Gabriel Baca Urbina

Recursos en línea

Introducción a la Seguridad informática

GRUPO EDITORIAL PATRIA

Introducción a la Seguridad Informática

Gabriel Baca Urbina

Introducción a la Seguridad Informática

Gabriel Baca Urbina

PRIMERA EDICIÓN EBOOK
MÉXICO, 2016

GRUPO EDITORIAL PATRIA

Para establecer comunicación con nosotros puede hacerlo por:

correo:
Renacimiento 180, Col. San Juan Tlihuaca, Azcapotzalco, 02400, México, D.F.

fax pedidos:
(01 55) 5354 9109 • 5354 9102

e-mail:
info@patriacultural.com.mx

home page:
www.patriacultural.com.mx

Dirección editorial: Javier Enrique Callejas
Coordinadora editorial: Estela Delfín Ramírez
Supervisor de preprensa: Gerardo Briones González/Jorge A. Martínez
Diseño de portada: Juan Bernardo Rosado Solís/Signx
Ilustraciones: Adrian Zamorategui Berber
Fotografías: © Thinkstockphoto

Revisión técnica:

Karla Nathali Porras Vázquez
Universidad Autónoma de Nuevo León

Daniel Sol Llaven
Universidad Nacional Autónoma de México

Introducción a la Seguridad Informática

Renacimiento 180, Colonia San Juan Tlihuaca
Azcapotzalco, México D. F.

Miembro de la Cámara Nacional de la Industrial Editorial Mexicana
Registro Núm. 43

ISBN ebook: 978-607-744-471-8

Impreso en México
Printed in Mexico

Primera edición ebook: 2016

Dedicatoria

A Daniel, Natalia, Aranza y Gabriel, en los que cada día
se cristaliza mi futuro.

A mis maestros por estar siempre a mi lado apoyándome.

Contenido

DESCARGAR

Prefacio

Hoy día, la información no se protege y preserva sólo para que no sea dañada, sino por la importancia y el uso que ésta tiene en todos los ámbitos de la vida. El comercio internacional, las instituciones bancarias y todo tipo de empresas mantienen sus operaciones gracias a que la información fluye a través de todos sus departamentos y áreas. La información se utiliza en cualquier empresa para realizar cuatro tipos de actividades: planeación, dirección, organización y control, las cuales fueron definidas hace más de 100 años por el ingeniero francés Henry Fayol. Lo que significa que la información se preserva para llevar a cabo en forma óptima el proceso administrativo dentro de cualquier organización, de cualquier tipo de actividad y cualquier tamaño.

Incluso en la computadora personal que se tiene en casa, quienes la utilizan también realizan una o varias de esas actividades, aunque a una escala mucho menor de lo que se hace en cualquier empresa u organización. Todos, de alguna forma u otra, administramos nuestras vidas con información valiosa; desde el joven estudiante que requiere de una computadora para realizar sus tareas estudiantiles, así como para organizarlas y controlar el contenido de toda la información que cotidianamente reúne y aprende, hasta el ama de casa o el profesional que requiere de una computadora para planear sus actividades, organizarlas y controlarlas.

Es tan valiosa la información, tanto en el ámbito personal como en el de las empresas, que es considerada un activo en extremo valioso; por esta razón, siempre está expuesta a amenazas. Imaginemos, aunque sea por un momento, que somos poseedores de grandes sumas de dinero en efectivo u oro que conservamos en nuestra casa, ¿qué es lo primero que haríamos para proteger esos activos? Sin duda, lo que haríamos sería resguardarlos lo más posible, a fin de evitar un robo, por la sencilla razón de que son demasiado valiosos. Y quien los roba o sustrae obtiene un beneficio personal y daña seriamente nuestro patrimonio.

La información funciona en forma muy similar. Constituye el activo más valioso que tiene una empresa, después del activo humano, por lo que

siempre está expuesta a sufrir un robo o un daño. Al ser víctima de robo o daño de información, una empresa se ve seriamente afectada, al grado de que puede llegar a detener sus actividades por esta causa. Los riesgos a que está expuesta la información, se conocen como físicos y lógicos. Los riesgos físicos son el daño que puede sufrir el hardware y en general las instalaciones del centro o área de cómputo de la empresa. Muchos de estos daños no son intencionales, sino naturales, como terremotos o inundaciones; no obstante, muchos otros sí lo son, obviamente causados por personas maliciosas.

Por su parte, todos los riesgos lógicos conocidos han sido creados y siguen siendo creados por personas que tienen la intención de dañar o robar información de los sistemas informáticos empresariales o de las computadoras personales de un hogar. Robar secretos tecnológicos de las empresas, robar información confidencial, robar cuentas y claves bancarias para vaciar cuentas de clientes en bancos o para realizar transferencias electrónicas no autorizadas de dinero son, entre muchos otros, algunos de los riesgos lógicos más comunes.

Este texto describe con detalle no sólo los riesgos físicos y lógicos a los que están expuestos todos los sistemas informáticos empresariales y computadoras personales, sino la forma en que se puede disminuir la probabilidad de ocurrencia de tales riesgos. De igual modo, también describe los mecanismos que se han ideado para proteger de riesgos lógicos a las transacciones económicas internacionales, así como las protecciones comunes que toda empresa debe adquirir para resguardar sus datos, como los firewall y una serie de dispositivos que pueden rastrear y detectar cualquier vulnerabilidad que tenga el sistema informático, con los cuales dicha vulnerabilidad puede disminuirse. Además, también presenta el procedimiento general para realizar informática forense y auditorías informáticas.

De esta forma, el capítulo 1, **Generalidades de la seguridad informática**, aborda el porqué la información es tan valiosa para cualquier organización, los tipos de seguridad informática y los objetivos de la seguridad informática. Asimismo, describe los tipos de riesgo que existen, menciona el concepto de vulnerabilidad y de amenaza informática y explica en qué consiste la

priorización de riesgos, los umbrales de tolerancia y el uso de la información en el proceso administrativo.

En el capítulo 2, **Criptografía**, se describen los métodos que pertenecen a la criptografía clásica, así como los criptogramas clásicos más conocidos y cómo funcionan, como el cifrado de Hill, el de Vigenere y el de Playfair; además, también se hace alusión a los cambios que modificaron la forma de cifrar, como contar con mejores computadoras, el surgimiento de la teoría de la información y el estándar DES (Data Encryption Standard), y se explica en qué consiste el cifrado simétrico y asimétrico, la clave pública, las normas ISO y el algoritmo Hash.

En el capítulo 3, **Características de una PKI y de una PMI**, se hace la descripción de un certificado en general, de un certificado digital y de un certificado de identidad, y cómo se obtiene cada uno de éstos. También se describe la Norma X.509, en qué consiste una autoridad raíz de certificación, la infraestructura de clave pública y la de clave privada, la infraestructura de la administración de privilegio, qué es un atributo y qué son los atributos de autoridad, qué es la fuente de autoridad o inicio de autoridad, las políticas de emisión de certificados, las prácticas de certificación y el papel que juegan los protocolos PKI y PMI en la seguridad informática.

En el capítulo 4, **La seguridad física y lógica en redes**, se describen los riesgos físicos y lógicos en las redes y centros de cómputo, el importante papel que tiene el Uptime Institute como garante de la seguridad física de los centros de cómputo, las pruebas biométricas que existen para la protección de acceso a centros de cómputo, en qué consiste la ingeniería social, las formas de ataque a redes de cómputo y PC, como la suplantación de la dirección IP, el uso de rastreadores de redes, los ataques a servidores de la Web, la inyección SQL, el correo spam, el ataque de secuencia de comandos, el análisis de puertos, los secuestros informáticos, los virus y las medidas preventivas, así como los sistemas de prevención de intrusiones y la forma de trabajar para los ataques de un hacker.

El capítulo 5, **Firewalls como herramientas de seguridad**, explica los principales tipos de ataques informáticos, como spoofing, negación del servicio, rootkit y bootnet, phishing, hace una breve descripción del modelo OSI,

explica lo que es un firewall y cómo funciona, los tipos de firewall que existen y qué es una zona desmilitarizada; asimismo, también menciona y describe los firewall de software y de hardware y los firewall de software de última generación, y hace alusión a las limitantes y políticas de los firewall. Por último, explica cómo elegir el firewall más adecuado.

En la primera parte del capítulo 6, **Las contingencias en seguridad informática e informática forense**, se describe con cierto detalle el plan de contingencia informática con sus tres subplanes: prevención, predicción y corrección o continuidad del negocio. Se determinan los parámetros a seguir antes de elaborar los planes, se clasifican los procesos que se realizan dentro del área de informática de la empresa, incluyendo los tipos de riesgo y las consecuencias en el caso de que suceda la amenaza, y cómo se aplican estos conceptos a la elaboración de cada uno de los subplanes; por último, se describen brevemente las normas ISO 27000 y la norma BS25999. En la segunda parte de este capítulo, se aborda el tema de la **informática forense**, qué es y cuándo se utiliza, sus principios y tipos de pruebas, los procedimientos científicos que utiliza, los cuales deben ser replicables, el hardware y software disponible en el mercado para realizar la informática forense y su tratamiento en dispositivos móviles de comunicación.

Por último, en el capítulo 7, **Auditoría en seguridad informática**, se describen los tipos de auditorías que existen, entre las que destacan la Auditoría informática y, dentro de ésta, la Auditoría en seguridad informática; asimismo, también se describen las etapas de una auditoría, los requisitos que pide el ISACA para ser un auditor en informática, los criterios que se deben emplear en una auditoría, cómo se realiza una auditoría, la cual incluye el plan de auditoría, la ejecución, mantener con ética y prudencia las evidencias y opiniones, el reporte de la auditoría y las herramientas disponibles en el mercado para realizar auditorías en informática.

Adicional a la sección de preguntas y respuestas que normalmente aparece al final de cada capítulo en gran parte de los libros de texto, en esta obra se han agregado las secciones: **¿Qué sabes?** y **Actividades de aprendizaje** a lo largo de cada uno de los capítulos, con el propósito de ubicar al alumno en sus saberes actuales, a fin de que, en caso de ser necesario, dirija sus esfuerzos

iniciales de aprendizaje hacia una actualización de conocimientos. Luego, una vez actualizado, con las Actividades de aprendizaje, el estudiante puede reforzar los conceptos adquiridos a lo largo de cada capítulo.

Además, cuentas con recursos adicionales en línea, los cuales puedes consultar en: www.sali.org.mx

Quiero agradecer a todo el personal de Grupo Editorial Patria por su invaluable trabajo de apoyo; en especial a Estela Delfín, gracias a cuya asesoría y dinámismo ha sido posible la terminación y publicación de este texto.

1

Objetivo general

Que el estudiante conozca el significado y las aplicaciones de seguridad informática en las organizaciones.

Objetivos específicos

- Distinguirás los principales tipos de seguridad informática.
- Revisarás el valor de la información para las instituciones.
- Plantearás argumentos que sustenten que la información es valiosa para cualquier organización.
- Revisarás los diferentes tipos de riesgos a los que está expuesta la información en cualquier organización.

Generalidades de la seguridad informática

¿Qué sabes?

- ¿Por qué es importante la información?, ¿Cómo medir su valor? ¿Cómo distinguir a la información importante de la que no lo es? ¿Cómo cambia el valor de la información en el tiempo?
- ¿Qué es la seguridad informática?
- ¿Qué es una amenaza de seguridad informática? ¿Cómo separarlas de los demás riesgos en un sistema de información?
- ¿Qué es el umbral de tolerancia al riesgo?

Competencias a desarrollar

- Que el alumno conozca y comprenda el concepto de seguridad informática.
- Reconocer el valor que tiene la información para cualquier empresa, organización o persona.
- Comprender que la información que contiene una PC o que está almacenada en los sistemas informáticos de una empresa, siempre está expuesta a algún tipo de riesgo.

1.1 Introducción

Tres personas distintas poseen un bien muy valioso para cada una de ellas.

La primera es un estudiante que tiene una PC (computadora personal) en la que conserva almacenados documentos importantes, junto a archivos triviales como fotografías y música. Los archivos importantes para el estudiante pueden ser todas las notas y los trabajos de diferentes asignaturas que ha elaborado en la computadora a lo largo de uno o varios semestres de estudios. También puede tener archivos confidenciales del lugar donde labora y que tiene almacenados para futuras referencias, así como números de cuentas bancarias, de tarjetas de crédito o referencias de otras operaciones con instituciones bancarias, entre muchos otros más. Por lo anterior, la PC que posee esta persona es tan valiosa como el trabajo que desempeña y sus datos financieros personales, por lo que perderlos o que alguien con malas intenciones se apropie de éstos, le podría causar un perjuicio muy grave.

La segunda persona es un hombre de familia que tiene una casa donde vive con su esposa y dos hijos pequeños. Debido a su trabajo, requiere viajar de manera frecuente durante varios días, por lo que le preocupa que su hogar sea seguro para que durante todo el día, y en especial por las noches, sea prácticamente imposible que algún extraño entre a su hogar a robar o a causar un daño físico a su familia. Para esta persona (como para cualquiera que tiene una familia), el bien más valioso es su propia familia, por lo que tratará de mantenerla segura en todo momento. La información en la seguridad de la familia y en la seguridad personal, también juega un papel muy importante. Actualmente, algunos teléfonos móviles tienen una aplicación de localización, que permite conocer en tiempo real dónde se encuentra la persona portadora del teléfono; en cuanto a la seguridad en el hogar, ya existen dispositivos comerciales que permiten desde grabar lo que sucede en casa las 24 horas del día los 365 días del año, hasta la activación instantánea de alarmas conectadas a cuerpos de seguridad, en cuanto una puerta o ventana exterior de la casa son violentadas para entrar.

La tercera persona es un empresario, quien además de tener una compañía donde se elaboran productos electrónicos de tecnología intermedia, también posee un laboratorio de investigación donde se diseñan y prueban innovacio-

nes tecnológicas que propician que su empresa sea líder en su sector de mercado. También podríamos imaginar a una institución financiera encargada de manejar el dinero de personas, empresas y del propio gobierno. En este caso, tanto para el empresario como para la entidad financiera, su activo más valioso, después del activo humano, es la información que posee. Ambas entidades, banco y empresa, quizá podrían aceptar que un desastre natural como un terremoto o uno intencional como un incendio los afectara económicamente, pero jamás aceptarían perder la información que poseen. Para la empresa que realiza las investigaciones en innovación tecnológica, la información técnica que posee lo es todo, mientras que para el banco, la información referente al dinero que tiene o que debe cada uno de los miles de clientes es lo más importante. Se puede asegurar que para cualquier empresa, independientemente del sector al cual pertenezca, si llegara a perder la información importante de sus diferentes áreas, sería muy difícil que recuperara su funcionamiento normal en poco tiempo. Este tipo de eventos se trata en el capítulo 6 en el apartado "Plan de continuidad en el negocio".

Activo, desde el punto de vista de la contabilidad, se define como cualquier cosa de valor, tangible o intangible, propiedad de una empresa.

Como se puede observar en los ejemplos anteriores, todas las personas piensan en el riesgo que corren los activos más valiosos para ellos; Ya sea la familia o la información. El hecho de poseer activos o cualquier cosa valiosa implica también el riesgo de perderlos. La protección de cualquier activo contra los riesgos que tiene de sufrir cualquier tipo de daño e incluso pérdida total, tiene un costo, el cual es directamente proporcional al tipo de protección que se otorgue al activo.

En este primer capítulo se describe por qué es tan valiosa la información en diferentes ámbitos, qué o quiénes la amenazan y en qué forma y cómo se puede pensar en términos de asegurar o de dar seguridad a la información que alguien posee, ya sea una persona física o una persona moral (empresa).

1.2 El valor de la información

En 1948, Norman Wiener, matemático estadounidense, acuñó por primera vez el término *cibernética* al usarlo en el título de su libro publicado en aquel año:

Cibernética o el control y comunicación de animales y plantas. El tema fundamental de las investigaciones de Wiener era el funcionamiento fisiológico de los seres vivos en cuanto al control interno que éstos tienen para que sus funciones corporales se regulen en forma autónoma y para comunicarse con su medio circundante. Durante sus estudios, Wiener pudo darse cuenta de que hay una comunicación interna dentro del cuerpo de todo ser vivo y que la retroalimentación de la información que ese organismo percibe del interior y del exterior es lo que le otorga el autocontrol y la comunicación. Internamente, la comunicación le permite a un organismo regular sus funciones fisiológicas de manera autónoma, mientras que externamente la comunicación le permite el reaccionar ante el ambiente y otros seres vivos. La palabra *cibernética* proviene del griego *kybernites*, que significa gobernar o gobernador, Así se le llamaba incluso al timonel de un barco.

Con estas ideas, Wiener sentó las bases para el desarrollo de la teoría del control y la teoría de sistemas. Además, también descubrió que estas ideas se pueden aplicar tanto a sistemas físicos como sociales y determinó que los sistemas complejos, como los seres vivos, primero afectan y luego se adaptan a su medio ambiente; no obstante, los seres vivos logran esta adaptación con base en la información que reciben, procesan y a cuyos resultados reaccionan para adaptarse. Estas ideas de Wiener derivaron en la postulación de la Teoría de la Información durante el decenio de 1960 pues son la base del desarrollo de los lenguajes de programación y, posteriormente, de toda la informática.

Aunque tal vez la idea más brillante de Wiener radica en que fue el primero en observar una similitud entre el funcionamiento de un ser vivo y una empresa. En aquel tiempo, en Estados Unidos de América y Europa ya existían enormes y complejas organizaciones que, desde el momento de su creación, afectaban al medio ambiente en muy diversas formas, recibían y procesaban información, y reaccionaban a esa información, se adaptaban a las condiciones cambiantes del medio ambiente, social y empresarial y eventualmente crecían o desaparecían. Este "ciclo de vida" es similar al de un ser vivo.

Entonces, Wiener se preguntó: ¿qué debemos hacer con una empresa para que se adapte con mayor rapidez al ambiente empresarial y social? La respues-

ta a esta interrogante es lógica: dotarla de un sistema de información similar a aquel que poseen los seres vivos. Desde entonces han pasado más de 50 años; y hoy en día es universalmente aceptada la idea de que las empresas con buenos sistemas de información, reaccionan y se adaptan con más facilidad a los constantes cambios de un medio ambiente lleno de incertidumbre y que la información manejada por esos sistemas es muy importante para cualquier compañía.

Después de Wiener, surgieron otros investigadores que desarrollaron ideas novedosas aplicadas al mejoramiento de las funciones de las empresas, siempre inspiradas en el funcionamiento de los seres vivos, en especial en el funcionamiento fisiológico y mental del humano. Si en el humano se distinguen el sistema circulatorio, el sistema digestivo y muchos otros, que son necesarios para la vida, en las empresas podemos identificar el sistema de producción, el sistema contable, y muchos otros. Al hablar de información, en el ser humano el sistema nervioso es el encargado principal de recibir, procesar y almacenar información, así como de reaccionar ante el medio ambiente, con base en dicha información. Las funciones fisiológicas reguladas en forma autónoma en el hombre, como la respiración, la digestión, la circulación sanguínea, y demás, necesitan la información que reciben, procesan y que determina las reacciones indispensables para la vida.

En la empresa, ya sea de manufactura o de servicios, el sistema de información es el símil del sistema nervioso. Si una parte de su sistema nervioso llegara a obstruirse o a inutilizarse provocaría que funcionara mal un dedo, un brazo o una pierna, un músculo e incluso podría afectar el funcionamiento de un sistema fisiológico completo y eventualmente a todo el cuerpo.

En la empresa sucede lo mismo. Una pequeña obstrucción en el flujo de la información en cualquier área de la compañía puede afectar el funcionamiento de esa pequeña área de la empresa, un sistema completo o incluso a toda la organización.

Hay que tener presente que todos los sistemas fisiológicos del cuerpo humano están conectados por información y que la ciencia médica los ha identificado en forma separada, sólo para efectos de estudio. Lo mismo sucede en

las empresas; todos los sistemas empresariales están conectados por información, y se han separado en diferentes disciplinas, sólo para efectos de estudio.

La información es fundamental para la vida de todo ser vivo, para cualquier tipo de empresa, así como también para la sociedad en general. Por ejemplo, si se observa a cualquier animal inmediatamente después de fallecer, notaremos que su aspecto físico se encuentra íntegro; sin embargo, es la falta de información que fluye del cerebro lo que hace que sus sistemas corporales autónomos dejen de funcionar, pues ya no reciben la información vital que los hace trabajar. Ahora bien, si se observa a cualquier empresa, ya sea de manufactura o de servicios, en un día de descanso absoluto, la empresa está íntegra físicamente, pero parece muerta por falta de información, pues no hay quien ordene encender las máquinas o los equipos para empezar a dar el servicio o a producir el producto.

La información es entonces el activo más valioso de cualquier empresa, después del activo humano. El hombre genera las órdenes y la información, pero ésta necesita fluir hacia las partes ejecutoras para que las compañías cobren vida y comiencen su actividad. El problema es que esa información, tanto en los seres vivos como en las empresas, corre el riesgo de ser dañada, o su flujo puede ser obstruido, lo que da lugar a un mal funcionamiento del ser vivo o de la organización.

Por un lado, se entiende que la información es vital para el funcionamiento de cualquier empresa y, por el otro lado, que la informática es la ciencia que estudia todos los procesos que se pueden hacer sobre la información, pero con la ayuda de dispositivos automáticos. Por tanto, si queremos que una empresa siempre funcione en forma adecuada, al menos desde el punto de vista en el cual se procesa la información, es imperativo tener la certeza de que esa información está segura en cualquiera de los procesos mencionados; es decir, en la recepción, el envío, el almacenamiento y el análisis de datos, que al ser procesados se convierten en información.

Informática es la ciencia que estudia la transmisión (recepción y envío), el almacenamiento y el análisis de datos, que al ser procesados se convierten en información, realizando estos procesos con la ayuda de un dispositivo automático.

¿Por qué ingeniería en seguridad informática? La raíz de la palabra *ingeniería* provine del latín, *ingenium*, que significa *ingenio* y *creatividad*. En este sentido, es innegable el ingenio que han tenido miles de investigadores para

desarrollar toda la TIC (Tecnología Informática y de Comunicación) precisamente para preservar y optimizar toda la información que fluye a través de los dispositivos electrónicos. Pero para las empresas la información resulta tan valiosa que también hay miles de personas mal intencionadas que buscan dañar, robar e incluso destruir dicha información, y en efecto, hay quien lo ha hecho con mucho ingenio.

Pero, ¿por qué hay personas mal intencionadas que buscan dañar, robar o destruir la información de las empresas o de los usuarios de un ordenador (computadora) personal convencional? En diversos casos se presume que sólo es para demostrar que socialmente son mucho más ingeniosos y creativos que la "gente buena" que está del otro lado de la mesa. Desde luego, habrá gente maliciosa que ejecute estas acciones por dinero; por ejemplo, robar secretos tecnológicos a otras empresas para venderlos al mejor postor o a la competencia o acceder a computadoras personales para extraer números de cuentas y claves bancarias para "vaciar" cuentas personales de ahorros o a los sistemas bancarios para hacer transferencias de dinero a su favor, además de miles de acciones maliciosas más.

Por esto, la seguridad informática siempre deberá verse como un acto de ingeniería, como un acto de creatividad, aun cuando en el ámbito académico siempre estaremos del lado de los que siempre procuran que las cosas sucedan de manera ética y con principios morales de actuación en cualquier tipo de situación.

Actividad de aprendizaje

En equipo de dos o tres personas realicen un video donde presenten el símil del cuerpo humano con la empresa o la sociedad, resaltando el valor de la información. Exhiban los trabajos en clase y seleccionen los tres mejores en función de la claridad con la que transmita la idea.

1.3 Definición y tipos de seguridad informática

En esta sección se retoman aquellos personajes que poseen algo valioso y saben que corren el riesgo de perderlo en forma total o parcial; el estudiante o un trabajador de alguna empresa que necesita una PC para trabajar, el padre de familia y su hogar y el empresario y su compañía.

En el caso del estudiante o el trabajador de alguna empresa con una PC cargada de datos personales, al tomar la decisión de no prestar a nadie su PC, elimina en gran parte el riesgo que tiene de perder su información; sin embargo necesita intercambiar información con otros, tanto de la empresa como de otras personas, ya sea directamente o a través de servicios disponibles en Internet, haciéndolo vulnerable a nuevos ataques electrónicos o cibernéticos.

Por su parte, la mayor preocupación de un padre de familia es la integridad física de los suyos, por ello tiene dispuestos e instalados en su casa muchos dispositivos electrónicos y no electrónicos para protegerse de los intrusos, como cerraduras de puertas exteriores con llaves especiales, puertas exteriores blindadas, herrería en las ventanas, etcétera; ahora bien, si quiere aumentar la seguridad aún más y cuenta con los medios económicos suficientes, también puede instalar una o varias cámaras exteriores que le permitirán grabar la actividad y observar quién se acerca a su casa en forma sospechosa y a qué hora; o colocar una cámara de video y voz por si alguien llama a la puerta y antes de abrir desea saber quién es y qué desea; o también puede instalar malla electrificada alrededor de su casa para que al momento en que alguien traspase cierto límite físico e intente ingresar a su casa en forma no autorizada, se active una alarma que suene con gran intensidad o incluso esté conectada a alguna corporación policiaca o agencia de seguridad. Cada medida extra, sin duda, incrementará la inversión en seguridad, pero también le dará más certeza y seguridad de la integridad de su hogar. La inversión que cada empresa haga en seguridad informática dependerá de lo valiosa que considere la información que posee. El gasto en seguridad informática para la Bolsa de Valores de Nueva York o para el sistema de defensa de los Estados Unidos, po-

dría parecer excesivo para cualquier empresa, pero para estas dos entidades, la seguridad está primero que el dinero, sin embargo, es evidente no todas las empresas o entidades gubernamentales van a invertir en la misma proporción.

Por su parte, el empresario también enfrenta los dos tipos de riesgos señalados: el electrónico y el físico, los cuales amenazan constantemente la seguridad de la información que existe dentro de su empresa. La seguridad de la información por vía electrónica tiene muchísimas aristas, como se tratará en capítulos posteriores. En cuanto a la seguridad física, todo empresario enfrenta dos posibilidades: el riesgo externo y el interno.

En este contexto, el riesgo externo es muy similar a aquel que enfrenta el padre de familia en su hogar, se trata simplemente de permitir la entrada sólo al personal autorizado a sitios restringidos, donde se encuentra físicamente y con mayor facilidad de acceso a la información importante. Para restringir el acceso a ciertas áreas en una empresa se ha ideado una enorme cantidad de dispositivos de autenticación de personas, como huella digital, reconocimiento del iris, reconocimiento de voz, etcétera. Pero, como siempre habrá intrusos que quieran ingresar de manera ilegal a las empresas, éstas deberán instalar una serie de dispositivos como cámaras de video de 24 horas de actividad, sensores de movimiento que activen el sonido de alarmas, entre muchos otros. Cada dispositivo adicional instalado, sin duda elevará el costo de la seguridad, pero disminuirá el riesgo de que personas externas puedan ingresar sin autorización a la empresa con fines oscuros.

No obstante, las empresas enfrentan todavía un riesgo mayor: el hecho de que personal de la propia compañía sea quien robe, dañe o borre información importante; aun cuando la selección de personal y las políticas de promoción y otras sean las adecuadas al interior de la empresa, siempre existe el riesgo de que los propios trabajadores puedan, sobre todo, robar información importante, ya sea para darla a otra compañía o para venderla al mejor postor. Si la empresa sorprende a un empleado robando información, éste podrá ser denunciado y enjuiciado por las autoridades correspondientes y enfrentar un juicio que lo lleve a la cárcel; sin embargo, eso no va a hacer que se recupere la información o que alguien externo a la organización ya se haya aprovechado de ésta. Por tanto, lo mejor es evitar al máximo que suceda este hecho.

Por lo anterior, se puede definir a la seguridad informática o de la información de la siguiente manera:

> *La seguridad informática es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.*

Esta definición se puede complementar señalando que en caso de que una amenaza a la seguridad se haga efectiva, debe procurar recuperar la información dañada o robada.

Muchos investigadores y autores especializados en el tema de la seguridad informática por lo común se centran sólo en las tres características de la información mencionadas; no obstante, de acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las TI (Tecnología Informática) de la empresa (COBIT por sus siglas en inglés), las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad, cada una de las cuales se describe a continuación.

1. **Efectividad.** Se trata de lograr que la información sea en realidad la necesaria para desarrollar cualquiera de las tareas que se desarrollan en la empresa u organización y sea adecuada para realizar los procesos del negocio, proporcionándola de manera oportuna, correcta, consistente y accesible.
2. **Eficiencia.** Significa que la información sea generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin.
3. **Confidencialidad.** Se refiere a que en todas las etapas del procesamiento de la información, ésta se encuentre protegida contra accesos no autorizados, los cuales pueden derivar en la alteración o robo de información confidencial.

4. **Integridad.** Significa que la información que se recibe sea precisa y esté completa (su contenido es el necesario) para los fines que se persiguen con su procesamiento, así como con su validez, de acuerdo con los valores y las expectativas del negocio.
5. **Disponibilidad.** Hace referencia a que la información necesaria para realizar cualquiera de las etapas del proceso administrativo esté a la mano cuando sea requerida por los procesos del negocio en cualquier momento.
6. **Apego a estándares.** Significa que en el procesamiento de la información se deberán acatar leyes de uso general o reglamentos y acuerdos internos y contractuales a los cuales está sujeto el proceso de negocios.
7. **Confiabilidad.** Significa que la información no haya sido alterada inapropiadamente.

En seguridad informática, además de las características anteriores, es necesario cuidar ciertos aspectos como el control de acceso y la autenticación, aunque éstos podrían incluirse en la característica de apego a estándares.

La autenticación consiste en verificar, la identidad de un usuario o de una entidad o sitio en la red; por ejemplo, verificar que si se va a realizar una transferencia bancaria en realidad se esté ingresando al portal del banco deseado y no a algún otro sitio que trate de suplantar a dicha institución bancaria y que autorice ciertas transacciones en forma fraudulenta para su beneficio. A la fecha se han definido dos tipos de autenticación: la de origen de datos, esto es conectarse al sitio real que uno desea, y la autenticación de entidad par, lo que garantiza el establecimiento del intercambio de datos con la entidad apropiada.

Por otro lado, el *no repudio* es la capacidad que se le otorga al sistema de evitar que un usuario niegue haber efectuado determinadas acciones, como haber originado ciertos datos, haberlos recibido o haberlos enviado. Por fortuna, hoy en día, la seguridad informática ha diseñado pruebas irrefutables para evitar que esto suceda, como generar en forma automática comprobantes de que un usuario realizó cualquiera de las actividades mencionadas, mismos que permanecen en la red.

En seguridad informática se agrega una característica más a la información: privacidad, la cual es distinta de la confidencialidad. De acuerdo con la "Recomendación UIT-T X. 805" emitida por la International Telecommunication Union, la privacidad está relacionada con la protección de la asociación de la identidad de los usuarios y sus actividades, mientras que la confidencialidad se refiere a la protección contra accesos no autorizados al contenido de los datos, tal como lo señala COBIT, lo cual se logra con el cifrado de datos o siguiendo el apego a estándares respecto al control de acceso a bases de datos.

La UIT-T agrega también el concepto de seguridad en la comunicación, que significa que la información sólo se transmitirá entre los puntos extremos autorizados; es decir, es una medida para controlar el tránsito de la información a través de la red y evitar que sea desviada o interceptada.

En este texto se hace énfasis en que la seguridad informática debe preservar las siete características que menciona COBIT para la información, además de las que agrega la seguridad informática, pues al carecer de una sola de éstas, se considera que la empresa no ha mantenido la información con toda la seguridad requerida.

La forma en que se ha estructurado la seguridad tiene dos aspectos principales: las áreas y los sectores. Hay áreas de infraestructura, de servicios y de aplicaciones; cada una de las cuales es vulnerable en algunos aspectos. El área de infraestructura, que incluye todos los dispositivos para hacer transmisiones a través de la red, como los centros de conmutación, los servidores y los enrutadores, encuentra vulnerabilidad desde los mismos dispositivos de transmisiones. Por su parte, el área de servicios, que incluye todos los servicios de red, de conectividad, arrendamiento de líneas y mensajería instantánea, encuentra ciertas partes vulnerables en cada uno de estos servicios. Por último, el área de aplicaciones, empezando con el servicio de Internet, es una gran fuente de vulnerabilidad.

Ahora bien, de acuerdo con los ejemplos citados antes, los tipos de seguridad informática pueden clasificarse en: externos, internos y electrónicos, estos últimos también son llamados de seguridad lógica y son aquellos riesgos provenientes de Internet y de todos los sistemas lógicos de funcionamiento de las computadoras. El primer riesgo es que la información recibida no pro-

venga de la fuente deseada o de aquella con la que se ha intentado la conexión. Se acuñó el término *autenticar* o *autenticación*, que consiste en probar que la identidad que solicita el usuario de un servicio, de una aplicación, de un mecanismo o simplemente de otro usuario, pueda ser verificada. Esta acción de autenticación busca garantizar que una entidad no esté usurpando una identidad, o que emita una respuesta no autorizada a otra entidad que haya solicitado dicha respuesta.

Se han definido dos tipos de autenticación: la de origen de datos que se relaciona con la conexión entre redes y la autenticación de entidad par, que es la que se presenta en una asociación sin conexión. La red, por medio de sus procedimientos, debe garantizar que se establezca un intercambio de datos o de información con la entidad requerida por el usuario, y no con otra que esté suplantando a la entidad real requerida. Por lo anterior, identificar el origen de datos es fundamental en la autenticación. Los protocolos exigen primero la identificación, luego se procede a la autenticación de esa entidad y al final se autoriza la comunicación. Algunas de las recomendaciones de la UIT-T de las series F, H, J, M y X, se refieren al término *autenticación*.

Como se dijo antes, COBIT considera que una información es de calidad si posee las siete características listadas en páginas anteriores, de lo contrario se hace necesario determinar la causa por la cual la información carece de una o varias de esas características.

Luego de haber señalado el significado de cada una de esas características, a continuación se mencionan algunas causas del porqué la información podría carecer de dichas características:

1. Si la información no tiene **efectividad** se puede deber a la falta de capacitación del personal responsable al no saber con exactitud cuál es la información que se requiere para realizar cualquiera de las cuatro etapas del proceso administrativo o alguno de los procesos del negocio.
2. Si la información no es **consistente**, en la mayoría de los casos se debe a que no existe un formato establecido para recibir, procesar, almacenar o enviar información, lo que provoca que ésta pueda ser alterada o robada

total o parcialmente. Pero, la falta de formatos estandarizados no es responsabilidad del trabajador sino de los directivos, quienes muchas veces no se ocupan de elaborar dichos formatos, como seguramente tampoco se encargan de preparar un manual de procedimientos o de procesos.

3. Si la información no es **oportuna** se puede deber a que la TI disponible no es la adecuada, ya sea porque la velocidad del procesador es baja, porque el sistema está saturado y se hace lento, porque no se tiene disponible un ancho de banda suficiente para transportar cierta cantidad de información o porque el personal no está suficientemente capacitado y toma más tiempo del necesario para realizar las actividades de procesamiento de la información.

4. Si la información no es **eficiente** puede deberse a un exceso o a un déficit en los recursos humanos o de TI. Por ejemplo, un error común en las empresas es proporcionar una PC con servicio de Internet a todos los empleados que lo requieran; sin embargo, esto suele ocasionar que una parte de su tiempo laboral lo dediquen a atender asuntos personales por Internet, consultando noticias o en las redes sociales. También suele ocurrir lo opuesto; es decir, que haya pocas PC disponibles y que el personal tenga que esperar a que se desocupe el equipo para poder realizar su trabajo. En este sentido, el personal puede causar que la información no sea eficiente si hay un exceso de trabajo que genera un retraso en el procesamiento; o bien, por falta de capacitación que hace que una persona tome demasiado tiempo en realizar actividades sencillas, por ejemplo, en capturar datos.

5. Si la información no tiene confidencialidad es muy probable que se deba a que no se ha invertido lo suficiente en proteger los datos, ya sea con encriptación, transmisión segura de datos o porque no se han empleado claves de acceso eficientes para consultar la información. Desde luego, no se puede descartar el acceso o el robo de información por parte de personal mal intencionado. Obsérvese que la mayoría de las causas que provocan que la información no tenga confidencialidad se debe a una baja seguridad en la protección de la información.

6. Si la información tiene fallas de **integridad** debe buscarse el origen en la alteración inapropiada por deficiencias de diseño en los procesos del negocio. En la mayoría de los casos, la información no está íntegra o completa porque en su captura o representación en una BD no existe un procedimiento completo para mantener la información en óptimas condiciones. La información también puede perderse por ataques de malware, provenientes de Internet o por el simple intercambio de información entre dispositivos móviles, en específico las USB. Para evitar esta última posibilidad, se deben adquirir los mejores antivirus disponibles en el mercado e invertir en dispositivos confiables de respaldo de información, además de realizar esta actividad con la mayor frecuencia que sea posible.

7. Si la información no tiene **disponibilidad**, por lo común se debe a flujos lentos de información o a la pérdida de la misma, la cual debe recuperarse después. Un flujo lento de información puede ser responsabilidad de una infraestructura tecnológica con capacidad insuficiente, ya sea en velocidad de procesamiento, sistema saturado, ancho de banda de red insuficiente, etcétera, aunque también puede deberse a que han ingresado virus a los sistemas y están provocando reacciones inesperadas en su funcionamiento, como lentitud extrema en el envío de información, también puede tener su origen en que el personal poco capacitado toma más tiempo del debido, ya sea en capturar, procesar, almacenar o enviar información.

8. Si la información no se **apega a estándares** suele deberse, en muchos casos, a directivos deshonestos o ignorantes de las leyes, quienes la mayoría de las veces no se preocupan por establecer o hacer respetar las reglas internas para el manejo de la información. Por ejemplo, todo directivo debe saber que existen reglas muy estrictas para el asiento contable de la información en el pago de impuestos o en el pago de prestaciones sociales a los trabajadores, o para obtener el costo de producción, el costo unitario del producto, etcétera. Sin embargo, esta carencia puede resolverse al contratar a un contador general bien capacitado que implemente las reglas necesarias para el manejo adecuado de toda la información. Como se dijo antes, una acción que puede causar grandes problemas, sobre todo en instituciones bancarias,

es que personal interno realice transferencias de dinero indebidas a su favor o haga cargos a tarjetas de crédito de los clientes para su beneficio, con lo cual viola los estándares internos que contemplan y obligan a los empleados a comportarse con honestidad dentro de la empresa.

9. Si la información no es **confiable** es muy probable que se deba a que uno o varios procesos relacionados con el manejo de la información no estén claramente establecidos, lo que causa confusión en los empleados que administran dicha información y que se generen reportes o resultados poco confiables, o simplemente que no sea posible confiar en su autenticidad por falta de altos estándares de seguridad acerca de los datos que maneja la empresa.

En la actualidad, hay tantos tipos de seguridad informática como fuentes de amenaza existen para esa seguridad; por ello, se debe garantizar la seguridad informática tanto para los agentes externos e internos, así como para los agentes electrónicos o lógicos. Dentro de los agentes externos e internos, el factor humano juega un papel muy importante como amenaza.

Actividad de aprendizaje

Elabora un mapa mental donde expliques la definición de seguridad informática. Comparte tu trabajo con tus compañeros para llegar a un mapa mental que contemple los elementos valiosos aportados por todos.

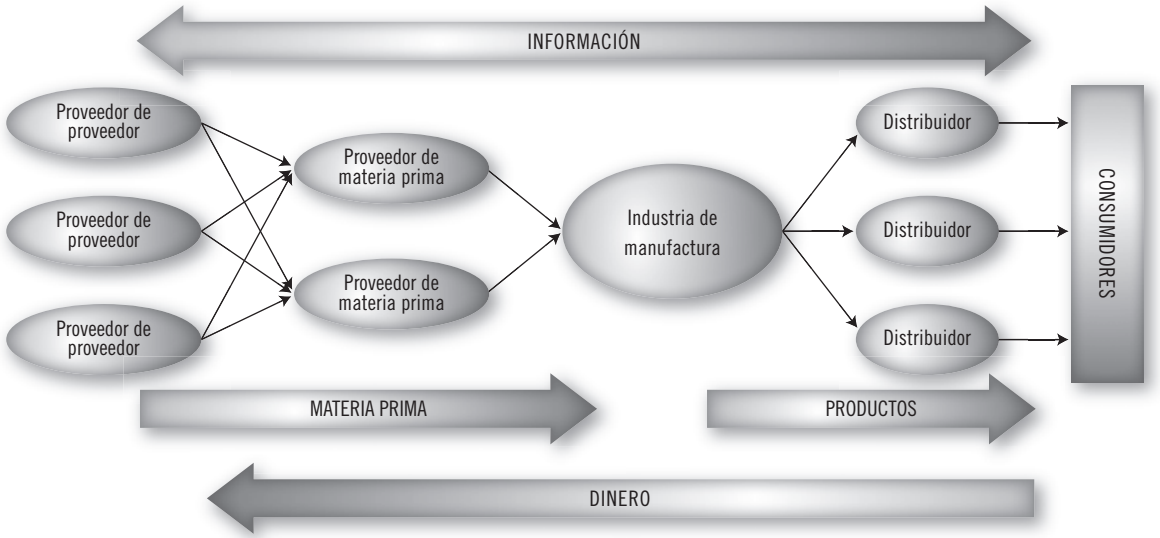
1.4 Objetivos de la seguridad informática

El objetivo de la seguridad informática no consiste sólo en preservar las siete características que señala COBIT. Si se quiere que siempre se mantengan esas características, entonces deberá formularse un plan para prevenir los principales tipos de ataque interno, externo, físico o electrónico sobre la información. Además, en caso de que llegara a suceder cualquier daño a la información, ya sea alteración o robo, también se debe contar con planes para la recuperación de esa información en su totalidad. Los planes de recuperación y el plan de contingencias se tratan en el capítulo 6. No todos los planes de recuperación de la información o del negocio tienen el mismo costo, el cual depende del daño que haya sufrido la información, incluyendo pérdida total, y de la clase de plan que haya sido aceptado por la alta dirección.

En este sentido, se hace indispensable que todo personal del área de informática dentro de una organización esté consciente de cuál es el objetivo final de la seguridad de los sistemas de información. Como se dijo antes, la diferencia entre un día de descanso y un día laboral, en una empresa de manufactura o de servicio, es que en los días laborables la información que fluye es lo que le da vida a la compañía.

Tómese como ejemplo a una empresa de manufactura donde existe el concepto llamado "cadena de suministros", que se muestra de forma esquemática en la figura 1.1.

Es interesante observar que toda empresa, de manufactura o de servicios, sólo tiene como objetivo satisfacer a sus clientes; sin ellos, la compañía no existiría. En la figura 1.1 se muestra que la materia prima fluye hacia la empresa y de ahí sale en forma de producto terminado para ser entregado a los consumidores finales, quienes pagan por el producto o servicio recibido. De manera que el dinero fluye en sentido inverso al que fluyen las materias primas y el producto, haciendo que ese dinero sea suficiente para pagar a los distribuidores del producto, a todos los empleados de la empresa de manufactura, a los proveedores de materia prima, y que además la empresa tenga una



› **Figura 1.1**
Cadena de suministros en una empresa de manufactura.

ganancia después de haber pagado impuestos al gobierno. Pero, lo más interesante de la figura 1.1 es que es posible ver cómo la información fluye a lo largo de toda la cadena en ambos sentidos.

Imagínese por un momento lo que pasaría si el flujo de la información se interrumpe en alguna parte de esa cadena y en cualquier sentido. La empresa podría no saber qué debe producir, cuánto, ni a quién hay que entregarle el producto, o cuánto le debe a cada proveedor, a cada empleado o cuánto hay que cobrar a cada punto de venta a la que ya ha entregado producto. Sin información la empresa no puede funcionar.

El trabajador del área de informática también debe saber que la empresa se administra realizando cuatro actividades básicas:

1. **Planeación.** Consiste en planear actividades futuras con base en datos históricos, no sólo de la empresa, sino también del área de informática, y en específico del área de seguridad informática: ¿cuántos ataques y desastres ha tenido la empresa sobre su información?, ¿de qué tipo han sido los ataques?, ¿con qué frecuencia han ocurrido?, ¿quién los ha perpetrado? Lo que haga la empresa para evitar a corto y largo plazos que esto vuelva a suceder se llama planeación, y la base para hacer una correcta planeación es la información histórica que se tenga.

2. **Dirección.** Se refiere a tomar decisiones concretas acerca de una serie de actividades alternativas que se tienen para realizar en el futuro inmediato. Después de que la empresa ha sufrido una serie de ataques y desastres sobre su información, en general los altos directivos toman la decisión de incrementar las medidas de seguridad, lo cual implica un alto costo. Pero, esta decisión siempre debe tomarse considerando los datos que se tienen de las pérdidas sufridas por los ataques informáticos y en el dinero disponible que tiene la empresa para incrementar la seguridad; no obstante, en general las decisiones de la dirección de la empresa se toman con base en información disponible.

3. **Organización.** Consiste en determinar ya sea el sitio más apropiado para colocar objetos, contratar más personal, determinar la secuencia óptima de actividades o determinar el orden de ideas más apropiado para lograr un objetivo. Para ello, se toma como base el estado actual del área de seguridad informática, se determina a qué nivel se quiere llegar y se organizan actividades entre el personal, así como la secuencia en que se llevarán a cabo las nuevas medidas de seguridad informática. Sólo se puede planear y establecer una organización si se cuenta con la información suficiente para ello.

4. **Control.** Se refiere a determinar parámetros que indiquen si ciertas actividades se están realizando conforme a un plan establecido con antelación. Supóngase que se elaboró un plan para incrementar la seguridad informática, se tomó la decisión de invertir cierta cantidad de dinero, se organizó y se implementó todo el plan, ahora es el momento de evaluar (controlar) si las nuevas medidas de seguridad informática están funcionando como se esperaba. Esta evaluación y control se hace con datos de antes y después. Como se dijo antes, sólo es posible llevar un buen control de actividades dentro de la empresa con información suficiente.

La seguridad informática tiene sentido cuando se sabe para qué se quieren preservar las características de la información; por ello es importante realizar en forma adecuada los cuatro pasos o etapas del proceso administrativo, así la

cadena de suministros funcionará en forma óptima, ya sea que se trate de una empresa de manufactura o de servicios. Si esta cadena funciona de la mejor manera posible, la empresa tendrá muchas más posibilidades de sobrevivir en un ambiente de mercado cada vez más competitivo. Todo esto se puede cumplir si se preservan siempre las siete características que debe tener la información mediante una seguridad informática adecuada y eficiente.

Aunado a lo anterior, hay que destacar que el objetivo de la seguridad informática es identificar las amenazas a las cuales está expuesta la información, minimizar los riesgos de esa exposición, gestionar la adecuada utilización de las TIC que tiene la empresa, garantizar que en caso de un desastre informático se tenga una recuperación del negocio inmediata e integral, y cumplir con el marco legal que se exige por el manejo de datos personales y empresariales de los clientes y socios de la empresa.

Actividad de aprendizaje

Elabora un esquema donde muestres las cuatro etapas que utilizan las empresas para su administración y en el que expliques qué papel juega la seguridad informática en cada una de estas etapas.

1.5 Análisis de riesgos

En términos generales, el riesgo se define como la posibilidad de que no se obtengan los resultados deseados. En informática, las empresas nunca desean sufrir un ataque externo o interno a sus sistemas de información, pero los ataques siempre suceden, de manera que esa posibilidad o probabilidad se materializa. La empresa siempre está amenazada de sufrir algún daño en su sistema informático, daño que puede provocar pérdidas de muchos tipos, y las amenazas son mayores cuando los sistemas de información presentan ciertos puntos débiles llamados "vulnerabilidades", de manera que se tiene mayor o menor riesgo dependiendo de la cantidad y número de vulnerabilidades que se tengan.

Las cuatro etapas del proceso administrativo (planeación, dirección, organización y control) siempre deben ejecutarse en el área de seguridad informática. Lo peor que puede hacer una empresa es ir agregando parches sobre los desastres que ya sucedieron con la información. Lo ideal es evitar riesgos mediante una buena planeación en seguridad informática, pues desde esta temprana etapa del proceso administrativo ya existen riesgos inminentes. Dicha planeación implica identificar las vulnerabilidades y medir el daño que pueden causar, de manera que al disminuir las vulnerabilidades, también disminuirá el riesgo de sufrir daños, no sólo en el aspecto informático, sino en toda la empresa.

Antiguamente, se tenía la noción de riesgo durante la planeación de un proyecto de seguridad informática después de verificar que los resultados no eran los que se habían planeado; por ejemplo, cuando fallaban el tiempo de ejecución, el presupuesto, la gente, el funcionamiento del hardware o del software, o cuando la seguridad informática presentaba deficiencias, entre muchas otras cosas más. En estos casos, lo primero que saltaba a la mente de los ejecutores de proyectos de seguridad informática era que las fallas podían provenir de distintas formas y fuentes, por lo que de las primeras cosas que tenían que hacer era i*dentificar los diferentes tipos y fuentes de riesgo.*

Aunque esta identificación de los riesgos constituía un avance, resolvía muy poco, pues se conocía poco de los riesgos. Por tanto, el siguiente paso

fue analizar los riesgos; conocer su origen, la magnitud en daño y el costo en caso de que el riesgo llegara a suceder. En este punto, los ejecutores de proyectos se dieron cuenta de que existen diferentes magnitudes de riesgos; esto es, hay riesgos que suceden y afectan al proyecto de manera imperceptible, hay otros que son lo contrario; es decir, suceden y pueden desviar al proyecto de su concepción original; y hay otros que suceden y ocasionan un costo muy elevado al reparar el daño. Además, también se observó que hay riesgos que existen, pero tienen muy poca posibilidad de ocurrir, en tanto que hay otros que ocurren con cierta frecuencia pero son innocuos, es decir, no dañinos.

La planeación de la seguridad informática no sólo consiste en identificar vulnerabilidades, medir impactos y disminuir el riesgo de que sucedan; también implica considerar los costos y, en ocasiones, hasta modificar el aparato administrativo.

Estas tres etapas (identificación, análisis y medidas para evitar y mitigar los efectos de los riesgos) constituyen la base de la llamada administración de riesgos en *proyectos de seguridad informática,* aunque con el paso del tiempo y la experiencia adquirida en la ejecución de miles de proyectos de este tipo, la administración de riesgos ha ido más allá de estas etapas iniciales básicas.

Una buena administración permite, entre otras cosas, gestionar en forma apropiada los riesgos y las oportunidades relacionadas con la seguridad informática. Hoy día, existen diferentes tipos de riesgos con diferentes orígenes, por lo que a continuación revisamos algunos de los más comunes.

Riesgos tecnológicos

Los *riesgos de origen tecnológico;* suelen ser cometidos por usuarios con muy poca experiencia, quienes no miden la magnitud de las consecuencias. En un proyecto de seguridad informática puede haber un cambio o ajuste en la organización de la empresa y en las normas tecnológicas. En este sentido, se consideran dos tipos de arquitectura: la de la organización y la tecnológica. La arquitectura de la organización es la nueva estructura organizacional que normalmente se genera como consecuencia del uso de un cambio profundo en la seguridad informática, que a su vez conlleva un cambio en los procesos; este tipo de arquitectura debe ser modificada con respecto a la estructura

organizacional que se tenía antes de implantar los nuevos protocolos lógicos y administrativos de seguridad informática. No obstante, si esta estructura no está bien diseñada y adaptada para el cambio, el riesgo de fracaso en la implantación de las nuevas medidas de seguridad es muy elevado, y lo mismo sucede con la arquitectura de la seguridad informática propiamente dicha.

Pero la implantación de nuevos procesos y tecnología en seguridad informática en una organización no se logra en poco tiempo, el cambio puede requerir meses para consolidarse. Mientras tanto, las interfaces entre el nuevo y el antiguo sistema de seguridad deben funcionar de manera eficiente, pues toda la experiencia en el manejo de procesos del sistema anterior deberá transmitirse y adaptarse de manera paulatina a las nuevas condiciones de trabajo que implican el uso de nuevas medidas de seguridad. En este contexto, el riesgo de fracaso es por no lograr la implementación o un retraso significativo en la implementación, pues los trabajadores siempre se resisten a los cambios.

El proyecto de seguridad informática debe estar alineado, lo que significa que debe contribuir, en lo particular, al logro de los objetivos del área de seguridad informática y, en lo general, al cumplimiento de los objetivos de toda la empresa. Si el proyecto no está alineado con la arquitectura o los estándares técnicos, entonces el nuevo sistema de seguridad no está contribuyendo a la implantación del proyecto, ni al progreso apropiado de la organización, por lo que se convierten más en un obstáculo que en un apoyo.

La elaboración de un proyecto y llevarlo a la práctica implica elaborar una serie de actividades que contemplen todas las facetas de dicho proyecto: la calidad de los planes, las previsiones del proyecto, los trabajos que se van a realizar y las técnicas que se van a emplear. Si éstas no son claras, completas y razonables, entonces se corre el riesgo de que el personal no sepa cómo actuar de manera adecuada ante cualquier contingencia, debido a que no habrá entendido con exactitud qué es lo que tiene que hacer ni qué se espera de él.

Quien ejecuta un proyecto de seguridad informática, ya sea que se trate de personal externo o de la propia empresa, debe comprometerse a entregar todos los procesos y medidas de seguridad que se van a implantar por escrito en un documento, el cual se conoce como "entregable". Si el entregable se encuentra en las primeras fases del proyecto y es poco claro y no se desarrolla

bajo especificaciones de calidad, con toda seguridad afectará todas las actividades que siguen en el proyecto.

Una de las partes de un proyecto de seguridad informática debe determinar no sólo los recursos económicos necesarios, sino también cuáles serán los costos de operación y las ganancias o ahorros probables que generará el proyecto en los años futuros. Por ejemplo, si se asignan menores recursos se corre el riesgo de no terminarlo en tiempo, de contratar personal de menor capacidad técnica o de adquirir tecnología no adecuada o con capacidad insuficiente para el desarrollo del proyecto, lo que puede causar problemas serios a la empresa. En cambio, si se asignan recursos mayores a los estrictamente necesarios, es probable que se adquieran equipos muy sobrados en capacidad o en aplicaciones, lo que puede provocar que la empresa pierda dinero y tenga una inversión en seguridad informática parcialmente ociosa.

Otra de las etapas del proceso administrativo que se debe planear correctamente son los mecanismos de control de riesgo. Sin los mecanismos de monitoreo y control de riesgo inofensivos, se incrementa la probabilidad de que ocurra un determinado riesgo, pues es más difícil saber si ese riesgo está progresando. Por el contrario, también puede suceder que se definan mecanismos de monitoreo y control muy estrictos para riesgos inocuos y de baja probabilidad de ocurrencia, con lo cual la organización perderá recursos económicos. Por tanto, debe existir la certeza de lo que se espera del proyecto de seguridad en términos del porcentaje de disminución o eliminación total de los riesgos actuales.

Todo proyecto implica el consumo de recursos para obtener ciertos beneficios, en este caso de eliminación o disminución de riesgos de seguridad informática, lo que a su vez también implica un dominio de las técnicas establecidas para el logro de ese fin; pero, si no se cuenta con el personal capacitado para determinar con precisión cuáles beneficios arrojará el proyecto, se corre el riesgo de desalentar a la alta dirección en la aprobación del proyecto e incluso desecharlo, cuando en realidad pudo haber sido una buena oportunidad de mejora.

Uno de los más grandes riesgos en los proyectos de seguridad informática, sin duda es la poca participación de los directivos de la organización. Como

se dijo antes, todo tipo de proyectos, no sólo los informáticos, necesitan de una participación fuerte y activa por parte de los directivos de la organización, pues de lo contrario el personal percibe que el proyecto no es tan importante como ellos pensaban y también empiezan a dedicar menos atención a los resultados del mismo. Si esta condición no se tiene desde el principio del proyecto, el riesgo de problemas es muy alto. La alta dirección debe tener el compromiso formal de apoyar al proyecto en los aspectos que le corresponden.

Otro aspecto de gran importancia es contar con el personal capacitado para la elaboración del proyecto. No puede haber buenos resultados si se siguen planes mal trazados, por ello es necesario seguir la metodología de manera puntual y esto sólo se logra si el personal que aplica cada una de las técnicas de dicha metodología está bien capacitado. Si bien es cierto que en muchos proyectos las técnicas de la metodología no pueden aplicarse de manera tan rígida, también queda claro que hay que hacer una serie de consideraciones de acuerdo con las características del proyecto, y este tipo de consideraciones sólo las puede aplicar el personal que no sólo está bien capacitado sino que cuenta con la experiencia necesaria en la elaboración de proyectos similares.

Sin lugar a dudas, un plan para adoptar sistemas de seguridad más estrictos puede generar un cambio organizacional necesario. En este sentido, el rediseño de los mecanismos y procesos para mejorar la seguridad informática puede ser de menor a gran escala. Pero, si el cambio organizacional no cambia acorde al cambio en los procesos y en el uso del nuevo esquema de seguridad, la implementación y operación del proyecto está destinada al fracaso, pues la organización no tendrá los elementos suficientes para asimilar el cambio. Por ende, todo el personal de la organización debe tener perfectamente claro todos aquellos aspectos que van a cambiar y la forma en que van a cambiar los procesos con la implementación del proyecto de seguridad informática. Si no hay suficiente claridad en estos cambios no se pueden esperar buenos resultados, lo cual implica un riesgo.

En la descripción de estos riesgos y sus orígenes claramente se observa la preocupación de que el cambio organizacional se efectúe de la mejor forma posible para la empresa y sus empleados. Es muy probable que muchos de los fracasos que se han dado en proyectos de seguridad informática se hayan

debido a la baja calidad en la administración o gestión de ese cambio que debe tener la organización, que de no producirse de manera adecuada conduce al fracaso y a una pérdida de dinero que puede ser considerable. Una cosa es identificar y hacer un muy buen plan para la gestión del cambio y otra cosa muy distinta es que la organización realice el cambio de manera adecuada, siempre que tenga la capacidad para hacerlo. De lo contrario, también se debe prever la capacitación, una necesidad que suelen tener todas las empresas.

La medición de resultados (indicadores de desempeño) se ha convertido en un factor fundamental en la práctica de la seguridad informática, por lo que a la fecha se han desarrollado indicadores de todo tipo, los cuales se incluyen dentro de las áreas de monitoreo y control. Es inaceptable haber invertido una buena cantidad de recursos en un proyecto de seguridad informática, para que una vez implementado éste no sea capaz de medir si se están logrando los resultados esperados.

Riesgos externos

El riesgo externo más simple se relaciona con la falta de recursos económicos internos en la organización, ante lo cual lo más común es solicitar un financiamiento para la realización del proyecto. Un vez que se han conseguido los recursos necesarios provenientes del exterior, entonces existirá un proveedor externo de capital, quien también, en algún momento, puede constituir un factor que retrase la entrega de los recursos por razones ajenas a la empresa.

Otro riesgo externo importante se relaciona con aquellos factores fuera del control de los equipos de proyecto. Obsérvese que se hace énfasis en la aseveración: fuera del control de los equipos del proyecto, lo cual no exime a los directivos de la organización. Estos factores pueden ser una avería en instalaciones mal hechas, incendios parciales, descomposturas en los equipos de trabajo, huelgas, etcétera; esto es, aquellos factores sobre los cuales los equipos de trabajo no tienen control, pero sí los directivos, quienes en ciertos casos tienen el control sobre algunos de estos factores, en el sentido de que la mayoría de éstos depende de la forma en que es administrada la organización. Si ocurriera cualquiera de esos eventos, se retrasaría el proyecto con consecuencias económicas considerables.

Dependencia de factores macroeconómicos que pueden afectar al proyecto

Además de los riesgos externos citados antes, existen otros factores, también externos, que ni siquiera la alta dirección de una empresa puede evitar; tal es el caso de las crisis económicas mundiales, como la ocurrida en 2007-2008, cuyos efectos se prolongaron más allá de ese par de años, lo que provocó serias afectaciones a muchas organizaciones y, por ende, a muchos más proyectos. No obstante, la ocurrencia de estos factores es inevitable y en ocasiones impredecible.

Algunos de estos riesgos no son cuantificables, por lo que su estimación resulta muy complicada. Se sabe que existen y que de llegar a ocurrir causarían retraso y pérdidas económicas en el desarrollo del proyecto. Por esta razón, es mejor aprender a administrar el riesgo a partir del momento en que el proyecto de implementación se ha generado, para que una vez que se haya implantado, se aprenda a administrarlo.

Recordemos que es mejor ser proactivo que reactivo o correctivo, por eso debe generarse una estrategia de administración del riesgo del proyecto, antes de iniciarlo. Las actividades de administración de riesgos incluyen, en primer lugar, identificar la fuente de riesgos, que como se observa en la lista anterior, se pueden atribuir desde el involucramiento de los altos directivos, hasta la contratación de personal poco especializado.

Dentro de cada uno de estos orígenes se generan a su vez más riesgos relacionados con la fuente principal del riesgo, la cual, como se observa, puede ser una fuente tanto interna como externa a la empresa. El problema de muchas organizaciones es que acostumbran esperar a que no ocurran los riesgos; por ello, cuando suceden, suelen afectar el desarrollo del proyecto, la implementación y la operación del nuevo esquema de seguridad informática en algún grado.

Vulnerabilidades y amenazas: causas y tipos

Amenazas

Se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se

produjese una violación de seguridad (no cumplimiento de alguno de los aspectos mencionados), afectando parte de la información y de la TI de la organización.

Cuando la información, la TI o cualquier otro tipo de activo es víctima de una amenaza, éstos no se ven afectados en todas sus dimensiones ni en la misma cuantía. Por tanto, una vez determinado que una amenaza podría perjudicar a un activo, hay que estimar cuán vulnerable es dicho activo en dos sentidos: 1) degradación, que significa cuán perjudicado resultaría el activo, y todo activo dañado tiene un costo en su reparación o reposición y 2) frecuencia, que significa cada cuándo se materializa la amenaza. Luego, habrá que determinar en qué consisten las amenazas que pueden afectar a cada activo de la empresa y causar un daño considerable.

De acuerdo con la recomendación UIT-T X. 800, una amenaza de seguridad constituye una violación potencial de la seguridad. Es potencial porque existe la probabilidad de que se genere un cambio intencional, pero no autorizado, del estado del sistema. Aunque también se considera una amenaza a la seguridad cuando es posible que haya una fuga de información, por supuesto no autorizada, pero no se modifica el estado del sistema, y simplemente se extraen datos importantes, como contraseñas, con el fin de realizar movimientos bancarios, como transferencias electrónicas de dinero.

Vulnerabilidad

Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza. En la actualidad se contempla que hay ataques intencionados y no intencionados, mismos a los que la empresa siempre es vulnerable, en mayor o menor medida. Cuando existe una vulnerabilidad en la seguridad informática, en general ésta se considera como un defecto de diseño, en la implementación del sistema o en su funcionamiento. La primera vulnerabilidad que puede suceder es que los diseñadores del sistema no sean capaces de prever todas las amenazas que existen o que pueden existir en el futuro, y como es imposible predecir el futuro, los sistemas siempre serán vulnerables. Otra vulnerabilidad, consecuencia de la anterior, es un

mal diseño del protocolo, que en su momento parece ser lo suficientemente seguro; sin embargo, al ponerlo en práctica, se descubren ciertas debilidades que no eran tan evidentes al momento de su diseño, aun cuando se supone que los organismos de normalización tienen la capacidad y la responsabilidad para tratar de manera adecuada todo lo relacionado con la seguridad de los protocolos, su implementación, configuración y funcionamiento.

Ataques no intencionados

Un ataque no intencionado es cuando un hecho perjudica a la información, a la TI o a la empresa sin que ocurra por las acciones intencionales de alguien. Por ejemplo, un incendio accidental, una inundación debida al mal tiempo, la falla de suministro de energía eléctrica por la caída de un rayo, una falla en un satélite de comunicación, errores o equivocaciones de usuarios, entre muchos otros.

Ataques intencionados

Se consideran ataques intencionados los accesos no autorizados al sistema, donde el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, con el fin de robar información o alterar registros o los emplea con fines inapropiados aun cuando tiene autorización para usarlos. Por ejemplo, un ataque destructivo puede tomar la forma de vandalismo, terrorismo, etcétera; realiza registros alterados para beneficiar a personal ajeno a la empresa o perjudicar a la propia empresa.

Todos los ataques lógicos a los sistemas de información que suelen provenir del exterior de la empresa son ataques intencionados, aunque algunos ataques no intencionados pueden provenir del interior de la propia empresa por la interacción entre sistemas. Los hackers, crackers, sniffers, spammers, samurái, piratas informáticos, creadores de virus, entre otros, actúan en general con la intención de demostrar públicamente su habilidad violando sistemas en apariencia seguros.

Otros ataques intencionados pueden provenir del interior de la propia empresa; son causados por empleados descontentos, ingenuos o con conocimiento insuficiente, ya que sobre estos últimos se aplica la ingeniería social, para explotar su vulnerabilidad en un ataque.

Administración de riesgo

A pesar de lo bien planeados que puedan resultar los ataques intencionados, éstos se pueden prevenir con ciertos procedimientos o mecanismos tecnológicos que reducen el riesgo. En este sentido, hay amenazas que se anulan simplemente con una organización adecuada, mientras que otras requieren de elementos técnicos (programas o equipos), seguridad física y de política de personal.

Antes de tomar cualquier medida preventiva o correctiva, habrá que plantearse las siguientes preguntas:

- ¿Cuánto se vería afectada la empresa si el activo (información o TI) no estuviera disponible?
- ¿Cuánto le afectaría a la empresa que el activo fuera modificado?
- ¿Qué importancia tendría para la empresa que gente externa a ésta conociera información contenida en bases de datos o en cualquier otro tipo de almacenamiento de datos?
- ¿Qué importancia tiene para la empresa que quien accede a información de la compañía en realidad no fuera quien dice ser?

La respuesta a estas preguntas se conceptualiza como el costo que tiene el que sucedan las amenazas, además de que constituye la magnitud del daño producido cuando la amenaza llega a suceder.

Por tanto, se recomienda que para incrementar la seguridad informática al interior de la nueva organización exista un área de Administración de riesgos, cuyo propósito principal es identificar los problemas potenciales antes de que ocurran para planear las actividades dirigidas a mitigar los impactos adversos que tengan estos riesgos sobre el logro de los objetivos durante toda la operación del nuevo sistema de seguridad informática.

Normalmente una modificación mal intencionada de la información en cualquier empresa, repercute negativamente, lo que trae como consecuencia un costo para recuperar la información original.

La administración de riesgos entonces está orientada a que no se afecten los objetivos de la empresa. Busca la participación abierta de todo el personal involucrado en la operación y aplicación de medidas de seguridad. Considera que si los riesgos se identifican desde el inicio del proyecto e inmediatamente

después de la implementación y la operación, éstos serán menos costosos y harán menos daño a la empresa que si se detectan más tarde. Por tanto, el enfoque debe ser proactivo más que correctivo.

La administración del riesgo se puede dividir en tres etapas:

1. Identificar y analizar o caracterizar el riesgo.
2. Definir una estrategia para administrar el riesgo.
3. Implementar planes de mitigación de efectos adversos cuando sea necesario.

La estrategia de administración de riesgos consiste básicamente en un plan que declara las acciones y el enfoque que se debe aplicar para controlar el riesgo. Dentro de estas acciones se encuentra identificar el origen del riesgo, que puede ser interno o externo al proyecto de la empresa. Esta identificación se debe hacer durante toda la operación de los sistemas de seguridad, pues conforme transcurre el tiempo, pueden surgir más riesgos cuyo origen proviene de diferentes fuentes. Desde luego, la identificación incluye delimitar con claridad las características de los riesgos detectados, magnitud, probabilidad de ocurrencia y grado de afectación a la operación de la empresa en caso de ocurrir, entre otras características.

Inicialmente se debe obtener, no sólo en el proyecto sino en su implantación y operación, una lista del origen (interno o externo) de los riesgos y una lista de las características de los riesgos detectados. La obligación de obtener estas dos listas lleva directamente a las actividades que han de realizarse, lo cual incluye buscar el origen de los riesgos en los requerimientos del proyecto y operación que tengan poca precisión, diseños poco factibles, tecnología no disponible, estimación de la programación del proyecto y estándares de operación poco realista, capacidad insuficiente de algunos participantes, financiamiento del proyecto, entre otras.

Después viene el trabajo consistente en caracterizar los riesgos, que incluye, ante todo, determinar los parámetros que definirán esas características,

las cuales son la probabilidad de ocurrencia, la consecuencia del riesgo y el valor mínimo que debe presentar el riesgo para poder iniciar actividades o para evitar o mitigar ese riesgo. En el caso de la probabilidad de ocurrencia, es infructuoso asignar valores numéricos a estas probabilidades, por lo que se ha optado por utilizar una escala ordinal como: riesgo improbable, riesgo poco probable, riesgo muy probable y certeza absoluta de que ocurrirá el riesgo. Con respecto a las consecuencias del riesgo, es imposible expresar dichas consecuencias en términos monetarios, por lo que se ha optado por la misma escala ordinal en términos tales como: consecuencia baja, media, alta, despreciable, significativa, crítica y catastrófica.

Estos tres parámetros, y sus límites máximos o mínimos, capacitan a quien toma las decisiones para administrar el riesgo y para comparar en forma adecuada los diferentes tipos de riesgo, ya que si se conocen con cierta precisión será más sencillo manejarlos. Al concluir estas determinaciones, se debe 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 a los más inocuos. En esta parte aún sigue vigente la determinación de los umbrales de cada riesgo a fin de iniciar 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 sea inminente que sucedan.

Dentro de la estrategia también es necesario considerar las diferentes técnicas de mitigación, como la simulación o los diseños alternativos de los procesos de la empresa. En tanto, para monitorear los riesgos habrá que definir los intervalos en que se debe monitorear y reevaluar el estatus del riesgo y comunicar en forma constante los resultados del monitoreo a la alta gerencia, a fin de tomar las decisiones necesarias de común acuerdo. Un plan de mitigación incluye métodos para evitar, reducir y controlar la probabilidad de ocurrencia, como el plan de mitigación que ha declarado límites máximos o mínimos que debe tomar el riesgo para empezar a actuar y hacer que éste regrese a niveles normales de tolerancia o de niveles de aceptación del riesgo, en los cuales se

supone que éste está bajo control. Desde luego que si se está elaborando una estrategia, ésta debe contener los puntos mencionados.

Pero, una estrategia de administración de riesgos no sólo debe incluir las actividades mencionadas, sino también aquellos métodos y herramientas que se van a utilizar para realizarlas, pues no sólo se trata de identificar, analizar y contar con planes para mitigar los riesgos, sino también de monitorear la evolución de los riesgos a lo largo de toda la operación de los sistemas de seguridad informática y de la forma en que esta evolución se irá comunicando a todos los participantes del sistema de seguridad. Después de determinar el intervalo de monitoreo, se hace una lectura del estatus y se compara la lectura contra los límites máximos o mínimos establecidos, para realizar las actividades de mitigación. Desde luego, en la estrategia se debe plantear que la frecuencia de monitoreo será mayor para los riesgos de más alta probabilidad de ocurrencia y más dañinos.

Debe quedar claro que la elaboración de la estrategia debe hacerse de forma que sea entendida por todos los participantes, antes de que dicha estrategia sea puesta en práctica. La estrategia es una declaración concisa que incluye contexto, condiciones y consecuencias en caso de que el riesgo realmente ocurra. La estrategia, junto con la identificación de riesgos, no busca señalar culpables antes de que los haya. Si éste fuera el enfoque, la estrategia estaría destinada a fracasar, pues los participantes se negarían a dar opiniones abiertas acerca de los riesgos que observan.

Es necesario mencionar que una buena identificación de riesgos sólo puede ser hecha por personal experimentado, ya que se requiere hacer comparaciones de la empresa bajo análisis con otras similares, lo que implica consultar tanto a expertos como aquellos resultados de experiencias que sobre riesgos se han obtenido con la operación de sistemas de seguridad similares, es por eso que sólo alguien con experiencia puede realizar en forma adecuada todas estas actividades. El uso de escalas ordinales para caracterizar los riesgos también hace evidente la necesidad de recurrir a los expertos en la materia, no porque el experto sólo sirva para manejar estas escalas, sino porque sólo él tiene más experiencia en cómo expresar la magnitud de estos parámetros para que los participantes en la operación del sistema de seguridad en realidad

presten la debida atención a los riesgos. Si este trabajo se hace de manera correcta, la alta dirección no sólo dará atención a las evaluaciones, sino también asignará con más facilidad los recursos necesarios con pleno convencimiento.

Sólo hasta que se han cumplido estos requisitos es posible establecer una política organizacional adecuada para administrar el riesgo, la cual establece lo que la alta dirección espera de una estrategia y de identificar, analizar y mitigar los riesgos.

Una vez que ya se tiene una estrategia y se ha adoptado una política de apoyo a ésta, entonces es posible asignar los recursos necesarios para su realización. Estos recursos pueden incluir bases de datos para administrar el riesgo, herramientas de mitigación del riesgo, herramientas para elaborar prototipos, recursos para modelado y simulación y, desde luego, recursos económicos.

En esta etapa es conveniente hacer una selección de los responsables del manejo de cada uno de los recursos asignados. Es importante resaltar que las personas a cargo de cada uno de los recursos deben tener la suficiente capacidad de manejo de los mismos. En caso necesario, se impartirá la capacitación adecuada para que el personal conozca la forma correcta de usar y administrar los recursos.

Ya que se han asignado los recursos y se han seleccionado a los responsables del uso adecuado de éstos, quienes se sabe están capacitados para ese trabajo, se continuará con la fase de monitoreo y control, no sólo de los riesgos sino también del uso de los recursos. En este caso, el monitoreo consiste en supervisar y registrar todos los hechos respecto a los riesgos y a la asignación y uso de los recursos, en tanto que controlar, como parte fundamental del proceso administrativo, significa inspeccionar y comprobar que los riesgos se están manejando de forma adecuada y que los recursos se están utilizando para los fines previstos, a fin de regular el funcionamiento de todo el esquema de identificación y administración de riesgos y recursos asignados.

Ambas actividades, monitoreo y control, se realizan mediante la elaboración de una serie de reportes que muestran el rastreo del comportamiento de los riesgos y del uso de los recursos, aunque los reportes no son la única forma de manejarlos, ya que por ejemplo, las grabaciones de voz o videos, también son formas que pueden ayudar al monitoreo y control.

Después se comparan las lecturas de los parámetros de riesgo reales contra las esperadas y se registra cómo han sido utilizados los recursos en dichas actividades. La necesidad de registros más precisos y frecuentes se hace evidente cuando se aplican planes de contingencia luego de que ha ocurrido un riesgo severo o catastrófico, de esta manera se debe aplicar el control en su máxima expresión.

Independientemente de que llegara a ocurrir un riesgo catastrófico, también es importante vigilar que todos los procesos descritos en la estrategia de la administración de riesgo se sigan tal y como fueron planeados. Los procesos deberán estar claramente definidos tanto en la estrategia como en los planes de mitigación. Si dichos procesos no existen o no están definidos con claridad, entonces los responsables no sabrán lo que deben hacer en cada situación. Por otro lado, si los procesos están bien definidos pero no se siguen correctamente, no se pueden garantizar los resultados deseados.

Actividad de aprendizaje

En el siguiente espacio y elabora un mapa mental que explique la administración del riesgo. Comparte con tus compañeros.

Categorización de riesgo

Un riesgo en seguridad informática sucede cuando una vulnerabilidad y una amenaza actúan al mismo tiempo. Dentro de estos orígenes genéricos de riesgo es útil crear categorías de riesgo, a fin de determinar con mayor facilidad las actividades de mitigación. Así, se pueden citar cuatro categorías de riesgo:

1. Los que se originan en cualquiera de las fases del proyecto, de la implementación del mismo o de la operación del sistema de seguridad informática.
2. Los que se originan en cualquiera de los procesos rediseñados que existen en la operación del nuevo sistema de seguridad.
3. Los que se originan en la tecnología utilizada para aplicar y controlar las medidas de riesgo.
4. Los que se originan en la forma de administrar el proyecto, su implantación y operación, lo cual incluye costos y origen de los fondos para estas tres fases.

Pero, no todos los riesgos son de alto impacto, por tanto se debe asignar un presupuesto distinto para mitigar cada uno de acuerdo con su importancia. Para ello, la identificación debe hacerse de forma clara y concisa, declarando las condiciones en las cuales llegaría a suceder y las consecuencias del evento.

La mayoría de los riesgos mencionados suceden en la etapa de evaluación del proyecto de seguridad informática; sin embargo, existe otros riesgos que suceden en la fase de operación, los cuales se describen en la tabla 1.1 .

Tabla 1.1 Elementos o factores de riesgo operativo[1]

	Elemento o factor de riesgo operativo	Clases
1	Sanciones legales	A. Multas
		B. Rechazar o no otorgar autorizaciones
		C. Intervenciones
		D. Vetar funcionarios
		E. Castigos legales a funcionarios

Continúa

[1] Tomado de Baca G., Solares P. Acosta E. (2012). Admistración Informática I. México: Grupo Editorial Patria.

Continuación

	Elemento o factor de riesgo operativo	Clases
2	Información	A. Errores no intencionales
		B. Información o datos modificados con dolo
		C. Falta de consolidación
		D. Entrega no oportuna
3	Operaciones (actividades)	A. Errores no intencionales
		B. Actividades mal realizadas intencionalmente
		C Corrupción en beneficio de personas ajenas a la organización
4	Tecnología	A. Errores no intencionales
		B. Alterar con intención la funcionalidad de las aplicaciones
		C. Usar la TI para beneficio de personas ajenas a la empresa
		D. Terceros que accedan a las aplicaciones de la empresa con objeto de alterar u obtener un beneficio indebido (crackers)
5	Robos y fraudes	A. Despojo físico o vía electrónica de bienes o valores (dinero o equipos) propiedad de la empresa o de los clientes
6	Desastres naturales	A. Cualquier suceso natural que demerite el valor o uso de bienes por la magnitud del acto (terremotos, inundaciones, incendios, descargas eléctricas, etc.)
7	Sabotaje	A. Empleados de la empresa que provocan daño intencional a los bienes y/o a las personas
8	Terrorismo o vandalismo	A. Terceros a la empresa que con dolo provocan daño a los bienes y/o personas
9	Empleados	A. Falta de conocimientos necesarios para el desempeño de su trabajo
		B. Actitudes negativas que provocan una baja de la moral
		C. Selección errónea del personal debida a la falta de evaluación del nivel de conocimientos y honradez durante la contratación
10	Productos y servicios	A. Debilidades de los productos comparados con la competencia
		B. Fallas en los servicios o productos

Es interesante observar en la tabla 1.1 que hace referencia al engaño o a la mala intención para alterar la información, por operar la TI de forma que permita el acceso a personas no autorizadas, por manipular la TI de modo que pueda fallar o por permitir la entrada de virus u otras amenazas; cualquier atentado contra la TI de la empresa constituye un atentado contra la información que contiene esa TI. Una vez que el proyecto ha sido aprobado, implementado y se encuentra en operación, la capacitación del personal es fundamental para que

el proyecto que ya opera genere los beneficios calculados. Se entiende que al implementar el nuevo sistema de seguridad informática ya se han instalado todos los dispositivos y las medidas señaladas por la Norma ISO 27000, para prevenir intrusiones no deseadas de cualquier tipo; no obstante, si el personal actúa en forma dolosa, entonces no hay manera de prevenir esta actitud más que mediante el cese de dicho personal. A menudo el tiempo que transcurre desde que esta persona actúa con dolo en perjuicio de la organización hasta el momento en que es detectada esa conducta y se identifica al culpable, puede ser largo y las consecuencias para la organización o empresa podrían ser catastróficas.

Aunque ya existe mucho software para controlar el movimiento de la información en las bases de datos (por ejemplo, cuántas veces se ha copiado cierta información, quién la copió, a dónde se envió, etc.), un buen hacker y un buen cracker siempre podrá tener acceso al sitio y a la información que él quiera; además, conoce y aplica las técnicas para borrar los rastros de su intrusión. Por esta razón, es importante señalar la importancia de instalar claves de acceso a la información privilegiada de las empresas.

Por tanto, se debe realizar un análisis cualitativo, seguido de un análisis de costos, identificando los niveles de riesgo aceptables, así como la manera de determinar cuándo y cómo se podrán superar los niveles de riesgo acordados. Asimismo, se debe documentar cualquier riesgo identificado con un impacto importante, así como designar a una persona con responsabilidad, autoridad y recursos para gestionar dicho riesgo. Las soluciones para eliminar, mitigar, trasladar, compartir o aceptar los riesgos, así como los planes para aprovechar oportunidades, deben estar basadas preferentemente en tecnologías conocidas o datos históricos.

Un hacker es una persona que conoce de informática y por ello puede tener acceso a sistemas informáticos y puede realizar modificaciones en ellos. Demuestran la vulnerabilidad de los sistemas pero los corrige, en tanto que un cracker rompe o quiebra un sistema de seguridad informático, invadiendo los sistemas, descifrando claves, robando contraseñas, robando datos o cualquier otra actividad ilícita, y esto lo hacer para perjudicar o para obtener un beneficio económico.

Los riesgos aceptados deben documentar las razones por las que se aceptan. Cuando se propone una solución para un riesgo identificado, primero hay que comprobar que no existe ningún efecto indeseable o nuevo riesgo introducido a raíz de su implementación y tener en cuenta el nivel de riesgo residual. Cuando se establecen contingencias para la gestión de riesgo en el calendario o en el presupuesto deben ser identificadas y mantenidas por separado.

Entre los ejemplos del riesgo de no obtener los beneficios deseados se encuentran:

- No alineación con la estrategia o políticas comerciales.
- No alineación con estándares técnicos, arquitectura, etcétera.
- Que los resultados no se puedan cuantificar (indicadores intermedio y final).
- Procesos de monitoreo de beneficios.
- Sensibilidad de los resultados a coyunturas o dependencias externas; por ejemplo, cambios en la economía, las condiciones de mercado o un sector industrial específico.
- Grado de cambio organizativo necesario (fondo y amplitud).
- Claridad del alcance del cambio organizativo necesario.
- Calidad del plan de gestión del cambio.
- Nivel de preparación y capacidad del negocio para adaptarse al cambio.
- Nivel de conocimiento y compromiso de la organización con el programa.
- Calidad y disponibilidad de promoción del negocio.
- Compromiso de la alta dirección del departamento de negocio.

No es sencillo cuantificar el riesgo en cualquiera de los puntos señalados; sin embargo el riesgo existe y hay que aprender a considerarlo y a administrarlo.

Priorización e impacto de riesgos

Como se dijo antes, no todos los riesgos son importantes, por lo que es necesario definir cuáles son los riesgos que en definitiva pueden afectar e, incluso, terminar con el proyecto, la implantación y la operación de un nuevo sistema de seguridad informática, y cuáles son aquellos riesgos que pueden suceder sin que haya mayores consecuencias.

Riesgos de prioridad 1

Se definen como aquellos riesgos que de llegar a suceder terminarían con la ejecución tanto del estudio del proyecto como de su implementación. Como ejemplo tenemos la falta de recursos económicos aunado a la incapacidad

de la empresa de conseguir financiamiento externo. Otro riesgo de este tipo es la falta de interés en el proyecto por parte de la alta dirección, ya que en ocasiones se termina el estudio del proyecto y pasan meses para que se tome la decisión de llevarlo a cabo, hasta que finalmente el proyecto es archivado; por tanto, desde antes de iniciar la evaluación del proyecto, debe haber un claro compromiso de la alta gerencia para apoyarlo. Un tercer riesgo de este tipo es una pésima determinación de la inversión requerida para el proyecto y de los costos operativos del nuevo sistema de seguridad, pues si estas determinaciones se hacen en forma deficiente, es posible hacer un presupuesto que se quede corto al momento de comprar la TI y su costo sea mucho mayor que el que se había presupuestado en un principio, por lo que si la organización no consigue los recursos adicionales, puede llevar al abandono del proyecto de seguridad.

Riesgos de prioridad 2

En general estos riesgos son externos, razón por la cual la organización no los puede controlar. Un ejemplo de este tipo de riesgos es cuando el proyecto de seguridad se deriva de la observación de un mercado en crecimiento y se plantea el objetivo de ganar más mercado, pero si acontece una crisis económica mundial, entonces los mercados en vez de expandirse, se contraen por algunos años. Si esto sucediera, la evaluación del proyecto deberá detenerse de inmediato, pues se sabe que en cuatro o cinco años el mercado tenderá a contraerse o a mantenerse estable, en vez de incrementarse.

Riesgos de prioridad 3

Se definen como aquellos riesgos que de llegar a suceder causarían perturbaciones a la programación de la evaluación, la implementación y/o la operación del nuevo sistema de seguridad, pero de ninguna forma podrían anularlo, tales como falta de capacitación, dificultad para conseguir información relevante para tomar decisiones, no determinar las métricas adecuadas para el control de la operación, no alinear la TI a la planeación estratégica de la organización, entre otros. Este tipo de riesgos suelen retrasan toda la programación, pero no anulan el proyecto.

Riesgos de prioridad 4

Son aquellos riesgos que de llegar a suceder afectan en forma mínima la evaluación, la implementación y la operación del nuevo sistema de seguridad. Aquí se incluyen todos los inconvenientes cotidianos que suceden sin mayor consecuencia, como enfermedades pasajeras de los participantes, viajes del director general que le impiden asistir a juntas relacionadas con el proyecto y tomar decisiones, falta por cortos periodos de material para trabajar, retraso en el suministro de recursos económicos, entre otros.

Umbrales de tolerancia

Un umbral de tolerancia se define como el valor máximo (o mínimo) que puede adquirir un factor de riesgo antes de intervenir para mitigar sus efectos. Desde luego que dadas las consecuencias de cada uno de los tipos de riesgo, los únicos que siempre deben tener determinados estos umbrales son los riesgos de prioridad 1, pues son los únicos que ponen en riesgo la viabilidad de la operación del sistema de seguridad. Los riesgos de prioridad 2 y, en menor medida, los de prioridad 3 y 4, aunque son molestos y pueden causar retrasos, no necesariamente deben contar con umbrales de tolerancia. De hecho, tiene un costo muy bajo el prevenir los riesgos de prioridad 2, 3 y 4, así que es relativamente sencillo y poco costoso evitarlos. Por tanto, hay que concentrar los esfuerzos en los riesgos de prioridad 1.

Una vez que se han identificado, localizado, priorizado y determinado los umbrales para cada uno de los riesgos, se deben establecer estrategias para evitar, en la medida de lo posible, no sólo que sucedan los riesgos sino que en caso de que llegaran a ocurrir, el impacto de tales eventos sea mínimo durante la operación del sistema de seguridad.

La estrategia debe tener su base en la visión que se quiera no sólo del desarrollo del nuevo sistema de seguridad, sino del resultado final esperado, de tal forma que cuando cualquiera de los riesgos detectados empiece a tener cierto impacto, se tomen las medidas necesarias, a fin de asegurar que se obtendrá el resultado deseado. Se recomienda que en todas las actividades de la administración de riesgo siempre estén involucrados los principales participantes del área de seguridad.

Un procedimiento para mitigar los riesgos de consecuencias catastróficas implica tener reservas económicas especiales para enfrentarlos, contar con el equipo especial y personal experto disponible para trabajos de restauración, tener a la mano contactos clave y recursos de emergencia para cualquier duda al respecto. Sin embargo, habrá riesgos que se deja que sucedan porque sus consecuencias se pueden soportar sin afectar significativamente al proyecto, o porque es inviable mitigar sus efectos.

La elaboración de todo el estudio de riesgos, en el que se incluyen la identificación, la priorización, los planes de mitigación, los planes de contingencia, etc., requiere de un análisis costo/beneficio. En este sentido, no hay duda de los beneficios que se obtienen por realizar un análisis muy completo de riesgos, pero el costo puede llegar a ser significativo. También hay que mencionar que se debe escuchar la opinión de todos los participantes del proyecto, pero el análisis de riesgo sólo está reservado para personal con experiencia.

Las etapas del proceso administrativo y la seguridad informática

Una vez que se tiene la idea general de lo que significa la seguridad informática, se es consciente de la importancia de la información para cualquier empresa u organización y se conocen los riesgos a los que está expuesta esa información, es conveniente mencionar en qué consiste la gestión del riesgo en seguridad informática.

En este punto se parte del hecho de que se tiene un sistema de seguridad informática, ya sea como proyecto para una empresa de nueva creación, o bien que la empresa ya está en funcionamiento y está interesada en implementar un nuevo sistema de seguridad informática, independientemente de que haya tenido problemas de intrusión de cualquier tipo en sus sistemas de información.

La primera etapa del proceso administrativo y, por ende, lo primero que se recomienda realizar para tener éxito al implantar un nuevo sistema de seguridad informática, es elaborar un proyecto para tal fin. Un proyecto nace a partir de una necesidad, en este caso la de proteger la información en una empresa u organización.

Como el área de seguridad informática o el área de sistemas, donde puede estar incluida la de seguridad, son parte de una empresa u organización, se parte del hecho de que la empresa ya ha realizado una planeación estratégica. Esto significa que ya ha declarado su misión, visión y objetivos; es decir, la empresa ya sabe para qué fue creada y a dónde se quiere llegar en el corto y en el largo plazos, y para lograrlo ya se ha planteado una serie de objetivos de ejecución inmediata.

Se debe aceptar que dentro de esos objetivos se encuentra el logro de un alto estándar o calidad en la seguridad informática, pues la empresa ya ha tomado conciencia de lo vital que es la información histórica y la que se genera día a día, para tomarla de base, realizar análisis y lograr su misión y visión.

La pregunta clave que debe hacerse la dirección de la empresa es: ¿A dónde queremos llegar en materia de seguridad informática?, independientemente de los problemas que haya tenido antes. Después de contestar esta pregunta, todo el equipo integrante del proyecto deberá asegurarse de que el nuevo sistema de seguridad informática esté alineado con la misión, la visión y los objetivos de la empresa. Esto significa que el área de seguridad informática y el nuevo proyecto deben contribuir a lograr la misión y la visión, y jamás deberán pensar que son un área separada de la empresa, con objetivos independientes. Desde el principio, ambas áreas deben saber que forman parte de toda la entidad llamada empresa y que su objetivo es asegurar la protección del recurso más valioso, después del recurso humano.

La segunda etapa del proceso administrativo es la dirección. Para saber cómo se debe dirigir a la empresa hacia el objetivo declarado de seguridad informática es necesario tomar decisiones, y las mejores decisiones siempre se toman con información, que si no está disponible, se investiga, se obtiene y analiza. En este caso, la información necesaria para tomar las mejores decisiones es determinar el tipo de amenazas, el tipo de riesgo y la vulnerabilidad de todo el sistema de información de la empresa, entendiendo por vulnerabilidad la parte o aspecto del equipo que no está protegido contra la amenaza detectada. Por tanto, es necesario determinar umbrales de tolerancia; esto es, hasta qué valores se podrá soportar un riesgo que ya está sucediendo. También habrá que clasificar al equipo, es decir a la TI, que posee la empresa de

acuerdo con el grado de importancia, así como también habrá que clasificar la información, ya que alguna será más importante que otra, y otra más será de alta confidencialidad para la empresa, por lo que habrá que asegurarla con mayores y mejores estándares de seguridad, para obtener una tabla de información como la que se observa en la tabla 1.2.

Tabla 1.2 Fuente de riesgos, amenazas y vulnerabilidad

ACTIVO	Prioridad	Amenaza		Tipo de riesgo	Vulnerabilidad		Umbral	
		lógica	física		humana	lógica	máximo	mínimo
Servidor								
Puertos								
Terminales								
Otros								

El contenido de la tabla 1.2 debe ser suficiente para tomar decisiones con respecto a lo que la empresa necesita de equipo (TI), software, recursos humanos e inversión.

El siguiente paso del proceso administrativo es la organización. En este punto es preciso que todas las decisiones que se han tomado respecto al nuevo sistema de seguridad informática se organicen, a fin de llevarlas a la práctica. Uno de los principales objetivos de la organización es emitir políticas, desde aquellas que tienen que ver con la contratación de personal hasta las que autorizan a ciertas personas a tener acceso a determinados archivos, a definir controles generales de acceso a la empresa y al área de seguridad informática y a establecer el tipo de controles y de políticas de promoción de personal, recordando que muchos intrusos de los sistemas de información son personal de la propia empresa que no está de acuerdo con la forma en que se les trata en un determinado momento o situación.

Otro punto muy importante del cual se encarga la organización del proyecto es definir los manuales de procedimientos, ahora llamados procesos, que son las actividades que deben realizarse porque tienen un propósito muy definido, los cuales son cuantificables. Por ejemplo, el proceso para acceder a información de prioridad 1, cómo hacer el registro de acceso y el formato

para reportar si la información fue copiada o enviada, así como las sanciones a empleados por uso de Internet que no esté relacionado con el trabajo que desempeña, entre muchos otros aspectos.

La cuarta etapa del proceso administrativo es el control. Una vez que la dirección de la empresa proporcionó todos los recursos que fueron solicitados y que la parte de la organización dictó las normas para trabajar en todos los sentidos, el control desarrolla parámetros que miden día a día, si el área de seguridad informática se está dirigiendo a donde quiere llegar. Por lo normal, elabora reportes periódicos del comportamiento de toda el área, calificando el desempeño de cada parámetro de control y señalando éxitos, fracasos y responsables.

Actividad de aprendizaje

Investiga en diferentes fuentes de información y con la ayuda de un procesador de textos elabora un reporte donde expliques las etapas de la seguridad informática. Cuida tu redacción y ortografía.

Normas para el análisis y administración del riesgos en TI

En la actualidad existe una serie de normas ISO (éstas se tratan con mayor profundidad en el siguiente capítulo), así como software comercial cuya única aplicación es la administración del riesgo. Para una mayor comprensión al respecto, a continuación se mencionan los datos más relevantes de estos aspectos.

- **Comunicación "A" 4609 del BCRA para entidades financieras.** Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con la tecnología informática y los sistemas de información.
- **ISO/IEC 27001.** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Metodologías de análisis de riesgos

- **Citicus One.** Software comercial de Citicus que implementa el método FIRM del Foro de Seguridad de la Información.
- **CRAMM.** CCTA Risk Assessment and Management Methodology. Originalmente desarrollado para uso del gobierno del Reino Unido, aunque ahora es propiedad de Siemens.
- **ISO TR 13335.** Precursor de la ISO/IEC 27005.
- **MAGERIT.** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible tanto en español como en inglés, es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (alineada a la ISO/IEC 27005 y otras metodologías internacionales).

La norma ISO 27000 presenta los requerimientos para una adecuada gestión de la seguridad de la información. Algunos de sus capítulos y su contenido se explican brevemente en los siguientes párrafos.

La ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y los indicadores recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios; la ISO 27003 consiste en una guía de implementación de SGSI (Sistemas de Gestión de Sistemas de Información) e información acerca del uso del modelo PDCA (siglas del inglés Plan, Do, Check, Act, Planear, hacer, verificar y actuar) y de los requerimientos de sus diferentes fases.

La ISO 27004 especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Dichas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

La ISO 27005 establece las directrices para la gestión del riesgo en la seguridad de la información, además de que también apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante

para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información.

La ISO 27006 especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

La ISO 27007 consiste en una guía de auditoría de un SGSI (Sistemas de gestión en sistemas informáticos).

La ISO 27011 consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones.

La ISO 27031 consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

La ISO 27032 consiste en una guía relativa a la ciberseguridad.

La ISO 27033 es una norma consistente en siete partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

Por último, la ISO 27034 consiste en una guía de seguridad en aplicaciones.

La naturaleza de los procesos de negocio siempre tendrá un gran efecto sobre los riesgos identificados. Procesos que involucran una tecnología probada tenderán, siendo todo lo demás igual, a involucrar menos riesgo que aquellos procesos que requieren innovación en cualquier sentido. El riesgo asociado con los procesos de negocios está en gran parte descrito en términos de su costo e impacto. Algunas salidas de los procesos de otras áreas de aplicación deben ser revisadas para identificar posibles riesgos.

Las herramientas y técnicas para la identificación del riesgo son[2]:

---

[2] Soler Ramos, José A., Staking, Kim B., Ayuso Calle, Alfonso, Beato, Paulina y Botín O´Shea, Emilio. (2001). Gestión de riesgos financieros, un enfoque práctico para países latinoamericanos. España: Gestión 2000.

- **Listas de verificación**

Las listas de verificación están organizadas típicamente por fuente de riesgo. Las fuentes pueden incluir el contexto del proyecto, otras salidas de procesos, el producto del proyecto o temas tecnológicos, así como fuentes internas tales como las habilidades de los miembros del equipo (o la falta de éstas). A la fecha, algunas áreas de aplicación han usado esquemas de clarificación de manera amplia para las fuentes de riesgo.

- **Flujogramas**

Los flujogramas son un apoyo al equipo de trabajo para entender las causas y los efectos del riesgo. La cuantificación del riesgo involucra el evaluar el riesgo y las interacciones del mismo, con el objetivo de evaluar el rango de posibles resultados del proyecto y de su operación. De manera principal se preocupa por determinar qué eventos de riesgo merecen respuesta.

Las oportunidades y amenazas pueden interactuar de maneras no anticipadas (los atrasos de programación pueden forzar a considerar una nueva estrategia que reduce de manera general la duración de todo el proyecto). Un solo evento de riesgo puede causar múltiples efectos, como el causado cuando se presenta una demora en la entrega de componentes claves, lo cual, a su vez, genera aumento de costos, retrasos en la programación y la entrega de un sistema de seguridad informática de menor calidad. Las técnicas matemáticas usadas pueden causar una falsa impresión de precisión y seguridad.

Actividad de aprendizaje

En equipo de dos o tres personas elaboren un díptico donde presenten las Metodologías de análisis de riesgos. Compartan su trabajo con sus compañeros de clase.

Comprueba tus saberes

1. Explica con detalle cuál fue la aportación de Norbert Wiener a la informática y por qué es importante esa aportación.

2. Redacta con tus propias palabras una definición de seguridad informática.

3. ¿Por qué se considera que la información es el activo más valioso que tiene una organización después del activo humano?

4. Elabora un mapa mental donde presentes cuáles son los tipos de seguridad informática que se describen en la bibliografía especializada.

5. Elabora una tabla donde presentes las siete características que debe tener la información de acuerdo con lo establecido por COBIT.

6. ¿Qué significa que la información no tenga efectividad? Da un ejemplo.

7. ¿Qué significa que la información no tenga apego a estándares?

8. Por medio de un esquema, presenta los componentes de una cadena de suministros.

9. Describe los cuatro pasos del proceso administrativo.

10. Define riesgo de manera general.

11. Elabora un mapa mental de los riesgos internos y externos a los que está expuesta la información en cualquier organización.

12. Define amenaza informática y describe cinco ejemplos de este tipo de amenaza.

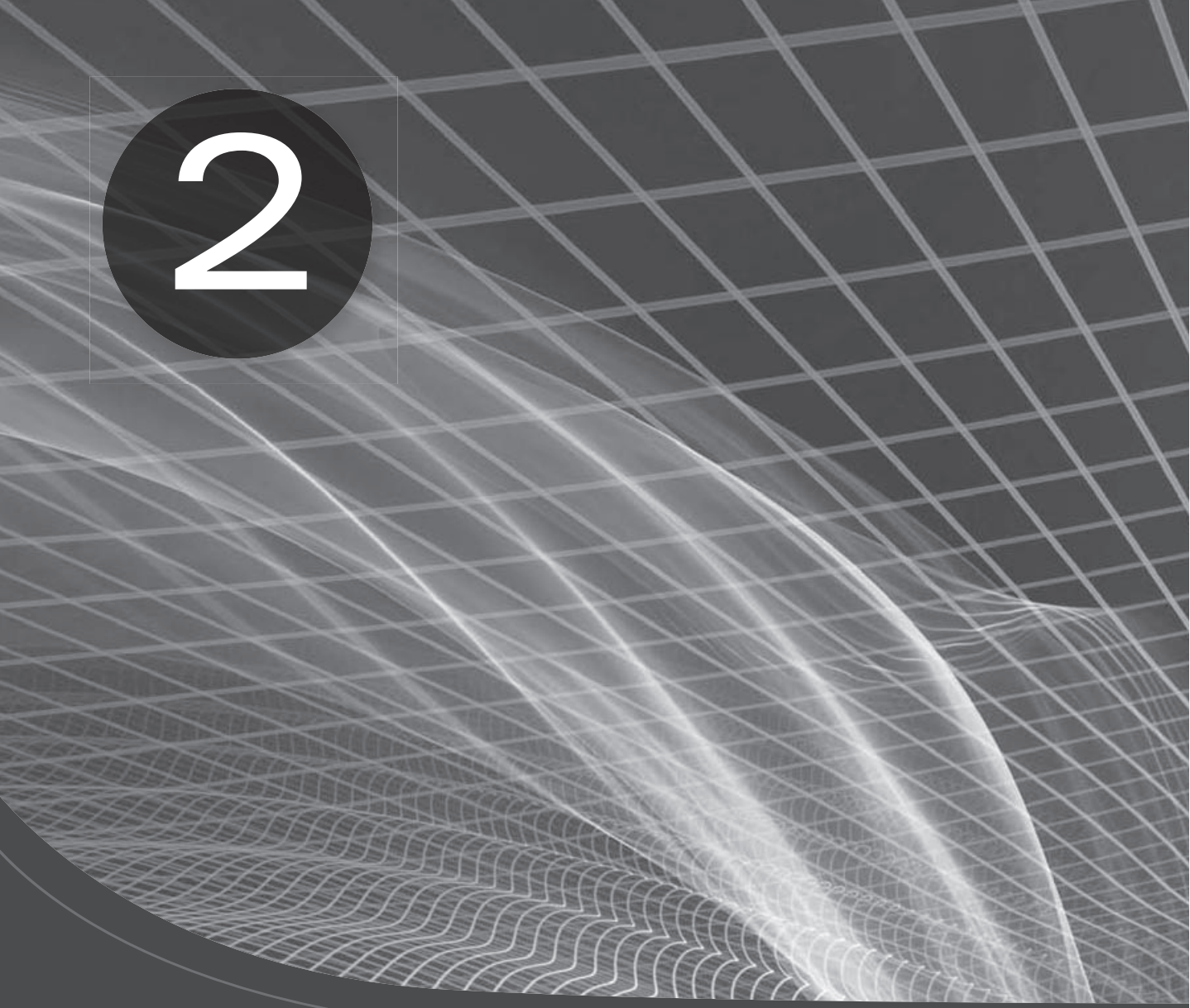
13. Menciona las principales vulnerabilidades que presenta la información dentro de una organización y, de acuerdo con lo visto en el capítulo, explica cuál sería la mejor opción para solucionarlas.

14. En equipo de dos o tres alumnos, elaboren un ensayo con la ayuda de un procesador de textos en el que presenten los siguientes conceptos: umbral de tolerancia al riesgo, categorías de riesgo y jerarquización del riesgo. Cuiden su redacción y ortografía. Presenten su bibliografía de acuerdo con la APA.

Referencias bibliográficas

1. Baca G., Acosta E., Solares, P. (2012). *Administración informática I.* México: Grupo Editorial Patria.
2. Fayol, Henry. (1961). *Administración industrial y general.* México: Herrero Hermanos.
3. Fingar, Peter & Smith, Howard. (2002). "Business Process Management. The third wave". En *Business Integration Journal.* Meghan-Kiffer Press.
4. Meyers, Mike. (2005). *Redes: gestión y soluciones.* España: Anaya Multimedia-Anaya Interactiva.
5. Villapecillin, M. M. (2005). *Arquitecturas de Red Multicapa: Conexión a base de datos.* España: Ra-Ma.
6. Turban, E. & Volonino, N. (2010). *Information Technology for management.* EUA: John Wiley and Sons.

2



Objetivo general

Que el estudiante comprenda el funcionamiento de los cifradores antiguos y los cifradores modernos.

Objetivos específicos

- Describirás el funcionamiento de al menos tres cifradores antiguos.
- Describirás el funcionamiento de al menos dos cifradores modernos.
- Conocerás la diferencia entre cifradores simétricos y cifradores asimétricos.
- Conocerás el significado del cifrado de una clave pública y su utilidad.

Criptografía

¿Qué sabes?

- ¿Por qué es importante la criptografía?
- ¿Qué relación tiene la criptografía con la seguridad informática?
- ¿Cuáles son las diferencias entre los cifradores simétricos y los cifradores asimétricos?

Competencias a desarrollar

- El alumno comprende el concepto de criptografía y su relación con la seguridad informática.
- El alumno describe, de manera general, el funcionamiento de algunos cifradores antiguos y modernos.
- El alumno comprende la diferencia entre cifrado de clave pública y clave privada.

2.1 Introducción

La palabra *cripta* proviene del griego y significa *esconder* o *encubrir*. La Real Academia Española (RAE) la define como *un lugar subterráneo donde se enterraba a los muertos.* Por extensión, la *criptografía* se define como el *arte de escribir con claves secretas o de manera enigmática.* Así, la *criptología* se considera un tratado acerca de los escritos secretos o cifrados, un criptograma es un documento cifrado y el *criptoanálisis* es el arte de descifrar criptogramas.

La necesidad de ocultar información al enviar mensajes tiene su origen en tiempos inmemoriales. La historia refiere muchos eventos de diversas guerras muy antiguas, cuando era necesario enviar mensajes de un ejército en el campo de batalla a las autoridades, gobernantes o reyes de alguno de los países en guerra. Mensajes que de ser interceptados por el enemigo, hubieran podido inclinar la victoria hacia una de las partes beligerantes, por lo que ya desde entonces se hablaba de mensajes encriptados.

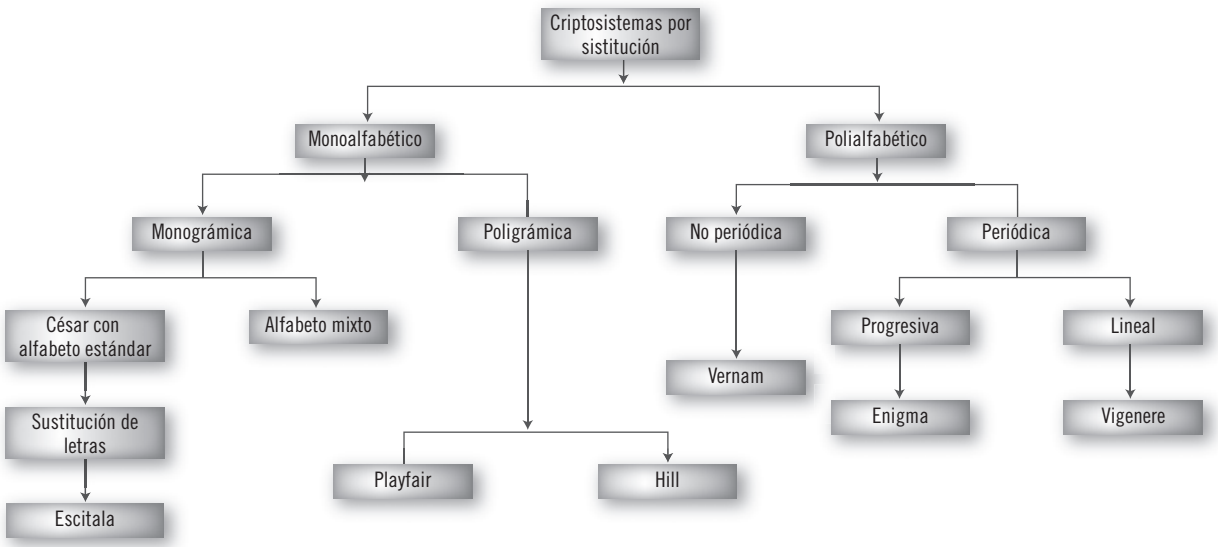
Dichos términos se adoptaron en informática cuando se hizo indispensable, y en algunos casos hasta una cuestión de vida o muerte, la necesidad de encubrir información secreta y confidencial que se enviaba a través de mensajes o cifras que sólo los interesados debían conocer. No necesitamos regresar siglos de historia para ver lo evidente de esta necesidad, sólo basta con citar un par de ejemplos actuales que lo describen a la perfección. Hoy día, si una persona hace una compra por Internet y paga con una tarjeta de crédito, durante el proceso de venta la empresa vendedora le solicita que anote su número de tarjeta de crédito y los números de la clave confidencial que aparecen al reverso de la tarjeta. Lo mismo sucede cuando una persona, empresa o banco llevan a cabo una transferencia electrónica de dinero, pues durante este proceso también se proporciona por Internet una serie de datos, que de caer en manos de personas mal intencionadas podrían tener consecuencias devastadoras para el cuentahabiente en cuestión.

2.2 Criptografía clásica

Se conoce con este nombre a todos los métodos utilizados para encriptar información y que han pasado a la historia por alguna razón, ya sea porque fueron de los primeros de los que se tiene registro, porque los utilizó algún

personaje famoso, porque en su tiempo se creían indescifrables y/o porque se utilizaron en conflictos bélicos y su descifrado determinó hacia cuál de los bandos beligerantes se inclinó la guerra.

En el esquema de la figura 2.1 se muestran los criptosistemas por sustitución, que son los de uso más extendido, y todos los tipos de criptogramas que se han desarrollado por este método de sustitución.



› **Figura 2.1**
Criptosistemas clásicos por sustitución.

Los primeros criptogramas de los que se tiene registro en la historia prescindían del uso de las matemáticas o los algoritmos. A la fecha se han identificado dos técnicas básicas de criptogramas clásicos: *sustitución* y *transposición*. En la técnica de sustitución quien envía el mensaje original, también llamado *mensaje claro* o *mensaje plano*, debe encriptarlo; es decir, escribirlo con una serie de claves o acomodos del texto plano, de tal forma que nadie lo pueda entender; en tanto, el receptor del mensaje deberá conocer cómo descifrar el mensaje a fin de entender con claridad el mensaje original o texto plano.

El cifrador más antiguo que se conoce es el que se ha bautizado con el nombre de Escítala, en honor a Escita, sitio donde los griegos lo desarrollaron y utilizaron por primera vez. Consiste en un bastón que utilizaba como símbolo de mando la más alta autoridad de Escita, el cual puede tener un diámetro uniforme a todo lo largo, o bien puede ser en forma cónica no muy

pronunciada, en donde se enrollaba una cinta y se escribía el mensaje original o en texto plano cuando la cinta se encontraba enrollada en el bastón y el mensaje se leía en forma horizontal. Cuando la cinta se desenrollaba del bastón, las letras no tenían ningún significado. Luego, la cinta se enviaba al destinatario quien poseía un bastón de idéntico diámetro, donde enrollaba la cinta y entonces podía leer el mensaje original. Utilizaba sólo un alfabeto.

Otros métodos de cifrado para ocultar mensajes importantes en textos consisten en sustituir la última letra del alfabeto por la primera, la segunda letra por la penúltima, la tercera letra por la antepenúltima, y así sucesivamente. De este modo, se podían enviar o descifrar mensajes como el siguiente:

RECOGE DINERO MISMO LUGAR

La sustitución de letras seguirá el siguiente orden: la A por la Z, la B por la Y, etcétera, tal como se muestra en la tabla 2.1.

Tabla 2.1 Patrón de sustitución de letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	**Sin cifrar**
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	**cifrado**

Mensaje cifrado:

IVXLTV WRMVIL NRHNL OFTZI

El mensaje cifrado puede hacerse todavía más difícil si no se separan las palabras, es decir:

IVXLTVWRMVILNRHNLOFTZI

Que equivaldría a decir: RECOGEDINEROMISMOLUGAR, lo cual es entendible para muchas personas, pero descifrarlo podría ser mucho más difícil sin la clave para desencriptarlo.

Otra forma de enviar mensajes cifrados consiste en leer el mensaje que está encriptado cada tres letras del mensaje claro; esto es, el mensaje impor-

tante se escribe encriptado en un texto cualquiera, el cual se descifra leyendo sólo cada tres letras del mensaje original. Por ejemplo, si se encripta sólo la primera palabra del mensaje anterior: **RECOGE**, el mensaje encriptado podría aparecer como: **poR mi EvaCua OriGenEs**; como se observa, si solo se lee cada tres letras del mensaje cifrado aparece la palabra RECOGE. Desde luego, dentro de las variantes de este tipo de cifrados también está la lectura cada 4, 5 o el espaciado de letras que se acuerde previamente en el cifrado.

Por otra parte, el tipo de cifrado conocido como *hermético* utiliza la técnica de transposición. De acuerdo con la historia, este tipo de cifrado fue utilizado por los hierofantes que cuidaban los templos en el antiguo Egipto. Consiste en escribir en un cuadrado de n por n letras, cuantas letras puedan caber en éste, donde el mensaje está oculto de manera aleatoria y la secuencia de lectura la proporciona una matriz que se sobrepone a la plantilla de letras donde está escrito el mensaje; en este caso, la plantilla de lectura tiene unos huecos, que es por donde se descifra el mensaje, siempre leyendo de izquierda a derecha y de arriba hacia abajo, y haciendo girar la plantilla lectora en el sentido de las manecillas del reloj. (Véase el mensaje cifrado que se muestra en la tabla 2.2).

Tabla 2.2 Mensaje cifrado

1	2	3	4	5	6	
W	Z	B	D	A	P	1
F	R	C	E	L	M	2
E	C	O	Z	R	N	3
F	Q	G	O	G	K	4
I	G	Y	E	J	I	5
H	T	W	H	D	F	6

Tabla 2.3 Lectura de mensaje cifrado transponiendo o superponiendo una plantilla lectora

1	2	3	4	5	6	
						1
	R		E			2
	C	O				3
		G				4
			E			5
						6

Como se observa en la tabla 2.3, la matriz para descifrar el mensaje tiene huecos en los cuadros 2-2, 4-2, 2-3, 3-3, 3-4 y 4-5, donde se lee la palabra RECOGE, recorriéndola en la forma acostumbrada, de izquierda a derecha y de arriba hacia abajo. Obsérvese también que si se aprovechan los mismos huecos y se gira la plantilla lectora en el sentido de las manecillas del reloj se puede continuar el mensaje, que no es el caso para esta plantilla.

Lo importante de cifrar un mensaje es que la forma de descifrarlo sea por completo aleatoria; es decir, que una computadora en los tiempos actuales no sea capaz de encontrar la forma en la cual fue hecho, por lo que de ningún modo tendrá manera de descifrar el mensaje escrito.

Se cree que cerca de 150 años a.C., un personaje griego llamado Polybios desarrolló otro cifrador que funciona mediante la técnica de sustitución. El criptograma de Polybios es similar al de los hierofantes egipcios, excepto porque éste sólo se limitaba a un cuadro de 5 filas por 5 columnas, de forma que sólo podía utilizar 25 letras del alfabeto, que al parecer eran las únicas que había en aquellos tiempos en Grecia (era evidente que no tenían ñ, ni w), de manera que hoy día se tendría que hacer una matriz de 6×6 y quedarían 3 espacios en blanco, con base en el alfabeto actual de 27 letras. Las letras se acomodaban en orden; es decir, en la primera fila y de izquierda a derecha A, B, C, etcétera. El criptograma clásico de Polybios se muestra en la tabla 2.4.

Tabla 2.4 Matriz de Polybios

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

En el caso de este tipo de cifrado, si se quería enviar la palabra RECOGE, el mensaje se cifraba en las casillas: 3-4, 5-1, 3-1, 5-3, 2-2 y 5-1. De este modo, la persona a la que estaba dirigido el mensaje sólo lo debía leer en esas posiciones de la matriz. Todo el resto del mensaje se construía de manera similar.

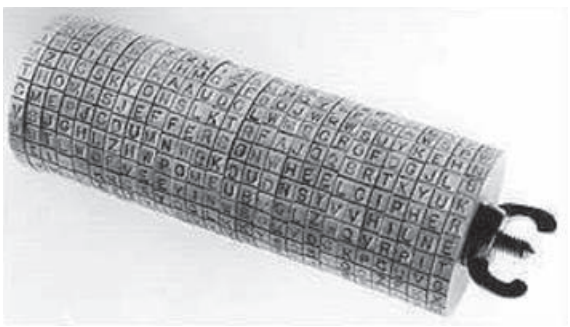
Unos pocos años después, en Roma se desarrolló el cifrador del César, que recibía este nombre en honor del emperador romano Julio César; desde luego, el César no lo inventó pero sí lo utilizó para enviar y recibir mensajes en las múltiples guerras que se libraron durante las conquistas romanas. Su funcionamiento es muy sencillo. Consiste en escribir las letras del alfabeto en un renglón; luego, en el renglón inmediato inferior se recorre la escritura del alfabeto tres lugares, tal como se muestra en la tabla 2.5. Como este cifrado utiliza un solo alfabeto, se dice que emplea la técnica de sustitución monoalfabética de la siguiente manera.

Tabla 2.5 Cifrador de César

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z			
			a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z

Por tanto, en este cifrador la palabra RECOGE aparecería como OBZMDB.

Un cifrador más reciente, desarrollado por Etienne Bazeries (de quien recibe su nombre), criptólogo francés del siglo XIX, consiste en 20 cilindros montados sobre un eje, cada uno contiene un alfabeto de 25 letras, por lo que se le conoce como polialfabético (en este caso, de nueva cuenta, son 25 y no 27 las letras de las que se compone, porque en Francia no existe la letra ñ y quizá en



› **Figura 2.2**
Cifrador de Bazeries.

aquellos tiempos tampoco existía la w). En este cifrador, el mensaje se escribe de izquierda a derecha. Cada disco del cifrador tiene un alfabeto completo de 25 letras, las cuales se encuentran en desorden diferente (véase figura 2.2).

Para elaborar un mensaje en el cifrador de Bazeries se elige un disco de referencia, el cual normalmente coincide con una marca especial que tiene todo el cifrador; entonces, a partir de ese disco, se dice, por ejemplo, que hay un generador –7, lo cual significa que si se va 7 posiciones hacia abajo de cada letra de la marca de referencia se encontrará el inicio del mensaje original y todas la letras de los discos restantes se acomodan de acuerdo con una posición aleatoria que elige la persona quien encripta el mensaje. Por ejemplo, si ya se tiene el inicio del mensaje en –7, la siguiente letra puede ser +3, la siguiente –19, etcétera, de manera que el mensaje cifrado que se envía puede ser –7, +3, –19, +24... ¡El número total de combinaciones que se pueden obtener de esta forma es de 25! (25 factorial), que equivale a un número de combinaciones posibles de 1 seguido por 25 ceros. Desde luego que para descifrarlo, quien recibe el mensaje necesita tener la posición de cada letra, respecto a la primera que es la referencia. A este tipo de cifrador se le puede catalogar como polialfabético periódico.

Entre los cifradores monoalfabéticos poligrámicos más importantes se encuentran el cifrador de Hill y el de Playfair.

Actividad de aprendizaje

Con base en lo aprendido en el tema de cifradores, crea un código y escribe un mensaje secreto; después intercámbialo con un compañero. ¿Cuánto tiempo tardó en descífralo?

Cifrador de Hill

El cifrador de Hill, llamado así en honor a su desarrollador, Lester Hill, quien fue el primero en proponer en 1929 el uso de un sistema de ecuaciones lineales que se pueden resolver con matrices, como método de encriptado con módulo 26 (el número de letras del alfabeto inglés). Su propuesta original consiste en que a partir del texto original o texto claro se conformen grupos de

tres, cuatro o más letras, cualquiera que sea el texto claro. Enseguida, para cada letra cifrada se propone una ecuación; por ejemplo, si se elige el grupo de tres letras, se forma una matriz de 3×3 y habrá tres ecuaciones, y si se forma un sistema de cuatro ecuaciones se forma una matriz de 4×4, que resuelve cada una de las incógnitas de las cuatro ecuaciones, y así sucesivamente

Por ejemplo, si el mensaje dice **DINERO DEPOSITADO EN ZURICH** y se hacen grupos de tres letras, éstas serán: DIN ERO DEP OSI TAD OEN ZUR ICH. Ahora bien, si se hacen grupos de cuatro letras, éstas serán: DINE RODE POSI TADO ENZU RICH, etcétera.

Es importante resaltar que este método no trabaja con matrices de dos letras y siempre estará en módulo 25 si es el alfabeto inglés o módulo 26 para el alfabeto español. En este método, antes de plantear las ecuaciones y las matrices, se asigna un número a cada letra del alfabeto en orden ascendente. Esta asignación se muestra en la tabla 2.6.

Tabla 2.6 Cifrador de Hill

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

El cifrado de Hill tiene la característica de que conforme se aumenta el número de letras de un grupo, el número de claves aumenta de manera casi exponencial. Entonces, se elige el grupo de letras que se va a utilizar, por ejemplo grupos de tres, que son tratados como un vector de tres dimensiones y se seleccionan en forma aleatoria los elementos de una matriz, en este caso de 3×3, los cuales constituyen la clave a utilizar. Los elementos de la matriz 3×3 deben tener valores entre 0 y 25 o 0 y 26, según sea el alfabeto que se utilice (con ñ o sin ñ).

Para la encriptación, el texto se divide en bloques o grupos de 3, 4 o más letras, de donde cada uno de los elementos se multiplica por los valores de la matriz 3×3. Como se dijo antes, todas las operaciones se realizan en módulo 25 o módulo 26, según el idioma que se elija. Realizar operaciones en módulo 26 significa que 26 = 0, 27 = 1, 28 = 2, etcétera. Por ejemplo, si se va a encriptar el

mensaje: **DINERO DEPOSITADO EN ZURICH** y se toman bloques de tres letras, primero se genera una matriz de claves y los vectores de esta matriz las elige el cifrador; es decir, la persona que va a cifrar los datos. Por tanto:

$$A = \begin{bmatrix} 7 & 5 & 9 \\ 5 & 8 & 4 \\ 4 & 7 & 3 \end{bmatrix}$$

Sea y_i las letras cifradas y x_i las letras del texto claro. Las ecuaciones que se plantean y que representan los vectores de la matriz son:

$$y_1 = 7x_1 + 5x_2 + 9x_3$$
$$y_2 = 5x_1 + 8x_2 + 4x_3$$
$$y_3 = 4x_1 + 7x_2 + 3x_3$$

Ahora bien, para el mensaje DINERO DEPOSITADO, los dos primeros grupos o bloques de tres letras se representan como DIN ERO, y en forma matricial:

$$x_1 = \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix} \text{ para DIN y } x_2 = \begin{bmatrix} 4 \\ 17 \\ 14 \end{bmatrix} \text{ para ERO}$$

Obsérvese que los coeficientes de estos vectores corresponden a los valores dados a cada letra en módulo 26, los cuales se muestran en la tabla 2.6.

Para cifrar el mensaje, se multiplican las matrices de las tres ecuaciones:

$$\text{cifrado DIN } C_1 = \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix} \begin{bmatrix} 7 & 5 & 9 \\ 5 & 8 & 4 \\ 4 & 7 & 3 \end{bmatrix}$$

$$\text{cifrado ERO } C_2 = \begin{bmatrix} 4 \\ 17 \\ 14 \end{bmatrix} \begin{bmatrix} 7 & 5 & 9 \\ 5 & 8 & 4 \\ 4 & 7 & 3 \end{bmatrix}$$

La solución de estas matrices genera el mensaje cifrado. Para que el método de Hill pueda cifrar, es necesario que la matriz de claves sea cuadrada, el determinante de la matriz sea diferente de cero y el inverso del determinante de la matriz sea un valor entero. Este texto no es un compendio de matemáticas, por lo que se sugiere al estudiante interesado cifrar el mensaje DINERO DEPOSITADO mediante el método de Hill, aquí aparece casi la mitad de la solución.

Cifrador de Vigenere

Este cifrador soluciona el punto más débil del cifrador de César, que radica en que el mensaje cifrado siempre tiene la misma longitud apartado del alfabeto normal; es decir, siempre se cifra igual. El cifrador de Vigenere está basado en diferentes series de caracteres o letras del cifrador de César, los cuales forman una tabla. En éste se usa una clave K de longitud L y se cifra letra por letra o carácter por carácter, sumando en módulo n en el texto claro con los elementos de esta clave. La tabla tiene una posición de inicio que es difícil de encontrar. La tabla es una matriz de 27×27, que como siempre, es el número de letras del alfabeto. Así, en la primera columna y en el primer renglón de este cifrador siempre aparece el alfabeto de la A a la Z; en el segundo renglón, el alfabeto empieza con la letra B y termina con la letra A, en el tercer renglón, el alfabeto empieza con la letra C y termina con la letra B, etcétera, y lo mismo sucede con las columnas.

Si a cada letra del alfabeto se le asigna un número progresivo, es decir, A = 1, B = 2..., se puede observar que cada letra tiene una posición distinta en cada columna y en cada renglón. Para generar la ecuación de cifrado $y_i = (x_i + z_i) \bmod 27$, y_i es la posición inicial de la primera palabra del mensaje cifrado y $(x_i + z_i)$ son las posiciones relativas de cada letra sucesiva del mensaje cifrado, en un alfabeto de 27 letras.

Cifrador Playfair

Recibe su nombre en honor a Lyon Playfair, que aunque no fue quien lo desarrolló, sí fue quien lo presentó ante el ejército inglés para que fuera

utilizado en la Primera Guerra Mundial. Es un cifrador muy elemental, pues consta de una matriz de 5×5, donde se escriben las letras del alfabeto inglés. Es importante destacar que en este cifrador la I-J van en una misma casilla y que usa la Ñ, la cual se anota en la misma casilla que la M (véase tabla 2.7 – sin Ñ–).

Tabla 2.7 Matriz de Playfair

A	B	C	D	E
F	G	H	I-J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Las reglas para cifrar mensajes en dicho cifrador son muy simples. Por ejemplo, para cifrar las palabras SITIADA HOY, primero se escribe la palabra en la esquina superior izquierda, sin repetir letras; es decir, las letras de la palabra sólo pueden aparecer una vez. Así, en este caso, ya no se anotan la segunda I ni la segunda A. Al terminar de escribir las palabras con estas eliminaciones, se escribe el alfabeto normal, tal y como aparece en la tabla original, pero ya no se repiten en la nueva tabla las letras que aparecen en el mensaje, es decir, ya no se escriben las letras SITAD en el resto de la tabla; por tanto, la tabla para empezar a cifrar quedaría como se observa en la tabla 2.8.

Tabla 2.8 Mensaje cifrado con la matriz de Playfair

S	I-J	T	A	D
H	O	Y	B	C
E	F	G	K	L
M	N	P	Q	R
U	V	W	X	Z

Obsérvese que como hay una I en el mensaje a cifrar, se escribe I-J en la casilla.

La siguiente regla es trabajar por pares de letras del mensaje a cifrar; en este caso: SI TI AD AH OY.

A continuación, la regla indica que si dos letras se encuentran en el mismo renglón de la matriz, éstas serán sustituidas por la letra que está a su derecha, mientras que si la letra que va a ser sustituida está en la columna de la extrema derecha, la letra que debe sustituirla es la que aparece en la primera columna de la izquierda en el mismo renglón; en el ejemplo siguiente, el primer digrama (bloque de letras formado por dos caracteres) SI aparece cifrado como JT, por lo que si se quiere cifrar AD, aparecerá como DS.

La siguiente regla señala que si dos letras del mensaje claro que van a ser cifradas se encuentran en la misma columna, éstas deberán sustituirse por aquellas letras que se encuentran inmediatamente abajo de cada una. En el siguiente ejemplo no aparece esta situación; sin embargo, si se supusiera que las letras fueran TY, éstas se deberían cifrar como YG.

Una tercera regla establece que si el digrama del mensaje claro que se va a cifrar aparece en extremos opuestos de diferentes filas, es decir si está en diagonal, en extremos opuestos, las letras del mensaje deberán sustituirse por las letras que correspondan a la otra diagonal al formarse un cuadrado. En el siguiente ejemplo no se tiene este caso, pero suponiendo que las letras fueran DH del mensaje claro, la H deberá sustituirse por la S y la D por la C, como se observa en tabla 2.9.

Tabla 2.9 Tercera regla del cifrador de Playfair

S				D
H				C

La cuarta y última regla establece que si en el mensaje original la cantidad de letras es impar, característica con la cual no es factible formar el digrama, o si el mensaje claro tiene una letra doble, como en CARRIL, o doble LL, como en LLAMA, entonces no se pueden aplicar las tres primeras reglas y se hace uso de una letra nula; por ejemplo, si al final del mensaje claro aparece la letra A sola, para hacer el digrama se agrega una X; así, el digrama queda como AX. Para el caso de las letras dobles se hace lo mismo; es decir, CARRIL quedaría como CARXIL y LLAMA quedaría como LXAMA.

Una máquina cifradora más moderna, y de las primeras en trabajar con electricidad, es la famosa máquina Enigma, desarrollada en 1923. Ésta fue utilizada con mucho éxito por los alemanes durante la Segunda Guerra Mundial. Consiste en una serie de rotores, o ruedas, que giran haciendo un "tic", como sonido con un impulso eléctrico. En dicha máquina, cada rotor puede adquirir 26 posiciones, correspondientes a cada una de las letras del alfabeto alemán. Una vez que un rotor ha adquirido la letra que corresponde al mensaje enviado, ésta se detiene, y entonces el segundo rotor empieza a girar hasta adquirir la letra del mensaje que le corresponde, las cuales además están cifradas, es decir, la A no corresponde a la A, por lo que puede corresponder a cualquiera de las 25 letras restantes del alfabeto. El método que usaba Enigma era muy similar al que utilizaba el cifrador de Bazeries, sólo que Enigma funcionaba con electricidad. Además, en éste el mensaje plano no era tan plano, pues Guten Morgen (¡buenos días!, en alemán) podría significar muchas cosas, por ejemplo: "hoy no hay ataque" o "mañana atacamos", o cualquier otra cosa, ya que las claves cambiaban con cierta frecuencia; así, en una semana "Guten Morgen" podría significar "mañana atacamos", pero la siguiente semana podría significar otra cosa muy diferente. Aun así, el código utilizado pudo ser descifrado por el inglés Alan Turing, lo que permitió, según importantes datos históricos, que la Segunda Guerra Mundial terminara al menos dos años antes, salvando millones de vidas, pues los aliados (Estados Unidos de América e Inglaterra), al descifrar el código, se adelantaron a las acciones bélicas alemanas y empezaron a ganar muchas batallas, lo que debilitó poco a poco al ejército alemán.

El cifrado, definido como el arte de escribir un código secreto, incluye la encriptación, la firma digital y el descifrado. Toda institución debe desarrollar políticas para cifrar sus datos, incluyendo políticas de distribución de claves. Por ejemplo, el cifrado de discos es una forma de proteger datos almacenados; en tanto que para los datos en tránsito se puede utilizar la emisión de certificados SSL, avalados por una autoridad certificadora que tiene implementada una infraestructura de clave pública.

Actividad de aprendizaje

Investiga en diferentes fuentes de información acerca de la vida de Alan Turing, la importancia de su trabajo y su relación con la seguridad. Con los datos recabados y la ayuda de un procesador de textos elabora un ensayo. Anota la bibliografía que utilizaste con el uso del formato APA. Cuida tu redacción y ortografía.

Cambios que afectaron la forma de cifrar

Desarrollo de computadoras cada vez más potentes

La historia de la computación, en general, y de las computadoras, en particular, es fascinante. Si se considera que se llama computación al sólo hecho de calcular (que es la raíz de la cual proviene esta palabra), entonces se puede decir que la computación o el cálculo es tan antiguo como el hombre mismo; pero, si en realidad se hace referencia a calcular con medios electrónicos, entonces la computación se considera que tiene sus inicios en 1938, con la aparición de la primera computadora que trabajaba con tubos de vacío llamados "bulbos". Esa fecha marca el inicio de la vertiginosa carrera en el avance en conocimientos y desarrollos en esta área.

Hacia 1947 se crea el primer transistor, que pronto reemplazaría a los bulbos, y sólo dos años más tarde, en 1949, aparece la primera memoria de datos basada en transistores. Para 1950 empiezan a aparecer los primeros lenguajes ensambladores; entonces se crean Basic y Fortran. Hacia 1964 aparece la primera supercomputadora y en 1972 está disponible en el mercado el primer disco flexible.

Pero es en 1974 que acontece un hecho sin precedentes y de importantes dimensiones para la seguridad informática, pues en ese año se crea el primer protocolo TCP, es decir, el primer protocolo para el control de transmisiones. Además, en ese mismo año aparece la primera LAN (red de área local). Ambos conceptos, TCP y LAN, son fuentes de riesgo para la seguridad informática; sin embargo, en aquel tiempo la seguridad carecía de importancia, la atención estaba enfocada en los maravillosos avances tecnológicos.

Para 1983, el sistema ARPANET, que se había creado para uso militar en Estados Unidos de América, cede su infraestructura a todo el público y se crea Internet, una de las principales fuentes de riesgo informático. En ese mismo año Microsoft lanza al mercado Word V1 y dos años más tarde ya está disponible Windows 1.0. Hacia 1990 se crea la idea de hipertexto y con éste se crea la Word Wide Web, la famosa www, que constituye una nueva forma de interactuar con Internet. También en ese año se crea el protocolo de transmisión HTTP, HTML y el concepto de URL.

Hasta aquí concluye este viaje a través de la historia de las TIC, debido a que los siguientes 25 años de historia de las TIC son bastante conocidos.

Esta evolución de las TIC hace relativamente sencillo descifrar textos encriptados, pues es bien conocido el poder de cálculo de las computadoras actuales. De hecho, el cifrado de Hill no se hizo muy popular en su tiempo, debido a los cálculos que implica, los cuales ahora se resuelven con gran rapidez con ayuda de las TIC.

La Teoría de la Información

En 1948, cuando más o menos empezó el desarrollo de las computadoras, Claude Shannon presentó la Teoría de la Información. Aunque ya desde 1940, Shannon se consideraba el primer investigador del lenguaje en analizarlo desde el punto de vista matemático y estadístico. No es propósito de este texto presentar la enorme cantidad de conceptos que Shannon desarrolló durante su carrera, sólo basta decir aquí que fue el primero en determinar cuántos espacios en blanco tiene un mensaje o un texto común y cuál es el porcentaje de veces que se utiliza cada letra, entre muchas otras cosas más.

A la fecha, es sabido que casi en cualquier idioma, los espacios en blanco de un texto constituyen cerca de 20% del texto y que tanto en inglés como en español la letra E ocupa casi 13% de todas las letras del texto y que la letra A aparece cerca de 10 por ciento. También se pueden analizar los llamados digramas del lenguaje; los más utilizados en español son DE, ES y EN, los cuales constituyen 2.5% de todas las palabras de un texto en español. Mientras que los digramas poco usados son LO, EL, LA, MI, NO, SI, YO, TU, etcétera, que aunque son muy conocidos, estadísticamente se utilizan menos de 0.5% en cualquier texto en español. También existen trigramas como POR, MIS, TUS, NOS, MAS, LAS, etcétera, y algunos tetragramas como PARA, COMO, etcétera.

En resumen, con respecto a las estadísticas de uso de letras en el lenguaje español se tiene:

- **Letras más utilizadas:** E = 13%, A = 11%, S = 8%, O = 8%, I = 7.2%, N = 7%, R = 7%, D = 6% y T = 5%.
- **Letras usadas entre 5% y 1%:** C, L, U, M, P, G, B, F, V.
- **Letras usadas menos de 1%:** El resto de letras del alfabeto que son: Y, Q, H, Z, J, X, W, K y la Ñ.
- **Letras menos usadas, con un porcentaje de uso máximo de 0.1%:** X, W, K y Ñ.

Aunque la Teoría de la Información de Shannon contiene muchísimos más conceptos, las estadísticas del lenguaje son lo que interesa en primer lugar para el análisis del cifrado de textos. Aunque un texto esté cifrado, un buen inicio para el análisis es contar los espacios en blanco, los digramas y los trigramas que contiene el texto cifrado. Luego, con las estadísticas de uso de cada una de las letras, el analista se va acercando, poco a poco, para descifrar el mensaje.

Aunado a esta teoría, en 1963, en Estados Unidos de América, se creó el código ASCII (American Standard Code for Information Interchange), que en 1969 cambió su nombre a ANSI (American National Standards Institute), que son las letras y símbolos que se muestran en la figura 2.3 y que se supone

Caracteres ASCII de control		
00	NULL	(carácter nulo)
01	SOH	(inicio encabezado)
02	STX	(inicio texto)
03	ETX	(fin de texto)
04	EOT	(fin transmisión)
05	ENQ	(consulta)
06	ACK	(reconocimiento)
07	BEL	(timbre)
08	BS	(retroceso)
09	HT	(tab horizontal)
10	LF	(nueva línea)
11	VT	(tab vertical)
12	FF	(nueva página)
13	CR	(retorno de carro)
14	SO	(desplaza afuera)
15	SI	(desplaza adentro)
16	DEL	(esc. vínculo datos)
17	DC1	(control disp 1)
18	DC2	(control disp 2)
19	DC3	(control disp 3)
20	DC4	(control disp 4)
21	NAK	(conf. negativa)
22	SYN	(inactividad sínc)
23	ETB	(fin bloque trans)
24	CAN	(cancelar)
25	EM	(fin del medio)
26	SUB	(sustitución)
27	ESC	(escape)
28	FS	(sep. archivos)
29	GS	(sep. grupos)
30	RS	(sep. registros)
31	US	(sep. unidades)
127	DEL	(suprimir)

Caracteres ASCII imprimibles					
32	espacio	64	@	96	`
33	!	65	A	97	a
34	“	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	‘	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	l
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

› **Figura 2.3**
Código ASCII.

ASCII extendido (Página de código 437)							
128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	í	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134		166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	
136	ê	168	¿	200		232	
137	ë	169	®	201		233	Ú
138	è	170	¬	202		234	Û
139	ï	171	½	203		235	Ù
140	î	172	¼	204		236	ý
141	ì	173	¡	205	=	237	Ý
142	Ä	174	«	206		238	¯
143	Â	175	»	207		239	
144	É	176		208		240	
145	æ	177		209	Ð	241	±
146	Æ	178		210	Ê	242	
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	
155	ø	187	╗	219		251	¹
156	£	188		220		252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	
159	ƒ	191	⊠	223	⊠	255	nbsp

que son todas las letras y símbolos necesarios para escribir en los idiomas inglés y español.

Para cifrar textos sólo se utilizan los códigos del 32 al 255, lo cual facilita la posibilidad de cifrar un texto y dificulta más el descifrado. Además de las letras del alfabeto normales; aparte se han clasificado las vocales mayúsculas y minúsculas acentuadas, así como las vocales mayúsculas y minúsculas que llevan diéresis. Dentro del código también se han clasificado:

- **Símbolos de uso frecuente:** ñ Ñ @ ¿? ¡!: ⁄ \
- **Símbolos matemáticos:** ÷ ½ ¼ ¾ × ±
- **Símbolos comerciales:** € £ ¥ ¢ $ © ® °
- **Comillas y paréntesis:** " ' ( ) [ ] { } «»

La Teoría de la Información, con todos sus conceptos, ha sido una piedra angular para el descifrado de textos.

Aparición del estándar de cifra DES

El DES (Data Encryption Standard) es un algoritmo desarrollado en un principio por IBM para proteger datos mediante el uso de claves privadas de cifrado; solicitado primero por la NBS (National Bureau Standards) y al final adoptado por el gobierno de Estados Unidos de América en 1977 como estándar de cifrado de toda información considerada importante, pero no clasificada para el gobierno. En 1980, el NIST (National Institute of Standards and Technology) estandarizó todos sus modos de operación, momento a partir del cual ha sido el más utilizado de los algoritmos de clave simétrica. El algoritmo original de IBM, que trabajaba sobre bloques de 128 bits, con una longitud de la clave también de 128 bits, se basaba en operaciones de lógica booleana.

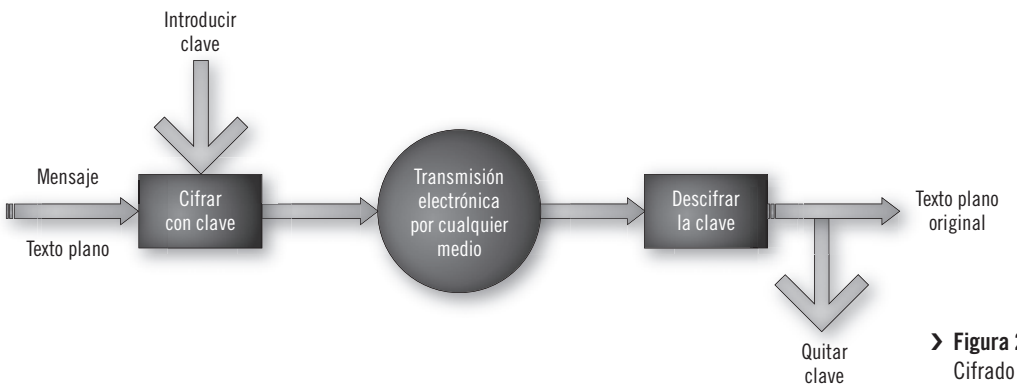
Antes de continuar, es conveniente explicar qué significa un algoritmo de clave simétrica y uno de clave asimétrica.

En el cifrado o criptografía simétrica, tanto el emisor como el receptor del mensaje claro tienen una llave o clave secreta que se utiliza ya sea para cifrar o para descifrar el mensaje claro. Como el mensaje se transmite a través de medios inseguros y la información se considera muy importante, se hace necesario protegerla. En la figura 2.4 se esquematiza el cifrado simétrico.

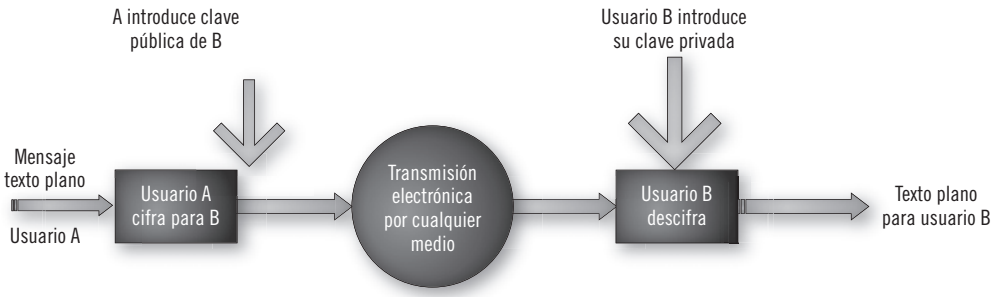
Además del cifrado simétrico, también existe el cifrado asimétrico, que requiere de dos claves o llaves: una pública y la otra privada, las cuales están relacionadas matemáticamente. Desde el punto de vista de la computación, es muy difícil conocer la llave privada a través de la clave pública. En la figura 2.5, que esquematiza el cifrado asimétrico, se puede observar que si un usuario A quiere enviar un mensaje claro al usuario B, debe utilizar una clave pública para cifrar y enviar el mensaje, el cual se envía por medios electrónicos inseguros; una vez que el mensaje llega al usuario B, éste utiliza su clave privada para descifrarlo.

Por otro lado, el cifrado simétrico se divide en cifrado por bloques y cifrado de flujo. En el cifrado por bloques, como su nombre lo indica, se cifran y descifran bloques de bits al mismo tiempo. Las operaciones que se hacen a los bits en varias ocasiones, llamadas rondas, son sustituciones, permutaciones, rotaciones y operaciones lógicas. Ejemplos de cifradores simétricos son: AES, DES y TDES. El TDES es el mismo DES original, pero debido a que los criptólogos encontraron cierta deficiencias, se determinó hacer tres veces las rondas de operaciones que se hacen con el DES, por lo que el TDES significa triple DES.

La desventaja que presentan los cifradores de bloque es que son capaces de multiplicar los bits de error, ya que cuando entran al proceso de descifrado puede haber muchos errores en la etapa de salida, los cuales se van incrementando en número. Aun así, éstos se consideran los cifradores más seguros, porque cada bit de salida depende de los bits de entrada y no existe correlación estadística entre los bits de entrada y los de salida.



› Figura 2.4
Cifrado simétrico.



› Figura 2.5
Cifrado asimétrico.

Por otro lado, el cifrado de flujo cifra y descifra bit por bit (ejemplos de estos cifradores son: RC4 y A5/1, respectivamente) tienen la desventaja de que se pueden diseminar los errores de sincronización que son causados por la inserción o eliminación de bits; es decir, si el sistema cifrador no está bien sincronizado con el sistema descifrador, este último puede arrojar datos falsos de todos los bits del texto plano que se ha recuperado, error que se corrige hasta que vuelva a haber sincronización de ambos sistemas. Aun cuando este sistema es más rápido que el sistema de bloques, no se utiliza precisamente por los problemas de falta de sincronización.

Se dice que uno de los cambios que modificaron la forma de cifrar fue la aparición del DES. Sin embargo, en virtud de que se encontraron ciertas debilidades en el DES, y como tiene una clave de sólo 64 bits, con sólo 56 que se utilizan efectivamente, ya que los otros 8 se usan para comprobar la paridad, bajo los mismos principios de funcionamiento, se desarrolló el AES (Advanced Encryption Standard), que también es un cifrador simétrico de bloques, el cual tiene bloques de 128 bits y claves de 128, 192 y 256 bits. Dependiendo del tamaño de la clave, en AES las rondas pueden ser 10 si la clave es de 128 bits, 12 si la clave es de 192 bits y 14 si la clave es de 256 bits. El AES fue llamado así por el NIST. Fue publicado en 2001 con el fin de reemplazar al 3DES o TDES y su predecesor DES, el cual fue creado en 1980 y para esa fecha estaba por completo desactualizado y superado. Mientras mayor es la cantidad de bits en un bloque, es mayor la dificultad para descifrarlo, por tanto, es muy usado para cifrar datos almacenados.

Hoy día, el AES es el cifrado más seguro. Funciona realizando cuatro transformaciones matemáticas:

1. *Sustitución no lineal de bytes.* Donde cada byte es reemplazado por otro de acuerdo con una tabla predeterminada de búsqueda.
2. *Mover de lugar las filas.* En esta transformación cada fila es rotada (cambiada de posición) de manera cíclica en determinado número de veces.
3. *Combinar los cuatro bytes de cada columna utilizando una transformación lineal.*
4. *Combinación de cada byte con la clave que se generó en una ronda.* Cada una de estas claves es una derivación de la clave de cifrado, efectuando una iteración de la clave mediante el uso de la operación XOR (⊕).

En la figura 2.6 se esquematiza el sistema de cifrado AES, donde se puede apreciar la introducción en cada ronda de las respectivas claves de esa ronda, y que cada ronda consiste en las cuatro operaciones de transformación mencionadas, excepto en la ronda final, donde ya no se mezclan las columnas.

Con el fin de que pueda observarse la complejidad del cifrado, a manera de ejemplo se presenta cómo se ejecuta la rotación de filas. AES se forma por arreglos matriciales de 4×4, la rotación de cada casilla siempre se ejecuta hacia la izquierda, operación que se efectúa hasta nueve veces.

Tabla 2.10 Matriz original

Número	0	1	2	3
0	$X_{0,0}$	$X_{0,1}$	$X_{0,2}$	$X_{0,3}$
1	$X_{1,0}$	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$
2	$X_{2,0}$	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$
3	$X_{3,0}$	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$

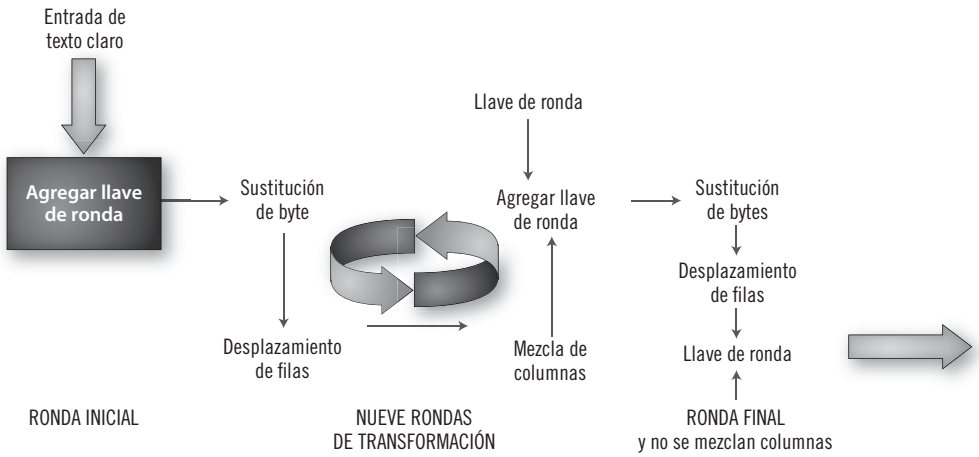
Tabla 2.11 Matriz con filas rotadas hacia la izquierda

Número	0	1	2	3
0	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,0}$
1	$X_{1,0}$	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$
2	$X_{2,2}$	$X_{2,3}$	$X_{2,0}$	$X_{2,1}$
3	$X_{3,3}$	$X_{3,0}$	$X_{3,1}$	$X_{3,2}$

Obsérvese en la tabla 2.11 que las filas 0, 2 y 3 fueron modificadas, al cambiar su posición hacia la izquierda.

Clave pública

El cuarto evento de gran importancia y trascendencia para el cifrado de textos fue la aparición de la clave pública, que fue desarrollada en 1976 por Diffie y



› **Figura 2.6**
Funcionamiento del sistema de cifrado AES.

Hellman. La clave pública se considera una de las bases de la seguridad en el envío de la información. Pero, no fue sino hasta 1978 que se desarrolló el más conocido y exitoso de los cifradores asimétricos: el RSA, nombre que se compone con la primera letra del apellido de cada uno de sus tres autores, Rivest, Shamir y Adleman. El RSA trabaja con una clave pública y una privada.

Otros destacados sistemas de cifrado asimétrico son: DSA y ElGamal, entre otros. A pesar de que la clave pública la puede obtener cualquier interesado, es imposible obtener la clave privada a partir de la clave pública. Ambas claves, la pública y la privada, se relacionan por una función matemática, la cual sirve para determinar las claves. Para descifrar ésta se utiliza la inversa de dicha función. Los cifradores asimétricos, al cifrar un mensaje, utilizan la factorización de enteros; mediante la cual, al cifrar un mensaje, el número entero se eleva a la potencia de la clave y el residuo es dividido por el producto de dos números primos. Al repetir el proceso con la otra clave se puede recuperar el texto claro, por lo que se considera un cifrado muy seguro.

Las dos claves con que trabaja la clave pública pertenecen a la misma persona que envía el mensaje. El texto claro siempre se debe cifrar con la clave pública y descifrar con la privada, ya que de lo contrario casi cualquier persona podría descifrar el texto con la clave pública.

Este sistema se desarrolló para evitar el problema de intercambio de claves cuando se utilizan sistemas de cifrado simétricos.

En cambio, en el cifrado asimétrico no es necesario que remitente y receptor estén de acuerdo en las claves de cifrado y descifrado que van a em-

plear, ya que sólo se necesita que el remitente consiga la clave pública del destinatario; es decir, el emisor envía la clave secreta, la cual se ha generado en forma aleatoria y ha sido cifrada con la clave pública del receptor, que es el único capaz de descifrarla utilizando su clave privada, así que no importa que el texto claro se envíe por canales poco seguros, pues nadie podrá descifrarlo, sólo quien posea la clave privada correspondiente.

En cierto sentido, el cifrado de clave pública es más sencillo de utilizar porque hay una de las dos claves, la pública, que se distribuye de manera masiva, en tanto que la privada sólo la tiene el propietario, aunque necesita mayor tiempo de proceso que aquel que requieren los cifrados simétricos, debido a que el tamaño de la clave es una medida de la seguridad del sistema; por ejemplo, si el sistema de cifrado es de 56 bits se deben probar 2^{56} claves, ahora imaginemos la cifra que se obtiene cuando las claves públicas tienen cifradores de hasta 1024 bits.

No obstante, en la actualidad ya se han desarrollado claves asimétricas basadas en curvas elípticas que son menos costosas; éstas se basan en un logaritmo discreto, con lo cual se logran claves de menor tamaño, cuyo beneficio es el uso de menos memoria y menores recursos de hardware para el cifrado y descifrado. La forma de cifrar con una curva elíptica consiste en trazar en un plano bidimensional (ejes cartesianos) una elíptica, donde la curva está compuesta por n puntos, cada uno definido por los valores que adquiere ese punto en los ejes x y y. Estos puntos son la representación de una ecuación de grado 3 (potencia 3). En este caso, para descifrar el texto plano es necesario calcular todos los pares de puntos que forman la curva, lo cual es bastante complicado. Un hecho muy conocido en matemáticas es que para calcular problemas que impliquen potencias de n cifras es más sencillo hacerlo con logaritmos. Una curva elíptica puede tener tantas formas como ecuaciones se puedan plantear. En la figura 2.7 se observa una curva elíptica típica. Si f(x) es una función unidireccional de la elíptica, es relativamente sencillo calcular y dibujar la curva, lo complicado es calcular la inversa de esa función, que equivale a descifrar el mensaje.

El uso de cifradores basados en curvas elípticas se debe a que otorga a los mensajes una elevada confidencialidad, lo que significa que nadie más puede leer

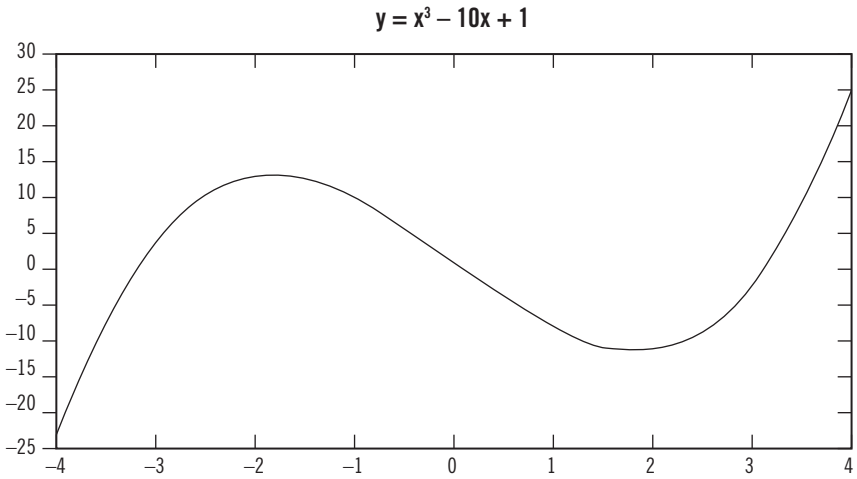
los mensajes cifrados excepto quien lo envía y el destinatario. De este modo, el texto no puede ser modificado, se mantiene íntegro, por lo que si nadie más lo ha podido leer, quien recibe el mensaje cifrado estará seguro de quién lo ha enviado.

Este tipo de cifrado es utilizado cada vez más por instituciones bancarias y de crédito, donde es muy importante mantener la secrecía de los números de cuentas o de NIP (número de identificación personal) que se solicita al utilizar tarjetas de crédito o de débito. Además, si el mensaje no es visible para nadie más que los interesados, no será posible modificar órdenes de retiro, transferencia de dinero o depósitos hechos a determinadas cuentas, y estas órdenes no podrán ser alteradas para beneficio de terceros.

El algoritmo de curva elíptica para firma digital es una variante del algoritmo de firma digital que utiliza curvas elípticas y que se basa en el algoritmo de ElGamal que funciona con un logaritmo discreto. La firma digital hace posible que una tercera parte imparcial sea la que verifique la autenticidad de un mensaje enviado a través de cualquier canal de comunicación.

La *fuerza de un protocolo criptográfico* se define en términos de su simétrico equivalente, y es una medida del nivel de dificultad para descifrar un texto cifrado, desde luego, sin tener la clave. El enfoque más común de criptoanálisis enfocado a descifrar la clave es usando la llamada *fuerza bruta,* término que significa el número de intentos hechos en determinado tiempo y el número de claves que se analizan antes de encontrar la que descifra el texto plano, lo cual es una medida del número de bits de la clave simétrica equivalente. Para el conocimiento y la fuerza bruta que se tiene hoy día, se considera que entre 128 y 256 bits le dan una fuerza mínima aceptable a una clave.

En Estados Unidos de América constituye un delito el no mantener la confidencialidad del número de seguridad social de un trabajador (además, también se considera una violación a las políticas internas de la empresa). En México, está penado legalmente hacer mal uso de los datos que una persona entrega a un banco o cualquier otra institución, cuando se tienen relaciones laborales o de negocio con esas instituciones. Si todos esos datos personales estuvieran cifrados, aunque una persona no autorizada tuviera acceso a las bases de datos, sería imposible que los pudiera leer y hacer mal uso de éstos, sin la clave correspondiente.



› **Figura 2.7**
Curva elíptica.

Por lo expuesto antes, se puede concluir que no existen sistemas de cifrado inviolables. Aunque algunos son mucho más difíciles de descifrar que otros, todos presentan puntos débiles, así como ventajas y desventajas. No se trata sólo de seleccionar aquel sistema que sea más seguro, puesto que muchas veces el hacer un sistema más seguro implica el uso de mucho mayores recursos de memoria y de hardware, los cuales elevan el costo de operación del sistema, que en ocasiones no compensa la preservación de la confidencialidad de los datos; por eso es mucho más costoso operar el sistema, que el valor que tiene cifrar y descifrar datos en términos del valor de la información que se maneja.

Cada día se desarrollan más y mejores sistemas de cifrado, cuyo objetivo es precisamente hacer que esos sistemas sean más seguros y disminuir el costo de su operación.

2.3 Administración y seguridad de los sistemas criptográficos

Todo el aspecto informático en torno al desarrollo de mejores y más baratos sistemas de cifrado se considera benéfico para todo tipo de empresas y público en general, en especial para todas aquellas personas que hacen compras, pagos

o transferencias de dinero por Internet. Sin embargo, es conveniente mencionar que todas las operaciones comerciales con mensajes cifrados en todo el mundo dependen de una adecuada gestión para su buen funcionamiento.

Gestión no es administración, sino que va más allá

Desde la década de 1950, en el mundo se creó la norma ISO (International Organization for Standardization), que desarrolló los Sistemas de Gestión de Calidad con la idea específica de establecer sistemas de mejora continua en las organizaciones, teniendo en cuenta a los directivos, los recursos de la empresa, la realización del servicio (o producto) y la medición, análisis y mejora de los procesos que coexisten en las organizaciones. La norma ISO 9000:2000 define a un sistema de Gestión de Calidad como:

> *Una parte del sistema de gestión de la organización enfocada en el logro de resultados, en relación con los objetivos de la calidad, para satisfacer las necesidades, expectativas y los requisitos de las partes interesadas, según corresponda.*

Los sistemas criptográficos son servicios disponibles a nivel internacional, en los que coexisten diferentes idiomas, diferentes idiosincrasias y, sobre todo, diferentes diseños de hardware, básicamente redes. Para que los millones de usuarios de sistemas criptográficos en todo el mundo tengan la certeza de que esos sistemas funcionan de la mejor manera posible, es necesario que dichos sistemas sean gestionados. Para lograrlo, se ha creado una serie de normas reguladoras, de las cuales sólo se mencionarán tres de las más conocidas y útiles.

Precisamente, ISO creó en 1980 el modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés; Open Systems Interconnection), como un marco de referencia para definir todo tipo de arquitecturas para la interconexión de sistemas de comunicaciones, casi como una necesidad, cuando la mayoría de las empresas en todo el mundo empezó a desarrollar todo tipo de redes de comunicación, creándose un caos, no sólo por el acelerado crecimiento de las redes internacionales, sino porque con éstas también surgió el problema de la diferencia de idioma y diferentes especificaciones técnicas. Cada proveedor de

redes tenía sus propias reglas. Por tanto, se trató de hacer que todas las redes, de cualquier proveedor, fueran compatibles en cualquier país, con lo cual se logró que la comunicación fuera efectiva en las redes a nivel mundial.

Como todos los documentos de ISO, lo que publicó fue una norma que define siete capas o etapas de cada una de las fases por las que deben pasar los datos para que transiten de un sitio a otro a través de una red de comunicaciones, y se crearon los protocolos respectivos para cada fase, de manera que sin importar el tipo de red y el proveedor de tecnología, todos entendieran que era necesaria una estandarización en la forma de comunicarse; de lo contrario, el proveedor que no se sujetara a la norma, simplemente su tecnología no sería útil para la comunicación internacional con cualquier otro proveedor; así, la nueva norma no tomó mucho tiempo en ser aceptada.

Las capas del modelo son los siguientes:

1. **Capa física.** Define la topología de la red y la forma en que se debe conectar cualquier computadora hacia la red, lo cual incluye tanto al medio físico (tipos de cable, tipo de conectores y características de la interfaz etc.), como a la forma de transmitir la información.
2. **Capa de enlace de datos.** Define con mucha puntualidad los protocolos necesarios para el control de flujo de datos, detección de errores y direccionamiento de los datos, tanto entre computadoras, como entre toda la red. Estos protocolos se deben seguir en cualquiera de las fases del modelo.
3. **Capa de red.** Los protocolos juegan un papel muy importante en este aspecto, pues aquí es donde se determina la ruta que seguirá la información y cuál será la información que viajará por determinada ruta. Esta capa asegura que la información enviada desde cualquier computadora siempre llegue al destino deseado, nacional o internacional, por medio de un direccionamiento lógico seleccionando la ruta más adecuada.
4. **Capa de transporte.** Como su nombre lo indica, analiza todos los aspectos para que los datos sean transportados de manera adecuada desde de su

origen hasta su destino exacto, sin importar el tipo de red, la cual puede ser física, como una LAN en una empresa, o a través de Internet hasta otro continente.

5. **Capa de sesión.** Cuando se establece un enlace con otra computadora, a dicho enlace se le llama sesión. Durante la sesión, entre las dos computadoras se realizan determinadas operaciones, como el envío de mensajes o el envío de paquetes de información. Esta capa asegura que la sesión, léase operaciones efectuadas entre computadoras, termine a satisfacción de las dos partes, transmisora y receptora, aunque la comunicación pueda interrumpirse por falta de tiempo de alguna de las partes, por falta de energía eléctrica o por cualquier otra causa; al final, todas las operaciones se deberán completar.

6. **Capa de presentación.** Es la responsable de que tanto el transmisor como el receptor de la información entiendan a cabalidad el diálogo que establezcan. A pesar de que la tecnología que cada uno utilice tenga diferente representación de los caracteres de los datos, básicamente estandariza la sintaxis y la semántica del lenguaje que se está transmitiendo. Asimismo, también puede comprimir datos sin que éstos pierdan sus propiedades lingüísticas.

7. **Capa de aplicación.** Esta capa garantiza que todas las aplicaciones de una computadora tengan acceso a los servicios que ofrecen las otras fases del modelo, lo que logra por medio de protocolos. De esta manera, hay un protocolo para cada aplicación, y siempre debe crearse uno nuevo para cada nueva aplicación que esté disponible; así, hay protocolos para servicio de Internet, para tener acceso a bases de datos o a archivos, etcétera. Todos los protocolos se manejan de manera automática en cuanto el usuario solicita determinada aplicación.

Actividad de aprendizaje

En equipo de dos o tres personas elaboren una presentación electrónica donde expliquen las siete capas por las que deben pasar los datos para que transiten de un sitio a otro a través de una red de comunicaciones. Expongan su trabajo frente al grupo.

Por otro lado, también se encuentra la Norma ISO 11770-1:2010, que define un modelo general para administrar claves, independientemente de que el usuario utilice un algoritmo determinado; sin embargo, si el usuario en realidad utilizará algoritmos asimétricos, para los cuales se requiere una clave pública, entonces la distribución de claves tiene ciertas especificaciones. Esta norma especifica los aspectos de la administración manual y automática de claves; por ejemplo, si la clave se obtiene on-line, la norma describe todas las operaciones que deben realizarse para obtener la clave, aunque no declara los detalles del protocolo necesario. Además, esta norma no define las políticas de seguridad que deben estar subyacentes a la consecución de una clave pública o privada.

Por la importancia de las claves manejadas, se han definido tres niveles:

1. Las de mayor secrecía o claves maestras, cuyo cambio no es tan frecuente y se entregan en forma manual.
2. Las de clave encriptada.
3. Las claves de datos que se envían on-line, las cuales se cambian a diario e incluso por sesión.

Existe un formato llamado Mensajes de Servicio Criptográfico que sirve para establecer las nuevas claves que reemplazarán a las que están en uso.

Otro apartado de ISO para el control de cifrado es el 27001-2013. Esta norma tiene dos áreas principales: la política para el uso del cifrado y la administración de claves. Tiene como objetivo describir los aspectos que se deben considerar para implantar en cualquier organización una política de cifrado, a fin de otorgar a la información las características de confidencialidad, integridad y autenticidad necesarias, debido a que ciertos datos, por su importancia, requieren de una protección especial que puede proporcionar el cifrado de esos datos.

La norma ISO/IEC 27001:2013 contiene los requisitos para establecer, implementar, mantener y determinar la mejora continua de un sistema de administración de la seguridad de la información dentro de cualquier tipo de

organización. También contiene los requisitos para la evaluación y el tratamiento de los riesgos a los que está expuesta la información; requisitos que se pueden ajustar en forma específica a las necesidades de la organización. Todos los requisitos de esta norma son genéricos, ya que es posible aplicarlos a cualquier tipo de organización, sin importar giro, tamaño o naturaleza de la organización.

La norma incluye los procesos que deben realizarse para la generación, el almacenamiento, la distribución, la eliminación y el archivado de claves, de acuerdo con la política de seguridad que se siga, además de que está relacionada con la infraestructura de seguridad para sistemas abiertos, que describe las características de los mecanismos que cubren diferentes aspectos de la seguridad.

Otro estándar para la administración de claves en las instituciones financieras es el que desarrolló el American National Standards Institute, conocido con el nombre de ANSI X9.17, el cual se enfoca en la distribución de claves secretas que utilizan técnicas simétricas de cifrado y define los protocolos que utilizan estas instituciones para transferir las claves cifradas. Tal vez ese tipo de instituciones, por el volumen de documentos cifrados que manejan, son las que necesitan cambiar las claves a diario, y en algunos casos hasta por sesión.

Otro algoritmo que también contribuye a mantener la integridad de los datos es el algoritmo de seguridad Hash, que constituye un proceso de cifrado para pasar de un bloque arbitrario de datos a una cadena de bits de tamaño fijo. Este algoritmo es una forma de validar que un archivo dado no ha cambiado desde que fue creado su algoritmo Hash. Esto es muy importante cuando se comparten aplicaciones y archivos de dominio público, pues en estos casos lo que interesa es la integridad de los archivos, mismos que pueden validarse en cualquier momento. Un algoritmo similar es el Message Digest, que trabaja de manera muy similar a un algoritmo Hash. Ambos algoritmos han sido publicados por el NIST.

A continuación se mencionan las normas ISO relacionado con la Seguridad Informática:

- **ISO/IEC 7498-1:1994.** Tecnología de la información. Interconexión de sistemas abiertos. Modelo básico de referencia.

- **ISO/IEC 9798-1:2010.** Tecnología de la información. Técnicas de seguridad. Requisitos de una entidad de autenticación. Parte 1.
- **ISO/IEC 9798-2:2008.** Tecnología de la información. Técnicas de seguridad. Requisitos de una entidad de autenticación. Parte 2. Mecanismos para la utilización de algoritmos de cifrado simétrico.
- **ISO/IEC 11770-1:2010.** Tecnología de la información. Técnicas de seguridad. Administración de claves. Parte 1. Infraestructura.
- **ISO/IEC 11770-2:2008.** Tecnología de la información. Técnicas de seguridad. Administración de claves. Parte 2. Mecanismos que utilizan técnicas simétricas.
- **ISO/IEC 11770-3.** Tecnología de la información. Técnicas de seguridad. Administración de claves. Parte 3. Mecanismos que utilizan técnicas asimétricas.
- **ISO/IEC 13157-1.** Tecnología de la información. Telecomunicaciones e intercambio de información entre sistemas. Seguridad NFC. Parte 1. NFC-SEC NFCIP-1 protocolo y servicios de seguridad.
- **ISO/IEC 13157-2.** Tecnología de la información. Telecomunicaciones e intercambio de información entre sistemas. Seguridad NFC. Parte 2. NFC-SEC utilizando el estándar de cifrado ECDH y AES.
- **ISO/IEC 13157-3.** Tecnología de la información. Telecomunicaciones e intercambio de información entre sistemas. Seguridad NFC. Parte 3. NFC-SEC utilizando el estándar de cifrado ECDH-256 y AES-GCM.
- **ISO/IEC 14443-3.** Tarjetas de identificación, tarjetas de circuito integrado sin contacto físico. Tarjetas de proximidad. Parte 3. Inicialización y anticolisión.
- **ISO/IEC 18031:2011.** Tecnología de la información. Técnicas de seguridad. Generación aleatoria de bits.
- **ISO/IEC 18031:2011/Cor.1:2014.** Tecnología de la información. Técnicas de seguridad. Generación aleatoria de bits. Corrección técnica 1.
- **ISO/IEC 18033-3:2010.** Tecnología de la información. Técnicas de seguridad. Algoritmos de cifrado. Parte 3. cifradores de bloque.

- **ISO/IEC 18092.** Tecnología de la información. Telecomunicaciones e intercambio de información entre sistemas. Comunicación de proximidad de campo. Interface y protocolo NFCIP-1.
- **ISO/IEC 19772:2009.** Tecnología de la información. Técnicas de seguridad. Autenticación del cifrado.
- **ISO/IEC 19772:2009/Cor.1:2014**. Tecnología de la información. Técnicas de seguridad. Procedimiento de autenticación.

Como se puede observar, hay decenas de Normas ISO que abarcan todos los aspectos de la seguridad informática y que fueron creadas para lograr una mejora continua de la calidad, de manera que en cuanto a seguridad informática lo que se busca es que, cada vez que se realice alguna actividad relacionada, ésta sea mejor que la anterior; asimismo, también se busca que se haga lo que dice la organización que está haciendo, y si lo hace, se espera que la calidad de la seguridad mejore.

También debe observarse que para que un sistema de seguridad informática funcione en forma adecuada no basta con desarrollar un algoritmo que supere a cualquiera de los ya existentes o que se tenga una infraestructura computacional para realizar miles de millones de cálculos para descifrar el algoritmo más seguro. Más allá de esto, que desde luego es necesario, se requiere saber cómo gestionar y operar administrativamente un sistema de seguridad informática.

Actividad de aprendizaje

En equipo de dos personas elaboren un póster donde presenten las normas ISO relacionado con la Seguridad Informática. Sean creativos en su diseño y presentación. Expongan sus trabajos.

Comprueba tus saberes

Responde cada una de las siguientes cuestiones.

1. Describe con tus propias palabras el significado del término *criptografía*.

2. Menciona las dos categorías generales de los criptogramas por sustitución.

3. ¿Qué es un criptograma por sustitución monoalfabético monográmico? Explícalo con la ayuda de un mapa mental.

4. Describe con detalle el funcionamiento de, al menos, dos criptogramas antiguos.

5. Con base en el funcionamiento del criptograma de los hierofantes, construye tu propio criptograma y envía algunos mensajes a un compañero.

6. Describe el funcionamiento del cifrador de Hill.

7. Describe en forma detallada las cuatro reglas para cifrar con el método de Playfair.

8. ¿Cuál fue la aportación Claude Shannon al cifrado de textos?

9. ¿Qué es un digrama y un trigrama? Menciona al menos tres ejemplos de cada uno.

10. Explica con tus propias palabras, ¿por qué son importantes los digramas y trigramas al descifrar un mensaje?

11. Describe en qué consisten los cifradores DES y TDES. Señala las diferencias entre éstos.

12. Menciona las diferencias entre un cifrado simétrico y un cifrado asimétrico.

13. Describe el cifrador AES.

14. Menciona al menos tres operaciones que se ejecutan al momento de cifrar con DES.

15. ¿Qué ventajas tiene sobre los otros métodos utilizar una curva elíptica para cifrar un texto?

16. ¿Qué son las ISO y cuál es su importancia en la criptografía?

17. Describe qué es el modelo OSI de ISO.

18. Elabora un esquema donde presentes las siete fases que contiene el estándar OSI de ISO.

19. Describe con tus propias palabras el estándar ANSI X9.17.

20. Describe con tus propias palabras qué es un algoritmo Hash de seguridad.

Referencias bibliográficas

1. Serie ISO 9000:2000. Sistemas de Gestión de Calidad. Recomendaciones para la mejora del desempeño.
2. Serie ISO 27000:2010. Sistemas de Seguridad Informática. Recomendaciones para la mejora del desempeño.
3. Zimmerman, Hubert. (1980) OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications.

Referencias electrónicas

1. http://www.abcdatos.com/tutorial/criptografia-curvas-elipticas.html
2. http://sistemasumma.com/2010/09/02/algoritmo-de-encriptacion-des/
3. http://es.wikipedia.org/wiki/Advanced_Encryption_Standard
4. http://www.codeplanet.eu/files/flash/Rijndael_Animation_v4_eng.swf
5. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
6. http://es.wikipedia.org/wiki/RSA
7. http://www.rsa.com/rsalabs/node.asp?id=2093
8. http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/#sthash.g49rE2Aj.dpuf
9. Worldlingo. Modo De Operación De La Cifra Del Bloque, [Seriada en línea]. Pág.2-4. Disponible en: URL:http://www.worldlingo.com/ma/enwiki/es/Block_cipher_modes_of_operation,[2010]

3

Objetivo general

Que el estudiante comprenda qué son y cómo funcionan una PKI y una PMI y cuál es su importancia en el comercio internacional.

Objetivos específicos

- Conocerás y comprenderás los tipos de certificados que existen en las transacciones internacionales de negocios.
- Conocerás y comprenderás el funcionamiento administrativo de la infraestructura de una PKI y de una PMI.
- Comprenderás cuál es el papel de las autoridades reguladoras de la emisión de certificados y cuáles son las políticas que aplican.

Características de una PKI y de una PMI

¿Qué sabes?

- ¿Sabes que es un certificado y para qué sirve?
- ¿Conoces los procedimientos para obtener un certificado de identidad?
- ¿Sabes qué es la norma X.509?
- ¿Conoces los protocolos para administrar, gestionar, crear, distribuir, almacenar y revocar certificados digitales (PKI)?
- ¿Cuál es la función de la administración de privilegios (PMI) y cómo funciona?
- ¿Sabes qué es un atributo y cómo se genera una clave de atributo?

Competencias a desarrollar

- El estudiante identifica la seguridad informática que prevalece al realizar negocios internacionales por Internet.
- El alumno describe con sus propias palabras las normas y estándares que se han adoptado a nivel internacional para incrementar la seguridad informática al realizar negocios con otros países.

3.1 Introducción

Desde hace unos 20 años es bien sabido que un uso más intensivo de las TIC (Tecnologías Informáticas y de la Comunicación) en una empresa u organización propicia que la información viaje mucho más rápido a lo largo de una cadena de suministros (véase capítulo 1, Generalidades de la seguridad informática); si la información viaja más de prisa, en consecuencia también se incrementa la productividad de la empresa y con ello aumenta el flujo de dinero y, por tanto, las ganancias monetarias.

Las TIC están formadas por cinco agrupaciones genéricas de TI:

1. **Software.** Son todos los programas, sistemas operativos, base de datos, paquetes comerciales y lenguajes de programación.
2. **Hardware.** Son todos los dispositivos físicos.
3. **Humanware.** Incluye a todo el personal involucrado en la manipulación, uso, operación, programación y explotación de los recursos computacionales.
4. **Netware.** Son todos los elementos y medios de comunicación y transferencia de datos, voz, imágenes, sonidos y textos.
5. **Supportware**. Comprende todo lo relacionado *y/o* involucrado en el mantenimiento y la actualización de toda la estructura tecnológica.

Pero no sólo se trata de contar con las TIC, desde luego incluyendo a la parte humana; también es necesario regular y normalizar el funcionamiento de las redes mundiales, en especial la comunicación que se establece durante el proceso de dicho comercio electrónico. Las normas, sin duda, facilitan el funcionamiento eficaz de las redes internacionales actuales; no obstante, para la realización de un trabajo conjunto óptimo, también se ha incrementado en gran medida el uso de protocolos, interfaces abiertas, aplicaciones del más diverso tipo y plataformas con nuevos usos. Aun cuando los diseñadores de estos dispositivos aseguran que sus protocolos y sistemas son inviolables, el

increíble y acelerado aumento de estos nuevos sistemas y protocolos también ha provocado un incremento en las amenazas a los que pueden estar expuestos y nuevos tipos de riesgos que pueden enfrentar. Hoy día, la infraestructura de comunicación global debe ser abierta, lo que trae como consecuencia que esté más expuesta a problemas de seguridad.

Por tanto, a fin de combatir, o al menos contrarrestar en forma parcial estos problemas, es necesaria la normalización en la infraestructura de las telecomunicaciones, los protocolos, las aplicaciones y la gestión de las redes; sin embargo, como se dijo antes, gestionar va mucho más allá de administrar.

La infraestructura de clave pública debe integrar tanto el cifrado de la clave pública o asimétrica, utilizada en la generación de la firma digital, como el cifrado de la clave simétrica que se utiliza para el cifrado y el Hash, también llamado Message Digest; además, debe también administrar una distribución segura de las claves públicas y privadas.

Este capítulo muestra cómo se lleva a cabo la gestión de redes mundiales de comunicación, la infraestructura necesaria para hacerlo, cómo se ha logrado estandarizar su funcionamiento y cuáles son los instrumentos que se han desarrollado para su control.

3.2 ¿Cómo empezó todo?

Imagina algunas situaciones cotidianas en la vida de la mayoría de las personas adultas. En la primera, supóngase que una persona desea retirar dinero de un cajero automático; para hacerlo, hay tres condiciones indispensables, la primera es que la tarjeta utilizada para el retiro del dinero sea auténtica; para ello, el mismo cajero automático emprende una verificación para su comprobación, mientras en la pantalla aparece el mensaje: "Verificando chip". Durante dicha comprobación, el cajero automático verifica que la tarjeta haya sido emitida por el banco, lo cual es cierto si identifica que el chip pertenece a dicha institución bancaria. La segunda condición es teclear el NIP (número de identificación personal) correcto. El cajero permite cierto número de intentos

para introducir el NIP correcto, después de fallar esos intentos, el cajero ya no concede más oportunidades. La tercera condición es que la tarjeta tenga suficientes fondos para proporcionar la cantidad solicitada de dinero.

En la segunda situación, supóngase que una persona acude a la sucursal de una institución bancaria a cambiar un cheque por una suma elevada de dinero, el cual está a su nombre. Los pasos que debe seguir, en orden estricto, el cajero que atiende a la persona en cuestión son:

1. Solicitar una identificación oficial vigente con fotografía. En México sólo se aceptan como identificaciones oficiales el pasaporte vigente, la cédula profesional y la credencial para votar emitida por el INE (Instituto Nacional Electoral), las cuales son expedidas por oficinas del gobierno federal. En las instituciones bancarias de México de ningún modo se aceptan como identificación la licencia de conducir o cualquier otro documento oficial.
2. Verificar que el nombre de la identificación presentada y el nombre que aparece escrito en el cheque sean exactamente iguales, de lo contrario le será imposible pagar el documento a la persona que lo solicitó.
3. Pasar el cheque a través de una banda magnética, cuya función es verificar que el documento sea auténtico, ya sea de ese banco o de otra institución.
4. Comparar en forma visual si la firma del emisor del cheque coincide con la firma del titular de la cuenta de cheques que tiene registrada el banco en su base de datos.
5. Verificar que la cuenta bancaria del emisor del cheque tenga los fondos suficientes para pagar la cantidad de dinero solicitada.
6. Pagar el cheque.

Conforme a lo anterior, es digno de observar todas las actividades de verificación de datos e identidad que debe efectuar el cajero de un banco antes de pagar un cheque, con el único fin de evitar que la institución bancaria sea defraudada al entregar dinero a la(s) persona(s) equivocada(s).

Por lo común, la autenticación de la identidad del usuario la hace el personal de ventanilla del banco; sin embargo, ésta se basa en una identificación avalada por el gobierno del país. La otra identificación (la de la firma del emisor del cheque), así como la verificación de fondos suficientes disponibles en la cuenta de cheques, desde luego está a cargo del banco.

Ahora considérense dos situaciones menos frecuentes. En una imagínese a un turista que viaja a un país donde la moneda oficial en circulación no es la misma que la de su país de origen. Si durante su viaje a aquel país, la persona quiere comprar o pagar algo, lo puede hacer de dos maneras distintas, bien puede llevar dinero en efectivo (dólares estadounidenses, euros, yenes, etc.) y pagar todo con la moneda en circulación, aunque en este caso si le roban o pierde su dinero se verá en verdaderos problemas en un país ajeno; o bien puede pagar con diversos tipos tarjetas con el logotipo de Master Card, Visa o algún otro aceptado a nivel internacional; en este caso, la operación que se realiza en el extranjero con el pago de tarjeta es exactamente igual a aquella que se efectúa en su propio país; es decir, al comprar en el otro país es como si lo estuviera haciendo en su lugar de origen. Además, si durante su viaje el turista realiza una compra en euros, tiene la ventaja de que el cargo que tenga en su tarjeta no lo pagará en euros sino en la moneda oficial de su país de origen. Otra ventaja es que si le roban o pierde su tarjeta en otro país, la mayoría de los bancos se la pueden reponer en muy poco tiempo en el país donde se encuentre el turista.

En la siguiente situación imagínese a un industrial mexicano que compra materia prima en China. Con base en muchos factores, se puede decir, con toda seguridad, que dicho empresario no efectuará la compra por única vez (aunque cabe la posibilidad de que así sea), además de que también es seguro que no pagará en efectivo. Para realizar este tipo de transacciones, en general existen ciertos mecanismos o protocolos bancarios que deben llevarse a cabo. En esta situación, lo primero que sucederá es que el vendedor chino, después de hacerle saber al comprador mexicano el monto de la venta, deberá especificarle si el pago lo requiere en yuanes (moneda oficial china), dólares, euros o en cualquier otra moneda. También deberá informarle al comprador en qué banco tendrá que hacer el depósito del pago y el número de cuenta,

pues por lo común la mercancía no se envía hasta que el pago esté totalmente liquidado.

Por su parte, el comprador mexicano, antes de realizar el pago, deberá verificar con total certeza varios aspectos. Primero, que el número de cuenta bancaria en la que se depositará el pago sea el correcto y que esté a nombre de la empresa china proveedora de materia prima. Luego, deberá confiar en que la institución bancaria de su país hará el envío de dinero en forma correcta al banco correcto y al número de cuenta correcta. El banco mexicano, por su parte, tendrá que informarle al empresario mexicano en cuánto tiempo la empresa china tendrá disponible el dinero de la compra en el banco indicado por la empresa china. Pasado dicho tiempo, el comprador mexicano deberá verificar con la empresa china que ya comprobó que el pago de materia prima se hizo de manera correcta, y hasta entonces procederá al envío de la mercancía.

Imagina los peores escenarios que le pueden suceder al comprador mexicano:

- El dinero se envió a una cuenta equivocada.
- No se envió la cantidad correcta de dinero.
- El banco chino o cualquier otro banco recibió el dinero, pero éste desapareció; es decir, se trataba de un banco "fantasma".
- El vendedor chino sostiene, luego de un tiempo, que no tiene disponible el dinero en el banco, a pesar de que el comprador mexicano siguió todas las instrucciones e hizo lo correcto.

Nuevamente, como se observa en este caso, el éxito de todo el proceso de venta, pago y entrega de mercancía depende de una serie de verificaciones y autenticaciones de la identidad de los participantes, a saber: el vendedor chino, el comprador mexicano (ambos personas físicas) y el banco mexicano que hace la transferencia de dinero al banco chino que recibe el dinero y lo transfiere a la cuenta del vendedor chino.

Todas las actividades de comercio internacional que se han descrito antes han existido desde hace cientos de años. Sólo que antaño, los procedimientos

de transferencia de fondos de las instituciones bancarias, aunque eran muy seguros resultaban muy lentos.

El comercio internacional globalizado e intenso inició en la década de 1990, con la firma de múltiples tratados internacionales de libre comercio entre diversos países del mundo. En aquel momento, las TIC se encontraban en pleno desarrollo; sin embargo, aún no estaban preparadas para intervenir y ser el motor que detonara un comercio internacional más intenso. Para ello era indispensable acelerar una forma de pagos internacionales entre empresas con todos los protocolos de seguridad necesarios. Pero también era necesario que todas las operaciones de comercio local e internacional se hicieran en la misma forma, es decir, era indispensable la estandarización de las actividades bancarias para la transferencia internacional de dinero, pues de lo contrario, en el caso del empresario que compra materia prima a una empresa china, el banco mexicano tendría procedimientos administrativos propios para la transferencia de fondos, los cuales podrían ser diferentes a los del banco chino o de otros países, y esto provocaría enormes dificultades y costos a los participantes de este tipo de transacciones.

Se tiene registro de que los primeros esfuerzos de estandarización en las comunicaciones iniciaron en 1865 con la creación de la Unión Telegráfica Internacional (ITU, por sus siglas en inglés). Por otro lado, en 1956, en Francia se creó el Comité Consultivo Internacional para la Telefonía y la Telegrafía (CCITT, por sus siglas en francés), aunque en 1992 cambió su nombre a ITU-T. Sin embargo, fue en 1925 que la ITU original inició el análisis de los servicios de telefonía internacional y de la telegrafía de larga distancia en París.

Hacia 1992, la ITU agregó una T a su nombre, de este modo se convirtió en la ITU-T, y de ser la Unión Telegráfica Internacional pasó a ser la Unión Internacional de Telecomunicaciones, con lo que se constituyó en el sector de estandarización de las telecomunicaciones, uno de los tres sectores de la ITU, y aunque sus siglas son las mismas, ITU, tiene un significado distinto. La misión de la ITU-T es asegurar la producción eficiente y oportuna de los estándares que conciernen a todas las comunicaciones mundiales, además de definir las tarifas y los principios contables que se aplicarán por el servicio internacional de telecomunicaciones.

En 1983, con la aparición en el mercado de las computadoras personales, empezaron a adoptarse tecnologías poco confiables, con un alto costo de operación; de hecho, en esa época el correo electrónico era considerado un recurso costoso y poco confiable, pues carecía de consenso general, ya que no se sabía hacia y hasta dónde iba a dirigirse esa nueva herramienta. Considera que Internet venía de Arpanet, de uso militar en Estados Unidos de América, y apenas empezaba a utilizarse entre los civiles, con la consiguiente resistencia al cambio de parte de los industriales cuando aparecen nuevas y revolucionarias tecnologías.

Sin embargo, en 1992, con la ITU-T ya en funcionamiento, se elaboraron los primeros estándares de comunicación a los que se les dio el nombre de *Recomendaciones*, término que aún sigue vigente hasta la fecha, sólo que ahora dichas recomendaciones se han hecho obligatorias cuando son adoptadas por un país que utiliza las redes internacionales de comunicación. La ITU-T trabaja en forma conjunta con la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y con la Fuerza de Trabajo de Ingeniería en Internet (IETF, por sus siglas en inglés), entidad que ha promovido toda la estandarización en el uso de Internet y ha generado, entre otras cosas, el protocolo TCP/IP; para su operación, esta organización siempre ha tenido el apoyo del gobierno de Estados Unidos de América.

Con la urgente necesidad de estandarizar las telecomunicaciones en todo el mundo debido al crecimiento exponencial del comercio mundial, con el aumento sustancial de las economías globalizadas en la mayoría de los países y con el apoyo de los organismos citados, en 1988 la ITU-T publicó la primera serie de estándares para redes de computadoras, llamada X.500, que cubre los servicios de un directorio electrónico, el cual apoya los requisitos de la serie de estándares X.400 sobre correo electrónico. El estándar X.400 fue incorporado a la suite de protocolos de Interconexión de Sistemas Abiertos (OSI, por sus siglas en inglés), así que se le puede identificar en ISO como ISO/IEC 9594. Por su parte, la suite de protocolos de Interconexión de Sistemas Abiertos, publicada en 1977, intenta estandarizar la red de computadoras a nivel mundial.

En 1991, Philip Zimmermann desarrolló el software PGP o software de *muy buena privacidad*, que se utiliza para el cifrado asimétrico o de clave pública,

la firma digital y la autenticación; es un software libre y relativamente sencillo de utilizar por cualquier tipo de usuario; Zimmermann es considerado uno de los primeros estudiosos en desarrollar un software de cifrado asimétrico (clave pública), para enviar información por Internet de manera más segura, mediante el uso de la autenticación de documentos por medio de firmas digitales.

Se puede decir que el sistema de cifrado de Zimmermann combina técnicas de cifrado simétrico y asimétrico, con el objetivo de aprovechar la rapidez del cifrado simétrico ya que permite una distribución de claves de forma más segura, además de garantizar el no repudio de los datos y la no suplantación. El sistema comprime el texto y genera una clave única por sesión que sólo se utiliza una vez, de manera que si alguien la llegara a descubrir, esta sería inútil en sesiones posteriores; se utiliza con un algoritmo simétrico del tipo 3DES (Triple DES) para cifrar el texto claro.

Por otro lado, el GNU (Good Privacy Guard), también llamado GPG, es una herramienta que ha reemplazado al sistema de cifrado PGP. Desde luego, éste también es un sistema de cifrado y firmas digitales, sólo que, a diferencia de PGP, GPG es un software libre, por lo que también se le conoce como General Public Licence; hasta hoy, se considera la licencia más utilizada, ya que garantiza a los usuarios la posibilidad de usar, estudiar, copiar y mejorar el software si alguien lo puede hacer, aunque cuando alguien lo logra, está obligado a distribuir la versión mejorada bajo los términos de la misma licencia, y de hecho está protegido para que otra persona no pueda apropiarse de la patente. Pero para que Zimmermann lograra desarrollar el PGP y pudiera utilizarse el PGP, la ITU-T tuvo que trabajar arduamente.

En este punto conviene recordar dos cosas. Primero, como se trata en el capítulo 2 (Criptografía), el cifrado simétrico y el cifrado asimétrico requieren de actividades de autenticación y de claves públicas y privadas. En los ejemplos que se citan en este capítulo acerca de personas que retiran dinero en cajeros automáticos, cobran un cheque o llevan a cabo actividades de comercio internacional se evidencia la necesidad de identificar a los usuarios y de autenticar una serie de características en las operaciones que realizan. A esas mismas necesidades se enfrentó la ITU-T, por lo que tuvo que desarrollar no sólo nuevos conceptos, sino también crear una serie de entidades capacitadas

para emitir los comprobantes de identidad en todo el mundo. Por ejemplo, en México, para cobrar un cheque en un banco se solicita una identificación oficial y las únicas identificaciones aceptadas son el pasaporte vigente, la cédula profesional o la credencial de elector emitida por el Instituto Nacional Electoral (antes IFE). Ahora bien, para operaciones bancarias a nivel mundial, ¿cuál sería una identificación válida y quién la emitiría, a fin de que los bancos de todo el mundo que realizaran operaciones de comercio internacional aceptaran como válidas dichas identificaciones?

Por lo anterior, la ITU-T, como parte de sus trabajos de normalización internacional, desarrolló una serie de conceptos y herramientas informáticas, cuya función es sustituir todas aquellas actividades que realiza la persona detrás de la ventanilla de un banco o aquellas funciones que ejecuta un cajero automático para otorgar dinero al poseedor de una tarjeta de crédito o débito. La mayoría de las personas que realizan operaciones con bancos comerciales están tan acostumbradas a dichas operaciones, que rara vez se detienen a pensar que todos los bancos han diseñado una serie de protocolos o actividades que deben seguirse para atender a los clientes que solicitan algún servicio.

El trabajo realizado por la ITU-T desde su creación es muy similar a dichos protocolos bancarios, excepto que en el caso de la ITU-T y del comercio internacional, la atención a clientes es por completo despersonalizada (es decir, no intervienen personas); los protocolos que ha desarrollado son válidos en todos los países que de manera voluntaria han aceptado estas normas, las cuales permiten el envío de información y datos de manera segura en todo el mundo. Como parte de sus protocolos bancarios, la ITU-T ha desarrollado los siguientes conceptos.

Actividad de aprendizaje

Elabora una línea del tiempo donde presentes la evolución de la ITU-T desde su creación hasta nuestros días. Entrégala a tu profesor.

3.3 Definición de conceptos

A continuación se presenta una serie de conceptos importantes que deben considerarse a lo largo del texto.

¿Qué es un certificado?

Si es emitido por una autoridad de certificación, un certificado es una confirmación de identidad y contiene información que se utiliza para proteger datos o establecer conexiones seguras de red. De este modo, el almacén de certificados, como su nombre lo indica, es el área del sistema donde se guardan los certificados.

Los propósitos que tiene la emisión de un certificado se listan a continuación:

- Asegurar la identidad de un equipo remoto.
- Probar su identidad ante un equipo remoto.
- Proteger los mensajes enviados por Internet (correos).
- Confirmar que el software procede de un editor de software.
- Proteger al software de alteraciones después de su publicación.
- Permitir que se cifren los datos en el disco.

Cuando el certificado emitido cumpla con su propósito, debe contener los siguientes datos:

- Versión del certificado.
- Número de serie.
- Algoritmo de firma.
- Algoritmo Hash de firma.
- Periodo de validez.
- Clave pública (por ejemplo, RSA de 2048 bits).
- Uso que se le dará a la clave (por ejemplo, para firma de certificados).
- Algoritmo de identificación.

- Huella digital.
- Nombre descriptivo.
- Autenticación del servidor.

Dependiendo de la información que contiene y el nombre del propietario del certificado, existen varios tipos de certificado. Son los siguientes:

- **Certificado personal.** Acredita la identidad del titular.
- **Certificado de pertenencia a empresa.** Además de la identidad del titular, acredita su vinculación con la entidad para la que trabaja.
- **Certificado de representante.** Además de la pertenencia a una empresa, acredita los poderes de representación que el titular tiene sobre la misma.
- **Certificado de persona jurídica.** Identifica a una empresa o sociedad y la autoriza a realizar trámites legales ante las administraciones o instituciones gubernamentales.
- **Certificado de atributo.** Permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal.
- **Certificado de servidor seguro.** Se utiliza en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- **Certificado de firma de código.** Garantiza la autoría y la no modificación del código de aplicaciones informáticas.

Para enviar un certificado están disponibles varios formatos de exportación de archivos, algunos de los más usados son:

- Estándar de sintaxis de cifrado de mensajes, certificado PKCS No. 7.P7B.
- X.509 codificado base 64 (.CER).
- DER binario codificado X.509 (.CER).

Un certificado de cualquier tipo tiene un formato general (véase tabla 3.1); dependiendo del tipo de certificado, en éste se agregan o se suprimen algunos datos, aunque en la última casilla siempre aparecerá la firma de la autoridad correspondiente; por ejemplo, si el certificado es de atributos, debe aparecer la firma de la autoridad de atributos. Algunos datos, como el algoritmo de cla-

ve pública y la misma clave, siempre aparecen en un certificado de identidad, pero no están presentes en un certificado de atributos. El formato general debe ser compatible con el estándar ISO/IEC 9594-8.

Tabla 3.1 Formato general de un certificado

Formato general
Versión
Núm. de serie
Algoritmo de firma
Periodo de validez
Propietario del certificado
Atributos
Identidad del emisor
Algoritmo de clave pública
Firma del emisor

Con los datos que se muestran en un certificado, la PKI verifica que el usuario es quien dice ser, ya que el usuario posee un certificado de atributos emitido por una autoridad de atributos, cuyas funciones y concepto pertenecen a una Infraestructura de Administración de Privilegios (PMI, por sus siglas en inglés).

En todos los países afiliados existen prestadores de servicios autorizados para expedir certificados de todos los tipos que hay, y que se describieron en párrafos anteriores. Es muy común que si un usuario paga por varios servicios, adquiere cualquier certificado en forma gratuita; de lo contrario, su costo puede fluctuar entre 15 y más de 1 000 USD (dólares estadounidenses) por año, si se requiere continuamente de varios tipos de certificados.

Actividad de aprendizaje

En equipo de dos o tres personas elaboren una presentación electrónica donde presenten, ¿qué es un certificado? Expongan sus trabajos frente al grupo.

Certificado digital

Un certificado digital, también conocido como certificado electrónico o certificado de clave pública, es un archivo creado por una organización, pública o privada, que ofrece servicios de certificación; dicha organización crea los datos de identidad de una persona física o moral, y de esa forma le otorga una identidad digital en Internet. Como este certificado da la categoría de autenticidad a un usuario o a un sitio web en Internet, se requiere una tercera parte neutral entre las partes involucradas en el intercambio de información para que ambas tengan la absoluta certeza de la identidad de su contraparte, y de esa forma puedan intercambiar información confidencial de manera segura. A esta tercera parte autenticadora de identidades se le llama autoridad certificadora.

Un certificado digital se utiliza para varias cosas, la principal, sin duda, es autenticar la identidad de las partes que intervienen en el intercambio de información: el transmisor y el receptor, ya sea una persona física, una persona moral (una empresa) o el propio gobierno. Cuando se hace intercambio de información que requiere de muy alta seguridad en la transmisión, en general se necesita una firma electrónica, que es la que garantiza tanto la integridad de los datos, como su confidencialidad y el sitio de su procedencia. Garantizar la integridad de los datos implica que éstos no sean alterados en su viaje por las redes. La confidencialidad implica que sólo las partes interesadas pueden conocer su contenido y nadie más.

En resumen, los certificados digitales son documentos electrónicos que confirman la identidad de una persona, física o moral (empresa), que tiene vínculos con una clave pública asociada a la clave privada. De esta forma, un certificado digital busca que la clave pública, junto con la firma digital del usuario, puedan ser verificados y validados por todos los interesados. La firma digital constituye un certificado firmado digitalmente por una autoridad de certificación; los participantes deben confiar en que la clave pública que reciben las autoridades de verificación sea la que pertenece al usuario.

Se han definido tres clases de certificados:

- **Clase 1.** Se otorgan a personas físicas. En éstos no se verifica la identidad de las personas que participan, por lo que es imposible autenticar su identidad y sólo se puede confirmar que el nombre de la persona física que aparece en el certificado es el mismo sujeto, de manera que sólo es útil para que un usuario verifique su propia identidad.
- **Clase 2.** Se otorgan a personas físicas. En éstos sí es posible confirmar que la información proporcionada por la persona solicitante es congruente con la información contenida en las bases de datos de cualquier entidad emisora de certificados; además, existe congruencia con otros datos del solicitante del certificado.
- **Clase 3.** Se pueden otorgar tanto a personas físicas (individuos) como personas morales (empresas). En este nivel de certificación ya es una exigencia probar la identidad con base en documentos legales emitidos ya sea por el gobierno o por un notario público.

De este modo, los certificados digitales, también llamados certificados de clave pública, sirven para identificar a quién pertenece un par de claves simétricas. En este caso, la función de la autoridad certificadora o de certificación (AC) al firmar con su clave privada un certificado es confirmar plenamente que existe un vínculo real entre una clave pública y el nombre del propietario de esa clave pública; sólo hasta entonces se puede publicar un certificado X.509, que garantiza que el contenido, por ejemplo de un sitio web, no puede ser alterado sin que alguien tenga conocimiento de ello.

Para que un usuario pueda comprobar que el certificado de clave pública que obtiene es válido, debe tener acceso a la clave pública válida de la AC que lo ha emitido; si al comparar las dos firmas, éstas son iguales, el certificado es auténtico. Pero, si el usuario aún tiene dudas acerca de la autenticidad del certificado, entonces tendrá que reconocer todas las firmas hasta llegar a la autoridad raíz, que es la única que puede firmar su propio certificado de autenticidad. Sólo con esta firma de la AC raíz es posible garantizar que los certificados que emite cualquier AC de nivel inferior no han sido falsificados, por lo que son auténticos.

Por lo anterior, es indispensable que dentro de la infraestructura de las PKI se tenga la absoluta seguridad de no alteración o suplantación en la distribución de claves públicas que son gratuitas y de que dichas claves públicas provienen de la AC raíz o de las AC autorizadas por la AC raíz.

¿Cómo se obtiene un certificado de identidad?

Los servicios de autorización para emitir certificados tienen una extensa demanda en una Infraestructura de Clave Pública (PKI, por sus siglas en inglés). Normalmente, los certificados de identidad tienen un periodo de vigencia mayor al que tienen los derechos de acceso o los privilegios del usuario. Al vencerse la vigencia de un certificado, éste se revoca, es decir ya no puede utilizarse, lo cual provoca un incremento enorme en la demanda de los servicios de autorización.

La autoridad de atributos (AA) no siempre es la que emite los certificados de identidad, aunque sí es la encargada de firmar los certificados de atributos y realizar la asignación de privilegios. Pero, ¿quién autoriza a la autoridad de atributos? Para ello, se creó otra entidad llamada fuente de autoridad (SOA, por sus siglas en inglés), que es la máxima autoridad para todas las autoridades de atributos, la cual se describe más adelante.

El procedimiento general para obtener cualquier tipo de certificado de servidor web consiste en solicitar el o los certificados a una autoridad de certificación mediante el uso de determinadas funciones de un software del servidor web, la cual, a su vez, hace la misma solicitud a la máxima autoridad, que es la fuente de autoridad (SOA), para que la autoridad de certificación garantice la identidad de la SOA, de este modo están garantizadas las identidades de las comunicaciones que se efectúen en forma digital. Esto se realiza mediante un formato de solicitud de firma de certificado (CSR, por sus siglas en inglés: Cerificate Signing Request).

Luego, la autoridad de certificación autentica la identidad de cada usuario y verifica que la clave pública que anota en el certificado sea de su propiedad (véase tabla 3.1). Si aprueba estas verificaciones, la autoridad de certificación cifra el certificado con su propia clave privada y lo firma digitalmente. Los certificados cifrados y firmados digitalmente se pueden distribuir a toda persona

que lo solicite, siempre que cumpla con los requisitos de autenticación de identidad. Para evitar que la autoridad de certificación distribuya certificados sin cumplir los requisitos, ésta a su vez es vigilada por la SOA.

Desde luego que la emisión de cualquier tipo de certificado está sujeta a ciertas reglas de emisión y gestión de certificados. Dichas reglas forman parte de la gestión de las PKI y tienen como objetivo formar un buen gobierno para las PKI, pues les otorga el marco legal que describe responsabilidades y obligaciones de toda autoridad de certificación, así como los derechos de los propietarios de los certificados, describiendo los procedimientos de operación de una PKI.

En realidad, la autoridad de certificación es un prestador de servicios, que puede ser una persona moral o física, que otorga servicios relacionados con las firmas electrónicas y expide certificados, de manera que actúa como intermediario de confianza entre los usuarios que desean intercambiar información con el uso de una firma electrónica. Para proporcionar estos servicios de certificación o emisión de certificados se basa en criterios internacionalmente reconocidos y aceptados, promoviendo la transparencia y la calidad en las prácticas de emisión de certificados. La base general es la norma X.509 publicada por la ITU-T.

¿Qué es la norma X.509?

Fue emitida por primera vez en 1988 y está asociada con toda la serie del estándar X.500 que ha sido implementada por todos los países que deseen hacerlo con el propósito de autenticar la identidad de esa nación, a fin de que dicha identidad sea utilizada en los tratados de libre comercio que han firmado entre sí los países involucrados, aunque el estándar X.509 tiene una organización más flexible para su uso en Internet. Propone un sistema jerárquico muy estricto para la emisión de certificados por parte de determinadas autoridades, donde existe una autoridad máxima y luego una serie de empresas particulares que tienen el permiso de esta autoridad para la emisión de certificados de todo tipo. En cuanto al aspecto puramente técnico de las TIC, también existe una jerarquía y autoridad en los servidores DNS, que puede ser organizacional o geográfica. Esto contrasta con el modelo PGP de

Zimmermann, donde cualquier persona, no sólo las entidades autorizadas, podían validar los certificados de generación de clave de otras personas o entidades.

En criptografía, la norma X.509 es un estándar de la ITU-T para las infraestructuras de clave pública (PKI) y de privilegios (PMI). Es el estándar de referencia, ya que especifica los formatos para los certificados de clave pública, de listas de revocación y de certificados de atributos, entre otros certificados. En realidad, el término *certificado X.509* se refiere al Certificado PKIX de la IETF (Internet Engineering Task Force), tal como aparece en la RFC (Request for comments, o petición de comentarios) 5280, al que se refiere comúnmente como PKIK para infraestructura de clave pública. El PKIK es el modelo de las entidades que gestionan la infraestructura de llave pública, designando sus funciones y protocolos.

La estructura prevista para el estándar de certificados se expresa en un lenguaje formal llamado Abstract Syntax Notation One y tiene un formato similar al que se muestra en la tabla 3.1, con ligeras variaciones, dependiendo del tipo de certificado.

SOA (Service Oriented Architecture)

Es una tecnología informática basada en estándares y componentes que tienen una interface de servicios web y hace énfasis en la reusabilidad y la independencia después de la implementación. La SOA es un caso particular de una autoridad de atributos, que desempeña un papel similar a la de autoridad raíz en una PKI. Se enfoca en sistemas construidos con base en servicios autónomos, como sucede en el comercio internacional, donde cada participante tiene una serie de servicios autónomos, pero al mismo tiempo todos tienen la necesidad de contar con un servicio web mundial estandarizado. Cuando se solicitan certificados de cualquier tipo provenientes de otros países, la SOA es la tecnología capaz de utilizar o reutilizar las aplicaciones que ya tiene cada usuario en su propio país, capacitando de esa forma a quien use la SOA a entrar de inmediato al mundo de los negocios internacionales. No es que la SOA autorice los certificados, sino que es la interface de los servicios web que permite la comunicación entre diferentes programas y tecnologías para que los

certificados sean autorizados y aceptados como válidos entre los diferentes países participantes.

Un servicio informático consiste en uno o varios programas interactuando con otros similares o incluso distintos, siempre que exista estandarización en los puntos clave para que esos programas puedan interactuar. Un buen servicio informático se adapta con rapidez a los nuevos servicios que aparecen constantemente en la red y nunca detiene la funcionalidad del sistema, al trabajar por medio de la recepción de mensajes y responder a los mismos, como es el caso de las solicitudes de certificados, las cuales deben ser respondidas a la brevedad posible. Así, la SOA posee una excelente arquitectura para prestar un excelente servicio informático.

Autoridad raíz de certificación

Cualquier entidad que se constituya como una autoridad de certificación forma parte de una jerarquía de autoridades, donde hay una autoridad más alta que el resto, llamada **autoridad raíz**, que posee sus propios certificados públicos y puede firmarlos ella misma, a diferencia de aquellas que están en un nivel jerárquico inferior, las cuales dependen de la firma de la máxima autoridad.

El certificado se "carga o se instala" en la computadora del usuario a través de un proceso incluido en diversos navegadores, como Internet Explorer, en sistemas operativos tipo Windows, que tienen funciones de importación de certificados, de manera que cada vez que se importa un certificado firmado por dicha autoridad de certificación puede ser validado, pues el usuario tiene la clave pública para validar la firma del certificado. Cuando este proceso se efectúa en la computadora del usuario para la obtención de certificados, se entiende que habrá la confianza de que éstos son verdaderos y válidos para realizar transacciones comerciales por Internet.

Infraestructura de clave pública (PKI)

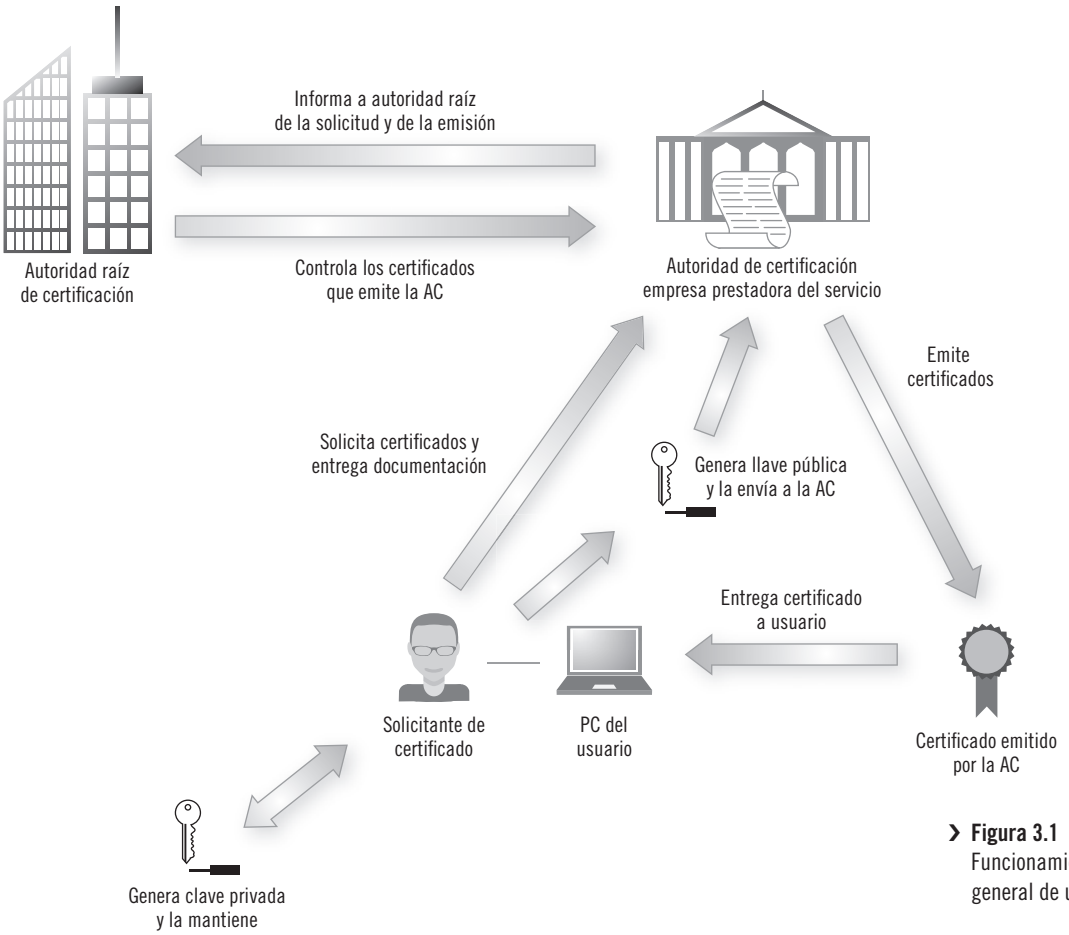
Se le llama infraestructura de clave pública (PKI, por sus siglas en inglés) al conjunto de políticas, procedimientos, personal especializado y TI que son necesarios para administrar, gestionar, crear, distribuir, almacenar, utilizar y

revocar certificados digitales y administrar cifrado de claves públicas. En una PKI es posible la transmisión electrónica segura de información para las actividades que al utilizar redes, ya sea Internet u otro tipo, es necesaria una seguridad informática alta, como es el caso de las instituciones bancarias y el comercio electrónico nacional e internacional. Toda persona que utiliza Internet tiene una clave de acceso, pero ésta resulta insuficiente cuando se transmite información en extremo valiosa, pues cuando se trata de esta información, se requiere que se conozca y se valide la identidad tanto del transmisor como del receptor de la información con el más alto grado de certeza.

Una PKI tiene como principal objetivo emitir y gestionar certificados de clave pública, en el cual se incluye la autoridad certificadora raíz, que es la única que tiene la autoridad de firmar su propio certificado, pues ya no existe una autoridad más alta que ella. Gestionar claves implica la creación de pares de claves, revocación de certificados, almacenamiento de claves en archivos y su destrucción una vez que los certificados han sido revocados.

Cualquier país que adopte una PKI debe seguir las políticas estandarizadas que exige la norma X.509, la cual contempla una *política de certificados* y una *declaración de las prácticas de certificación*, que son documentos publicados por la autoridad certificadora con base en la Norma X.509 de la ITU-T, donde se garantiza una base común de trabajo. Esto ha generado la oportunidad de poder realizar negocios y comercio internacional con seguridad y confianza. Todo aquello relacionado con el intercambio de información generado por esas actividades tiene un funcionamiento estandarizado, es decir, un certificado de clave pública emitido en un país, que es válido en cualquier otro país que haya adoptado la misma normatividad. En la figura 3.1 se esquematiza el funcionamiento general de una PKI.

La estandarización también otorga una misma base jurídica para el establecimiento de confianza entre empresas particulares, así como entre entidades de gobierno de los diferentes países que participan en el comercio internacional. Sin embargo, para que exista una verdadera autenticación para utilizar los certificados de clave pública, es necesario que los usuarios en ambos extremos del intercambio de información proporcionen firmas digitales mediante el valor de la clave privada correspondiente, pues si sólo utilizaran



› **Figura 3.1**
Funcionamiento general de una PKI.

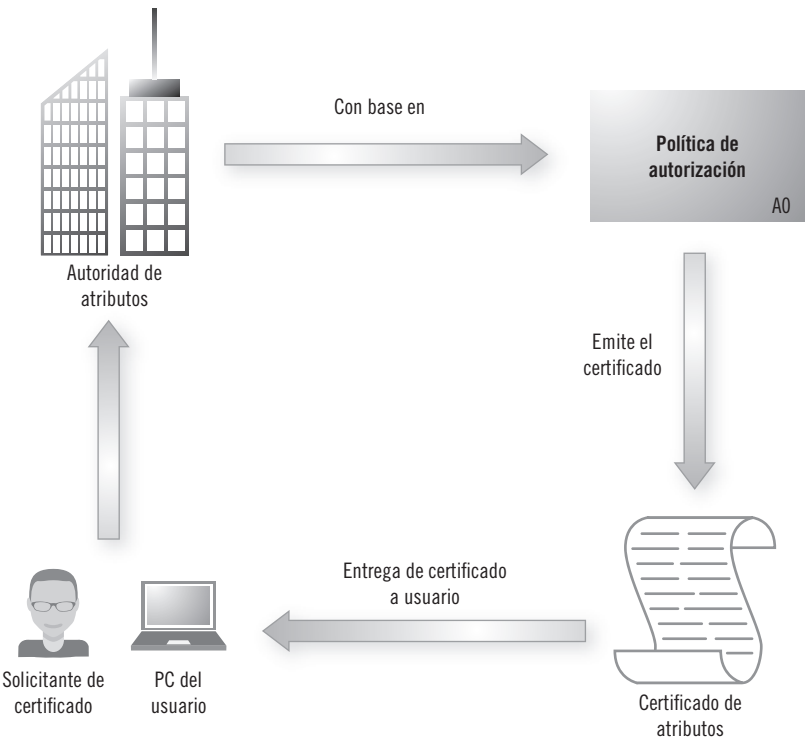
la clave pública estarían expuestos a ataques malintencionados cuando la información enviada viaja de un país hacia otro.

Infraestructura de la administración de privilegio (PMI)

La administración de privilegio (PMI, por sus siglas en inglés) es el proceso de administrar la autorización de un usuario para ingresar a determinado sistema basado en las recomendaciones X.509 de la ITU-T, que tiene como objetivo principal diseñar mejores controles de acceso a los sistemas y a sus recursos. Por tanto, la administración de privilegios constituye la práctica de control y de administración de la identidad de usuarios digitales, así como los derechos de esas identidades para realizar acciones sobre ciertos recursos de la red o de bases de datos. Así como la infraestructura de clave pública (PKI) autentica usuarios, la infraestructura de administración de privilegio (PMI) hace

lo propio, de manera similar, con la autorización, mediante la utilización de certificados de atributos (CA), los cuales mantienen los privilegios de los usuarios en la forma de atributos, sustituyendo a los certificados de clave pública (PKC) para el mantenimiento de las claves públicas. La PMI tiene fuentes de autoridad y atributos de autoridad que proporcionan a los usuarios con la emisión de los certificados de atributos, sustituyendo en esta emisión a las autoridades de certificación que sólo emiten a los usuarios los certificados de clave pública.

Como la PMI es una infraestructura para administrar privilegios, se han definido tres entidades: 1) el objeto, que es el recurso que se debe proteger, 2) el poseedor o tenedor del privilegio y 3) el verificador del privilegio. El poseedor del privilegio utiliza este privilegio para hacer uso del objeto protegido, el cual puede utilizar para escribir, borrar, ejecutar, etcétera, en tanto que el verificador del privilegio determina si el poseedor del privilegio puede hacer uso del objeto en los términos que desea el poseedor de ese privilegio; para determinar si puede hacer uso del objeto, el verificador se basa en la política



› **Figura 3.2** Funcionamiento general de una PMI.

de privilegios vigente, en las variables presentes en el entorno en ese momento, las cuales varían con el tiempo, y en los privilegios que tiene el poseedor del privilegio. En la figura 3.2 se muestra el funcionamiento de una PMI.

Por otro lado, dentro de una PMI existen dos esquemas particulares:

1. **Esquema de control de acceso.** Muestra cómo actúa el verificador para permitir el acceso al poseedor de privilegios de acuerdo con la política de acceso.
2. **Esquema de roles.** Asigna determinados privilegios al poseedor con su respectivo certificado.

La fuente de autoridad o inicio de autoridad (SOA, por sus siglas en inglés; Start of Authority) es la responsable de la asignación inicial de privilegios.

La infraestructura para la administración de privilegio, a su vez, tiene como base la infraestructura de clave pública, pues las autoridades de certificación

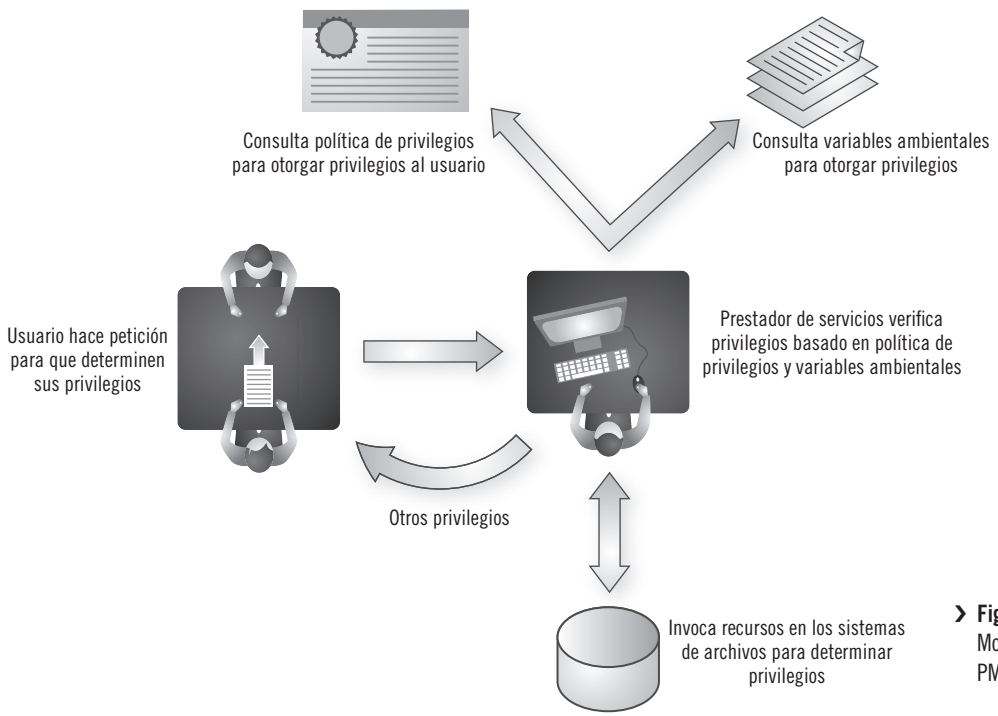


Figura 3.3 Modelo de control PMI X.509.

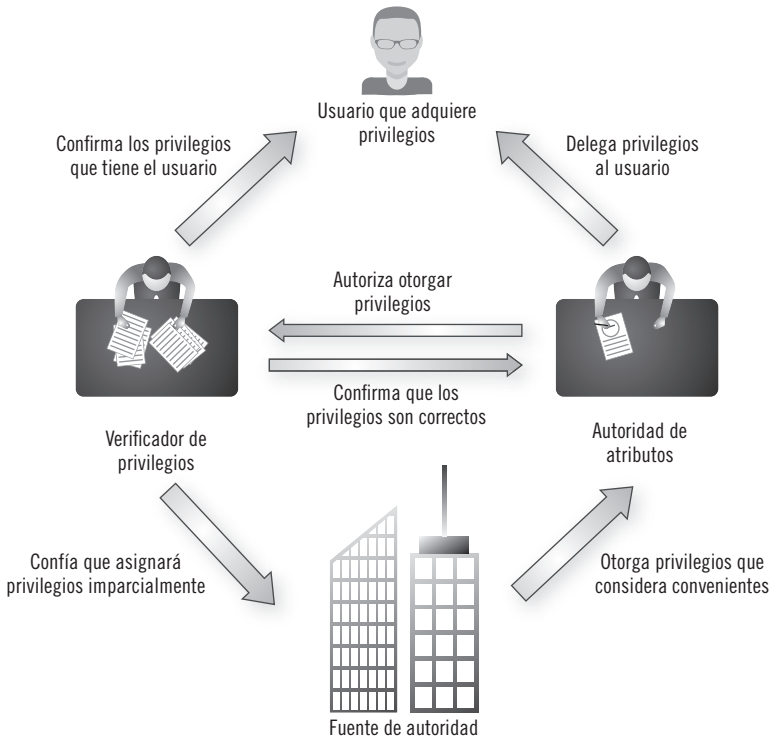


Figura 3.4
Modelo de delegación de privilegios de PMI con el estándar X.509.

tienen que firmarse digitalmente por el emisor de las autoridades de atributo, mientras que la infraestructura de clave pública se utiliza para validar la firma de las autoridades de atributo.

En la figura 3.3 se muestra el modelo de control de la PMI, de acuerdo con la norma X.509, mientras que en la figura 3.4 se observa el modelo de delegación de privilegios de la PMI, de acuerdo con la norma X.509.

Para una mejor comprensión acerca del significado de una PKI y de una PMI, más adelante se explicará de manera breve cuál es el contenido de las políticas de emisión de certificados y las prácticas de certificación, ambos elementos esenciales de estas infraestructuras.

La asignación de privilegios se basa en los atributos de cada usuario, por lo que a continuación se explican estos conceptos.

Atributos

Un atributo es la información que describe a un usuario o al medio ambiente de redes o digital. Los atributos pueden almacenarse como pares de valores

clave; por ejemplo, para un usuario, un atributo puede ser "puesto dentro de la empresa = jefe de área", pero, si se habla de atributos de medio ambiente, un atributo de la ubicación de una empresa es, por ejemplo: "área de ubicación = noreste", o bien el atributo se toma de otras fuentes como metadatos. Atributos de usuario pueden ser: nombre, edad, puesto que ocupa en la empresa, área a la que pertenece, entre muchos otros. Por otro lado, los atributos de medio ambiente proporcionan datos de entrada importantes para tomar decisiones de acceso y son independientes del usuario que pretende accesar. Ejemplos de atributos de medio ambiente son: estatus de amenaza para la seguridad del país, hora del día, dirección IP, entre otras.

Autoridad de atributos (AA)

También llamado almacén de atributos, es la autoridad que firma los certificados de atributos y está habilitada para asignar los privilegios; normalmente no es la misma autoridad que emite los certificados de identidad. La infraestructura de administración de privilegios (PMI) es la infraestructura creada para gestionar tanto los atributos como los privilegios de los usuarios. Es una base de datos; también puede consistir en un directorio donde los sistemas se agregan, modifican y guardan atributos con absoluta seguridad. Una autoridad de atributos es una fuente confiable de datos para el control de acceso basado en atributos. Algunos dispositivos que se pueden configurar como autoridades de atributos son las bases de datos MySQL, directorios LDAP y algunos servicios de la Web.

ABAC (Attributes Based Acces Control)

El Control de Acceso Basado en Atributos (ABAC) separa la autenticación y la autorización, al separar las preguntas: "¿quién eres?" y "¿qué puedes hacer?" Asimismo, evalúa los datos descriptivos disponibles, también llamados atributos, contra las políticas establecidas, con el propósito de determinar si el usuario está autorizado para accesar a determinada fuente de datos que es requerida por el usuario. Es una tecnología informática que evalúa políticas de seguridad contra valores de atributos relevantes y determina autorizar el requerimiento de un usuario.

Generación de la clave del atributo

Para que el ABAC trabaje se ha diseñado un algoritmo aleatorio que sólo puede ser ejercido por la autoridad de atributos. Tiene como requerimiento de entrada la clave secreta de la autoridad y un conjunto de atributos en el dominio de la autoridad. Al final se obtiene la clave secreta del usuario, que es la que se utiliza para tener acceso a los datos de sus atributos.

Fuente de autoridad o inicio de autoridad (SOA)

Aunque tienen las mismas iniciales (SOA), no hay que confundir la arquitectura orientada a servicios (Service Oriented Architecture) con la fuente de autoridad o inicio de autoridad (Start of Authority), la cual sirve como base para dar autoridad a ciertos servidores instalados en diferentes zonas, ya sea organizacionales o geográficas. Los servidores son de sistemas de nombre de dominio (DNS, por sus siglas en inglés) y se configuran para cargar los datos de una zona; así, la SOA administra los registros de cada autoridad. Utiliza dos tipos de recursos para determinar las propiedades de autoridad que tiene la zona.

El registro de recursos del inicio de autoridad (SOA) indica el nombre de origen de la zona, así como otras propiedades de ésta, y contiene el nombre del servidor que es la fuente primaria de información en dicha zona. Además, el registro del nombre que tiene el servidor (NS, por sus siglas en inglés; Name Server) se utiliza para denotar cuál o cuáles servidores DNS tienen autoridad en esa zona. Todo aquel que consulta la lista de los NS (nombre del servidor) y de cuántos servidores registrados consta, automáticamente conocerá cuál servidor tiene más autoridad. Los servidores listados en NS (nombre del servidor) y RR (registro de recursos) se consideran una fuente de autoridad para los demás servidores. El registro de recursos de los SOA y de los NS tiene un papel especial en la configuración de la zona. Cuando se agrega una nueva zona a los registros, la jerarquización de autoridad entre los servidores se efectúa de manera automática al usar una consola DNS.

Políticas de emisión de certificados

Una política de certificación o de emisión de certificados es un documento que declara cuáles son los principales actores de una PKI, qué papel tienen éstos y cuáles son sus responsabilidades. Siempre es posible tener acceso a las políticas de certificación y al nivel de aseguramiento asociado con el certificado, por lo que se puede tomar una decisión dependiendo de la confianza acerca de la cual se quiera estar seguro con respecto a la certificación.

Las políticas generales de certificación son las siguientes:

a. **Arquitectura.** Es un documento que describe la arquitectura general de una PKI, en el que se declaran los principales actores de la PKI y la forma general en que funciona el proceso de certificación.

b. **Uso de los certificados.** Describe los usos autorizados y prohibidos de los certificados. Cuando se emite un certificado, los atributos que contiene deben declarar para cuáles usos se emitió el certificado; por ejemplo, puede haberse emitido para firma digital, de correo electrónico, para cifrado de datos, para autenticación de un servidor web, para el uso de HTTPS o para la delegación de autoridad para emisiones posteriores. Asimismo, también se deben declarar los usos prohibidos para el tipo de certificado que se ha emitido.

c. **Identificación y autenticación del nombre.** En el documento también debe describirse la forma en la cual se han elegido los nombres de los certificados. Al llenar una solicitud para obtener un certificado, ya sea la autoridad de certificación, o en su caso la autoridad de registro, si se delega la autoridad, es la encargada de verificar la información que proporciona el solicitante (por ejemplo, su identidad), lo cual asegura que la autoridad de certificación no será parte de un robo de identidad.

d. **Generación de la clave.** Es un punto importante que también debe mencionarse en una política de emisión de certificados, ya que es posible que a los propios usuarios se les permita generar su propia clave, pero para que ellos la generen deberán someterla a una AC. Una PKI también

puede prohibir a los usuarios que generen sus propias claves, aunque esto es poco probable, pero si es así, entonces deberá indicarles formas más seguras para la generación de las claves que necesitan, por ejemplo, utilizando un equipo que sea un módulo de seguridad.

e. **Procedimientos.** Una gran parte del documento de las políticas para la emisión de certificados describe los procedimientos para una solicitud, emisión, aceptación, renovación, modificación de clave y revocación. Esa descripción deberá indicar lo que debe hacer cada uno de los actores[1] de una PKI para que todos acepten el nivel de seguridad del certificado.

f. **Controles operativos.** En las políticas se incluye un capítulo sobre los controles de procedimientos, los controles físicos y los controles de acceso al sistema implicados en una PKI que aseguren la integridad de los datos, su disponibilidad y su confidencialidad.

g. **Controles técnicos.** Describe los requerimientos técnicos para determinar el tamaño de las claves, la protección de claves privadas y otros tipos de controles del aspecto puramente técnico, entre los que se incluyen redes y computadoras.

h. **Listas de revocación de certificados.** Son muy importantes para el funcionamiento seguro de una PKI, ya que un certificado se puede revocar (suspender su vigencia), al encontrar cualquier error en cualquier procedimiento, por mínimo que éste sea, como presentar identidad falsa o que no se pueda comprobar que la AC no haya seguido a consciencia todo el proceso de certificación.

i. **Auditoría y evaluación.** La generación de las listas de revocación son resultado de auditorías que se practican a las AC, mediante las cuales se evalúa si éstas han funcionado con estricto apego a las reglas establecidas en todo el manual de políticas y procedimientos. La evaluación consiste en verificar paso a paso el cumplimiento de tales políticas y reglas por parte de las AC.

---

[1] En este contexto, el uso del término ***actor*** no está ligado al concepto tradicional de la palabra y sólo se usa para hacer referencia a cada una de las personas que intervienen en cualquier procedimiento.

Prácticas de certificación

La *Declaración de prácticas de certificación* y las *Políticas de emisión de certificados* son los únicos instrumentos que establecen reglas aplicables a la solicitud, validación, aceptación, entrega, emisión y revocación de certificados, así como aplicaciones y restricciones de estas actividades, que se basan en las recomendaciones de la ITU-T X.509. No es objeto de este texto mostrar de manera extensa el contenido de dichas prácticas, por lo que sólo se citan las partes principales de su contenido, acompañadas de breves comentarios.

Contenido general de prácticas de certificación.

a. **Responsabilidades de una autoridad certificadora (agencia prestadora de estos servicios).** Contar con la infraestructura material y humana necesaria, proteger en todo momento los datos de las personas físicas y morales, aprobar (denegar), emitir, revocar, publicar certificados emitidos, proporcionar al solicitante los medios necesarios para que genere sus datos de creación de firma electrónica bajo la responsabilidad del solicitante, contar con los recursos materiales y humanos para evitar la alteración del contenido de los certificados y cumplir con el marco jurídico y las reglas generales de prestadores de servicio de este tipo.

b. **Obligaciones de una autoridad certificadora.** Mantener un registro de todos los certificados emitidos, administrando las bases de datos actuales e históricos que contengan la información de los certificados digitales emitidos, así como proteger los datos de los usuarios de acuerdo con la política de manejo de información confidencial. La AC también debe garantizar que cada uno de sus nombres distintivos sea único, con lo que se asegura que cada certificado emitido también sea único.

c. **Obligaciones y responsabilidades de los solicitantes de certificados digitales.** Establecer su password y generar sus claves, pública y privada, solicitar un certificado digital a través de una AC, conocer y aceptar el acuerdo de prestación de servicios, ejecutar todas las actividades de la *Declaración de prácticas de certificación*, cumplir con las obligaciones derivadas

del uso de una firma electrónica, descargar su certificado digital que ya ha sido registrado, hacerse responsable de la seguridad de su clave privada y evitar el uso no autorizado de sus datos personales y su firma electrónica.

d. **Responsabilidades de la parte que confía.** Evaluar en forma independiente la procedencia y el uso del certificado en cualquier mensaje de datos, así como utilizar el software y hardware apropiados para verificar la firma digital y otras operaciones de cifrado que quiera llevar a cabo. La confianza proviene precisamente de la verificación de la validez y vigencia de los certificados.

e. **Identificación y autenticación.** La verificación de la identidad del solicitante sólo podrá realizarse por la AC, previa presentación de una serie de documentos oficiales probatorios de su identidad, teniendo la AC el derecho de solicitar información adicional a la que normalmente se requiere, a fin de verificar sin duda alguna la identidad del solicitante.

f. **Revocación de certificados.** En México, el periodo de validez de los certificados digitales de la AC (agencia prestadora de servicios) es de al menos 10 años. Son emitidos por la fuente raíz (la Secretaría de Economía), en tanto que los certificados que emite la agencia prestadora de servicios a los solicitantes tienen una vigencia de un año, vigencia que se señala en el certificado. Al término de ese periodo, el certificado automáticamente deja de tener validez oficial y el usuario puede solicitar la renovación del mismo o un nuevo certificado.

g. **Procedimiento de operación.** Las obligaciones del solicitante son: conocer el procedimiento a seguir; descargar, llenar, completar y enviar el formato de solicitud; solicitar el certificado por medio de la dirección electrónica que se le indique; generar su par de claves (pública y privada), el solicitante deberá mantener la clave privada en su computadora, mientras que la clave pública deberá enviarla a la AC. Por su parte, la AC (agencia prestadora de servicios) procesa toda la información que recibe del solicitante, recibe la clave pública generada por el solicitante y comunica a todas las partes interesadas, básicamente a la fuente raíz, que se ha emitido con éxito un nuevo certificado digital.

h. **Existen procedimientos para mantener la vigencia de los certificados y procedimientos para su revocación y procedimientos para publicar la lista de los certificados revocados.** En el estándar X.509 existe un sistema de registro del tiempo para anotar la fecha y la hora de expedición del certificado, el cual está conectado al sistema de la fuente raíz.

Aun cuando son muy similares, existen algunas diferencias significativas entre las PKI y las PMI, aunque, tal vez, la diferencia más importante es que las PKI están más relacionadas con la autenticación o la identificación, mientras que las PMI están más relacionadas con la autorización en el uso de recursos. Otras diferencias consisten en que una PKI tiene una autoridad de certificación raíz y una PMI tiene una autoridad fuente, una PKI tiene una autoridad de certificación y una PMI tiene una autoridad de atributos que otorgan ciertos privilegios, una PKI emite certificados de clave pública y una PMI emite certificados de atributos. Al imponer una política de privilegios a los usuarios, se garantiza una política de seguridad preestablecida por la autoridad fuente.

Actividad de aprendizaje

En equipo investiguen en diferentes fuentes de información y elaboren una tabla donde presenten las diferencias entre las PKI y las PMI. Entreguen su trabajo a su profesor.

El papel de los protocolos en PKI y PMI

Como los negocios internacionales tienen su base en Internet, o cualquier otro tipo de red, para el intercambio de información confidencial en forma segura es necesario recordar algunos conceptos importantes que existen para el uso de Internet, así como mencionar los protocolos indispensables en el uso de redes seguras. La mayoría de estos conceptos se utilizan de manera recurrente en capítulos posteriores.

Protocolo

Es el conjunto definido de procedimientos que se adoptan para asegurar la comunicación entre dos conjuntos de procesos que existen dentro de una misma capa dentro de una jerarquía de capas.

Capa (nivel)

Conjunto de funciones entre los límites superior e inferior dentro de una jerarquía lógica de funciones, que tiene propósitos distintos a aquellos que tiene otra capa dentro de la misma jerarquía y que normalmente proporciona un servicio a cualquier jerarquía superior. Por ejemplo, el modelo de referencia para la interconexión de sistemas abiertos tiene siete capas.

Interface de capa

Es la interface entre capas adyacentes de una jerarquía de capas.

Modelo de referencia para la interconexión de sistemas abiertos

La interconexión de sistemas abiertos (OSI, por sus siglas en inglés) es una organización jerárquica de todas las relaciones estructuradas en siete capas, entre una red de telecomunicación, sus usuarios y los servicios de telecomunicación que puede ofrecer la red.

Protocolo de acceso

Es un protocolo utilizado en la interface usuario-red que hace que el usuario pueda emplear los servicios y las instalaciones de una red de telecomunicación.

Liga de protocolo de acceso

La LAP (Link Acces Protocol) es un conjunto formal de ligas de sincronización y procedimientos de control de errores para llevar información a través de la interface usuario-red. Normalmente se asocia una liga de protocolo de acceso con la capa de liga de los datos del modelo de referencia de interconexión de sistemas abiertos.

DNS

El sistema de nombre de dominio (DNS, por sus siglas en inglés) es un sistema para computadoras, servicios o cualquier recurso conectado a Internet o a redes privadas, para asignar nombres jerárquicamente distribuidos. Se asocia con otra información por medio de nombres de domino asignados a cada una

de las entidades participantes. Traduce nombres de dominio que pueden ser memorizados con facilidad por las personas a la dirección numérica IP, necesaria para propósitos de servicios de computadora y otros dispositivos en todo el mundo. El DNS es un componente esencial de la funcionalidad de la mayoría de los servicios de Internet, pues constituye el servicio primario de los directorios de Internet.

Dominio

Es una parte de una red de computadoras, donde tanto los recursos como las direcciones están bajo el control de una autoridad específica. Un esquema de dominio puede ser organizacional o geográfico.

Nombre de dominio

Es el nombre que identifica a un dominio. La estructura y organización de los nombres de un dominio dependen de la red que está en funcionamiento.

Dominio de seguridad

En la sección 6.60 ITU-T X.1252 se define como un conjunto de elementos, políticas de seguridad, autoridad de seguridad y un conjunto de actividades relevantes en los que se manejan los elementos de acuerdo con una política de seguridad.

HTTPS

El protocolo de Transferencia de Hiper-Texto (HTTPS) es la versión segura del http (Hyper Text Transfer Protocool) de uso cotidiano. La diferencia entre ambos radica en que con el HTTPS es posible llevar a cabo actividades de e-commerce, ya que permite realizar transacciones comerciales y de otra índole en forma segura. En algunos navegadores, como Firefox o Explorer, cuando se emplea un protocolo https se puede ver el icono de un candado que aparece en la barra principal del navegador. Además, en la barra de direcciones se ve que "http://" será sustituido por "https://".

El protocolo HTTPS es más seguro porque la página web codifica la sesión con certificado digital. De este modo, el usuario tiene ciertas garantías de

que la información que envíe desde dicha página no podrá ser interceptada y utilizada por terceros. Estos certificados de seguridad son conocidos como SSL. Cuando dichos certificados estás instalados en la página web se puede ver el candado al que se hizo referencia antes. Por otro lado, si hay instalados certificados de validación extendida, además del candado, la barra de URL del navegador toma un fondo verdoso (siempre que se utilicen versiones recientes de los navegadores). Por esta razón es muy utilizado por entidades bancarias, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales, incluyendo las contraseñas.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado más apropiado para el tráfico de información confidencial que el protocolo HTTP, de este modo se consigue que la información confidencial, como identificación del usuario y password, no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Cookie de HTTP

También conocido como cookie web, cookie de Internet o cookie de buscador, o sólo cookie, es un conjunto pequeño de datos enviados desde un sitio web que se almacenan en el buscador web del usuario al momento en que éste realiza alguna búsqueda en ese sitio web. Cada vez que el usuario carga ese sitio web, el buscador regresa el cookie al servidor para notificar la actividad previa del usuario en ese sitio. Se supone que un cookie es un mecanismo confiable de los sitios web que recuerda la información almacenada en determinados sectores de la memoria, a lo que se le llama estado. Pero, cuando esa información afecta a otros datos de entrada, sobre todo si operan programas en serie, se le llama información de estado completo. Un cookie registra la actividad de búsqueda o cuáles páginas fueron visitadas en meses e incluso en años previos. Un cookie no puede tener virus o instalar malware en una PC, pero sí es capaz de almacenar passwords y cualquier dato que el usuario haya introducido a la memoria, como números de tarjetas de crédito.

Sin embargo, los cookies que son de interés y de uso común para la seguridad informática son los cookies de autenticación utilizados por los servidores web, primero para saber si el usuario está conectado a determinada red y luego para conocer con quién está conectado, pues si no se tuviera este tipo de cookies, el sitio no sabría si enviar una página que contiene información confidencial o solicitar la autenticación de ambos usuarios, el emisor y el receptor de esa información. La seguridad de un cookie de autenticación depende de la seguridad de sitio web emisor y del buscador web del usuario y de si los datos que el cookie ha almacenado están encriptados. Sin embargo, un hacker con cierta habilidad puede leer los datos almacenados por el cookie, y así tener acceso a los datos del usuario o a otros sitios a donde pertenece el cookie, mediante el uso de la identidad del usuario.

Dirección IP (Internet Protocol)

La dirección IP, también llamada "número IP", es la dirección de una computadora huésped utilizada en el protocolo de Internet. La dirección IP corresponde a un nombre de dominio calificado. Hasta este momento, se forma de 32 bits y suele representarse por una secuencia de cuatro números decimales, cada una en un rango que va de 0 a 255, separados por un punto. En una computadora, la IP tiene dos partes: una que corresponde al número de red en la que se localiza esta computadora y otra que identifica a la computadora dentro de la red en la cual se encuentra. Un protocolo de Internet (IP) no está limitado a Internet y puede ser usado en otras redes.

URL (Uniform Resource Locator)

El localizador uniforme de recursos (URL, por sus siglas en inglés) es una secuencia estandarizada de caracteres para localizar y accesar un recurso de Internet. A continuación de presentan varios ejemplos de su formato general para identificar un sitio web, un archivo o un servicio.

1. http://www.iec.ch. Se trata del URL del sitio de la International Electrotechnical Commision. En éste, la **ch** es el nombre de dominio de máxima jerarquía. Pero, si el URL es: http://www.iec.ch/about/mission-e.htm,

entonces indica que es un texto en inglés, donde se describe la misión y los objetivos de la IEC, y este archivo puede ser accesible por medio del protocolo HTTP.

2. news:comp.os.unix. Se trata de un fórum cuyo nombre es comp.os.unix.
3. news:AR234@news.iso.org. Se trata de un artículo identificado como AR234, almacenado en el huésped news.iso.org.

Portal

Es la página de un proveedor de servicio que proporciona una revisión y un acceso voluntario a una serie de servicios y sitios web. El portal puede configurarse en forma automática de acuerdo con el perfil del usuario que se haya almacenado. Normalmente cualquier portal está asociado a un buscador. El término "*portal*" también se utiliza para designar al proveedor del servicio.

SSL (Capa de enchufe de seguridad)

Es un protocolo de seguridad que puede configurarse para proteger los puertos de un servidor. SSL requiere un certificado X.509 firmado por una autoridad de certificados.

Testigo (Token) de seguridad

En un control digital de acceso es una cadena de información, tal como una clave cifrada o un password, que permite a un sistema reconocer a un usuario autorizado para accesar a ese sistema. Las señales, testigos o tokens de seguridad son elementos utilizados dentro de un STS.

STS (Secure token service)

Es un servicio que emite, valida, realiza reclamaciones, renueva y cancela tokens de seguridad.

SSO (single sign-on)

La firma única es un enfoque de ingeniería que permite al usuario proporcionar sus datos de identificación, tales como identificación de usuario y password,

para tener acceso a múltiples aplicaciones. La firma única también permite a algunas aplicaciones web autenticar a los usuarios sin tener acceso a sus datos de seguridad que lo identifican, como un password.

TLS (Transport Layer Security)

Es un protocolo de estándar cifrado para trabajar con seguridad en Internet, que opera en una aplicación a un nivel bajo, de manera que el usuario no percibe que está utilizando el protocolo. Se construye sobre SSL y fue desarrollado por IETF.

SSH (Secure Shell)

El SSH, que se traduce como un protocolo de órdenes seguras, es el nombre de un protocolo y del programa que lo implementa. Con este protocolo es posible conectarse a máquinas remotas a través de una red. Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribirlas al conectarse a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro. El SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Comprueba tus saberes

1. ¿Quién es Philip Zimmermann y por qué es importante su trabajo?

2. Define con tus propias palabras qué es una PKI.

3. Define con tus propias palabras qué es una PMI.

4. ¿Qué es la ITU-T y qué papel tiene en el incremento del comercio internacional?

5. ¿Qué acredita la norma X.509?

6. ¿Qué es un protocolo?

7. ¿Qué es HTTPS?

8. ¿Qué es un cookie de HTTPS?

9. Define con tus propias palabras el concepto de autoridad raíz.

10. Define con tus propias palabras el concepto de fuente de autoridad.

11. Describe en qué consisten los atributos de un usuario.

12. Cita y explica al menos tres políticas de certificación.

13. Cita y explica al menos tres prácticas de certificación.

14. Describe cuál es el uso de un URL.

15. ¿Qué es una dirección IP?

Referencias bibliográficas

1. ITU-T y UIT. (2008). La seguridad en las telecomunicaciones y las tecnologías de la información y la comunicación. ITU-T.
2. Gómez, Álvaro. (2011). Enciclopedia de la Seguridad Informática. Segunda edición. Ed. Alfaomega.

Referencias electrónicas

1. https://www.eldos.com/sbb/delphi-pki-php
2. https://web.archive.org/web
3. https://www.eurologic.es/conceptos/certificadios%20digitales.html
4. https://www.rfc-editor.org/rfc/rfc2459.txt
5. https://www.itu.int/rec/T-REC-X-509
6. https://searchsecurity.techtarget.com/definition/X.509
7. https://www.pscworld.com/pscworld
8. https://oa.upm.es/33681/1/PFC.pdf
9. https://espejos.unesco.org.uy/simplac.2002/ponencias/Segurm%
10. http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=732-08-01
11. https://en.wikipedia.org/wiki/Certificate_policy
12. https://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n
13. https://technet.microsoft.com/en-us/library/cc779148(v=ws.10).aspx
14. Agencia de certificación electrónica: http://www.ace.es
15. PKSC: http://www.rsasecurity.com
16. http://www.f-secure.com/
17. http://www.seguridadenlared.org/

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.

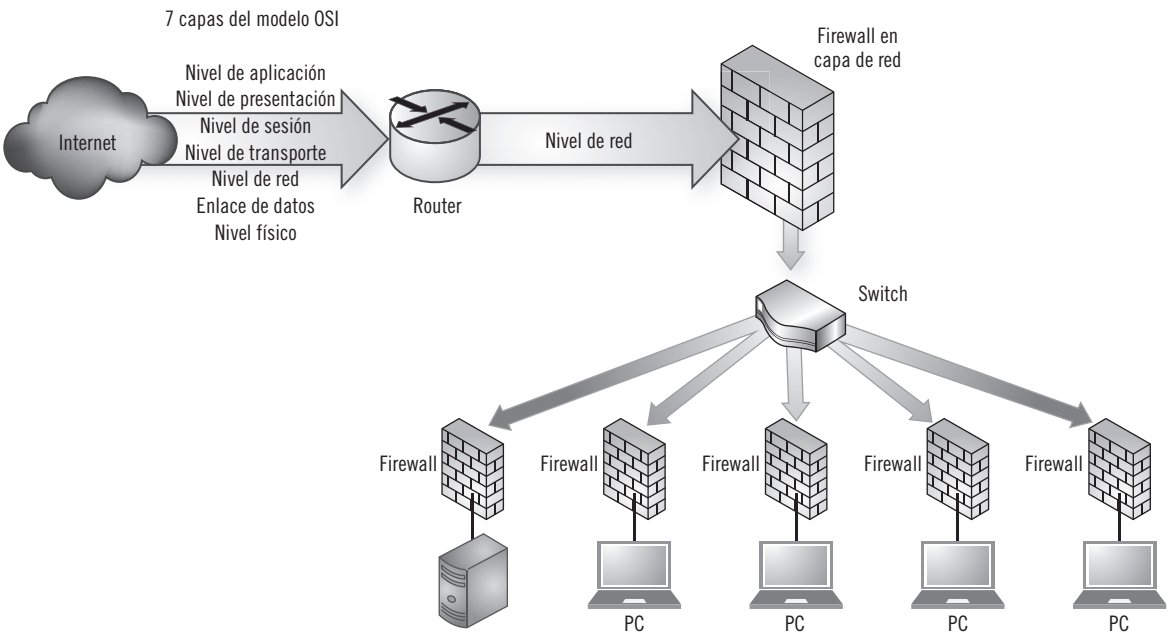
5.4 ¿Qué es un firewall y cómo funciona?

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.

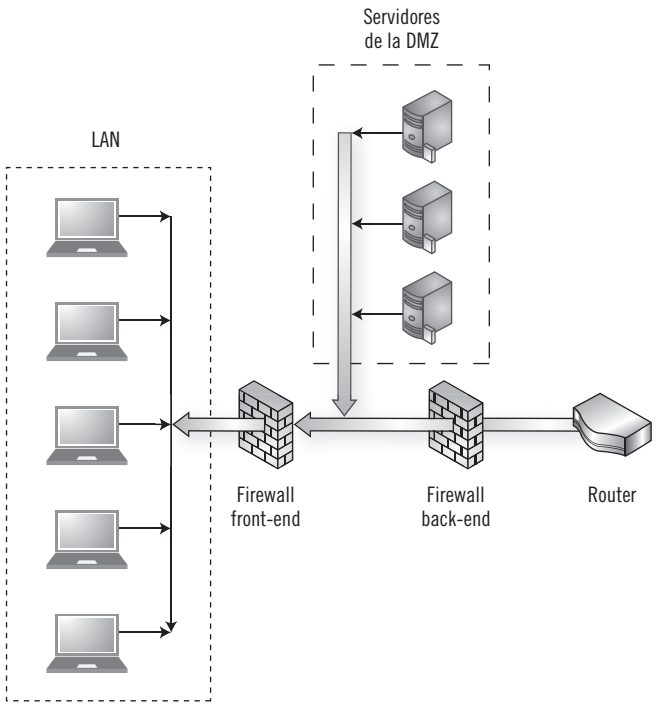
Si bien es cierto que una de las ventajas del uso del servicio FTP es que ofrece la máxima velocidad en la conexión, lo cual es muy útil cuando se envían archivos de gran tamaño, también es cierto que su principal desventaja

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.

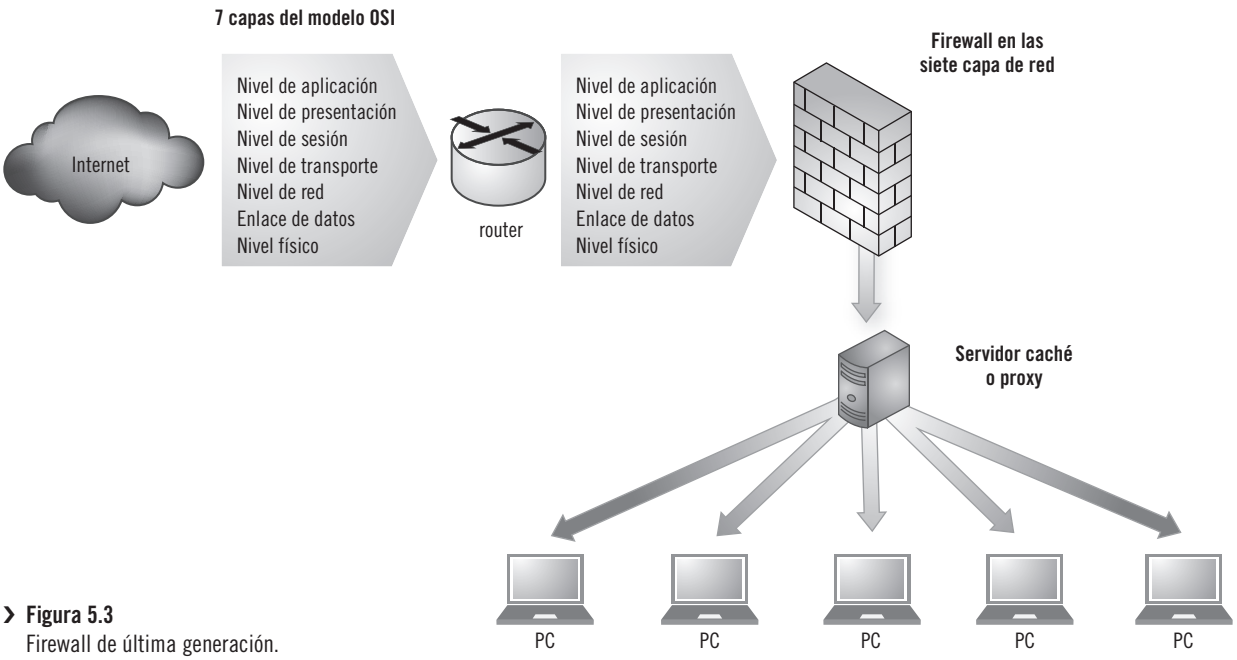
La función del firewall ISA de capas múltiples consiste en proteger los recursos que las empresas u organizaciones tienen en la red de accesos no autorizados, ataques de hackers y virus maliciosos, además de controlar el acceso de los clientes a Internet. Un ISA es en realidad un software conocido como 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

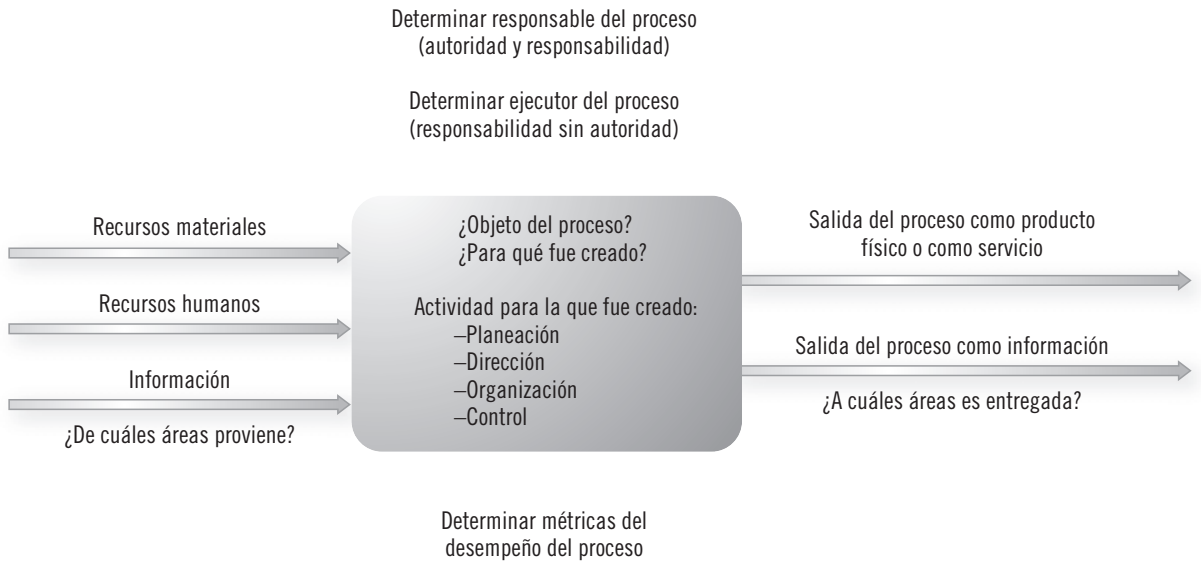
es posible detener el control de calidad del producto, ya que es impensable elaborar productos durante tan sólo una hora, sin saber a ciencia cierta cuál es la calidad que se va a entregar al consumidor. Si la empresa es de servicios, podrá detenerse cualquier área, pero el servicio, sobre todo si ya 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.

Actividad de aprendizaje

En equipo creen un video donde presenten la informática forense. Sean creativos en su elaboración. La duración del video no debe ser mayor a 10 minutos. Compartan su trabajo con el grupo y seleccionen los tres mejores.

Comprueba tus saberes

1. Explica con tus propias palabras el concepto general de *buen gobierno.*

2. Describe el concepto de buen gobierno en informática.

3. De acuerdo con COBIT, ¿en cuál parte de la declaración del Buen Gobierno de las TIC se contempla la elaboración de un plan estratégico para contingencias informáticas?

4. Explica de manera breve el contenido de la Norma ISO 31000.

5. Describe con tus propias palabras el contenido de la Norma ISO 27000.

6. Explica el contenido general de la norma BS 25999.

7. Define con tus propias palabras el riesgo de acuerdo a la Norma ISO 31000.

8. Describe al menos tres beneficios que obtiene una organización si decide administrar sus riesgos informáticos.

9. ¿En qué consiste un plan de contingencia informática?

10. Menciona el contenido del plan de prevención de riesgos.

11. Describe el contenido del plan de predicción de riesgos.

12. Explica con tus propias palabras el contenido del plan de recuperación del negocio o plan de corrección.

13. Menciona al menos tres características que tiene un proceso para que pueda ser identificado.

14. ¿A qué se refiere la clasificación cualitativa de la relevancia de los procesos?

15. Menciona al menos cinco riesgos físicos internos.

16. Menciona dos riesgos físicos externos.

17. Menciona al menos siete riesgos lógicos.

18. Describe con tus propias palabras en qué consiste la segunda parte del plan de prevención de contingencias.

19. Define con tus propias palabras qué es un plan de recuperación del negocio.

20. Menciona los tres pasos que componen el plan de recuperación del negocio.

21. ¿Cuáles son las cuatro actividades del Círculo de Deming?

22. Describe con tus propias palabras al menos cinco beneficios que se obtienen al adoptar la Norma ISO 27000.

23. Menciona las cinco fases de un plan de continuidad del negocio.

24. Cita al menos cinco documentos que requiere la Norma 25999-2.

25. Escribe con tus propias palabras una definición de informática forense.

26. Describe los pasos del método científico.

27. ¿Cuáles son los principios en los cuales se basa la informática forense?

28. Describe con tus propias palabras los cuatro factores que se requieren para evaluar las pruebas científicas que se presentan en un juicio legal.

Referencias bibliográficas

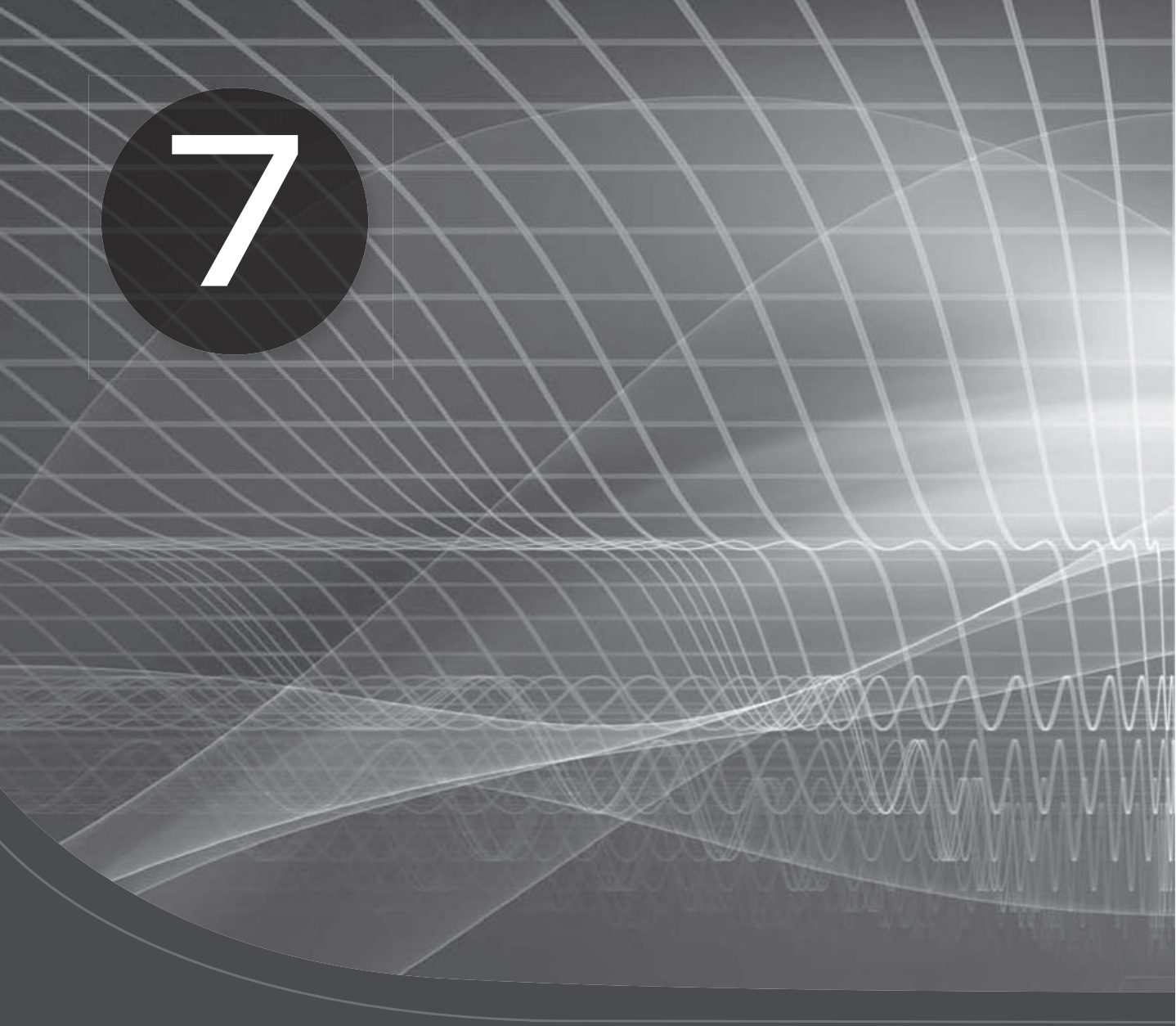
1. Pironti, John. *Five Key Information Security Incident Response Playbooks.* Vol. 17, 2015 | At ISACA.
2. Rigante, Franco. *CISA, CRISC, PMP. 8 Practical Steps to Starting Risk Identification*. 14 July 2015 | ISACA Now Blog.

Referencias electrónicas

1. www.isaca.org
2. http://articulos.softonic.com/eliminar-metadatos-documentos-doc-jpg-mp3-pdf?ex=SWH-1566.0
3. https://es.wikipedia.org/wiki/Plan_de_contingencias
4. https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio
5. https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_la_continuidad
6. https://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres
7. http://criminalistica.mx/areas-forenses/audio-video-y-fotografia/1101-ique-es-la-informatica-forense-o-forensic
8. http://advisera.com/27001academy/es/what-is-bs-25999/
9. http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio

10. https://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres
11. https://www.blackbagtech.com/software-products/mobilyze.html
12. https://es.wikipedia.org/wiki/Miner%C3%ADa_de_datos
13. http://isobuster.softonic.com/
14. http://browserpassworddecryptor.softonic.com/
15. http://bulletspassview.softonic.com/
16. http://wirelesskeydump.softonic.com/
17. http://www.alexbarnett.com/chatsniper.htm
18. http://www.nirsoft.net/utils/my_last_search.html
19. http://www.mcafee.com/us/downloads/free-tools/rifiuti.aspx
20. http://fid3.com/products/fi-tools
21. http://metadata-analyzer.softonic.com/
22. http://www.moonsols.com/windows-memory-toolkit/
23. http://osforensics.softonic.com/
24. http://windows-file-analyzer.softonic.com/
25. http://diskdigger.softonic.com/
26. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#sthash.Xkay1rQG.dpuf
27. http://testdisk.softonic.com/

7



Objetivo general

Que el estudiante conozca los aspectos más relevantes de una auditoría informática y, en especial, de una auditoría de seguridad de la información.

Objetivos específicos

- Comprenderás el concepto y la importancia de una auditoría informática.
- Identificarás las etapas que comprende la realización de una auditoría informática.
- Conocerás algunas de las herramientas disponibles en el mercado para realizar una auditoría informática.

Auditoría en seguridad informática

¿Qué sabes?

- ¿Cómo definirías una auditoría informática?
- ¿Qué aspectos se deben considerar en una auditoría informática?
- ¿Por qué es importante realizar una auditoría informática?
- ¿Te gustaría ser auditor informático?

Competencias a desarrollar

- El alumno describe y entiende los aspectos fundamentales de una auditoría en seguridad informática.
- El alumno comprende la importancia de realizar en forma periódica auditorías de seguridad informática, tanto internas como externas.

7.1 Introducción

En la actualidad se utilizan dos metodologías para la evaluación de sistemas: *Análisis de riesgos* y *Auditoría informática*, lo que implica dos enfoques distintos. Por una parte, la auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras que el análisis de riesgos facilita la evaluación de los riesgos para tomar medidas preventivas, como se trata en el capítulo 6, Las contingencias en seguridad informática e informática forense.

La palabra *auditoría* tiene un significado muy amplio. Por ejemplo, en el *Diccionario Oxford* se le define como *el examen oficial de las finanzas de un negocio (o de la calidad) para ver que sean ciertas y correctas*. No obstante, este mismo diccionario también la define como *alguien que asiste a un curso sin derecho a recibir reconocimiento; en español diríamos oyente*. Por su parte, el *Diccionario Durvan de la lengua española* define *auditoría* como *el empleo del auditor*, en tanto que al *auditor* lo define como *un funcionario de un cuerpo jurídico que informa sobre la interpretación y la aplicación de las leyes y propone la resolución correspondiente a los procesos instruidos por un tribunal*. De estas dos definiciones vemos que tanto auditor como auditoría están relacionados con el verbo latino *audire* o *auditus*, que significa oír o escuchar, o examinar e interpretar la aplicación de ciertas leyes.

En el mundo de los negocios, la auditoría más conocida, y quizá la más antigua, es la *auditoría contable,* que es la que define el *Diccionario Oxford*; de ahí que a partir de la utilidad y las enormes ventajas de una auditoría contable, el mundo industrial y empresarial comenzó a auditar muchas de las actividades que se realizan en una organización o empresa. De esta forma, una definición más actualizada de la palabra *auditoría* es la que se presenta a continuación:

> *Es un examen crítico y sistemático que normalmente realiza un grupo de personas expertas e independientes de la entidad auditada, con el objetivo de verificar que dicha entidad cumpla con las normas, leyes, procesos, etcétera, bajo las cuales opera o lleva a cabo su actividad. Tal verificación se debe realizar utilizando métodos de investigación o de verificación en general aceptados por el área de actividad sobre*

El *Diccionario Merrian Webster* refiere que la palabra auditoría tiene su origen en el latín *auditus* o *audire*, que significa el acto de escuchar. Hoy día, se tiene conocimiento de que a mediados del siglo xv se empezó a utilizar la palabra en el idioma inglés. En realidad, la lengua del latín es más antigua que el inglés y de la palabra *audit* derivan otras, como auditorio, audífonos, audición, etcétera; todas relacionadas con el verbo castellano oír.

la que se efectúe la auditoría, de modo que se realice una evaluación profunda de la forma en que se están realizando las actividades en el área auditada.

En la anterior definición hay varios aspectos importantes a destacar: toda organización empresarial, industrial o de gobierno opera bajo ciertas políticas, normas o leyes que debe acatar en forma cotidiana; por ejemplo, en el aspecto contable, la forma de registrar las entradas y salidas de dinero son la base para la declaración de impuestos (en México), y se fundamentan, primero, en la Ley general del impuesto sobre la renta y, luego, en el Boletín B-10 del Colegio de Contadores; por tanto, al elaborar sus registros contables, toda empresa o negocio debe hacerlo con un estricto apego a esas leyes y normas. Ahora bien, si de lo que se trata es de la calidad de un producto, en la actualidad existe una serie de parámetros estadísticos de calidad que aparecen en normas oficiales de calidad, emitidas por la Secretaría de Salud en México, a las cuales deberá apegarse toda industria que elabore determinado producto.

En esta misma definición también se menciona que los métodos de evaluación o de verificación que implica la auditoría deben ser reconocidos y aceptados, tanto por todos los auditores del ramo, como por las entidades que son auditadas, para que los resultados sean válidos. Por último, también hace énfasis en que los auditores deben ser personas altamente capacitadas e independientes de la entidad auditada. Ambos requisitos son importantes, pues para poder realizar un análisis profundo y emitir una opinión válida se requiere que el personal que realice la auditoría no sólo domine el área de auditoría, sino que también sea ajena a la entidad auditada, a fin de que su opinión no se vea influenciada por presiones del personal que trabaja en la entidad auditada. En este punto conviene recordar que existe la auditoría fiscal, donde personal del gobierno audita a empresas particulares para verificar si la declaración de impuestos que presentó la empresa ante el SAT es verídica y confiable; de lo contrario, la empresa auditada podría ser sujeta a multas y el propietario de la misma sería juzgado por defraudación fiscal.

Como éstos, se pueden citar cientos de ejemplos de que todas las actividades empresariales están regidas en todo momento por leyes o normas;

por tanto, los dueños, el administrador o el director general de la empresa u organización deben ser los primeros interesados en conocer si al interior del negocio se obedecen dichas directrices en las actividades cotidianas de la organización, por lo que se considera la persona indicada para ordenar la ejecución de auditorías en las diferentes áreas.

Existen diversas clasificaciones de los diferentes tipos de auditorías que se practican a las empresas u organizaciones; sin embargo, para los objetivos que se plantean en este libro, a continuación sólo se citan las más conocidas.

- En la actualidad, las auditorías más conocidas son las que se realizan a todas las normas ISO para otorgar certificaciones en lo que regula cada norma. Hoy día existen normas ISO para casi todas las actividades de las empresas de manufactura y de servicios.
- Auditoría a las certificaciones en las normas BS 25999 y del Uptime Institute, cuyo objetivo es obtener dichas certificaciones.
- Auditoría contable, que busca analizar las finanzas o estados financieros de una empresa.
- Auditoría ambiental, que se encarga de examinar si una empresa contamina el ambiente con sus emisiones contaminantes al agua, al suelo o a la atmósfera.
- Auditoría administrativa, cuya finalidad es analizar si los procesos y funciones administrativas dentro de una empresa se realizan de manera eficaz y eficiente.
- Auditoría informática, cuyo objetivo es recabar, agrupar y evaluar evidencias para determinar si el sistema informático salvaguarda los activos (hardware y software), mantiene la integridad de los datos y ayuda a lograr la misión y la visión de la empresa mediante el uso eficiente y eficaz de los recursos informáticos. Asimismo, verifica el estricto apego a las normas y leyes correspondientes y, en general, de la gestión eficaz de todas las TIC que posea la organización. Esta auditoría, a su vez, se subdivide en auditorías a las diferentes áreas que comprenden las TIC:
  - Auditoría de la gestión de las TIC. Considera la contratación de bienes y servicios, la documentación de los programas, etcétera.

- Auditoría Legal del Reglamento de Protección de Datos. Verifica el cumplimiento legal de las medidas de seguridad exigidas por la Ley general de protección de datos personales.
- Auditoría de los datos. Realiza la clasificación de los datos y estudia las aplicaciones y análisis de los flujogramas.
- Auditoría de las bases de datos. Audita los controles de acceso y los protocolos de autorización de nuevos usuarios, de actualización, de integridad y calidad de los datos.
- Auditoría de la seguridad física. Verifica la ubicación de la organización, a fin de evitar ubicaciones de riesgo, y en algunos casos no revelando la ubicación física de ésta. En general, se refiere a los aspectos mostrados en el capítulo 6, Las contingencias en seguridad informática e informática forense.
- Auditoría de la seguridad lógica. Se refiere a todos los aspectos mostrados en el capítulo 6, Las contingencias en seguridad informática e informática forense.
- Auditoría de las comunicaciones. Se refiere a la auditoría de los procesos de autenticación y cifrado en los sistemas de comunicación, al uso eficiente de redes internas y externas y al uso de cualquier dispositivo empleado por la empresa para comunicarse de manera interna y externa.

Actividad de aprendizaje

Elabora un esquema donde se visualicen los diferentes tipos de auditorías antes presentados y resaltes su importancia. Entrega tu trabajo a tu profesor.

Como el tema central de este texto es la seguridad informática, la auditoría en este campo versa exclusivamente alrededor de este tema y no de todo lo que puede incluir una auditoría informática en general.

Existen claras diferencias entre las funciones del control informático y las de la auditoría informática, ya que el área informática establece los procesos informáticos seguros, mientras que el control interno establece los controles; entonces, la auditoría informática evalúa el grado de control.

Las funciones básicas del control interno informático son las siguientes:

- Administración de la seguridad lógica.
- Funciones de control con otros departamentos.
- Control de normas y cumplimiento del marco jurídico.
- Desarrollo y actualización del plan de contingencias, manuales de procedimientos, etcétera.
- Desarrollo de las normas internas de seguridad informática.
- Definición de los procedimientos de control.
- Control de los soportes físicos, como el equipo y dispositivos de acceso.
- Control y restricción del acceso a información privilegiada.
- Control de la calidad del software.
- Control de la calidad del servicio informático.
- Control y manejo de claves de cifrado.
- Vigilancia del cumplimiento de las normas y los controles.
- Control de medidas de seguridad física o corporativa en la informática.
- Responsable de datos personales.

Todas estas funciones tienen como objetivo general el control informático, a fin de que haya un uso seguro y confiable de las TIC entre los usuarios, la informática y el control interno, todos éstos auditados por la auditoría informática.

Actividad de aprendizaje

Elabora un diagrama de flujo donde muestres las funciones básicas del control interno informático.

7.2 Las etapas de una auditoría

Toda auditoría constituye un proceso crítico y sistemático, lo que significa que todos los auditores siguen ciertos pasos establecidos con anterioridad en su examen, mediante los cuales pueden observar puntos muy finos de cada una de las actividades que se realizan en la empresa u organización que están auditando. Las etapas comunes de una auditoría son:

1. **Planeación de la auditoría.** La primera actividad de un auditor es recabar todos los documentos internos referentes a políticas establecidas y normas que deben acatarse, por ejemplo, normas de calidad del producto, ambientales, etcétera, y verificar que se estén cumpliendo estrictamente en la empresa u organización, mediante la observación de las actividades cotidianas de los trabajadores y con un trabajo apegado a las normas y los estándares reconocidos, como los de COSO, IFAC, IIA e ISACA, en el caso de la informática.
2. **Realización de la auditoría.** En este punto, el auditor observa y verifica la forma en la que se realizan las actividades de manera cotidiana, por lo que requiere de la colaboración de todo el personal del área auditada. Aquí, el auditor solicita bitácoras de registro de actividades, hace entrevistas personales a los trabajadores y, sobre todo, realiza observaciones de la forma de trabajo con métodos de análisis reconocidos y aprobados a nivel mundial.

   Durante los trabajos de auditoría a un área específica de la empresa u organización, el auditor no sólo entrevista al personal de dicha área, sino también al personal de áreas relacionadas. Durante las entrevistas se aplican encuestas o cuestionarios formulados con anterioridad.

   En tanto, durante las observaciones, el auditor recaba suficientes datos para realizar análisis estadísticos y listas de verificación.

   En el ámbito industrial, empresarial u organizacional es bien sabido que cada vez que se va a llevar a cabo una auditoría, el personal se prepara para que "todo esté en orden", y una vez pasada la auditoría las cosas se

COSO (Committee of Sponsoring Organizations of the Treadway Commission): Iniciativa de cinco organismos para la mejora de control interno dentro de las organizaciones.

IFAC (International Federation of Automatic Control), fundada en 1957 como una federación internacional, donde cada uno de los países miembros envía representantes de las sociedades científicas y de ingeniería que existen en su propio país.

IIA (Institute of Internal Auditors), con más de 180 000 miembros en casi 190 países, es el líder de los profesionales en auditoría interna, autoridad reconocida y principal educador en su área.

relajan un poco. Para evitar esta situación es conveniente realizar auditorías internas con relativa frecuencia, por ejemplo, cada dos meses; y externas cada seis meses. Esto evitará el estrés que causa la auditoría y mantendrá al personal siempre en el límite, como si cada día fuera a haber una auditoría, que es lo que en realidad se necesita en el área de seguridad informática.

En este punto, también es muy importante que el jefe de área haga saber a los trabajadores que la auditoría en realidad es un beneficio para la empresa, en vez de concebirla como una molestia o una amenaza a la conservación de los puestos de trabajo. Los trabajadores deben estar convencidos de que una auditoría externa los evaluará en la eficiencia de trabajo del área y dará constancia de que en realidad desempeñan sus labores como se espera que lo hagan. En seguridad informática, no suelen observarse fallas en los planes de contingencia, hasta que una amenaza se vuelve realidad; por tanto, de lo que se trata es que la auditoría siempre mantenga al personal alerta para que nunca, o muy raras veces, una amenaza logre dañar al área informática y a la empresa.

3. **Análisis de los datos recabados y de las condiciones observadas.** Una vez que el auditor concluyó en forma exhaustiva la etapa 2, analiza a fondo todos los datos recabados y compara los resultados contra estándares generalmente aceptados. Para ello, puede hacer uso de cualquier herramienta gráfica, como diagramas de flujo, gráficas de cualquier tipo o incluso mapas conceptuales. En este punto es importante la preparación, capacidad y especialización del auditor o del grupo de auditores. Por su condición de especialista, el análisis de un auditor es objetivo y siempre debe estar perfectamente sustentado para poder realizar el último paso de la auditoría.

4. **Elaboración de un informe escrito y emisión de una opinión.** La última etapa, después de que el auditor ha realizado un análisis a fondo de los datos obtenidos, es emitir una opinión, la cual puede estar orientada en cuatro sentidos:

- Opinión limpia, u opinión sin calificación, lo que significa que durante la auditoría no se encontró ninguna deficiencia relevante acerca de lo observado y se considera que cada trabajador realiza su trabajo de manera correcta, acatando leyes y normas establecidas. Para la emisión de esta opinión, el auditor debe presentar evidencias para demostrarlo.
- Opinión negativa o con calificación, lo que implica una serie de observaciones relevantes acerca de algunas deficiencias que presentan los procesos que se llevan a cabo en el área auditada. Respecto al área de seguridad informática, las observaciones podrían estar relacionadas con el hecho de que en determinados puntos o procesos se observaron puntos de vulnerabilidad o exposición al riesgo que representan un peligro para la empresa. Al emitir esta opinión el auditor no observó debilidad material o física.
- Opinión adversa, lo que significa que, además de las observaciones del inciso anterior, también se observaron deficiencias materiales o físicas.
- Sin opinión, se refiere a que el auditor no tuvo oportunidad de hacer todas las observaciones requeridas, ya sea por obstrucción de los propios trabajadores o porque la documentación o las evidencias de trabajo no estaban disponibles, de manera que el auditor prefiere no emitir una opinión, pues considera que no recabó las pruebas suficientes.

En cualquier caso, siempre se aconseja que antes de emitir una opinión, el auditor se reúna primero con el jefe o director del área auditada, luego con el director general y, al final, se lleve a cabo una reunión de los tres con todo el personal. Siempre habrá algo importante que decir, desde una felicitación, hasta una llamada de atención, ya sea por deficiencias observadas o por falta de cooperación para realizar la auditoría.

Todos los esfuerzos que se hacen para que la empresa o el área de informática sean auditadas obedecen a que esta práctica siempre trae beneficios, como los que se mencionan a continuación.

- En primer lugar, el director general conocerá, de parte de una persona externa muy capacitada, si el área auditada en realidad trabaja como se espera que lo haga.
- Muchas auditorías son para obtener certificaciones, de manera que cuando se logra cualquier certificación, ISO, BS, Uptime Institute, ISACA, etcétera, la empresa puede anunciar públicamente la certificación, con lo que genera confianza entre los propios empleados, proveedores y, clientes de la empresa, lo que garantiza una mejora en el clima laboral.
- El director general y la junta de accionistas de la empresa constatan que los recursos económicos invertidos están siendo bien empleados.

Actividad de aprendizaje

En equipo localicen una empresa o institución donde se efectúen auditorías informáticas, verifiquen con el personal cuáles son las etapas que siguen para realizar la auditoría y qué problemas tienen al realizarla. Con la ayuda de un video o presentación electrónica expongan sus trabajos frente al grupo.

Requisitos para ser auditor en informática

Como se dijo antes, un auditor es una persona de alta preparación, es un especialista en su área. Para obtener una licencia de Auditor Certificado en Sistemas de Información (CISA, por sus siglas en inglés; Certified Information Systems Auditor), licencia avalada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA, por sus siglas en inglés; Information Systems Audit and Control Association), los aspirantes deben cumplir con los siguientes requisitos, de acuerdo con lo que se establece en la página de la ISACA (www.isaca.org):

1. Aprobar el examen de Código Profesional de Ética de la ISACA.

2. Comprobar cinco años de experiencia en auditoría de sistemas de información, control interno y seguridad informática.
3. Estar actualizado con cursos de educación continua en los últimos años.
4. Si no se pueden comprobar los puntos 2 y 3, se pueden sustituir por el punto 5.
5. Un año de experiencia en auditoría de sistemas, control interno y seguridad informática, además de:
6. haber completado de 60 a 120 horas de estudios profesionales, que pueden ser sustituidos por uno o dos años de experiencia, respectivamente, de auditoría de sistemas, control interno y seguridad informática.
7. Dos años de instructor de tiempo completo en alguna universidad de prestigio en campos relacionados; por ejemplo, ciencias computacionales, contabilidad, auditoría de sistemas de información, que pueden ser sustituidos por un año de experiencia de auditoría de sistemas de información, control interno y seguridad informática.
8. Presentar un examen de conocimientos que consta de 200 preguntas de opción múltiple que deben ser contestadas en cuatro horas. El examen está dividido en cinco áreas (hasta el manual de 2012): 1) el proceso de auditoría de SI (14%), 2) Gobierno de TI (14%), 3) Administración del ciclo de vida de infraestructura y sistemas (19%), 4) Soporte y entrega de servicios de TI (23%) y 5) Protección de los activos de información (30%).
9. Para no perder la certificación, el auditor debe concluir de manera satisfactoria determinado número de horas anuales de cursos de actualización. El número de horas dependerá del tipo de curso.

Criterios que se deben emplear en una auditoría

Cuando un hecho se evalúa de manera profesional, siempre debe haber una serie de criterios bien entendidos acerca de la forma de hacer las cosas. Un investigador en informática forense, así como un auditor en cualquier área, en este caso en seguridad informática, debe tener la preparación adecuada,

lo que incluye un comportamiento ético fuera de toda duda al realizar una auditoría. Además, el primer criterio que debe aplicar es el de la *objetividad*.

Ser objetivo implica reportar lo que se está observando, sin sesgos de grupos de trabajo, de políticas internas de la empresa o de personas interesadas en que el resultado de la auditoría aparezca de cierta forma. Un *reporte objetivo de auditoría* debe declarar directamente los problemas o debilidades encontradas, sin palabras ambiguas que pudieran conducir a una interpretación equivocada de los resultados del reporte.

Una auditoría se realiza para encontrar vulnerabilidades del sistema o una fuerte exposición a riesgos de ataques físicos o lógicos. El criterio de *relevancia* implica que el reporte debe centrarse en destacar estos puntos, vulnerabilidad y riesgos que, de suceder, podrían poner a la empresa en peligro de detenerse temporalmente e, incluso, amenazar su supervivencia. Hay muchos riesgos y tipos de daños que pueden causar a la empresa, pero el auditor deberá enfocarse de manera especial en los que son en realidad relevantes, por el peligro que representan.

Una cosa es reportar un riesgo elevado en un punto del sistema, y otra es poder evidenciarlo y medirlo. El siguiente criterio que debe tener el auditor es el de *medición cuantitativa de los problemas.* En el capítulo 6, Las contingencias en seguridad informática e informática forense, se mencionó al menos un método para demostrar que un tipo de riesgo tenía más probabilidad que otros riesgos, de suceder o de repetirse; por tanto, el auditor, con su amplia preparación, deberá reportar no sólo el tipo de riesgo detectado y la magnitud del daño que causaría, sino también la posibilidad, expresada cuantitativamente de que suceda determinado riesgo.

Por otro lado, el lenguaje técnico que utilice el auditor en su reporte será entendido por el jefe o director del área de informática o de sistemas de la empresa, pero el reporte de un auditor suele ser analizado también por otras personas, como el director general o, incluso, algunos accionistas de la organización, quienes quizá no posean los conocimientos para entender el lenguaje técnico. Por ello, el cuarto criterio que debe aplicar el auditor es el de *expresión sencilla del problema,* a fin de que el reporte pueda ser entendido por casi cualquier persona, de manera que no se preste a diversas

interpretaciones. El lenguaje utilizado debe ser claro y simple, explicando los tecnicismos que pudiera ser necesario emplear en el reporte.

Es importante mencionar que todos los involucrados en una auditoría deberían conocer que los criterios mencionados son criterios generales que han sido emitidos y aceptados por cuerpos colegiados o agrupaciones de profesionales en esa área de conocimiento y, que además, dichos criterios se han hecho públicos y están a disposición de cualquier persona que quiera consultarlos. Los nombres asignados a los criterios varían de acuerdo al tipo y área de la auditoría donde se aplican, pero la idea que conlleva su nombre es lo más importante, y esa idea siempre prevalece, sin importar el área donde se utilicen. Esto es lógico, no se puede utilizar la misma terminología en una auditoría informática que en una contable, o en una auditoría de calidad; sin embargo, la idea de los criterios generales debe prevalecer en cualquier tipo de auditoría.

Los estándares de contabilidad del sector público internacional (IPSAS, por sus siglas en inglés) son un conjunto de estándares contables emitidos por el Concejo de IPSAS, para su uso en entidades del sector público en todo el mundo, para la preparación de los estados financieros. Estos estándares están basados en los Estándares de los Reportes.

Todas las auditorías han tomado los criterios e ideas de la *auditoría contable*, que fue el primer tipo de auditoría que se desarrolló hace cerca de cien años. Controlar el estado financiero de una empresa fue la primera preocupación de las organizaciones de aquel tiempo, y aún sigue siendo una gran preocupación. Esta antigüedad hace que los criterios y estándares de la auditoría contable sean los más completos y más aceptados internacionalmente, que es lo que están buscando las auditorías en todas las áreas de aplicación, como las ISO en todo su espectro, y la auditoría informática de ISACA y de COBIT, iniciando por la aceptación internacional por parte de empresas privadas.

7.3 Cómo se realiza una auditoría

A continuación se explica con detalle, cómo se debe realizar una auditoría.

El plan de la auditoría

El auditor debe comprender la actividad de la empresa que será auditada, entender sus áreas de riesgo, los principales riesgos a los cuales está expuesta

y, con base en esos parámetros, comprometerse a realizar la auditoría de una forma objetiva, pues cada tipo de organización está sujeta a leyes de manejo de información distintas. Por ejemplo, una institución bancaria no está sujeta a las mismas leyes de control de la privacidad de datos personales que una empresa que fabrica ropa. De hecho, no sólo las instituciones bancarias, sino todas aquellas que realicen ventas por Internet, como aerolíneas, hoteles internacionales, etcétera, o que estén autorizadas para realizar transferencias electrónicas de dinero, deben contar con sistemas inviolables. Estos sistemas informáticos se rigen por leyes o reglamentos mucho más estrictos que aquellos que poseen las empresas que no realizan ventas por Internet. Una auditoría informática no la puede hacer cualquier auditor certificado por ISACA, ya que se requiere de una mayor especialización.

Por esta razón, y como parte de la elaboración del plan de auditoría, el auditor debe contemplar todos los recursos que necesitará durante la realización de la auditoría a una organización, a fin de hacer un compromiso y cumplir con todas las expectativas planteadas, incluyendo no rebasar el presupuesto ni dejar algún riesgo sin evaluar. También, como parte del plan, el auditor determinará las herramientas que necesitará para reunir evidencias, realizar pruebas del funcionamiento adecuado de ciertos dispositivos de seguridad y verificar que estén disponibles dentro de la empresa, de lo contrario, él deberá conseguirlas.

Todo auditor debe entregar por escrito el plan de la auditoría, a fin de que éste sea aprobado por la empresa auditada en todos los sentidos: contenido, presupuesto y requerimientos. Para ello, el plan debe contener los objetivos de la auditoría, ya que no es lo mismo auditar la seguridad que auditar la gestión de los sistemas. Asimismo, debe especificar el enfoque de la auditoría, el tiempo que tomará realizarla, los recursos necesarios para llevarla a cabo y las responsabilidades de todos los involucrados, tanto del personal interno que será entrevistado, como de los mismos auditores; no hay que olvidar que una auditoría suele ser realizada por un grupo de expertos y rara vez por una sola persona.

El plan también debe declarar las técnicas y los dispositivos que serán empleados para recabar evidencias, así como los procedimientos o métodos

para verificar los resultados de las evidencias obtenidas; sobre todo si alguna evidencia tiene efecto o uso legal. Cada uno de los miembros del grupo auditor, de acuerdo con su experiencia, debe aportar los métodos o técnicas más apropiados para recabar evidencias durante la auditoría.

Cada actividad establecida en el plan de auditoría debe declararse con un tiempo de ejecución, aunque el plan general puede experimentar ajustes de actividades y tiempo, según las condiciones que se vayan presentando, lo cual también debe especificarse en el plan, sobre todo si durante la ejecución de la auditoría se encuentran anormalidades inesperadas y es necesario estar completamente seguro de estos nuevos hallazgos. Desde luego, el tiempo estimado de cada actividad de la auditoría será más preciso en la medida en que el auditor líder tenga más experiencia en auditorías similares.

Todos los interesados deberán recibir una copia del plan de auditoría aprobado por la dirección general, a fin de que conozcan cuál será su actividad durante la realización de ésta. La mayoría de las personas de la empresa serán entrevistadas, mientras que la participación de otras será determinante en el éxito de la auditoría.

Ejecución de la auditoría

Iniciar la ejecución de una auditoría no es sólo ponerse a trabajar. Como la auditoría suele ser labor de un grupo de auditores, las actividades de cada miembro se asignan de acuerdo con su experiencia. Asimismo, antes de iniciar, siempre se debe informar al grupo de auditores diversos aspectos, entre los que destacan la manera en la que se va a controlar el avance del trabajo individual, hasta dónde llega la responsabilidad de cada quien en caso de que se presente algún conflicto durante la ejecución y el reporte que cada auditor debe entregar del trabajo realizado; en general, se acostumbra que antes de entregar el informe definitivo, cada miembro del equipo revise el trabajo de otro u otros compañeros auditores, a fin de enriquecer el contenido final.

Durante la ejecución, cada auditor deberá obtener la mejor evidencia posible para sustentar la emisión de cualquier evaluación relacionada, cuidando de no sobrepasar el tiempo ni el presupuesto estimado; no obstante, si alguien considera que la evidencia obtenida no es suficiente para los fines que se

persiguen, deberá hacer un nuevo intento para conseguirla. Si esto procede, siempre se deberá realizar bajo un formato preestablecido en el plan de la auditoría. El auditor nunca debe olvidar que el método que siguió para la obtención de la evidencia debe tener una base científica y debe ser reproducible por cualquier otro auditor calificado, de manera que ambos puedan llegar al mismo resultado o conclusión.

Al momento de obtener evidencias acerca de determinado punto de la auditoría, no hay que olvidar el criterio de medir cuantitativamente lo que sea medible, como vulnerabilidades, deficiencias, efectos negativos, frecuencia de repetición, errores cometidos, controles que no funcionan, etcétera; esto básicamente debe expresarse con números y no con comentarios como: "en varias ocasiones no se ha efectuado el escaneo de puertos abiertos". Por ejemplo, un reporte de preferencia correcto debe decir: "en 50 ocasiones programadas, en que debió hacerse un escaneo de puertos abiertos, no se realizó en 8 de éstas; por tanto, la red fue vulnerable 16% del tiempo". Para obtener este tipo de datos, una política de seguridad de la empresa debe ser: "llevar una bitácora con todas las actividades programadas de supervisión de medidas de seguridad y cada vez que se realice dicha actividad, anotar en la bitácora todos los datos que se relacionan a continuación".

- Fecha
- Hora
- Persona que realizó la actividad
- Número de puertos que se encontraron abiertos
- Descripción de la causa por la que estaban abiertos
- Mencionar si hubo intrusión o intento de intrusión en algún puerto abierto
- Cuántas y cuáles

Sin embargo, si en la empresa auditada no existe tal política de supervisión, el auditor está obligado a anotar: "falta de política de seguridad adecuada en...", y esta ausencia se tomará como una vulnerabilidad y se propondrá como un punto de mejora.

La recomendación aquí es, entonces, expresar, en la medida de lo posible, todas las observaciones hechas de manera cuantitativa, haciendo énfasis en que las políticas de seguridad internas deben dar lugar a estas mediciones cuantitativas o, en su defecto, evidenciando la falta de políticas adecuadas o de políticas no claras en este sentido. Hay que recordar que muchas medidas de seguridad se deben tomar por ley, de manera que la observación de dichas medidas debe ser mucho más rigurosa, pero sobre todo conociendo al pie de la letra las exigencias legales.

Con el propósito de recabar evidencia durante una auditoría, se recomienda llevar un registro de los métodos empleados por el auditor, junto con los resultados obtenidos con cada método aplicado. Para ello, existen varios métodos generales para recabar evidencias. Entre los principales se pueden mencionar los siguientes.

- Preguntas en entrevistas persona a persona
- Procedimientos analíticos
- Observación
- Inspección de registros escritos (en papel o electrónicos)
- Pruebas de funcionamiento de dispositivos

Además de los anteriores, es posible seguir cualquier otro método, siempre y cuando éste sea reconocido y tenga validez legal, además de que haya sido utilizado en otras auditorías, dentro o fuera de la empresa en la que se realiza la auditoría.

Uno de estos métodos de investigación consiste en revisar los registros de control que ejecuta la empresa en forma cotidiana. Antes, ya se mencionó la necesidad de consultar este tipo de registros, en papel o electrónico, ya que constituyen una buena evidencia de las deficiencias o los aciertos del control de la seguridad informática. Además, también es importante que la empresa cuente con políticas y procedimientos muy claros en este aspecto; de lo contrario, no se podrá culpar a los trabajadores de omitir hacer algo que nadie les dijo por escrito que hicieran.

Por esta razón, los auditores deberán conocer y llevar consigo por escrito, durante la auditoría, todas las políticas y los procedimientos que se deben realizar por parte del personal. Incluso puede haber una política escrita; por ejemplo, *"se deberá ejercer un control cotidiano sobre las principales fuentes de riesgo informático que pudieran existir en la empresa",* pero si esta política general no se acompaña de un procedimiento por escrito sobre cómo ejercer o ejecutar ese control, la falla no será atribuible a los trabajadores sino a las autoridades.

Para aclarar esto es preciso establecer de manera puntual que el director general y el director o jefe de sistemas son los responsables de elaborar el plan general de contingencias, mientras que el director de sistemas es el encargado de dirigir la implantación del plan y de los tres subplanes; luego, él mismo debe controlar que funcionen de acuerdo con lo planeado para que se alcancen los objetivos del plan de contingencias. El control es una de las cuatro fases del proceso administrativo que incluye todas las actividades que se deberán emprender a fin de garantizar que las actividades y operaciones reales coincidan con las planeadas. El control siempre se ejerce con datos y resultados cuantitativos, y para que esos datos se generen es necesario diseñar formatos y actividades específicas con tiempos de ejecución, todo esto comunicado por escrito a los trabajadores, quienes también informarán por escrito que llevaron a cabo las actividades programadas, en tiempo, en forma y en cantidad, al llenar los formatos establecidos.

Toda esta trama debe ser conocida a la perfección por el auditor, pues los registros son una de las principales fuentes de evidencia con las que cuenta para evaluar el desempeño de la seguridad informática en una empresa. Además, también debe considerar si la evidencia recabada por los registros es suficiente para emitir una opinión. Sin embargo, las evidencias no sólo se obtienen a partir de registros escritos, también pueden provenir de entrevistas personales, en cuyo caso es mucho más difícil tomar las opiniones verbales como base científica para emitir juicios.

Una evidencia obtenida con base científica significa que si otro auditor sigue el mismo procedimiento de análisis llegará a obtener la misma evidencia y, por tanto, emitirá la misma opinión; es decir, una evidencia científica es reproducible.

Considerando que en el plan de la auditoría se propuso la mejor alternativa para reunir suficientes evidencias en cuanto a costo y tiempo, si durante su ejecución no se observa que la alternativa propuesta ha obtenido buenos

resultados, no importa elevar el costo y el tiempo, si con ello se van a obtener las evidencias suficientes y con base científica; el incremento del tiempo y costo es uno de los riesgos de la ejecución, ya que lo que importa es lograr los objetivos de la auditoría.

En este sentido, las mejores evidencias son aquellas que se obtienen de manera escrita, en lugar de expresiones orales; obtenidas por profesionales en el área, en vez de aquellas que provienen del personal de la empresa auditada.

Mantener con ética y prudencia las evidencias y las opiniones

Mediante el contrato que se firma para realizar la auditoría, el auditor o el grupo de auditores están autorizados para revisar y, por tanto, conocer información privilegiada del área auditada. Por esta razón, deben tener una arraigada ética, a fin de que la dirección general de la empresa esté totalmente segura de que los datos confidenciales no serán revelados y que serán mantenidos con la misma prudencia tiempo después de haber terminado la auditoría.

Éste es un punto muy delicado. Por eso, al planear y autorizar la auditoría, debe quedar por escrito cuáles datos podrán revelarse ante autoridades civiles, en caso de que sea necesario acudir a estas instancias por algún problema. Por otro lado, el auditor debe conocer a la perfección las leyes civiles a fin de poder discernir cuál información debe mantenerse bajo reserva para hacerla pública y cuál debe comunicarse a las autoridades civiles, en caso de detectar algún fraude o acto ilegal por parte de la empresa auditada, aunque el contrato de auditoría haya prohibido la divulgación acerca de dicha información.

Por esa razón, se recomienda que el auditor conozca a la empresa, al medio en el cual se desenvuelve y a los controles que tiene en el área de auditoría. Con la investigación que realiza en la auditoría, y con las evidencias que obtiene, puede detectar irregularidades tanto del sistema, como de los procedimientos violatorios de leyes civiles y las personas que están involucradas. Si éste fuera el caso, está obligado a comunicar de inmediato cualquier tipo de irregularidad detectada al jefe del área de sistemas y al director general; sobre todo aquellas irregularidades que de mantenerse pueden afectar seriamente

Enron Corporation, una empresa del sector energético con sede en Houston, Texas, empleaba a más de 2 000 personas antes de declararse en quiebra en el año 2001. Una serie de técnicas contables fraudulentas solapadas por su empresa auditora, Arthur Andersen, que en esos años tenía prestigio mundial, le permitió colocarse como la séptima empresa en ganancias en Estados Unidos de América, cuando en el año 2000 obtuvo ingresos por más de 100 mil millones de dólares, por lo que se esperaba que fuera la empresa dominante en su sector por muchos años; en vez de eso, se convirtió en el fraude empresarial más grande en la historia de aquel país. La empresa estaba coludida con los auditores de Arthur Andersen, quienes "maquillaban" los resultados financieros de Enron, haciendo parecer que sus ganancias eran enormes, pero lo que ocultaban eran grandes pérdidas. Enron solicitó protección por bancarrota en Europa el 30 de noviembre de 2001 y en Estados Unidos de América el 2 de diciembre del mismo año. Después de estas fechas, las acciones de Enron en la Bolsa de Valores de Nueva York, se desplomaron de 80 dólares por acción, a un dólar por acción. Auditores con reconocimiento internacional, pero sin ética, ocasionaron el desastre.

a la empresa. Además, en el caso de detectar irregularidades más graves, también deberá comunicarlo de inmediato a las autoridades civiles.

Reporte de la auditoría

Luego de finalizar la investigación que implica la auditoría y de ordenar y analizar toda la información recabada, se procede a realizar el *reporte final de la auditoría*. Antes de presentarlo para su entrega definitiva, se recomienda comentar los resultados con el jefe del área de sistemas y con el director general de la organización. Los resultados de la auditoría deben expresarse, en la medida de lo posible, en términos cuantitativos, pues esto proporciona una idea más cercana de los problemas que se identificaron. Si hay problemas graves, en general también hay culpables. Comentar los resultados antes de la entrega final le permite al auditor observar si las personas consultadas están de acuerdo con el informe final, no con el objeto de modificarlo a su conveniencia, sino para que puedan recomendar la verificación de ciertos resultados en caso de que no estén de acuerdo con algunos puntos, ya sea por otros métodos de análisis o incluso por una tercera parte externa y ajena al problema detectado. Si fuera así, las evidencias obtenidas con el nuevo auditor ajeno al problema se incorporan al reporte final original como un *addendum*, es decir, como un reporte válido pero que ha sido añadido al original.

Si la auditoría contiene observaciones "normales", en el sentido de que las fallas detectadas o errores humanos cometidos en realidad nunca pusieron en riesgo a la empresa, entonces no habrá conflicto en la entrega y recepción del reporte final de la auditoría, pues ésta sólo contendrá recomendaciones menores para mejorar la seguridad informática. En general, los auditores conservan los resultados de una auditoría durante varios años, en especial si es el mismo despacho de auditores el que ha auditado a esa empresa por varios años.

7.4 La auditoría en la práctica

En el capítulo 6, Las contingencias en seguridad informática e informática forense, se aborda el tema del plan de contingencia, el cual, como se explica

en dicho capítulo, es parte de una política de seguridad informática que está formada por controles de los riesgos y por procedimientos. Cuando se diseñan los controles, éstos no sólo deben ser completos, simples en la medida de lo posible y adecuados a los riesgos que pretenden controlar. La mayoría de estos controles son automáticos, aunque algunos todavía son una combinación de controles manuales y automáticos, lo que implica una combinación de software y de procedimientos.

El auditor externo o interno revisa que cada uno de los diferentes controles implantados siempre funcionen como se espera que funcionen y, sobre todo, que cumplan con las normas internas y externas, de acuerdo con el nivel de riesgo detectado y conforme a los objetivos de seguridad dictados por la dirección general y el director de sistemas o área de informática de la organización.

Por su parte, la dirección o jefatura de sistemas es la encargada de definir, de común acuerdo con la dirección general, las políticas para los sistemas de información basados en las exigencias de la organización, así como las normas de funcionamiento del área de sistemas, por lo que tiene la obligación de publicar y hacer llegar los procedimientos, estándares, metodología y normas aplicables a todas las áreas de informática, no sólo a los usuarios internos sino también a los externos.

Por su parte, el control interno informático define la periodicidad de las revisiones a las que deben sujetarse todos los controles implantados. Si la periodicidad es muy corta para algunos controles, suele utilizarse la auditoría interna, en tanto que para una revisión y evaluación general del estado y funcionamiento de los controles de seguridad se requiere de una auditoría externa. Las normas implantadas definen de manera muy clara todos los estándares que deben cumplirse; entre éstos, el de la periodicidad de las auditorías.

Los objetivos del control de la seguridad deben ser lo suficientemente claros, de manera que a partir de éstos resulte relativamente sencillo elaborar procedimientos eficaces, ya que llevando a cabo los procedimientos prescritos se logran los objetivos de control; por esta razón, constituye una exigencia que los objetivos estén documentados, aprobados y apoyados por la dirección general y la dirección de sistemas.

Un gran número de empresas sólo realizan análisis de vulnerabilidades en periodos previos a las auditorías. Sin embargo, se sabe de la cantidad de nuevos virus y amenazas informáticas que aparecen casi a diario, de manera que si sólo se programa una auditoría al año, sería un gran error realizar este análisis exclusivamente antes de la auditoría. No hay una frecuencia idónea para hacer este análisis, pero se recomienda que sea "tan frecuentemente como sea posible", sin que sea muy costoso, en términos de tiempo y dinero para la empresa.

Por otro lado, está la tecnología disponible en el mercado, que incluye hardware y software, la cual se concibe como la herramienta que ayuda a controlar los riesgos informáticos y que se utiliza con base en los procedimientos de control, con el fin de poder alcanzar los objetivos. Como se puede observar, objetivos, procedimientos, tecnología y normas están estrechamente relacionados, así que si alguno de estos aspectos falta o se omite, los demás no tienen mucho sentido, aunque trabajen en forma coordinada. El trabajo de un auditor es, precisamente, verificar que estos cuatro elementos estén bien definidos dentro del plan de contingencias y las políticas de seguridad, y que todos ellos interactúen en forma adecuada.

En el capítulo 6, Las contingencias en seguridad informática e informática forense, se define el contenido del plan de contingencia con sus tres subplanes y se presentan unas tablas que muestran un análisis de riesgo dentro de una empresa, las cuales no sólo contienen el tipo de riesgos físicos y lógicos a los que puede estar expuesta una organización, sino también muestran la magnitud del daño que puede ocasionar cada riesgo o exposición al riesgo que tiene la empresa, así como la frecuencia con la que han sucedido ciertos riesgos.

En términos exclusivos de la auditoría en seguridad informática, el auditor debe tomar como base las tablas del capítulo 6 y verificar que en cada uno de los riesgos detectados los controles se estén llevando de manera correcta con base en el conocimiento que tiene de las políticas y normas vigentes en la empresa acerca de seguridad. Luego, deberá verificar que los procedimientos se estén realizando conforme a lo previsto. Hay que recordar que todas las normas, políticas y procedimientos han sido entregados por escrito a todo el personal y al auditor, quien debe tener en cuenta los principios de la seguridad informática al momento de hacer la auditoría y revisar y verificar si ha habido apego a las políticas internas.

Los principios de la política en seguridad informática son:

- **Responsabilidad individual.** Significa que cada persona es responsable de sus actos, pues sus acciones son observadas, guardadas y analizadas.
- **Derechos de acceso.** Es la forma en que cada miembro de la organización puede acceder al uso de los recursos informáticos de la empresa y a determinada información.
- **Privilegio mínimo.** Significa que la política debe establecer que sólo los trabajadores del área de informática tengan acceso a los recursos mínimos para desempeñar de manera satisfactoria su trabajo. El uso de otros recursos no autorizados a un trabajador significa una violación a la política interna, por lo que es necesario llevar un registro de actividades y, cada vez que se utilice una computadora, se requiere de una clave personal para ejercer este control.
- **Separación de funciones.** Se refiere a que cada persona tiene obligaciones y responsabilidades, y éstas nunca deben mezclarse con las de otras personas, a fin de que si alguien comete un fraude, no parezca que fue otra persona quien lo cometió.
- **Redundancia.** Significa que debe haber múltiples copias de toda la información, en especial de aquella que es más relevante, pero bien resguardadas y en diferentes sitios geográficos.
- **Reducción y control del riesgo lógico.** Un principio básico de la seguridad informática es reducir y controlar el riesgo lógico de manera aceptable y a un costo admisible.
- **Realización periódica de auditorías internas y externas.** El último principio de la seguridad informática es realizar en forma periódica auditorías internas y externas, a fin de monitorear y controlar el desempeño de la seguridad.

Actividad de aprendizaje

En equipo elaboren un díptico en el que presenten de forma creativa los principios de la política en seguridad informática. Expongan su trabajo frente al grupo.

Por otro lado, los controles para la seguridad informática consisten de software para detectar vulnerabilidades; sin embargo, dichos controles en realidad no protegen por completo de los ataques, sino que detectan una posible intrusión, y si la intrusión se puede detectar, entonces sí es posible prevenir el ataque, pues los escaneos de seguridad permiten tener una idea del nivel de seguridad que tienen los sistemas, por lo que es aconsejable su uso. Pero, si ni siquiera se tiene la idea de la vulnerabilidad de un sistema, es más difícil protegerlo de ataques e intrusiones.

El trabajo del auditor parece hasta cierto punto sencillo, pero requiere una enorme capacitación en su campo, pues si la empresa auditada maneja información muy especializada, entonces con seguridad habrá adoptado algún modelo de acceso a la información o de seguridad. Por ejemplo, si la empresa tiene un departamento de investigación y desarrollo muy activo, el resultado de esas investigaciones puede valer millones de dólares, como es el caso de las investigaciones de los laboratorios que han desarrollado nuevos medicamentos contra el SIDA y algunos tipos de cáncer o de las instituciones bancarias que tienen cuentas de personas o empresas que manejan muchísimo dinero, a las cuales sólo tienen acceso unas cuantas personas. En esos casos, las empresas, suelen adoptar modelos de seguridad especiales. Aquí se hace una descripción somera de tres de esos modelos

Después de hacer las pruebas sobre el funcionamiento correcto de los controles, el auditor entrega un reporte en los siguientes términos, recordando que los riesgos anotados en todas las tablas no son exhaustivos y sólo son para ejemplificar el procedimiento.

Tabla 7.1 Reporte de funcionamiento de controles de riesgos físicos internos

Riesgo físico interno	Método de análisis	Observaciones
Fallas en la conexión de una red		
Fallas en el funcionamiento de un equipo		
Interrupción del servicio de energía eléctrica		
Suficiente capacidad de memoria del sistema		
Renuncia intempestiva de personal		
Ingeniería social interna o externa		
Seguridad de acceso al área de informática		
Seguridad de acceso a cierta información		
Protección contra fuego		
Exposición a un calor intenso		
Cercanía a recipientes de alta presión		

Con el uso de la tabla 7.1, el auditor debe reportar los métodos que empleó para evaluar la eficiencia del control de los riesgos físicos internos a los que está expuesta la empresa y las observaciones que sean necesarias. Además, está obligado a mencionar cuál método utilizó para realizar la verificación.

Modelo de Bell-Lapadula

Creado por William Elliot Bell y Len Lapadula para el ejército de Estados Unidos de América, el modelo divide el permiso de acceso de los usuarios de la información con base en etiquetas de seguridad que tienen cuatro categorías: no clasificado, confidencial, secreto y top secret (ultra secreto). Como se observa, el modelo hace énfasis en la confidencialidad más que en la integridad, definiendo los estados *seguro* e *inseguro*. Si un estado es *seguro*, la única forma de que una persona tenga acceso a cierta información es si la forma de acceso está en concordancia con la política de seguridad, lo cual se comprueba comparando los papeles de acreditación que tiene la persona que solicita acceso con la clasificación que tiene la información; por ejemplo, si una persona solicita acceso a información top secret está obligada a presentar documentos o claves de acceso que lo acrediten como persona autorizada para consultar ese tipo de información. El modelo define dos reglas: control de acceso requeridas por ley (MAC, por sus siglas en inglés; Mandatory Access Control) y una regla de control de acceso discrecional (DAC, por sus siglas en inglés; Discretionary Access Control), cada una con tres propiedades:

1. **Propiedad de seguridad simple**. Se refiere a que una persona de determinado nivel de seguridad no puede tener acceso a consultar información de un nivel superior al suyo.
2. **Propiedad de restricción**. Se refiere a que una persona de determinado nivel de seguridad está restringida para escribir un documento que pertenece a un nivel de seguridad más bajo.
3. **Propiedad discrecional**. Se refiere a que una persona puede crear contenido sólo en su nivel de acceso o superior, pero para consultar información, sólo puede hacerlo para su nivel o un nivel inferior.

Modelo de Brewer-Nash

Desarrollado en 1989 por David Brewer y Michael Nash, también conocido como modelo de la Muralla china. El enfoque de este modelo fue concebi-

do para proponer controles que minimicen los conflictos de intereses en organizaciones comerciales, construido sobre un modelo de flujo de información. Se le llama modelo de la Muralla china porque crea una barrera lógica entre el usuario y la información a la cual no tiene acceso, y aunque dos usuarios tengan el mismo nivel de acceso, no necesariamente podrán consultar la misma información. El modelo hace énfasis en la confidencialidad, porque los datos que se manejan no pueden leerse por solicitantes distintos a los interesados, pero si esto llegara a ocurrir, el modelo garantiza que la información obtenida por los solicitantes no pueda ser difundida en otros medios de comunicación.

Este modelo es muy utilizado entre consultores comerciales, quienes tienen acceso a datos confidenciales de las empresas a las cuales asesoran; sin embargo, no podrían utilizar estos datos para beneficio de otra empresa, (lo cual crearía un conflicto de intereses) aplicando de manera adecuada la política de este modelo, con lo que se garantiza la confidencialidad de los datos.

En general, existe una clasificación jerárquica de datos del negocio en todos los modelos de seguridad reconocidos, en la que suelen considerarse tres niveles:

- **Nivel inferior.** Formada por partes individuales de información, cada una de las cuales sólo pertenece a una empresa. A este tipo de información se le considera como un *objeto*.
- **Nivel intermedio.** Todos los objetos pertenecientes a la misma empresa se agrupan y se les denomina *datos de la empresa*.
- **Nivel superior.** Todos los datos de las empresas que están en competencia se agrupan en las llamadas *clases de conflictos de interés.*

La política de seguridad se establece con base en los *objetos* relacionados con el conjunto de *datos de la empresa* y el nombre de la *clase de conflicto de interés* al cual pertenece. Luego, se establecen las reglas de acceso a la información, las cuales se explican a continuación.

- Cuando una persona haya accedido a un objeto en particular, sólo podrá accesar a otros objetos que se encuentren dentro del mismo conjunto de datos de la empresa o que se hallen en un conflicto de intereses diferente.
- Una persona sólo puede tener acceso a un conjunto de datos de empresas por cada clase de conflicto de intereses.

Actividad de aprendizaje

En equipo de dos o tres personas investiguen en diferentes fuentes de información acerca del modelo Brewer-Nash. Preparen una presentación electrónica donde expongan su investigación frente al grupo.

Modelo HRU

Llamado así en honor de sus creadores, de quienes se toma la primera inicial de su nombre, Harrison, Ruzzo y Ullman. Es un modelo de seguridad en una computadora, a nivel del sistema operativo, enfocado a la integridad de los derechos de acceso en el sistema. Se considera una extensión del modelo Graham-Denning, que se basa en la idea de un conjunto finito de procedimientos que están disponibles para editar los derechos de acceso de una persona sobre un objeto; en general el objeto es determinada información. Es uno de los pocos modelos que se basa en un algoritmo para determinar derechos de acceso a la información.

El modelo define un sistema de protección que consta de un conjunto de derechos genéricos y de un conjunto de comandos u órdenes, los cuales se forman con operaciones básicas y tienen una lista de precondiciones que requieren ciertos derechos que se presentan por pares *persona-objeto*. Los requisitos originales pueden modificar la matriz de acceso agregando o suprimiendo derechos de acceso para cada par *persona-objeto*. La creación de nuevos pares *persona-objeto* requiere que ambos no tengan un registro previo en la configuración que está activa, en tanto que para suprimir un derecho, se necesita que la persona y el objeto tengan un registro previo en la configuración activa.

En este modelo se discute si el algoritmo toma una configuración inicial arbitraria y contesta a la siguiente pregunta: ¿Existe una secuencia arbitraria de comandos que agrega un derecho genérico a una celda de la matriz de acceso que no existía en la configuración inicial? La respuesta es NO, de manera que el problema general es que el algoritmo no toma decisiones propias, pero basta una operación básica para que el modelo empiece a tomar decisiones; desde luego, la operación básica debe ser agregada por una persona.

Tabla 7.2 Reporte de control de riesgos físicos externos

Riesgo físico externo	Método empleado	Observaciones
Instalación protegida contra terremotos		
Protección contra inundaciones		

Para la tabla 7.2, el único método para la evaluación es la observación, tanto de las condiciones internas del edificio donde se aloja la empresa, como de las condiciones externas donde se ubica el edificio.

Tabla 7.3 Reporte de control de riesgos lógicos

Riesgo lógico	Método de análisis	Observaciones
Ingeniería social		
Suplantación de la dirección IP		
Ataques con analizadores de red		
Ataques a servidores de la web		
Inyección SQL		
Correo spam		
Ataque de secuencia de comandos		
Ataques con analizador de puertos		
Secuestros informáticos		
Virus informáticos		
Spyware		
Spoofing		
Negación del servicio		
Rootkit		
Botnet		
Phishing		

Para reportar la tabla 7.3, en el mercado existe una enorme variedad de dispositivos y software para probar la efectividad de las medidas y los controles que se han implantado para prevenir que sucedan los riesgos lógicos. No obstante, por más medidas que se tomen para prevenir este tipo de riesgos, es casi imposible estar exento de estas vulnerabilidades, mientras existan personajes como los llamados *gurús*, que *on line* dan cursos de cómo hackear sistemas, los *copy-hackers*, o *piratas informáticos*, que roban información de computadoras personales o de empresas y la comercializan para su beneficio, como música o libros antes de que éstos salgan al mercado, los *samurái*, quienes son hackers profesionales que trabajan por dinero, robando información por encargo, o los *creadores de virus,* quienes se ufanan de haber desarrollado virus famosos que han causado mucho daño y que ha sido difíciles de eliminar durante mucho tiempo.

Actividad de aprendizaje

Elabora un mapa mental donde expliques el modelo HRU.

El problema de la seguridad y de los controles se remonta a muchos años atrás. En 1989 se desarrolló el COPS (Computer Oracle and Password System), que fue el primer escáner de vulnerabilidad para el sistema operativo Unix, que tuvo un uso muy amplio. Aún hoy día, algunas computadoras lo pueden reconocer, pero ya se han desarrollado escáneres mucho más específicos y de uso en tecnologías distintas a Unix. Un escáner de vulnerabilidad es un software diseñado para evaluar debilidades en computadoras, sistemas de cómputo, redes y aplicaciones. El problema, como siempre, es que puede ser usado tanto por los administradores de redes como por los atacantes. El COPS escanea al menos 12 vulnerabilidades, cada una auditando una parte del sistema operativo.

A este escáner le siguió la Herramienta Administradora de la Seguridad para el Análisis de Redes (SATAN, por sus siglas en inglés; Security Administrator Tool for Analyzing Netwoks), lanzado al mercado en 1995, que es un escáner que analiza la vulnerabilidad de computadoras que están en red; sin embargo, tiempo después su nombre fue cambiado a SANTA (Security Analysis Network Tool for Administrators). La ventaja de este software es que es libre, describe los servicios mal configurados y verifica las vulnerabilidades en algunos servicios. SANTA también dejó de tener vigencia a partir del año 2000, por lo que a la fecha ya es muy poco utilizado.

Hay otra herramienta, conocida con el nombre de Herramienta de Redes Integradas para Administradores de Seguridad (SAINT, por sus siglas en inglés; Security Administrator's Integrated Network Tool), que se basa en SATAN, y que puede escanear objetos protegidos por Firewall, además de que actualiza vulnerabilidades y riesgos que son reportados por el CERT (Computer Emergency Response Team). Asimismo, también emite alertas en la pantalla para cuatro niveles de daños de las vulnerabilidades. De este modo, si emite un color rojo, indica que el problema es crítico; si es amarillo, se trata de un problema al que hay que poner mucha atención; si es café se trata de problemas potenciales y si es verde la vulnerabilidad está en los servicios. Sólo se encuentra disponible para Linux.

Sin embargo, hay otras herramientas que aunque fueron creadas hace tiempo, se han actualizado y aún siguen vigentes. Tal es el caso de Nmap,

Actividad de aprendizaje

En equipo de dos o tres personas investiguen en diferentes fuentes de información acerca de la Herramienta de Redes Integradas para Administradores de Seguridad, así como sus ventajas y desventajas. Elaboren un ensayo y no olviden anotar la bibliografía consultada.

lanzado al mercado en 1997, que también es un escáner de seguridad utilizado para descubrir irregularidades en el sistema operativo, hosts y servicios en una red de cómputo, con lo cual crea un mapa de la red, lo que consigue al enviar paquetes especiales a hosts específicos y luego al analizar la respuesta. Nmap tiene la ventaja de que puede hacer el escaneo a pesar de que en la red haya condiciones especiales, como latencia y congestión; es compatible con varias plataformas.

Se llama *latencia* al tiempo que le toma a un paquete (de información) ir del origen a su destino, o bien al tiempo de ida y vuelta origen-destino-origen. Hay software, como Ping, que realizan estas mediciones.

Uno de los escáneres más utilizados es Nessus, que puede detectar las vulnerabilidades que permiten a un hacker remoto controlar o accesar a datos del sistema, además de que también detecta fallas en la configuración, fallas en los password, ataques de diccionario, negación de servicio contra los TCP/IP que se han utilizado con más frecuencia e, incluso, puede preparar al sistema para auditorías sobre la seguridad del uso de las tarjetas de crédito más utilizadas, debido a la enorme cantidad de fraudes que se han presentado con ese tipo de tarjetas.

En criptoanálisis, un ataque de diccionario constituye una técnica para descifrar archivos encriptados o mecanismos de autenticación, mediante la determinación de su clave, lo que hace revisando millones de posibilidades. Recibe este nombre porque es similar a consultar una palabra en un diccionario.

Existen otros programas llamados escáner para la seguridad de una aplicación web, que entabla comunicación con una aplicación de la web a través de un front-end, con el propósito de detectar vulnerabilidades potenciales de seguridad en una aplicación web o alguna debilidad en la arquitectura, mediante la realización de pruebas de caja negra. En general, este tipo de escáneres no tienen acceso al código fuente, de manera que cuando detectan vulnerabilidades lo hacen por medio de un ataque. Un escáner de este tipo es Nikto Web Scanner, que es un escáner del servidor de la web, que realiza pruebas sobre servidores de la web para detectar unos 6 700 archivos potencialmente malignos CGI (Common Gateway Interface), que es una tecnología que utilizan los servidores de la web. Este escáner puede detectar algún software desactualizado del servidor mediante la realización de chequeos de tipos específicos de

El concepto de caja negra consiste en un dispositivo, un sistema o un objeto del que sólo se puede observar lo que entra y lo que sale (o características que transfiere), sin saber cómo funciona por dentro.

SNMP, Protocolo Simple de Administración de Red, es un protocolo de capa de aplicación (modelo OSI), que facilita el intercambio de información de la administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver los problemas de la red y planear su crecimiento.

un servidor; además, captura e imprime cualquier cookie que se haya recibido. También puede revisar elementos de la configuración del servidor, como la presencia de archivos múltiple index y opciones del servidor HTTP. Su ventaja es que es software libre.

De acuerdo con los fabricantes, existen dos herramientas que suelen utilizarse en las auditorías. La primera es GFI LANguard Network Security Scanner, que específicamente ayuda a la detección de vulnerabilidades en una red de cómputo. La otra herramienta es Retina Network Security Scanner, que es capaz de descubrir vulnerabilidades potenciales y conocidas. Además, también permite realizar análisis de riesgos con base en la seguridad, lo cual puede ser muy útil para una empresa al momento de determinar las políticas y normas de seguridad; desde luego, es muy útil en una auditoría.

En el mercado hay disponible un escáner de amplio espectro que logra detectar vulnerabilidades y sistemas operativos remotos; además, muestra el estatus de puertos estándar y la información del SNMP; asimismo, también detecta vulnerabilidad en la Interfaz de Entrada Común (CGI, por sus siglas en inglés; Common Gateway Interface), que es una tecnología muy importante para la WWW (World Wide Web), y en Llamadas de Procedimiento Remoto (RPC, por sus siglas en inglés; Remote Procedure Call), que es una técnica para la comunicación entre procesos en una o más computadoras conectadas en red, vulnerabilidades en la Capa de Conexión Segura (SSL, por sus siglas en inglés; Secure Sockets Layer), que son protocolos criptográficos que proporcionan comunicaciones seguras a través de una red, como Internet, en servidores que tengan SQL (Structured Query Language), FTP (File Transfer Protocol), SMTP (Flight Message Transfer Protocol) y POP3 (Post Office Protocol), y algunas otras actividades de detección de vulnerabilidades.

En este punto resulta necesario mencionar que existen Centros de Operaciones de Seguridad (COS) que constituyen una central de seguridad informática, para prevenir, monitorear y controlar la seguridad en redes e Internet. Puede realizar desde un diagnóstico de vulnerabilidades, respuesta a incidentes, neutralización de ataques, planes y programas de prevención, administración de riesgos, alertas de virus informáticos, hasta prestar servicios de recuperación de desastres. El COS cuenta con firewalls, sistemas de detección

de intrusos, software antivirus actualizado casi a diario y todo lo necesario para vigilar la actividad de Internet en tiempo real las 24 horas, de los 365 días del año. En COS, todas las anormalidades detectadas en Internet son analizadas y rastreadas por expertos certificados en estándares de seguridad. La mayoría de los COS están ubicados en las áreas del mundo con mayor desarrollo informático.

En la actualidad, se han identificado unas 200 herramientas informáticas disponibles en el mercado que logran detectar vulnerabilidades en redes de cómputo. El auditor, de acuerdo con su experiencia y la tecnología de la red disponible y utilizada en la empresa auditada, es el responsable de decidir cuáles herramientas utilizará para la detección de vulnerabilidades. Con esta base, y después de realizar entrevistas, revisar registros de control y analizar toda la información recabada, el auditor puede emitir su dictamen.

El director de seguridad de la información de una organización o empresa que aún no ha adoptado las mejores prácticas en seguridad, ni posee una cultura para la seguridad, debe iniciar una estrategia para la seguridad de la información, mediante el desarrollo de un programa y la creación de una cultura de la seguridad. El enfoque que adopte será determinante en el éxito de esas iniciativas. Cualquiera que sea el enfoque adoptado, implica necesariamente cambiar algunos procesos, alguna tecnología y la cultura de los empleados hacia el aspecto de la seguridad informática. Estos cambios se deben administrar en forma adecuada.

La administración de estos cambios implica hacer uso de un conjunto de procesos que aseguren que todos aquellos cambios que se quieren implementar se hagan de manera controlada y sistemática; además, éstos deben fomentar que los empleados, en general, empiecen a trabajar con una nueva cultura de las mejores prácticas en la seguridad de la información y se pueda vencer la resistencia al cambio.

Una vez iniciado el cambio y la implementación, habrá que realizar algunas actividades tan pronto como sea posible. La primera se refiere al gobierno de la seguridad de la información, que implica establecer y mantener los procesos adecuados y una estructura de la seguridad de la información que garantice, entre otras cosas, que la estrategia está alineada a la misión, la visión

y los objetivos de la organización, que el riesgo se maneja en forma apropiada y que los recursos materiales y humanos se utilizan de manera responsable.

La segunda actividad inmediata es asegurarse de que el riesgo se está administrando a los niveles que le van a permitir a la empresa alcanzar sus objetivos y que se está cumpliendo con las políticas de seguridad acordadas.

La tercera actividad consiste en asegurarse de que la administración y el desarrollo del programa de seguridad son acordes con la estrategia de seguridad que se ha planeado.

Por último, la cuarta actividad consiste en planear, establecer y administrar de manera adecuada la capacidad de detectar, investigar, responder y recuperarse con rapidez de cualquier incidente sobre la seguridad de la información, minimizando el impacto causado sobre el negocio.

En un principio, el cambio parecerá confuso en resultados y difícil de completar, pero gran parte del éxito de este tipo de cambios depende más de la habilidad de quien está al frente, que de los conocimientos técnicos que pueda tener. Hay que recordar que se está tratando de cambiar la cultura de una empresa; es decir, se está intentando cambiar la actitud y la forma de pensar de los trabajadores hacia el aspecto de la seguridad de la información. Hoy día, hay muchas recetas y consejos para hacerlo, pero al final es el liderazgo de promotor quien logra el éxito.

De acuerdo con Kotter[1], se sugieren ocho pasos para lograr este cambio en forma adecuada. No se recomienda omitir ningún cambio, ni modificar la secuencia de los pasos, pues podría conducir a problemas en la consecución del éxito.

1. **Hacer sentir a los empleados que el cambio es urgente.** Hay que sensibilizar desde la alta gerencia hasta cada una de las áreas de la empresa, explicando los beneficios que tiene la seguridad en la información con los requerimientos de la industria, las tendencias del mercado, la competencia y la necesidad de acatar todas las leyes y los reglamentos sobre

[1] Kotter, John P. (1995). "Leading Change: Why Transformation Efforts Fail", en *Harvard Business Review*.

seguridad de la información. Es muy conveniente motivar a la alta gerencia para que sea ésta la que promueva más este cambio de cultura hacia los empleados, lo cual se puede hacer por medio de conferencias, pláticas y dando información escrita sobre incidentes sucedidos en seguridad en grandes empresas, y las consecuencias negativas que esto ha acarreado, así como también mostrar los beneficios que han obtenido grandes organizaciones cuando han hecho las cosas de manera correcta.

2. **Hay que formar un grupo de gran influencia.** En toda organización existen líderes carismáticos en cada área. Si el líder del proyecto del cambio de cultura logra convencer a esos líderes, ellos a su vez convencerán con más facilidad a los demás trabajadores, pues el líder carismático es a quien todos escuchan y siguen. Hay que identificar a éstos líderes y convencerlos de los beneficios del cambio de cultura.

3. **Crear una estrategia y una visión de la seguridad de la información.** La guía hacia el éxito del cambio recae en gran parte en que se tenga la visión y la estrategia de seguridad. La visión, desde el punto de vista estratégico, es la forma y condiciones en que el líder visualiza cómo estará la empresa en no más de dos años, de manera que conforme pase el tiempo trabajando en el cambio de cultura organizacional, será necesario ir actualizando la visión de cambio, pues con el tiempo irán cambiando las condiciones de la cultura de la organización.

4. **Comunicar a otras áreas la estrategia y visión de la seguridad de la información.** Estos dos puntos no deben sólo quedar en el área de informática o de sistemas, sino que deben permear a todas las áreas de la organización. Kotter recomienda que en cualquier tipo de junta que se realice en la empresa y que haya presentación electrónica, lo primero que aparezca al inicio de la reunión sea una diapositiva recordando el cambio de cultura de la organización respecto a la seguridad informática.

5. **Involucrar a todos los trabajadores en la visión de la seguridad.** Sin importar el nivel jerárquico de los empleados, se debe permitir que todos participen y tengan un papel activo dentro de la estrategia de seguridad.

Hay que identificar y eliminar cualquier obstáculo que impida el éxito. Es conveniente revisar periódicamente políticas internas, dar capacitación continua y realizar las reestructuraciones administrativas cuando sea necesario.

6. **Hay que hacer público cualquier logro que se obtenga en la visión.** Si todo está bien planeado, poco a poco se irán consiguiendo puntos importantes de la visión de la seguridad. Hay que publicar en toda la empresa aquellos logros que más repercutan en beneficio de la empresa y, sobre todo, aquellos que han requerido menor presupuesto. Esto mostrará a la alta gerencia que ha tomado una buena decisión apoyando el cambio de cultura hacia la seguridad informática, y con seguridad la seguirá apoyando.
7. **No alardear demasiado los logros.** Hay que hacer púbicos los logros, pero si se alardea demasiado se corre el riesgo de crear poca motivación para continuar, pensando que todo es muy fácil. Lo que se recomienda es lo que se llama "institucionalizar los cambios". Esto implica la creación de la cultura, es decir, que en vez de desmotivar a los empleados por los logros obtenidos, hay que dirigir esa euforia a que la empresa realmente se acostumbre a la nueva forma de tratar con la seguridad informática, de modo que sea la nueva manera de comportarse hacia todos los aspectos de la seguridad.
8. **Institucionalizar los cambios.** Independientemente de la cantidad y el tipo de logros que vayan sucediendo, lo importante es asegurar un cambio permanente de ética, valores y cultura hacia la seguridad de la información, asegurando que los empleados ya no regresarán hacia las antiguas prácticas sobre este aspecto tan importante en cualquier organización.

Actividad de aprendizaje

En equipo elaboren un póster donde presenten de forma creativa los ocho pasos para cambiar la cultura empresarial hacia la seguridad informática que Kotter recomienda. Expongan su trabajo frente al grupo.

Comprueba tus saberes

1. Define con tus propias palabras el concepto de auditoría.

2. Menciona, al menos, cuatro tipos de auditoría que existen en el área de informática o de sistemas.

3. Menciona al menos cinco funciones del control interno informático.

4. Describe en forma personal las cuatro etapas de que consta una auditoría.

5. Describe con tus propias palabras los tipos de opinión que puede emitir un auditor al terminar de realizar una auditoría.

6. Describe al menos dos modelos de seguridad para el acceso a la información.

7. ¿En qué consisten los beneficios que obtiene una empresa al ser auditada?

8. Explica los nueve requisitos que pide ISACA para otorgar un certificado de auditor.

9. ¿Cuáles son los criterios que se deben emplear en una auditoría?

10. ¿En qué consiste el criterio de medición cuantitativa?

11. Describe con detalle cómo se realiza una auditoría.

12. ¿Qué es una *addendum* en una auditoría y cuándo se utiliza?

13. Explica al menos cuatro productos informáticos disponibles en el mercado que se utilizan con frecuencia para realizar auditorías de seguridad informática.

14. De los ocho pasos sugeridos por Kotter para cambiar la cultura empresarial hacia la seguridad informática, ¿cuál o cuáles te parecen más importantes y por qué?

Referencias bibliográficas

1. Gómez, A. (2011). *Enciclopedia de la Seguridad Informática*. Segunda edición. México. Editorial Alfaomega.
2. Portantier, F. (2012). *Seguridad Informática.* Buenos Aires. Fox Andina; Dalaga.

Referencias electrónicas

1. https://www.isaca.org/cism
2. http://www.monografias.com/trabajos12/cofas/cofas.shtml#ixzz3pne2Bjp5
3. https://en.wikipedia.org/wiki/COPS_(software)
4. https://en.wikipedia.org/wiki/Nmap
5. https://en.wikipedia.org/wiki/Nessus_(software)
6. https://en.wikipedia.org/wiki/Dictionary_attack
7. https://en.wikipedia.org/wiki/Web_application_security_escáner
8. https://en.wikipedia.org/wiki/Nikto_Web_Scanner
9. https://en.wikipedia.org/wiki/Security_Administrator_Tool_for_Analyzing_Networks
10. http://www.vulnerabilityassessment.co.uk/xscan.htm
11. https://en.wikipedia.org/wiki/HRU_(security)
12. https://es.wikipedia.org/wiki/Modelo_Brewer-Nash
13. https://es.wikipedia.org/wiki/Modelo_Bell-LaPadula

Apéndice

El ciclo de vida de los proyectos informáticos

Introducción

En general, un proyecto se define como un plan de acción que al asignarle cierto monto de capital y aplicarle insumos de varios tipos, generará un bien o un servicio que va a satisfacer una necesidad del ser humano o de una organización en particular. Para que se desarrolle un proyecto de cualquier tipo, primero es necesario detectar la necesidad que va a dar origen al proyecto, después definir el producto o servicio específico que se producirá y, finalmente, satisfacer de la manera óptima la necesidad detectada.

En los proyectos informáticos, el concepto se aplica en los mismos términos. En un mundo donde cada vez es más necesario el uso de las computadoras en todas las actividades de las personas y el uso de las redes de computadoras para las empresas, las necesidades que se tienen de las Tecnologías de la Información y la Comunicación (TIC) no sólo son crecientes, sino cada vez más diversas. De esta forma, en el ambiente de las TIC, y básicamente en las organizaciones, se pueden generar tantos proyectos informáticos como necesidades sean detectadas. Así, es posible encontrar proyectos de inversión en TIC que comprenden la instalación de redes, de centros de cómputo, de respaldo de datos, entre muchos otros proyectos; sin embargo, el tipo más recurrente de proyectos informáticos es el desarrollo de software en las organizaciones.

Hoy día, existe una enorme cantidad de software comercial para realizar un número inimaginable de diferentes tareas, entre los que destacan: Office de Windows, Visio para elaborar todo tipo de dibujos, software para todos los

niveles de matemáticas y hasta software lúdico, también con una inmensa variedad disponible a nivel comercial; y un largo etcétera. A pesar de esta situación, las grandes empresas, en su lucha diaria por el mercado de sus productos o servicios, se ven forzadas a una constante innovación en la forma en que producen, distribuyen, venden o cobran sus productos o servicios. Para cada una de estas innovaciones se requiere un nuevo software que, desde luego, no se encuentra disponible en el mercado.

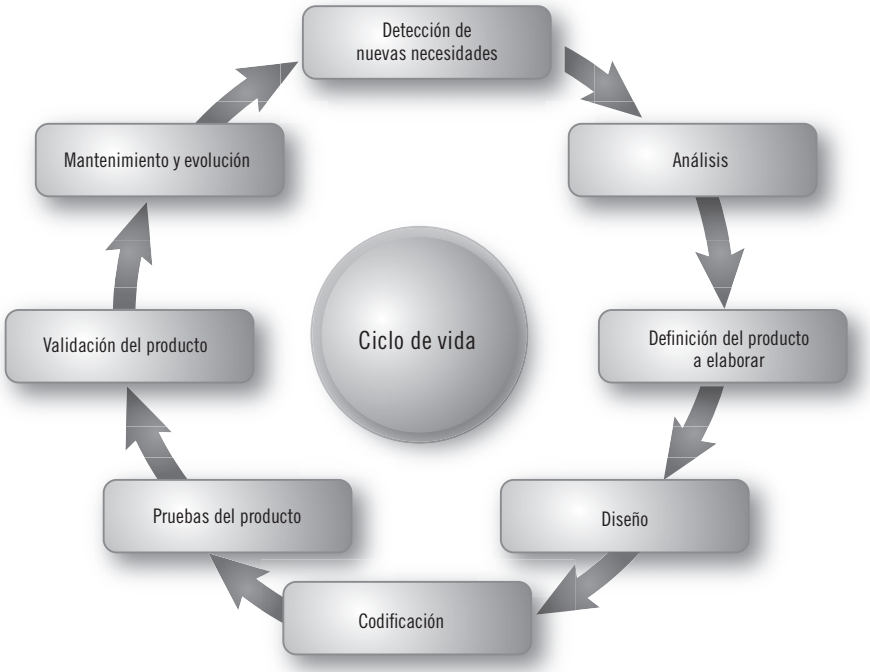
El ciclo de vida de los proyectos informáticos

Un número muy elevado de proyectos en informática se debe al desarrollo de sistemas y, por tanto, al desarrollo del software correspondiente. Es tan frecuente este tipo de proyectos, que a la fecha se ha desarrollado el concepto de "ciclo de vida de los proyectos". En este contexto, el concepto de "ciclo" se entiende como una serie de actividades o cursos de acción que tienen un inicio y un fin. En general, los sistemas de información se clasifican de acuerdo con su aplicación del sistema en: sistemas transaccionales, sistemas de soporte para la toma de decisiones y sistemas expertos. A partir de esta clasificación se puede observar que la creciente necesidad de desarrollar software para uso específico para cada organización, se debe a que las transacciones (compra-venta), toma de decisiones y sistemas expertos adquiere un matiz distinto, dependiendo del sector comercial al cual pertenece la empresa, a su tamaño y a la innovación en sus formas de trabajar en las distintas áreas de esa organización.

El ciclo de vida de un proyecto informático para el desarrollo de un sistema de información se observa en forma esquemática en la figura A.1.

Detección de nuevas necesidades

Como se mencionó al principio, un proyecto inicia con la detección de necesidades por parte de la organización. Por lo común, ello sucede cuando se realiza una innovación en alguna de las múltiples áreas de una organización productora de algún bien o generadora de un servicio y de inmediato se detecta la necesidad de desarrollar un nuevo sistema de información y el soft-



› **Figura A.1**
Ciclo de vida de un proyecto informático.

ware correspondiente. La necesidad también puede surgir cuando se identifica un problema en el flujo de información en determinada área de trabajo y es imposible resolver o superar dicho problema con el sistema que se cuenta en ese momento, ya sea que éste sea manual o computarizado.

Análisis

La siguiente etapa del ciclo consiste en analizar a profundidad la forma en que funcionaría el nuevo sistema de información, a partir de las necesidades que declara cada una de las partes que van a participar en la operación del nuevo sistema. Cada una de estas partes, que puede ser áreas o personas, es capaz de recibir, procesar, almacenar o enviar información a otra área o persona. El análisis comprende todas las operaciones (transacciones, toma de decisiones o actividades específicas) que cada área y cada persona debe realizar con el nuevo sistema de información. Luego, se elabora un diagrama donde se muestra la nueva forma en que deberá fluir la información, ya sea para resolver el problema que se tiene o para que la innovación propuesta para realizar el trabajo funcione de manera óptima.

Definición del producto a elaborar

Una vez cubiertas las dos primeras etapas del ciclo se procede a definir en forma teórica el producto (software) que se pretende elaborar. La definición del producto implica la definición formal de todas las actividades y operaciones que el nuevo sistema y el nuevo software deberán realizar.

Diseño

De la definición teórica se pasa al diseño del producto, que significa pasar de la teoría a la práctica. El diseño implica pasar de "el nuevo sistema debe hacer esto" a "la forma en que el nuevo sistema hará esto se puede lograr de esta manera".

Codificación

La siguiente parte del ciclo de vida es la codificación, programación o escritura en código de las instrucciones que tendrá el software para realizar las operaciones delineadas en la teoría.

Prueba del producto

Una vez terminada la codificación del software, el siguiente paso es la etapa de prueba, para la cual se diseñan diversas pruebas con el propósito de verificar que tanto el software como el sistema funcionen como se espera que lo hagan.

Validación

Esta etapa implica la aceptación de que las pruebas realizadas y aprobadas pueden ser puestas en práctica en el funcionamiento cotidiano de la empresa. En ésta se documenta el sistema y se entrega al cliente el sistema en funcionamiento, junto con la documentación.

Mantenimiento y evolución

El mantenimiento de un nuevo sistema informático no implica necesariamente que haya algún defecto en su funcionamiento, aunque éste sea un hecho

común y resulte indispensable ajustar la programación para eliminar ese pequeño defecto de funcionamiento, el mantenimiento también implica una evolución del sistema. Cuando el nuevo sistema ya opera en forma normal y satisfactoria, alguno de los usuarios del mismo o el jefe de sistemas piensa que el software, además de las funciones que ya tiene, también podría realizar algunas más en beneficio de la organización o con el fin de satisfacer algunas necesidades que no se habían detectado desde un principio. Si se aceptan tales propuestas de modificación y adición de nuevas funciones, entonces se procede a la realización de los cambios a la codificación, de modo que el sistema evoluciona de manera positiva para hacerse más robusto con cada nueva adición.

Inicio de un nuevo ciclo

Si los cambios propuestos para mejorar el sistema actual son demasiados y profundos, o se detectan nuevas necesidades en otras áreas de la organización, el ciclo se repite. La repetición de este ciclo para el desarrollo de nuevos productos es lo que hace que las organizaciones se mantengan en mejora continua de su desempeño en el mercado.

Cada nuevo proyecto siempre tiene determinados objetivos, cuyas características, en general, pueden ser las siguientes.

1. **Específicos.** Siempre debe quedar claro cuáles serán las características puntuales del producto a desarrollar.
2. **Medibles.** En todo momento debe ser posible cuantificar los beneficios, ya sea en términos de tiempo ahorrado, beneficios monetarios o ventajas competitivas que se tendrán con el nuevo producto.
3. **Realistas.** Siempre debe ser posible obtener el nivel de cambio reflejado en el objetivo.
4. **Limitados en tiempo.** Implica tener una programación del cumplimiento de cada una de las siete fases del proyecto. Empero, la primera no cuenta para esta programación, porque un problema se puede detectar en

cualquier momento, así como una innovación en la forma de trabajar que implique la necesidad de un nuevo sistema de información; sin embargo, no son temas que estén sujetos a ser pensados o ideados en un tiempo determinado.

Cualquier metodología de construcción de software de aplicación debería tener, al menos, los siguientes rasgos:

a) Comprender todo el proceso de desarrollo del sistema de información (a pesar de que existen metodologías restringidas a determinadas etapas: análisis, programación, etc.).

b) Favorecer una correcta gestión del proyecto informático.

c) Garantizar una comunicación fluida entre las personas que intervienen en el proyecto mediante la documentación que se genera.

d) Facilitar el proceso de pruebas y, sobre todo, el mantenimiento futuro y la evolución de la aplicación.

e) Proporcionar ayudas automatizadas durante el proceso de construcción y mantenimiento que faciliten la pesada tarea de obtener documentación; y, además, que también permitan determinar si la metodología es utilizada de manera correcta.

f) Hacer visible y controlable el progreso en la construcción del sistema de información que se quiere llevar a cabo.

g) Estar preparada para asumir mejoras en el futuro y poder adaptarse a los cambios en la tecnología informática.

h) Poder ser enseñada y transferida.

Cuando existe una necesidad, en este caso la mejora de sistemas de información, la elaboración de software se ha considerado como un proceso enorme dividido en una serie de procesos más pequeños, atendiendo a todas las necesidades y actividades que surgen durante la elaboración del producto o nuevo

software. Por último, como se ha aclarado, la elaboración de software se considera un proceso, por lo que para estandarizar ese proceso se ha desarrollado una serie de metodologías, las cuales han evolucionado. La industria de desarrollo de software ha sido durante muchos años una industria cuyos procesos se consideran muy caóticos, pero, poco a poco, se han desarrollado metodologías que han ayudado a estandarizar algún aspecto de este proceso; por ejemplo, *Rational Unified Process* (RUP®) de IBM®, *Microsoft Solution Framework* (MSF®) de Microsoft® y *Project Managemen Body of Knowledge* (PMBoK®), del PMI®.

Sin embargo, una metodología que ha conjuntado los principales aspectos de las metodologías anteriores y de otras teorías, como el enfoque de sistemas y el control total de la calidad, es CMMI (Capability Maturity Model Integrated o Modelo Integrado de Capacidad y Madurez); aunque esta metodología fue desarrollada de manera exclusiva para el desarrollo de software, sus ideas y filosofía pueden aplicarse para la mejora de procesos en cualquier tipo de industria, y de hecho así ha sido. CMMI (Capability Maturity Model Integrated) es una metodología desarrollada por el SEI (Software Engineering Institute), que a su vez es un centro de desarrollo e investigación patrocinado por el Departamento de Defensa de los EUA y por la Carnegie Mellon University. CMMI tiene un uso muy extendido a varias áreas de la industria de manufactura y de desarrollo de software, debido a que más que ser una metodología para desarrollar software, constituye una metodología para la mejora de procesos.

CMMI ha definido 22 áreas de procesos, pero estas áreas sólo son válidas para empresas que desarrollan software, de manera que el primer punto importante es que si se quieren aplicar los principios subyacentes de CMMI en otro tipo de empresas, esa empresa primero deberá definir sus propias áreas de procesos, algunas de las cuales eventualmente van a coincidir con aquellas áreas de procesos de empresas dedicadas al desarrollo de software. Las áreas de procesos que ha definido CMMI para el desarrollo de software son:

1. Análisis causal y de resolución.
2. Administración de la configuración.
3. Análisis de decisión y resolución.

4. Administración integrada de proyectos.
5. Análisis y medición.
6. Innovación y despliegue organizacional.
7. Definición de proceso organizacional.
8. Enfoque en el proceso organizacional.
9. Desempeño en el proceso organizacional.
10. Capacitación organizacional.
11. Integración de producto.
12. Control y monitoreo de proyecto.
13. Planeación de proyecto.
14. Aseguramiento de la calidad de producto y proceso.
15. Administración cuantitativa del proyecto.
16. Desarrollo de requerimientos.
17. Administración de requerimientos.
18. Administración de riesgo.
19. Administración de acuerdos con el proveedor.
20. Solución técnica.
21. Validación.
22. Verificación.

Aunque no es objeto de este apéndice profundizar en esta metodología, es posible observar que las 22 áreas de procesos que señala CMMI se pueden enmarcar en las ocho etapas mencionadas en la figura A.1, del ciclo de vida de proyectos. Sólo hay que puntualizar que cuando en cualquiera de las 22 áreas de procesos se habla de proyecto, se hace referencia al proyecto de desarrollo de software; así, al hablar de monitoreo y control se refiere al control del proyecto de desarrollo de software, para no incurrir en retrasos en la entrega

del producto; al hablar del área de administración de riesgo, se refiere al riesgo que tiene el proyecto de fracasar, por lo que hay que controlar dicho riesgo, etcétera.

Un aspecto importante del modelo de CMMI es que está conformado por una serie de partes que al ser desarrolladas van arrojando claridad a todo el proyecto, de forma que para todas las personas involucradas en el mismo, empezando por el solicitante, pueden visualizar a la perfección cómo se va a desarrollar el proyecto de la elaboración del nuevo software, lo cual infunde confianza en todos los participantes. Las partes que contiene cada una de las 22 áreas de proceso son:

a) **Declaración de propósitos.** Describe el propósito del área de proceso y es un componente informativo. Por ejemplo, la declaración del propósito del área Definición del Proceso Organizacional es "establecer y mantener un conjunto utilizable de procesos organizacionales y estándares del medio ambiente de trabajo".

b) **Notas introductorias.** Esta sección describe los principales conceptos cubiertos en el área de proceso y es un componente informativo. Un ejemplo de nota introductoria del área de proceso Planeación de Proyecto es: "La planeación empieza con los requerimientos que definen el producto y el proyecto".

c) **Áreas relacionadas de procesos**. Listan las referencias a áreas de procesos relacionadas y reflejan relaciones de alto nivel entre las áreas de proceso. Es un componente informativo. Un ejemplo en el área de proceso relacionada con Planeación de Proyecto es: "Refiérase al área de proceso de Administración del riesgo para más información acerca de la identificación y el manejo de riesgos".

d) **Metas específicas**. Describe las características únicas que deben estar presentes para satisfacer un área de procesos. Es un componente requerido del modelo y se usa en evaluación para ayudar a determinar si un área de proceso está satisfecha. Un ejemplo del área de proceso Administración

de la Configuración es: "La integridad de las líneas base se establece y mantiene". Sólo la declaración de la meta específica es un componente requerido del modelo. El título de meta específica, precedido por un número de meta, y cualquier nota asociada con la meta se consideran componentes del modelo informativo.

e) **Metas genéricas.** Se les llama "genéricas" porque la misma declaración de meta se aplica a múltiples áreas de proceso. Describe las características que deben estar presentes para institucionalizar el proceso que implementa un área de proceso. Es un componente requerido del modelo y se usa en evaluaciones para determinar si un área de proceso está satisfecha. Un ejemplo de meta genérica es: "El proceso es institucionalizado como un proceso definido". Sólo la declaración de meta genérica es un componente requerido del modelo, cualquier nota adicional es un componente informativo.

f) **Metas específicas y prácticas específicas**. Ambas proporcionan un resumen de alto nivel de las metas específicas, que son los componentes requeridos, y las prácticas específicas, que son los componentes esperados. Ambas son componentes informativos.

g) **Prácticas específicas.** Es la descripción de una actividad que se considera importante al realizar la meta específica asociada. Las prácticas específicas describen las actividades que se espera que resulten en la realización de una meta específica de un área de proceso. Es un componente esperado del modelo. Ejemplo del área de proceso Control y Monitoreo de Proceso es: "El monitoreo concuerda contra aquellos identificados en el plan de proyecto". Sólo la declaración de una práctica específica es un componente esperado del modelo.

h) **Productos típicos de trabajo.** Lista muestras de productos de una práctica específica. Esos ejemplos se llaman productos típicos de trabajo porque con frecuencia son otros productos de trabajo que son útiles pero que no aparecen en la lista. Un componente informativo del modelo es un producto típico de trabajo. Un ejemplo en la práctica específica es: "Monito-

rear los valores actuales de los parámetros de la planeación del proyecto contra el proyecto". En tanto, en el área de proceso Monitoreo y Control del Proceso un ejemplo es: "Registro de desviaciones significativas".

i) **Subprácticas.** Es una descripción detallada que proporciona una guía para interpretar e implementar una práctica específica o genérica. Las subprácticas son declaradas como prescripciones, pero son un componente informativo; es decir, sólo dan ideas que pueden ser útiles para la mejora del proceso. Un ejemplo de subpráctica para la práctica específica es: "Tómese acción correctiva sobre problemas identificados"; mientras que en el área de proceso Monitoreo y Control de Procesos un ejemplo es: "Determine y documente las acciones apropiadas necesarias para los problemas identificados".

j) **Prácticas genéricas.** Son llamadas "genéricas" porque la misma práctica se aplica a múltiples áreas de proceso. Es la descripción de una actividad que se considera importante al realizar una meta genérica asociada. Es un componente esperado del modelo. Un ejemplo de práctica genérica para meta genérica es: "El proceso está institucionalizado como un proceso administrado", la práctica es: "Proporcionar los recursos adecuados para realizar el proceso, desarrollando productos del trabajo y proporcionando los servicios del proceso". Sólo la declaración de la práctica genérica es un componente esperado del modelo, lo demás son componentes informativos del modelo.

Referencias bibliográficas

SEI. CMMI for Development V1.2, 2006.