera.

En informática, como se vio en capítulos anteriores, existe un enemigo invisible al que se le llama hacker, que puede ser un individuo o un grupo de personas con la intención de atacar en formas muy distintas a una empresa u organización; cuando los hackers atacan, en realidad se considera una guerra,

pues éstos nunca se detienen y su objetivo siempre es causar un daño. Por tanto, si una organización que ha sido atacada y ha sufrido un daño considerable, puede demandar y encarcelar al atacante, es seguro que lo va a hacer, como ya ha sucedido en muchas ocasiones en todo el mundo. Incluso, para combatirlos se ha creado y desarrollado la informática forense, cuyo objetivo principal es hallar al culpable del ataque, para que en el marco de la legalidad éste reciba un castigo, aunque ya haya pasado mucho tiempo después del incidente.

En otras ocasiones, el enemigo no es una persona sino la propia naturaleza la que ataca a una organización en forma de terremotos o inundaciones, afectando a la TI de una organización.

Con base en lo expuesto antes, en la *planeación estratégica* se deben definir la misión, la visión y los objetivos, primero de la organización en general y luego los del área de informática en particular. Se dice que la misión, la visión y los objetivos del área de informática siempre deben "estar alineados" con la misión y la visión de toda la organización, lo que significa que todos los planes que emprenda el área de informática deben contribuir a la consecución de la misión y la visión general de la organización; de lo contrario, se podrían emprender acciones que parezcan atractivas en el papel y que van a consumir recursos económicos y de otro tipo, pero no ayudarían mucho a lograr lo que en realidad quiere la empresa. De nuevo, de acuerdo con COBIT, en el bloque de planificación y organización de la TI se requiere un plan estratégico de la TI y no sólo un plan (idealizado).

Como existe una enorme diversidad de empresas y organizaciones que utilizan TIC, es imposible declarar una misión y una visión genéricas, pues cada una de estas empresas, de acuerdo con su giro y actividad, tienen misiones y visiones distintas, de manera que es posible suponer que esta declaración ya existe, y el citado texto sólo se enfocaría a una misión y una visión que quizá tenga un área de informática de cualquier empresa.

La misión debe declarar el objetivo para el cual se creó el área de informática, mientras que la visión debe declarar cómo se ve o se vislumbra el área de informática al cabo de dos o tres años máximo, a partir de su estado actual. Con esto en mente, se declara la misión y la visión que podría tener cualquier

empresa u organización con un uso intensivo de las TIC, como la que se observa a continuación.

Misión del área de informática

Actualizar continuamente las TIC utilizadas por la empresa, operarlas de manera ética y transparente y tomar las medidas necesarias para preservar su funcionamiento e integridad.

Visión del área de informática

En dos años, el área de informática de la empresa será un área 100 por ciento confiable en cuanto al manejo ético, a la preservación de la integridad de la información y de las TIC y a la calidad de las medidas de seguridad que se tengan para evitar pérdidas o daños de la información y de las TIC que se posean.

Si estas declaraciones las ha emitido el director del área de informática, de común acuerdo con el director general de la organización, entonces se debe entender que podrá contar con los recursos necesarios de todo tipo para cumplir con la misión y la visión del área. De poco sirve elaborar planes de prevención perfectos, si no se tiene el apoyo de la dirección general en cuanto a los recursos monetarios y de personal que dichos planes van a consumir. Ésta debe ser la base sobre la cual se diseñen los planes de contingencia informática.

En el sentido de que la planeación debe ser estratégica, ésta implica considerar al enemigo contra quien se va a luchar; por tanto, es muy importante tener registros o estadísticas de los ataques o daños que han sufrido tanto la información como las TIC de la organización en los últimos años. Pero las estadísticas no sólo deben ser de la empresa, también hay que estar actualizados en cuanto a la información que se publica en revistas especializadas respecto a la tendencia de los tipos de ataques informáticos que han afectado a otras organizaciones en fechas más recientes; por ejemplo los ataques más frecuente de suplantación de la dirección IP, porque los hackers han encontrado una nueva forma de realizarlo, contra la cual las empresas aún no están preparadas; o que los atacantes han encontrado una forma totalmente novedosa de robar

datos confidenciales, contra la cual aún no se han desarrollado suficientes métodos de prevención. Sólo bajo este esquema es que un plan de contingencias informáticas adquiere más sentido; de lo contrario, se convierte en una planeación idealizada que, desde luego, también tiene utilidad.

Con estos antecedentes, ya se puede tener una definición de *plan de contingencia informática.*

> *La* contingencia informática *es una serie de actividades que se deben realizar a fin de prevenir y predecir cualquier tipo de ataque informático que pueda sufrir la organización, estas actividades también incluyen corregir o restaurar los daños causados a fin de mantener las actividades normales tanto del área informática, así como de la empresa u organización.*

Se puede considerar que el plan estratégico consta de tres partes o subplanes:

1. Plan de prevención.
2. Plan de predicción.
3. Plan de corrección o de continuidad del negocio.

El objetivo del plan estratégico general es proporcionar los fundamentos y ajustes organizacionales para diseñar, implementar, monitorear, revisar y disminuir la probabilidad de ocurrencia de riesgos y amenazas. Los fundamentos incluyen políticas, objetivos y reglamentos para administrar el riesgo, mientras que los ajustes de la organización consideran planes, relaciones, recursos, procesos y actividades.

Sin embargo, antes de que una organización elabore cualquiera de los tres tipos de planes, primero debe hacer una serie de precisiones acerca de lo que deben hacer dichos planes, para lo cual es necesario identificar y medir. Hay que determinar lo que en realidad es valioso para la empresa, no sólo en el área de informática. Asimismo, hay que determinar a cuáles riesgos está

expuesta el área de informática y medir aquellos que resultarían realmente graves si llegaran a suceder, además de determinar cuáles son los ataques informáticos más comunes, los cuales cambian con el tiempo, pues los hackers se actualizan más rápido que las empresas. Por último, hay que determinar el costo de cada plan, con base en lo que van a proteger comparado contra el costo que tiene dicha protección.

Elaborar los planes no es tan complicado como llevarlos a cabo. Las empresas casi siempre tienen restricciones presupuestales, lo que hace que carezcan de algunas herramientas apropiadas para enfrentar la exposición a los riesgos informáticos; asimismo, también falta dinero para contratar a buenos asesores, y por lo común los equipos disponibles en el área de sistemas no son suficientes en capacidad ni en cantidad y casi nunca se tienen estadísticas de todos los incidentes informáticos que han ocurrido en la empresa.

Aun cuando la elaboración de planes convenciera a la alta gerencia de aportar los recursos necesarios, la solución no se obtendría de inmediato y la empresa seguirá expuesta a riesgos, muchos de ellos desconocidos, que podrían comprometer su estabilidad y supervivencia. Por tanto, hay que iniciar tan rápido como sea posible, en la medida de las posibilidades de la empresa. De acuerdo con Rigante (www.isaca.org), se sugieren estos pasos para iniciar con la identificación de escenarios de riesgos:

1. Tomar como base estándares internacionalmente reconocidos y guías tales como COBIT 5, que contiene 111 ejemplos de escenarios de riesgo para TI. También se puede consultar MAGERIT, que incluye numerosas amenazas informáticas para cada tipo de activo/recurso con la correspondiente medida preventiva. O bien, está ISACA, que es una asociación internacional que tiene enorme cantidad de datos y cuenta con especialistas que pueden ayudar en multitud de problemas.
2. Analizar los objetivos de la empresa con el propósito de identificar los riesgos relacionados a la TI que pudieran obstaculizar la consecución de dichos objetivos.

ISACA (Asociación para el Control y Auditoría de Sistemas de Información) es una asociación profesional internacional enfocada al gobierno de TI; sus siglas reflejan el amplio rango de profesionales en TI a los que les es útil.

3. Reunir información del know-how de expertos dentro de la empresa, que puedan comprometerse con el proceso de administrar los riesgos a los que está expuesta la TI.
4. Evaluar nuevas vulnerabilidades de los activos/recursos de TI que tiene la empresa.
5. Aplicar la "ingeniería inversa" sobre los controles requeridos por las leyes y los reglamentos vigentes con el objetivo de inferir o detectar posibles amenazas provenientes de esos controles.
6. Analizar los incidentes de los riesgos de operación que han llevado a pérdidas, a fin de detectar escenarios que se han hecho realidad en los riesgos de TI.
7. Sólo hasta que se hayan reunido muchos datos de riesgos materializados, la empresa podrá definir de manera formal el enfoque del análisis que va a emprender. Por lo común, la aprobación del enfoque propuesto requiere ser aprobado por muchas instancias de la empresa.
8. Los escenarios de riesgos materializados de TI que se analizan en la empresa deben actualizarse en forma regular, dependiendo de las nuevas amenazas que surjan en el campo de la informática y los sistemas, del desarrollo de nuevos estándares, de nuevos desarrollos tecnológicos, y de que la empresa cuente con personal más capacitado para administrar el riesgo de TI.

Ingeniería inversa es obtener información o un diseño a partir de un producto, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado.

Una vez identificados los principales riesgos informáticos que ya han sucedido, no sólo en la empresa sino también fuera de ella, es posible iniciar la elaboración de los tres subplanes, asignando prioridades de ataque-defensa.

Actividad de aprendizaje

En equipo de dos o tres personas elaboren un póster donde presenten los pasos para llevar a cabo la identificación de escenarios de riesgos. Sean creativos. Expongan sus trabajos al grupo.

6.3 Determinación de parámetros antes de elaborar los planes

En analogía con el cuerpo humano, los sistemas informáticos dentro de una organización equivalen al sistema nervioso. No es necesario explicar mucho para estar conscientes de las graves consecuencias que tendría para la vida normal de una persona si sólo una pequeña parte de su sistema nervioso sufriera un daño que le provocará algún grado de desconexión o paralización durante un tiempo, aunque fuera breve. Sin embargo, un ser humano que sufriera un traumatismo en el sistema nervioso de una mano, un brazo o una pierna, estaría discapacitado en cierto sentido, aunque podría seguir viviendo, pero hay ciertas partes del cuerpo, como el cerebro, los pulmones y el corazón que no pueden detener su funcionamiento, ni siquiera un minuto; es decir, hay partes del cuerpo que realizan ciertos procesos orgánicos que son vitales y otras que realizan procesos, que si bien son importantes, no son vitales; de este modo, hay muchos seres humanos que viven sin vesícula biliar, páncreas, un riñón, etcétera, que aunque desempeñan procesos importantes, el cuerpo humano puede prescindir de ellos. Lo mismo sucede en las empresas u organizaciones.

La información es la que mantiene trabajando todas las partes de la empresa, pero no todas las áreas o partes de la empresa son vitales, ni todos los procesos que se desarrollan en cada área empresarial lo son. Si el flujo de información se llegara a detener en algún punto de la empresa, podría llegar a ser fatal, en tanto que la interrupción en el flujo de información en otras áreas podría representar sólo un retraso en las actividades de esa área. Lo ideal, al igual que en el ser humano, es que nunca se llegue a detener el flujo de información, ni siquiera por breves instantes.

Por esta razón, el primer paso en la elaboración de un plan de contingencia es determinar las áreas que son vitales para la organización; por ejemplo, si la empresa es de manufactura, no se puede detener la producción, pues esto implicaría que el producto no llegará a tiempo al cliente, ni en la cantidad suficiente; lo cual redundaría en perder clientela. El cliente es la razón de ser de toda empresa, no sólo por ser la fuente de ingreso, sino porque tampoco

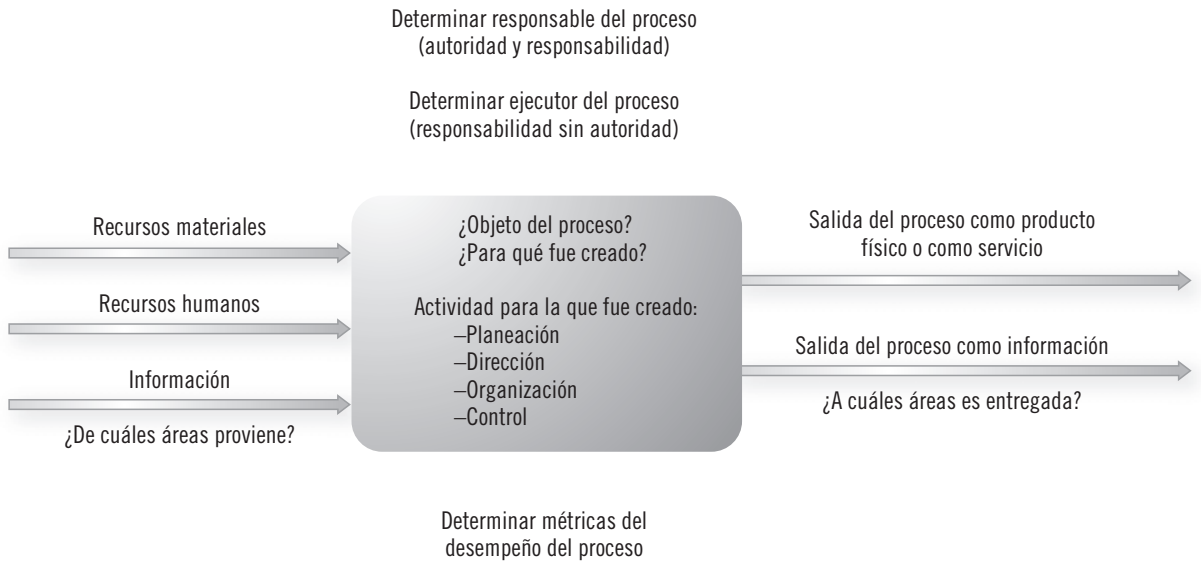
es posible detener el control de calidad del producto, ya que es impensable elaborar productos durante tan sólo una hora, sin saber a ciencia cierta cuál es la calidad que se va a entregar al consumidor. Si la empresa es de servicios, podrá detenerse cualquier área, pero el servicio, sobre todo si ya está programado ejecutarlo con el cliente, no se puede detener, ya sea que éste sea en la ventanilla de un banco o dando mantenimiento a la maquinaria de una empresa de manufactura.

En estos sencillos ejemplos es posible observar cómo el flujo de información se puede detener en el área de dirección, en los almacenes, en recursos humanos, etcétera, hasta por varias horas, y no pasará de una perturbación en un día laboral en la empresa. Esto mismo debe hacerse en el área de informática, donde hay procesos vitales y procesos de apoyo; por tanto, el primer paso es elaborar una lista con todas las áreas, primero de toda la empresa y luego las áreas de informática y distinguir aquellas que son vitales para la empresa.

Una vez identificadas las áreas vitales para la empresa, lo siguiente es identificar los procesos sustantivos o vitales de cada área, debido a que éstos ejecutan los procesos que agregan valor al producto (o al servicio) y, por tanto, generan valor o ganancia para la empresa. Es relativamente sencillo determinar lo que es un proceso para identificarlo, pues tiene una serie de características que lo definen (véase figura 6.1).

Luego, hay que determinar la relevancia del proceso en términos del grado de afectación para la empresa en caso de que el proceso en cuestión llegara a interrumpirse por falta de información. La importancia o relevancia de un proceso sólo se puede medir cualitativamente, de manera que es posible clasificarlo en:

- **Proceso vital o crítico.** Es aquel cuya interrupción, aunque sea durante breves minutos, causa un daño relevante, económico o de imagen hacia la empresa. Por ejemplo, cuando en un banco se interrumpe el servicio por problemas en la red interna, como caída del sistema informático, aunque sea por pocos minutos.
- **Proceso importante continuo.** Proceso de apoyo en la actividad cotidiana de la empresa. Su ejecución puede interrumpirse incluso por horas, sin



› **Figura 6.1**
Características para definir un proceso.

dañar seriamente a la economía o a la imagen de la empresa, pero debe ejecutarse a diario o varias veces por semana; por ejemplo, respaldar la información, rastreo de puertos, entre otros.

- **Proceso importante intermitente.** Es aquel cuya actividad se puede suspender por días sin causar daños relevantes; por ejemplo, la evaluación del desempeño del personal, la planeación anual de ventas y la elaboración del mantenimiento predictivo de la maquinaria, entre otros. En general, son procesos que se ejecutan una o dos veces al año por breves periodos.

Quizá parezca redundante decir "proceso importante", pues todos los procesos son importantes, ya que de no serlo, no existirían, y como se observa en la figura 6.1, serían actividades hechas sin sentido, sin un objetivo definido.

Una vez que los procesos se han definido y jerarquizado, habrá que hacer lo mismo con los riesgos a los que está expuesta la empresa. Al referirse en específico al área de informática, existen dos tipos genéricos de riesgos: los físicos y los lógicos.

Los riesgos físicos, a su vez, se dividen en internos y externos:

- Riesgos físicos internos

a. Fallas en la conexión de una red.

b. Fallas en el funcionamiento de un equipo.

c. Interrupción del servicio de energía eléctrica.

d. Saturación de la capacidad de memoria del sistema.

e. Renuncia intempestiva de personal.

f. Ingeniería social interna o externa.

g. Sistemas débiles en la seguridad de acceso al área de informática, que permitan el acceso de gente extraña o maliciosa en horario de oficina o por las noches.

h. Sistemas débiles para protección contra fuego generado por instalaciones eléctricas deficientes o por un descuido del personal.

i. Que el área de informática esté expuesta a un calor intenso o cerca de recipientes de alta presión, como calderas o compresores (esto es probable en empresas de manufactura).

- Riesgos físicos externos

A. Protección insuficiente contra terremotos que ocasionen daños a las instalaciones.

B. Protección insuficiente contra inundaciones.

Actividad de aprendizaje

Selecciona tres riesgos físicos internos y dos riesgos físicos externos, y anota una posible solución a cada uno de ellos. Comparte con tus compañeros.

Por su parte, los riesgos lógicos ya fueron tratados en los capítulos 4 (La seguridad física y lógica en redes) y 5 (Firewalls como herramientas de seguridad), aunque no de manera exhaustiva, por lo que sólo se vuelven a mencionar para efectos de los planes de contingencia.

i. Ingeniería social
ii. Suplantación de la dirección IP
iii. Ataques con analizadores de red
iv. Ataques a servidores de la web
v. Inyección SQL
vi. Correo spam
vii. Ataque de secuencia de comandos
viii. Ataques con analizador de puertos
ix. Secuestros informáticos
x. Virus informáticos (gusanos, troyanos, bombas lógicas, etc.)
xi. Spyware
xii. Spoofing
xiii. Negación del servicio
xiv. Rootkit
xv. Botnet
xvi. Phishing

Y los que vayan surgiendo

En el capítulo 4 (La seguridad física y lógica en redes) se hace referencia al Uptime Institute, formado desde 1993 por un grupo de empresas, el cual, entre otras cosas, ofrece consultoría y certificación para data center, aunque en realidad es más conocido por ofrecer certificaciones. Las empresas que logran una certificación de este instituto en cualquiera de sus cuatro niveles

Un data center son instalaciones que contienen sistemas de cómputo y ofrecen servicios de telecomunicaciones y almacenamiento de datos.

› **Figura 6.2**
Data center.

son consideradas empresas muy confiables en lo que respecta a garantizar la continuidad en el funcionamiento del área de informática. Obtener una certificación de este tipo puede requerir desde la construcción de una nueva edificación, hasta la reforma de una en operación; pero, por lo común, asesoran a empresas de informática con operaciones en crisis inminente por fallas en la infraestructura, baja confiabilidad o no conformidad con las normas y los estándares regulados.

La necesidad de una certificación surge en respuesta a una necesidad o vulnerabilidad concreta, de forma que una empresa con este tipo de problemas, que logra adquirir una certificación, prácticamente tiene garantizada la eliminación de todos los riesgos físicos internos y externos a que pudiera estar expuesta, también enumerados y analizados en el capítulo 4.

La siguiente parte en la determinación de estos parámetros, antes de intentar la elaboración de cualquier plan de contingencia, es determinar la gravedad de afectación en la empresa en caso de que el riesgo detectado llegara a suceder, para lo cual se podría hacer una estimación cualitativa de la probabilidad de que suceda un riesgo y el valor mínimo que debe tener ese riesgo para poner en marcha el plan de la contingencia en su fase de mitigación o corrección del daño. Una escala cualitativa de la probabilidad de ocurrencia es expresar la probabilidad como despreciable, baja, media, alta. En tanto, la calificación de la consecuencia, una vez que la amenaza se ha vuelto real y el riesgo ha sucedido, puede catalogarse como inocua, significativa, crítica o catastrófica.

Al establecer estas determinaciones, lo siguiente es entregar el o los criterios para caracterizar los riesgos y la asignación de prioridades de acuerdo con la severidad de las consecuencias, desde los más dañinos hasta los más inocuos. En esta parte permanece vigente la determinación de los umbrales de cada riesgo que inicien acciones tendientes a mitigarlos, en caso de que

sucedan; esto es, los límites mínimos y máximos en los que se debe tomar acción inmediata, a fin de tener los menores costos y el menor daño posible con las medidas tomadas cuando los riesgos ya hayan sucedido o cuando resulte inminente que sucedan.

6.4 Plan de prevención

Si se quiere prever que algo no suceda, primero se debe conocer contra qué hay que prevenirse. Una vez que se han hecho todas las identificaciones y determinado todos los parámetros mencionados en el apartado 6.3 para iniciar la elaboración del plan de prevención de contingencias, lo siguiente es elaborar una serie de tablas informativas como las que se muestran a continuación (véanse tablas 6.1 a 6.5), suponiendo que sólo existen esas áreas y esos riesgos.

Tabla 6.1 Áreas del departamento de sistemas y la importancia de los procesos que realizan

Área	Número de procesos vitales o críticos	Número de procesos continuos	Número de procesos discontinuos
1. Dirección de sistemas	3	5	2
2. Administración de servidores	3	4	1
3. Administración de red	4	6	1
4. Mantenimiento de la red	5	8	5
5. Recepción de datos	2	7	3
6. Procesamiento de datos	2	15	6
7. Almacenamiento y respaldo de datos	6	10	3

En la tabla 6.1 deben registrarse todos los procesos que realiza cada área y clasificarse de acuerdo con su importancia. Por su parte, en la tabla 6.2 se hace una matriz de las áreas de informática contra el tipo de riesgo a que cada una está expuesta, al suponer que esos son todos los riesgos físicos, internos y externos, con los que puede estar amenazada la integridad física de esa área.

El tipo de riesgo físico se ha identificado con un número que corresponde a los riesgos físicos planteados en el apartado 6.3, de manera que en las intersecciones de esta tabla es posible detectar con facilidad el tipo de riesgo al cual está expuesta cada área. Desde luego que el llenado de las intersecciones de la tabla es sólo para efectos de ejemplificar su utilidad.

Tabla 6.2 Áreas de informática y los riesgos físicos a los que están expuestas

Área	Tipo de riesgo										
	a	b	c	d	e	f	g	h	i	A	B
1. Dirección de sistemas	x				x	x			x		
2. Administración de servidores		x	x				x	x		x	x
3. Administración de red				x	x	x			x	x	
4. Mantenimiento de la red	x	x	x		x	x		x			x
5. Recepción de datos	x		x	x	x		x	x		x	
6. Procesamiento de datos		x	x	x		x					x
7. Almacenamiento y respaldo de datos	x	x	x		x	x	x		x	x	x

Luego, se debe construir una tercera tabla que muestre a cada una de las áreas el tipo de riesgo que ya ha sufrido y cómo han clasificado, tanto la dirección general de la empresa, como el director del área de sistemas, el que haya sucedido cierto riesgo en determinada área (véase tabla 6.3).

Tabla 6.3 Áreas de sistemas e intensidad de la consecuencia de acuerdo con el riesgo físico

Área	Consecuencia inocua	Consecuencia significativa	Consecuencia crítica	Consecuencia catastrófica
1. Dirección de sistemas	b, c	d	e	f, h
2. Administración de servidores		c, b		B
3. Administración de red		c	f	B
4. Mantenimiento de la red		c		B
5. Recepción de datos		c	g, f	h, c, B
6. Procesamiento de datos		c	g	i h, B
7. Almacenamiento y respaldo de datos			g, c	b, d, i, h, B, A

La tabla 6.3 indica cuáles son las áreas que, de dañarse con un tipo especial de riesgo, pondrían a la empresa en verdaderos problemas debido a la interrupción en el flujo de información. (Recuérdese que las anotaciones que aparecen en la tabla 6.3 no pertenecen a alguna empresa y son sólo para fines didácticos.)

Luego, se puede elaborar una cuarta tabla que muestre la frecuencia de los riesgos que ya han sucedido y las áreas que afectaron. Por ejemplo, el área de almacenamiento y respaldo de datos nunca ha sido afectada por una falla de los dispositivos de almacenamiento y, sin embargo, se sabe que de suceder un ataque a esta área la consecuencia para la empresa sería catastrófica. El objetivo de las tablas 6.1 a 6.3 es saber lo que no debe suceder en cuanto a riesgos físicos en cada área, a fin de prevenir que nunca lleguen a suceder en realidad; es decir, cuidar al máximo esta posibilidad de ocurrencia. Esta cuarta tabla se va a presentar en el plan de predicción de contingencias.

Para los ataques lógicos a las redes o a las computadoras personales sólo habría que elaborar las tablas 6.2 y 6.3, ya que el director del área de sistemas o el administrador de la red, entre otros, aunque estén conectados en red, en su computadora personal con seguridad mantienen datos confidenciales respecto al área de sistemas o de informática, y esa computadora en especial está en riesgo de sufrir cualquiera de los ataques mencionados. Por esta razón, en las tablas que se elaboren para los riesgos lógicos, es necesario mantener exactamente las mismas áreas.

Las tablas 6.4 y 6.5 tienen el mismo formato que las tablas 6.2 y 6.3, excepto que en vez de que el tipo de riesgo sea físico, se muestran los riesgos lógicos y la consecuencia que pueden causar a la empresa cualquiera de los ataques lógicos mencionados, los cuales también se clasifican en inocuos (molestos), significativos, críticos y catastróficos.

Tabla 6.4 Áreas expuestas a diferentes tipos de riesgos lógicos

Área	Tipo de riesgo															
	i	ii	iii	iv	v	vi	vii	viii	ix	x	xi	xii	xiii	xiv	xv	xvi
1. Dirección de sistemas	x				x	x			x					x	x	
2. Administración de servidores		x	x				x	x		x	x	x		x		x
3. Administración de red				x	x	x			x	x				x	x	
4. Mantenimiento de la red	x	x	x		x	x		x			x	x	x		x	
5. Recepción de datos	x		x	x	x		x	x		x		x			x	x
6. Procesamiento de datos		x	x	x		x					x	x				x
7. Almacenamiento y respaldo de datos	x	x	x		x	x	x		x	x	x	x	x			

Tabla 6.5 Áreas de sistemas e intensidad de la consecuencia de acuerdo con riesgo lógico

Área	Consecuencia inocua	Consecuencia significativa	Consecuencia crítica	Consecuencia catastrófica
1. Dirección de sistemas	iii, v, xi	viii, vi,	iv, xii	iv, vi, vii
2. Administración de servidores		i, ii		x, xii, xiii
3. Administración de red		iv, ix,		v, viii
4. Mantenimiento de la red	i, iii, x			ix, x, xiv
5. Recepción de datos				vii, viii, ix
6. Procesamiento de datos			ii, iv	v, vi, viii
7. Almacenamiento y respaldo de datos			viii, xv, xvi	ivx, xv, xvi

De momento ya se ha delineado el primer punto a desarrollar, que es la obtención de los datos necesarios para elaborar el *plan de prevención de contingencias*. Si la empresa no cuenta con suficientes recursos económicos para contratar los servicios de una subsidiaria del Uptime Institute, o simplemente no quiere hacer uso de esos servicios, el siguiente punto que deberá desarrollar en el plan de prevención es determinar los recursos materiales y humanos que se requieren para llevar a cabo dicho plan. En este punto son muy importantes los datos de las tablas 6.1 a 6.5, tanto de riesgos físicos como de riesgos lógicos.

En la segunda parte del plan de prevención es necesario contestar las preguntas:

- **¿Qué se va a resguardar o a proteger?**
  También hay que considerar los equipos que tienen que protegerse destacando todas sus características.
- **¿Contra qué se va a proteger?**
  Para responder a esta pregunta se utiliza la información de las tablas anteriores, haciendo énfasis en el tipo de riesgos a los que cada área está expuesta.
- **¿Cómo se van a proteger tanto áreas como equipos?**
  Aquí lo más importante es hacer una lista de las necesidades materiales para realizar la prevención. Por ejemplo, en los riesgos físicos podría requerirse mejor protección contra incendios, cursos de cómo protegerse contra la ingeniería social, implantar controles biométricos de acceso a áreas restringidas más efectivos de los que ya tuviera la empresa, etcétera, y todo eso cuesta dinero. En lo que respecta a los riesgos lógicos, es necesario determinar cuántos firewall hay que instalar, si se instalará sólo firewall de hardware, sólo de software o ambos, o si es necesaria una zona desmilitarizada, con qué frecuencia se debe realizar un rastreo de puertos, etcétera; sin embargo, muchas de estas medidas pueden requerir la compra de equipo especializado, lo cual resulta muy costoso.
- **¿Quién estará a cargo de las actividades que conlleva el plan de prevención?**
  En este punto puede ser necesaria una pequeña reestructuración organizacional del área de sistemas o informática, pues para que cualquier plan sea efectivo se requieren responsables y que cada uno de los integrantes del área conozca a la perfección sus obligaciones en caso de contingencia informática. Este punto también incluye el hecho de que pudiera requerirse personal extra.
- **¿Con qué frecuencia hay que hacer supervisiones a fin de comprobar que la organización siempre esté preparada o prevenida para evitar que suceda algún tipo de ataque?**

Una cosa es hacer un plan y otra muy distinta es ponerlo en práctica, de tal suerte que haya una probabilidad mínima de sufrir un daño debido a un ataque físico o lógico. Por tanto, en este punto se debe hacer una programación de la periodicidad con la cual es necesario verificar que cada una de las medidas preventivas propuestas está vigente y actualizada.

Una vez que se han respondido a satisfacción las preguntas anteriores y se han presentado varias alternativas, sobre todo de tipo tecnológico, derivadas de las respuestas a éstas, el siguiente paso es determinar el costo de cada alternativa. Pero aquí no se trata de seleccionar la de menor costo, sino de hacer un balance entre el costo de la alternativa contra la protección que proporcionará, lo cual depende del tipo de empresa.

En capítulos anteriores se ha argumentado que la información es el activo más valioso de cualquier organización, sólo después del recurso humano; sin embargo, no tiene el mismo valor la información, por ejemplo, de una empresa que presta servicios de fumigación industrial, que el valor que tiene la información para una institución bancaria o para el Servicio de Administración Tributaria (SAT), encargado de la recaudación de los impuestos de los contribuyentes en México. Desde luego, a todas las empresas les interesa conservar íntegra su información, pero el daño que causaría a la organización la alteración de la información o incluso la pérdida es muy distinto en una empresa de fumigación industrial que en una institución bancaria o en el SAT. Un banco o el SAT estarán dispuestos a invertir lo que sea necesario para evitar o prevenir cualquier tipo de ataque, ya sea físico o lógico, con el consiguiente daño que implica.

En resumen, los pasos del *plan de prevención* son:

1. Identificar y medir el tipo de riesgos al que está expuesta la empresa, en especial el área de informática.
2. Identificar los equipos informáticos que están más expuestos o desprotegidos hacia los diferentes riesgos.
3. Con base en lo anterior, determinar el personal, los equipos y el software necesarios, adicionales a los que ya se tienen, para proteger en todos los

sentidos al área de informática de cualquier amenaza física o lógica; es decir, lo extra necesario para llevar a cabo el plan.

4. Reasignar puestos y responsabilidades al personal que estará a cargo del plan de prevención de contingencias informáticas.
5. Determinar varias alternativas del plan de contingencias con su respectivo costo, el cual debe incluir personal, equipo y software adicionales necesarios.
6. Seleccionar la alternativa que presente el mejor balance entre costo-protección contra amenazas, de acuerdo con el valor que la empresa le otorgue a su información.

Actividad de aprendizaje

Elabora un diagrama de flujo o esquema donde presentes los pasos de un plan de prevención.

6.5 Plan de predicción

Ya se ha hablado de que es posible asignar una medición cualitativa a la probabilidad de ocurrencia de cualquier tipo de amenaza, y en esta escala la probabilidad se puede expresar como despreciable, baja, media y alta. Por otro lado, también ya se describieron los diferentes tipos de riesgos; los físicos internos se numeraron de la "a" a la "i", los físicos externos como "A" y "B", y los lógicos del "i" al "xvi". Ahora, habrá que construir una tabla que muestre las mismas áreas de informática o de sistemas; en el renglón superior de ésta habrá que enlistar todos los riesgos, mientras que en las casillas se deberá anotar la probabilidad de ocurrencia de cada tipo de riesgo, usando la notación de riesgos: despreciable (d), baja (b), media (m) y alta (a), tal como se muestra en la tabla 6.6.

Tabla 6.6 Frecuencia de riesgos que han sucedido respecto a cada área de informática

	Tipo de riesgo																								
Área	a	b	c	d	e	f	g	h	i	A	B	i	ii	iii	iv	v	vi	vii	viii	ix	x	xi	xii	xiii	xiv	xv	xvi
1																											
2																											
3																											
4																											
5																											
6																											
7																											

Para hacer las anotaciones pertinentes es necesario contar con una serie de datos históricos recientes, tanto de las amenazas físicas como de los ataques lógicos que ha sufrido cada área de informática, no sólo dentro de la empresa, sino también, si es posible, conseguir datos de lo que ha sucedido en otras empresas. Hay dos formas de llenar los cuadros de la tabla 6.6. La primera consiste en anotar en cada casilla el número de ataques sufridos o amenazas que han sucedido en cada área, y de ahí inferir cuáles tienen más probabilidad de ocurrencia. La segunda consiste en tener una lista del número de ataques y

amenazas que han sucedido y traducir esos datos a la escala de probabilidad cualitativa mencionada; por ejemplo, si la computadora de la dirección ha sufrido 21 ataques de spam en el último mes, esa será una probabilidad alta, y a partir de ese número se determinará cómo se consideran las probabilidades de acuerdo con el número de ataques sufridos, de manera que los cuadros de la tabla 6.6 se llenen con las letras d, b, m y a, en vez de números.

Pero no es tan sencillo tomar decisiones. Si bien la tabla 6.6 puede ser un buen indicador de qué área está siendo más atacada y qué tipo de ataque o ataques está teniendo, no es lo mismo que la computadora de la dirección general tenga spam, a que un servidor haya tenido una suplantación de dirección IP, por lo que para tomar decisiones de prevención, es necesario considerar los aspectos que muestran las cuatro tablas, es decir, tipo de riesgo, gravedad de la consecuencia del ataque y frecuencia del ataque, y con base en esos datos determinar una política de administración del riesgo, la cual es una declaración de las intenciones de una organización respecto al riesgo.

La política que seguirá la empresa u organización respecto al riesgo implica la actitud que se va a tomar una vez que se ha analizado el contenido de las tablas anteriores. Esta actitud no siempre consiste en eliminar por completo todos los riesgos, eso es ideal pero muy costoso. Un riesgo se puede tomar, disminuir su probabilidad de ocurrencia o eliminar.

Un riesgo que se puede tomar es que haya spam en algunos host o en algunas computadoras personales y determinar un umbral del riesgo; por ejemplo, si no disminuye mucho la velocidad de las computadoras atacadas, puede no tomarse ninguna acción, pero si esa actuación lenta sobrepasa cierto nivel, entonces se deberán tomar medidas contra el spam. Otro riesgo factible de tomar es enviar semanalmente (o con otra frecuencia) respaldos de la información fuera de la empresa en una instalación no propia, para que en el peor de los casos no se pierda más que los datos de una semana; sería una política riesgosa, pero puede caber en una empresa, dependiendo de lo valiosa que sea la información para dicha empresa.

Por otra parte, disminuir la probabilidad de riesgo representa aplicar un monitoreo continuo con el propósito de observar si el número de los ataques registrados en una tabla similar a la 6.6 han disminuido en un tiempo

razonable, luego de haber tomado y puesto en práctica ciertas medidas. Quizá se observe que sí han disminuido los ataques, pero no al nivel esperado, por lo que habrá que tomar una decisión: o se mantiene ese nivel de incidencia de riesgos o se invierte en forma adicional para disminuir más la incidencia de ataques. Incluso, puede ser que ya se haya invertido en la prevención de ciertos ataques, pero no se ha observado ninguna disminución en su incidencia, lo que significa que se tomaron las medidas equivocadas o el plan de prevención se está aplicando mal y es necesario realizar un nuevo plan.

Pero, como se dijo antes, hay riesgos tanto físico como lógicos que deben eliminarse casi a cualquier precio; no obstante, es la dirección general de la empresa la que decide cuál debe ser la acción correcta a seguir, después de un análisis a conciencia de todos los datos que muestran tablas similares a las mostradas (véanse tablas 6.1 a 6.6), desde luego con la asesoría del director de sistemas o del área de informática, tomando como principal consideración las consecuencia para la empresa en caso de que suceda un ataque o se cristalice una amenaza.

Debido a la naturaleza de la informática, que con seguridad es la ciencia que tiene más dinamismo en su evolución y, por tanto, en sus cambios e innovaciones, aunque se inviertan muchos recursos para eliminar en su totalidad algunos riesgos, siempre quedará un riesgo residual, que en el caso de la informática es un riesgo desconocido. Día a día se desarrollan vacunas contra diversos virus o se diseñan nuevos dispositivos para detectar intrusos; no obstante, el hacker siempre tratará de ir un paso adelante, o poco tiempo después de que se ha diseñado una protección más segura contra ataques, este ya habrá encontrado el antídoto, así que el riesgo residual siempre estará presente.

6.6 Plan de corrección o plan de continuidad en el negocio

A lo largo de la historia de los ataques físicos o lógicos ha habido algunos que han sido tan fuertes, al grado que han detenido la actividad de una empresa durante días. Como se dijo antes, la información es el impulso que da

vida a las actividades de una organización, por lo que aquellas empresas que han perdido datos o cuyo flujo de información ha sido dañado o interrumpido durante horas o días, en realidad se han visto en serios problemas de sobrevivencia.

Continuidad del negocio es un concepto que abarca tanto el *planeamiento para recuperación de desastres* como el *planeamiento para el restablecimiento del negocio*. El *planeamiento para recuperación de desastres o catástrofes* se define como la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan, a fin de restablecer las funciones críticas de la parte operativa del negocio. Tanto el planeamiento para recuperación de desastres como el planeamiento para el restablecimiento del negocio se diferencian del planeamiento de prevención de pérdidas en que este último implica la calendarización de actividades como respaldo de sistemas, autenticación y autorización (seguridad), revisión de virus y monitoreo de la utilización de sistemas (en especial para verificaciones de capacidad). El plan de prevención se concibe para que nunca se llegue a poner en práctica el plan de continuidad del negocio.

Dentro del plan general de contingencia, también se contempla el tercer subplan o plan de corrección, también llamado *plan de continuidad del negocio*, en el cual se define la forma en que la organización se recuperará ante el caso de un desastre informático. El plan se determina con base en los resultados de los análisis de la evaluación de riesgos, al determinar cuáles riesgos son de consecuencias catastróficas, y de impacto en el negocio, en caso de suceder; en general, contempla ubicaciones alternativas, opciones para recuperación de datos, recuperación de recursos humanos, comunicaciones, equipamiento, gestión de proveedores, etcétera, así como todo tipo de actividades que en verdad sean críticas para que el negocio pueda volver a funcionar de manera normal.

Etapa de identificación de consecuencias

Para la determinación de las consecuencias se utilizan los datos de la columna, *"Consecuencia catastrófica"*, de la tabla 6.3. Es importante distinguir con claridad entre elaborar esta tabla y definir en qué consiste la consecuencia

catastrófica. Sólo hasta que se haga esta definición será posible saber qué se va a reparar o a sustituir y los efectos que conllevará para el negocio; hasta entonces se podrán determinar los recursos que hay que tener disponibles para enfrentar la consecuencia.

Tal vez la consecuencia catastrófica más obvia para cualquier empresa es perder toda su información por cualquier causa, desde un virus o el ataque de un intruso que tuvo acceso físico a las instalaciones y borró de manera intencional la información, hasta un incendio o un terremoto. Independientemente de cuál sea la consecuencia que se haya identificado, en este punto también deberá determinarse el costo que tendría para la organización si dicha catástrofe llegara a suceder, pues ésta será la base de comparación cuando se presente el costo del plan de corrección o de continuidad del negocio.

Etapa de determinación de los recursos necesarios para enfrentar con éxito la consecuencia

Una vez concluida a satisfacción la etapa de identificación y costo de las consecuencias para el negocio, se procede a determinar los cinco aspectos del plan en la etapa de recuperación o reparación.

1. **Equipos del área de informática que sufrirían un daño irreparable con un incidente,** los cuales deberán ser adquiridos de nuevo; este daño puede incluir una parte del edificio, mismo que habrá de repararse; esto es muy común en temblores o incendios.
2. **Determinar la logística (secuencia de actividades) necesaria para reiniciar el funcionamiento del negocio.** Aquí se señalan aquellas actividades o procesos que en realidad son críticos en el sentido que deban ser atendidos y puestos en funcionamiento en primer lugar.
3. **Asignar responsabilidades en un organigrama elaborado en exclusiva para casos de riesgos catastróficos**. Se refiere a que de llegar a ocurrir algún riesgo catastrófico, el organigrama no necesariamente será igual a aquel de las operaciones normales del área de sistemas o de informática; esto puede implicar la contratación de personal que se dedique ex-

clusivamente a vigilar la vigencia y operatividad del plan de corrección y recuperación.

4. **Determinar los costos que implica adoptar el plan de corrección y recuperación.** Esto puede implicar que se compre de nuevo hardware o software, se contrate personal nuevo o deban repararse algunas máquinas o determinadas partes del edificio.
5. **Delinear un programa de simulacros de catástrofe.** Contempla un programa de auditorías cuyo objetivo es verificar que se haga lo que se debe hacer, y un programa de verificación periódica encargado de que las medidas adoptadas en caso de catástrofe informática estén listas para activarse en cualquier momento.

Siguiendo con el supuesto de que a consecuencia del evento catastrófico la empresa pierda toda la información de un servidor o de varios servidores, el siguiente paso consiste en determinar si es necesario sustituir el o los servidores, o sólo volver a cargarlos con software y la información. Si el incidente fue a causa de fuego, es seguro que deberá invertirse más en medidas preventivas para evitar y combatir el fuego en el momento en que suceda; pero, si la causa es un terremoto y hay peligro de que el edificio colapse, la alternativa es respaldar la información en otra instalación alejada de donde se ubica la empresa, un lugar que en realidad esté libre del riesgo de fuego y de consecuencias de terremotos, lo cual implica una inversión adicional sustancial, ya que en este caso habría que contratar más personal.

Asimismo, deberá hacerse un cálculo exacto del costo, pues un respaldo de información de profundidad, como la instalación de una sede alternativa de respaldo de datos, deberá trabajar los 365 días del año, las 24 horas del día. Luego, vendrían los simulacros de pérdida total de información en la empresa matriz, para observar la respuesta de la sede alterna de respaldo, respuesta que debe ser casi instantánea, con cero pérdidas de información, y esa sede alterna es donde habría que realizar las auditorías.

En ésta etapa también es posible determinar el tiempo promedio de recuperación de la catástrofe; a menor tiempo de recuperación, mayor costo.

Etapa de toma de decisión

Con todos los datos recabados en las primeras dos etapas del plan de corrección y continuidad del negocio, ya es posible tomar una buena decisión. Lo más recomendable es generar al menos dos alternativas, pues si sólo se tiene una alternativa la única decisión que habría que tomar sería llevar a cabo el plan o no realizarlo, lo cual podría ser mortal para la empresa. La decisión se debe basar en los beneficios obtenidos expresados en términos monetarios, comparados con el costo de elaborar y realizar el plan; los beneficios se pueden calcular como el costo que tendría la empresa en caso de que sucediera una catástrofe informática y que no se tuviera ningún plan de corrección o de continuidad del negocio.

En cualquiera de los tres subplanes siempre se debe buscar la eficacia y la eficiencia. Por *eficacia* de un plan se debe entender que cuando se aplique, éste debe hacer lo que se espera de él; por ejemplo, el plan de prevención en realidad debe prevenir cualquier tipo de contingencia física o lógica. En tanto, *eficiencia* se refiere a que el plan de prevención funcione al menor costo posible, sin disminuir la eficacia de la prevención. Además, todos los subplanes deberán elaborarse de manera que estén alineados con la misión y la visión general de la organización, así como también con la misión y la visión del área de informática de la organización, lo cual significa que los subplanes deberán contribuir, en todas sus actividades, para alcanzar esa misión y visión.

Para lograr la eficacia, la eficiencia y la alineación de los tres subplanes, la dirección general de la organización debe inculcar con el ejemplo una serie de valores a todo el personal propio, además de proveedores y clientes. Dentro de todos los valores humanos que existen, hay tres básicos que siempre deben adoptarse: la honestidad, la ética y el compañerismo. La *honestidad* se deberá reflejar en el hecho de que todo el personal, en especial aquel que labora en el área de informática, al preguntársele acerca de las condiciones de seguridad física y lógica del área, deberá contestar si percibe un riesgo que nadie ha notado, porque la exposición a ese riesgo podría ser la culpa de cierta persona o del mismo personal que está siendo cuestionado, sin impor-

tar las consecuencias administrativas que pudieran surgir para ese personal. En tanto, por *conducta ética* se entiende que nadie debe aprovecharse, para beneficio personal, de la posición jerárquica que ocupe en la organización o del conocimiento que pueda tener o haya adquirido por su mismo trabajo, de información privilegiada que esté almacenada en el área, de claves de acceso a los sistemas lógicos, o claves de acceso físico a las instalaciones, o de puntos de vulnerabilidad que pudieran existir dentro de las instalaciones, entre otros aspectos.

Cultura de la organización o cultura organizacional, son las serie de principios de conducta bajo la cual se rige todo el personal de una organización de manera cotidiana y bajo cualquier circunstancia de presión laboral.

Por último, por *compañerismo* se debe entender la disposición personal de cualquier trabajador de ayudar a resolver problemas o a apoyar en ciertas labores de trabajo, aunque tal apoyo esté fuera de su área de responsabilidad administrativa.

Si estos principios de conducta no sólo los declara el director general de la organización o la empresa, sino que los hace patentes con el ejemplo cotidiano, con el paso del tiempo todo el personal se empapará con esa conducta y principios de modo que se conviertan en la cultura de la organización. Cualquier tipo de proyecto empresarial, ya sea que se trate de subplanes de contingencias informáticas, adopción de cualquier norma, ISO, BS, etcétera, sólo tienen éxito cuando reciben un apoyo decidido de la dirección general.

Como el mercado de recuperación de desastre aún experimenta cambios estructurales significativos, este cambio presenta oportunidades para las empresas de la nueva generación a fin de que se especialicen en la planificación de continuidad de negocio y la protección de datos fuera de sitio.

Actividad de aprendizaje

Investiga en diferentes fuentes de información y, con la ayuda de un procesador de textos, elabora un ensayo donde expliques con detalle cada una de las etapas mencionadas del plan de corrección. Anota la bibliografía consultada. Cuida tu redacción y ortografía.

› **Figura 6.3**
Norma ISO 27000.

6.7 Norma ISO 27000

Ésta norma ISO especifica los requisitos para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad informática con base en el *Círculo de Deming*, consistente en *planear, hacer, verificar* y *actuar*, repitiendo el ciclo en forma indefinida hasta mejorar las condiciones iniciales, en este caso de seguridad informática.

La norma ISO 27000 se refiere a los Sistemas de Gestión de la Seguridad de la Información, y como todas las ISO, es una norma internacional que permite el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas que la procesan, por medio de la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Por su parte, la norma ISO 27001 sugiere ante todo el conocimiento de la organización y su contexto, la comprensión de las necesidades y de las expectativas de las partes interesadas y la determinación del alcance del SGSI, antes de adoptar dicha norma.

Como en toda la serie de normas ISO, en las citadas normas se hace patente la necesidad de que todos los empleados de la organización contribuyan al establecimiento de ésta, con el apoyo de la alta dirección, área que debe demostrar su liderazgo y compromiso mediante la elaboración de la política de seguridad que se aplicará, misma que debe conocer toda la organización.

La norma enfatiza la importancia de la determinación de riesgos y oportunidades cuando se planifica un Sistema de Gestión de Seguridad de la Información, así como el establecimiento de objetivos de seguridad de la información y el modo de lograrlos. Dicho logro depende en gran parte de que la organización cuente con los recursos, las competencias, la conciencia, la comunicación y la información documentada pertinente en cada caso.

La norma indica que para cumplir con los requisitos de seguridad de la información se debe planificar, implementar y controlar los procesos de la organización, así como hacer una valoración de los riesgos de la seguridad de la información y un tratamiento de éstos. Asimismo, también establece la necesidad y la forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de

Gestión de Seguridad de la Información, a fin de asegurar que funciona según lo planeado.

Es conveniente recordar que ninguna norma ISO es obligatoria. De ahí que a esta norma se le llame gestión de la seguridad, ya que propone una serie de medidas administrativas que radican básicamente en registrar todas las actividades que se determinó realizar en los planes de seguridad que se han implementado, esperando que, en la medida de lo posible, todas esas actividades se realicen tal y como están descritas en el plan de contingencias, con lo cual la seguridad informática mejorará poco a poco.

Grado de madurez, se refiere a una escala de medición inicialmente desarrollada por CMMI (Capacity and Maturity Model Integrated) que consta de cinco etapas. Conforme la etapa es mayor, la empresa tiene más madurez para enfrentar los riesgos de la seguridad informática

De acuerdo con la propaganda que exhibe la propia norma, la empresa que la adopta obtiene, entre otros, los siguientes beneficios:

- Garantía independiente de los controles internos, ya que cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Garantía de que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica que los riesgos de la organización estén identificados, evaluados y gestionados en forma correcta, al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso que debe tener la alta directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al sistema de gestión de la seguridad de la Información (SGSI) elegido.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI,

liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, por especialistas en aspectos legales de las nuevas tecnologías y de leyes de confidencialidad en la protección de datos y sistemas de gestión de seguridad de la información.

Se puede obtener una certificación en SGSI mediante un proceso en el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado. Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación trienal.

› **Figura 6.4**
Información de la norma BS 25999.

La norma 27000 dentro de los estándares ISO/IEC, tiene varias páginas adicionales, desde luego, tratando el mismo tema; por ejemplo, la ISO 27000: contiene la descripción general y el vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman. La UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos", es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSI deberán ser certificados por auditores externos a las organizaciones.

Por su parte, ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles. La ISO 27003 es una guía para la implementación de un SGSI. La ISO 27004: especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados. La ISO 27005 es una guía para la administración de riesgos en la seguridad informática. La ISO 27006 especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad, y la ISO 27007 es una guía para presentarse ante una auditoría. La ISO 27000: consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.

6.8 Norma BS 25999 para la continuidad del negocio

La BS 25999 es una norma certificable en la que se tiene como objeto la gestión del plan de continuidad del negocio fundamentalmente enfocado a la disponibilidad de la información, uno de los activos más importantes en la actualidad para cualquier organización. La norma se creó ante la necesidad que tienen las organizaciones de implementar mecanismos o técnicas que minimicen los riesgos a los que están expuestas, a fin de conseguir una alta disponibilidad de las actividades de su negocio. Ésta fue desarrollada por un amplio grupo de expertos reconocidos a nivel mundial en los sectores de la industria y la administración. Constituye una actualización de normas anteriores.

La norma consiste en una serie de "recomendaciones o buenas prácticas", para facilitar la recuperación de los recursos que permiten el funcionamiento normal de un negocio, en caso de que ocurra un desastre. En este contexto, se tienen en cuenta tanto los recursos humanos como las infraestructuras, la información vital, las tecnologías de la información y los equipos que la soportan.

La norma consta de dos partes:

- La primera es un documento de orientación que proporciona las recomendaciones prácticas para la BCM (Bussines Continuity Management, o gestión de la continuidad del negocio).
- La segunda establece los requisitos para un sistema de gestión de la continuidad. Ésta es la parte de la norma que se certifica a través de una etapa de implementación, auditoría y posterior certificación.

El núcleo de esta normativa es el plan de continuidad del negocio, cuyas fases principales son:

- Evaluación e identificación de los riesgos (identificación de amenazas internas y externas).

- Análisis de impacto en el negocio. Valoración del impacto de las amenazas en el negocio.
- Desarrollo de planes para la continuidad del negocio.
- Implementación de los planes para la continuidad del negocio.
- Comunicación y formación del plan de continuidad del negocio.
- Mantenimiento y pruebas periódicas del plan de continuidad del negocio.

La BS 25999-2 es una norma británica que rápidamente se ha convertido en la principal norma para gestión de la continuidad del negocio; aunque se trata de una norma nacional británica, ya se utiliza en muchos otros países y se predice que pronto será aceptada como una norma internacional (ISO 22301).

Los siguientes son algunos de los procedimientos y documentos más importantes requeridos por la BS 25999-2:

- Alcance del SGCN: identificación precisa de la parte de la organización en la cual se aplica la gestión de la continuidad del negocio.
- Política de SGCN: definición de objetivos, responsabilidades, etcétera.
- Gestión de recursos humanos.
- Análisis de impactos en el negocio y evaluación de riesgos.
- Definición de estrategia de continuidad del negocio.
- Planes de continuidad del negocio.
- Mantenimiento de planes y sistemas.

Esta norma establece la necesidad de determinar los conocimientos y las habilidades necesarias de identificar los cursos de capacitación adecuados, de realizar dichos cursos, de verificar si los conocimientos y las habilidades requeridas se han logrado y si es necesario llevar registros. La BS 25999-2 exige la realización de programas de concienciación, además de informar a todo el personal acerca de la importancia de la gestión de la continuidad del negocio.

El análisis de impactos en el negocio se encarga de actividades importantes de la organización, pues define el periodo máximo tolerable de interrupción, la interdependencia de acciones individuales, determina qué actividades

son críticas, analiza los acuerdos existentes con proveedores y socios y establece el objetivo de tiempo de recuperación.

La evaluación de riesgos se efectúa para establecer cuáles desastres y demás interrupciones en las actividades comerciales podrían producirse y cuáles serían sus consecuencias; pero también para determinar qué vulnerabilidades y amenazas podrían llevar a esas interrupciones comerciales. Con base en una evaluación de este tipo, la organización determina cómo reducir la probabilidad de riesgos y cómo se mitigarían en caso de que se produjeran.

Las actividades de respuesta a incidentes de seguridad en la información constituyen un desafío de supervivencia para las empresas que no están preparadas para afrontarlas. Por ello, es necesario que la empresa cuente con guías, métodos, procedimientos y apoyo de recursos materiales y humanos, que garanticen que la empresa se va a recuperar del incidente de seguridad y que seguirá trabajando con normalidad en muy poco tiempo.

De acuerdo con Rigante (www.isaca.org), los incidentes informáticos más frecuentes son:

1. **Alteración, robo o daño a la información.** Cuando se tiene un incidente de este tipo, se requieren técnicas forenses para identificar no sólo quién realizó el ataque, sino para determinar cómo lo hizo. El problema es que el incidente se convierte en un asunto legal que puede afectar a la empresa, cuando muchos de sus clientes saben lo sucedido. Con frecuencia, las técnicas que utilizan los investigadores forenses difieren mucho de aquellas técnicas utilizadas por el personal interno de la empresa en sus investigaciones. Lo que interesa a la empresa es el remedio inmediato, aunque también quieren conocer la verdad, en tanto que a los investigadores forenses les interesa llegar a la verdad, sin importar el tiempo.
2. **Intrusión en el sistema de un código malicioso (virus).** Un código malicioso puede infectar con mucha rapidez a toda una red o a toda la infraestructura tecnológica de la empresa si no se le detiene a tiempo. Para ello, lo primero es definir los métodos de identificación y de entendimiento

de las intenciones y los impactos lógicos y materiales que pudiera causar en el negocio, además de comparar estos datos con los perfiles de riesgo que, por política interna, ha adoptado la empresa; esto definirá el nivel de esfuerzo que es necesario para reparar los daños que ya se sabe que va a causar. Si no se logra identificar el código malicioso, entonces la empresa está en verdaderos problemas.

3. **Ataque por personal de la empresa.** Muchas empresas creen que es imposible que algún trabajador, incluso de confianza, sea capaz de causar un incidente informático. Si llega a suceder, el primer problema es probarlo, localizar al culpable y luego enfrentar legalmente al sindicato (si el trabajador es sindicalizado) o ir a un tribunal a desahogar el caso. Para que la identificación y las pruebas sean más fáciles de obtener, las empresas deben tener políticas y procedimientos para identificar, documentar y monitorear todas las actividades de los trabajadores, limitando su acceso a ciertas áreas y determinada información. Otro problema que enfrenta la empresa es que cualquier trabajador sospechoso de realizar actividades ilícitas con la información, por lo común es suspendido en forma temporal de su cargo mientras es investigado, lo cual hace que la empresa deba ser capaz de sustituir a esa o esas personas de inmediato.

4. **Daños físicos a los equipos o al edificio con daño a los datos.** Muchas áreas de informática se enfocan sólo a la prevención de incidentes lógicos en el sistema, descuidando la parte de exposición a riesgos físicos, lo que permite que algún intruso pueda accesar con mucha facilidad a las instalaciones y robar físicamente equipos, memorias o archivos en papel. La empresa debe estar preparada para que no le afecte una pérdida de este tipo y tener los elementos necesarios para acudir a un tribunal de justicia con pruebas del robo.

5. **Negación del servicio en la red.** Este tipo de ataques suceden porque es muy sabido que van a impactar la disponibilidad de los sistemas, los cuales son una base importante para el negocio. Por tanto, es conveniente tener contactos cercanos con la empresa proveedora de servicios de Internet y

el personal capacitado y destinado a atender de inmediato este tipo de incidentes, pues ambos son claves en la identificación del atacante y en la reparación inmediata de la interrupción del servicio.

Tomar todas las medidas apropiadas declaradas en el plan general de contingencias, junto con sus tres subplanes, ha hecho que la probabilidad de incidentes informáticos sea cada día menor en muchas empresas. Por tanto, siempre debe haber pruebas periódicas de que el plan de continuidad del negocio está listo para funcionar en cualquier momento.

Actividad de aprendizaje

En el siguiente espacio elabora un mapa mental donde presentes la norma BS 2599. Compara tu mapa con el de tus compañeros.

6.9 Informática forense

La palabra *forense* proviene del latín *forero*, que significa *forastero* o *que viene de afuera.* Aplicada a la informática, constituye la rama de esta disciplina que se encarga de analizar toda la información, las intrusiones y los ataques que provienen de afuera de la empresa o de la red de cómputo donde reside originalmente la información. Por su parte, en el ámbito cotidiano, al término *forense* se le asocia con las pruebas científicas utilizadas por la policía al tratar de resolver un delito.

Como se ha visto a lo largo de este texto, la información es tan importante para las organizaciones, y en miles de ocasiones ha sido víctima de ataques e intrusiones que se consideran un delito grave, que se creó la *informática forense* con el propósito de rastrear e identificar al intruso o atacante, y así determinar la forma en que se llevó a cabo el ataque y tomar este conocimiento de base para diseñar y desarrollar cada vez mejores dispositivos que ayuden a prevenir más intrusiones y ataques dañinos a las organizaciones.

Muchas intrusiones son verdaderos delitos de orden legal, como el robo de información privilegiada, entre los que destacan los secretos tecnológicos o las patentes, y los fraudes financieros, como vaciar cuentas de usuarios de tarjetas, transferencias electrónicas fraudulentas, etcétera. En estos casos, tanto las organizaciones afectadas, como los clientes de instituciones bancarias que han sido objeto de robos de dinero vía electrónica, interponen demandas legales para encontrar a los culpables del fraude, de manera que la informática forense se erige como un gran auxiliar en la solución de conflictos de este tipo, en especial de protección de datos, privacidad de la información, robos electrónicos y espionaje industrial, entre otros conflictos. Los expertos en informática forense han auxiliado a las autoridades del orden público al desarrollar procedimientos para identificar, asegurar, extraer y analizar pruebas, y presentar evidencias científicas que demuestren la culpabilidad (o inocencia) de las personas incriminadas en el delito informático. La metodología de la informática forense sigue estrictamente el método científico en sus investigaciones.

Los pasos del método científico son los siguientes:

1. **Identificar el problema que se pretende resolver.** Ejemplo: el área de finanzas de una institución bancaria detectó un fraude electrónico mediante el cual las cuentas de cinco clientes por transferencia electrónica fueron vaciadas.
2. **Planteamiento de una hipótesis.** Una hipótesis es una suposición. De este modo, el investigador informático hace una suposición respecto al método de hackeo empleado, el sitio desde el cual se cometió el fraude, con el fin de identificar al culpable.
3. **Búsqueda de fuentes de información.** El investigador forense inicia una búsqueda con ayuda de otros trabajadores de la institución bancaria, para obtener todos los datos posibles sobre el ilícito cometido.
4. **Diseño de un procedimiento para verificar la hipótesis.** El investigador diseña un método para obtener pruebas que verifiquen (o rechacen) su hipótesis, que no necesariamente debe ser estandarizado, pues dependerá de las características del fraude, y sigue paso a paso el procedimiento hasta tener suficiente evidencia.
5. **Análisis de los datos recabados.** Puede haber muchísima información recabada durante la investigación; así que el investigador debe tener conocimientos suficientes para discernir cuál información es válida como prueba legal y cuál información no es relevante.
6. **Presentación de resultados.** El investigador presenta resultados y conclusiones, que al estar suficiente y científicamente respaldados durante toda la investigación, tienen validez legal, lo que significa que un inculpado puede ser encarcelado con base en las pruebas presentadas por el investigador.

En este ejemplo, el problema es claro.

Una institución bancaria ha sufrido un robo, por lo que debe responder al cliente por el dinero que depositó en una cuenta en esa institución bancaria. Ante esta situación, al banco le interesa encontrar al culpable, quizá no para recuperar el dinero, sino para evitar fraudes

posteriores perpetrados por la misma persona. Las pruebas que presente el investigador no pueden violar ningún derecho civil del inculpado, además de que deben estar suficientemente sustentadas como para proceder en forma legal.

En investigación científica, *pares* (peers en inglés) se refiere a otros investigadores con calidad y preparación similar a aquel que presenta la evidencia.

Los resultados de la investigación pueden presentar cuatro resultados:

- Identificar y poner en prisión al verdadero culpable.
- Identificar y poner en prisión a un inocente.
- Identificar al culpable pero queda en libertad por falta de pruebas.
- Identificar y poner en libertad a un inocente.

Como se ve a continuación, ser un investigador informático (aunque en general es un equipo interdisciplinario de expertos en informática y otras áreas) constituye un trabajo de enorme responsabilidad civil, por lo que los métodos empleados en la investigación deben ser hechos con la máxima rigurosidad científica.

La informática forense se basa en cuatro principios:

1. Toda investigación en este campo debe apegarse a estándares legales.
2. Todo investigador o grupo de investigación en informática forense debe tener una preparación rigurosa en técnicas forenses.
3. La investigación debe basarse sólo en técnicas forenses internacionalmente aceptadas.
4. Las técnicas para reunir evidencias y revisar el contenido de computadoras, servidores, etcétera, ya sea personales o de una red privada, siempre deben llevarse a cabo con un permiso escrito de los interesados.

Por otro lado, para evaluar las pruebas científicas que se presentan en un juicio legal se recurre a cuatro factores:

- Tipo de pruebas realizadas.
- Toda prueba presentada debe haber sido revisada y aprobada por pares.

- En todo resultado de una investigación siempre habrá una tasa de error, la cual se debe calcular y luego tenerse en cuenta al momento de dictar un veredicto.
- Todas las pruebas utilizadas en la investigación deben ser reconocidas y aceptadas por la comunidad científica de ese campo de estudio.

En informática forense todas las evidencias son digitales, tales como documentos (Word, Excel, etc.), archivos, fotografías, videos, e-mails, SMS, fax, bases de datos, archivos de registros de actividad (toda actividad de los e-mail se almacena en la computadora), que sean susceptibles de un tratamiento digital, y que legalmente sean evidencias válidas en un juicio. En la actualidad, todavía existe una polémica internacional acerca de la forma correcta en la que deben presentarse las evidencias digitales en un juicio, para que dichas evidencias puedan ser la base de un veredicto legal.

Hoy día, es tan complicado el tema legal, que las autoridades han optado por exigir a las empresas que en vez de presentar evidencias digitales para juicios del orden civil, sean las empresas las que están obligadas a adoptar una serie de medidas de seguridad informática, a adquirir una serie de hardware y software para prevenir ataques e intrusiones informáticas y prevenir la fuga de información confidencial tipo Wikileaks. De manera que aquellas empresas que no lo hagan, es su responsabilidad. Incluso, la ley está analizando penalizar a aquellas empresas que no adopten las medidas necesarias para preservar su seguridad informática en niveles aceptables.

Lo mínimo que se les exige es que no borren ningún archivo de almacenamiento de la actividad de cada computadora de la empresa y que conserven esa información, incluyendo los correos electrónicos (recibidos y enviados), durante al menos 10 años, para lo cual se requiere que todas las empresas elaboren políticas de administración informática en este sentido y, desde luego, que todos los empleados conozcan a la perfección esas políticas. Otra exigencia cada vez mayor es que los datos confidenciales o secretos industriales estén cifrados con claves privadas, lo cual puede dificultar su lectura y, con ello, proteger la información que contienen.

La minería de datos o exploración de datos (etapa de análisis de "Knowledge Discovery in Databases", o KDD) es un campo de las ciencias de la computación referido al proceso que intenta descubrir patrones de conducta o tendencias en grandes volúmenes de conjuntos de datos. Utiliza los métodos de la inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos. El objetivo general del proceso de minería de datos consiste en extraer información de un conjunto de datos y transformarla en una estructura comprensible para su uso posterior.

Sin embargo, un informático forense no siempre está dedicado a investigar fraudes. El investigador, en su trabajo cotidiano, también puede ayudar a las empresas a incrementar las medidas preventivas contra fraudes informáticos, auditar los procedimientos del plan de contingencia, auxiliar en el planteamiento de mejores políticas de seguridad, entre otras actividades de ayuda.

Hardware y software para la informática forense

Es evidente que una de las grandes preocupaciones de las empresas es la seguridad informática. Por ello, las empresas desarrolladoras de hardware y software han lanzado al mercado una gran cantidad de productos enfocados a ayudar a los investigadores de la informática forense a hacer mejor su trabajo. En los últimos años, con el incremento en el uso de teléfonos celulares (móviles), los delitos informáticos también se han incrementado de manera sustancial. De este hecho se puede deducir que tanto víctimas como atacantes, intrusos, asesinos, etcétera, todos tienen un teléfono móvil, por lo que muchas empresas desarrolladoras de hardware y software se han enfocado al aspecto forense de dispositivos móviles de comunicación.

A la fecha, se han desarrollado dispositivos (hardware y software juntos en el mismo equipo) creados para violar el passcode de iphones, para recuperar en forma física y digital, los datos que han sido borrados de los teléfonos móviles, para búsqueda de palabras clave en correos electrónicos, SMS y MMS, con el propósito de buscar contenidos de referencia cruzada y buscar la historia de llamadas a uno o varios números específicos, ya sea de teléfonos celulares o teléfonos fijos, por fecha y por horario de llamadas; incluso, se ha dotado a algunos dispositivos de minería de datos con interface gráfica.

Sólo como ejemplo, a continuación se describen brevemente algunos productos comerciales.

Informática forense en dispositivos móviles de comunicación

La empresa sueca Micro Systemation desarrolló el XRY, un producto para obtener evidencia digital forense en dispositivos móviles, como teléfonos, smartphones, GPS y tabletas. Es un hardware que permite conectar el dispositivo móvil a una PC, mientras el software se encarga de extraer los datos. Es posible recuperar los

datos de manera forense, lo que significa que puede utilizarse para investigaciones de delitos civiles, operaciones de inteligencia y para casos de investigación electrónica de datos. Sin embrago, extraer datos de un teléfono móvil es mucho más difícil que extraer datos de una PC normal, pues los teléfonos tienen un sistema operativo propietario que dificulta esa extracción, además de que cada día salen al mercado nuevos modelos de teléfonos móviles con software distinto o mejorado, lo que dificulta la aplicación generalizada del producto XRY. La última versión del producto incluye el poder recuperar datos de aplicaciones de smatphones que tengan Android, o dispositivos como iPhone y Blackberry.

Mobilyze es una herramienta móvil para realizar búsquedas puntuales sobre la enorme cantidad de información que se almacena cotidianamente en un teléfono móvil, información que puede ser utilizada como evidencia legal, permitiendo al usuario accesar dispositivos con iOS y Android. Basta con instalar la herramienta y conectar el Smartphone o la tableta a un puerto de USB para que Mobilyze empiece a colectar la información relevante del usuario del teléfono. La información se obtiene en minutos y puede enviarse a un laboratorio de informática forense para un mejor análisis.

El Lantern Device, por su parte, capacita al usuario para observar quién se está comunicando con quién. Se diseñó para descifrar miles de piezas de información. Cuenta con un código para proteger PC y redes, además de que puede manejar las identificaciones de los SMS, analizar las ligas (links) y actualizar constantemente el mensajero de código Kik y de código AIM; además, tiene Skype actualizado, cuenta con extracción lógica y física de datos de dispositivos con Android y con iOS, realiza extracciones lógicas vía USB y de redes con Android, es capaz de importar el registro detallado de llamadas de cualquier teléfono, realizar búsquedas de palabras clave globales y a nivel local, realizar análisis de conjuntos de hash, entre muchas otras aplicaciones.

Recuperación de archivos

Si lo que se requiere es un recuperador de archivos que lea los sectores del disco duro o de una tarjeta para buscar restos reconocibles y recupere fragmentos de archivos, existe el DiskDigger. A través de éste se localiza la unidad investigada, se selecciona el tipo de archivo y, por último, se escanea el disco o la tarjeta en busca de residuos del archivo. Es de los pocos dispositivos que puede encontrar restos de archivos en el disco duro.

Por su parte, la herramienta Test Disk repara tablas de particiones, copia archivos desde algunas particiones y recupera particiones borradas, arranques desde una copia de seguridad y archivos borrados del sistema FAT. Aunque para recuperar datos también existe el Iso Buster, que lee discos ópticos dañados que leen CD, DVD o HD-DVD y recupera la mayoría de archivos tanto de esos dispositivos de almacenamiento como de discos duros convencionales y USB.

Si se quiere escanear los archivos de la memoria caché en el buscador de la Web, se puede utilizar My Last Search, que además es capaz de localizar todas las preguntas que el usuario hizo a los buscadores más comunes, como Google y Yahoo, y a los sitios de redes sociales más populares como Twitter, Facebook y My Space. La utilidad muestra en una tabla todas las preguntas o solicitudes que se hicieron. En informática forense se dice que todo intruso o hacker siempre hace muchas preguntas y lleva a cabo muchas búsquedas antes de perpetrar algún ilícito, por lo que esta herramienta es muy utilizada.

Uno de los principios de la informática forense es que toda la metodología de investigación y análisis que se utilice en un caso deberá estar bien documentada y debe ser reproducible por cualquier otro investigador, con cierto margen de error aceptable. Sin embargo, hay muy pocas herramientas en las que los analistas forenses pueden confiar para examinar los datos encontrados en archivos de Microsoft propietario. Con mucha frecuencia, en las investigaciones de delitos se requiere la reconstrucción de toda la información que recicla el sujeto investigado, en estos casos la herramienta Rifiuti v1.0 investiga la estructura de los datos encontrados en el repositorio de reciclado de archivos. Esta palabra significa "basura" en italiano y puede trabajar en múltiples plataformas y ejecutarse en Windows, Mac OS X, Linux y plataformas BSD.

Si la investigación forense quiere buscar archivos por categorías, en vez de extensiones, o sólo sobre algunos pocos tipos de archivos, entonces se puede utilizar FI TOOLS (File Investigator Tools, o herramienta para la investigación de archivos), que investiga la mayoría de los tipos de archivos con gran precisión, y puede buscar archivos por tipo, por contenido, por la plataforma/sistema operativo, por el método de almacenamiento de los datos y por los atributos del archivo, lo que hace a través de los metadatos de los archivos.

Si un detective informático necesita buscar archivos con gran rapidez en una computadora, encontrar datos ocultos y comprobar la actividad reciente, pero no tiene las herramientas adecuadas, estas operaciones le requerirán muchísimo tiempo. OS Forensics es un conjunto de utilidades para informática forense, y para todas aquellas personas que deseen comprobar qué se ha hecho con una computadora. Esta herramienta se instala en memorias USB y cuenta con un gestor de casos. Con sus utilidades se puede buscar texto e imágenes, recopilar rastros de actividad (páginas visitadas, dispositivos conectados, contraseñas), buscar archivos borrados y disfrazados, visualizar el contenido de la memoria RAM o crear un informe del sistema.

Por último, Windows File Analyzer es una herramienta de análisis forense que procesa varios tipos de archivo, como bases de datos de miniaturas (los archivos Thumbs.db), archivos de precarga (Prefetch), documentos recientes, historial de Internet Explorer y basura de la papelera de reciclaje. Windows File Analyzer recoge información útil para quien desee averiguar más acerca de la actividad reciente de un usuario. Los análisis son rápidos y ofrecen abundante información, pero Windows File Analyzer no permite guardar los resultados como archivo ni recoge datos de otros navegadores.

Recuperación de contraseñas

Por su parte, el Browser Password Decryptor recupera contraseñas almacenadas en los navegadores web, y es compatible con Mozilla Firefox, Google Chrome y otros navegadores. La respuesta a la búsqueda la muestra en una tabla, con el navegador, la URL, el usuario y la contraseña, pudiendo exportar la tabla con todos los datos a un archivo HTML. Esta herramienta se utiliza en copias de seguridad y análisis forenses.

Pero, si lo que se quiere es conocer las contraseñas que están detrás de los asteriscos, basta tener la ventana abierta donde están los asteriscos ocultando la contraseña y ejecutar Bullets Pass View, y las contraseñas se muestran en una tabla por orden de aparición, junto con el programa asociado y el título de la ventana. Es compatible con Windows Vista y 7, aunque algunos programas resisten esta recuperación de contraseñas, como Chrome o Firefox. Otra utilidad para este fin es Wireless Key Dump, que puede extraer claves Wi-Fi almacenadas en

Windows de redes inalámbricas, incluso con esta última utilidad, se muestra el listado de puntos de acceso, su método de cifrado y la clave hexadecimal y ASCII.

Un software forense diseñado para obtener evidencias digitales en el sitio del incidente es el Chat Sniper, que analiza logs y datos que quedan después de utilizar AOL, MSM o Yahoo instant Messenger. Éste puede mostrar los nombres de los usuarios con su número de cuenta y recuperar imágenes enviadas y recibidas cuando en los correos electrónicos existe intercambio de imágenes.

Para metadatos y memoria

Si se quiere consultar los metadatos de Word (Office), como nombre, iniciales, nombre de la empresa, ruta de almacenamiento de los datos, resúmenes, revisiones y texto culto, entre otros, se puede utilizar el Metadata Analyzer, ya que esta información privada está disponible para terceras personas. Esta herramienta analiza los documentos de Office de Word, Excel y Power Point, en PDF Adobe, para prevenir divulgación accidental de esa información privada. Estos programas *insert*an la información sobre el nombre de autor(es) anterior(es), nombre de compañía(s), cantidad de veces que el documento fue guardado y otras propiedades incorporadas y personalizadas, y Metadata Analyzer advierte de la información de este tipo.

La herramienta Moon Sols Window Memory contiene lo necesario para realizar toda clase de adquisición o conversión de memoria como respuesta a cualquier incidente, o para un análisis forense para desktops de Windows, servidores o un ambiente virtualizado. Puede trabajar con archivos de hibernación de Microsoft Windows. Toda la memoria completa crash dump de Windows se diseñó como el formato de memoria física para que pueda ser analizado por Microsoft Windows Debugger, que es la mejor herramienta de Windows para análisis de la memoria física, y Moon Sols convierte todas las memorias físicas desechables de Windows en Microsoft Crash desechable, en concordancia con Microsoft Windows Debugger.

Ésta es sólo una pequeña muestra del hardware y software disponible en forma comercial de manera que un equipo de informática forense, prácticamente tiene todo lo necesario para llevar a cabo un exitoso análisis forense, identificando a los autores de fraudes, intrusiones y todo tipo de ataques informáticos. El problema es que los hackers tienen disponibles las mismas herramientas.