



Fundamentos de Ciberseguridad

Guía de Estudio, 2^a edición

ISACA®

ISACA (isaca.org) ayuda a profesionales de todo el mundo a liderar, adaptar y garantizar la confianza en un mundo digital en evolución, ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo profesional innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro con 140 000 profesionales en 180 países. ISACA también ofrece Cybersecurity Nexus™ (CSX), un recurso holístico de ciberseguridad, y COBIT®, un marco de referencia de negocio para el gobierno de la tecnología de las empresas.

Descargo de responsabilidad

ISACA ha diseñado y creado la *Guía de Estudio de Fundamentos de Ciberseguridad, 2ª edición* principalmente como un recurso educativo para los profesionales de la ciberseguridad. ISACA no afirma, declara ni garantiza que el uso de esta guía de estudio asegura un resultado exitoso en cualquier examen de certificado o certificación. La guía de estudio fue creada de manera independiente al examen de Fundamentos de Ciberseguridad. No se divultan al público copias de los exámenes actuales o anteriores, y tampoco se han empleado para la preparación de esta publicación.

Reserva de derechos

© 2017 ISACA. Todos los derechos reservados. Ninguna parte de esta publicación puede ser usada, copiada, reproducida, modificada, distribuida, exhibida, almacenada en un sistema de recuperación o transmitida en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros), sin previa autorización por escrito de ISACA.

ISACA

1700 E Golf Road | Suite 400

Schaumburg, IL 60173 | USA

Teléfono: +1.847.660.5505

Fax: +1.847.253.1755

Correo electrónico: info@isaca.org

Sitio web: www.isaca.org

Envíe sus comentarios: www.isaca.org/cyber-fundamentals-study-guide

Participe en el Centro de Conocimiento de ISACA (ISACA Knowledge Center): www.isaca.org/knowledge-center

Siga a ISACA en Twitter: <https://twitter.com/ISACANews>

Únase a ISACA en LinkedIn: ISACA (Oficial), <http://linkd.in/ISACAOOfficial>

Indique que le gusta ISACA en Facebook: www.facebook.com/ISACAHQ

AGRADECIMIENTOS

El desarrollo de la *Guía de Estudio de Fundamentos de Ciberseguridad, 2^a edición* es el resultado del esfuerzo colectivo de muchos voluntarios. Participaron miembros de ISACA de todo el mundo, ofreciendo generosamente su talento y experiencia.

Agradecimiento especial a Patric J.M. Versteeg, CISA, CISM, CRISC, CGEIT, CSX-P, VSec, Paises Bajos, quien actuó como revisor principal.

Revisores expertos

Gurvinder P. Singh, CISA, CISM, CRISC, Sydney Trains, Australia

John Tannahill, CISM, CGEIT, CRISC, J. Tannahill & Associates, Canadá

Balasubramaniyan Pandian, CISSP, ISO27kLA, Triquesta, Singapore

KyoungGon Kim, CISA, CISSP, Deloitte, Corea del Sur

Derek Grocke, HAMBS, Australia

Vilius Benetis, CISA, CRISC, NRD CS, Lituania

Alberto Ramirez Ayon, CISA, CISM, CRISC, CBCP, CIAM, Seguros Monterrey New York Life, México

Matthew Morin, Cylance, Inc., EE.UU.

Consejo Directivo de ISACA

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Presidente

Theresa Grafenstine, CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, U.S. House of Representatives, EE.UU., Vicepresidenta

Robert Clyde, CISM, Clyde Consulting LLC, EE.UU., Director

Leonard Ong, CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski, CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoría de Informática Ltd., Brasil, Director

Eddie Schwartz, CISA, CISM, CISSP-ISSEP, PMP, EE.UU., Director

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., Sudáfrica, Director

Zubin Chagpar, CISA, CISM, PMP, Amazon Web Services, Reino Unido, Director

Rajaramiyer Venketaramani Raghu, CISA, CRISC, Versatelist Consulting India Pvt. Ltd., India, Director

Jeff Spivey, CRISC, CPP, Security Risk Management, Inc., EE.UU., Director

Robert E Stroud, CGEIT, CRISC, Forrester Research, EE.UU., ex Presidente

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, ex Presidente

Greg Grocholski, CISA, SABIC, Arabia Saudí, ex Presidente

Matt Loeb, CGEIT, FASAE, CAE, ISACA, EE.UU., Director

Grupo de trabajo de Ciberseguridad

Eddie Schwartz, CISA, CISM, CISSP-ISSEP, PMP, EE.UU., Presidente

Niall Casey, Johnson & Johnson, EE.UU.

Stacey Halota, CISA, CISSP y CIPP, Graham Holdings, EE.UU.

Tammy Moskites, CISM, Venafi, EE.UU.

Lisa O'Connor, Accenture, EE.UU.

Ron Ritchey, JPMorgan Chase & Co., EE.UU.

Marcus Sachs, North American Electric Reliability Corporation, EE.UU.

Greg Witte, CISM, CISSP-ISSEP, PMP, G2, Inc., EE.UU.

Rogerio Winter, Ejército Brasileño, Brasil

Reconocimiento Especial por el Apoyo Financiero

ISACA New Jersey Chapter

Página dejada en blanco intencionadamente

CONTENIDO

Sección I: Introducción y visión general de la ciberseguridad	3
Tema 1—Introducción a la ciberseguridad.....	5
Tema 2—Diferencia entre seguridad de la información y ciberseguridad	11
Tema 3—Objetivos de la ciberseguridad.....	13
Tema 4—Gobierno de la ciberseguridad.....	15
Tema 5—Dominios de la ciberseguridad	19
Sección 1—Evaluación de conocimientos	21
Sección 2: Conceptos de Ciberseguridad	23
Tema 1—Riesgo	25
Tema 2—Tipos y vectores de ataque comunes	33
Tema 3—Políticas.....	39
Tema 4—Controles de ciberseguridad	45
Sección 2—Evaluación de conocimientos	48
Sección 3: Principios de Arquitectura de Seguridad	49
Tema 1—Visión general de la arquitectura de seguridad	51
Tema 2—El modelo OSI	55
Tema 3—Defensa en profundidad.....	59
Tema 4—Control de flujo de información	61
Tema 5—Aislamiento y segmentación.....	68
Tema 6—Registro, monitorización y detección	71
Tema 7—Fundamentos, técnicas y aplicaciones de cifrado.....	75
Sección 3—Evaluación de conocimientos	83
Sección 4: Seguridad de Redes, Sistemas, Aplicaciones y Datos	85
Tema 1—Controles de proceso—Evaluaciones del riesgo.....	87
Tema 2—Controles de proceso—Gestión de la vulnerabilidad	91
Tema 3—Controles de proceso—Pruebas de penetración	93
Tema 4—Seguridad de la red	97
Tema 5—Seguridad del Sistema Operativo.....	105
Tema 6—Seguridad de las aplicaciones	111
Tema 7—Seguridad de los datos	115
Sección 4—Evaluación de conocimientos	118
Sección 5: Respuesta a Incidentes	119
Tema 1—Evento vs. incidente.....	121
Tema 2—Respuesta a incidentes de seguridad.....	125
Tema 3—Investigaciones, retenciones legales y preservación	127
Tema 4—Análisis forense	129
Tema 5—Planes de recuperación de desastres y de continuidad del negocio	133
Sección 5—Evaluación de conocimientos	137
Sección 6: Implicaciones de seguridad y adopción de la tecnología evolutiva	139
Tema 1—Panorama actual de amenazas	141
Tema 2—Amenazas persistentes avanzadas.....	143
Tema 3—Tecnología móvil—Vulnerabilidades, amenazas y riesgos	147

Tema 4—Consumerización de TI y dispositivos móviles	153
Tema 5—La nube y la colaboración digital	157
Sección 6—Evaluación de conocimientos	161
Anexo A—Declaraciones de conocimientos	165
Anexo B—Glosario.....	167
Anexo C—Respuestas de la Evaluación de conocimientos.....	191

GUÍA DE ESTUDIO DE FUNDAMENTOS DE CIBERSEGURIDAD

¿Por qué convertirse en un profesional de la ciberseguridad? La protección de la información es una función crítica para todas las empresas, industrias y sociedades modernas. La ciberseguridad es un campo cada vez más amplio y cambiante, y es crucial que los conceptos centrales que enmarcan y definen este campo sean entendidos por los profesionales que estén interesados e involucrados en las implicaciones de seguridad de las tecnologías de la información (TI). La *Guía de Estudio de Fundamentos de Ciberseguridad, 2ª edición* está diseñada con este fin, así como para también dar una idea de la importancia de la ciberseguridad, y el papel integral de los profesionales de la ciberseguridad. Esta guía abarca cinco áreas clave de la ciberseguridad: 1) conceptos y definiciones básicas de la ciberseguridad, 2) principios de arquitectura de seguridad, 3) seguridad de redes, sistemas, aplicaciones y datos , 4) respuesta a incidentes y 5) las implicaciones de seguridad derivadas de la adopción de tecnologías emergentes.

Al finalizar esta guía, el alumno será capaz de:

- Comprender las definiciones y conceptos básicos de ciberseguridad.
- Entender los principios básicos de la gestión de riesgos y la evaluación de riesgos relacionados con las amenazas de ciberseguridad.
- Aplicar los principios de arquitectura de seguridad.
- Identificar los componentes de una arquitectura de seguridad.
- Definir los conceptos de la arquitectura de seguridad de redes.
- Comprender los conceptos y la metodología de análisis de software malintencionado (malware).
- Reconocer las metodologías y técnicas para la detección de intrusiones en servidores y redes, por medio de tecnologías de detección de intrusión.
- Identificar herramientas de evaluación de vulnerabilidades, incluyendo herramientas de código abierto y sus capacidades.
- Comprender el fortalecimiento de la seguridad del sistema.
- Comprender los principios, herramientas y técnicas para pruebas de penetración.
- Definir los principios, modelos, métodos y herramientas para gestión de sistemas de redes.
- Entender la tecnología de acceso remoto y los conceptos de administración de sistemas.
- Distinguir las vulnerabilidades y amenazas de seguridad de los sistemas y aplicaciones.
- Reconocer los principios de gestión del ciclo de vida del sistema, incluyendo la seguridad y la usabilidad del software.
- Definir los tipos de incidentes (categorías, respuestas y períodos de tiempo para las respuestas).
- Describir la recuperación de desastres y la planificación de la continuidad del negocio.
- Entender las metodologías de respuesta a incidentes, y manejo de las mismas.
- Comprender las herramientas de correlación de eventos de seguridad, y cómo pueden utilizarse los diferentes tipos de archivo para verificar comportamientos atípicos.
- Reconocer las implicaciones de investigación de hardware, sistemas operativos y tecnologías de red.
- Familiarizarse con los conceptos básicos, prácticas, herramientas, tácticas, técnicas y procedimientos de procesamiento de datos forenses digitales.
- Identificar los métodos de análisis de tráfico de red.
- Reconocer las nuevas y emergentes tecnologías de la información y tecnologías de seguridad de la información.

Página dejada en blanco intencionadamente



Sección 1:

Introducción y visión general de la ciberseguridad

Los temas tratados en esta sección incluyen:

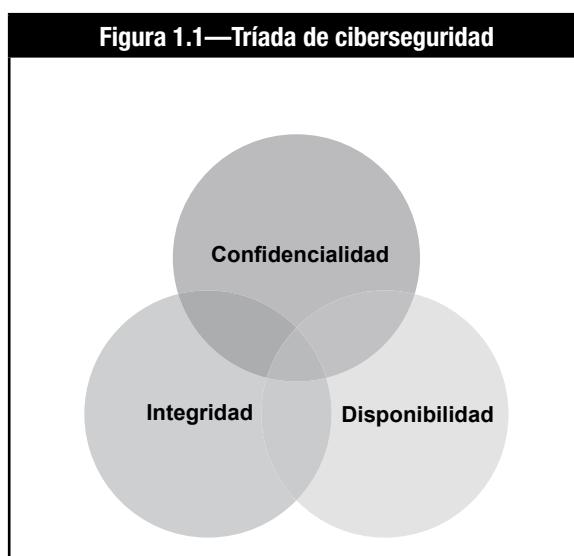
1. Introducción a la ciberseguridad
2. Diferencia entre seguridad de la información y ciberseguridad
3. Objetivos de la ciberseguridad
4. Gobierno de la ciberseguridad
5. Dominios de la ciberseguridad

Página dejada en blanco intencionadamente

TEMA 1—INTRODUCCIÓN A LA CIBERSEGURIDAD

LA EVOLUCIÓN DE LA CIBERSEGURIDAD

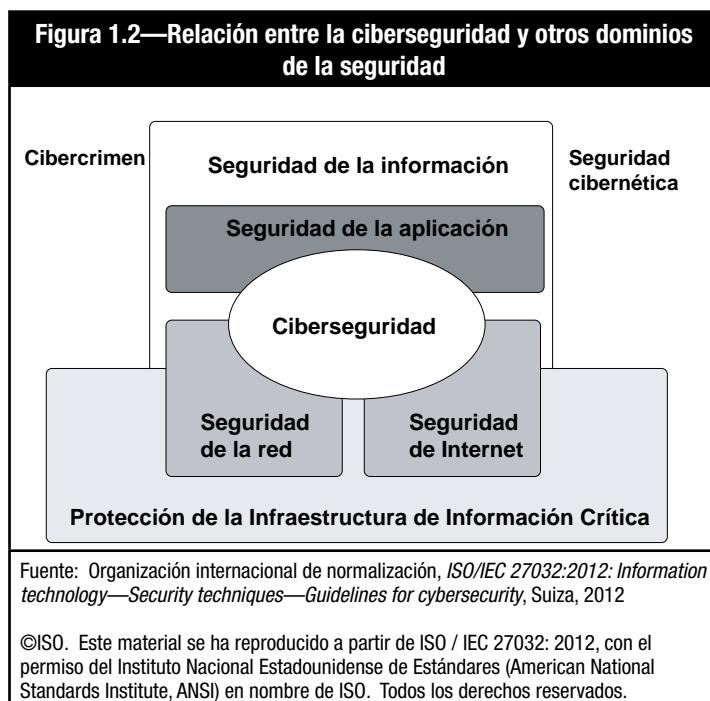
Salvaguardar la información ha sido una prioridad desde que las personas han necesitado mantener la información de una forma segura y privada. Incluso las técnicas de cifrado simples como César fueron creadas para garantizar la confidencialidad. Pero conforme el tiempo y la tecnología avanzan, también lo hacen las exigencias de seguridad. Hoy en día, el objetivo de la seguridad de la información es triple, involucrando los componentes críticos de confidencialidad, integridad y disponibilidad (ver **figura 1.1**). Los tres componentes tienen que ver con la protección de la información. La **confidencialidad** significa protección contra el acceso no autorizado, mientras que la **integridad** significa protección contra modificaciones no autorizadas, y la **disponibilidad** significa protección frente a las interrupciones en el acceso.



Los términos "ciberseguridad" y "seguridad de la información" se suelen usar indistintamente, pero en realidad la ciberseguridad es una parte de la seguridad de la información. Concretamente, la **ciberseguridad** se puede definir como la **protección de los activos de información, abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados**.

Generalmente, la ciberseguridad hace referencia a las amenazas que afectan a una entidad debido a la existencia de un ciberespacio global. A diferencia de la seguridad de la información, la ciberseguridad no incluye los peligros naturales, los errores personales o la seguridad física. Para decirlo de una manera más simple, si eliminamos las amenazas derivadas de un comportamiento humano ofensivo y adverso que vienen a través de sistemas interconectados, la ciberseguridad no sería un problema, y la seguridad de la información por sí sola sería suficiente.

La **Figura 1.2** muestra las complejas relaciones entre la ciberseguridad y otros dominios de la seguridad, tal y como se describen en la Organización internacional de normalización (ISO) 27032. Por ejemplo, no todos los servicios de infraestructuras críticas (por ejemplo, el agua, el transporte) afectarán directa o significativamente al estado de la ciberseguridad dentro de una organización. Sin embargo, la falta de medidas apropiadas de ciberseguridad puede afectar negativamente a la disponibilidad y fiabilidad de los sistemas de infraestructuras críticas que son utilizadas por los proveedores de estos servicios (por ejemplo, las telecomunicaciones).¹



La gestión de las cuestiones de ciberseguridad exige la coordinación entre muchas entidades —públicas y privadas, locales y globales— puesto que la ciberseguridad está estrechamente vinculada a la seguridad de Internet, las redes empresariales y domésticas y la seguridad de la información. Ello puede ser complicado porque debido a cuestiones de seguridad nacional, algunos servicios de infraestructuras críticas no pueden ser discutidos de una forma abierta, y el conocimiento de las debilidades de estos servicios puede tener un impacto en la seguridad. Por lo tanto, se necesita un marco básico para el intercambio de información y la coordinación de incidentes para asegurar a las partes interesadas que las cuestiones de ciberseguridad se están tratando.²

CIBERSEGURIDAD Y CONCIENCIACIÓN SITUACIONAL

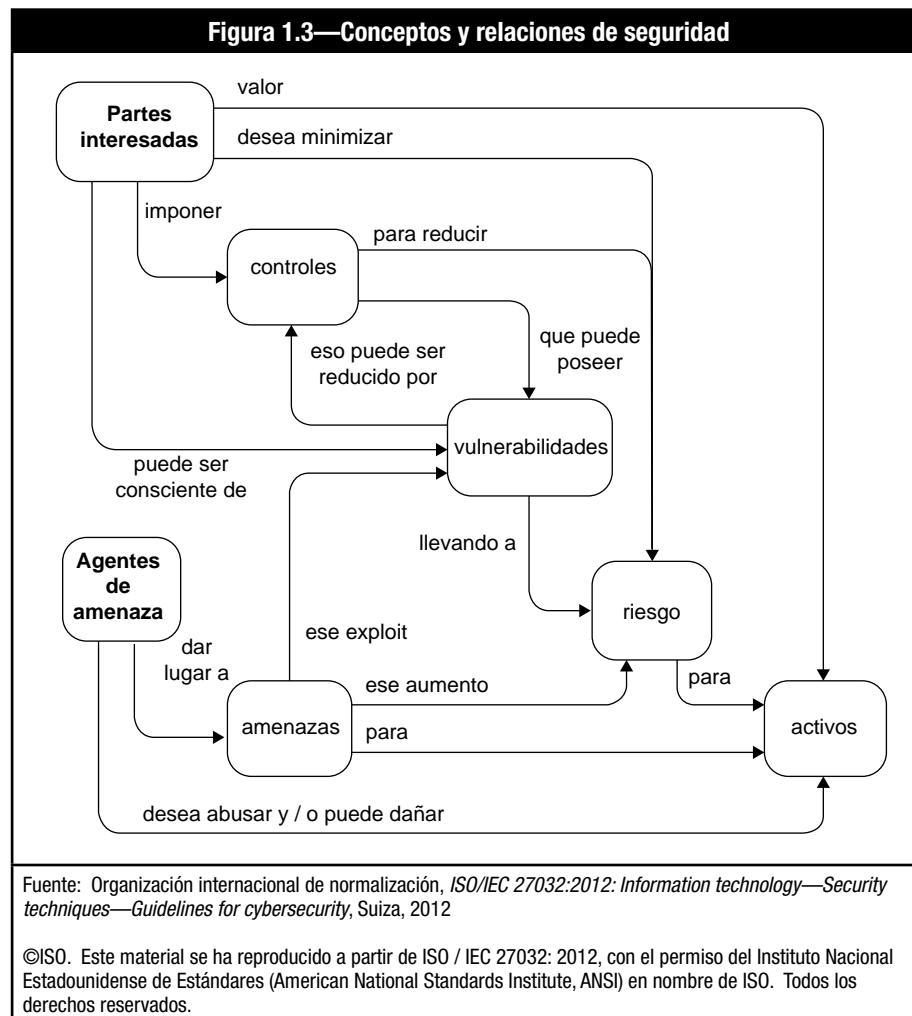
La ciberseguridad juega un papel significativo en el panorama cibernetico actual que está en constante evolución. Las nuevas tendencias en movilidad y conectividad presentan una amplia variedad de desafíos, puesto que los nuevos ataques continúan desarrollándose al mismo tiempo que las tecnologías emergentes. Los profesionales de la ciberseguridad deben estar informados y deben ser flexibles para identificar y gestionar eficazmente nuevas amenazas potenciales, tales como las amenazas persistentes avanzadas (APTs). **Las APTs son ataques de un adversario que posee niveles sofisticados de experiencia y que además dispone de tiempo, paciencia y recursos significativos, que permiten al atacante crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataque.**

Para proteger con éxito sus sistemas e información, los profesionales de la ciberseguridad deben mostrar un alto grado de conciencia situacional. Este tipo de conciencia se adquiere con el tiempo, ya que generalmente se desarrolla a través de la experiencia dentro de una organización específica. Cada organización tiene su propia cultura distintiva, lo que significa que las condiciones varían mucho de una organización a otra. Por lo tanto, es fundamental que los profesionales de la ciberseguridad tengan una comprensión detallada del entorno en el que operan y ser profundamente conscientes de las amenazas que afectan a otras organizaciones e industrias para garantizar que se mantiene el conocimiento relevante.

¹ Organización internacional de normalización, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Suiza, 2012

² *Ibid.*

La protección de los activos contra las amenazas es una preocupación primordial para la seguridad en general. A su vez, las amenazas se clasifican en función de la probabilidad (es decir, posibilidad) de que afecten a los activos protegidos. En seguridad, las amenazas que están relacionadas con actividades maliciosas u otras actividades humanas a menudo reciben mayor atención. La **Figura 1.3** ilustra estos conceptos y relaciones de seguridad.



La responsabilidad de proteger estos activos recae en las partes interesadas para quienes estos activos tienen valor. Por lo tanto, las partes interesadas deben tener en cuenta las amenazas al evaluar el riesgo a estos activos. Esta evaluación del riesgo, discutida en la sección 4.1, ayudará en el proceso de selección de los controles. Los controles se usan para proteger activos, reducir vulnerabilidades e impactos, y / o reducir el riesgo a un nivel aceptable. Deben ser monitorizados y revisados para asegurar que cada control específico sea adecuado para contrarrestar el riesgo a mitigar para el que ha sido diseñado. Es importante tener en mente que el riesgo no puede ser eliminado totalmente, permanece el riesgo residual. Las partes interesadas deben tratar de minimizar el nivel de riesgo residual. También puede ser necesario utilizar recursos externos para garantizar que los controles funcionen correctamente.

El entorno empresarial, en particular, tiende a impulsar las decisiones sobre el riesgo. Por ejemplo, una pequeña empresa de nueva creación puede ser mucho más tolerante con el riesgo que una empresa grande y consolidada. Por lo tanto, puede ser útil hacer referencia a los criterios generales enumerados a continuación cuando se evalúan los factores que afectan la seguridad de una organización específica.

Respecto a la tecnología, muchos factores pueden afectar a la seguridad, tales como:

- Nivel de complejidad de las TI
- Conectividad de red (por ejemplo, interna, de un tercero, pública)
- Instrumentación y dispositivos de la industria especialista
- Plataformas, aplicaciones y herramientas utilizadas
- En sistemas en la nube o en sistemas híbridos
- Apoyo operativo para la seguridad
- La comunidad de usuarios y sus capacidades
- Herramientas de seguridad, nuevas o emergentes

Al evaluar los planes de negocio y el entorno empresarial general, considere impulsores, tales como:

- Naturaleza del negocio
- Tolerancia al riesgo
- Apetito de riesgo
- Misión, visión y estrategia de seguridad
- Alineamiento con la industria y tendencias de seguridad
- Requisitos de cumplimiento y regulaciones específicos de la industria
- Requisitos regionales de cumplimiento y regulatorios
 - País o estado en el que se opera
- Fusiones, adquisiciones y alianzas
 - Considerar el tipo, la frecuencia y el nivel resultante de la integración
- Servicios de externalizados o proveedores

Aunque los impulsores de negocios y de la tecnología no pueden predecirse con certeza, se deben anticipar razonablemente y gestionar tan eficientemente como sea posible. El fracaso en la predicción de los impulsores clave de seguridad refleja la incapacidad para reaccionar con eficacia ante las circunstancias cambiantes del negocio, lo que a su vez se traduce en una seguridad reducida y en la pérdida de oportunidades de mejora.

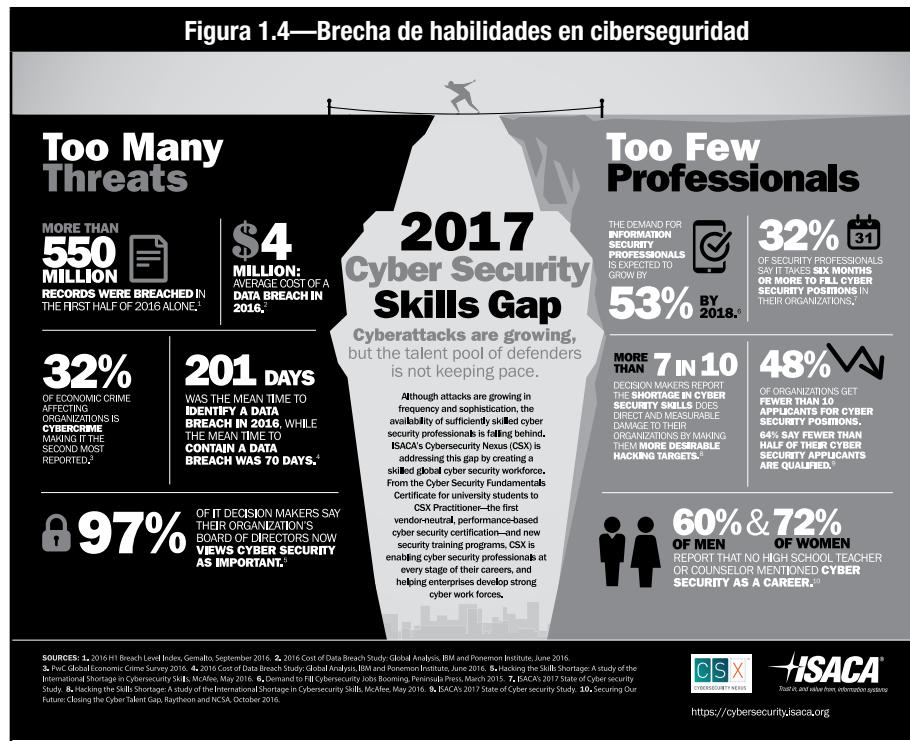
BRECHA EN LAS HABILIDADES DE CIBERSEGURIDAD

La ciberseguridad es un campo que demanda profesionales cualificados que posean los conocimientos básicos, la educación y el liderazgo de pensamiento necesario para hacer frente a las dificultades que acompañan el cambio tecnológico constante. Los vectores de amenazas avanzados, las tecnologías emergentes y las innumerables regulaciones requieren de profesionales de la ciberseguridad expertos en tecnología, así como en negocios y en comunicación.

La ciberseguridad se encarga tanto de las amenazas internas como de las externas a los activos de información digital de una organización, centrándose en los procesos críticos de datos electrónicos, procesamiento de transacciones, análisis de riesgo y la ingeniería de seguridad de los sistemas de información.

Se estima que hay entre 410.000 a 510.000 profesionales de seguridad de la información en todo el mundo, y se espera que la demanda aumente un 53% para 2018 con más de 4,2 millones de puestos de trabajo disponibles. Sin embargo, estudios e informes recientes sugieren que simplemente no hay suficientes profesionales capacitados para cubrir dichos puestos.

Mientras que el panorama de la ciberseguridad ha evolucionado, el conjunto de habilidades entre los profesionales de la ciberseguridad, existentes o potenciales, no lo ha hecho al mismo ritmo. Hay una carencia de profesionales especialistas en ciberseguridad, tal y como se muestra en la **figura 1.4**. Según el estudio de ISACA *Estado de la ciberseguridad en 2017*, el 48% de las organizaciones reciben menos de 10 solicitantes para puestos de ciberseguridad, y el 64% dice que menos de la mitad de sus solicitantes de ciberseguridad están cualificados.³ Asimismo, el Comisario de la Agenda Digital de la Unión Europea (UE) cree que el creciente déficit de capacidades en ciberseguridad está amenazando la competitividad de la UE. Las brechas de habilidades se observan tanto en aspectos técnicos como en aspectos de negocio de la seguridad. Esta guía ofrece una visión general de estas prácticas de negocio y técnicas, junto con otras metodologías y procedimientos relacionados con la ciberseguridad.



³ ISACA, Estudio sobre el Estado de la ciberseguridad en 2017, <https://cybersecurity.isaca.org>

Página dejada en blanco intencionadamente

TEMA 2—DIFERENCIA ENTRE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

La **seguridad de la información** trata con la información, independientemente de su formato - incluye documentos en papel, propiedad digital e intelectual, y las comunicaciones verbales o visuales. La **ciberseguridad**, por otro lado, se ocupa de la protección de los activos digitales – cualquier cosa incluida en redes, hardware, software, así como la información que es procesada, almacenada en sistemas aislados o transportada a través entornos de información interconectados. Además, conceptos tales como ataques patrocinados por naciones-estados y amenazas avanzadas persistentes (APTs) pertenecen casi exclusivamente a la ciberseguridad. Puede ser útil pensar en la ciberseguridad como un componente de la seguridad de la información.

Por lo tanto, para eliminar cualquier tipo de confusión, el término **ciberseguridad** se define en esta guía como la **protección de activos de información** que aborda las amenazas a la información procesada, almacenada y transportada a través de los sistemas de información interconectados.

LA PROTECCIÓN DE ACTIVOS DIGITALES

En el núcleo de su marco de seguridad cibernética, el Instituto Nacional de Normas y Tecnología (NIST) identifica cinco funciones clave necesarias para la protección de los activos digitales. Estas funciones coinciden con metodologías de gestión de incidentes e incluyen las siguientes actividades:⁴

- **Identificar**—Usar el entendimiento de la organización para minimizar el riesgo de los sistemas, activos, datos y capacidades.
- **Proteger**—Diseñar salvaguardas para limitar el impacto de los eventos potenciales en servicios e infraestructuras críticas.
- **Detectar**—Implementar actividades para identificar la ocurrencia de un evento de ciberseguridad.
- **Responder**—Tomar las medidas adecuadas tras conocerse un evento de seguridad.
- **Recuperar**—Planificar para tener resiliencia y recuperar de forma oportuna los servicios y capacidades comprometidos.

⁴ Instituto Nacional de Normas y Tecnología (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, EE.UU., 2014, www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Página dejada en blanco intencionadamente

TEMA 3—OBJETIVOS DE LA CIBERSEGURIDAD

La ciberseguridad requiere que las partes interesadas en el área del ciberespacio estén activas en la seguridad, más allá de la protección de sus propios activos. Deben estar preparadas para identificar y abordar los riesgos emergentes y los retos para mantener los activos protegidos. La ciberseguridad trabaja con la seguridad de la información y está más allá de la simple seguridad de Internet, redes y / o aplicaciones. Requiere trabajar con todos estos componentes para mantener el ciberespacio útil y confiable.

La ciberseguridad tiene como propósito cumplir ciertos objetivos en la protección de los activos digitales. Estos incluyen la confidencialidad, integridad y disponibilidad de los activos entre otros aspectos. Estas estrategias se analizarán más adelante de una forma más detallada.

CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Para entender mejor la ciberseguridad y la protección de activos digitales, es útil tener en cuenta tres conceptos clave que se utilizan para guiar las políticas de seguridad de la información, como se muestra en la **figura 1.5**. Los conceptos son:

- Confidencialidad
- Integridad
- Disponibilidad



La **confidencialidad** es la protección de la información contra el acceso no autorizado o la divulgación. Diferentes tipos de información requieren diferentes niveles de confidencialidad, y la necesidad de confidencialidad puede cambiar a lo largo del tiempo. La información personal, financiera y médica requiere un mayor grado de confidencialidad que, por ejemplo, las actas de una reunión del personal. Del mismo modo, algunas empresas necesitan proteger información sobre futuros productos competitivos antes de lanzarlos al mercado, pero puede que tengan que hacer pública esa misma información después.

Los datos deben ser protegidos frente a la divulgación indebida de acuerdo a su sensibilidad y los requisitos legales aplicables. La confidencialidad de la información digital puede ser mantenida usando diferentes medios, incluyendo controles de acceso, permisos para los archivos y cifrado.

La **integridad** es la protección de la información contra la modificación no autorizada. Por ejemplo, si un banco transfiere \$10.000 a otra institución financiera, es importante que la cantidad no cambie a \$100.000 durante dicho intercambio. El concepto de integridad también se aplica a mensajería electrónica, archivos, software y configuraciones.

Cualquier violación de la integridad es importante, ya que puede ser el primer paso de un ataque exitoso contra la disponibilidad o confidencialidad del sistema. Los sistemas contaminados y los datos corruptos deben ser tratados de inmediato con el objetivo de evaluar el nivel potencial de violación o daños. La integridad de los activos digitales puede ser controlada y verificada mediante registros de acceso, firmas digitales, resúmenes criptográficos, cifrado y controles de acceso.

La disponibilidad garantiza el acceso oportuno y confiable al uso de la información y los sistemas. Esto incluye salvaguardas para asegurar que los datos no se eliminan de forma accidental o malintencionada. Esto es particularmente importante en un sistema de misión crítica, ya que cualquier interrupción en su disponibilidad puede resultar en una pérdida de productividad e ingresos. Del mismo modo, la pérdida de datos puede afectar la capacidad de la dirección para tomar decisiones y respuestas efectivas. La disponibilidad puede protegerse mediante el uso de redundancia, copias de seguridad y la implementación de la gestión y planificación de la continuidad del negocio (para más información, consulte la Sección 5, Tema 5).

Los impactos, las consecuencias potenciales y los métodos de control de la confidencialidad, integridad y disponibilidad se muestran en la **figura 1.6**.

Figura 1.6—Modelo de Confidencialidad, Integridad y Disponibilidad y sus impactos relacionados

Requerimiento	Impacto y Consecuencias potenciales	Métodos de control
Confidencialidad: La protección de la información contra la divulgación no autorizada	<p>La pérdida de confidencialidad puede resultar en las siguientes consecuencias:</p> <ul style="list-style-type: none"> • La divulgación de información protegida por leyes de privacidad • La pérdida de confianza del público • La pérdida de ventaja competitiva • Acciones legales contra la empresa • Interferencia con la seguridad nacional • Pérdida de cumplimiento 	<p>La confidencialidad puede ser preservada utilizando los siguientes métodos:</p> <ul style="list-style-type: none"> • Controles de acceso • Permisos de archive • Cifrado
Integridad: La exactitud y completitud de la información de acuerdo con valores y expectativas de la empresa	<p>La pérdida de integridad puede resultar en las siguientes consecuencias:</p> <ul style="list-style-type: none"> • Imprecisión • Decisiones erróneas • Fraude • Fallos de hardware • Pérdida de cumplimiento 	<p>La integridad puede ser preservada utilizando los siguientes métodos:</p> <ul style="list-style-type: none"> • Controles de acceso • Registros de acceso • Firmas digitales • Resúmenes criptográficos • Copias de seguridad • Cifrado
Disponibilidad: La capacidad de acceder a la información y a los recursos requeridos por los procesos de negocio	<p>La pérdida de disponibilidad puede resultar en las siguientes consecuencias:</p> <ul style="list-style-type: none"> • La pérdida de funcionalidad y eficacia operativa • La pérdida de tiempo productivo • Multas de los reguladores o una demanda • Interferencia con los objetivos de la empresa • Pérdida de cumplimiento 	<p>La disponibilidad puede ser preservada utilizando los siguientes métodos:</p> <ul style="list-style-type: none"> • Redundancia de redes, sistemas, datos • Arquitecturas de sistemas altamente disponibles • Replicación de datos • Copias de seguridad • Controles de acceso • Un plan de recuperación de desastres o plan de continuidad de negocios bien diseñado

NO REPUDIO

El no repudio es una consideración importante en la ciberseguridad. Se refiere al concepto de garantizar que un mensaje u otra información es genuina. Cuando se envía información, es importante verificar que proviene de la fuente de la que se dice que proviene. El no repudio provee un medio para que la persona que envía o recibe información no pueda negar que envió o recibió dicha información. Se implementa a través de firmas digitales y registros de transacciones.

TEMA 4—GOBIERNO DE LA CIBERSEGURIDAD

GOBIERNO, GESTIÓN DE RIESGOS Y CUMPLIMIENTO

La estructura y gobierno de cada organización son diferentes y varían en función del tipo de organización. Cada organización tiene su propia misión (negocio), tamaño, industria, cultura y normas legales. Sin embargo, todas las organizaciones tienen la responsabilidad y el deber de proteger sus activos y operaciones, incluyendo su infraestructura de TI y la información. En el más alto nivel, esto se conoce generalmente como gobierno, gestión del riesgo y cumplimiento (GRC: del inglés Governance, Risk and Compliance). Algunas entidades implementan estas tres áreas de manera integrada, mientras que otras pueden tener enfoques menos amplios. Independientemente de la aplicación, cada organización necesita un plan para gestionar estos tres elementos.

El **gobierno** es la responsabilidad de la Junta Directiva y la Gerencia de la organización. Un programa de gobierno tiene varios objetivos:

- Proporcionar orientación estratégica
- Asegurarse de que se cumplan los objetivos
- Determinar si el riesgo se está gestionando apropiadamente
- Verificar que los recursos de la organización se están utilizando de manera responsable

La **gestión del riesgo** es la coordinación de las actividades que dirigen y controlan una empresa con respecto al riesgo. La gestión de riesgos requiere el desarrollo e implementación de controles internos para gestionar y mitigar los riesgos en toda la organización, incluyendo los riesgos financieros, operativos, de reputación, de inversión, el riesgo físico y el ciber riesgo.

El **cumplimiento** es el acto de adherirse a, y la capacidad de demostrar adhesión a, los requisitos obligatorios definidos por leyes y regulaciones. También incluye requisitos voluntarios que resultan de las obligaciones contractuales y las políticas internas.

La ciberseguridad es responsabilidad de toda la organización en todos sus niveles. En la siguiente sección se describen algunas de las funciones específicas en la gestión del ciber riesgo en la mayoría de las organizaciones.

ROL DEL PROFESIONAL DE LA CIBERSEGURIDAD

Los deberes del profesional de ciberseguridad incluyen el análisis de la política, las tendencias y la inteligencia. Al hacer uso de la solución de problemas y de las habilidades de detección, ellos buscan comprender mejor cómo un adversario puede pensar o comportarse. La complejidad inherente de su trabajo requiere que los profesionales de ciberseguridad posean no sólo una amplia gama de habilidades técnicas de TI, sino también capacidades analíticas avanzadas. Un profesional de la ciberseguridad puede ser un profesional y / o parte de la alta administración.

ROLES EN LA SEGURIDAD DE LA INFORMACIÓN

Debido a que la ciberseguridad es parte de la seguridad de la información, en algunas ocasiones hay una superposición entre los términos y la forma en que son aplicados a las estructuras de gestión y los títulos. Para los propósitos de esta discusión, asumiremos que el término seguridad de la información abarca los roles y funciones de la ciberseguridad.

Comité de dirección

El gobierno de la ciberseguridad requiere contribuciones y dirección estratégica. Depende del compromiso, los recursos y la responsabilidad de la gestión de la ciberseguridad y requiere de un medio a través del cual la junta directiva pueda determinar si su intención ha sido alcanzada. Un gobierno eficaz sólo puede lograrse mediante la participación de la alta dirección en la aprobación de políticas y un apropiado seguimiento y la medición unidos a la presentación de informes y análisis de tendencias.

Los miembros del consejo tienen que ser conscientes de los activos de información de la organización y de las operaciones críticas de negocio en curso. El consejo debe contar periódicamente con los resultados de alto nivel de las evaluaciones de riesgos globales y el análisis de impacto del negocio (BIAs), los cuales identifican la rapidez con la que las unidades y los procesos esenciales del negocio tienen que volver a su plena operación después de un desastre. Como resultado de estas actividades, los miembros de la junta directiva deben identificar los activos clave que quieren proteger y verificar si los niveles de protección y las prioridades son apropiados a un estándar de debida diligencia.

La actitud de la gerencia debe conducir a un gobierno eficaz de la seguridad. Corresponde a la alta dirección establecer un ejemplo positivo en este sentido, ya que el personal de los niveles inferiores es mucho más propenso a cumplir con las medidas de seguridad cuando ven que sus superiores, respetan las mismas medidas. El respaldo de la gerencia ejecutiva a los requisitos de seguridad asegura que las expectativas de seguridad se cumplan en todos los niveles de la empresa. Las penalizaciones por incumplimiento deben ser definidas, comunicadas y ejecutadas desde el nivel del consejo de dirección hacia abajo.

Más allá de estos requisitos, la junta directiva tiene la obligación permanente de supervisar las actividades relacionadas con la ciberseguridad. La alta dirección tiene la responsabilidad legal y ética de ejercer el debido cuidado en la protección de los activos clave de la organización, incluyendo su información confidencial y crítica. Por lo tanto, se requiere su implicación y supervisión.

Dirección ejecutiva

El equipo que forma la dirección ejecutiva de una organización es responsable de asegurar que las funciones organizacionales, recursos e infraestructura de apoyo necesarias, están disponibles y se utilizan adecuadamente para cumplir con las directrices de la junta directiva, el cumplimiento normativo y otras demandas.

En general, la dirección ejecutiva recurre al jefe de seguridad de la información (CISO) u otro alto gerente de ciberseguridad para definir el programa de seguridad de la información y su posterior gestión. A menudo, también se espera que el gerente de ciberseguridad proporcione formación y orientación al equipo de gestión ejecutiva. El rol de gerente en esta situación es opuesto al tomador decisiones, y a menudo se limita a la presentación de opciones y la información de apoyo de las decisiones clave. En otras palabras, el gestor de la ciberseguridad actúa como consultor.

La dirección ejecutiva establece el tono para la gestión de la ciberseguridad dentro de la organización. El nivel de participación visible y la inclusión de la gestión de riesgo de la información en las actividades y las decisiones clave de negocio indican a los demás gerentes el nivel de importancia que se espera que ellos concedan a la gestión del riesgo en las actividades de sus organizaciones.

Gerente de seguridad de la información

El nombre exacto de la persona que supervisa la seguridad de la información y la ciberseguridad varía de una organización a otra. Uno de los nombres más comunes es oficial de seguridad de la información (CISO: del inglés, Chief Information Security Officer), pero algunas organizaciones prefieren el término jefe de seguridad (CSO: del inglés, Chief Security Officer) para denotar la responsabilidad de todos los asuntos de seguridad, tanto físicos como digitales. Del mismo modo, las responsabilidades y la autoridad de los directores de seguridad de información varían dramáticamente entre las organizaciones.

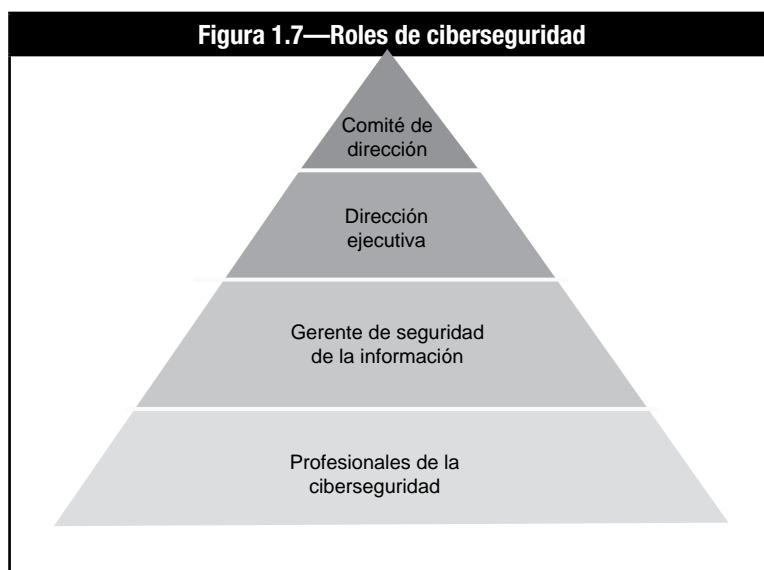
En general, el gerente de ciberseguridad será responsable de:

- El desarrollo de la estrategia de seguridad
- Supervisar el programa y las iniciativas de seguridad
- Coordinarse con los propietarios de los procesos de negocio para mantener la alineación continua
- Garantizar que se realicen las evaluaciones de riesgo e impacto al negocio.
- Desarrollar estrategias de mitigación de riesgo
- Hacer cumplir las políticas y el cumplimiento normativo
- Monitorizar la utilización y eficacia de los recursos de seguridad
- Desarrollar e implementar una monitorización y métricas
- Dirigir y monitorizar actividades de seguridad
- Gestionar incidentes de ciberseguridad y su resolución, así como incorporar las lecciones aprendidas

Profesionales de la ciberseguridad

En la mayoría de las organizaciones, la ciberseguridad es gestionada por un equipo de expertos en la materia y por profesionales en ciberseguridad, incluyendo arquitectos de seguridad, administradores, forenses digitales, administradores de incidentes, investigadores de vulnerabilidad y especialistas en seguridad de red. Juntos diseñan, implementan y gestionan procesos y controles técnicos y responden a los eventos e incidentes.

Estos profesionales trabajan dentro de la dirección, las políticas, las directrices, los mandatos y los reglamentos establecidos por el consejo de directores, ejecutivos y gestores de la ciberseguridad. Los roles de ciberseguridad se muestran en la **figura 1.7**.



Página dejada en blanco intencionadamente

TEMA 5—DOMINIOS DE LA CIBERSEGURIDAD

Existen cinco dominios de la ciberseguridad. Cada dominio está cubierto en detalle en cada sección de esta guía. Este tema proporciona una visión general de cada dominio. Los cinco dominios de la ciberseguridad son:

- Conceptos de ciberseguridad
- Principios de arquitectura de seguridad
- Seguridad de Redes, Sistemas, Aplicaciones y Datos
- Respuesta a Incidentes
- Implicaciones de seguridad y adopción de la tecnología evolutiva

CONCEPTOS DE CIBERSEGURIDAD

Este dominio presenta una discusión sobre conceptos críticos, tales como:

- Gestión básica de riesgos
- Vectores comunes de ataque y agentes de amenazas
- Los patrones y tipos de ataques
- Tipos de políticas y procedimientos de seguridad
- Procesos de control de ciberseguridad

Se abordan todos estos conceptos en relación a cómo éstos influyen en las políticas de seguridad y los procedimientos en materia de amenazas de ciberseguridad. Cada tema considera diversos enfoques centrados en las mejores prácticas de seguridad.

PRINCIPIOS DE ARQUITECTURA DE SEGURIDAD

Este dominio proporciona información que ayuda a los profesionales de la seguridad a identificar y aplicar los principios de la arquitectura de seguridad. En él se discute una variedad de temas, incluyendo:

- Arquitectura e infraestructura comunes de seguridad y marcos de trabajo
- Conceptos de seguridad perimetral
- Topología del sistema y conceptos sobre perímetro de seguridad
- Cortafuegos (Firewall) y cifrado
- El aislamiento y la segmentación
- Métodos de monitorización, detección y registros de acceso

Estos temas se presentan poniendo especial atención en las mejores prácticas de seguridad. Se discuten varios tipos de arquitecturas de seguridad para ilustrar la importancia que tienen las capas de controles para lograr una defensa en profundidad.

SEGURIDAD DE REDES, SISTEMAS, APlicACIONES Y DATOS

Este dominio aborda técnicas básicas de bastionado de sistemas y medidas de seguridad, incluyendo:

- Controles de procesos
 - Evaluaciones de riesgos
 - Gestión de vulnerabilidad
 - Pruebas de penetración
- Mejores prácticas para la securización de redes, sistemas, aplicaciones y datos
 - Amenazas y vulnerabilidades de seguridad en sistemas y aplicaciones
 - Controles eficaces para la gestión de vulnerabilidades

Estas discusiones tienen como objetivo ayudar a los profesionales de la ciberseguridad a evaluar su tolerancia al riesgo y responder apropiadamente a vulnerabilidades.

RESPUESTA A INCIDENTES

En este dominio se articula la distinción fundamental entre un evento y un incidente. Más importante aún, se describen las medidas necesarias para responder ante un incidente de ciberseguridad. Cubre los siguientes temas:

- Categorías de incidentes
- Planes de recuperación de desastres y de continuidad del negocio
- Pasos de respuesta a incidentes
- Análisis forense y preservación de evidencias

Estas discusiones tienen por objetivo proporcionar a los profesionales principiantes el nivel de conocimientos necesario para responder a incidentes de ciberseguridad de una manera competente.

IMPLICACIONES DE SEGURIDAD Y ADOPCIÓN DE LA TECNOLOGÍA EVOLUTIVA

Este dominio describe el panorama de amenazas actual, incluyendo un análisis de las vulnerabilidades asociadas con las siguientes tecnologías emergentes:

- Dispositivos móviles (Trae tu propio dispositivo [del inglés Bring Your Own Device, BYOD], Internet de las Cosas [del inglés Internet of Things, IoT])
- Computación y almacenamiento en la nube
- Colaboración digital (social media)

Aunque el panorama de amenazas actual sigue evolucionando, esta sección destaca los desarrollos recientes que más probablemente impactarán a los profesionales de ciberseguridad. Por ejemplo, discute las implicaciones de traer su propio dispositivo (BYOD: del inglés Bring Your Own device) y señala el riesgo presentado por las aplicaciones móviles y web. También hay una extensa discusión de las APTs y sus objetivos más frecuentes.

SECCIÓN 1—EVALUACIÓN DE CONOCIMIENTOS

1. Tres controles comunes que se utilizan para proteger la disponibilidad de información son:
 - A. redundancia, copias de seguridad y controles de acceso.
 - B. cifrado, permisos de archivos y controles de acceso.
 - C. controles de acceso, archivos de registros (logs) y firmas digitales.
 - D. hashes, archivos de registros (logs) y las copias de seguridad.
2. Seleccione todas las opciones que apliquen. El gobierno corporativo tiene varios objetivos, entre ellos:
 - A. proporcionar orientación estratégica.
 - B. asegurar que se cumplen los objetivos.
 - C. verificar que los recursos de la organización se están utilizando adecuadamente.
 - D. dirigir y monitorizar las actividades de seguridad.
 - E. asegurar que el riesgo se gestiona correctamente.
3. Escoja tres. De acuerdo con el marco de referencia del NIST, cuáles de las siguientes se consideran funciones clave necesarias para la protección de activos digitales?
 - A. Cifrar
 - B. Proteger
 - C. Investigar
 - D. Recuperar
 - E. Identificar
4. ¿Cuál de las siguientes es la mejor definición de la ciberseguridad?
 - A. El proceso por el cual una organización gestiona el riesgo de la ciberseguridad a un nivel aceptable
 - B. La protección de la información contra el acceso no autorizado o divulgación
 - C. La protección de los documentos en papel, digitales y la propiedad intelectual, y las comunicaciones verbales o visuales
 - D. La protección de los activos de información, mediante el tratamiento de las amenazas a la información procesada, almacenada o transportada por sistemas de información conectados a través de redes.
5. ¿Cuál de los siguientes roles de ciberseguridad es responsable de gestionar los incidentes y su remediación?
 - A. Consejo de dirección
 - B. Comité Ejecutivo
 - C. Gestión de la seguridad
 - D. Profesionales de la ciberseguridad

Ver respuestas en el Anexo C.

Página dejada en blanco intencionadamente



CYBERSECURITY NEXUS

Sección 2:

Conceptos de Ciberseguridad

Los temas tratados en esta sección incluyen:

1. Riesgo
2. Tipos y vectores de ataque comunes
3. Políticas
4. Controles de ciberseguridad

Página dejada en blanco intencionadamente

TEMA 1—RIESGO

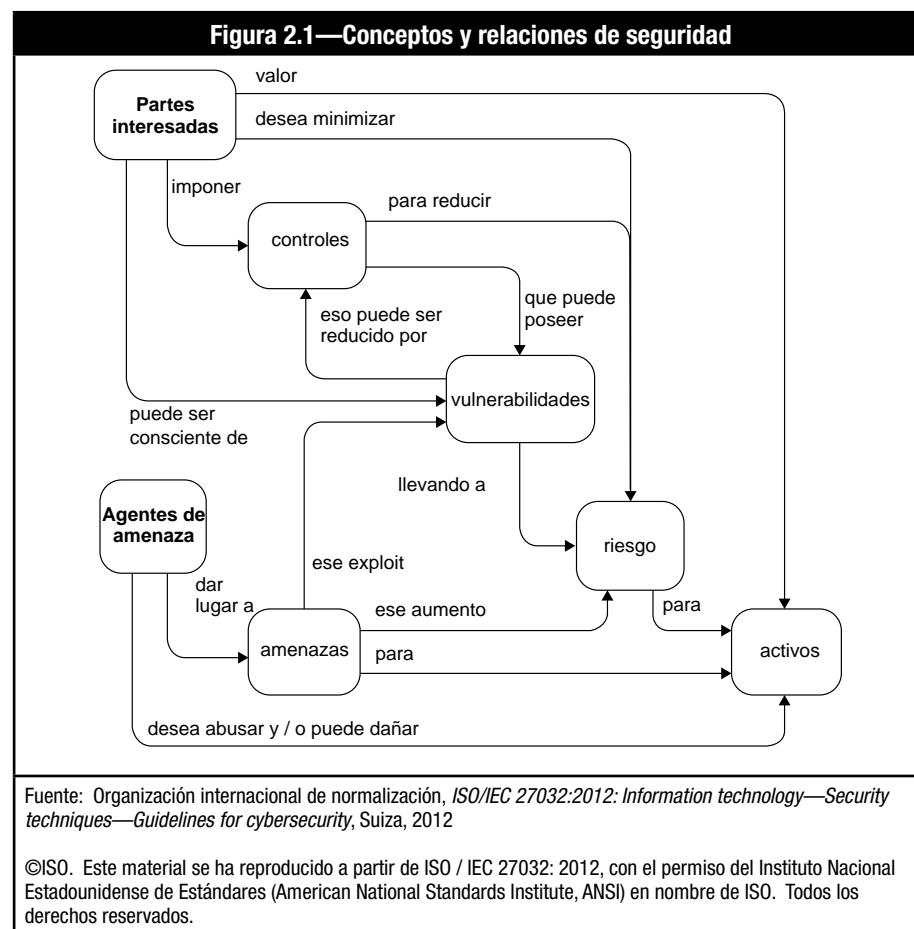
El deber principal de la ciberseguridad es identificar, mitigar y gestionar el ciberriesgo a los activos digitales de una organización. Ciberriesgo es aquella parte de la gestión global del riesgo que se centra exclusivamente en el riesgo que se manifiesta en el dominio ciber (Entornos de información interconectados). Aunque la mayoría de la gente tiene una comprensión inherente de la palabra riesgo en su vida diaria, es importante comprender el riesgo en el contexto de la ciberseguridad, lo cual significa saber cómo determinar, medir y reducir el riesgo de manera efectiva.

La evaluación de riesgos es una de las funciones más importantes de una organización de la ciberseguridad. Las políticas eficaces, las implementaciones de seguridad, la asignación de recursos y la preparación para la respuesta a un incidente dependen todas de la comprensión de los riesgos y amenazas a los que se enfrenta una organización. Utilizar un enfoque basado en el riesgo para la ciberseguridad permite una toma de decisiones que se basa en información relevante para proteger la organización y usar los presupuestos y los recursos limitados de una manera efectiva. Si los controles no se implementan basándose en el conocimiento de los riesgos reales, entonces los activos de la organización no estarán protegidos adecuadamente mientras que otros activos serán sobreprotegidos, lo cual supone un derroche de recursos.⁵

Con demasiada frecuencia, los controles de ciberseguridad se implementan con poca o ninguna evaluación de riesgos. Una encuesta mundial de ISACA realizada a responsables de gestión de TI, auditores y gerentes de seguridad, mostró que más del 80% de las empresas creen que “los riesgos de seguridad de la información, o bien no se conocen, o sólo se evalúan parcialmente” y que “el analfabetismo y la falta de conciencia del riesgo en las TI” son los principales retos en la gestión de riesgos.⁶ Por lo tanto, entender el riesgo y las evaluaciones de riesgo son requisitos fundamentales para cualquier profesional de seguridad.

CONCEPTOS CLAVE Y SUS DEFINICIONES

Un resumen visual de los términos clave se presenta en la Organización internacional de normalización (ISO) / Comisión Internacional Electrotécnica (IEC) 27032 (**figura 2.1**).



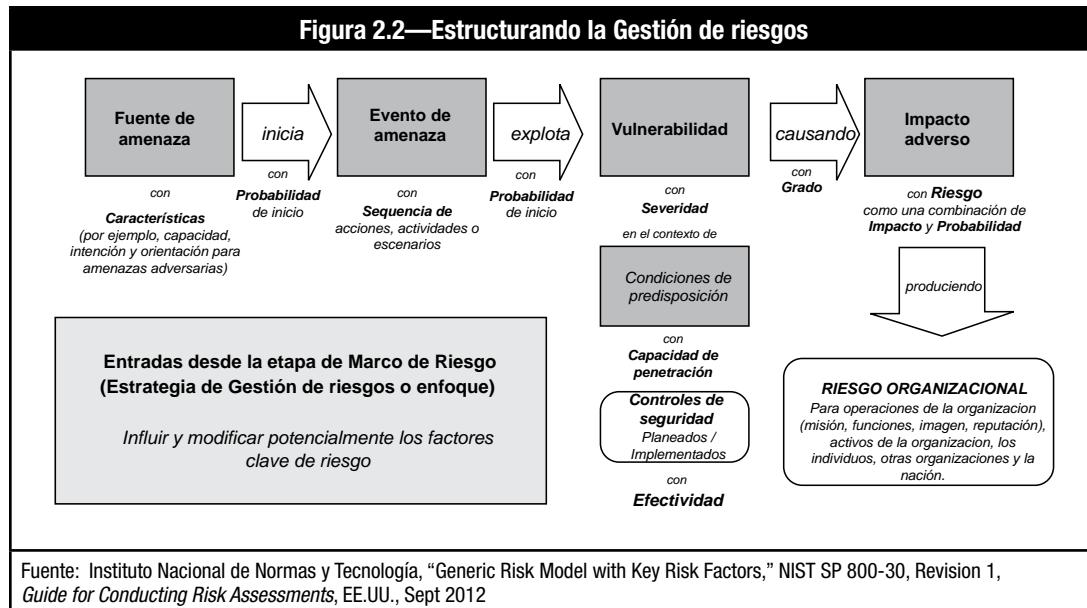
⁵ Anderson, Kent, “A Business Model for Information Security,” *ISACA® Journal*, Vol. 3, 2008

⁶ ISACA, “Top Business/Security Issues Survey Results,” EE.UU., 2011

Hay muchas definiciones posibles de riesgo – algunas generales y otras más técnicas. Adicionalmente, es importante distinguir entre un riesgo y una amenaza. Aunque muchas personas utilizan las palabras amenaza y riesgo como sinónimos, éstas tienen dos significados muy diferentes. Al igual que con cualquier concepto clave, existen variaciones en la definición dependiendo de la organización. Para los propósitos de esta guía, vamos a definir los términos de la siguiente manera:

- **Riesgo**—La combinación de la probabilidad de un evento y sus consecuencias (ISO / IEC 73). El riesgo se mitiga a través del uso de controles o salvaguardas.
- **Amenaza**—Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de una manera que pueda dañarlo. ISO / IEC 13335 define una amenaza en términos generales como una posible causa de un incidente no deseado. Algunas organizaciones hacen una distinción entre una fuente de amenaza y un evento de amenaza, clasificando una fuente de amenaza como el proceso real o el agente que intenta causar daño, y un evento de amenaza como el resultado de la actividad maliciosa de un agente de amenaza.
- **Activos**—Bien de valor tangible o intangible que vale la pena proteger, incluyendo a las personas, la información, la infraestructura, las finanzas y la reputación.
- **Vulnerabilidad**—Debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer el sistema a amenazas adversas provenientes de eventos de amenaza. Aunque gran parte de la ciberseguridad se centra en el diseño, implementación y gestión de controles para mitigar el riesgo, es fundamental para los profesionales de la seguridad entender que el riesgo nunca puede ser eliminado. Más allá de la definición general de riesgos dada anteriormente, existen otros tipos más específicos de riesgo que se aplican a la ciberseguridad.
- **Riesgo inherente**—Nivel de riesgo o exposición sin tener en cuenta las acciones que la dirección ha tomado o puede tomar (por ejemplo, la implementación de los controles).
- **Riesgo residual**—Incluso después de que las salvaguardas hayan sido adoptadas, siempre habrá un riesgo residual, que se define como el riesgo que permanece después de que la dirección haya implementado una respuesta al riesgo.

La **figura 2.2** ilustra un ejemplo de cuántos de estos términos clave entran en juego en el momento de plantear un enfoque de gestión de riesgos.



Marcos y Estándares de Clasificación e Identificación de Riesgos⁷

Los profesionales de la ciberseguridad tienen a su disposición varias fuentes de estándares y marcos de clasificación e identificación de riesgos. La siguiente lista no es completa y existen muchos otros estándares. Sin embargo, esta lista puede ayudar al profesional de la ciberseguridad a escoger un marco o estándar que sea apropiado para su organización. Muchos países e industrias tienen estándares específicos que las organizaciones bajo su jurisdicción deben usar. El uso de un estándar

⁷ ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

reconocido puede proporcionar credibilidad y completitud al programa de evaluación y gestión del riesgo de la organización y ayudar a asegurar que el programa de gestión de riesgos es exhaustivo y minucioso.

ISO 31000:2009 Gestión de riesgos—Principios y pautas

ISO 31000:2009 afirma:

Este estándar internacional recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco cuyo propósito sea integrar el proceso de gestión del riesgo en el gobierno, estrategia y planificación, gestión, políticas de informes, valores y cultura generales de la organización.

Aunque la práctica de la gestión de riesgos haya sido desarrollada a lo largo del tiempo y dentro de muchos sectores para satisfacer diversas necesidades, la adopción de procesos consistentes dentro de un marco completo puede ayudar a asegurar que el riesgo es gestionado con eficacia, de manera eficiente y de forma coherente en toda la organización. La aproximación genérica descrita en este estándar proporciona los principios y las pautas para gestionar cualquier tipo de riesgo de una manera sistemática, transparente y creíble en cualquier ámbito y contexto.⁸

COBIT® 5 para Riesgos

COBIT 5 para Riesgos se describe de la siguiente forma:

COBIT 5 proporciona un marco de referencia exhaustivo que asiste a las empresas a alcanzar sus objetivos para el gobierno y la dirección de la tecnología de información (TI) de la empresa. En pocas palabras, COBIT 5 ayuda a las empresas a crear un valor óptimo a partir de las TI manteniendo un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite que las TI sean gobernadas y gestionadas de manera holística en toda la empresa, de una forma que tenga en cuenta la totalidad de las áreas funcionales del negocio y TI, y que considere además los intereses relacionados con las TI de las partes interesadas internas y externas.

COBIT 5 para Riesgos ... se basa en el marco de COBIT 5 enfocándose en el riesgo y proporcionando una orientación más detallada así como una guía práctica a los profesionales del riesgo y otras partes interesadas en todos los niveles de la empresa.⁹

IEC 31010:2009 Gestión de riesgos—Técnicas de evaluación de riesgos

IEC 31010:2009 afirma:

Las organizaciones de todos los tipos y tamaños se enfrentan a un abanico de riesgos que pueden afectar la consecución de sus objetivos.

Estos objetivos pueden relacionarse con varias de las actividades de la organización, desde iniciativas estratégicas a sus operaciones, procesos y proyectos, y se pueden reflejar en términos sociales, medio ambientales, tecnológicos, en resultados de protección y seguridad, en medidas comerciales, financieras y económicas, así como en un impacto a la reputación social, cultural y política.

Todas las actividades de una organización implican riesgos que deben ser gestionados. El proceso de gestión de riesgos ayuda a la toma de decisiones al tener en cuenta la incertidumbre y la posibilidad de futuros eventos o circunstancias (intencionadas o no) y sus efectos sobre los objetivos acordados.¹⁰

ISO/IEC 27001:2013 Tecnología de la información—Técnicas de seguridad—Gestión de la seguridad de la información

—Requisitos

ISO 27001:2013 afirma:

La organización definirá y aplicará un proceso de evaluación de riesgos para la seguridad de la información que: c) identifique los riesgos para la seguridad de la información:

- 1) aplique el proceso de evaluación de riesgos para la seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información comprendida dentro del alcance del sistema de gestión de la seguridad de la información; y
- 2) identificar los propietarios del riesgo.¹¹

⁸ ISO; ISO 31000:2009 Risk Management—Principles and Guidelines, Suiza, 2009

⁹ ISACA, COBIT 5 para Riesgos, EE.UU., 2013

¹⁰ ISO; IEC 31010:2009 Risk Management—Risk Assessment Techniques, Suiza, 2009

¹¹ ISO; ISO/IEC 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements, Suiza, 2013

ISO/IEC 27005:2011 Information Technology—Security Techniques—Information Security Risk Management

ISO/IEC 27005 afirma:

Este estándar internacional provee pautas para la gestión de los riesgos asociados a la seguridad de la información en una organización, respaldando en particular los requisitos de un Sistema de gestión de la seguridad de la información (SGSI) en base a la ISO/IEC 27001. No obstante, este estándar no proporciona ninguna metodología específica para la gestión del riesgo asociado a la seguridad de la información. Le corresponde a la organización definir su enfoque de gestión de riesgos, dependiendo, por ejemplo, del alcance del SGSI, el contexto de la gestión de riesgos o el sector industrial. Un gran número de metodologías existentes pueden ser usadas dentro del marco descrito en este estándar internacional para implementar los requerimientos de un ISMS.¹²

Publicaciones especiales del NIST

El NIST tiene un amplio abanico de publicaciones disponibles en csrs.nist.gov. En las siguientes secciones, se discuten algunas de estas publicaciones relacionadas con el riesgo de TI

Publicación especial 800-30 Revisión 1 del NIST: Guía para la realización de evaluaciones de riesgo

La Publicación especial 800-30 Revisión 1 del NIST describe la evaluación de riesgo de la siguiente forma:

Las evaluaciones de riesgo son una pieza clave en la gestión efectiva del riesgo y facilita la toma de decisiones en los tres niveles de la jerarquía de la gestión del riesgo, incluyendo el nivel de organización, el nivel de procesos de negocio/misión, y el nivel de sistema de información.

Como la gestión del riesgo es un proceso continuo, las evaluaciones del riesgo son efectuadas a lo largo de todo el ciclo de vida de desarrollo del sistema, desde la adquisición del pre-sistema (p.ej., análisis de la solución material y desarrollo de la tecnología), pasando por la adquisición del sistema (p.ej., desarrollo de la ingeniería/fabricación y producción/despliegue), hasta llegar a su mantenimiento (p.ej., operaciones/soporte).¹³

Publicación especial 800-39 del NIST: Gestionando el riesgo de seguridad de la información:

La publicación especial 800-39 del NIST afirma:

El propósito de la Publicación especial 800-39 es proporcionar orientación para un programa de gestión de riesgos de la seguridad de la información que abarque de forma integrada la totalidad de las operaciones de la organización (p.ej., misión, funciones, imagen y reputación), sus activos, las personas, otras organizaciones y la nación resultantes de la operación y uso de los sistemas de información federales. La Publicación especial 800-39 proporciona un acercamiento estructurado, aunque flexible, a la gestión de riesgos de una forma intencionadamente amplia, con detalles específicos sobre evaluación, respuesta y monitorización del riesgo de forma continua y apoyándose en otros estándares y guías del NIST.¹⁴

Identificación de riesgos (Escenarios de riesgo)¹⁵

Un escenario de riesgo es una descripción de un acontecimiento posible cuya aparición tendrá un impacto incierto sobre la consecución de los objetivos de la empresa, pudiendo ser positivo o negativo. El desarrollo de escenarios de riesgo proporciona un modo de conceptualizar el riesgo que puede ayudar en el proceso de identificación del mismo. Los escenarios también son usados para documentar el riesgo en relación a los objetivos de negocio u operaciones impactados por acontecimientos, haciéndolos útiles como base para la evaluación cuantitativa del riesgo. Cada riesgo identificado debería ser incluido en uno o varios escenarios, y cada escenario debería estar basado en un riesgo identificado.

El desarrollo de los escenarios de riesgos se basa en la descripción de un posible evento de riesgo y la documentación de los factores y áreas que puedan verse afectados por el evento de riesgo. Cada escenario debe estar relacionado con un impacto u objetivo de negocio. Los eventos de riesgo pueden incluir falla del sistema, pérdida de personal clave, robo, interrupciones de redes, fallas de energía, o cualquier otra situación que pudiera afectar la misión y las operaciones del negocio. La clave para desarrollar escenarios efectivos es enfocarse en posibles eventos de riesgo relevantes y reales.

¹² ISO/IEC; ISO/IEC 27005:2011 *Information Technology—Security Techniques—Information Security Risk Management*, Suiza, 2011.

¹³ NIST; *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments*, EE.UU., 2012

¹⁴ NIST; *NIST Special Publication 800-39: Managing Information Security Risk*, EE.UU., 2011

¹⁵ ISACA, *COBIT 5 para Riesgos*, EE.UU., 2013

El desarrollo de escenarios de riesgo basados puramente en la imaginación es un arte que a menudo requiere creatividad, reflexión, asesoramiento y juicio. Los incidentes que hayan ocurrido en el pasado pueden ser usados como base de futuros escenarios, de manera que su desarrollo requiera menos esfuerzo. Los escenarios de riesgo basados en eventos pasados deberán ser totalmente analizados para asegurar que situaciones similares no vuelvan a ocurrir en formas que pudieran haberse evitado. Los escenarios de riesgo se pueden desarrollar desde una perspectiva descendente que esté dirigida por los objetivos del negocio, o desde una perspectiva ascendente originada desde diversas entradas, tal y como se muestra en la **figura 2.3**.



Fuente: ISACA, COBIT 5 para Riesgos, EE.UU., 2013, figura 36

Enfoque de arriba-abajo

Un enfoque arriba-abajo para el desarrollo del escenario se basa en el conocimiento de los objetivos de negocio y en cómo un evento de riesgo afecta a la consecución de dichos objetivos. Bajo este modelo, el profesional de la gestión de riesgos busca el resultado de los eventos identificados por la dirección, que puedan ralentizar la consecución de los objetivos de negocio identificados por la alta dirección. Varios escenarios son desarrollados para permitir a la organización examinar la relación entre el evento de riesgo y el objetivo de negocio, de forma que el impacto del evento de riesgo pueda ser medido. Relacionando directamente el escenario de riesgo al negocio, se puede educar e involucrar la alta dirección en la forma de entender y medir el riesgo.

El enfoque arriba-abajo es apropiado para la gestión del riesgo general de la compañía ya que incluye tanto los eventos de riesgos relacionados con las TI como los que no están relacionados. Un beneficio de este enfoque es que dado que es más general, es más fácil que la gerencia lo acepte, incluso si la gerencia habitualmente no está interesada en las TI. El enfoque arriba-abajo también se encarga de los objetivos que la dirección ha identificado como importantes para ella.

Enfoque abajo-arriba

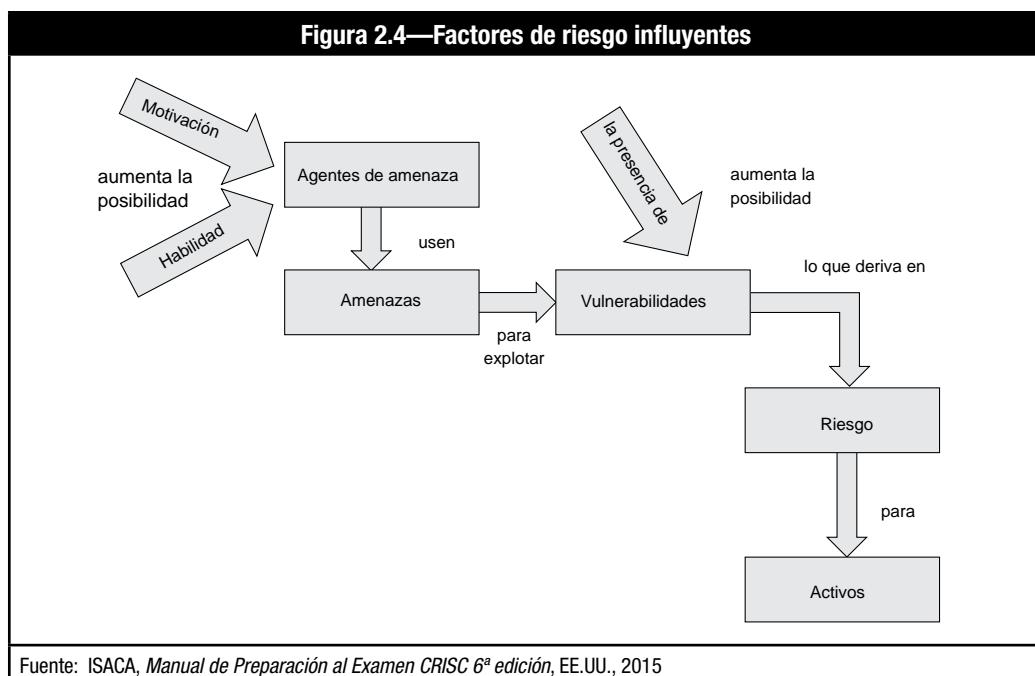
El enfoque abajo-arriba para desarrollar los escenarios de riesgos, se basa en describir los eventos relacionados específicamente con situaciones de Ciberseguridad, típicamente situaciones hipotéticas concebidas por el personal que realiza las tareas en procesos específicos. El profesional de ciberseguridad y el equipo de evaluación comienzan con uno o más escenarios de riesgos genéricos y después los perfeccionan para identificar sus necesidades organizacionales individuales incluyendo la construcción de escenarios complejos que tengan en cuenta eventos coincidentes.

El desarrollo de escenarios usando el enfoque abajo-arriba puede ser una buena forma de identificar escenarios que son altamente dependientes de los trabajos técnicos específicos de un proceso o sistema, y que no serían evidentes a nadie que no esté íntimamente ligado con ese trabajo, pero podría tener importantes consecuencias para la organización. Un inconveniente del desarrollo de escenarios de abajo-arriba es que es puede resultar más difícil mantener el interés de la dirección en escenarios con alta especialización técnica.

PROBABILIDAD E IMPACTO¹⁶

Probabilidad es la medida de la frecuencia en que un evento puede ocurrir, la cual depende de si hay una posible causa para el evento (amenaza) y el grado en el que el particular tipo de evento puede afectar a su objetivo (vulnerabilidad), teniendo en cuenta cualquier control o contramedida que la organización ha implementado para reducir su vulnerabilidad. En el contexto de identificación del riesgo, la probabilidad es utilizada para calcular el riesgo que una organización afronta basándose en el número de eventos que pueden ocurrir en un determinado periodo de tiempo (normalmente en un año).

El riesgo al que se enfrentan las organizaciones es una combinación de amenazas conocidas y desconocidas dirigidas contra sistemas que tienen una combinación de vulnerabilidades conocidas y desconocidas. Una evaluación de vulnerabilidades que no identifica vulnerabilidades no es igual a un sistema invulnerable en sentido absoluto. Sólo significa que el tipo de vulnerabilidades que la evaluación intentaba detectar no fueron detectadas. La falta de vulnerabilidades detectadas puede deberse a su ausencia o puede ser debida a un falso negativo debido a fallos en la configuración de una herramienta o una errónea revisión manual. En el caso de un test de penetración que no ha contado con información previa y que no ha identificado ninguna oportunidad de explotación de un sistema, puede ser que el equipo no tuviera suerte o que tuviera falta de imaginación; en caso de un atacante externo es probable que no ocurra de la misma manera. Incluso si existen vulnerabilidades conocidas en el sistema, el sistema puede ser vulnerable a vulnerabilidades desconocidas, la mayoría de las cuales son descubiertas cada día (algunas de ellas almacenadas o vendidas para futuros usos como exploits de día cero). La probabilidad de un ataque es frecuentemente un componente de factores externos tales como la motivación del atacante, tal y como se muestra en la **figura 2.4**.



Dada una combinación de amenazas y vulnerabilidades desconocidas es difícil, para el profesional de ciberseguridad, proporcionar una completa estimación de la probabilidad de éxito de un ataque. El análisis de vulnerabilidades y los tests de penetración proporcionan al profesional de ciberseguridad valiosa información para estimar esta probabilidad porque:

- Aunque la presencia de una vulnerabilidad no garantiza que exista una amenaza correspondiente, la naturaleza “siempre disponible” de los sistemas de información junto con la rápida velocidad de procesamiento hacen que el ataque a un sistema de información sea mucho más probable que el ataque a un sistema físico.
- Una vulnerabilidad conocida por una herramienta de evaluación también es conocida por los agentes de amenazas, a excepción de los más brillantes de entre ellos que desarrollan ataques que dirigen contra vulnerabilidades comunes.
- La presencia de una o más vulnerabilidades conocidas - a menos que éstas hayan sido previamente identificadas y el riesgo sea aceptado por la organización por una buena razón- sugiere una debilidad en el programa de seguridad global.

¹⁶ ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

Al evaluar una amenaza, los profesionales de ciberseguridad a menudo analizan la probabilidad y el impacto de la amenaza con el fin de clasificarla y priorizarla entre otras amenazas existentes.

En algunos casos en los que se dispone de datos claros y estadísticos, la probabilidad puede ser una cuestión de probabilidad matemática. Esto es cierto en situaciones como eventos climáticos o desastres naturales. Sin embargo, a veces los datos precisos simplemente no están disponibles, como suele ser el caso del análisis de la amenaza de agentes humanos en entornos de ciberseguridad. Algunos factores crean situaciones en los que la probabilidad de ciertas amenazas es más o menos predominante en una organización determinada. Por ejemplo, una conexión a internet predispondrá un sistema a que sus puertos sean explorados. Por lo general, las clasificaciones cualitativas como “Alto, Medio, Bajo” o “Cierto, Muy Probable, Poco Probable, Imposible” se pueden utilizar para clasificar y priorizar las amenazas derivadas de la actividad humana. Sin embargo, cuando se utilizan clasificaciones cualitativas, el paso más importante es definir con rigor el significado de cada categoría y utilizar definiciones de manera consistente a lo largo del proceso de evaluación.

Para cada amenaza identificada, el impacto o magnitud del daño que se espera que resulte también deben ser determinados. El impacto de una amenaza puede tomar muchas formas, pero a menudo tiene una consecuencia operativa de algún tipo, ya sea financiera, reputacional o jurídica. Los impactos pueden ser descritos ya sea cualitativa o cuantitativamente, pero al igual que ocurre con las probabilidades, las clasificaciones cualitativas se suelen usar con más frecuencia en la evaluación de riesgos de ciberseguridad. Asimismo, cada clasificación debe estar bien definida y ser utilizada consistentemente. En ciberseguridad, los impactos también se evalúan en términos de confidencialidad, integridad y disponibilidad.

Los profesionales de la ciberseguridad deben asegurar que la dirección no desarrolla una falsa sensación de ciberseguridad como resultado del análisis de vulnerabilidades y de pruebas de penetración que no hayan conseguido encontrar vulnerabilidades, por el contrario, los dos tipos de tests deben proporcionar un conocimiento de la organización y su postura de seguridad.

ENFOQUES DE RIESGO

Una serie de metodologías están disponibles para medir el riesgo. Diferentes industrias y profesiones han adoptado diversas tácticas basadas en los siguientes criterios:

- Tolerancia al riesgo
- Tamaño y ámbito del entorno en cuestión
- Cantidad de datos disponibles

Es particularmente importante entender la tolerancia al riesgo de una organización al considerar cómo medir el riesgo. Por ejemplo, un enfoque general para la medición del riesgo suele ser suficiente para las organizaciones con tolerancia al riesgo, como las instituciones académicas o las pequeñas empresas. Sin embargo, se requiere de una evaluación de riesgos más rigurosa y de mayor profundidad para entidades con una baja tolerancia al riesgo. Esto es especialmente relevante para cualquier entidad fuertemente regulada, como una institución financiera o un sistema de reserva de vuelos, donde cualquier momento de indisponibilidad tendría un impacto operacional significativo.

ENFOQUES DE RIESGOS DE CIBERSEGURIDAD

Hay tres enfoques diferentes para la implementación de la ciberseguridad. Cada enfoque se describe brevemente a continuación.

- **Ad hoc** —Un enfoque ad hoc simplemente implementa la seguridad sin una lógica o criterio particular. Las implementaciones ad hoc pueden ser impulsadas por el departamento de marketing destinado a líneas de venta, o pueden reflejar un nivel de experiencia en la materia, conocimiento o capacitación que es insuficiente en el diseño y aplicación de salvaguardas.
- **Basado en cumplimientos** —También conocido como seguridad basada en estándares, este enfoque depende del cumplimiento de reglamentos o normas para determinar las implementaciones de seguridad. Los controles se aplican con independencia de su aplicabilidad o necesidad, lo cual se traduce en muchas ocasiones en una actitud mecánica de la seguridad donde priman las “checklist de controles”.
- **Basado en riesgos** —La seguridad basada en riesgos depende de la identificación del riesgo único al que una organización en particular se enfrenta y del diseño e implementación de los controles de seguridad que son necesarios para hacer frente a ese riesgo por encima y más allá de la tolerancia al riesgo y de las necesidades de negocio de dicha organización. El enfoque basado en riesgos se basa normalmente en el uso de escenarios.

En realidad, la mayoría de las organizaciones con programas de seguridad maduros utilizan una combinación de enfoques basados en riesgos y cumplimiento. De hecho, la mayoría de las normas o reglamentos como ISO 27001, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), la Ley Sarbanes-Oxley (SOX) o la Ley de Portabilidad y Responsabilidad de Seguro de Salud (HIPAA) requieren evaluaciones del riesgo para impulsar la implementación particular de los controles requeridos.

RIESGO DE TERCEROS

El control de la ciberseguridad puede ser más difícil cuando hay terceros involucrados, especialmente cuando diferentes entidades tienen diferentes culturas de seguridad y diferentes tolerancias al riesgo. Ninguna organización está aislada, y la información debe ser compartida con otros individuos u organizaciones, a menudo denominados terceros. Es importante entender los riesgos de terceros, tales como el intercambio de información y el acceso a la red, ya que esto se refiere a la ciberseguridad.

La externalización (outsourcing) es común tanto a nivel nacional como internacional, ya que las compañías se concentran en sus competencias fundamentales y en formas de recortar gastos. Desde el punto de vista de seguridad de la información, estos acuerdos pueden presentar riesgos que pueden ser difíciles de cuantificar y potencialmente difíciles de mitigar. Casi siempre, tanto los recursos como las habilidades de las funciones que se contratan a proveedores externos no se encuentran dentro del control de la organización, lo cual puede representar un riesgo. Los proveedores pueden operar en base a diferentes criterios y puede ser difícil controlarlos. La estrategia de seguridad debe ser especialmente cuidadosa cuando considere externalizar servicios de seguridad, asegurando que no representan un punto crítico de fallo o que existe un plan de respaldo adecuado en el escenario de una falla del proveedor de servicio.¹⁷

El riesgo que supone la externalización también puede materializarse debido a fusiones y adquisiciones. Normalmente, las diferencias significativas en la cultura, los sistemas, la tecnología y las operaciones entre las partes presentan numerosos retos de seguridad que deben identificarse y abordarse. En estas situaciones, la seguridad se suele considerar a posteriori, ello supone un reto para el gerente de seguridad que debe hacerse un hueco en estas actividades y evaluar los riesgos para que sean tenidos en cuenta por la gerencia.¹⁸

¹⁷ ISACA, *Manual de Preparación al Examen CISM 15^a edición*, EE.UU., 2016

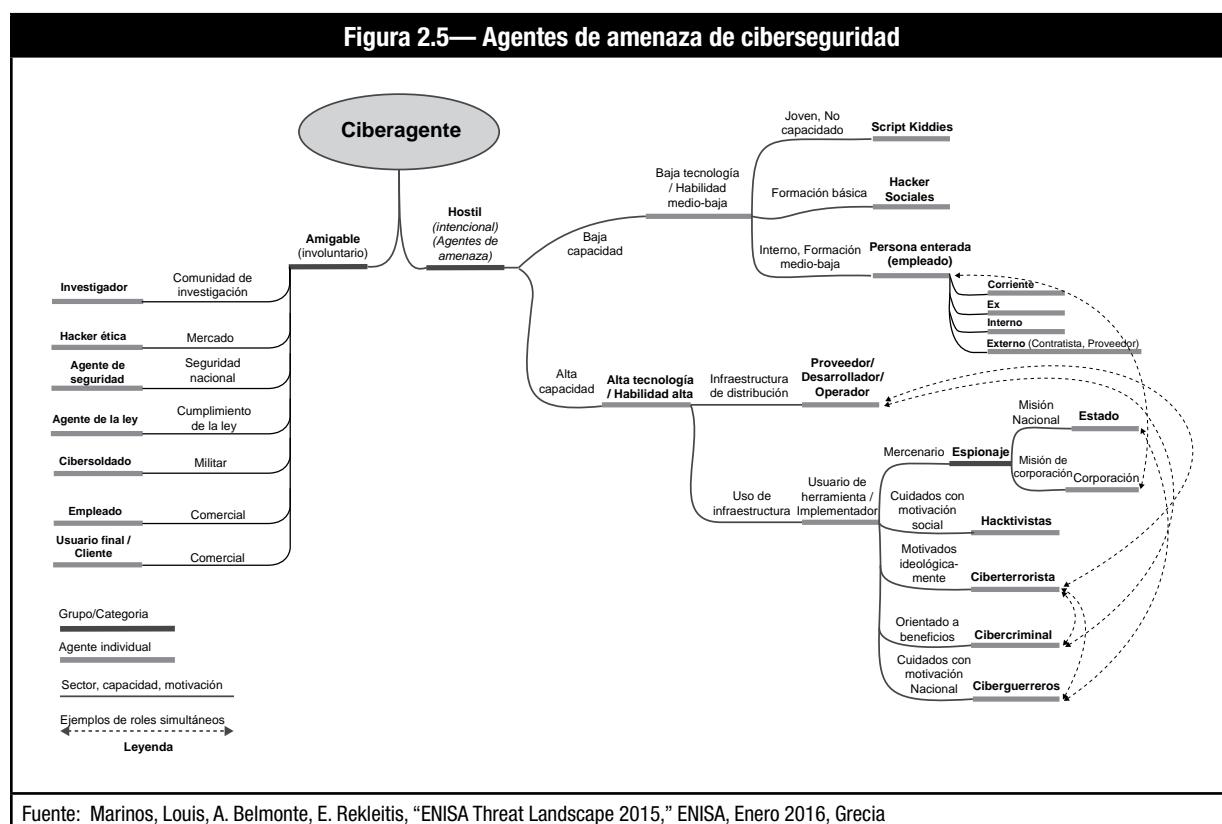
¹⁸ *Ibid.*

TEMA 2—TIPOS Y VECTORES DE ATAQUE COMUNES

Los vectores y las metodologías de ataque no dejan de evolucionar, lo que representa una amenaza significativa para el cliente. Aunque algunos ataques se hacen al azar sin ningún objetivo particular en mente, los ataques dirigidos se llevan a cabo contra destinatarios que se han sido investigados e identificados como útiles por los atacantes. Los ataques de phishing a menudo se dirigen a los destinatarios que tienen acceso a datos o sistemas a los que el atacante desea obtener acceso. En otros casos, el malware se despliega en ataques generalizados con la esperanza de que llegará a tantos sistemas vulnerables como sea posible, aunque estas situaciones no se consideran ciberataques. Un número importante de agentes de amenaza y patrones de ataque ha aparecido en el actual panorama de amenazas. Es esencial para los profesionales de la ciberseguridad poder identificar estas amenazas con el fin de gestionarlas adecuadamente.

AGENTES DE AMENAZA

La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) ha identificado los agentes de amenaza que existen en el panorama actual, tal y como se muestra en **figura 2.5**.



Los agentes de amenaza comunes incluyen los siguientes elementos:

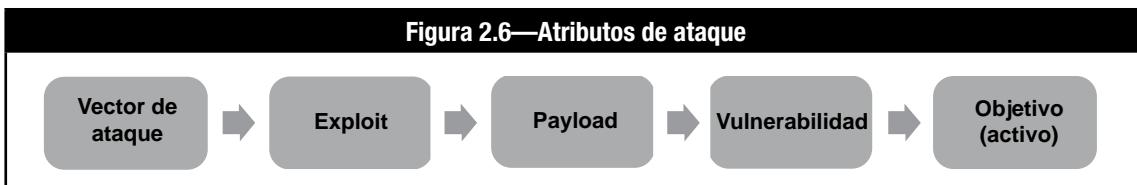
- **Corporaciones**—Se tiene constancia que las corporaciones han roto los perímetros de seguridad y realizado acciones maliciosas contra otras organizaciones para obtener ventajas competitivas.
- **Cibercriminales**—Motivados por el afán de lucro, estos individuos están involucrados en transacciones financieras fraudulentas.
- **Ciber terroristas**—Se caracterizan por su disposición a usar la violencia para lograr sus objetivos, con frecuencia se dirigen a infraestructuras críticas y grupos gubernamentales.
- **Ciberguerreros**—A menudo comparados con hacktivistas, los ciberguerreros, también conocidos como cibercombatientes, son ciudadanos motivados a nivel nacional que pueden actuar en nombre de un partido político o en contra de otro partido político que los amenaza.

- **Empleados**—A pesar de que suelen tener métodos y herramientas de bajo nivel tecnológico, los empleados insatisfechos ya sean antiguos o actuales representan un riesgo de ciberseguridad evidente. Todos estos ataques son adversos, pero algunos no están relacionados con los ciberataques APT.
- **Hacktivistas**—A pesar de que a menudo actúan de forma independiente, los hackers con motivaciones políticas pueden tener como objetivo personas u organizaciones específicas para lograr diversos fines ideológicos.
- **Estados nacionales**—Los estados nacionales a menudo se focalizan en gobiernos y entidades privadas para obtener inteligencia o llevar a cabo otras actividades destructivas. Poseen un alto nivel de sofisticación.
- **Hackers Sociales**—Con habilidades en ingeniería social, estos atacantes están frecuentemente implicados en el ciberacoso, robo de identidad y la recolección de otra información confidencial o de credenciales.
- **Script Kiddies**—Los script kiddies son personas jóvenes que están aprendiendo a hackear; suelen trabajar solos o en grupo y están involucrados principalmente en inyecciones de código y los ataques distribuidos de denegación de servicio (DDoS).

ATRIBUTOS DE ATAQUE

Mientras que el riesgo se mide por su daño potencial, un **ataque** es la ocurrencia real de una amenaza. Más específicamente, un ataque es una actividad realizada por un agente de amenaza (o adversario) contra un activo. Desde el punto de vista de un atacante, el activo es un **objetivo**, y el camino o ruta utilizada para acceder a la meta (activo) se conoce como un **vector de ataque**. Hay dos tipos de vectores de ataque: de entrada (Ingress) y de salida (Egress) (también conocido como exfiltración de datos). Mientras que la mayoría de los análisis de ataque se concentran en los de entrada, o intrusión, a los sistemas, algunos ataques están diseñados para eliminar los datos de los sistemas y redes (p ej, empleados que roban datos). Por tanto, es importante tener en cuenta ambos tipos de vectores de ataque.

El atacante debe enfrentarse a cualquiera de los controles implantados y/o utilizar un código para explotar debilidades (**exploit**) para aprovechar una vulnerabilidad. Otro atributo de un ataque es el **mecanismo de ataque**, o el método utilizado para entregar el exploit. A menos que el atacante esté llevando a cabo personalmente el ataque, el mecanismo de ataque puede implicar un exploit, que entrega el payload al objetivo. Un ejemplo puede ser un archivo pdf malicioso generado por un atacante y entregado por correo electrónico. Los atributos de un ataque se muestran en la **figura 2.6**.



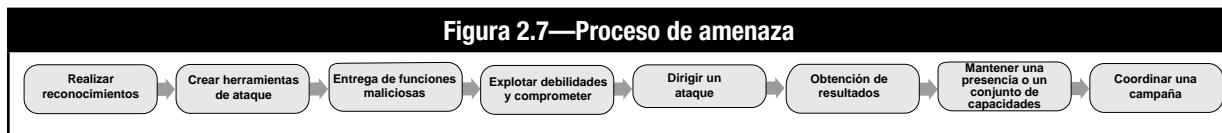
El análisis detallado de los ciberataques requiere de una gran experiencia tanto técnica como de a materia tratada, y es una parte importante de la ciberseguridad. Cada uno de los atributos de ataque (vector de ataque, exploit, payload, vulnerabilidad, objetivo) proporciona puntos únicos donde poder ubicar los controles para prevenir o detectar el ataque. También es importante entender cada uno de estos atributos durante el análisis y la investigación de un ataque real. Por ejemplo, el exploit utilizado para entregar el payload, a menudo deja artefactos o evidencias que pueden ser utilizados por los analistas e investigadores técnicos para entender el ataque y posibilitar la identificación de los autores. El análisis de la ruta de exfiltración de datos puede identificar oportunidades adicionales para prevenir o detectar la eliminación de los datos u obtener evidencias, incluso si el ataque fue capaz de conseguir su objetivo.

Los ataques pueden ser analizados y clasificados en función de su tipo y de los patrones de uso. A partir de estas características, es posible hacer generalizaciones que faciliten un mejor diseño y mejores controles. Hay dos grandes categorías de eventos de amenaza: adversos y no adversos. Un **evento de amenaza adverso** lo realiza un agente de amenaza humano (o adversario), mientras que un **evento de amenaza no adverso** es normalmente el resultado de un error, un mal funcionamiento o un percance de cualquier tipo.¹⁹

¹⁹ MITRE, Common Attack Pattern Enumeration and Classification (CAPEC), Febrero 2014, <http://capec.mitre.org>

PROCESO DE ATAQUE GENERALIZADO

Mientras que cada ataque es diferente, la mayoría de los eventos de amenaza adversos siguen un proceso común, tal y como se muestra en la **figura 2.7** y se describe a continuación.



- Realizar reconocimientos:** El adversario recoge información usando una variedad de técnicas, pasivas o activas, las cuales pueden incluir:
 - Pasivo:
 - Escuchar el tráfico de red
 - Descubrir información de la organización a partir de fuentes de información libres (Grupos de noticias; comunicaciones de empresa relativas a diseños de IT o a su arquitectura de TI)
 - Google Hacking
 - Activo:
 - Escanear el perímetro de la red
 - Ingeniería social (Llamadas falsas, Phishing de bajo nivel)
- Crear herramientas de ataque:** El adversario diseña las herramientas necesarias para llevar a cabo un ataque en el futuro, que incluye:
 - Phishing o ataques selectivos de phishing
 - Generar páginas web falsas o certificados falsos
 - Crear y operar organizaciones falsas y posicionarlas en la cadena de suministro para inyectar componentes maliciosos
- Entrega de funciones maliciosas:** El adversario inserta o instala todo aquello que sea necesario para llevar a cabo el ataque que puede incluir lo siguiente:
 - La introducción de malware en los sistemas de información de la organización
 - La colocación de individuos infiltrados en posiciones privilegiadas dentro de la organización
 - La instalación de sniffers o dispositivos de escaneo en redes y sistemas objetivo
 - Introducción de hardware o componentes críticos manipulados en los sistemas de organización o en las cadenas de suministro
- Explotar debilidades y comprometer:** El adversario se aprovecha de la información y los sistemas con el fin de comprometerlos, lo que incluye:
 - Split tunneling o conseguir acceso físico a las instalaciones de la organización
 - La filtración de datos o información sensible
 - Explotación de sistemas “multi tenant” (ej. Multiples clientes en recursos o plataformas compartidos) en un entorno de nube pública (ej. Atacando puntos de acceso públicos; programas de interfaces de aplicación [API's])
 - Lanzando exploits de día cero
- Dirigir un ataque:** El adversario coordina las herramientas de ataque o realiza actividades que interfieran con las funciones de la organización. Los métodos potenciales de ataque incluyen:
 - Intercepción de comunicaciones o ataques de interferencias inalámbricas
 - Ataques de denegación de servicio (DoS) o ataques distribuidos de denegación de servicio (DDoS)
 - Interferencias a distancia o ataques físicos a las instalaciones o infraestructuras de la organización
 - Secuestro de sesión o ataque de “hombre en el medio”
- Obtención de resultados:** El adversario causa un impacto adverso, que puede incluir:
 - Obtener acceso no autorizado a sistemas y/o información sensible
 - La degradación de los servicios o capacidades de la organización
 - Crear, corromper o borrar datos críticos
 - Modificar el flujo de control de los sistemas de información (ej. Sistemas de control industrial, sistemas de control de supervisión y adquisición de datos (SCADA))
- Mantener una presencia o un conjunto de capacidades:** El adversario continua la explotación y el compromiso del sistema usando las siguientes técnicas:
 - Ofuscando las acciones de adversario o interfiriendo con los sistemas de detección de intrusión (IDS)
 - Adaptando los ciberataques en base a las medidas de seguridad de la organización

8. **Coordinar una campaña:** El adversario coordina una campaña contra la organización que puede implicar las siguientes medidas:
- Ataques de múltiples etapas
 - Ataques internos y externos
 - Ataques generalizados y adaptables

EVENTOS DE AMENAZA NO ADEVEROSOS

Aunque la mayoría de los ataques son el resultado de un esfuerzo coordinado, hay otros eventos que pueden plantear varios tipos de riesgos para una organización y pueden ayudar a un adversario en un posible ciber-ataque. Algunos de los eventos de amenazas no adevversos más comunes son:

- Manipulación inapropiada de la información crítica o sensible por parte de usuarios autorizados
- Configuración incorrecta de privilegios
- Incendio, inundación, huracán, tormentas o terremotos en las instalaciones primarias o en las de respaldo
- Introducción de vulnerabilidades en productos de software
- Errores genéricos de disco u otros problemas causados por la antigüedad de los equipos

MALWARE, RANSOMWARE Y TIPOS DE ATAQUE²⁰

El **malware**, también conocido como código malicioso, es el software diseñado para obtener acceso a los sistemas informáticos objetivo, robar información o interrumpir las operaciones computacionales. Hay varios tipos de malware, siendo los más importantes los virus informáticos, gusanos y troyanos, los cuales se diferencian por la forma en que operan o se extienden.

Por ejemplo, el gusano informático conocido como Stuxnet destaca por el potencial de su malware para interrumpir los sistemas de control de supervisión y de adquisición de datos (SCADA) y los controladores lógicos programables (PLC), normalmente utilizados para automatizar los procesos mecánicos en las fábricas o plantas de energía. Descubierto en 2010, Stuxnet se utilizó para comprometer los sistemas y el software del programa nuclear Irání. Tiene tres componentes:

1. Un **gusano** que lleva a cabo las rutinas relacionadas con el payload
2. Un **fichero de enlace** que propaga copias del gusano
3. Un **rootkit** que oculta los procesos maliciosos para evitar ser detectado

Otros tipos comunes de malware incluyen:

- **Virus**—Un virus informático es un trozo de código que puede replicarse a sí mismo y propagarse de un ordenador a otro. Se requiere manipularlo o ejecutarlo para replicarse y/o causar daños.
- **Gusano de red**—Una variante del virus informático, que es básicamente una pieza de código auto-replicante diseñado para propagarse a través de las redes. No se requiere intervención o ejecución para que se replique.
- **Troyanos**—Una pieza de malware que obtiene acceso a un sistema objetivo al esconderse dentro de una aplicación real. Los troyanos suelen dividirse en categorías que reflejan sus propósitos.
 - Un troyano móvil común es Hummer, un tipo de malware de Android. En los 6 primeros meses del 2016, casi 1.4 millones de dispositivos fueron infectados diariamente por Hummer. El malware utiliza uno de los 18 métodos de rooting para ganar acceso privilegiado de administración al dispositivo. A continuación, muestra publicidad e instala juegos y aplicaciones pornográficas en el dispositivo móvil.²¹
- **Red de computadoras infectadas con código malicioso (Botnet)**—Derivado del término “robot network”, se trata de una red numerosa, automatizada y distribuida de ordenadores previamente comprometidos que pueden ser controlados simultáneamente para lanzar ataques a gran escala tales como una denegación de servicio (DoS).

Existe otra serie de términos que también se utilizan para describir los tipos más específicos de malware, caracterizados por sus propósitos. Estos incluyen:

- **Software espía (spyware)**—Una clase de malware que recopila información sobre una persona u organización sin el conocimiento de dicha persona u organización.
- **Sistemas de publicidad (adware)**—Diseñado para mostrar anuncios (generalmente no deseados) a los usuarios.

²⁰ ISACA, *Amenazas persistentes avanzadas: Cómo gestionar el riesgo para su negocio*, EE.UU., 2013

²¹ Bisson, David; “Hummer Malware the No. 1 Mobile Trojan in the World,” *Tripwire*, 1 Julio 2016, www.tripwire.com/state-of-security/latest-security-news/hummer-malware-the-1-mobile-trojan-in-the-world

- **Software maligno de petición de rescate (Ransomware)**—También conocido como “código rehén” (del inglés “hostage code”), se trata de un tipo de malware de extorsión que bloquea o cifra los datos o funciones y exige un pago para desbloquearlos. Hay varios tipos disponibles para cada sistema operativo. Ataques recientes de Ramsonware incluyen:
 - **GhostCrypt**—Mediante el uso del cifrado AES, GhostCrypt cifra los datos del dispositivo infectado para obtener Bitcoins de la víctima. Cuando el Ramsonware cifra una pieza de información, incluye el apéndice .Z81928819. GhostCrypt también genera un archivo “leeme.txt” (READ_THIS_FILE.txt) como recordatorio del rescate que debe pagarse.²²
 - **SNSLocker**—Utilizando cifrado AES y añadiendo una cadena RSNlocked al final de los datos afectados, este Ransomware cifra datos y pide un rescate de 300 \$ (pagables en Bitcoin) para proporcionar una solución de descifrado.²³
- **Software de registro de teclado (Keylogger)**—Una clase de malware que registra de forma silenciosa las pulsaciones de teclado de los usuarios y, en algunos casos, el contenido de la pantalla.
- **Rootkit**—Una clase de malware que oculta la existencia de otro tipo de malware mediante la modificación del sistema operativo subyacente.

OTROS TIPOS DE ATAQUE

Además del malware y del ransomware, hay muchos otros tipos de ataques. Algunos de los patrones de ataque más comunes son los siguientes:

- **Amenazas persistentes avanzadas (APT)**—Ataques complejos y coordinados dirigidos contra una entidad u organización específica. Requieren una cantidad sustancial de investigación y tiempo, a menudo les lleva meses o incluso años para su plena ejecución. APT es un término que refleja el nivel de complejidad; sin embargo, no puede probarse si un ataque particular fue una APT o no. Tras haber descubierto un ataque, determinado su nivel de complejidad e investigado la cantidad de tiempo y recursos dedicados al ataque, se puede determinar si el ataque fue una APT o no.
- **Puerta trasera**—Medio a través del cual se recupera el acceso a un sistema comprometido mediante la instalación de software o la configuración de software existente que permita el acceso remoto en las condiciones definidas por el atacante.
- **Ataque de fuerza bruta**—Ataque mediante el cual se intentan todas las combinaciones posibles de contraseñas o claves de cifrado hasta dar con la correcta.
- **Desbordamiento de búfer**—Ocurre cuando un programa o proceso intenta almacenar en una memoria intermedia (área de almacenamiento temporal de datos) más datos de los que se tenía la intención de contener. Puesto que los buffers son creados para contener una cantidad limitada de datos, la información adicional que tiene que ir a alguna parte—puede desbordar hacia buffers adyacentes, corrompiendo o sobrescribiendo los datos válidos contenidos. Aunque puede ocurrir accidentalmente por error de programación, el desbordamiento de búfer es un tipo cada vez más común de ataque a la seguridad en la integridad de los datos. En los ataques de desbordamiento de buffer, los datos adicionales pueden contener códigos de tipo de ataque a la seguridad en la integridad de los datos.
- **Cross-site scripting (XSS)**—Tipo de inyección en el cual scripts (secuencias de comandos) maliciosos se inyectan en los sitios web benignos y de confianza. Los ataques de Cross-site scripting (XSS) ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Los defectos que permiten que estos ataques tengan éxito son bastante generalizados y se producen en cualquier lugar de una aplicación web que utiliza la entrada de un usuario dentro de la salida generada sin validar o codificarlo.
- **Ataque de denegación de servicio (DoS)**—Asalto a un servicio desde un único origen que lo desborda con un número tan alto de solicitudes que supera sus capacidades, con el resultado de una parada total del servicio o una operación a una velocidad significativamente reducida.
- **Ataque de “hombre en el medio”**—Estrategia de ataque en la que el atacante intercepta el flujo de comunicación entre dos partes del sistema víctima y luego reemplaza el tráfico entre los dos componentes con el propio, asumiendo con el tiempo el control de la comunicación.
- **Ingeniería social**—Cualquier intento de explotar las vulnerabilidades sociales para obtener acceso a la información y/o sistemas. Se trata de una “estafa” que engaña a otros para divulgar información o abrir software o programas maliciosos.
- **Phishing**—Un tipo de ataque vía correo electrónico (e-mail) que intenta convencer a un usuario de que el emisor es genuino, pero con la intención de obtener información para su uso en ingeniería social.
- **Spear phishing / Phishing de Ingeniería Social**—Ataque de phishing, donde se utilizan técnicas de ingeniería social para hacerse pasar por un ente fiable para obtener información importante, como contraseñas de la víctima.
- **Spoofing**—Falsificación de la dirección de envío de una transmisión con el fin de ganar acceso ilegalmente a un sistema seguro.

²² Tripwire, “May 2016: The Month in Ransomware,” Tripwire, 6 Junio 2016, www.tripwire.com/state-of-security/security-data-protection/may-2016-the-month-in-ransomware

²³ Ibid. ²⁴ OWASP, SQL Injection, www.owasp.org/index.php/SQL_Injection

- **Structure Query Language (SQL) injection**—De acuerdo a OWASP²⁴ Un ataque de SQL Injection consiste en la inserción o inyección de una consulta SQL a través de los datos de entrada desde el cliente a la aplicación. Un exploit de inyección de código SQL exitoso, puede leer datos sensibles de la base de datos, modificar los datos de la base de datos (insertar/actualizar/eliminar), ejecutar operaciones de administración en la base de datos (como apagar la DBMS), recuperar el contenido de un fichero concreto presente en el sistema de ficheros de la DBMS y en algunos casos lanzar comandos al sistema operativo. Los ataques de inyección SQL son un tipo de ataques de inyección en los que comandos SQL son injectados en entradas planas de datos para producir la ejecución de comandos SQL predefinidos.
- **Exploit de día cero**—Vulnerabilidad que se explota antes de que el creador/proveedor del software sea consciente de su existencia.

TEMA 3—POLÍTICAS

PROPÓSITO DE LAS POLÍTICAS

Las políticas de seguridad de la información son un elemento primordial de la ciberseguridad y el gobierno de seguridad general. Especifican los requisitos y definen las funciones y responsabilidades de todos los miembros de la organización, junto con los comportamientos esperados en diversas situaciones. Por lo tanto, deben crearse correctamente, aceptarse y validarse por la junta directiva y la alta dirección antes de ser comunicadas en toda la organización. Durante este proceso, puede haber ocasiones en las que otros documentos deben ser creados para hacer frente a situaciones únicas separadas de la mayor parte de la organización. Esto puede ser necesario cuando una parte de la organización tiene un requisito regulatorio específico para proteger ciertos tipos de información.

CICLO DE VIDA DE LAS POLÍTICAS

Además de un marco de política, otro aspecto importante de las políticas de seguridad de la información es su ciclo de vida de desarrollo, mantenimiento, aprobación y excepción.

Cada documento de cumplimiento debe tener un proceso formal para ser creado, revisado, actualizado y aprobado por lo menos una vez al año. Además, puede haber la necesidad legítima de una excepción a la política; por lo tanto, es necesario un proceso claro de cómo una excepción estará aprobada por la alta dirección y supervisada durante el ciclo de vida.

DIRECTRICES

Existe un gran número de atributos de políticas recomendables que deben de tenerse en consideración:

- Las políticas de seguridad deben ser una articulación de una estrategia de seguridad de la información bien definida que capta la intención, las expectativas y la dirección de la gestión.
- Las políticas deben ser claras y de fácil comprensión para todas las partes interesadas.
- Las políticas deben ser cortas y concisas, escritas en un lenguaje sencillo.

La mayoría de las organizaciones deben crear políticas de seguridad antes de desarrollar una estrategia de seguridad. Aunque muchas organizaciones tienden a seguir un enfoque ad hoc para el desarrollo de la estrategia de seguridad, también hay casos, especialmente en las organizaciones más pequeñas, donde se han desarrollado prácticas efectivas que pueden no estar reflejadas en las políticas escritas. Las prácticas vigentes que tratan en forma adecuada los requerimientos de la seguridad pueden ser de mucha utilidad para establecer el desarrollo de políticas y estándares. Este enfoque reduce al mínimo las interrupciones de organización, las comunicaciones de las nuevas políticas y la resistencia a las limitaciones nuevas o poco conocidas.

DOCUMENTOS DE CUMPLIMIENTO Y MARCOS DE POLÍTICA

Los **documentos de cumplimiento**, tales como las políticas, normas y procedimientos, esbozan las acciones que se requieren o prohíben. Las violaciones pueden estar sujetas a acciones disciplinarias.

Algunos tipos de documentos de cumplimiento comunes se muestran en la **figura 2.8**.

Figura 2.8—Tipos de documentos de cumplimiento	
Tipo	Descripción
Políticas	Comunican actividades y conductas requeridas y prohibidas.
Normas	Interpreta políticas en situaciones específicas
Procedimientos	Proporcionan detalles sobre cómo cumplir con las políticas y normas
Directrices	Proporciona una guía general en asuntos tales como “qué hacer en situaciones específicas”. Estos no son requerimientos que deban de cumplirse, pero son muy recomendados.

Algunas organizaciones no pueden implantar todos estos tipos de documentos. Por ejemplo, las organizaciones más pequeñas pueden simplemente tener políticas y procedimientos; otros pueden tener las políticas, normas y procedimientos, pero no directrices.

TIPOS DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El número y el tipo de políticas que la organización opte por aplicar varían en función del tamaño, la cultura, el riesgo, los requisitos regulatorios y la complejidad de las operaciones de dicha organización. Sin embargo, a continuación se listan algunos ejemplos comunes y tipo de información que deben contener.

Política general de seguridad de la información

La mayoría de las organizaciones tiene una política de seguridad de la información a alto nivel que puede mantenerse como una política única o bien servir como base para otros documentos de cumplimiento. Para las grandes empresas, es una práctica común subdividir las políticas por tema para abordar toda la seguridad de la información. Un ejemplo de dicha subdivisión se muestra en la **figura 2.9**.



Cada una de estas políticas requiere la participación del responsable de seguridad de la información. A continuación se muestran ejemplos de un posible alcance relevante para la seguridad de la información se muestran a continuación:²⁵

- Continuidad del negocio y Recuperación ante desastres:
 - Análisis del impacto en el negocio (BIA)
 - Planes de contingencia para el negocio con recuperación confiable
 - Requerimientos de recuperación para sistemas críticos
 - Umbrales definidos y desencadenantes para contingencias y escalado
 - Plan de recuperación de desastre (DRP)
 - Formación y pruebas
- Gestión de activos:
 - Clasificación de los datos y propiedad
 - Clasificación de los sistemas y propiedad
 - Utilización de recursos y priorización
 - Gestión del ciclo de vida de los activos
 - Protección de activos
- Reglas de conducta:
 - Uso aceptable y comportamiento en el trabajo, incluyendo privacidad, internet/email, dispositivos móviles, BYOD, etc.
 - Uso aceptable y comportamiento fuera del trabajo, incluyendo las redes sociales, blogs

²⁵ ISACA, *COBIT® 5 para Seguridad de la Información*, EE.UU., 2013

²⁶ Ibid.

- Adquisición / Desarrollo / Mantenimiento
 - Seguridad de la información a lo largo del ciclo de vida, definición de requisitos y procesos de compras y adquisiciones
 - Prácticas de codificación segura
 - Integración de la seguridad de la información en la gestión de cambios y en la gestión de la configuración
- Gestión de proveedores:
 - Gestión de contratos
- Comunicaciones y Operaciones:
 - Arquitectura de seguridad de la información TI y diseño de aplicaciones
 - Acuerdos de nivel de servicio
- Cumplimiento:
 - Proceso de evaluación del cumplimiento de la seguridad de la información TI
 - Desarrollo de métricas
 - Repositorios de evaluación
- Gestión de riesgos:
 - Plan de gestión de riesgos de la organización
 - Perfil de riesgo de información

La publicación y la duración de las políticas de seguridad de la información varían mucho de una empresa a otra. Algunas empresas consideran suficiente una política de seguridad de la información compuesta por una visión general de una página. En estos casos, la política podría considerarse un resumen de directivas, y debe describir claramente los enlaces a otras políticas específicas. En otras empresas, la política de seguridad de la información está completamente desarrollada, y contiene casi toda la orientación detallada necesaria para poner en práctica los principios. Es importante entender lo que las partes interesadas esperan en términos de cobertura y adaptación a esta expectativa.

Independientemente de su tamaño o grado de detalle, la política de seguridad de la información necesita un alcance claramente definido. Esto implica:

- La definición de lo que la empresa entiende por seguridad de la información
- Las responsabilidades asociadas con la seguridad de la información
- La visión de seguridad de la información, acompañada de objetivos adecuados, métricas y el motivo de cómo la visión es apoyada por la cultura y la conciencia de la seguridad de la información
- Explicación de cómo la política de seguridad de la información se alinea con otras políticas de alto nivel
- Elaboración de información específica sobre los temas de seguridad, tales como gestión de datos, evaluación de riesgos de la información y cumplimiento de las obligaciones legales, reglamentarias y contractuales

Además de los elementos discutidos anteriormente, una política puede afectar potencialmente el presupuesto del ciclo de vida de seguridad y gestión de costes. Planes estratégicos de seguridad de información y gestión de la cartera se pueden añadir también.

La política debe ser comunicada de forma activa a toda la empresa y distribuida a todos los empleados, contratistas, empleados temporales y otros proveedores. Las partes interesadas deben saber los principios de información, los requisitos de alto nivel, y los roles y responsabilidades de seguridad de la información. La responsabilidad de la actualización y revalidación de la política de seguridad de la información corresponde a la función de ciberseguridad.

Otras políticas o procedimientos de seguridad posibles incluyen el control de acceso, la información del personal y de los incidentes de seguridad.

Política de control de acceso

La política de control de acceso proporciona un acceso adecuado a los grupos de interés internos y externos para lograr los objetivos de negocio. Esto puede ser medido por indicadores tales como, entre otros:

- Número de violaciones de acceso que excedan la cantidad permitida
- La cantidad de interrupciones de trabajo debido a derechos de acceso insuficientes
- Número de incidentes de segregación de funciones o resultados de auditoría

Además, la política de control de acceso debe garantizar que el acceso en situaciones de emergencia es apropiadamente permitido y revocado de manera oportuna. Las métricas relacionadas con este objetivo incluyen el número de solicitudes de acceso de emergencia y el número de cuentas de emergencia activas que han superado los límites de tiempo de aprobación.

La política de control de acceso debe cubrir los siguientes temas, entre otros:

- Ciclo de vida de provisión de acceso físico y lógico
- Menor privilegio/ privilegio basado en la necesidad de conocer
- Segregación de funciones
- Acceso de emergencia

Esta política es para todas las unidades de negocio correspondientes, proveedores y terceros. Las actualizaciones y revalidaciones deben involucrar a los recursos humanos, los datos y los propietarios de sistemas, la seguridad de la información y la alta dirección. Una política nueva o actualizada debe ser distribuida a todas las unidades de negocio correspondientes, a proveedores y a terceros.

Política de seguridad de la información del personal

El objetivo de la política de seguridad de la información del personal incluye, pero no se limita a, los siguientes objetivos:

- Ejecutar verificaciones de antecedentes regulares de todos los empleados y personas en posiciones clave. Esta meta puede medirse contando el número de controles de antecedentes completos para el personal clave. Esto puede ser amplificado con el número de verificaciones de antecedentes de personal renovado en base a una frecuencia predeterminada.
- Adquirir información sobre el personal clave en puestos de seguridad de la información. Esto puede ser controlado contando el número de personal en puestos clave que no han rotado de acuerdo a una frecuencia predefinida.
- Desarrollar un plan de sucesión para todos los puestos clave en seguridad de la información. Un punto de partida es una lista de todas las posiciones críticas de seguridad de la información que carecen de personal de respaldo.
- Definir e implementar procedimientos adecuados para la terminación. Esto debe incluir detalles sobre la revocación de los privilegios el acceso a sus cuentas.

Esta política es para todas las unidades de negocio correspondientes, proveedores y terceros. Las actualizaciones y revalidaciones deben involucrar a los recursos humanos, el oficial de privacidad, el departamento legal, seguridad de la información y la protección de las instalaciones. Una política nueva o actualizada debe ser distribuida a los empleados, el personal contratado, los vendedores bajo contrato y los empleados temporales.

Política de respuesta a incidentes de seguridad

Esta política se encarga de la necesidad de responder a los incidentes (de ciberseguridad) de manera oportuna con el fin de recuperar la actividad empresarial. La política debe incluir:

- Una definición de un incidente de seguridad de información
- Una declaración de cómo los incidentes serán manejados
- Requisitos para el establecimiento del equipo de respuesta a incidentes, con roles y responsabilidades
- Requisitos para la creación de un plan de respuesta a incidentes probado, el cual proporcionará los procedimientos y directrices documentadas para:
 - Criticidad de incidentes
 - Procesos de informes y escalado
 - Recuperación (incluyendo):
 - Los objetivos de punto de recuperación (RPO): El RPO se determina tomando como base la pérdida de datos aceptables en el caso de interrupción de las operaciones. Indica el punto más reciente de tiempo para el cual es aceptable la recuperación de los datos, que por lo general es la última copia de respaldo. El RPO cuantifica efectivamente la cantidad permitida de pérdida de datos en caso de interrupción. Según el volumen de datos, se aconseja reducir el tiempo entre las copias de respaldo para evitar una situación en la que la recuperación se vuelva imposible debido al volumen de datos que debe restaurarse. También podría darse el caso que el tiempo que se requiere para restaurar un gran volumen de datos hace que sea imposible lograr el RTO.²⁷
 - Los objetivos de tiempo de recuperación (RTO) para el retorno al estado de confianza, incluyendo:
 - Investigación y conservación del proceso.
 - Pruebas y formación.
 - Reuniones posteriores a los incidentes para documentar el análisis de la causa raíz y las mejoras de las prácticas de seguridad de la información que impiden acontecimientos futuros similares
 - Documentación del Incidente y cierre

²⁷ ISACA, *Manual de Preparación al Examen CISM 15^a edición*, EE.UU., 2016

Esta política se destina a todas las unidades de negocio correspondientes y los empleados clave. Las actualizaciones y revalidaciones deben involucrar a la función de seguridad de la información. Una política nueva o actualizada debe ser distribuida a los empleados clave.

Marcos de política

La forma en que los documentos de cumplimiento se relacionan y apoyan entre sí se llama un marco de política. Un marco define los diferentes tipos de documentos y lo que está contenido en cada uno de ellos. Las organizaciones pueden tener marcos simples de política o marcos relativamente complejos en función de sus necesidades particulares. Las organizaciones deben definir una política de ciberseguridad separada, pero ésta debe siempre formar parte del marco global de políticas de seguridad de la información.

Página dejada en blanco intencionadamente

TEMA 4—CONTROLES DE CIBERSEGURIDAD

La ciberseguridad es un entorno dinámico y cambiante, y requiere una vigilancia continua, actualización, pruebas, parches y cambios a medida que la tecnología y el negocio evolucionan. Estos controles son fundamentales para mantener la seguridad dentro de la infraestructura de TI de cualquier organización. El no abordar estos procesos es una de las principales causas de brechas de seguridad en las organizaciones.

Un recurso excelente para adquirir más conocimientos profundos en controles de ciberseguridad es el Centro para la Seguridad de Internet (del inglés, Center for Internet Security, CIS) para los Controles de Seguridad Críticos para una defensa efectiva. El CIS proporciona directrices factibles para parar la mayoría de los ataques penetrantes y peligros en el entorno actual. Los Controles de Seguridad Críticos del CIS se derivan de los patrones comunes de ataque ya que provienen de los informes de amenazas líderes de una amplia comunidad de profesionales de la industria. Estos informes proporcionan a los profesionales de ciberseguridad una manera organizada de abordar estas amenazas comunes y sus ataques.²⁸

GESTIÓN DE IDENTIDADES

La ciberseguridad se basa en el establecimiento y mantenimiento de los perfiles de usuario que definen los controles de autenticación, autorización y acceso para cada usuario. Hoy en día, las organizaciones tienen una variedad de procesos y herramientas *ad hoc* para la gestión y la disposición de información de identidades de usuarios. La gestión de identidades se centra en la racionalización de los diversos procesos de negocio necesarios para gestionar todas las formas de identidades en una organización, desde la inscripción hasta la retirada.

La capacidad de integrar los procesos de negocio y la tecnología tiene una importancia crítica en el modelo emergente, ya que enlaza las personas con los sistemas y servicios. Un objetivo clave en la gestión de identidades es centralizar y estandarizar este proceso para que se convierta en un servicio consistente y común en toda la organización.

La gestión de identidades se compone de muchos componentes que proporcionan una infraestructura colectiva y común, incluidos los servicios de directorios, servicios de autenticación (validación de quién es el usuario) y los servicios de autorización (asegurar el usuario tiene privilegios adecuados para acceder a los sistemas basados en un perfil personalizado). También incluye capacidades de gestión de usuarios como provisión o eliminación de usuarios y puede incluir la utilización de gestión de identidades federada (del inglés, federated identity management, FIM).

FIM permite a un usuario de una entidad de negocio acceder a recursos de otra unidad de negocio de una forma transparente, segura y confiable. Single Sign-on Federado (SSO) entre el dominio que provee la identidad y el dominio de un proveedor facilita la transferencia segura y confiable de identificadores de usuarios y otros atributos. FIM también soporta confianza y seguridad basada en estándares para aplicaciones publicadas tales como los servicios web.

APROVISIONAMIENTO Y DESAPROVISIONAMIENTO

El aprovisionamiento del usuario es parte del proceso de contratación de la organización donde se crean las cuentas de usuario. Las contraseñas y derechos de control de acceso se asignan generalmente basados en las obligaciones del trabajo de los usuarios. Esto puede ser un proceso complicado, ya que los usuarios pueden necesitar acceso a muchos recursos diferentes, tales como sistemas, bases de datos, correo electrónico, aplicaciones y servicios remotos, cada uno de los cuales tiene su propio control de acceso, contraseñas, claves de cifrado u otros requerimientos de autorización y autenticación. Además, los derechos de control de acceso cambian a menudo basándose en la transferencia de los requisitos de trabajo, por lo que es con frecuencia necesario actualizar los controles de acceso y eliminar el acceso que ya no se necesita. Del mismo modo, cuando un usuario deja una organización, sus cuentas deben ser desaprovisionadas – lo cual significa que todas las cuentas y accesos deben ser suspendidos o eliminados de manera oportuna.

AUTORIZACIÓN²⁹

El proceso de autorización usado para el control de acceso requiere que el sistema pueda identificar y diferenciar entre usuarios. Las reglas de acceso (autorizaciones) especifican quién puede acceder a qué. Por ejemplo, el control de acceso se basa a menudo en el menor privilegio, lo cual significa otorgar a los usuarios únicamente los accesos necesarios para realizar sus funciones. El acceso debe estar en una base documentada en base a los tipos de “necesidad de conocer” y “necesidad de hacer”.

²⁸ Center for Internet Security (CIS), *The CIS Critical Security Controls for Effective Cyber Defense*, www.sans.org/critical-security-controls
²⁹ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

El acceso a la computadora puede ser establecido a diferentes niveles (por ejemplo, archivos, tablas, elementos de datos, etc.). Cuando los auditores de seguridad de la información revisan la accesibilidad a los ordenadores, tienen la necesidad de conocer qué se puede hacer con los accesos y qué está prohibido. Por ejemplo, las restricciones de acceso a nivel de archivo incluyen en general lo siguiente:

- Sólo lectura
- Escribir, crear o actualizar solamente
- Sólo borrar
- Sólo ejecutar
- Una combinación de todo lo anterior

El tipo menos peligroso de acceso es el de sólo lectura, siempre y cuando la información a la que se acceda no sea sensible ni confidencial. Esto es así porque el usuario no puede alterar o usar el archivo informático más allá de la visualización básica o impresión.

LISTAS DE CONTROL DE ACCESO³⁰

Para proporcionar autorizaciones de seguridad a los archivos y recursos (facilities) enumerados anteriormente, los mecanismos de control de acceso lógico utilizarán tablas de autorización de acceso a las que también se hace referencia como listas de control de acceso (Access Control Lists - ACLs) o tablas de control de acceso. Las ACLs se refieren a un registro de:

- Usuarios (incluyendo grupos, máquinas, procesos) a los que se les ha dado permiso para usar un recurso particular de sistema, y
- Los tipos de acceso permitidos.

Las ACLs varían considerablemente en su funcionalidad y flexibilidad. Algunas sólo permiten especificaciones para ciertos grupos pre-establecidos (por ejemplo, dueño, grupo, y global) mientras que las ACLs más avanzadas permiten mucha más flexibilidad, como por ejemplo grupos definidos por usuarios. También las ACLs más avanzadas pueden usarse para negar explícitamente acceso a una persona o grupo en particular. Con las ACLs más avanzadas, el acceso puede ser otorgado a la discreción del que elabora la política (implementada por el administrador de seguridad) o usuario individual, dependiendo de cómo los controles sean implementados técnicamente. Cuando un usuario cambia sus funciones de trabajo dentro de una organización, a menudo sus antiguos derechos de acceso no son eliminados antes de agregar los nuevos accesos requeridos. Sin eliminar los antiguos derechos de acceso, podría haber un problema potencial de segregación de funciones.

LISTAS DE ACCESO^{31, 32}

Las listas de acceso filtran el tráfico en las interfaces de la red basado en criterios específicos, proporcionando así seguridad básica de red. Sin listas de acceso, los dispositivos de red pasan todos los paquetes. Por el contrario, después de crear una lista de acceso y aplicarla a una interfaz, sólo pasa el tráfico que las reglas establecidas permitan, en base a una declaración implícita de “negar todos” añadida automáticamente a la lista. Entender la colocación y el impacto de una lista de acceso es esencial porque los errores pueden detener el tráfico de red en su totalidad.

GESTIÓN DE USUARIOS PRIVILEGIADOS

El acceso privilegiado permite a los administradores mantener y proteger los sistemas y las redes. Los usuarios privilegiados a menudo pueden acceder a cualquier información almacenada dentro de un sistema, lo que significa que pueden modificar o burlar las salvaguardas existentes, tales como controles de acceso y los registros de acceso. “Usuarios privilegiados” es un término que normalmente hace referencia a los administradores de sistemas, redes, servidores o puestos de trabajo.

Debido a este acceso elevado, las organizaciones tienen que pensar cuidadosamente acerca de los usuarios y cuentas privilegiadas y aplicar controles adicionales a los mismos. Los controles comunes incluyen:

- Limitar el acceso privilegiado a sólo aquellos que lo requieran para llevar a cabo sus funciones de trabajo
- Realizar verificaciones de antecedentes de los individuos con acceso elevado
- Implementar el registro adicional de la actividad asociada a cuentas privilegiadas
- Mantener responsabilidad sobre cada acción impidiendo que se compartan cuentas privilegiadas
- Utilizar contraseñas más fuertes u otros controles de autenticación para proteger cuentas privilegiadas del acceso no autorizado
- Revisar periódicamente los privilegios de las cuentas y eliminar los que ya no se requieren
- Requerir a los usuarios privilegiados que mantengan dos cuentas (privilegiada y no privilegiada) y exigir el uso de cuentas no privilegiadas para tareas generales uso del correo electrónico, documentación acceso a internet, etc.

³⁰ Ibid.

³¹ Wilson, Tracey. “Basics of Access Control Lists: How to Secure ACLs,” 16 Mayo 2012, <http://blog.pluralsight.com/access-control-list-concepts>

³² Cisco; *Access Control Lists: Overview and Guidelines*, Cisco IOS Security Configuration Guide, www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacs.pdf

GESTIÓN DE CAMBIOS

La gestión de cambios es esencial para la infraestructura de TI. Su propósito es asegurar que esos cambios a procesos, sistemas, software, aplicaciones, plataformas y configuraciones se introducen de una manera ordenada y controlada. Los controles se implementan en la forma de un proceso de revisión estructurado destinado a evaluar y minimizar la posibilidad de interrupción que un cambio propuesto, la actividad de mantenimiento o un parche pueden introducir. Los controles efectivos aseguran que todos los cambios se clasifican, priorizan y autorizan. El proceso generalmente incluye mecanismos para el seguimiento y la documentación de los cambios para demostrar la responsabilidad y el cumplimiento de las mejores prácticas.

Es importante señalar que la gestión del cambio no es un proceso independiente; se basa en otros procesos y controles. Por lo tanto, se requiere un conocimiento exhaustivo de las operaciones de la empresa y la infraestructura para que sea implementado de manera efectiva.

GESTIÓN DE LA CONFIGURACIÓN

El mantenimiento de las configuraciones de seguridad de los dispositivos de redes, sistemas, aplicaciones y otros recursos de TI es de vital importancia para garantizar que los controles de seguridad estén correctamente instalados y mantenidos. Como las organizaciones crecen y evolucionan, también lo hace la posibilidad de cambios y disfunciones. Para gestionar estos cambios y minimizar su potencial de interrumpir las operaciones, la eficiencia y los beneficios, es necesario desarrollar procesos formales. Estos procesos de gestión de la configuración pueden ser bastante complejos, ya que soportan muchas otras actividades dentro de la empresa.

La implementación de un proceso de gestión de la configuración tiene varios beneficios para la seguridad, incluyendo:³³

- La verificación del impacto en los elementos relacionados
- La evaluación del riesgo de una propuesta de cambio
- La capacidad de inspeccionar diferentes líneas de defensa para posibles debilidades
- El seguimiento de los elementos de configuración en contra de las líneas de base de configuración de seguridad aprobadas
- Conocimiento de las investigaciones después de un fallo de seguridad o de la interrupción de las operaciones
- El control de versiones y la autorización de producción de componentes de hardware y software

GESTIÓN DE PARCHES

Los parches son soluciones a los errores de programación de software. En muchos casos, las vulnerabilidades de seguridad son introducidas por errores de codificación. Por lo tanto, es vital que los errores de software que se identifican como vulnerabilidades de seguridad sean parcheados tan pronto como sea posible. La mayoría de los proveedores de software lanzan regularmente actualizaciones de software y parches conforme las vulnerabilidades son identificadas y corregidas.

La falta de aplicación de parches a vulnerabilidades de seguridad conocidas es la causa más común de las brechas de seguridad. Por lo tanto, los parches son una parte importante de la gestión de vulnerabilidades, y las organizaciones deben establecer procesos para identificar los parches que son relevantes para su infraestructura de TI. Una vez que el parche necesario es identificado, debe ser probado para asegurar que no repercuta negativamente en las operaciones. Despues de que el parche se ha verificado, puede ser programado e instalado en su caso.

³³ ISACA, *Configuration Management Using COBIT 5*, EE.UU., 2013

SECCIÓN 2—EVALUACIÓN DE CONOCIMIENTOS

Instrucciones: Seleccione la respuesta correcta para completar cada una de las declaraciones que se muestran a continuación. Use cada palabra una sola vez.

BANCO DE PALABRAS

Activo	Parches	Rootkit
Vector de ataque	Payload	Normas
Directrices	Políticas	Amenaza
Gestión de identidades	Procedimiento	Vulnerabilidad
Software malintencionado (malware)	Ciberriesgo	

1. El deber principal de la ciberseguridad es identificar, mitigar y gestionar _____ a los activos digitales de una organización.
2. Un(a) _____ es cualquier cosa capaz de actuar contra un activo, de una manera que puede causar daño.
3. Un(a) _____ es algo valioso que merece protección.
4. Un(a) _____ es una debilidad en el diseño, implementación, operación o controles internos de un proceso, que podría ser aprovechada para violar la seguridad del sistema.
5. El camino o ruta utilizada para obtener acceso a la activo objetivo se conoce como un(a) _____ .
6. En un ataque, el contenedor que entrega el exploit al objetivo se llama un(a) _____ .
7. _____ comunican actividades y conductas requeridas y prohibidas.
8. _____ es un tipo de malware que oculta la existencia de otro malware, mediante la modificación del sistema operativo subyacente.
9. _____ proporcionan detalles sobre cómo cumplir con las políticas y normas.
10. _____ proporcionan una guía general y recomendaciones sobre qué hacer en situaciones específicas.
11. _____, también conocido como código malicioso, es el software diseñado para obtener acceso a los sistemas informáticos objetivo, robar información o interrumpir las operaciones computacionales.
12. _____ se utilizan para interpretar las políticas en situaciones específicas.
13. _____ son soluciones a los errores de programación de software y codificación.
14. _____ incluye muchos componentes, tales como los servicios de directorio, servicios de autenticación y autorización, y las capacidades de gestión de usuarios, tales como el aprovisionamiento y desaproporcionamiento.

Ver respuestas en el Anexo C.



Sección 3:

Principios de Arquitectura de Seguridad

Los temas tratados en esta sección incluyen:

1. Visión general de la arquitectura de seguridad
2. El modelo OSI
3. Defensa en profundidad
4. Control de flujo de información
5. Aislamiento y segmentación
6. Registro, monitorización y detección
7. Fundamentos, técnicas y aplicaciones de cifrado

Página dejada en blanco intencionadamente

TEMA 1—VISIÓN GENERAL DE LA ARQUITECTURA DE SEGURIDAD

La arquitectura de seguridad describe la estructura, los componentes, las conexiones y el diseño de los controles de seguridad dentro de la infraestructura de TI de una organización. Las organizaciones tienen diferentes tipos de arquitecturas de seguridad que determinan las particularidades de diferentes subsistemas, productos y aplicaciones. Estos datos influirán a su vez en el enfoque que una organización tiene para la **defensa en profundidad**, o la práctica de establecer múltiples capas de defensa para proporcionar una protección añadida.

La arquitectura de seguridad muestra cómo se implementa la defensa en profundidad, así como la manera en la que se vinculan las capas de control. Por lo tanto, es esencial para el diseño y la implementación de controles de seguridad en cualquier entorno complejo.

Cada componente de un sistema dado plantea su propio riesgo de seguridad. Debido a que la topología de la arquitectura de seguridad varía de una organización a otra, una serie de diferentes variables y riesgo debe tenerse en cuenta al abordar la topología de una organización en particular. Esta sección discutirá dichas variables individualmente, junto con las mejores prácticas para gestionar exitosamente su riesgo relacionado.

EL PERIMETRO DE SEGURIDAD

Muchos controles y arquitecturas de seguridad actuales se desarrollaron con el concepto de perímetro- una frontera bien definida (virtual en su mayoría) entre la organización y el mundo exterior. En estos modelos de ciberseguridad, el foco está **centrado en la red** o **centrado en los sistemas**. En el modelo centrado en el sistema, el énfasis está en la colocación de los controles a nivel de red y del sistema para proteger la información almacenada en su interior. Un modelo alternativo es el **centrado en los datos**, que hace hincapié en la protección de datos, independientemente de su ubicación.

Con la llegada del Internet, la externalización, los dispositivos móviles, la nube y otros servicios alojados, el perímetro se ha ampliado considerablemente. En consecuencia, existen nuevos riesgos y vulnerabilidades significativas que enfrentar en este entorno hiperconectado y extendido. El perímetro es, pues, una importante línea de defensa que protege la empresa contra amenazas externas, y su diseño debe reflejar una actitud proactiva hacia la prevención de riesgo potencial.

Un componente importante de la seguridad perimetral es el perímetro de internet. Este perímetro garantiza un acceso seguro a internet para los empleados de la empresa y los usuarios visitantes que residen en todos los lugares, incluidos los que participan en el teletrabajo o trabajo a distancia. Con el fin de garantizar la seguridad del correo electrónico, los teléfonos IP y las aplicaciones web, el sistema de nombres de dominio (DNS), etc., el perímetro de Internet debe:

- Establecer el tráfico entre la empresa e internet
- Evitar que archivos ejecutables se transfieran a través de adjuntos de correo electrónico o la navegación web
- Monitorizar la actividad irregular en los puertos de red internos y externos
- Detectar y bloquear el tráfico del punto final interno infectado
- Controlar el tráfico de usuarios hacia internet
- Identificar y bloquear el tráfico anómalo y paquetes maliciosos reconocidos como potenciales ataques
- Eliminar las amenazas como el spam de correo electrónico, virus y gusanos
- Hacer cumplir las políticas de filtrado para bloquear el acceso a sitios web que contengan malware o contenido cuestionable

El perímetro también debe proporcionar protección para redes privadas virtuales (VPN), redes de área amplia (WAN) y redes de área local inalámbricas (WLAN).

Para las VPN, esta protección debe ser triple:

1. Terminar el tráfico VPN cifrado iniciado por usuarios remotos.
2. Proporcionar un concentrador (hub) para la terminación del tráfico VPN cifrado desde sitios remotos, organizaciones.
3. Proporcionar un concentrador (hub) para los usuarios tradicionales del servicio dial-in.

INTERDEPENDENCIAS

Como se mencionó anteriormente, las arquitecturas de TI modernas suelen ser descentralizadas y sin perímetro. Esto incluye un número creciente de plataformas y servicios basados en la nube, así como un cambio en la potencia de computación y patrones de uso hacia los dispositivos móviles inteligentes, tales como las tabletas o los teléfonos inteligentes. Como consecuencia, tanto el número de posibles objetivos de ataque fuera de los límites de la organización como el número de vectores de ataque ha crecido. Por el contrario, el grado de control sobre los entornos sin perímetro se ha reducido

significativamente, sobre todo en las empresas que permiten la integración parcial o total de los dispositivos móviles que son propiedad de los usuarios (p. ej el BYOD). Estos cambios tienen importantes ramificaciones para la arquitectura de seguridad.

En las arquitecturas TI distribuidas y descentralizadas, es probable que aumente el riesgo de terceros, a menudo como una función del movimiento de aplicaciones críticas, plataformas y elementos de infraestructura en la nube. Para las plataformas, la infraestructura de almacenamiento y los repositorios de datos basados en la nube, el enfoque de la ciberseguridad se está desplazando hacia los contratos y acuerdos de nivel de servicio (SLA). Al mismo tiempo, los proveedores de servicios en la nube se enfrentan a un mayor riesgo de ataques y violaciones debido a la aglomeración y la agrupación de los datos e información sensibles. Además de las preocupaciones sobre los servicios de terceros, existe un riesgo legal significativo. Las empresas que experimentan una pérdida de datos sensibles pueden no estar en condiciones de interponer un recurso contra los autores porque el proveedor en la nube a menudo tiene que iniciar una acción legal.

Independientemente de las medidas de seguridad de información genéricas llevadas a cabo por una empresa, a menudo existen áreas expuestas dentro de las arquitecturas de TI. El ciber crimen y los perpetradores de la ciberguerra siguen apuntando a los “puntos débiles” en los elementos y sistemas de la arquitectura. En contraposición a los ataques indiscriminados y oportunistas, las APTs y el ciber crimen siempre se basan en la investigación preparatoria y una visión de la empresa objetivo. Esto, a su vez, eleva el nivel de exposición de partes débiles o sin seguridad de la arquitectura general. Estos puntos vulnerables incluyen sistemas heredados, partes sin parches en la arquitectura, el uso compartido de los dispositivos móviles y muchos otros.

ARQUITECTURAS Y MARCOS DE SEGURIDAD

Actualmente existe un gran número de enfoques de arquitectura, y muchos de ellos han evolucionado a partir del desarrollo de la arquitectura de la empresa. Aunque sus detalles específicos pueden ser diferentes, todos ellos generalmente tienen como objetivo articular qué procesos realiza un negocio y cómo esos procesos se ejecutan y se aseguran. Estos enfoques articulan la organización, funciones, entidades y relaciones que existen o que deben existir para llevar a cabo un conjunto de procesos de negocio.

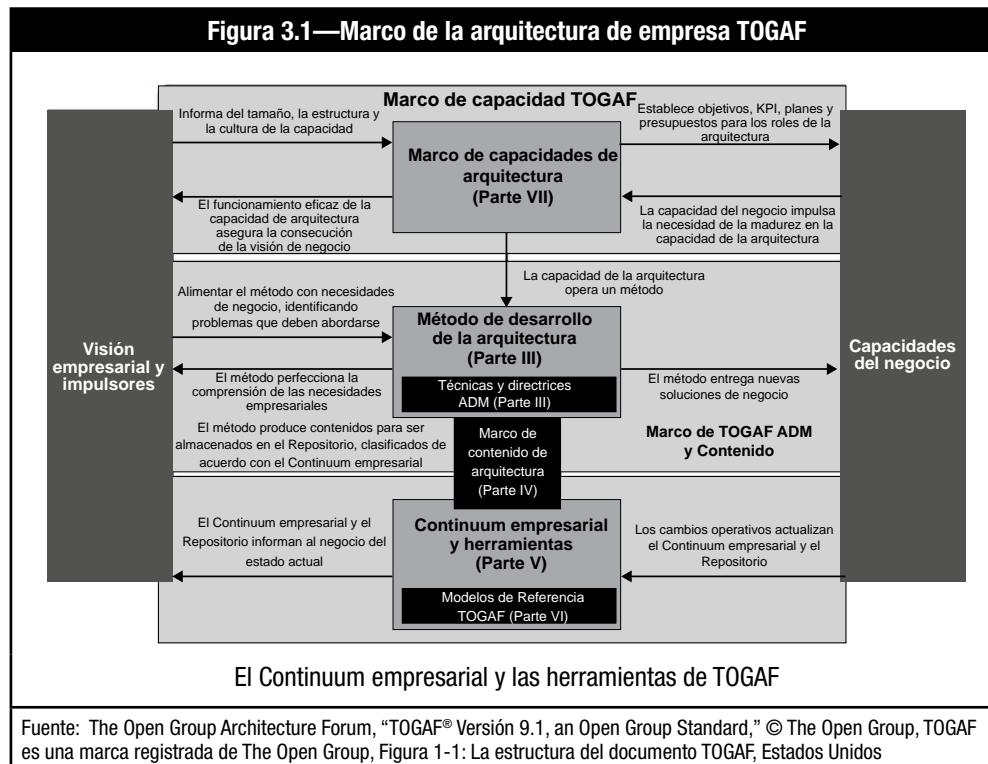
Del mismo modo, los modelos de arquitectura de seguridad normalmente se dividen en dos categorías: modelos de procesos y modelos de marcos. Los marcos permiten una gran flexibilidad en cómo se desarrolla cada elemento de la arquitectura. La esencia de un marco es describir los elementos de la arquitectura y cómo éstos se relacionan entre sí, mientras que un modelo de procesos es más directivo en su enfoque de los procesos utilizados para los distintos elementos. Un ejemplo reciente de modelo de procesos es un servidor web construido por bloques donde está exactamente especificado cómo un servidor web debe ser desplegado y qué procesamiento está o no permitido en cada bloque.

EL MARCO ZACHMAN Y SABSA

Así como existen muchos tipos diferentes de empresas, existen muchos enfoques diferentes de arquitecturas de seguridad. Por ejemplo, el enfoque del marco Zachman que desarrolla la matriz de quién, qué, por qué, dónde, cuándo y cómo es compartida por la Arquitectura de Seguridad Aplicada a los Negocios de Sherwood (SABSA). La matriz contiene columnas que muestran los aspectos de la empresa que pueden ser descritos o modelados, mientras que las filas representan diferentes puntos de vista desde los cuales se pueden considerar esos aspectos. Este enfoque proporciona una estructura lógica para la clasificación y organización de elementos de diseño, lo que mejora la integridad de la arquitectura de seguridad.

EL MARCO DE ARQUITECTURA DEL OPEN GROUP (TOGAF)

Otro marco de arquitectura es el Marco de Arquitectura del Open Group (The Open Group Architecture Framework, TOGAF). Desarrollado por el Open Group en los años 1990, este enfoque de alto nivel y holístico aborda la seguridad como un componente esencial de la concepción global de la empresa. El objetivo de TOGAF es asegurar que los proyectos de desarrollo de arquitectura cumplan los objetivos del negocio, que sean sistemáticos y que sus resultados sean repetibles. En la **figura 3.1** se aprecia el proceso de arquitectura TOGAF y su relación con las operaciones de las empresas.

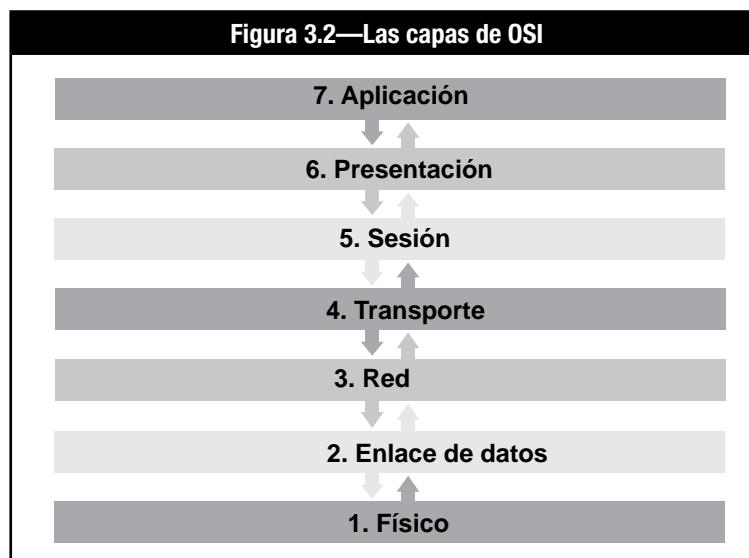


Página dejada en blanco intencionadamente

TEMA 2—EL MODELO OSI

El Modelo de interconexión de sistemas abiertos (OSI) se utiliza para describir protocolos de red. Debido a que rara vez se implementa en redes reales, se considera una referencia para estandarizar el desarrollo de las redes reales. OSI fue la primera definición abierta no propietaria para redes.

El modelo OSI define grupos de funcionalidad requeridos para los equipos de la red en capas, donde cada capa implementa un protocolo estándar para su funcionalidad. Hay siete capas del modelo OSI, que se muestran en la **figura 3.2**.



Cada capa OSI realiza una función específica para la red:

- **La capa física (Capa 1)**—Gestiona señales entre los sistemas de red
- **La capa de enlace de datos (Capa 2)**—Divide los datos en tramas que pueden ser transmitidas por la capa física
- **La capa de red (Capa 3)**—Traduce direcciones de red y dirige los datos del emisor al receptor
- **La capa de transporte (Capa 4)**—Asegura que los datos se transfieren de forma fiable en la secuencia correcta
- **La capa de sesión (Capa 5)**—Coordina y gestiona las conexiones de usuario
- **La capa de presentación (Capa 6)**—Da formato, cifra y comprime los datos
- **La capa de aplicación (Capa 7)**—Media entre aplicaciones de software y otras capas de servicios de red

TCP/IP

El conjunto de protocolos utilizado como el estándar de facto para internet es conocido como el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP). El modelo TCP/IP incluye tanto protocolos orientados a red como de soporte a aplicaciones, operando en las Capas 3 y 4 del modelo OSI.

Versiones del protocolo de Internet

Actualmente, existen dos versiones del protocolo IP que operan en la Capa 3—IPv4 e IPv6.

IPv4 es la cuarta revisión del protocolo IP y el más usado para la conexión de dispositivos en Internet. Utiliza un esquema de direcciones de 32 bit que permite algo más de 4 mil millones de direcciones. Con el actual predominio de dispositivos conectados a Internet, se espera que tarde o temprano IPv4 se quede sin direcciones disponibles. Por este motivo, IPv6 ha sido desarrollado para hacer frente a esta preocupación.³⁴

IPv6, también llamado IPng (nueva generación) es la última versión de IP y es una actualización más evolucionada de IPv4. IPv6 fue creada para permitir un crecimiento de Internet para el número de equipos conectados y la cantidad de datos transmitidos. Se espera que IPv4 e IPv6 coexistan durante algún tiempo.³⁵

³⁴ Beal, Vangie. “What is the Difference Between IPv6 and IPv4?”, Webopedia, 22 enero 2014, www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html

³⁵ Ibid.

La **figura 3.3** muestra algunos de los estándares asociados con el conjunto TCP/IP y dónde encajan dentro del modelo OSI. Es interesante observar que el conjunto de protocolos TCP/IP se desarrolló antes que el marco OSI; por lo tanto, no hay ninguna coincidencia directa entre los estándares de TCP/IP y las capas del marco.

Figura 3.3—Asociación de OSI con el conjunto TCP/IP

Modelo OSI	Capas conceptuales de TCP/IP	Unidad de Datos de Protocolo (PDU)	Protocolos TCP/IP	Equipos	Funciones de las capas	Funciones de las capas	
7	Aplicación	Aplicación	Datos	HTTP Protocolo de transferencia de archivos (FTP) Protocolo simple de transporte de correos (SMTP) TFTP NFS Protocolo de servidor de nombres (NSP)	Pasarela (Gateway)	Provee interfaz de usuario	Servicios de archivo, impresión, mensajes, base de datos y aplicaciones
6	Presentación			Protocolo simple de administración de redes (SNMP) Protocolo de control de terminal remoto (Telnet) LPD X Windows DNS DHCP/BootP		Presenta datos Maneja tareas de procesamiento, como por ejemplo, encriptación	Servicios de encriptación, compresión y traducción de datos
5	Sesión					Mantiene separados los datos de aplicaciones diferentes	Control de diálogo
4	Transporte	Transporte	Segmento	Protocolo de control de transmisión (TCP) Protocolo de datagrama de usuario (UDP)	Switch de capa 4	Provee entrega confiable o no confiable	Conexión de extremo a extremo
3	Red	Interfaz de red	Paquete	ICMP ARP RARP Protocolo de Internet (IP)	Enrutador (router) Switch de capa 3	Provee direccionamiento lógico que los routers utilizan para determinar la ruta	Enrutamiento
2	Enlace de datos	Interfaz LAN o WAN	Estructura	Ethernet Fast Ethernet FDDI Token Ring Protocolo punto a punto (PPP)	Switch de capa 2 Puente AP inalámbrico NIC	Combina los paquetes en bytes, y los bytes en tramas Provee acceso a medios utilizando dirección MAC Realiza detección de errores, pero no corrección de errores	Envío de tramas
1	Físico		Bits		Concentrador Hub Repetidor NIC	Mueve bits entre dispositivos Especifica voltaje, velocidad de alambre y pin-out de los cables	Topología física

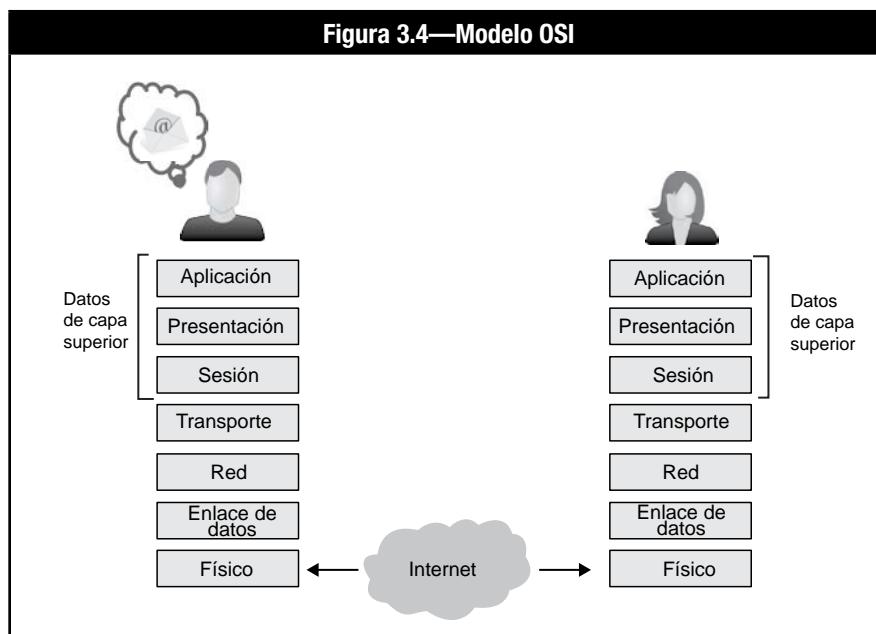
Fuente: ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015, figura 4.23

ENCAPSULACIÓN

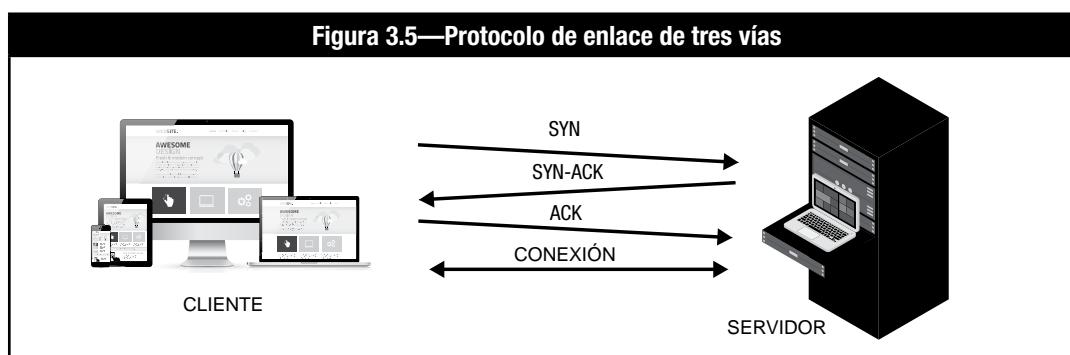
La encapsulación es el proceso de añadir información de direccionamiento de datos a medida que se transmiten por la pila OSI. Cada capa confía en los servicios proporcionados por la capa inferior. Cada capa del modelo OSI sólo se comunica con su par de destino. Lo hace utilizando datagramas o unidades de datos de protocolo (PDU). Consulte la **figura 3.3** anterior para los nombres de PDU.

El modelo OSI se muestra en la **figura 3.4**. Los datos de la capa superior se transmiten a la capa de transporte como segmentos y son “envueltos” con una cabecera para su identificación. Estos segmentos se transmiten a la capa de red en forma de paquetes de nuevo con una cabecera. Los datos se desglosan en tramas en la capa de enlace de datos y también tienen información de control anexa. En la capa física, los datos se transforman en bits (1s y 0s) para su entrega a la red de destino.

Una vez en el destino, cada capa del extremo receptor se despoja de la información de direccionamiento correspondiente y la pasa a la pila OSI hasta que el mensaje es entregado. Este proceso se llama desencapsulación.



Los servicios de comunicaciones en la Capa 4 del modelo OSI se categorizan como orientados a conexión o no orientados a conexión. TCP proporciona una entrega confiable y secuenciada con comprobación de errores. Las conexiones se establecerán a partir de un protocolo de enlace de tres vías (three-way handshake), y por lo tanto son orientadas a conexión, tal y como se muestra en la **figura 3.5**. El Protocolo de Datagramas de Usuario (UDP) es un protocolo no orientado a conexión utilizado en los escenarios donde la velocidad es más importante que la comprobación de errores y la entrega garantizada. UDP hace uso de las sumas de verificación (checksums) para la integridad de los datos.



Página dejada en blanco intencionadamente

TEMA 3—DEFENSA EN PROFUNDIDAD

Debido a que ningún control o contramedida puede eliminar el riesgo, a menudo es importante usar varios controles para proteger un activo. Este proceso de defensa por capas se conoce como **defensa en profundidad**, pero también se conoce como protección en profundidad o seguridad en profundidad. Este proceso obliga a un adversario a vencer o evitar más de un control para tener acceso a un activo.

La defensa en profundidad es un concepto importante en el diseño eficaz de una estrategia o arquitectura de seguridad de la información. Cuando son diseñadas e implementadas correctamente, las múltiples capas de control proporcionan múltiples oportunidades para la monitorización con el fin de detectar el ataque. El agregar controles adicionales también crea un retraso por lo que el ataque puede ser interrumpido y preventido.

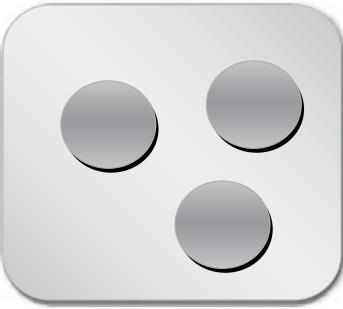
El número y los tipos de capas necesarios varían en función del valor de los activos, la criticidad, la fiabilidad de los controles y el grado de exposición. Es probable que una dependencia excesiva en un solo control genere un falso sentido de confianza. Por ejemplo, una compañía que depende exclusivamente de un cortafuegos (firewall) puede ser objeto de numerosas metodologías de ataque. Una defensa adicional puede consistir en el uso de la educación y la sensibilización para crear un “firewall humano”, lo que puede constituir una capa crítica de defensa. La segmentación de la red puede constituir otra capa defensiva.

Utilizar una estrategia de defensa en profundidad para los controles de aplicación tiene varias ventajas, incluyendo el aumento del esfuerzo que se requiere para un ataque con éxito y la creación de oportunidades adicionales para detectar o retrasar un atacante. Hay varias formas en que la defensa en profundidad se pueda implementar, como se muestra en la **figura 3.6**.³⁶

Figura 3.6—Tipos de implementación de defensa en profundidad		
Tipo de defensa	Representación gráfica	Descripción
Anillos concéntricos (o capas anidadas)		Crea una serie de capas anidadas que deben ser anuladas para completar un ataque. Cada capa retrasa al atacante y ofrece oportunidades para detectar el ataque.
Redundancia superpuesta		Dos o más controles que trabajan en paralelo para proteger un activo. Proporciona puntos de detección múltiples y superpuestos. Esta es más efectiva cuando cada control es diferente.

³⁶ Encurve, LLC.

Figura 3.6—Tipos de implementación de defensa en profundidad (*cont.*)

Tipo de defensa	Representación gráfica	Descripción
Segregación o compartimentación		<p>Compartimenta el acceso a un activo, requiriendo dos o más procesos, controles o individuos para acceder o usar el activo.</p> <p>Ésta es efectiva al proteger activos de muy alto valor o en ambientes donde la confianza es un problema.</p>

Fuente: Encurve, LLC.

Otra forma de pensar en la defensa en profundidad es desde una perspectiva de arquitectura:

- **Defensa en profundidad horizontal**—Los controles se colocan en varios lugares en el camino de acceso a un activo, lo cual es funcionalmente equivalente al modelo de anillos concéntricos anterior mostrado en la **figura 3.6**
- **Defensa en profundidad vertical**—Controles colocados en diferentes capas del sistema - hardware, sistema operativo, las aplicaciones, bases de datos o nivel del usuario

El uso de técnicas de defensa en profundidad requiere una planificación eficaz y la comprensión de las fortalezas y debilidades de cada tipo, así como la manera en que los controles interactúan. Es fácil crear un sistema de controles demasiado complejo, y el hecho de tener un número excesivo de capas puede ser tan perjudicial como tener un número muy bajo. Cuando desarrolle implementaciones de defensa en profundidad, considere las siguientes preguntas:

- ¿A qué vulnerabilidades se dirige cada capa o control?
- ¿Cómo mitiga la capa dicha vulnerabilidad?
- ¿De qué manera depende o interactúa cada control con el resto de controles?

TEMA 4—CONTROL DE FLUJO DE INFORMACIÓN

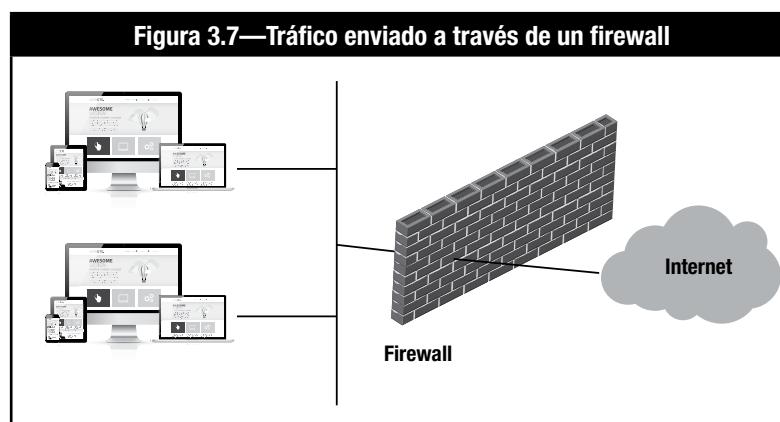
La apertura a internet hace que cada red corporativa conectada a ella sea vulnerable a los ataques. Los intrusos (hackers) en Internet podrían entrar en una red corporativa y hacer daño de diferentes maneras: robando o dañando datos importantes, dañando los sistemas individuales o toda la red, mediante el uso de los recursos informáticos corporativos o a través de la red y los recursos corporativos para hacerse pasar por un empleado de la empresa. Los cortafuegos (firewalls) se construyen como un medio de seguridad perimetral para estas redes.

Un **firewall** se define como un sistema o combinación de sistemas que establece un límite entre dos o más redes, formando típicamente una barrera entre un entorno seguro y un entorno abierto tal como internet. Éste aplica reglas para controlar el tipo de tráfico que entra y sale de una red. La mayoría de los firewalls comerciales están diseñados para manejar los protocolos de Internet más utilizados.

Los firewalls eficaces deben permitir a las personas en la red de la empresa acceder a Internet al mismo tiempo que evitan que otras personas en Internet obtengan acceso a la red corporativa para causar daño. La mayoría de las organizaciones siguen una filosofía de negar todo, lo que significa que el acceso a un determinado recurso será negado a menos que un usuario pueda proporcionar una razón específica de negocio o la necesidad de acceso a la fuente de información. Lo contrario de esta filosofía de acceso, que no es ampliamente aceptada, es la filosofía de aceptar todo, en virtud de la cual se permite el acceso a todos a menos que alguien pueda definir zonas para denegar el acceso.

CARACTERÍSTICAS GENERALES DE LOS FIREWALLS

Los firewalls separan redes entre sí y protegen el tráfico entre ellas. Ver la **figura 3.7**.



Junto con otros tipos de seguridad (por ejemplo, sistemas de detección de intrusos [IDS] / Sistemas de prevención de intrusiones [IPS]), los firewalls controlan el punto más vulnerable entre una red corporativa e internet, y pueden ser tan simples o tan complejos como las políticas de seguridad de la información corporativa lo demanden.

Hay muchos tipos diferentes de firewalls, pero la mayoría de ellos permiten a las organizaciones:

- Bloquear el acceso a determinados sitios en Internet.
- Limitar el tráfico en el segmento de servicios públicos de la organización a direcciones y puertos relevantes.
- Impedir que determinados usuarios tengan acceso a ciertos servidores o servicios.
- Supervisar y registrar la comunicación entre una red interna y otra externa para investigar las intrusiones en la red o detectar alteraciones internas.
- Cifrar los paquetes que se envían entre diferentes ubicaciones físicas dentro de una organización mediante la creación de una VPN a través de internet (por ejemplo, la seguridad IP [IPSec], túneles VPN seguros). Se pueden extender las funcionalidades de algunos firewalls de modo que puedan también proporcionar protección contra virus y ataques dirigidos a explotar las vulnerabilidades conocidas del sistema operativo.

TIPOS DE FIREWALL DE RED

En general, los tipos de firewalls de red disponibles hoy en día se dividen en las siguientes categorías:

- Filtrado de paquetes
- Sistemas de Firewall de aplicación (Application Firewall Systems)
- Inspección a nivel del estado (Stateful Inspection)
- Firewall de próxima generación (NGFW)

Los diferentes tipos de firewall se explican en las siguientes secciones. Se proporciona un resumen en la **figura 3.8**.

Figura 3.8—Tipos de Firewall

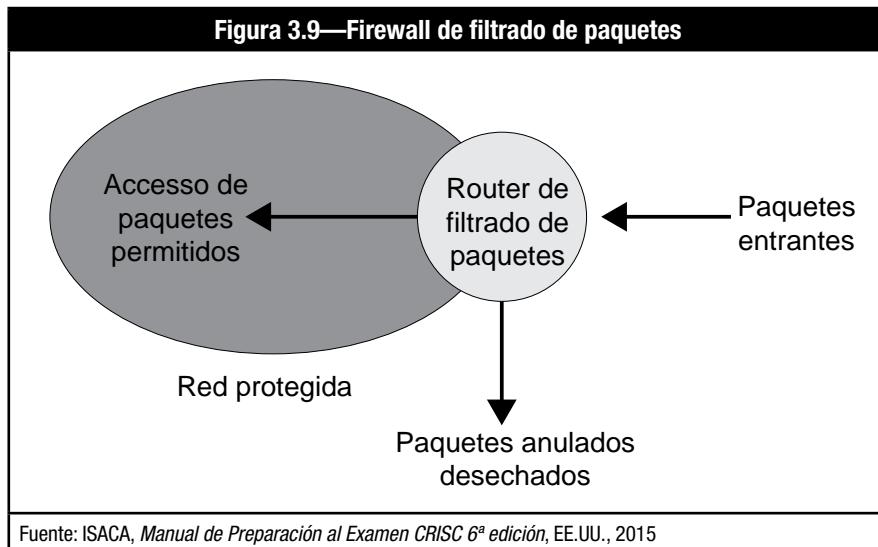
Primera generación	Un simple router de filtrado de paquetes que examina individualmente los paquetes y aplica reglas basadas en direcciones, protocolos y puertos.
Segunda generación	Mantiene registros de todas las conexiones en una tabla de estado. Ésto le permite aplicar reglas basadas en paquetes dentro del contexto de la sesión de comunicaciones.
Tercera generación	Opera en la Capa 7 (capa de aplicación) y es capaz de examinar el protocolo usado en las comunicaciones, como el Protocolo de transferencia de hipertexto (HTTP). Estos cortafuegos son mucho más sensibles a actividades sospechosas relativas al contenido del mensaje en sí mismo, no sólo a la información del direccionamiento.
Próxima generación	Llamados a veces de Inspección profunda de paquetes (Deep Packet Inspection, DPI), son una versión mejorada de los cortafuegos de tercera generación e incorporan la funcionalidad de Sistema de prevención de intrusiones (IPS) y a menudo son capaces de inspeccionar conexiones SSL (Secure Sockets Layer) o SSH (Secure Shell).

Fuente: ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

FIREWALLS DE FILTRADO DE PAQUETES

Los firewalls de primera generación eran firewalls basados en el filtrado de paquetes que se desplegaban entre la red privada e Internet. En el filtrado de paquetes, un enrutador de filtrado examina el encabezado de cada paquete de datos que viaja entre Internet y la red corporativa. Las cabeceras de los paquetes contienen información, incluida la dirección IP del remitente y el receptor, junto con los números de puerto (aplicación o servicio) autorizados para utilizar la información transmitida. En base a esa información, el router sabe qué tipo de servicio de internet (por ejemplo, el servicio basado en la web o Protocolo de transferencia de archivos [FTP]) se utiliza para enviar los datos, así como la identidad del remitente y el receptor de los datos. De esta manera, el router puede prevenir el envío de ciertos paquetes entre Internet y la red corporativa. Por ejemplo, el router puede bloquear todo el tráfico desde y hacia destinos sospechosos. Ver la **figura 3.9**.

Figura 3.9—Firewall de filtrado de paquetes



Fuente: ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

Debido a que se permite el intercambio directo de paquetes entre los sistemas externos y los sistemas internos, el potencial de un ataque está determinado por el número total de sistemas anfitriones (hosts) y de servicios a los que el enrutador de filtrado de paquetes permite el tránsito. Los firewalls de filtrado de paquetes son por lo tanto los más adecuados para las redes más pequeñas. Las organizaciones con muchos routers pueden enfrentarse a dificultades de diseño, codificación y mantenimiento de la base de reglas.

Debido a que sus reglas de filtrado se realizan en la capa de red, los firewalls de filtrado de paquetes son generalmente estables y simples. Esta simplicidad tiene ventajas y desventajas, como se muestra en la **figura 3.10**.

Figura 3.10—Firewall de filtrado de paquetes	
Ventajas	Desventajas
Simplicidad de un “choke point” (cuello de botella) de red	Vulnerable a ataques de filtros no configurados de manera apropiada
Mínimo impacto en el rendimiento de la red	Vulnerable a ataques de túnel sobre servicios permitidos
Poco costoso o gratuito	Todos los sistemas de red privada son vulnerables cuando un router de filtrado de paquete se ve comprometido

A la luz de estas ventajas y desventajas, el filtrado de paquetes es más efectivo cuando se implementa con seguridad básica y monitorización en mente.

Algunos de los ataques más comunes contra los cortafuegos (firewalls) de filtrado de paquetes son:

- **IP spoofing**—En este tipo de ataque, el atacante falsifica la dirección IP, ya sea la de un host de la red interna o bien la de un host de la red de confianza. Esto permite que el paquete que se envía pase la base de reglas del firewall y penetre el perímetro del sistema. Si el spoofing usa una dirección IP interna, el firewall puede ser configurado para rechazar el paquete basándose en el análisis de la dirección del flujo de paquetes. Sin embargo, los atacantes con acceso a una dirección IP externa segura o confiable pueden suplantar esa dirección, dejando a la arquitectura del firewall indefensa.
- **Especificación de enrutamiento en la fuente**—Este tipo de ataque se centra alrededor de todo el enrutamiento que un paquete IP debe tomar cuando atraviesa internet desde el host de origen hasta el host de destino. En este proceso, es posible definir la ruta de manera que evita el firewall. Sin embargo, el atacante debe conocer la dirección IP, la máscara de subred y la puerta de enlace predeterminada para lograr esto. Una defensa clara en contra de este ataque es examinar cada paquete y descartar aquellos que tienen la Especificación de enrutamiento en la fuente habilitada. Tenga en cuenta que esta contramedida no será efectiva si la topología permite una ruta que se salta el choke point (cuello de botella).
- **Ataque de paquetes fragmentados en miniatura (Miniature fragment attack)**—Mediante este método, un atacante fragmenta el paquete IP en unos más pequeños y los envía a través del firewall. Esto se hace con la esperanza de que sólo la primera secuencia de paquetes fragmentados será examinada, permitiendo al resto pasar sin revisión. Esto sólo es posible si la configuración predeterminada permite dejar pasar paquetes residuales. Los ataques de paquetes fragmentados en miniatura pueden ser contrarrestados mediante la configuración del servidor de seguridad para descartar todos los paquetes donde está habilitada la fragmentación IP.

SISTEMAS DE FIREWALL DE APLICACIÓN

Los enrutadores de filtrado de paquetes permiten el flujo directo de paquetes entre los sistemas interno y externo. El riesgo primario de permitir el intercambio de paquetes entre los sistemas interno y externo es que las aplicaciones anfitrionas (host) que residen en los sistemas protegidos de la red deben ser aseguradas contra cualquier amenaza que planteen los paquetes admitidos.

En contraposición a los routers de filtrado de paquetes, las pasarelas (gateways) de aplicación y de nivel de circuito permiten que la información fluya entre sistemas, pero no permiten el intercambio directo de paquetes. Por lo tanto, los sistemas de firewall de aplicación proporcionan mayores capacidades de protección que los routers de filtrado de paquetes.

Los dos tipos de sistemas de firewall de aplicación se montan sobre sistemas operativos reforzados (es decir, bien seguros) como Windows® y UNIX®. Éstos trabajan a nivel de aplicación del modelo OSI.

Los dos tipos de sistemas de Firewall de aplicación son:

- **Gateways de nivel de aplicación**—Los gateways de nivel de aplicación son sistemas que analizan los paquetes a través de un conjunto de servidores proxy -uno para cada servicio (por ejemplo, el Protocolo de transmisión de hipertexto [HTTP] proxy para el tráfico web, proxy FTP). La implementación de múltiples servidores proxy, sin embargo, impacta el rendimiento de la red. Cuando el rendimiento de la red es una preocupación, un gateway de nivel de circuito puede ser una mejor opción.

- **Gateways de nivel de circuito**—Comercialmente, los gateways de nivel de circuito son bastante raros. Debido a que utilizan un servidor proxy para todos los servicios, son más eficientes y también operan a nivel de aplicación. Allí, las sesiones TCP y UDP se validan, por lo general a través de un único proxy de propósito general, antes de abrir una conexión. Esto difiere de las gateways de nivel de aplicación, las cuales requieren un proxy especial para cada servicio de nivel de aplicación.

Ambos emplean el concepto de servidor expuesto (bastion hosting) en que manejan todas las solicitudes entrantes provenientes de Internet a la red corporativa como por ejemplo las solicitudes de FTP y de la Web. Los servidores expuestos están muy fortificados contra los ataques. Cuando sólo hay un host manejando las peticiones entrantes, es más fácil mantener la seguridad y rastrear los ataques. En el caso de un robo, sólo el sistema de firewall está comprometido, no toda la red.

De esta manera, ninguno de los equipos o sistemas de la red corporativa puede ser contactado directamente para solicitudes desde Internet, lo cual proporciona un nivel o capa de seguridad efectivo.

Adicionalmente, los sistemas de cortafuegos (firewall) basados en aplicaciones están configurados como servidores proxy para actuar en nombre y representación de alguien que está dentro de la red privada de una organización. En lugar de basarse en una herramienta genérica de filtrado de paquetes para gestionar el flujo de los servicios de Internet a través del firewall, se incorpora en el sistema de firewall un código específico llamado servidor proxy. Por ejemplo, cuando alguien dentro de la red corporativa quiere acceder a un servidor en Internet, una solicitud desde el ordenador se envía al servidor proxy. El servidor proxy contacta al servidor de Internet y el servidor proxy envía la información desde el servidor de Internet a la computadora dentro de la red corporativa. Al actuar como un intermediario, los servidores proxy pueden mantener la seguridad examinando el código de programa de un determinado servicio (por ejemplo, FTP, Telnet). A continuación, los modifica y lo asegura para eliminar vulnerabilidades conocidas. El servidor Proxy puede también registrar todo el tráfico entre Internet y la red.

Una de las características disponibles en los dos tipos de sistemas de firewall es la capacidad de traducción de direcciones de red (NAT). Esta capacidad toma las direcciones de red internas privadas, que no son utilizables en Internet, y las asigna a una tabla de direcciones IP públicas asignadas a la organización, que se pueden utilizar a través de Internet.

Los firewalls de aplicación tienen ventajas y desventajas, como se muestra en la **figura 3.11**.

Figura 3.11—Firewall de aplicación

Ventajas	Desventajas
Proporcionan seguridad para los protocolos usados con más frecuencia	Reducción de rendimiento y escalabilidad conforme crece el uso de internet
Por lo general esconden la red de redes externas no confiables	
Tienen la habilidad de proteger toda la red a limitar los robos a la misma firewall	
Tienen la habilidad de examinar y asegurar el código de programar	

FIREWALLS DE INSPECCIÓN DE ESTADO

Un firewall de inspección de estado, también conocido como el filtrado de paquetes dinámico, hace un seguimiento de la dirección IP de destino de cada paquete que sale de la red interna de la organización. Cada vez que se recibe una respuesta a un paquete, se hace referencia a su registro para determinar si el mensaje entrante se hizo en respuesta a una solicitud que la organización envió. Esto se hace correlacionando la dirección IP de origen del paquete entrante con la lista de direcciones IP de destino, que es mantenida y actualizada. Este enfoque previene cualquier ataque iniciado y originado por un extraño.

En contraste con los firewalls de aplicaciones, los firewalls de inspección de estado proporcionan control sobre el flujo de tráfico IP. Lo hacen mediante el pareo de la información contenida en los encabezados de paquetes IP orientados a la conexión o sin conexión en la capa de transporte, contra un conjunto de normas autorizadas por la organización. En consecuencia, tienen ventajas y desventajas, como se muestra en la **figura 3.12**.

Figura 3.12—Firewall de inspección de estado	
Ventajas	Desventajas
Proporcionan un mayor control sobre el flujo de tráfico IP	Son complejas de administrar
Mayor eficiencia en el intensivo de CPU, en comparación con los sistemas de firewall de aplicación de tiempo completo	

SIN ESTADO VS. CON ESTADO

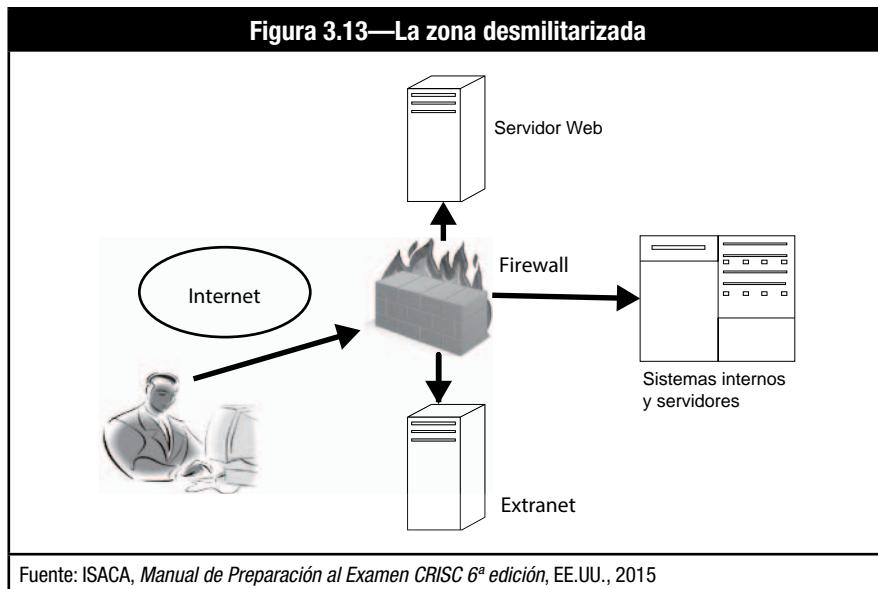
El filtrado sin estado no mantiene el estado de las sesiones de conexión TCP en curso. En otras palabras, no tiene memoria de qué números de puerto de origen el cliente de la sesión seleccionó. Los firewalls con estado mantienen un seguimiento de las conexiones TCP. El firewall mantiene una entrada en caché para cada conexión TCP abierta. Los firewalls sin estado tienen un rendimiento superior al de los firewalls con estado, pero no son tan sofisticados.

Como el tráfico UDP no tiene estado, las aplicaciones que requieren de éste para operar desde Internet a la red corporativa deben ser usadas con moderación e implementando controles alternativos (p.ej. la segregación de redes o el uso de firewalls de aplicación, NGFWs e IDS/IPS).

EJEMPLOS DE IMPLEMENTACIONES DE FIREWALL

Las implementaciones de firewalls pueden sacar provecho de la funcionalidad disponible en una variedad de diseños de firewalls para proveer un enfoque por capas robusto para proteger los activos de información de una organización. Las implementaciones comúnmente usadas, que están disponibles en la actualidad incluyen los siguientes:

- **Cortafuegos (firewall) de servidor (host) de filtrado (Screened-host Firewall)**—Este enfoque, que utiliza un enrutador de filtrado de paquetes y un servidor expuesto (bastion host), implementa la seguridad básica de capas de red (filtrado de paquetes) y una seguridad de servidor de aplicación (servicios de proxy). Un intruso en esta configuración debe penetrar dos sistemas separados antes de que la seguridad de la red privada pueda ser comprometida. Este sistema de firewall está configurado con el servidor expuesto conectado a la red privada, mientras que un router de filtrado de paquetes está entre Internet y el servidor expuesto. Las reglas de filtrado del router permiten el tráfico de entrada para acceder sólo al servidor expuesto, el cual bloquea el acceso a los sistemas internos. Debido a que los hosts internos residen en la misma red que el servidor expuesto, la política de seguridad de la organización determina si a los sistemas internos se les permite el acceso directo a Internet, o si se les exige que usen los servicios proxy en el servidor expuesto.
- **Firewall de base dual (dual-homed firewall)**—Este es un sistema de firewall que tiene dos o más interfaces de red, cada una de las cuales está conectada a una red diferente. Un firewall de base dual generalmente actúa para bloquear o filtrar total o parcialmente el tráfico que trata de pasar entre las redes. Un sistema de firewall de base dual es una variante más restrictiva de un sistema de screened-host firewall en el cual un servidor expuesto de base dual está configurado con una interfaz establecida para servidores de información y otra para equipos host de la red privada.
- **Firewall de zona desmilitarizada (DMZ) o firewall de subred proyectada (screened-subnet firewall)**—Como se muestra en la **figura 3.13**, esta es una red pequeña, aislada de los servidores públicos de una organización, los servidores de información de servidor expuesto y grupos de módem. La DMZ conecta la red no fiable a la red de confianza, pero existe en su propio espacio independiente para limitar el acceso y la disponibilidad de recursos. Como resultado, los sistemas externos pueden acceder sólo al servidor expuesto y posiblemente servidores de información en la DMZ. El router interno gestiona el acceso a la red privada, aceptando sólo el tráfico originado desde el servidor expuesto. Las reglas de filtrado en el enrutador externo requieren el uso de servicios de Proxy aceptando únicamente el tráfico saliente en el servidor expuesto. Los beneficios clave de este sistema son que un intruso debe penetrar tres dispositivos separados, las direcciones de red privada no son reveladas a Internet y los sistemas internos no tienen acceso directo a Internet.



PROBLEMAS DEL FIREWALL

Los problemas que enfrentan las organizaciones que han implementado los firewalls incluyen los siguientes:

- **Errores de configuración**—Los firewalls mal configurados pueden permitir que servicios desconocidos y peligrosos pasen libremente.
- **Demandas de monitorización**—Es necesario aplicar y revisar la configuración de la bitácora (log) adecuadamente, sino las actividades de vigilancia podrían no siempre ocurrir regularmente.
- **Mantenimiento de políticas**—Las políticas de firewall podrían no mantenerse con regularidad.
- **La vulnerabilidad a los ataques basado en aplicaciones y en entrada de datos**—La mayoría de los firewalls operan en la capa de red; por lo tanto, no detienen ataques basados en aplicaciones o basados en la introducción de datos, como la inyección de SQL y los ataques de desbordamiento de búfer. La generación más reciente de firewalls es capaz de inspeccionar el tráfico a nivel de la capa de aplicación y parar algunos de estos ataques.

PLATAFORMAS DE FIREWALL

Los firewalls pueden ser implementados usando plataformas de hardware, de software o virtuales. La implementación basada en hardware proporcionará rendimiento con una mínima sobrecarga del sistema. Aunque las plataformas de firewalls basados en hardware son más rápidas, no son tan flexibles o escalables como los firewalls basados en software. Los firewalls basados en software son generalmente más lentos y sobrecargan significativamente los sistemas. Sin embargo, son flexibles y tienen servicios adicionales; por ejemplo, pueden incluir comprobación de contenido y de virus antes de pasar el tráfico a los usuarios.

Generalmente, para firewalls es mejor usar equipos dedicados (appliances), en lugar de servidores convencionales. Un appliance es un dispositivo cuyo software y configuración vienen preinstalados en un servidor físico que está conectado entre dos redes. Los appliances son normalmente instalados con sistemas operativos reforzados. Cuando se usan firewalls basados en servidores, los sistemas operativos de éstos son a menudo vulnerables a ataques. Cuando los ataques a los sistemas operativos tienen éxito, el firewall puede verse comprometido. En general, los firewalls de tipo appliance son significativamente más rápidos de instalar y también más rápidamente recuperables.

FIREWALL DE NUEVA GENERACIÓN^{37, 38, 39, 40}

NGFWs (del inglés Next Generation Firewall) son cortafuegos que tienen como objetivo hacer frente a dos limitaciones clave relativas a las variantes anteriores: 1) la incapacidad para inspeccionar la carga útil del paquete y 2) la incapacidad para distinguir entre tipos de tráfico web. Un NGFW es un sistema de seguridad de red adaptable capaz de detectar y bloquear ataques sofisticados. Los NGFWs suelen realizar funciones tradicionales, como el filtrado de paquetes, la inspección de estado y la traducción de direcciones de red (NAT), pero introducen el conocimiento a nivel de la capa de aplicación, incorporan la tecnología de inspección profunda de paquetes (DPI) y ofrecen distintos grados de protección integral contra amenazas, como la prevención de pérdida de datos (DLP), el sistema de prevención de intrusiones (IPS), el filtrado web y la inspección SSL (Secure Sockets Layer) / SSH (Secure Shell).

El **conocimiento a nivel de la capa de aplicación (application awareness)** es “la capacidad de un sistema de mantener información sobre aplicaciones conectadas para optimizar su funcionamiento y el de los subsistemas que ejecutan o controlan.”⁴¹ Esto es importante porque la discriminación entre el tráfico legítimo y malicioso es cada vez más difícil en medio del aumento de los servicios web. La capacidad de un NGFW de diferenciar entre tipos de tráfico web tales como una aplicación web de negocios autorizada y un sitio de streaming de medios, independientemente del puerto o protocolo, ayuda al cumplimiento de las políticas corporativas, ofreciendo del mismo modo una visión de las actividades y el comportamiento del usuario.

La DPI permite comparación de la carga útil (payload) con las firmas de ataques conocidos, malware, etc. La DPI proporciona una gran cantidad de información sobre el tráfico lo cual ayuda a determinar que tráfico es normal, haciendo que la detección de anomalías sea más eficaz, sobre todo en las redes más complejas.

Dependiendo de su organización, se le puede solicitar revisar, recomendar o especificar soluciones de proveedores. Tenga en cuenta que, si bien muchas soluciones de próxima generación proclaman funciones similares, la forma en que lo hacen a menudo está basada en su interpretación de los conceptos y la aplicación de la tecnología propietaria. Aun con lo sofisticado que los firewalls de nueva generación puedan ser hoy en día, esta no debería ser su única línea de defensa.

FIREWALL DE APLICACIÓN WEB⁴²

Un firewall de aplicación web es un complemento de servidor, appliance o filtro adicional que puede ser empleado para aplicar reglas a una aplicación web específica (normalmente a una comunicación HTTP). Opera en los niveles más altos del modelo OSI, nivel 7 generalmente, mientras que los cortafuegos de red operan en los niveles 3 y/o 4. Puede ser personalizado para identificar y bloquear muchos tipos de ataques, como el Cross-site scripting (XSS) y la Inyección de SQL. La personalización de las reglas de un WAF requiere mucho trabajo y esfuerzo. Cuando se realizan cambios en la aplicación, las reglas del WAF deben ser cambiadas también.

³⁷ Ohlhorst, Frank, “Next-Generation Firewalls 101,” Network Computing, 1 de marzo 2013, www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097

³⁸ Miller, Lawrence C.; *Next-Generation Firewalls for Dummies*, Wiley Publishing, Inc., EE.UU., 2011

³⁹ Rouse, Margaret, “Next-generation firewall,” enero 2014, TechTarget, SearchSecurity, <http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW>

⁴⁰ My Digital Shield, “Firewalls Don’t Cut It Anymore – Why You Need Next Generation Firewalls,” 28 agosto 2014, www.mydigitalshield.com/firewalls-dont-cut-anymore-need-next-generation-firewalls

⁴¹ Wigmore, Ivy; “Application Awareness,” enero 2013, TechTarget, <http://whatis.techtarget.com/definition/application-awareness>

⁴² Open Web Application Security Project (OWASP), *Web Application Firewall*, www.owasp.org/index.php/Web_Application_Firewall

TEMA 5—ASILAMIENTO Y SEGMENTACIÓN

REDES DE ÁREA LOCAL VIRTUALES

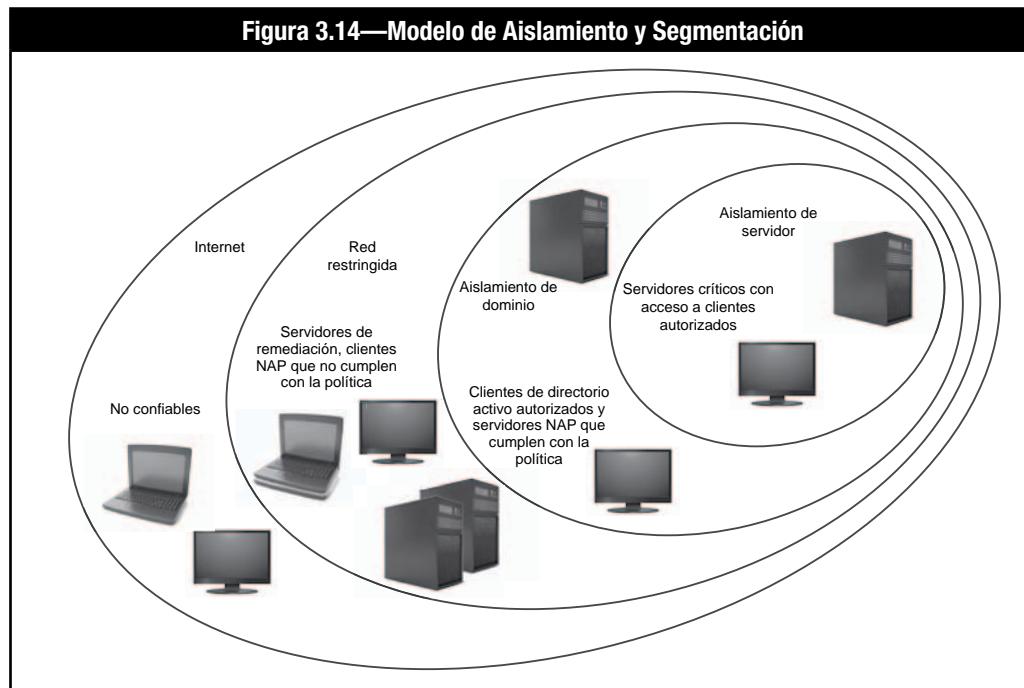
Una técnica común para la implementación de seguridad de la red es segmentar la red de una organización para que cada segmento se pueda controlar, monitorizar y proteger por separado. **Las Redes de área local virtuales (VLAN)** son grupos de dispositivos en una o más LAN segmentadas lógicamente, generalmente sin utilizar cifrado adicional.

Se establece configurando puertos en un conmutador, de modo que los dispositivos conectados con estos puertos puedan comunicarse como si estuvieran conectados al mismo segmento físico de red, a pesar de que están ubicadas en segmentos de LAN diferentes. La segmentación del tráfico de red de esta manera permite a una organización mantener diferentes tipos de datos separados el uno del otro.

Una VLAN se compone de conexiones lógicas en lugar de conexiones físicas y, por lo tanto, permite una gran flexibilidad. Esta flexibilidad permite a los administradores segmentar los recursos de red para obtener un rendimiento óptimo al restringir el acceso de los usuarios a los recursos de red sólo a las personas que lo requieren. En la conmutación de Capa 4 (capa de transporte OSI), parte de la información de aplicaciones se toma en cuenta junto con las direcciones de Capa 3. Para la capa de IP, esta información incluye los números de puerto de protocolos como TCP y UDP. Estos dispositivos, a diferencia de los switches de capa 3, tienen un mayor uso de recursos porque tienen que almacenar información de protocolo basada en aplicaciones. Sólo la información de direccionamiento se almacena en las capas 2 y 3.

ZONAS DE SEGURIDAD Y ZONAS DESMILITARIZADAS

Mediante la creación de zonas separadas, los controles pueden ser aplicados a un nivel más granular basado en los sistemas, la información y las aplicaciones en cada área. Las zonas separadas pueden crear una defensa en profundidad, donde se pueden implementar capas adicionales de autenticación, control de accesos y vigilancia. El aislamiento y la segmentación se muestran en la **figura 3.14**.



La mayoría de las organizaciones separan sus sistemas internos de Internet mediante un servidor de seguridad o firewall. Sin embargo, algunos sistemas y servicios, tales como los servidores web, deben estar disponibles fuera de la red interna. Esto se puede lograr con un segmento de red llamado una **zona desmilitarizada (DMZ)**, dentro del cual se instalan una cantidad acotada de sistemas, aplicaciones y datos en un segmento conectado al público. Los servidores ubicados en una DMZ minimizan la exposición a ataques.

La DMZ funciona como una red pequeña y aislada para los servidores públicos de una organización, para puntos de terminación de las Redes privadas virtuales (VPN) y para bancos de módems. Típicamente, las DMZ están configuradas para limitar el acceso desde Internet y desde la red privada de la organización. El acceso de tráfico entrante está restringido en la red DMZ por el enrutador externo y el por firewall, protegiendo así la organización contra ciertos ataques mediante la limitación de los servicios disponibles para su uso. En consecuencia, los sistemas externos únicamente pueden acceder a aquellos ubicados en la DMZ.

Página dejada en blanco intencionadamente

TEMA 6—REGISTRO, MONITORIZACIÓN Y DETECCIÓN

La monitorización, la detección y el registro son partes integrantes de la ciberseguridad. Con posibles ataques potenciales y pérdida de información en ambas partes, es necesario monitorizar los datos e información que fluye hacia dentro y fuera de la organización. Como se ilustra en este tema, hay una cantidad de métodos y herramientas que una organización puede usar para detectar y registrar problemas potenciales. La mayoría de estos métodos tienen que ver con los conceptos centrales de comunicaciones de ingreso y salida de la red y la prevención de pérdida de datos.

REGISTRO⁴³

Un registro de log es un historial de los acontecimientos que ocurren dentro de los sistemas y las redes de una organización. Los registros de log representan una de las herramientas más valiosas para monitorizar controles y detectar riesgos, pero a menudo son infráutilizados. Un registro de log debería contener un historial de todos los acontecimientos importantes que ocurren en un sistema, incluyendo:

- Hora del evento
- Cambios en los permisos de un archivo
- Arranque o parada de un sistema
- Acceso o salida de un usuario en un sistema
- Cambios en los datos
- Errores y violaciones
- Tareas fallidas

Las revisiones de registros de log pueden identificar acontecimientos de riesgo relevantes como violaciones en el cumplimiento de políticas, comportamientos sospechosos, errores, sondeos o escaneos, y actividades anormales. Un fallo en la revisión de los registros de log puede tener como resultado que la organización no tenga conocimiento de que se esté llevando a cabo un ataque. Los registros de log pueden ser requeridos en cumplimiento de la legislación y del marco regulatorio y deben ser preservados para un análisis forense posterior en caso de ser necesario. El profesional de la ciberseguridad puede encontrar útil el uso de herramientas de análisis durante la revisión de los registros de log, con el fin de filtrar los datos pertinentes.

Asegurar una segregación de funciones apropiada y la sincronización horaria es particularmente importante cuando se trata de archivos de registro de log. La capacidad de cambiar configuraciones de sistema debería segregarse de la capacidad de revisar, modificar o suprimir registros de log, con el fin de asegurar que la organización puede ejercer una supervisión apropiada de las funciones administrativas. Sin sincronización horaria es extremadamente difícil correlacionar la información de diferentes registros de log (servidor, router, firewall) para analizar la aparición de un evento.

Los retos más comunes relativos al uso efectivo de los registros de log incluyen:

- Tener demasiados datos
 - Dificultad en la búsqueda de información relevante
 - Configuración inapropiada (p.ej. no estar habilitados o no tener los datos apropiados)
- Modificación o borrado de datos antes de su lectura (p.ej. espacio de almacenamiento demasiado pequeño)

SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE EVENTOS

Para prepararse ante un incidente e identificarlo, las organizaciones utilizan una gran variedad de herramientas de seguridad, tales como evaluaciones de vulnerabilidades, firewalls y sistemas de detección de intrusiones (IDS), que recogen un gran volumen de datos. Sin embargo, los equipos de seguridad tienen que analizar e interpretar esta abrumadora cantidad de datos, denominada sobrecarga de datos de registro de log. Una solución emergente a este problema es la gestión de eventos de seguridad (del inglés Security Event Management, SEM). Los sistemas SEM agregan y correlan de forma automática los datos de registro de eventos de seguridad a través de múltiples dispositivos de seguridad. Esto permite a los analistas de seguridad centrarse en una lista manejable de eventos críticos.

Los incidentes de seguridad a menudo están compuestos por una serie de eventos que se producen en toda una red. Al correlar datos, el SEM puede coger muchos eventos aislados y combinarlos para crear un solo incidente de seguridad relevante. Estos sistemas utilizan tanto la correlación basada en reglas como la estadística. Las correlaciones basadas en reglas crean reglas específicas para cada situación, estableciendo un patrón de eventos. La correlación estadística utiliza algoritmos para calcular los niveles de amenaza incurridos por los acontecimientos relevantes sobre diversos activos de TI.

⁴³ ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

Hay una gran variedad de soluciones SEM disponibles que proporcionan monitorización en tiempo real, correlación de eventos, notificaciones y vistas de consola. Además, los sistemas de gestión de eventos y seguridad de la información (SIEM) toman las capacidades de los SEM y las combinan con características de análisis histórico e informes de los sistemas de gestión de la información de seguridad (SIM).

Los equipos de seguridad de la información deben analizar periódicamente las tendencias encontradas de los sistemas SEM o SIEM, tales como los tipos de ataques intentados o los recursos que son objetivo con más frecuencia. Esto permite a la organización investigar los incidentes, así como asignar los recursos adecuados para prevenir futuros incidentes.

Una organización que usa a menudo SIEM para monitorización y detección es un Centro de operaciones de seguridad (del inglés Security Operation Center, SOC). Un SOC es un equipo organizado creado para mejorar la postura de seguridad de una organización y responder a incidentes de seguridad.⁴⁴

INGRESS, EGRESS Y PREVENCION DE PERDIDA DE DATOS

Hay dos tipos de vectores de ataque: de entrada (Ingress) y de salida (Egress) (también conocido como exfiltración de datos). **Ingress** se refiere a las comunicaciones de la red que entran, mientras **Egress** se refiere a las comunicaciones de la red que salen. Mientras que la mayoría de los análisis de ataques se concentran en el ingreso o intrusión dentro de los sistemas, si la meta del adversario es el robo de información o datos, entonces es importante considerar el vector o camino para sacar los datos de los sistemas y redes del propietario. El software para la prevención de pérdida de datos (DLP) es útil en este aspecto. Un programa exitoso de prevención de pérdida de datos ayuda a la organización a proteger su información y prevenir la exfiltración de datos sensibles.

La soluciones DLP fuertes cubren tres estados primarios de la información. **Datos en reposo** se refiere a los datos almacenados. Las soluciones DLP deben ser capaces de registrar dónde son almacenados varios tipos de archivos. Las aplicaciones gusano (crawler) exploran la información de estos archivos buscando datos sensibles como números de la seguridad social o información de tarjetas de crédito. Estos gusanos determinan si la ubicación del almacenamiento sigue reglas predefinidas.

Datos en tránsito se refiere a los datos que viajan a través de la red. La inspección profunda de paquetes (DPI) se usa para analizar los datos con contenido sensibles. Las soluciones DLP pueden alertar, manejar e incluso bloquear, poner en cuarentena o encriptar información controlada basada en controles.

Finalmente, las buenas soluciones DLP manejan los **datos en uso**, los cuales son datos en movimiento, a nivel de la estación de trabajo del usuario. Estos incluyen el envío de información a las impresoras, memorias USB o incluso la copia y pegado en el portapapeles. Las soluciones DLP usan agentes de software para establecer las reglas de uso de los datos. Los tres tipos de información, datos en reposo, datos en movimiento y datos en uso, deben ser considerados para crear una solución de DLP completa.

ANTIVIRUS Y ANTI-MALWARE

El software malicioso es uno de los vectores de ataque más comunes usados por los adversarios para comprometer los sistemas. Por lo tanto, ciertos controles son requeridos para su detección y prevención.

Históricamente, controles de anti-malware, frecuentemente conocidos como detectores de virus, eran aplicaciones a nivel de servidor que escaneaban el tráfico de entrada, como los emails, y buscaban patrones (firmas) que identificaban los problemas conocidos. Mientras que ésto puede ser efectivo para ciertas amenazas, no puede detectar códigos maliciosos que aún están por identificar.

Los métodos heurísticos para detectar malware desconocido usan técnicas específicas para identificar códigos de comportamiento maliciosos comunes y marcarlos como sospechosos.

El anti-malware puede ser controlado a través de diferentes mecanismos, incluyendo:

- Restricción del tráfico de salida, para prevenir que el malware pueda exfiltrar datos o comunicarse con los sistemas de control usados por el adversario.
- Políticas y concienciación que preparen a los usuarios a evitar abrir emails sospechosos o archivos adjuntos y poder reconocer los localizadores uniformes de recursos (URL) que pueden introducir códigos maliciosos.
- Múltiples capas de software anti-malware que usan una combinación de identificación de firmas y un análisis heurístico para identificar posibles códigos maliciosos.

⁴⁴ Paganini, Pierluigi, "What is a SOC (Security Operations Centers)?," Security Affairs, 24 mayo 2016, <http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html>

SISTEMA DE DETECCIÓN DE INTRUSIONES⁴⁵

Otro elemento para securizar las redes que complementa las implementaciones de firewall es un Sistema de detección de intrusiones (del inglés Intrusion Detection System, IDS). Un IDS funciona junto con enrutadores y con cortafuegos monitorizando las anomalías en el uso de la red. Protege los recursos de los sistemas de información (SI) de una compañía tanto de abusos externos como internos. Un IDS opera de manera continua en el sistema, ejecutándose en segundo plano (background) y notificando a los administradores cuando detecta una amenaza percibida. Las amplias categorías de IDSs incluyen:

- **IDSs basados en la red**—Identifican ataques dentro de la red monitorizada y mandan un aviso al operador. Si un IDS basado en la red está puesto entre internet y el firewall, detectará todos los intentos de ataques, sin importar si entran o no al firewall. Si el IDS está puesto entre el firewall y la red corporativa, detectará los ataques que entran al firewall, es decir, detectará a los intrusos. El IDS no es un substituto de un firewall, sino que complementa su función.
- **IDSs basados en host**—Estos están configurados para un ambiente específico y monitorizarán los distintos recursos internos del sistema operativo para advertir sobre un posible ataque. Pueden detectar la modificación o ejecución de archivos y emitir un aviso cuando se intenta ejecutar un comando privilegiado.

Los componentes de un IDS son:

- Sensores responsables de la recolección de datos en forma de paquetes de red, registro de archivos, rastreo de sistema de llamadas, etc.
- Los analizadores que reciben la información entrante proveniente de los sensores y que determinan la actividad de intrusos
- Una consola de administración

Los tipos de IDS incluyen:

- **Basados en firmas**—Estos sistemas de IDS protegen contra los patrones de intrusión detectados. Los patrones de intrusión que pueden identificar son almacenados en forma de firmas.
- **Basados en estadísticas**—Estos sistemas necesitan una definición detallada del comportamiento conocido y esperado de los sistemas.
- **Redes neuronales**—Un IDS que tiene esta característica monitoriza los patrones generales de actividad y de tráfico en la red y crea una base de datos. Es similar al modelo estadístico pero con una funcionalidad de auto aprendizaje.

Los IDS basados en firmas no son capaces de detectar todos los tipos de intrusiones debido a limitaciones en sus reglas de detección. Por otro lado, los sistemas basados en estadísticas pueden reportar muchos eventos fuera de la actividad normal definida que siguen siendo actividades normales en la red. Una combinación de modelos basados en firmas y en estadísticas provee una mejor protección.

Características de los IDS

Las características disponibles en un IDS incluyen:

- Detección de intrusos
- Habilidad para recolectar evidencias de una actividad intrusiva
- Respuesta automatizada (por ejemplo: terminación de la conexión, mensaje de alerta)
- Política de seguridad
- Interfaz con las herramientas del sistema
- Gestión de política de seguridad

Limitaciones de los IDS

Un IDS no puede ayudar en las siguientes debilidades:

- Debilidad en la definición de las políticas (ver sección de Políticas)
- Vulnerabilidades en el nivel de aplicación
- Puertas traseras de las aplicaciones
- Debilidades en la identificación y en la autenticación de esquemas

⁴⁵ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

Políticas de IDS

Una política de IDS debe establecer la acción a llevar a cabo por el personal de seguridad en el caso de que se detecte un intruso.

Las acciones incluyen:

- **Interrumpir el acceso**—Si hay un riesgo significativo para los sistemas o datos de la organización, la interrupción inmediata es el procedimiento habitual.
- **Rastrear el acceso**—Si el riesgo para los datos es bajo, la actividad no se ve amenazada de inmediato o es recomendable analizar el punto de entrada y método de ataque, el IDS se puede usar para rastrear el origen de la intrusión. Esto puede ser usado para determinar y corregir cualquier debilidad del sistema y para recolectar evidencias del ataque, que puedan ser usadas en una subsecuente acción judicial.

En cualquier caso, la acción requerida debe ser determinada con antelación por la administración e incorporada dentro de un procedimiento. Esto ahorrará tiempo cuando se detecte una intrusión, lo cual puede impactar en la posible pérdida de datos.

SISTEMAS DE PREVENCIÓN DE INTRUSOS

Un IPS (Sistema de Prevención de Intrusiones) es un sistema diseñado no solo para detectar ataques, sino también para prevenir que los servidores víctimas se vean afectados por dichos ataques. Un IPS complementa las herramientas de firewall, antivirus y antispyware para proveer una protección más completa contra las amenazas emergentes.

La tecnología IPS se ubica normalmente en el perímetro de la red corporativa, en todos los puntos de entrada/salida, para examinar los flujos de tráfico de red y prevenir ataques zero-day, como gusanos y virus. Los métodos de detección empleados por un IPS son reglas basadas en anomalías e inspección basada en firmas de los paquetes de red. Un IPS bien gestionado ayuda a asegurar que las amenazas son rechazadas en el perímetro de la red; un IDS proporciona visibilidad y confirmación de la actividad interna en los nodos críticos de red.

La mayor ventaja de un IPS es que puede bloquear un ataque cuando ocurre; en lugar de simplemente mandar una alerta, ayuda activamente a bloquear tráfico malicioso y no deseado.

Sin embargo, al igual que con un IDS, el IPS debe estar debidamente configurado y ajustado para ser efectivo. Los valores de configuración del umbral que sean demasiado altos o demasiado bajos conducirán a una efectividad limitada del IPS. Adicionalmente, se han levantado sospechas de que un IPS puede constituir una amenaza en sí mismo, ya que un atacante inteligente podría enviar comandos a un gran número de hosts protegidos por un IPS con el fin de provocar su mal funcionamiento. Esa situación podría tener un resultado potencialmente catastrófico en el típico ambiente de computación corporativo de hoy en día, donde la continuidad del servicio es crítica. Además, los IPS pueden generar falsos positivos que provoquen serios problemas si se emplean respuestas automáticas.

TEMA 7—FUNDAMENTOS, TÉCNICAS Y APLICACIONES DE CIFRADO

El **cifrado** es el proceso de convertir un mensaje en texto plano en una forma codificada segura de texto, llamado texto codificado. El texto codificado no puede ser entendido sin convertirlo de vuelta, a través del descifrado - el proceso inverso - a un texto plano. Esto se hace vía función matemática y con una contraseña especial requerida para el descifrado llamada clave. En muchos países, el cifrado está sujeto a leyes gubernamentales y regulaciones que limitan el tamaño de la clave o definen lo que no puede ser encriptado.

El cifrado es parte de una ciencia más amplia de lenguajes secretos llamada criptografía, la cual es generalmente usada para:

- Proteger la información almacenada en las computadoras contra la visualización y manipulación no autorizadas
- Proteger los datos que viajan a través de las redes contra interceptación y manipulación no autorizadas
- Disuadir y detectar alteraciones accidentales o intencionales de los datos
- Verificar la autenticidad de una transacción o documento

El cifrado está limitado en el sentido que no puede prevenir la pérdida de datos. Es posible comprometer los programas de cifrado si las claves de cifrado no están protegidas adecuadamente. Por lo tanto, el cifrado debe ser visto como una forma esencial, pero incompleta, de control de acceso que debe ser incorporada dentro del programa de seguridad general de los ordenadores de una organización.

ELEMENTOS CLAVE DE SISTEMAS CRIPTOGRÁFICOS

Los elementos clave de los sistemas criptográficos incluyen:

- **Algoritmo de cifrado**—Función o cálculo basado en las matemáticas que cifra / descifra información.
- **Clave de cifrado**—Pieza de información similar a una contraseña que hace que el proceso de cifrado y descifrado sean únicos. Un usuario necesita la clave correcta para acceder o descifrar un mensaje, ya que una clave incorrecta convierte el mensaje en un texto ilegible.
- **Longitud de la clave**—La longitud predeterminada de la clave. Cuanto más larga sea la clave, más difícil será comprometerla en un ataque de fuerza bruta donde se prueban todas las combinaciones posibles de claves.

Los sistemas criptográficos efectivos dependen de una gran variedad de factores que incluyen:

- Fuerza del algoritmo
- Discreción y dificultad para comprometer una clave
- No existencia de puertas traseras mediante las cuales, un archivo cifrado puede ser descifrado sin conocer la clave
- Incapacidad de descifrar partes de un mensaje de texto codificado y así prevenir ataques de texto plano conocidos
- Propiedades de un texto plano conocido por un perpetrador

SISTEMAS DE CLAVES

Hay dos tipos de sistemas criptográficos:

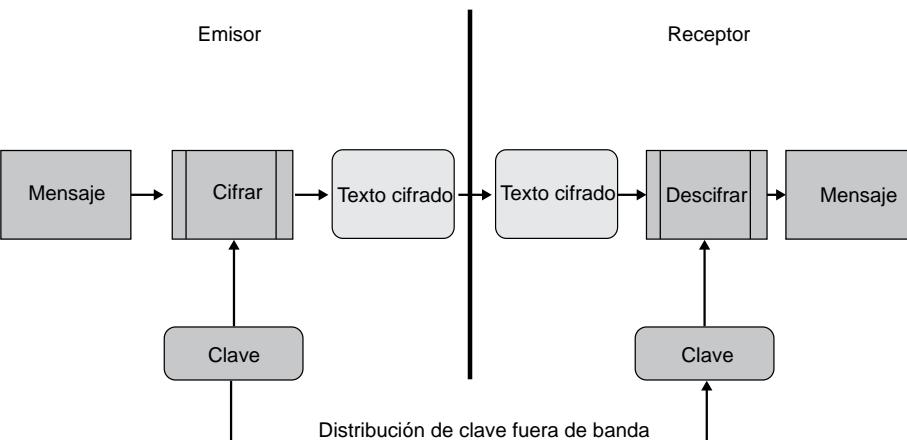
- **Sistemas de clave Simétrica**—Estos usan una clave única, secreta y bidireccional que cifra y descifra.
- **Sistemas de clave Asimétrica**—Estos usan pares de claves, unidireccionales y complementarias, una de las cuales cifra mientras que la otra descifra. Típicamente, una de estas claves es secreta, y la otra es públicamente conocida.

Los sistemas de clave pública son sistemas criptográficos asimétricos. La mayoría de las transacciones cifradas en internet usan una combinación de claves privadas y públicas, claves secretas, funciones hash (valores fijos derivados matemáticamente de un mensaje de texto) y certificados digitales (que prueban la posesión de una clave pública de cifrado) para lograr confidencialidad, integridad del mensaje, autenticación y no rechazo, ya sea por el remitente o destinatario (también conocida como infraestructura de clave pública PKI). Esencialmente, las claves y valores hash son usados para transformar una serie de caracteres en un valor más corto y de longitud definida o en una clave que represente el texto original. Este proceso de cifrado permite que los datos sean almacenados y transportados con una exposición reducida para que los datos permanezcan seguros mientras se mueven a través del Internet u otras redes.

CLAVE DE CIFRADO SIMÉTRICA (PRIVADA)

Los sistemas criptográficos de claves simétricas están basados en un algoritmo de cifrado simétrico, el cual utiliza una clave secreta para cifrar el texto plano a texto codificado y la misma clave para descifrar el texto codificado al texto plano correspondiente. En este caso, se dice que la clave es simétrica porque la clave de cifrado es la misma que la clave de descifrado. Un ejemplo de una criptografía simétrica se muestra en la **figura 3.15**.

Figura 3.15—Criptografía simétrica



Fuente: ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

El sistema criptográfico con clave simétrica más común solía ser el Estándar de Encriptación de Datos (DES). DES se basa en un algoritmo público aprobado por el Instituto Nacional de Normas y Tecnología (NIST) y emplea claves de 56 bits (más 8 bits adicionales usados para verificar la paridad). Los bits en el texto plano se procesan en bloques de 64 bits a la vez y, como tal, DES pertenece a la categoría de cifrado en bloque (en comparación con el cifrado en secuencia, que codifica un bit cada vez).⁴⁶

NIST retiró DES porque ya no se considera una solución criptográfica robusta, ya que todo su espacio completo de claves puede ser forzado por un sistema informático de gran tamaño en un período de tiempo relativamente corto. Se propusieron extensiones de DES (Triple DES o 3DES) para extender el estándar DES y retener la compatibilidad en sentido inverso (aplica el algoritmo de cifrado DES tres veces a cada bloque de datos).⁴⁷

En 2001, NIST reemplazó DES por el Estándar de Encriptación Avanzado (AES), un algoritmo público que soporta claves cuyo tamaño varía entre 128 y 256 bits. Otro algoritmo de clave simétrica que se usa comúnmente, aunque considerado frágil e inseguro, es RC4, un cifrado en secuencia que se utiliza a menudo en las sesiones de protocolos SSL/TLS.⁴⁸

Hay dos grandes ventajas en los sistemas de cifrado de clave simétrica tales como DES o AES:

- El usuario solo tiene que saber una clave tanto para el cifrado como el descifrado.
- Los sistemas criptográficos de clave simétrica son generalmente menos complicados y, por lo tanto, requieren menos capacidad de procesamiento que las técnicas asimétricas. Son ideales para el cifrado de datos masivo.

Las desventajas de este método incluyen:

- Dificultad en la distribución de las claves—Entregar las claves en mano a aquellos con los que quieras intercambiar datos puede ser un reto, particularmente en los entornos de comercio electrónico donde los clientes son entidades desconocidas y sin una relación de confianza.
- Limitaciones del secreto compartido—Una clave simétrica no puede ser usada para firmar documentos electrónicos o mensajes debido al hecho de que el mecanismo está basado en un secreto compartido.

Un algoritmo avanzado de cifrado se conoce como Triple DES o 3DES. Triple DES provee un método relativamente simple de incrementar el tamaño de la clave del DES para proteger la información sin la necesidad de diseñar un algoritmo de cifrado de bloque completamente nuevo.

⁴⁶ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

⁴⁷ Ibid.

⁴⁸ Ibid.

CLAVE DE CIFRADO ASIMÉTRICA (PRIVADA)

Los sistemas criptográficos de clave pública desarrollados para distribución de claves, resuelven el problema de proveer claves simétricas a dos personas que, no se conocen entre sí, pero quieren intercambiar información de forma segura. Basado en un proceso de cifrado asimétrico, dos claves trabajan en conjunto como una pareja. Una clave se usa para cifrar los datos; la otra se usa para descifrar los datos. Cualquiera de las claves puede ser usada para cifrar o descifrar, pero una vez que la clave ha sido usada para encriptar los datos, solo su compañera puede ser usada para desencriptarlos. La clave que fue usada para cifrar los datos no puede ser usada para desencriptarlos. De esta manera, las claves son asimétricas en el sentido que están inversamente relacionadas las unas con las otras.

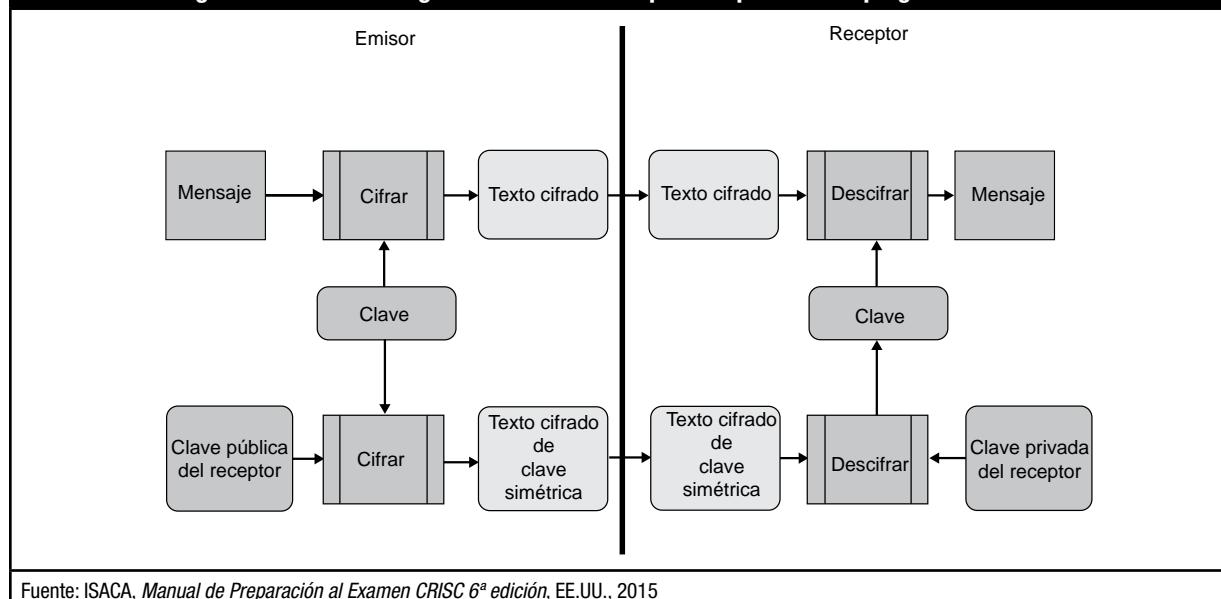
Las claves asimétricas son generalmente usadas para mensajes cortos, como cifrar las claves simétricas DES o crear firmas digitales. Si las claves asimétricas fueran usadas para cifrar datos masivamente (grandes mensajes), el proceso sería muy lento; esta es la razón por la que se usan en el cifrado de mensajes cortos, tales como compendios o firmas.

En el cifrado asimétrico, una de las claves – el secreto o clave privada – es conocida solo por una persona. La otra clave - la clave pública – es conocida por mucha gente. En otras palabras, un mensaje que ha sido enviado cifrado por la clave secreta (privada) del remitente puede ser descifrado por cualquiera con la clave pública correspondiente. De esta manera, si la clave pública descifra el mensaje satisfactoriamente, uno puede estar seguro del origen del mensaje porque solo el remitente (propietario de la clave privada correspondiente) pudo haber cifrado el mensaje. Esto forma una base de autenticación y no rechazo, ya que después el remitente no puede manifestar que él no generó el mensaje.

Un mensaje que ha sido enviado cifrado usando la clave pública del destinatario puede ser generado por cualquiera, pero solo puede ser leído por el destinatario. Esta es una de las bases de la confidencialidad. En teoría, un mensaje que ha sido cifrado dos veces, primero por la clave secreta del remitente, y segundo por la clave pública del destinatario, logra tanto los objetivos de autenticación como de confidencialidad, pero comúnmente no es usado porque puede generar problemas de rendimiento.

Una desventaja del uso de los algoritmos asimétricos es que suponen una mayor carga de proceso y son más lentos que los algoritmos simétricos. Por este motivo, el cifrado asimétrico se usa normalmente para cifrar únicamente mensajes cortos. De hecho, el uso más común de los algoritmos asimétricos es la distribución de claves simétricas pudiendo entonces ser empleadas por los participantes para una comunicación rápida y segura, tal y como se muestra en la **figura 3.16**.⁴⁹

Figura 3.16—Uso de algoritmos asimétricos para respaldar la criptografía simétrica



⁴⁹ ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

CRİPTOSISTEMA DE CURVA ELÍPTICA

Aunque la criptografía de clave pública garantiza la seguridad de los mensajes, las claves largas y los problemas matemáticos que usa tienden a ser ineficientes. Una forma alternativa y más eficiente de criptografía de clave pública es la criptografía de curva elíptica (ECC), la cual está ganando prominencia como método por incrementar la seguridad usando recursos mínimos. Se cree que la ECC demanda menos capacidad de proceso y por lo tanto ofrece más seguridad por bit. Por ejemplo una ECC con clave de un solo bit ofrece la misma seguridad que una RSA basada en sistema con clave de 1,204 bits.

La ECC trabaja bien con computadores en red que requieren una fuerte criptografía. Sin embargo, tiene algunas limitaciones como el ancho de banda y la capacidad de procesamiento.

CRİPTOGRAFÍA CUÁNTICA

La criptografía cuántica es la siguiente generación de criptografía que resolverá los problemas existentes asociados con los actuales sistemas criptográficos, específicamente la generación aleatoria y distribución segura de claves criptográficas simétricas. Está basada en la aplicación práctica de las características de los más pequeños “granos” de luz (fotones) y las leyes de la física que gobiernan su generación, propagación y detección.

FIRMA DIGITAL

Una **firma digital** es una identificación electrónica de una persona o entidad creada mediante un algoritmo de clave pública. Sirve como mecanismo para verificar la integridad de los datos y la identidad del remitente por parte del receptor. Para verificar la integridad de los datos, un algoritmo criptográfico de función de hashing, llamado checksum, es computarizado en contra de todo el mensaje o documento electrónico, el cual genera una pequeña cadena de valores de longitud fija, normalmente 128 bits. Este proceso, también conocido como algoritmo de firma digital, crea un resumen o suma de validación de bits (digest) del mensaje (por ejemplo: una versión extrapolada más pequeña del mensaje original).

Tipos comunes de algoritmos de suma de validación (digest) de mensajes son SHA-256 y SHA-512. Estos algoritmos son funciones de sentido único, a diferencia de los algoritmos de clave pública y privada. El proceso de crear una suma de validación de mensaje no se puede invertir. Están diseñados para aplicaciones de firma digital donde un gran documento electrónico o serie de caracteres, tales como un documento de texto, una hoja de cálculo, un registro de una base de datos, el contenido de un disco duro o una imagen JPEG, tienen que ser comprimidos de forma segura antes de ser firmados por una clave privada. Todos los algoritmos de resumen de mensaje (digest) toman un mensaje de longitud arbitraria y producen un resumen de mensaje de 128 bits.

El siguiente paso, el cual verifica la identidad del remitente, consiste en cifrar la suma de validación utilizando la clave privada del remitente, la cual “firma” el documento con la firma digital del remitente para verificar la autenticidad del mensaje. Para descifrarlo, el destinatario usa la clave pública del remitente, probando que el mensaje solamente pudo haber venido de él. Este proceso de autenticación del remitente es conocido como no repudio porque el remitente no puede después declarar que no generó el mensaje.

Una vez descifrado, el destinatario recalculará el hash usando el mismo algoritmo de función de hashing que se encuentra en el documento electrónico, comparando los resultados con lo que fue enviado, para asegurar la integridad del mensaje. Por lo tanto, la firma digital es un método criptográfico que asegura:

- **Integridad de los datos**—Cualquier cambio en el texto plano del mensaje acabaría con la imposibilidad del destinatario del mensaje de calcular el mismo hash del mensaje.
- **Autenticación**—El destinatario puede asegurar que el mensaje ha sido enviado por el remitente declarado ya que sólo el auténtico remitente tiene la clave secreta.
- **No repudio**—El remitente declarado no puede después negar la generación y envío del mensaje.

Las firmas digitales y el cifrado de clave pública son vulnerables a ataques de “hombre en el medio” de manera que las claves privada y pública de la firma digital del remitente pueden ser falseadas. Para protegerse de tales ataques, se ha diseñado una autoridad independiente de autenticación del remitente. La PKI desempeña la función de autenticar de forma independiente la validez de la firma digital del remitente y de las claves públicas.

APLICACIONES DE SISTEMAS CRIPTOGRAFICOS

El uso de criptosistemas por parte de las aplicaciones, por ejemplo en el email y transacciones de internet, generalmente requieren una combinación de parejas de claves públicas y privadas, claves secretas, funciones hash y certificados digitales. El propósito de aplicar estas combinaciones es lograr confidencialidad, integridad del mensaje o no repudio por parte del remitente o del destinatario. El proceso generalmente requiere que el remitente realice un hashing del mensaje dentro de un mensaje cifrado o codifique un pre-hash para mantener la integridad del mensaje, el cual se encripta usando la clave secreta del remitente para preservar la autenticidad, integridad y no repudio (p.ej. una firma digital).

Usando su clave secreta, el remitente cifrará el mensaje. Después, la clave secreta se cifrará con la clave pública del receptor, la cual ha sido validada a través del certificado digital del receptor y que otorga confidencialidad al mensaje. El proceso de recepción finaliza revirtiendo lo que ha sido hecho por parte del remitente. El destinatario usa su clave privada para descifrar la clave secreta del remitente. Usa la clave secreta para descifrar el mensaje, para exponerlo. Si el código pre-hash ha sido cifrado con la clave privada del remitente, el receptor verifica su autenticidad usando la clave pública contenida en el certificado digital del remitente y descifra el código pre-hash, el cual provee el no repudio al contenido del mensaje del remitente. Con el objetivo de garantizar la integridad, el receptor calcula un código post-hash, el cual debe ser igual al código pre-hash. Ejemplos específicos de este método o de variantes relacionadas se encuentran descritos abajo.

Seguridad de la capa de transporte (TLS)⁵⁰—La TLS es un protocolo criptográfico que proporciona comunicaciones seguras en Internet. TLS es un protocolo en la capa de sesión o conexión de uso generalizado para la comunicación entre los exploradores y los servidores de la web. Además de la privacidad en la comunicación, también proporciona autenticación de extremo. Los protocolos permiten que las aplicaciones cliente-servidor puedan comunicarse de una manera diseñada para prevenir el espionaje, la manipulación o la falsificación de mensajes

TLS involucra un número de etapas básicas:

- Negociación entre los pares para soporte del algoritmo
- Intercambio de clave pública, basada en encriptación y autenticación basada en certificados
- Cifrado de tráfico basado en cifrado simétrico

Durante la primera etapa, el cliente y el servidor negocian qué algoritmo criptográfico usarán. Las implementaciones actuales respaldan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA o Fortezza
- Para cifras simétricas: RC4, IDEA, Triple DES o AES
- Para funciones hash de una sola vía: SHA-1 o SHA-2 (SHA-256)

TLS se ejecuta en capas sobre el protocolo de transporte TCP y provee seguridad a los protocolos de aplicación, incluso si se utiliza más comúnmente con HTTP para formar un Protocolo seguro de transferencia de hipertexto (HTTPS). HTTPS es parecido a HTTP, solo que con una sesión encriptada vía protocolos TLS (o SSL). HTTPS sirve para asegurar páginas World Wide Web para aplicaciones. Además, en comercio electrónico, la autenticación se puede usar en actividades interempresariales (B-to-B) (para las que se autentican el cliente y el servidor) y en la interacción entre empresa y consumidor (B-to-C) (en la que sólo se autentica al servidor).

Además de TLS, el protocolo de capa segura de socket (SSL) también se usa ampliamente en las aplicaciones del mundo real, a pesar de que ahora se objeta su uso, ya que se descubrió una vulnerabilidad significativa en 2014. TLS es un desarrollo adicional de SSL, pero TLS y SSL no son intercambiables. La interoperabilidad de SSL y TLS es imposible.

Protocolo seguro de transferencia de hipertexto (HTTPS)—Como un protocolo de capa de aplicación, HTTPS transmite mensajes individuales o páginas de forma segura entre un cliente web y el servidor mediante el establecimiento de una conexión de tipo TLS. Usando la designación https:// en la URL en lugar de la estándar http://, HTTPS dirige el mensaje hacia un número de puerto seguro en lugar de la dirección de puerto web por defecto. Este protocolo utiliza las características de seguridad de SSL pero lo hace más bien como mensaje en lugar de un protocolo orientado a sesión.

⁵⁰ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

Red privada virtual (VPN)—Una VPN es una red privada segura que utiliza la infraestructura pública de telecomunicaciones para transmitir datos. En comparación con un sistema mucho más costoso de líneas propias o alquiladas que sólo pueden ser utilizadas por una compañía, las VPN son utilizadas por empresas tanto para extranets como para áreas amplias de Intranets. Utilizando cifrado y autenticación, una VPN cifra todos los datos que pasan entre dos puntos de Internet, manteniendo la privacidad y la seguridad. El cifrado se necesita para hacer la conexión virtual de forma privada. Una tecnología VPN usada comúnmente es el IPSec, que usa normalmente los algoritmos de cifrado DES, Triple DES o AES.

IPSec—IPSec se usa para la comunicación entre dos o más anfitriones (hosts), o dos o más subredes, o entre anfitriones (hosts) y subredes. Este protocolo de seguridad de paquetes en la capa de red IP establece VPNs a través de métodos de cifrado en modo transporte y túnel. Para el método de transporte, las porciones de datos de cada paquete - referidos como el Encapsulado de carga útil de seguridad (ESP) – son cifradas para alcanzar la confidencialidad. En el modo túnel, la carga útil de ESP y su cabecera son cifrados. Para alcanzar el no repudio, se aplica una cabecera de autenticación (del inglés authentication header, AH).

Estableciendo sesiones de IPSec en cualquier modo, se realizan asociaciones de seguridad (del inglés security associations, SA). Las SAs definen cuales son los parámetros de seguridad que deberían aplicarse entre las partes de la comunicación como algoritmos de cifrado, claves, vectores de inicialización, rango de vida de claves, etc.

Para incrementar la seguridad de IPSec, se usa cifrado asimétrico vía Asociación de Seguridad de Internet y el Protocolo de Administración de Clave / Oakley (ISAKMP/Oakley), el cual permite la administración de claves, uso de claves públicas, negociación, establecimiento, modificación y supresión de SAs y sus atributos. Para la autenticación, el remitente usa certificados digitales. La conexión se vuelve segura asegurando que se lleva a cabo la generación, autenticación y distribución de las SAs y las claves criptográficas.

Secure Shell SSH—SSH es un programa cliente-servidor que abre una sesión de línea de comandos segura y cifrada desde Internet para el acceso remoto. Similar a una VPN, SSH usa cifrado fuerte para proteger los datos, incluyendo contraseñas, archivos binarios y comandos de administración, que son transmitidos entre los sistemas de una red. SSH se implanta normalmente validando las credenciales de ambas partes vía certificados digitales. SSH es útil para asegurar los servicios Telnet y FTP. Se implanta en la capa de aplicación, lo cual difiere de la operación en la capa de red (tal y como ocurrió con la implementación IPSec).

Extensiones multipropósito seguras de correo de internet (S/MIME)—S/MIME es un protocolo estándar de seguridad de email que valida la identidad del remitente y del destinatario, verifica la integridad del mensaje y asegura la privacidad del contenido del mensaje, incluyendo los archivos adjuntos.

Transacción electrónica segura (SET)—SET es un protocolo desarrollado conjuntamente por VISA y MasterCard para securizar transacciones de pago entre todas las partes involucradas en las transacciones de tarjetas de crédito. Al ser una especificación de sistemas abiertos, SET es un protocolo orientado a aplicación que usa cifrado de confianza de terceros y procesos de firma digital por medio de una infraestructura PKI de instituciones de confianza de terceros, para manejar la confidencialidad de la información, la integridad de los datos, la autenticación del usuario de la tarjeta, la autenticación del vendedor y la interoperabilidad.

INFRAESTRUCTURA DE CLAVE PÚBLICA

Si un individuo quiere enviar mensajes o documentos electrónicos y firmarlos con una firma digital usando un sistema criptográfico de clave pública, ¿cómo puede distribuir la clave pública de forma segura? Si la clave pública es distribuida electrónicamente, puede ser interceptada y cambiada. Para prevenir que ésto ocurra, se usa un marco de referencia conocido como infraestructura de clave pública (PKI). PKI permite a una entidad reconocida expedir, mantener y revocar certificados de clave pública.

PKI permite a los usuarios interactuar con otros usuarios y aplicaciones para obtener y verificar identidades y claves desde fuentes de confianza. La implantación real de PKI varía de acuerdo a requerimientos específicos. Elementos clave de la infraestructura son los siguientes:

- **Certificados digitales**—Un certificado digital se compone de una clave pública e información acerca de la identificación del propietario de la clave pública. El propósito de los certificados digitales es asociar la clave pública con la identidad del individuo a fin de comprobar la autenticidad del remitente. Estos certificados son documentos electrónicos, digitalmente firmados por alguna entidad de confianza con su clave privada (transparente a los usuarios) que contiene información acerca del individuo y su clave pública. El proceso requiere que el remitente “firme” un documento adjuntando un certificado digital emitido por una entidad de confianza. El destinatario del mensaje y el certificado digital que lo acompaña confía en la clave pública de la autoridad de certificación (CA) de confianza (que se incluye con el certificado digital o se obtiene

separadamente) para autenticar el mensaje. El destinatario puede vincular el mensaje a una persona, no solo a una clave pública, por la confianza en esa entidad. El estado y valores del certificado del usuario actual deben incluir:

- Un nombre de usuario distintivo
- Una clave pública real
- El algoritmo usado para incorporar la firma digital dentro del certificado
- Un periodo de validez del certificado

• **Autoridad de certificación (CA)**—Una CA es una autoridad en una red que emite y gestiona credenciales de seguridad y claves públicas para la verificación o encriptación de firmas de mensajes. La CA avala la autenticidad del dueño de la clave pública. El proceso requiere una CA que toma la decisión de emitir un certificado basado en la evidencia o conocimiento adquirido al verificar la identidad del remitente. Como parte de la PKI, una CA consulta a una Autoridad de registro (RA) para verificar la información proveniente del solicitante del certificado digital. Si la RA verifica la información del solicitante, entonces la CA puede entonces emitir el certificado. Una vez verificada la identidad del remitente, la CA firma el certificado con su clave privada para distribuirlo al usuario. Una vez recibido, el usuario verificará la firma del certificado con la clave pública de la CA (por ejemplo, CAs tales como VeriSign™ emiten certificados a través de navegadores de Internet). La CA ideal está acreditada (alguien en quien el usuario confía) por el nombre o su posicionamiento clave. Un certificado siempre incluye la clave pública del propietario, la fecha de expiración y la información del propietario. Los tipos de CA pueden incluir:

- Organizacionalmente fortalecidas, tienen control coercitivo sobre aquellos individuos dentro de su alcance
 - De responsabilidad fortalecida, por ejemplo escogiendo opciones comerciales disponibles (tales como VeriSign) para obtener un certificado digital. La CA es responsable de gestionar el certificado a lo largo de todo su ciclo de vida.
- Elementos clave o subcomponentes de la estructura de la CA incluyen la Declaración de Prácticas de Certificación (del inglés certification practice statement, CPS), RAs y Listas de Revocación de Certificados (del inglés certificate revocation lists, CRLs).

• **Autoridad de registro**—Una RA es una autoridad en una red que verifica las peticiones de usuarios para solicitar un certificado digital y que a su vez solicita a una CA para que emita dicho certificado. Como entidad opcional y distinta de una CA, una RA sería usada por una CA con una gran base de clientes. Las CAs usan a las RAs para delegar algunas de las funciones administrativas asociadas con el registro y verificación de parte o toda la información que necesita una CA para emitir certificados o CRLs y para desempeñar otras funciones de administración de certificado. Sin embargo, aun con este acuerdo, la CA sigue siendo responsable de firmar certificados digitales o CRLs. Las RAs son parte de la infraestructura PKI. El certificado digital contiene una clave pública que se usa para cifrar mensajes y verificar firmas digitales. Si una RA no está presente en la estructura establecida de una PKI, se supone que la CA tiene el mismo tipo de funcionalidades que aquellas definidas para una RA. Las funciones administrativas que una RA particular lleva a cabo variarán de acuerdo a las necesidades de la CA, pero deben mantener el principio de establecer o verificar la identidad del subscriptor. Estas funciones pueden incluir lo siguiente:

- Verificar la información suministrada por el sujeto (funciones de autenticación personal)
- Verificar el derecho del sujeto a los atributos de certificado solicitados
- Verificar que el sujeto realmente posee la clave privada que está siendo registrada y que concuerda con la clave pública requerida por un certificado (generalmente denominada prueba de posesión [del inglés proof of possession, POP]).
- Notificar que se ha comprometido una clave o los casos de finalización donde se requiere la revocación.
- Asignar nombres con fines de identificación

Generar secretos compartidos para usar durante las fases de inicialización y elección de certificado del registro

- Iniciar el proceso de registro con la CA en nombre y representación de la entidad final objeto

- Iniciar el proceso de recuperación de clave.

Distribuir los tokens físicos (como por ejemplo smart cards) que contienen las claves privadas

- Lista de certificados revocados (CRL)—Es un instrumento para verificar la validez continua de los certificados por los que la autoridad de certificación (CA) es responsable. La CRL detalla los certificados digitales que ya no son válidos porque fueron revocados por la CA. El margen de tiempo entre dos actualizaciones es crítico y es también un riesgo durante la verificación de los certificados digitales
- Declaración de prácticas de certificación (del inglés certification practice statement, CPS)—CPS es un conjunto detallado de reglas que rigen las operaciones de las CAs. Provee un conocimiento del valor y la confianza de los certificados emitidos por una determinada CA en los siguientes términos:
 - Los controles de los que dispone una organización.
 - El método que usa para validar la autenticidad de los solicitantes de certificados.
 - Las expectativas de las CAs sobre cómo sus certificados van a ser utilizados.

DATOS ALMACENADOS

El cifrado es un modo efectivo y cada vez más práctico para limitar el acceso a la información confidencial mientras está almacenada. El método de protección tradicional - una contraseña - tiene debilidades inherentes y, en muchos casos, es fácilmente adivinable. Las listas de control de acceso (ACL) que definen quién tiene acceso también son efectivas, pero a menudo tienen que ser usadas conjuntamente con sistemas operativos o aplicaciones. Es más, las ACL no pueden prevenir un uso inadecuado de información por los administradores de los sistemas, ya que pueden tener un control total del ordenador. El cifrado puede eliminar este problema de seguridad, y también puede proteger los datos de los hackers quienes, por medio de software malicioso, pueden obtener los derechos de administración del sistema. El cifrado también ayuda a proteger datos cuando un ordenador o disco cae en manos equivocadas. Muchos programas de cifrado de emails también pueden ser aplicados a los datos almacenados. También hay algunos productos de cifrado que se enfocan en la protección de archivos para ordenadores y dispositivos móviles inteligentes.

RIESGO DEL CIFRADO Y PROTECCIÓN DE CLAVE

La seguridad de los métodos de cifrado descansa principalmente en el secreto de las claves. En general, cuanto más se usa una clave, más vulnerable se vuelve ante una amenaza. Por ejemplo, mediante fuerza bruta las herramientas de craqueo de contraseñas actuales para ordenadores personales, pueden averiguar en pocas horas cada una de las combinaciones posibles de claves de un algoritmo criptográfico de hashing con una clave de 40 bits.

La aleatoriedad en la generación de claves también es un factor significativo a la hora de comprometer una clave. Cuando las contraseñas se encuentran ligadas a una generación de claves, la fuerza de cifrado del algoritmo se ve disminuida, en particular cuando se usan palabras comunes. Esto reduce significativamente las combinaciones del espacio de claves para buscar la clave. Por ejemplo, una contraseña de 8 caracteres es comparable a una clave de 32 bits. Cuando se cifran claves a través de contraseñas, una contraseña que carece de aleatoriedad disminuirá las capacidades de cifrado de un algoritmo de 128 bits. Por lo tanto, es esencial aplicar reglas de sintaxis de contraseñas efectivas y que las contraseñas fácilmente adivinables sean prohibidas.

SECCIÓN 3—EVALUACIÓN DE CONOCIMIENTOS

1. Seleccione todas las opciones que apliquen. El perímetro de Internet debería:
 - A. detectar y bloquear el tráfico de los puntos finales internos infectados.
 - B. eliminar las amenazas como el spam de correo electrónico, virus y gusanos.
 - C. formatear, cifrar y comprimir los datos.
 - D. controlar el tráfico de usuarios con destino internet.
 - E. monitorizar la actividad dañina en los puertos de red internos y externos.

2. La capa de _____ del modelo OSI asegura que los datos se transfieren de forma fiable en la secuencia correcta, y la capa de _____ coordina y gestiona las conexiones de usuario.
 - A. Presentación, enlace de datos
 - B. Transporte, sesión
 - C. Física, aplicación
 - D. Enlace de datos, red

3. Escoja tres. Los principales beneficios del sistema DMZ son:
 - A. las DMZs se basan en conexiones lógicas en vez de físicas.
 - B. un intruso debe penetrar tres dispositivos separados.
 - C. las direcciones de red privadas no se dan a conocer en Internet.
 - D. excelente rendimiento y escalabilidad, a medida que aumenta el uso de Internet.
 - E. los sistemas internos no tienen acceso directo a Internet.

4. ¿Cuál de las siguientes define mejor el papel del cifrado dentro de un programa global de ciberseguridad?
 - A. El cifrado es el principal medio para asegurar los activos digitales.
 - B. El cifrado depende de secretos compartidos, y por lo tanto es un medio de control poco fiable.
 - C. Los elementos de cifrado de un programa deben ser manejados por un criptógrafo de terceros.
 - D. El cifrado es una forma esencial, pero incompleta, de control de acceso.

5. El número y tipos de capas necesarias para la defensa en profundidad son una función de:
 - A. valor del activo, la criticidad, la fiabilidad de cada control y el grado de exposición.
 - B. agentes de amenaza, gobierno corporativo, cumplimiento y la política de dispositivos móviles.
 - C. configuración de red, controles de navegación, interfaz de usuario y tráfico en la VPN.
 - D. el aislamiento, la segmentación, los controles internos y los controles externos.

Ver respuestas en el Anexo C.

Página dejada en blanco intencionadamente



Sección 4:

Seguridad de Redes, Sistemas, Aplicaciones y Datos

Los temas tratados en esta sección incluyen:

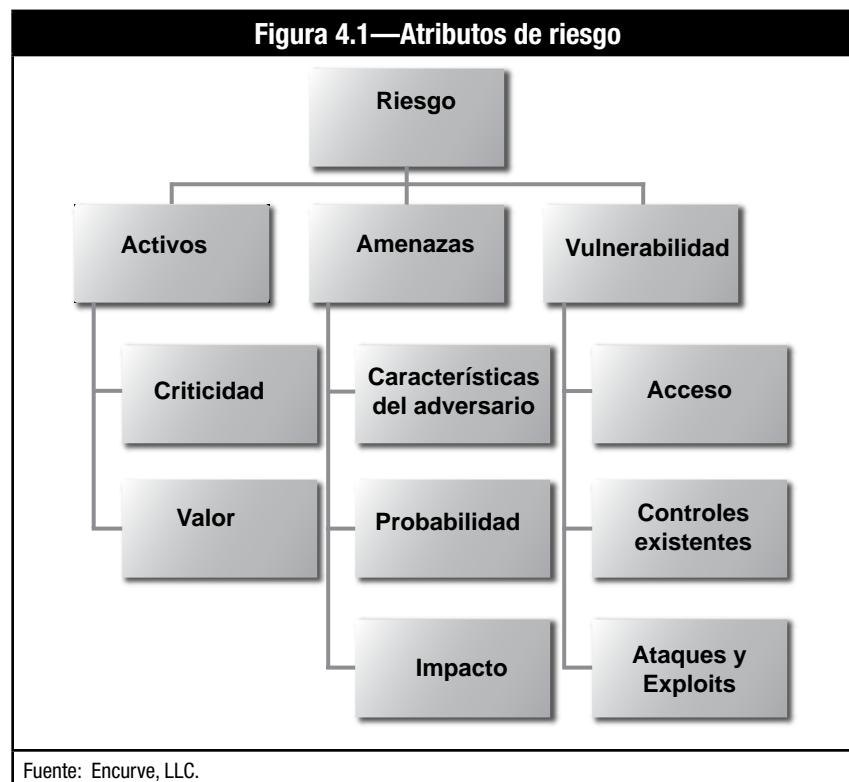
1. Controles de proceso—Evaluaciones del riesgo
2. Controles de proceso—Gestión de la vulnerabilidad
3. Controles de proceso—Pruebas de penetración
4. Seguridad de la red
5. Seguridad del sistema operativo
6. Seguridad de las aplicaciones
7. Seguridad de los datos

Página dejada en blanco intencionadamente

TEMA 1—CONTROLES DE PROCESO—EVALUACIONES DEL RIESGO

Tal y como se mencionó anteriormente, el **riesgo** se define como la posibilidad de pérdida de un activo digital como resultado de una amenaza que explota una **vulnerabilidad**. Cada uno de estos atributos de riesgo debe ser analizado para determinar el riesgo particular de una organización. El proceso a través del cual se lleva a cabo este tipo de análisis se denomina **evaluación de ciberriesgo**.

Mientras que cada metodología de evaluación del riesgo tiene diferentes matices y enfoques, la mayoría comparte tres elementos comunes: la identificación de activos, la evaluación de amenazas y la evaluación de la vulnerabilidad, tal y como se muestra en la **figura 4.1**.

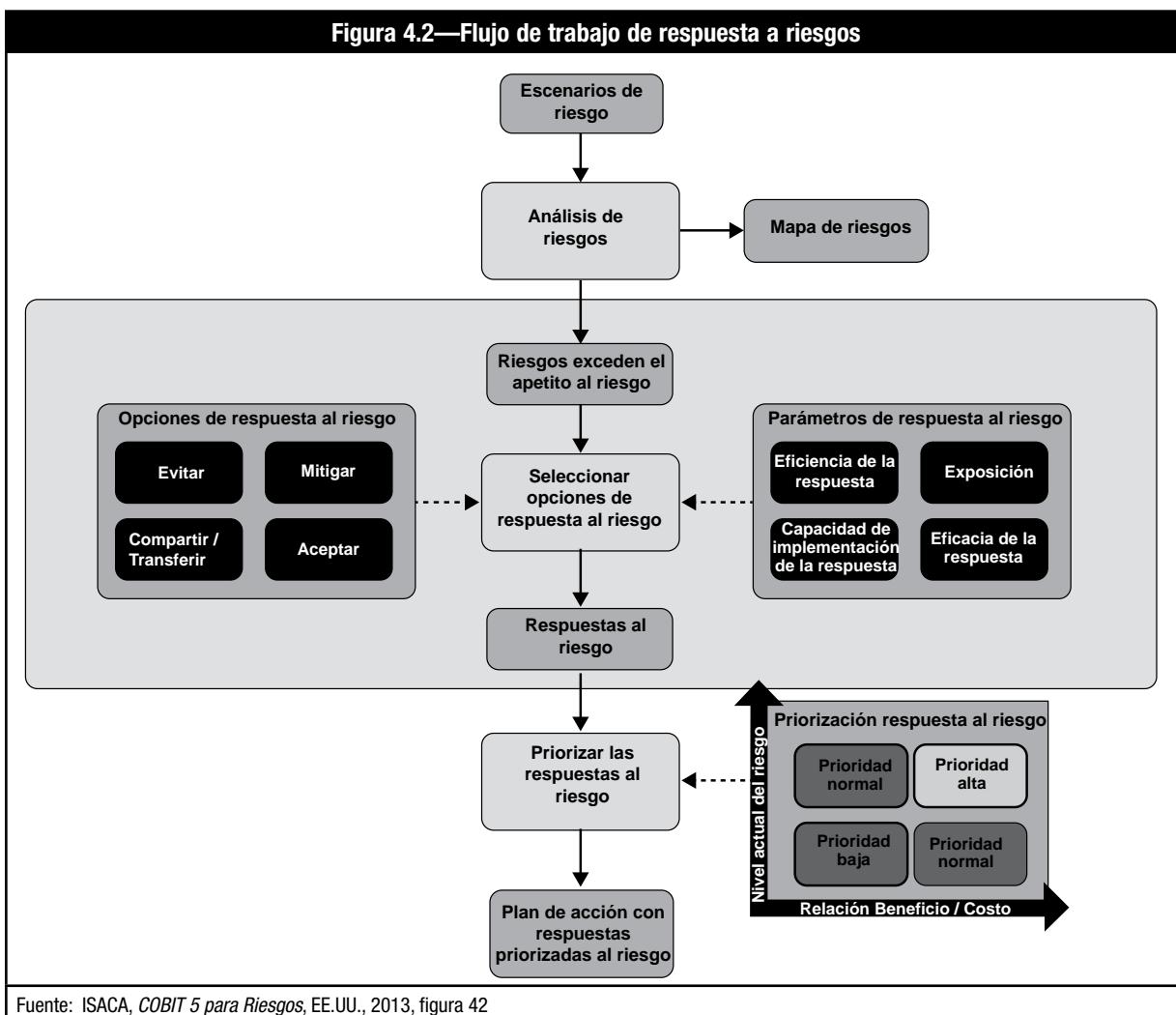


Este proceso comienza con un examen de las fuentes del riesgo (amenazas y vulnerabilidades) por sus consecuencias positivas y negativas.

Después de evaluar cada uno de estos atributos, el riesgo puede ser clasificado de acuerdo a la probabilidad y el impacto. La información utilizada para estimar el impacto y la probabilidad generalmente proviene de:

- Experiencia o datos y registros pasados (por ejemplo, reporte de incidentes)
- Prácticas confiables, estándares o directrices internacionales
- Investigación y análisis de mercado
- Experimentos y prototipos
- Modelos económicos, de ingeniería o de otro tipo
- Asesoría de especialistas y expertos

Por último, los controles existentes y otras estrategias de mitigación son evaluados para determinar el nivel y la eficacia de la mitigación actual del riesgo e identificar las deficiencias y brechas que requieren atención. Un flujo de trabajo de respuesta a riesgos se muestra en la **figura 4.2**.



Es fundamental para todo profesional de la ciberseguridad comprender los conceptos básicos y la nomenclatura de los procesos de evaluación del riesgo. Si el riesgo no se analiza correctamente, la implementación de la seguridad corre el riesgo de quedar en puras conjeturas. En las siguientes secciones, los procesos comunes de evaluación del riesgo serán abordados con más detalle.

ANÁLISIS DE RIESGOS

Como se dijo anteriormente, se usa una gran variedad de métodos que aportan datos de activos, amenazas y vulnerabilidades, y que analizan dichos datos para determinar el riesgo. La mayoría se basan en algún proceso que empareja y prioriza probabilidades e impactos. Adicionalmente, los análisis del riesgo se pueden orientar hacia una de las entradas, haciendo que la evaluación del riesgo esté orientada al activo, orientada a la amenaza u orientada a la vulnerabilidad, tal y como se muestra en la **figura 4.3**.⁵¹

Figura 4.3—Orientaciones en la evaluación del riesgo

Orientación	Descripción
Activo	En primer lugar se definen los activos importantes, y a continuación se analizan las amenazas potenciales a esos activos. Se identifican las vulnerabilidades que podrían ser aprovechadas para acceder al activo.
Amenaza	En primer lugar se determinan las amenazas potenciales, y a continuación se desarrollan los escenarios de amenazas. A partir de los escenarios, se determinan las vulnerabilidades y los activos de interés para el adversario en relación a la amenaza.
Vulnerabilidad	En primer lugar se identifican las vulnerabilidades y deficiencias, a continuación los activos expuestos, y finalmente se determinan los eventos de amenaza de los que se podrían aprovechar.

Ninguna orientación de análisis es mejor que otra; sin embargo, cada una tiene un sesgo que, si no se considera, podría debilitar el proceso de análisis resultando en algún riesgo no identificado o no correctamente priorizado. Algunas organizaciones realizarán las evaluaciones del riesgo usando más de una orientación para compensar el sesgo potencial y generar un análisis más minucioso.

LA EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD

Una vez que el riesgo es identificado y priorizado, los controles existentes deberían ser analizados para determinar su efectividad en la mitigación del riesgo. Este análisis dará lugar a una clasificación final del riesgo basado en el riesgo que tiene controles adecuados, el que tiene controles inadecuados y el que no tiene controles.

Un criterio muy importante en la selección y evaluación del control es que el coste del control (incluyendo su operación) no debería superar el valor del activo que está protegiendo.

CRITERIOS DE ÉXITO DE LA EVALUACIÓN DEL RIESGO

Elegir el método exacto de análisis, incluyendo enfoques cualitativos o cuantitativos y determinar la orientación del análisis, requiere una considerable planificación y conocimiento de metodologías específicas de evaluación de riesgos. Para tener éxito, el proceso de evaluación del riesgo debería ajustarse a los objetivos de la organización, abordar adecuadamente el entorno que está siendo evaluado y utilizar metodologías de evaluación que se ajusten a los datos que pueden ser recabados.

El alcance de la evaluación debe estar claramente definido y comprendido por todos los involucrados en el proceso de evaluación del riesgo. El proceso debería ser lo suficientemente simple para ser realizado dentro del alcance y duración del proyecto pero lo suficientemente riguroso como para producir resultados significativos.

Es importante entender el apetito de riesgo de la organización y las consideraciones culturales cuando se realiza una evaluación de riesgo. Los aspectos culturales pueden tener un impacto significativo en la gestión del riesgo. Por ejemplo, las instituciones financieras tienen culturas más formales y reguladas donde la selección e implementación de controles estrictos es aceptable, mientras que una pequeña empresa que se inicia puede ver algunos tipos de controles de seguridad como un obstáculo para el negocio.

Por último, la evaluación del riesgo no es un proceso que se lleve a cabo una sola vez. Ninguna organización es estática; la tecnología, los negocios, la regulación y requisitos legales, las personas, las vulnerabilidades y las amenazas están en continuo cambio y evolución. Por lo tanto, la evaluación exitosa del riesgo es un proceso continuo para identificar los riesgos nuevos y los cambios en las características de los riesgos existentes y conocidos.

⁵¹ Instituto Nacional de Normas y Tecnología (NIST), *Publicación Especial 800-30, Guía para Realizar Análisis de Riesgos*, EE.UU., Septiembre 2012

GESTIÓN DEL RIESGO

Para aquellos riesgos que tienen controles inadecuados o que no tienen controles, existen muchas opciones para abordar cada riesgo, tal y como se muestra en la **figura 4.4**.

Figura 4.4—Estrategia de respuesta al riesgo

Respuesta al riesgo	Descripción
Reducir el riesgo	La implementación de controles o contramedidas para reducir la probabilidad o el impacto de un riesgo a un nivel dentro de los umbrales de tolerancia al riesgo de la organización.
Evitar el riesgo	Los riesgos pueden evitarse no participando en una actividad o negocio.
Transferir o compartir el riesgo	El riesgo puede ser transferido a un tercero (por ejemplo, aseguradoras) o compartido con un tercero a través de un acuerdo contractual.
Aceptar el riesgo	Si el riesgo está dentro de los umbrales tolerables del riesgo de la organización o si el coste de mitigar el riesgo es mayor que la pérdida potencial, entonces una organización puede asumir el riesgo y absorber las pérdidas.

La estrategia que la organización escoja depende de muchos factores diferentes tales como los requisitos regulatorios, la cultura, la misión, la capacidad de mitigar el riesgo y la tolerancia al riesgo.

UTILIZANDO LOS RESULTADOS DE LA EVALUACIÓN DE RIESGOS

Los resultados de las evaluaciones de riesgo se utilizan para una variedad de funciones de gestión de la seguridad. Estos resultados necesitan ser evaluados en términos de misión de la organización, tolerancia al riesgo, presupuestos y otros recursos, y costes de mitigación. En base a esta evaluación, se puede elegir una estrategia de mitigación para cada riesgo y se pueden diseñar e implementar los controles y contramedidas apropiados.

Los resultados de la evaluación de riesgos también pueden ser utilizados para comunicar las decisiones de riesgo y las expectativas de la dirección a toda la organización a través de políticas y procedimientos.

Por último, las evaluaciones del riesgo se pueden utilizar para identificar las áreas donde las capacidades de respuesta a incidentes necesitan ser desarrolladas para detectar y responder al riesgo inherente o residual rápidamente o allí donde los controles de seguridad no pueden abordar adecuadamente la amenaza.

TEMA 2—CONTROLES DE PROCESO—GESTIÓN DE LA VULNERABILIDAD

Continuamente se descubren vulnerabilidades por lo que las organizaciones deben estar constantemente en alerta para identificarlas y remediarlas rápidamente.

Las organizaciones deben identificar y evaluar las vulnerabilidades para determinar la amenaza y el impacto potencial y para determinar el mejor curso de acción para hacer frente a cada vulnerabilidad. Las vulnerabilidades pueden identificarse por la información proporcionada por los distribuidores de software (por ejemplo, a través de la distribución de parches y actualizaciones) y usando procesos y herramientas que identifican vulnerabilidades conocidas en el entorno específico de la organización. Las dos técnicas más comunes son los análisis de vulnerabilidades y las pruebas de penetración.

GESTIÓN DE VULNERABILIDADES

La gestión de vulnerabilidades se inicia mediante la comprensión de los activos de TI y dónde residen - tanto física como lógicamente. Esto se puede hacer mediante el mantenimiento de un inventario de activos que detalla información importante acerca de cada activo tal como la ubicación (física o lógica), la criticidad del activo, el propietario del activo en la organización y el tipo de información que el activo almacena o procesa.

ESCANEOS DE VULNERABILIDADES

El escaneo de vulnerabilidad es el proceso de utilización de herramientas propietarias o de código abierto para buscar vulnerabilidades conocidas. A menudo, las mismas herramientas utilizadas por los adversarios para identificar las vulnerabilidades son utilizadas por las organizaciones para localizar vulnerabilidades proactivamente.

Hay muchas variedades de herramientas de evaluación de vulnerabilidades. Varias distribuciones Linux (p.ej., Kali Linux) proporcionan herramientas de código abierto. Herramientas comerciales (p.ej., Core Impact, Nessus®, Nmap®) son usadas a menudo para escanear la infraestructura de TI, las aplicaciones web, las bases de datos o combinaciones de ellas. Las actualizaciones autorizadas de la base de reglas de vulnerabilidades se dividen en dos categorías: basadas en host y basadas en la red. No tiene sentido nombrar todas las herramientas porque las necesidades y los presupuestos individuales varían. Del mismo modo, un mayor coste no siempre equivale a mayor funcionalidad y se pueden encontrar herramientas que son gratuitas o que tienen versiones de prueba gratuitas. Se deberían investigar y seleccionar las herramientas en base a las necesidades corporativas y en base al retorno de la inversión, teniendo en cuenta que las combinaciones de herramientas suelen proporcionar un mayor conocimiento de la situación de seguridad de las redes.

Los escaneos de vulnerabilidades deberían llevarse a cabo con regularidad para identificar nuevas vulnerabilidades y garantizar que las vulnerabilidades previamente identificadas han sido corregidas correctamente.

EVALUACIÓN DE VULNERABILIDADES

La definición más simple de una vulnerabilidad es una debilidad explotable que se traduce en una pérdida. El método utilizado para aprovechar una vulnerabilidad se llama “exploit”. Las vulnerabilidades pueden existir de muchas formas diferentes y en diferentes niveles de la arquitectura (por ejemplo, a nivel físico, de sistema operativo, en la aplicación). La **figura 4.5** provee una lista con los tipos más comunes de vulnerabilidades.

Figura 4.5 –Tipos comunes de vulnerabilidades

Tipo de Vulnerabilidad	Causa	Ejemplos de Ciberseguridad
Técnica	Errores de diseño, implementación ubicación o configuración	<ul style="list-style-type: none"> • Errores de codificación • Contrasenñas inadecuadas • Puertos de red abiertos • Falta de monitorización
Procesar	Errores en la operación	<ul style="list-style-type: none"> • Falta de monitorización de los registros (logs) • Falta de parcheo del software
Organizacional	Errores en la gestión, en las decisiones, en la planificación o debidos a la ignorancia	<ul style="list-style-type: none"> • Falta de políticas • Falta de concienciación • Fallos al implementar controles
Emergente	Interacciones entre entornos o cambios en ellos	<ul style="list-style-type: none"> • Fallos interorganizacionales • Errores de interoperabilidad • Implementar nuevas tecnologías

Es importante analizar las vulnerabilidades en el contexto de cómo son explotadas, y tanto las vulnerabilidades como los exploits deben tenerse en cuenta en las evaluaciones de vulnerabilidades. Las vulnerabilidades y los exploits pueden identificarse de muchas maneras. A un nivel técnico, se pueden usar herramientas automatizadas (tanto de código abierto como propietarias) para identificar las vulnerabilidades comunes en las implementaciones y configuraciones del equipo y de la red. Otras herramientas de análisis de vulnerabilidades incluyen fuentes de código abierto y fuentes propietarias tales como SANS, MITRE y OWASP, proveedores de software, incidentes históricos, etc.

CORRECCIÓN

Una vez que se identifican y evalúan las vulnerabilidades, puede llevarse a cabo la corrección apropiada para mitigar o eliminar la vulnerabilidad. Muy a menudo, la corrección se llevará a cabo a través de un proceso de gestión de parches, pero también puede requerir la reconfiguración de controles existentes o la adición de nuevos controles.

INFORMES Y MÉTRICAS

La gestión de vulnerabilidades incluye el seguimiento de vulnerabilidades y los esfuerzos de corrección para mitigarlas. Esto permite proporcionar buenas métricas cualitativas a la dirección de la organización sobre el número y los tipos de vulnerabilidades, los impactos potenciales y el esfuerzo necesario para mitigarlos.

TEMA 3—CONTROLES DE PROCESO—PRUEBAS DE PENETRACIÓN

Las pruebas de penetración incluyen la identificación de las vulnerabilidades existentes y, posteriormente, el uso de métodos conocidos de exploit con el objetivo de:

- Confirmar las exposiciones.
- Evaluar el nivel de eficacia y la calidad de los controles de seguridad existentes.
- Identificar cómo las vulnerabilidades específicas exponen los recursos de TI y los activos.
- Asegurar el cumplimiento.

Dado que las pruebas de penetración simulan ataques reales, deben ser planificadas cuidadosamente. El no hacerlo puede dar lugar a resultados ineficaces, impacto negativo o daños a la infraestructura de TI de la organización, la responsabilidad potencial o el enjuiciamiento penal. Es importante tener en cuenta varias consideraciones antes de llevar a cabo cualquier prueba de penetración:

- Definir claramente el alcance de la prueba incluyendo qué sistemas o redes se encuentran dentro y fuera del alcance, el tipo de exploits que pueden usarse y el nivel de acceso permitido. Estos exploits pueden incluir redes, ingeniería social, la web, aplicaciones móviles y otros tipos de pruebas.
- Recabar permiso escrito explícito de la organización autorizando la prueba. Éste es el único estándar aceptado por la industria para distinguir el servicio como autorizado y legal.
- Asegurar que los testers (ejecutores de las pruebas) implementan procedimientos del tipo “Do no harm” (“no hacer daño”) para garantizar que los activos no se vean perjudicados por eventos tales como borrado, denegación de servicio (DoS) u otros impactos negativos.
- Establecer planes de comunicación y escalado para que la organización y los testers se comuniquen rápidamente durante las pruebas.

QUIÉN REALIZA LAS PRUEBAS DE PENETRACIÓN

Las pruebas de penetración requieren conocimiento especializado de las vulnerabilidades, los exploits, la tecnología informática y el uso de herramientas de prueba. No deberían ser realizadas por profesionales no capacitados o no cualificados. Cualquier prueba de penetración debería ser cuidadosamente planificada para mitigar el riesgo de causar una interrupción del servicio, y los resultados requieren una interpretación cuidadosa y la eliminación de falsos positivos.

Una creencia ampliamente extendida es que las pruebas de penetración no son una prioridad porque normalmente suelen encontrar algún agujero en la defensa de la organización. Se suele pensar que si una organización puede diseñar una prueba de penetración que tenga éxito (o sea, crear/identificar la vulnerabilidad), es mejor gastar el dinero en solucionarlo que en probar la vulnerabilidad.

Las pruebas de penetración pueden ser encubiertas (cuando el personal general de TI no conoce que la prueba se va a llevar a cabo) para que las reacciones de detección y respuesta de la organización también se pongan a prueba. Además, las pruebas de penetración pueden ser externas, desde fuera de la organización, o internas, a partir de un sistema tras el firewall de la organización.⁵²

MARCOS CONCEPTUALES DE LAS PRUEBAS DE PENETRACIÓN

Las pruebas de penetración deberían usar un marco conceptual para asegurar su repetibilidad, su consistencia y su alta calidad en diversos tipos de pruebas de seguridad.

Los marcos conceptuales de pruebas de seguridad incluyen:⁵³

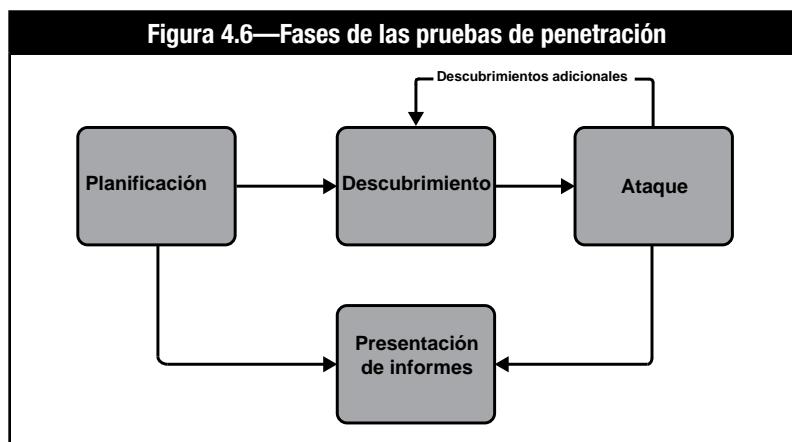
- **Guía de pruebas de penetración PCI**—Proporciona una buena introducción a las herramientas de prueba
- **Estándar de ejecución de las pruebas de penetración**—Proporciona una guía técnica práctica a las pruebas de penetración
- **Marco conceptual de las pruebas de penetración**—Proporciona una guía completa de las pruebas de penetración y herramientas de prueba
- **Marco conceptual de la seguridad de sistemas de información (ISSAF)**—Proporciona una guía técnica completa de pruebas de penetración
- **Manual de metodologías de código abierto en pruebas de seguridad (OSSTMM)**—Proporciona una metodología para probar la seguridad operacional y puede soportar ISO 27001

⁵² Encurve, LLC.

⁵³ Open Web Application Security Project (OWASP), *Penetration testing methodologies*, www.owasp.org/index.php/Penetration_testing_methodologies

FASES COMUNES EN LAS PRUEBAS DE PENETRACIÓN

Las pruebas de penetración se pueden dividir en cuatro fases principales comunes, tal y como se muestra en la **figura 4.6**.



Las fases incluyen:

- 1. Planificación**—En la fase de planificación, se fijan los objetivos, se define el alcance y se aprueba y documenta la prueba por parte de la dirección. El alcance determina si la prueba de penetración es interna o externa, limitada a ciertos tipos de ataques o limitada a ciertas redes o activos.
- 2. Descubrimiento**—En la fase de descubrimiento, el ejecutor de la prueba de la penetración recopila información mediante la realización de investigaciones sobre la organización y escanea las redes para la identificación de puertos y servicios. Las técnicas utilizadas para recopilar información incluyen:
 - Interrogación de DNS, consultas WHOIS y escuchas (sniffing) de redes para descubrir información sobre el nombre del host y la dirección IP
 - Buscar en servidores web y servidores de directorio los nombres de los empleados y la información de contacto
 - Captura de banners para obtener información de aplicaciones y servicios
 - Enumeración NetBIOS para obtener información del sistema
 - Rebuscar en la basura y recorrer las instalaciones para obtener información adicional
 - Uso de herramientas de búsqueda online de infraestructuras de Internet, tales como Shodan⁵⁴, hasta sistemas y servicios expuestos pasivamente a perfiles
 - Ingeniería social, como hacerse pasar por personal de ayuda y pedir contraseñas, hacerse pasar por un usuario y llamar el help desk para restablecer contraseñas o enviar correos electrónicos fraudulentos

También se lleva a cabo una evaluación de las vulnerabilidades durante la fase de descubrimiento. Esto implica la comparación de los servicios, aplicaciones y sistemas operativos del host escaneado con bases de datos de vulnerabilidades.

- 3. Ataque**—La fase de ataque es el proceso de verificación de vulnerabilidades identificadas previamente intentando explotarlas. Metasploit® alberga una base de datos pública de exploits de calidad garantizada. Clasifican los exploits para pruebas seguras.

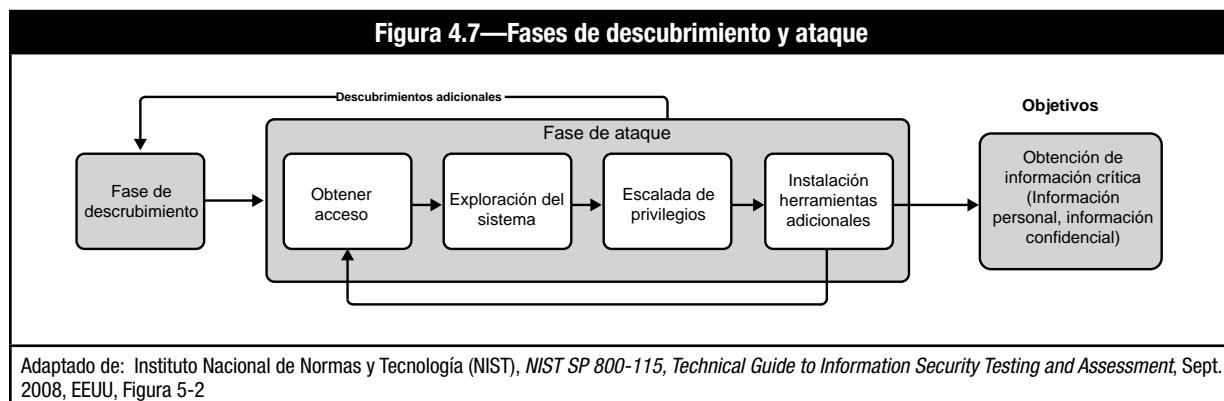
A veces los intentos de explotación no brindan acceso al ejecutor de las pruebas, pero sí le dan información adicional sobre el objetivo y sus posibles vulnerabilidades. Si un tester es capaz de explotar una vulnerabilidad, se pueden instalar más herramientas en el sistema o en la red para acceder a sistemas o recursos adicionales.

Un payload es el software que permite a un usuario controlar un sistema informático después de que éste haya sido explotado. El payload típicamente se adjunta al exploit y es entregado por él. El payload más popular de Metasploit se llama Meterpreter, el cual permite al usuario cargar y descargar archivos del sistema, tomar capturas de pantalla y recoger hashes de contraseñas. Las fases de descubrimiento y de ataque se ilustran en la **figura 4.7**.

⁵⁴ Más información disponible en www.shodan.io/.

4. Presentación de informes: La fase de presentación de informes se produce simultáneamente con las otras fases.

Se desarrolla un plan de evaluación durante la fase de planificación. Los registros se mantienen durante las fases de descubrimiento y de ataque. Y al final de la prueba de penetración, se desarrolla un informe para describir las vulnerabilidades identificadas, asignar calificaciones de riesgo y proporcionar planes de mitigación.



Página dejada en blanco intencionadamente

TEMA 4—SEGURIDAD DE LA RED

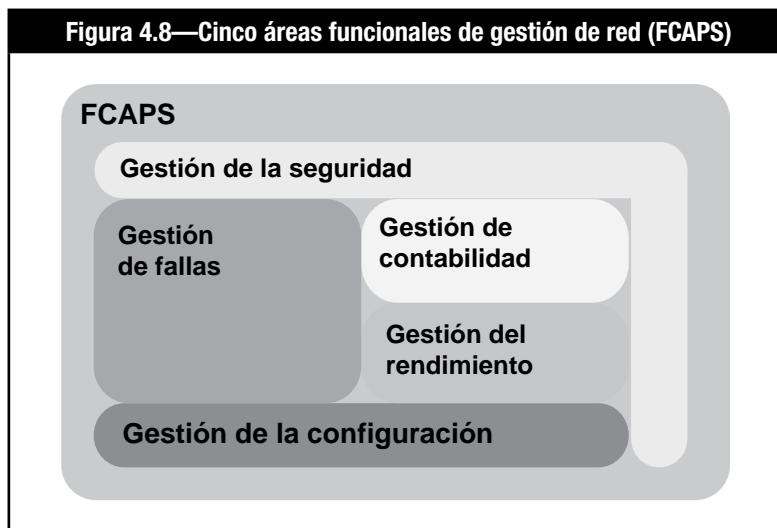
GESTIÓN DE REDES

La gestión de redes es el proceso de evaluación, monitorización y mantenimiento de los dispositivos de red y las conexiones. Las funciones recomendadas de gestión de red se enumeran en un modelo que consta de cinco áreas funcionales (FCAPS).

Estas cinco áreas funcionales, introducidas por la Organización internacional de normalización (ISO) y posteriormente desarrollada por la Unión internacional de telecomunicaciones (ITU) se muestran en la **figura 4.8** a continuación:

- **Gestión de errores**—Detectar, aislar, notificar y corregir errores encontrados en la red. En esta categoría se analiza el tráfico, las tendencias, las consultas SNMP y las alarmas para la detección automática de errores.
- **Gestión de la configuración**—Aspectos de la configuración de los dispositivos de red incluyen la gestión de archivos de configuración, gestión de inventario y gestión de software.
- **Gestión de las cuentas**—Información del uso de los recursos de la red.
- **Gestión del rendimiento**—Monitorizar y medir diversos aspectos de las métricas de rendimiento para que se pueda mantener un rendimiento aceptable. Esto incluye el tiempo de respuesta, la utilización del enlace y las tasas de error. Los administradores pueden monitorizar las tendencias y alarmas de umbral.
- **Gestión de la seguridad**—Proporcionar acceso a los dispositivos de red y a los recursos de la empresa a personas autorizadas. Esta categoría se enfoca en la autenticación, autorización, firewalls, segmentación de red, IDS y notificaciones de intentos de violaciones de seguridad.

Figura 4.8—Cinco áreas funcionales de gestión de red (FCAPS)



RED DE ÁREA LOCAL (LAN)⁵⁵

Una LAN cubre un área local pequeña, desde unos pocos dispositivos en una sola habitación hasta una red distribuida por varios edificios. El aumento del ancho de banda a precios razonables ha reducido el esfuerzo de diseño que se requiere para proveer soluciones LAN con una adecuada relación coste/efectividad para organizaciones de cualquier tamaño.

Las nuevas LAN son casi siempre implementadas utilizando el protocolo switched Ethernet (802.3). El cableado de pares trenzados (redes LAN 100-Base-T o mejor y LAN inalámbricas [WLAN]) conecta los switches de piso a las estaciones de trabajo e impresoras en el área más cercana. Los switches de planta se pueden conectar entre sí con cableado Base-T1000 o de fibra óptica. En las organizaciones más grandes, los switches de piso pueden estar conectados con switches más grandes y más rápidos cuyo propósito sea enrutar correctamente los datos de switch a switch.

⁵⁵ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

A medida que las LAN crecen y el tráfico aumenta, el requisito de planear cuidadosamente la configuración lógica de la red se vuelve cada vez más importante. Los planificadores de redes tienen que estar altamente capacitados y tener muchos conocimientos. Sus herramientas incluyen monitores de tráfico que les permiten monitorizar los volúmenes de tráfico en los enlaces críticos. Rastrear los volúmenes de tráfico, las tasas de errores y los tiempos de respuesta es tan importante en las redes LAN grandes como en los servidores distribuidos y los mainframes.

COMPONENTES DE LAN⁵⁶

Los componentes comúnmente asociados con las LANs son repetidores, hubs, puentes (bridges), conmutadores (switches) y enrutadores (routers):

- **Repetidores**—Dispositivos de capa física que extienden el alcance de una red o que conectan dos segmentos de red independientes. Los repetidores reciben señales de un segmento de red y amplifican (regeneran) la señal para compensar señales (analógicas o digitales) que están distorsionadas debido a una reducción de la intensidad de la señal durante la transmisión (es decir, la atenuación). Los repetidores Wi-Fi para uso casero son populares en la actualidad.
- **Concentradores (hubs)**—Dispositivos de capa física que sirven como el centro de una red de topología de estrella o un concentrador de red. Los concentradores pueden ser activos (si repiten las señales enviadas a través de ellos) o pasivos (si sólo separan las señales).
- **Switches de capa 2**—Los conmutadores de capa 2 son dispositivos de nivel de enlace de datos que pueden dividir e interconectar segmentos de la red y ayudar a reducir los dominios de colisión en las redes basadas en Ethernet. Además, los conmutadores almacenan y retransmiten tramas, filtrando y reenviando paquetes entre segmentos de red, basándose en las direcciones de origen y destino MAC de la capa 2, tal como los puentes (bridges) y los concentradores (hubs) hacen en la capa de enlace de datos. Los conmutadores, sin embargo, proveen una funcionalidad más robusta que los puentes (bridges) a través del uso de protocolos más sofisticados de capa de enlace de datos, que son implementados a través de hardware especializado llamado circuitos integrados de aplicación específica (del inglés called application-specific integrated circuits, ASIC). Los beneficios de esta tecnología son la eficiencia de rendimiento obtenida a través de la reducción de costes, la baja latencia o tiempo de inactividad, y un mayor número de puertos en un conmutador con capacidades dedicadas de ancho de banda de alta velocidad. Los conmutadores son también aplicables en las especificaciones de la tecnología WAN.
- **Enrutadores (routers)**—Similares a los puentes (bridges) y a los conmutadores (switches) en el hecho que conectan dos o más segmentos de red físicamente separados. Los segmentos de red conectados mediante un enrutador, sin embargo, siguen siendo lógicamente independientes y pueden funcionar como redes independientes. Los enrutadores operan en la capa de red OSI examinando direcciones de red (es decir, enrutando información codificada en un paquete IP). Examinando la dirección IP, el enrutador puede tomar decisiones inteligentes para dirigir el paquete a su destino. Los enrutadores se diferencian de los conmutadores que operan en la capa de enlace de datos en que utilizan las direcciones lógicas de red, utilizan diferentes direcciones/segmentos de red de todos los puertos, bloquean la información de broadcast, bloquean el tráfico a direcciones desconocidas, y filtran el tráfico basado en la información de la red o el host. Los enrutadores (routers) no suelen ser tan eficientes como los conmutadores (switches), ya que son dispositivos basados en software y examinan cada paquete que viene a través de ellos, lo que puede crear cuellos de botella significativos dentro de una red. Por lo tanto, se debería tener mucho cuidado respecto a dónde se ubican los enrutadores (routers) en una red. Esto debería incluir equilibrar conmutadores en el diseño de red así como también aplicar principios de balanceo de carga con otros enrutadores para consideraciones de eficiencia de rendimiento.
- **Switches de capa 3 y 4**—Los avances en la tecnología de conmutación también han dado a los switches las capacidades de operación en la capa 3 y la capa 4 del modelo de referencia OSI.
 - Un switch de capa 3 va más allá de la capa 2, actuando en la capa de red del modelo OSI como un enrutador. El switch de capa 3 mira el protocolo de red del paquete entrante (por ejemplo, IP). El conmutador compara la dirección de destino de IP con la lista de direcciones en sus tablas, para calcular de manera activa la mejor forma de enviar un paquete a su destino. Esto crea un circuito virtual (es decir, el conmutador (switch) tiene la capacidad de segmentar la LAN dentro de sí mismo y creará un camino entre el dispositivo que recibe y el que transmite para enviar los datos). A continuación envía el paquete a la dirección del destinatario. Esto proporciona el beneficio añadido de reducir el tamaño de los dominios de difusión de red. Los dominios de difusión deberían estar limitados o alineados a las áreas funcionales de negocio o grupos de trabajo dentro de una organización, para reducir el riesgo de fuga de información de aquellos que no tienen la necesidad de saber, donde los sistemas pueden ser un objetivo y sus vulnerabilidades explotadas. La principal diferencia entre un router y un switch de Capa 3 es que un router realiza la conmutación de paquetes usando un microprocesador, mientras que un switch de Capa 3 realiza la conmutación mediante hardware ASIC (circuitos integrados de aplicación específica).
 - Un switch de capa 4 permite la conmutación basada en políticas. Con esta funcionalidad, los switches de Capa 4 pueden reducir la carga de un servidor equilibrando el tráfico a través de un grupo de servidores, basándose en información de la sesión individual y del estado.
- **Switches de Capa 4-7**—También conocidos como switches de contenido, conmutadores de servicios de contenido, conmutadores-web o switches de aplicación. Se utilizan comúnmente para equilibrar la carga entre grupos de servidores. El equilibrio de cargas se puede basar en HTTP, HTTPS y/o VPN, o para cualquier tráfico TCP/IP de aplicaciones que utilice un puerto específico. Los conmutadores de contenido también se pueden utilizar para realizar operaciones estándar, tales como cifrado/descifrado SSL para reducir la carga sobre los servidores que reciben el tráfico, y para centralizar la gestión de certificados digitales.

⁵⁶ Ibid

SEGURIDAD LAN/WAN

Las LAN y WAN son particularmente susceptibles a amenazas relacionadas con las personas y los virus, debido a la gran cantidad de las personas que tienen derechos de acceso.

Las funciones administrativas y de control disponibles con el software de redes pueden ser limitadas. Los proveedores de software y los usuarios de las redes han reconocido la necesidad de proveer funcionalidades de diagnóstico para identificar la causa de los problemas cuando la red se cae o funciona de manera inusual. Sólo ahora el uso de mecanismos de acceso basados en Logon-IDs y contraseñas con equipos asociados de administración se está convirtiendo en un estándar (es decir, redes como aplicaciones). Las funcionalidades para dar permiso de lectura, escritura y ejecución para archivos y programas son opciones disponibles en algunas versiones del sistema operativo de red, pero rara vez se encuentran en las LANs registros automatizados con el detalle de la actividad realizada (pistas de auditoría). Afortunadamente, las nuevas versiones de software de red tienen considerablemente más funcionalidades de control y de administración.

Las LANs pueden representar una forma de computación descentralizada. El procesamiento local descentralizado provee el potencial para un ambiente informático más ágil; sin embargo, las organizaciones no siempre dan la oportunidad de desarrollar eficientemente el personal para abordar los problemas técnicos, operativos y de control que representa la tecnología compleja de LAN. Como resultado de ello, a los administradores locales de LAN a menudo les falta la experiencia, la pericia y el tiempo para manejar con efectividad el ambiente de computación.

CONTROL DE ACCESO A LA RED (NAC)

El control de acceso a la red (NAC) se centra en controlar el acceso a una red utilizando políticas que describen cómo los dispositivos pueden acceder de forma segura a los nodos de red la primera vez que intentan acceder a esa red. Algunas características incluyen la integración de un proceso de corrección automática que corrige los nodos no conformes antes de permitir el acceso y de autorizar la infraestructura de red para que trabaje con servicios de back office y computación de usuario final para asegurar que la red es segura antes de autorizar el acceso.

RIESGOS Y PROBLEMAS DE REDES LAN

Las LAN facilitan el almacenamiento y la recuperación de los programas y datos usados por un grupo de personas. El software y las prácticas de la LAN también necesitan proporcionar la seguridad de estos programas y datos. Desafortunadamente, la mayoría del software de LAN proporciona un nivel bajo de seguridad. Se ha enfatizado en el suministro de la capacidad y la funcionalidad en lugar de la seguridad. Como resultado, el riesgo asociado con el uso de redes de área local incluye:

- La pérdida de integridad de datos y de los programas a través de cambios no autorizados
- La falta de protección de los datos vigentes a través de la incapacidad para mantener el control de versiones
- La exposición a actividades externas a través de una verificación limitada de usuarios y el acceso potencial del público a la red a partir de conexiones de llamada telefónica
- Infección por virus y gusanos
- Revelación indebida de datos causado por disposiciones de acceso general en lugar de utilizar la base de “necesidad de saber”
- La violación de las licencias de software mediante el uso de copias de software sin licencia o números excesivos de copias
- El acceso ilegal simulando ser o disfrazándose como un usuario legítimo de LAN.
- Escucha de información realizada por usuarios internos (Sniffing) (obteniendo información de la red, aparentemente sin ningún valor, pero que puede ser usada para lanzar un ataque, como por ejemplo información sobre las direcciones de la red)
- La suplantación del usuario interno (Spoofing) (reconfiguración de una dirección de red para simular ser una dirección diferente)
- Destrucción de los datos de registro y de auditoría

Las medidas de seguridad de la LAN dependen del producto del software, de la versión del producto y de su implementación. Normalmente, las funcionalidades administrativas de seguridad de red que están disponibles son:

- Declaración de la propiedad de los programas, archivos y almacenamiento
- Limitar el acceso a sólo lectura
- Implementar el bloqueo de los registros y archivos para prevenir una actualización simultánea
- Hacer cumplir los procedimientos de identificación de inicio de sesión /contraseña del usuario, incluyendo las reglas relativas a la longitud, el formato y la frecuencia de cambio de las contraseñas
- Usar switches para implementar políticas de seguridad de puertos en vez de usar concentradores o routers poco manejables, para impedir que hosts no autorizados, con direcciones MAC desconocidas, se conecten a la LAN
- Cifrar el tráfico local utilizando el protocolo IPSec (seguridad IP)

El uso de estos procedimientos de seguridad requiere tiempo de administración que se debe dedicar a la implementación y al mantenimiento. La administración de la red es a menudo inadecuada, proporcionando acceso global debido a que el soporte administrativo disponible es limitado cuando el acceso limitado sería más apropiado.

TECNOLOGÍA INALÁMBRICA⁵⁷

Las tecnologías inalámbricas, en el sentido más sencillo, permiten que uno o más dispositivos se comuniquen sin conexiones físicas (es decir, sin requerir red o cableado periférico). La tecnología inalámbrica es una tecnología que permite a las organizaciones adoptar soluciones de negocio electrónico con un gran potencial de crecimiento. Las tecnologías inalámbricas utilizan transmisiones de radio frecuencia /señales electromagnéticas por el espacio libre como medio para transmitir datos, mientras que las tecnologías por cable emplean señales eléctricas a través de cables. Las tecnologías inalámbricas abarcan desde sistemas complejos tales como redes inalámbricas de área extensa (WWAN), redes inalámbricas de área local (WLAN) y teléfonos celulares, hasta sencillos dispositivos tales como audífonos, micrófonos y otros dispositivos inalámbricos que no procesan ni almacenan información. Incluyen también dispositivos Bluetooth® con un minitransceptor de radiofrecuencia y dispositivos infrarrojos, tales como controles remotos, algunos teclados de computadora y ratones inalámbricos, y auriculares estéreo de alta fidelidad inalámbricos, todos los cuales requieren de una línea directa de visión entre el transmisor y el receptor para cerrar el enlace.

Sin embargo, la tecnología inalámbrica introduce nuevos elementos que deben ser tratados. Por ejemplo, las aplicaciones existentes pueden necesitar ser readaptadas para hacer uso de los interfaces inalámbricos. Además, es necesario tomar decisiones respecto a la conectividad general, para facilitar el desarrollo de aplicaciones móviles completamente inalámbricas, u otras aplicaciones que se basan en la sincronización de transferencia de datos entre los sistemas móviles de computación y la infraestructura corporativa. Otros aspectos incluyen banda estrecha, falta de un estándar maduro, y problemas de seguridad y de privacidad no resueltos.

Las redes inalámbricas sirven como mecanismo de transporte entre dispositivos, y entre dispositivos y las redes alámbricas tradicionales. Las redes inalámbricas son muchas y diversas pero frecuentemente son categorizadas en cuatro grupos basados en su rango de cobertura:

- WANs
- LANs
- Redes inalámbricas de área personal (WPANs)
- Redes inalámbricas ad hoc

REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)⁵⁸

Las WLANs permiten mayor flexibilidad y portabilidad que las redes tradicionales de área local. A diferencia de una LAN tradicional, que requiere un cable para conectar la computadora de un usuario con la red, una WLAN conecta a la red computadoras, tabletas, teléfonos inteligentes y otros componentes usando un dispositivo de punto de acceso. Un punto de acceso, o hub de red inalámbrica, se comunica con dispositivos equipados con adaptadores inalámbricos de red dentro de un radio específico del punto de acceso; se conecta con una LAN cableada de Ethernet por medio de un puerto RJ-45. Los dispositivos de puntos de acceso tienen típicamente áreas de cobertura de hasta 300 pies (aproximadamente 100 metros). Esta área de cobertura se llama una celda o radio. Los usuarios se mueven libremente dentro de la celda con su portátil u otro dispositivo de red. Las celdas de los puntos de acceso pueden vincularse para permitir a los usuarios circular incluso dentro de un edificio o entre edificios. WLAN incluye 802.11, HyperLAN, HomeRF y otros. Las WLAN se denominan comúnmente puntos de acceso (hotspots) de Wi-Fi.

Las tecnologías WLAN se ajustan a una variedad de estándares y ofrecen diferentes niveles de características de seguridad. Las principales ventajas de los estándares son el fomentar la producción en masa y permitir que los productos de múltiples proveedores puedan interesar. El estándar más útil usado actualmente es el estándar IEEE 802.11.

802.11 se refiere a una familia de especificaciones para la tecnología WLAN. 802.11 especifica una interfaz por aire (over-the-air) entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos.

⁵⁷ Ibid

⁵⁸ Ibid

PROTECCIONES EN REDES INALÁMBRICAS

La transmisión inalámbrica de datos está sujeta a un mayor riesgo de intercepción que el tráfico por cable, de la misma forma que es más fácil interceptar llamadas hechas a través de teléfonos móviles que llamadas desde un teléfono fijo. No es necesario pinchar manualmente la conexión, ya que existen herramientas que pueden usarse en remoto para interceptar la conexión de forma encubierta. La transmisión inalámbrica de información confidencial debería ser protegida con un cifrado fuerte. Una conexión inalámbrica insegura expone a los usuarios a escuchas ilegales, lo cual puede llevar a la exposición de información confidencial, mensajes interceptados o abuso de conexiones. Los ejemplos incluyen:

- El email puede ser interceptado y leído o modificado.
- Hackers pueden reemplazar las credenciales de un usuario con información falsa que lleve al servidor de destino a rechazar los intentos de acceso del usuario, causando así denegación del servicio (DoS).
- Una persona no autorizada puede acceder a una red inalámbrica no segura y usar sus recursos, incluyendo conectividad a internet gratis.

El cifrado basado en el estándar IEEE 802.11 (Wired Equivalent Privacy, WEP) utiliza claves simétricas, privadas, lo que significa que el controlador de la interfaz de red (del inglés network interface controller, NIC) del usuario final que está basado en radio y el punto de acceso deben tener la misma clave. Esto conduce a dificultades periódicas a la hora de distribuir nuevas claves a cada NIC. Como resultado, las claves permanecen inalteradas en las redes durante largos períodos de tiempo. Con claves estáticas, diversas herramientas de hacking pueden irrumpir fácilmente en los mecanismos de cifrado WEP que son relativamente débiles.

Los estándares de seguridad inalámbricos continúan evolucionando. El método más comúnmente usado para redes de área local inalámbricas es 802.11i (WPA2) y Acceso Wi-Fi protegido (WPA), que usa claves dinámicas y un servidor de autenticación con credenciales que aumentan su protección contra los hackers.

WEP y WPA cumplen con las versiones evolucionadas de los estándares inalámbricos 802.11 especificados por el IEEE, siendo WPA compatible con versiones más avanzadas de 802.11, incluso teniendo en cuenta las limitaciones de WPA. La clave está protegida por una frase de contraseña (passphrase) que no tiene forzosamente una longitud robusta. WPA es un subconjunto de desarrollo del estándar 802.11i. El estándar completo insta a la seguridad mejorada mediante la implementación de AES, lo que muchos suministradores han introducido en sus dispositivos sólo como una opción.

WPA y WPA V2 (preferida) son aplicables a la mayoría de las redes inalámbricas y generalmente usados en redes formadas por PCs. Los mensajes transmitidos usando dispositivos inalámbricos portátiles también deberían ser protegidos mediante cifrado y, allá donde sea posible, se pueden usar métodos VPN para proporcionar seguridad adicional. Por ejemplo, el BlackBerry® Enterprise Server integra el email corporativo en el dispositivo y usa Triple DES para cifrar la información entre la BlackBerry y el servidor de correo corporativo.

Las claves públicas también se usan en dispositivos móviles. ECC se usa ampliamente en tarjetas inteligentes y su uso en teléfonos móviles va en aumento. ECC es ideal para dispositivos pequeños porque el algoritmo, que combina geometría plana con álgebra, puede alcanzar una autenticación más segura con claves más pequeñas si lo comparamos con métodos tradicionales, tales como RSA, que usa principalmente factorización algebraica. Las claves más pequeñas se adaptan mejor a dispositivos móviles; sin embargo, se puede objetar que ECC no es tan riguroso como los algoritmos tradicionales de clave pública porque su fecha de creación es más reciente que algoritmos como RSA. Con el incremento de la capacidad de cálculo de los ordenadores, la longitud de las claves se está convirtiendo en un problema menor para las aplicaciones de PC.

PUERTOS Y PROTOCOLOS⁵⁹

Un puerto es una conexión lógica. Cuando se utiliza el protocolo de comunicaciones de Internet TCP/IP (Transmission Control Protocol/Internet Protocol), la designación de un puerto es la forma en que un programa cliente especifica a un determinado programa servidor cuál es el equipo que está ubicado en una red. Básicamente, un número de puerto es una forma de identificar el proceso específico al que un mensaje de Internet u otra red será dirigido cuando llegue a un servidor. Para TCP, UDP (User Datagram Protocol) e ICMP (Internet Control Message Protocol), un número de puerto es un número entero de 16 bits que se pone en la cabecera unido junto con una unidad de información (una unidad de mensaje). Este número de puerto se pasa lógicamente entre las capas de transporte de cliente y servidor, y físicamente entre la capa de transporte y la capa de protocolo de Internet, y luego se reenvía.

⁵⁹ Moody, R. "Ports and Port Scanning: An Introduction," *ISACA Journal*, Volume 4, 2001

Las aplicaciones de alto nivel que utilizan TCP/IP tales como el protocolo web y HTTP usan puertos con números pre asignados. Estos son puertos bien conocidos, a los que han sido asignados números por la Autoridad de asignación de números de Internet (del inglés Internet Assigned Numbers Authority, IANA). A algunos procesos de aplicación se les dan números de puerto dinámicamente cuando se realiza cada conexión.

LOS NUMEROS DE PUERTO

Los números de puerto permitidos van de 0 a 65535. Los puertos del 0 al 1023 están reservados para ciertos servicios privilegiados – los puertos reconocidos. Por ejemplo, para el servicio HTTP, el puerto 80 se define como el valor predeterminado. Debido a que está pre asignado, el puerto 80 y algunos otros puertos no tienen que especificarse en el localizador uniforme de recursos (URL). Eso permite al usuario escribir simplemente una dirección de Internet o URL, como por ejemplo www.isaca.org, sin especificar el número de puerto al final de la URL; en este caso www.isaca.org:80. Cualquiera de estos dos formatos funcionará en el navegador.

Numeros de protocolo y servicios de misiones

Los números de puerto se dividen en tres rangos: los puertos reconocidos, los puertos registrados y los puertos dinámicos y/o privados. Los registros IANA listan todos los números de puerto reconocidos y registrados:

- **Los puertos reconocidos**—Del 0 al 1023: Controlados y asignados por IANA, en la mayoría de los sistemas puede ser utilizado sólo por los procesos del sistema (o raíz) o por los programas ejecutados por usuarios con privilegios. Los puertos asignados utilizan la primera parte de los posibles números de puerto. Inicialmente, estos puertos asignados estaban en el rango 0 - 255. Actualmente, la gama de puertos asignados gestionados por la IANA se ha ampliado al rango 0 - 1023.
- **Los puertos registrados**—Del 1024 al 49151: Enumerados por la IANA, en la mayoría de los sistemas pueden ser utilizados por procesos o programas ordinarios ejecutados por usuarios comunes.
- **Los puertos dinámicos y/o privados**—Del 49152 al 65535: No listados por IANA debido a su naturaleza dinámica.

Cuando se inicia un programa servidor a través de una conexión de puerto, se dice que se une a su número de puerto designado. Cuando otro programa cliente quiere usar ese servidor, también debe enviar una solicitud para unirse al número de puerto designado. Los puertos son utilizados en TCP para nombrar los extremos de las conexiones lógicas que transportan conversaciones duraderas. En la medida de lo posible, estas mismas asignaciones de puerto se utilizan con UDP.

Por ejemplo, una solicitud de un archivo es enviada a través del software de navegador a un servidor accesible desde Internet. La petición puede ser tratada por la aplicación de protocolo de transferencia de archivos (FTP) de ese host que reside en un determinado servidor interno. Para pasar la petición al proceso de FTP que reside en dicho servidor remoto, la capa de software TCP del ordenador (el navegador) especifica el número de puerto 21, (el puerto asignado por IANA para una solicitud de FTP) en el número entero de puerto de 16-bit que se anexa a la solicitud como parte de la información de cabecera. En el servidor remoto, la capa TCP leerá el número de puerto (21) y reenviará la solicitud al programa FTP ubicado en el servidor. Los servicios comunes son implementados en el mismo puerto a través de diferentes plataformas. Por ejemplo, el servicio se ejecuta generalmente en el puerto 80, se use el sistema operativo Unix o Windows. Estos mecanismos de la capa de transporte, junto con las direcciones IP de una conexión (emisor y receptor) identifican de forma única una conexión.

En una configuración de ordenadores de Internet básica que utiliza varios ordenadores, un servidor web se instala detrás de un firewall y sus bases de datos se instalan en un segundo equipo detrás de un segundo firewall. Otras configuraciones son perfectamente posibles. En algunos casos, existe una intranet corporativa con usuarios internos y un servidor de base de datos detrás de un firewall, un servidor web, otro firewall y usuarios externos (también es útil contar con acceso externo a las herramientas del servidor web). Cada firewall podría permitir el acceso a los puertos abiertos por el software del servidor web. En muchas aplicaciones de software de servidor, un número de puertos se configura de forma predeterminada, por ejemplo, HTTP-80, HTTPS-443 (el número de puerto de servidor web seguro estándar), SMTP-25 y otros.

Tunelización

El uso de un protocolo para el envío de otra información que no es la del propósito de ese protocolo se llama tunelización. En la tunelización, los hackers maliciosos internos o externos usan el protocolo como un camino establecido, o túnel, dirigiendo el intercambio de información para un propósito ilícito.

Un túnel ICMP usa las peticiones de eco ICMP (echo ICMP) y los paquetes de respuesta para establecer una conexión encubierta entre dos ordenadores remotos (un cliente y un proxy). La tunelización ICMP puede ser utilizada para saltarse las reglas de los firewalls a través de la ofuscación del tráfico real. Dependiendo de la implementación del software de tunelización ICMP, este tipo de conexión también puede ser categorizado como un canal de comunicación cifrado entre dos ordenadores. Sin una adecuada inspección a fondo de los paquetes o una revisión de registros (logs), los administradores de red no serán capaces de detectar este tipo de tráfico a través de su red.

La tunelización HTTP es una técnica mediante la cual las comunicaciones realizadas utilizando diversos protocolos de red se encapsulan usando el protocolo HTTP; normalmente, dichos protocolos pertenecen a la familia TCP/IP. Por lo tanto, el protocolo HTTP actúa como un envoltorio para el canal dentro del cual el protocolo de red tuneliza las comunicaciones. La comunicación HTTP con su canal encubierto se llama túnel HTTP.

El software de tunelización HTTP consiste en aplicaciones de tunelización HTTP cliente-servidor que se integran con el software de aplicación existente, permitiendo que sean usadas en condiciones de conectividad de red restringida, incluyendo redes con cortafuegos, redes tras servidores proxy, y la traducción de direcciones de red.

REDES VIRTUALES PRIVADAS (VPN)

Al diseñar una VPN, es importante asegurar que la VPN puede transportar todos los tipos de datos de manera segura y privada a través de cualquier tipo de conexión. La tunelización transporta los datos de las capas superiores través de una VPN mediante protocolos de capa 2. Un extremo del túnel es el cliente, y el otro extremo es un dispositivo de conectividad o un servidor de acceso remoto. Los tipos comunes de tunelización incluyen:

- **Protocolo de túnel punto a punto (PPTP)**—Un protocolo de capa 2 desarrollado por Microsoft® que encapsula datos de protocolo de punto a punto. Es simple, pero menos seguro que otros protocolos de túnel.
- **Protocolo de túnel de capa 2 (L2TP)**—Un protocolo que encapsula los datos del protocolo de punto a punto y que es compatible entre equipos de diferentes fabricantes. Los puntos finales no tienen que residir en la misma red de conmutación de paquetes y pueden permanecer aislados del resto del tráfico.
- **VPN Capa de sockets seguros**—Un tipo de VPN de capa 3 que puede utilizarse con navegador web estándar y usa protocolos de seguridad de capa de transporte (TLS) para cifrar el tráfico.
- **VPN IPSec**—Las VPN basadas en IPSec protegen los paquetes IP de capa 2 y 3 entre redes o hosts remotos y un nodo/pasarela IPSec ubicado en el extremo de una red privada.

VOZ SOBRE PROTOCOLO DE INTERNET (VOIP)⁶⁰

Los usuarios a menudo esperan que todas las comunicaciones de voz sean confidenciales. Cualquier dispositivo VoIP es un dispositivo IP; por tanto, es vulnerable a los mismos tipos de ataques que cualquier otro dispositivo IP. Un hacker o virus podrían potencialmente dejar indisponibles las redes de datos y de voz de forma simultánea en un sólo ataque. Además, las redes de VoIP siguen siendo vulnerables a escuchas de paquetes a través de la red, ataques de denegación de servicio (DoS), interrupción del flujo del tráfico y fraude telefónico. Las escuchas de paquetes a través de la red permitirían la divulgación de información sensible, como información de usuario, lo cual puede resultar en robo de identidad que puede ser utilizada para atacar a otros subsistemas de datos. El escaneo de puertos es a menudo un precursor de la escucha de paquetes potencial de la red VoIP. La capacidad de escuchar paquetes en la red es cada vez más fácil ya que son muchas las herramientas disponibles de forma fácil en sitios web de código abierto, en contraste con los equipos especializados de diagnóstico utilizados para la multiplexación por división de tiempo (del inglés time division multiplexing, TDM) que tienen un coste más elevado.

El ataque de denegación de servicio (DoS), o el desbordamiento de la red de datos mediante una gran cantidad de datos, es un problema común en la protección de las redes de datos, que necesita ser revisado a medida que la calidad del servicio (QoS) se implementa en las redes VoIP. Muy a menudo se pasa por alto el dispositivo final IP, pero podría ser un objetivo de ataque y ser el blanco de una inundación de datos, provocando el reinicio del dispositivo y su indisponibilidad.

La interrupción del flujo de tráfico permite una mayor explotación de las dos vulnerabilidades anteriores, mientras que el redireccionamiento de paquetes facilita la determinación de las rutas de paquetes, aumentando la probabilidad de escuchas (sniffing).

Los paquetes de voz viajan “en claro” sobre redes IP, por lo que pueden ser vulnerables a escuchas no autorizadas de paquetes. A menos que se use cifrado basado en la red, todos los paquetes de voz RTP viajan en claro por la red y podrían ser capturados o copiados por cualquier dispositivo de monitorización de red.

Las redes VoIP poseen una serie de características que necesitan de requisitos de seguridad especiales. No existe el concepto de tiempo de inactividad programado en telefonía. Las indisponibilidades pueden causar indignación masiva o pánico generalizado del cliente. También podría producirse divulgación de información confidencial que, al igual que la pérdida de otro tipo de datos, podría afectar negativamente a la organización. Muchos equipos de seguridad pasan la mayor parte de su tiempo previniendo que ataques externos penetren el firewall corporativo o los servidores bastión con acceso a Internet. Sin embargo, muchas empresas hacen poco o ningún esfuerzo para proteger la infraestructura de red interna o los servidores de

⁶⁰ Khan, K., “Introduction to Voice-over IP Technology”, ISACA Journal, Volume 2, 2005, www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Introduction-to-Voice-over-IP-Technology1.aspx

los ataques desde el interior. En el contexto de las comunicaciones de voz, un ejemplo típico es un empleado que escucha las llamadas telefónicas personales o confidenciales corporativas de otro empleado.

ACCESO REMOTO⁶¹

Muchas organizaciones requieren conectividad de acceso remoto a los recursos de información para diferentes tipos de usuarios, tales como empleados, proveedores, consultores, socios de negocio y representantes de clientes. Para proporcionar esta capacidad, existe una variedad de métodos y procedimientos para satisfacer la necesidad de negocio de una organización para este nivel de acceso.

El acceso remoto basado en TCP/IP Internet es un método rentable que permite que las organizaciones aprovechen las infraestructuras de red pública y las opciones de conectividad disponibles, donde los proveedores de servicios de Internet (ISP) administran módems y servidores de llamada, y donde los módems DSL y de cable reducen todavía más los costes de la organización. Para usar de manera efectiva esta opción, las organizaciones establecen una red privada virtual sobre Internet para comunicar con seguridad los paquetes de datos a través de esta infraestructura pública. Las tecnologías VPN disponibles aplican el estándar IPsec de IETF (Internet Engineering Task Force). Las ventajas son su ubicuidad, facilidad de uso, conectividad poco costosa, y un acceso de sólo lectura, consulta o copia. Las desventajas incluyen que son considerablemente menos fiables que los circuitos dedicados, carecen de una autoridad central, y pueden presentar dificultades a la hora de resolver problemas.

Las organizaciones deberían ser conscientes de que usar VPN para permitir el acceso remoto a sus sistemas puede crear agujeros en su infraestructura de seguridad. El tráfico cifrado puede esconder acciones no autorizadas o software malicioso que puede ser transmitido a través de dichos canales. Los sistemas de detección de intrusiones (IDS) y escáneres de virus capaces de descifrar el tráfico para el análisis y a continuación cifrarlo y remitirlo al punto final VPN deberían ser considerados controles preventivos. Una buena práctica consiste en terminar todas las VPNs en el mismo punto final en un llamado concentrador de VPN, y no aceptará VPNs dirigidas a otras partes de la red. Para reducir impactos potenciales de riesgo de acceso VPN, se implementan controles de arquitectura para restringir el tráfico de acceso remoto a determinados sistemas con seguridad robustecida o protegidos contra virus, portales de acceso remoto, y segmentos de red no sensibles.

El riesgo de acceso remoto incluye:

- DoS, donde los usuarios remotos pueden no tener acceso a los datos o aplicaciones que son vitales para poder llevar a cabo su tarea cotidiana
- Terceros malintencionados que pueden tener acceso a aplicaciones críticas o a datos valiosos por medio del uso de las debilidades en el software de comunicaciones y protocolos de red
- Software de comunicaciones mal configurado, que puede tener como consecuencia el acceso o la modificación no autorizada de los recursos de información de una organización
- Dispositivos mal configurados en la infraestructura informática corporativa
- Sistemas host indebidamente asegurados que podrían ser explotados por un intruso teniendo acceso remoto
- Problemas de seguridad física en computadoras de usuarios remotos

Los controles de acceso remoto incluyen:

- Políticas y estándares
- Autorizaciones apropiadas
- Mecanismos de identificación y autenticación
- Herramientas y técnicas de cifrado, como por ejemplo el uso de VPN
- Gestión de sistemas y redes (p.ej., NAC)
- Restringir el acceso a sistemas, redes, y aplicaciones controlados

⁶¹ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

TEMA 5—SEGURIDAD DEL SISTEMA OPERATIVO

FORTALECIMIENTO DEL SISTEMA/PLATAFORMA

El fortalecimiento del sistema es el proceso de implementación de los controles de seguridad en un sistema informático. Es común que la mayoría de los proveedores de ordenadores dejen abiertos los controles predeterminados, favoreciendo la facilidad de uso por encima de la seguridad. Esto introduce vulnerabilidades significativas, a menos que el sistema sea fortalecido.

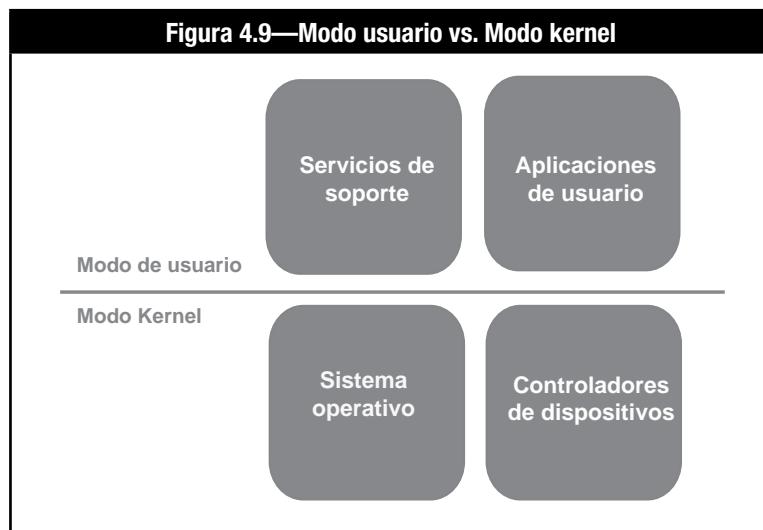
El proceso de determinar qué se robustece y hasta qué nivel varía según el sistema operativo, aplicaciones instaladas, uso del sistema/plataforma y exposición. Asimismo, los controles concretos disponibles para el fortalecimiento varían. Algunos controles comunes incluyen:

- Autentificación y autorización
- Permisos del sistema de archivos
- Privilegios de acceso
- Registro y monitorización del sistema
- Servicios del sistema
- Restricciones de configuración

Independientemente del sistema operativo específico, el fortalecimiento del sistema debería aplicar el principio de privilegios mínimos o control de acceso.

MODOS DE OPERACIÓN

La mayoría de los sistemas operativos tienen dos modos de operación—el modo **kernel** para la ejecución de instrucciones reservadas para el funcionamiento interno del sistema; y el modo **usuario** para las actividades normales. En el modo kernel, no hay protecciones de errores o actividades maliciosas y todas las partes del sistema y la memoria son accesibles. Ver la figura 4.9.



Los sistemas operativos permiten el acceso controlado a las operaciones en modo kernel mediante llamadas al sistema, que por lo general requieren privilegios. Estos privilegios se definen en base a usuarios o programas y deberían limitarse en virtud del principio de privilegios mínimos.

La mayoría de los ataques buscan obtener el acceso privilegiado o acceso en modo kernel al sistema, con el fin de eludir otros controles de seguridad.

PERMISOS DEL SISTEMA DE ARCHIVOS

Los sistemas operativos tienen sistemas de archivos que administran los archivos de datos almacenados en el sistema y proporcionan los controles de acceso para determinar qué usuarios (o programas) tienen qué tipo de acceso a un archivo. Los accesos comunes a archivos incluyen controles de creación, modificación, lectura, escritura y eliminación.

CREDENCIALES Y PRIVILEGIOS

El acceso que un usuario en particular tiene a un sistema se controla a través de una serie de mecanismos. Las credenciales de un usuario definen quiénes son y qué permisos tienen para acceder a los recursos dentro del sistema.

Las contraseñas son el mecanismo estándar para autenticar a un usuario en el sistema y deben ser administradas correctamente para asegurar que no sean fáciles de adivinar o de comprometer. La mayoría de los sistemas operativos proporcionan controles para las contraseñas, tales como longitud mínima, tiempo de vigencia para cada contraseña en particular y el número de intentos permitidos para utilizar una contraseña antes de denegar el acceso.

Otro de los controles clave de usuario son los privilegios asignados a un usuario en particular. Estos privilegios deben ser cuidadosamente seleccionados y controlados para evitar el mal uso o el compromiso. La asignación de privilegios debería seguir el principio de privilegios mínimos requeridos para que un usuario haga su trabajo.

Los administradores también pueden limitar las formas en que los usuarios pueden tener acceso a los sistemas. Por ejemplo, los administradores pueden establecer restricciones de inicio de sesión en función de la hora del día, el tiempo total de la sesión, la dirección de origen y los intentos fallidos de inicio de sesión.

FORTALECIMIENTO DE LA PLATAFORMA

Los profesionales de seguridad deben entender los tipos y funciones de las cuentas en cada plataforma que están protegiendo. Por ejemplo, Windows diferencia entre archivos y dispositivos tales como impresoras, mientras que todo en UNIX se considera como archivo, lo cual incluye los dispositivos físicos.

El fortalecimiento es un proceso que reduce la vulnerabilidad limitando los vectores de ataque que podrían ser usados como puntos de compromiso. Un sistema fortalecido es aquel que no almacena datos sensibles que no se necesitan inmediatamente para soportar una operación de negocio. Adicionalmente, toda funcionalidad innecesaria está deshabilitada, incluyendo puertos, servicios y protocolos que no son requeridos para el uso que se pretende del sistema en el entorno corporativo. Muchos dispositivos y sistemas vienen con cuentas de invitado o contraseñas por defecto que deberían ser cambiadas o deshabilitadas como parte del proceso de fortalecimiento.

El fortalecimiento de servidores es el proceso de fortalecimiento, pero aplicado a servidores. El fortalecimiento de servidores es importante para proteger los servidores de una organización frente a ataques.

Para el profesional de ciberseguridad, identificar la localización de la información crítica es imprescindible, no sólo para la seguridad, sino también para la respuesta a incidentes.

En UNIX, los directorios siguientes requieren consideración adicional:

- /etc/passwd—Mantiene información de las cuentas de usuario y contraseñas
- /etc/shadow—Conserva la contraseña cifrada de la cuenta correspondiente
- /etc/group—Contiene información de grupo para cada cuenta
- /etc/gshadow—Contiene información segura de los grupos de cuentas
- /bin—Ubicación de los archivos ejecutables
- /boot—Contiene los archivos de arranque del sistema
- /kernel—Archivos kernel
- /sbin—Contiene archivos ejecutables, a menudo para la administración
- /usr—Incluye los comandos administrativos

⁶² ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

En Windows, no se requiere mirar nada más que el Registro (Registry) – una base de datos jerárquica central que almacena los parámetros y opciones de configuración.⁶³ Una “sección” (hive) es un grupo lógico de claves, subclaves y valores del registro que tiene un conjunto de archivos de soporte y copias de seguridad de sus datos.⁶⁴

- HKEY_CURRENT_CONFIG—Contiene información volátil generada en el arranque
- HKEY_CURRENT_USER—Ajustes específicos del usuario actual
- HKEY_LOCAL_MACHINE\SAM—Contiene información de las cuentas local y de dominio
- HKEY_LOCAL_MACHINE\Security—Contiene la política de seguridad referenciada y aplicada por el kernel
- HKEY_LOCAL_MACHINE\Software—Contiene ajustes de software y Windows
- HKEY_LOCAL_MACHINE\System—Contiene información sobre la configuración de sistema de Windows
- HKEY_USERS\.DEFAULT—Perfil de la cuenta del sistema local

La mayoría de ficheros de soporte para las hives están en el directorio %SystemRoot%\System32\Config. Estos ficheros se actualizan cada vez que un usuario inicia sesión.⁶⁵

CONOCIMIENTO DE LINEAS DE COMANDO

Los profesionales de ciberseguridad a menudo utilizan herramientas de línea de comandos como parte de su rutina de seguridad. La siguiente lista proporciona 10 populares herramientas de línea de comandos para la ciberseguridad:

- **Nmap**—Escáner de puertos de red y detector de servicio
- **Metasploit**—Software de prueba de penetración
- **Aircrack-ng**—Programa de craqueo de claves 802.11 WEP y WPA-PSK
- **Snort®**—IDS/IPS de código abierto
- **Netstat**—Muestra información detallada del estado de la red
- **Netcat**—Herramienta de red que lee y escribe datos a través de conexiones de red, utilizando el protocolo TCP / IP
- **Tcpdump**—Analizador de paquetes basado en línea de comandos
- **John the Ripper**—Software de craqueo de contraseñas
- **Kismet**—Detector de red inalámbrica de capa 2 802.11, sniffer e IDS
- **OpenSSH/PuTTY/SSH**—Programa para iniciar sesión o ejecutar comandos en una máquina remota. Los comandos UNIX útiles para el profesional de ciberseguridad están listados en la **figura 4.10**.

Figura 4.10—Comandos UNIX

Comando	Descripción
finger {userid}	Mostrar información de un usuario
cat	Mostrar o concatenar archivos
cd	Cambiar de directorio
chmod	Cambia los permisos de un archivo Nota: Los permisos de UNIX se administran mediante la notación octal por usuario, grupo y otros. La manipulación de los permisos no es parte del objetivo de este material, pero es una actividad crítica conforme se avanza en la carrera de ciberseguridad.
cp	Copiar
date	Mostrar fecha y hora actual
diff	Mostrar diferencias entre archivos de texto
grep	Encontrar cadena de caracteres en un archivo

⁶³ Microsoft Press, *Microsoft Computer Dictionary, 5th edición*, EE.UU., 2002

⁶⁴ Microsoft, *Registry Hives*, <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724877%28v=vs.85%29.aspx>

⁶⁵ *Ibid*

Figura 4.10—Comandos UNIX (cont.)

Comando	Descripción
ls	Lista de directorio. Opciones útiles: -a Mostrar todos los archivos* -d Mostrar sólo los directorios -l Mostrar listado largo -u Mostrar archivos por su acceso (el más reciente primero) -U Mostrar los resultados por creación (el más reciente primero) Nota: A diferencia de Windows, UNIX no ofrece la oportunidad de “dejar visibles” los archivos ocultos. Identificados como “archivos de puntos” (del inglés “dot files”), los nombres de estos archivos comienzan con un “.”, y a continuación el nombre. Para ver estos archivos protegidos del sistema, se debe utilizar la opción -a. [ls -a ó ls -al]
man	Mostrar ayuda
mkdir	Crear un directorio
mv	Mover / Renombrar archivo
ps	Mostrar procesos activos
pwd	Mostrar el directorio actual
rm	Borrar archivo
rmdir	Borrar directorio
sort	Ordenar los datos
whoami	Muestra con qué nombre de usuario se está conectado

VIRTUALIZACIÓN

La virtualización proporciona a las empresas una oportunidad significativa para incrementar la eficiencia y reducir los costos en sus operaciones de TI.

A grandes rasgos, la virtualización permite que múltiples sistemas operativos (huéspedes o “guests” en inglés) coexisten en el mismo servidor físico (anfitrión o “host” en inglés) de forma aislada los unos de los otros. La virtualización crea una capa entre el hardware y el sistema operativo huésped para administrar los recursos de procesamiento y memoria compartida en el anfitrión. A menudo, una consola de administración proporciona acceso administrativo para gestionar el sistema virtualizado. Existen ventajas y desventajas, tal y como se muestra en la figura 4.11.

Figura 4.11—Ventajas y desventajas de la virtualización

Ventajas	Desventajas
<ul style="list-style-type: none"> Los costos de hardware de servidor pueden reducirse tanto para las compilaciones de servidor como para su mantenimiento. Varios sistemas operativos pueden compartir capacidad de procesamiento y espacio de almacenamiento que a menudo se desperdicia en los servidores tradicionales, reduciendo de este modo los costos operativos. El tamaño físico de los servidores puede reducirse dentro del centro de datos. Un mismo anfitrión (host) puede tener varias versiones del mismo sistema operativo, o incluso varios sistemas operativos, para facilitar las pruebas de las aplicaciones para determinar diferencias de rendimiento. La creación de copias duplicadas de invitados (guests) en ubicaciones alternativas puede representar un soporte a los esfuerzos de continuidad del negocio. El personal de soporte de la aplicación puede tener varias versiones del mismo sistema operativo, o incluso varios sistemas operativos, en un mismo anfitrión (host) para facilitar el soporte a los usuarios que trabajan en distintos entornos. Una misma máquina puede alojar una red de varias capas en un laboratorio de capacitación sin tener que ocuparse de configuraciones costosas de los equipos físicos. Organizaciones más pequeñas que han realizado pruebas en el entorno de producción pueden mejorar la forma de configurar entornos de desarrollo y de pruebas a nivel lógico que sean independientes y rentables. Si está bien configurado, un único control de acceso bien creado en el anfitrión (host) puede proporcionar mayor control para los múltiples invitados del anfitrión. 	<ul style="list-style-type: none"> Una configuración inadecuada del anfitrión (host) podría crear vulnerabilidades que afecten no sólo al anfitrión, sino también a los invitados. La explotación de vulnerabilidades o los ataques de denegación de servicio contra un anfitrión (host) podrían llegar a afectar a todos los invitados. Una situación comprometida en la consola de gestión podría otorgar acceso administrativo no aprobado a los invitados del anfitrión. Los problemas de rendimiento del sistema operativo propio del anfitrión podrían impactar a cada uno de los invitados de éste. Podrían producirse fugas de datos entre los invitados si el anfitrión no libera y asigna memoria de forma controlada. Los protocolos no seguros para el acceso remoto a la consola de gestión y los invitados podrían dar lugar a una exposición de las credenciales administrativas.

Fuente: ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015, figura 5.14

Si bien la virtualización ofrece ventajas significativas, también conlleva riesgos que una empresa debe gestionar de forma efectiva. Dado que el anfitrión (host) de un entorno virtualizado representa un único punto posible de fallo en el sistema, un ataque exitoso en el anfitrión podría dar lugar a una situación comprometida mayor, tanto en alcance como en impacto.

Para hacer frente a este riesgo, las empresas a menudo pueden aplicar y adaptar en un entorno virtualizado de servidores los mismos principios y buenas prácticas que se utilizarían para una granja de servidores. Estos incluyen los siguientes:

- Fuertes controles de acceso lógico y físico, especialmente a través del anfitrión (host) y su consola de gestión
- Prácticas acertadas de gestión de la configuración y fortificación del sistema para el anfitrión, incluyendo parches, antivirus, servicios limitados, registros, permisos apropiados y otros parámetros de configuración
- Una segregación de red apropiada, incluyendo evitar máquinas virtuales en la zona desmilitarizada (DMZ) y colocar herramientas de gestión en un segmento distinto de la red
- Prácticas estrictas de gestión de cambios

SISTEMAS ESPECIALIZADOS

Algunos sistemas informáticos y aplicaciones son muy especializados, y pueden tener amenazas y riesgos únicos, que requieren diferentes tipos de controles.

Ejemplos de sistemas especializados incluyen sistemas de **control de supervisión y adquisición de datos (SCADA)**, **Sistemas de control industrial (ICS)**, u otros sistemas de seguimiento o control en tiempo real, que operan en entornos especializados.

Los sistemas SCADA controlan procesos industriales y de fabricación, generación de energía, sistemas de control de tráfico aéreo, así como comunicaciones de emergencia y sistemas de defensa.

Históricamente, estos sistemas fueron diseñados como sistemas independientes (stand-alone), y debido a la naturaleza en tiempo real de sus aplicaciones, a menudo no tenían ningún software adicional que ralentizara las operaciones. Sin embargo, estos sistemas comúnmente no están en red y con frecuencia tienen pocos de los controles comunes que se encuentran en los sistemas más comerciales.

Debido a la importancia de estos sistemas en las operaciones críticas, estos pueden ser el blanco de muchos adversarios diferentes, y el impacto de un ataque exitoso puede ser catastrófico o incluso mortal.

Muchos sistemas SCADA existentes, no consideraron la seguridad en su diseño o implementación, y mientras los proveedores mejoran la seguridad, estos sistemas requieren una evaluación cuidadosa de los riesgos y amenazas y a menudo requieren controles especiales para compensar las debilidades inherentes.

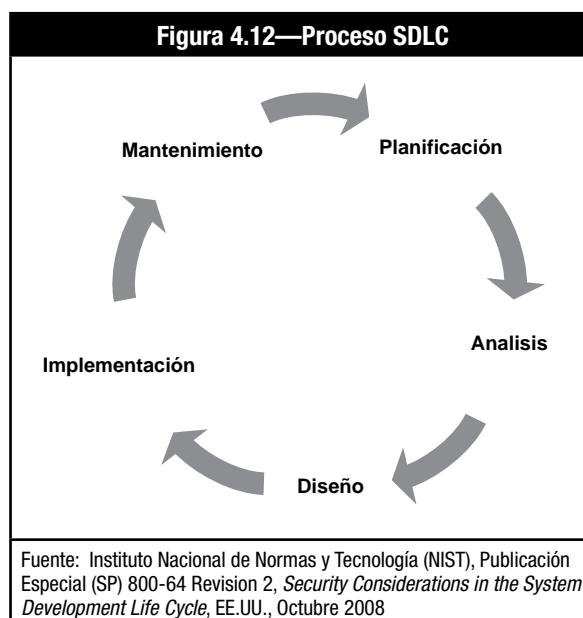
Página dejada en blanco intencionadamente

TEMA 6—SEGURIDAD DE LAS APLICACIONES

Las aplicaciones inseguras dejan expuesta su organización a atacantes externos, que pueden tratar de utilizar código no autorizado para manipular las aplicaciones y acceder, robar, modificar o eliminar información confidencial. Se deben aplicar medidas de seguridad de aplicaciones durante la fase de diseño y desarrollo de la aplicación, seguidas de contramedidas de seguridad rutinarias utilizadas durante todo el ciclo de vida.

CICLO DE VIDA DEL DESARROLLO DE SISTEMAS (SDLC)

Las organizaciones a menudo dedican recursos importantes (por ejemplo, personas, aplicaciones, instalaciones y tecnología) para desarrollar, adquirir, integrar y mantener los sistemas de aplicaciones, que son fundamentales para el funcionamiento eficaz de los procesos clave del negocio. El proceso SDLC, que se muestra en la **figura 4.12**, guía las fases desplegadas en el desarrollo o la adquisición de un software y, dependiendo de la metodología, incluso puede incluir el retiro controlado del sistema.



El SDLC incluye:

- Los procesos de TI para la gestión y control de la actividad del proyecto
- Un objetivo para cada fase del ciclo de vida, que se describe típicamente con resultados clave, una descripción de las tareas recomendadas y un resumen de los objetivos de control relacionados para la gestión eficaz
- Pasos incrementales o entregables que sientan las bases para la siguiente fase

Específicamente, el SDLC es un proceso formal para caracterizar los requisitos de diseño y debe incluir:

- Los requisitos de negocio que contengan descripciones de lo que un sistema debe hacer
- Los requisitos funcionales y los casos de uso que describan cómo los usuarios interactúan con un sistema
- Los requisitos técnicos, las especificaciones de diseño y de codificación describan cómo el sistema va a interactuar, las condiciones en las que el sistema funcionará y los criterios de información que el sistema deberá cumplir
- Los requisitos de mitigación y control de riesgos, para proteger la integridad del sistema, la confidencialidad de la información almacenada, procesada o comunicada, así como mecanismos de autenticación y autorización adecuados

Seguridad dentro del SDLC

El diseño y la implementación de los controles a menudo se llevan a cabo como un proyecto de desarrollo de sistemas. Si bien hay varias técnicas de gestión de proyectos que pueden ser utilizadas para gestionar proyectos de desarrollo de sistemas, deben ser una parte integral y tan importante como otras, dentro del proceso del SDLC.

Requerimientos de diseño

No tener en cuenta la seguridad en el diseño de un sistema o aplicación, es uno de los principales factores que contribuyen a las vulnerabilidades de la ciberseguridad de hoy en día, por lo que es más fácil que los sistemas se vean comprometidos. Con demasiada frecuencia la seguridad es tenida en cuenta en el último momento, y sólo después de identificar debilidades, siendo entonces aplicados controles de manera “ad hoc”.

La seguridad y mitigación de riesgos deberían ser criterios formales de diseño en cualquier proceso de SDLC, comenzando con la evaluación de las amenazas y riesgos del sistema propuesto, la identificación de los controles, la implementación de dichos controles, pruebas y revisión.

Los diez riesgos OWASP más importantes (OWASP Top Ten)

El Proyecto abierto de seguridad de aplicaciones web (del inglés Open Web Application Security Project, OWASP) publica una lista de los 10 riesgos de seguridad de aplicaciones más importantes. La **Figura 4.13** muestra los diez riesgos de seguridad de aplicaciones más importantes en el año 2013.

Figura 4.13—Los diez riesgos de seguridad de aplicaciones más importantes en 2013

Vector de ataque	Descripción del Riesgo de seguridad
Inyección	Los fallos de inyección ocurren cuando los datos que no son de confianza, se envían a un intérprete. El atacante puede engañar al intérprete para que ejecute comandos involuntariamente o acceder a datos no autorizados. Los fallos de inyección son frecuentes y, a menudo se encuentran en las consultas SQL y LDAP, así como en comandos del sistema operativo.
Ruptura de la autenticación y gestión de la sesión	Si una función de aplicación relacionada con la autenticación o gestión de sesiones no se implementa correctamente, puede permitir a un usuario malintencionado poner en peligro las contraseñas, claves o tokens de sesión y suplantar a los usuarios legítimos.
Cross-Site Scripting (XSS)	Los fallos XSS ocurren cuando una aplicación toma datos que no son de confianza y los envía a un navegador web sin la validación adecuada. Esto es el fallo más frecuente de seguridad de aplicaciones web. Los atacantes pueden utilizar XSS para secuestrar sesiones de usuario, insertar contenido hostil, desconfigurar sitios web y redirigir a los usuarios.
Referencias directas a objetos inseguras	Una referencia directa a un objeto se produce cuando un desarrollador expone una referencia a un objeto de implementación interna. Los atacantes pueden manipular estas referencias para acceder a datos no autorizados.
Mala configuración de seguridad	Configuraciones de seguridad se deben definir, implementar y mantener en aplicaciones, marcos, servidores de aplicaciones, servidores web, servidores de bases de datos y plataformas. Una mala configuración de seguridad puede dar a los atacantes el acceso no autorizado a los datos o la funcionalidad del sistema.
Exposición de datos confidenciales	Si las aplicaciones web no garantizan adecuadamente los datos sensibles a través del uso de cifrado, los atacantes pueden robar o modificar los datos sensibles, tales como los registros de salud, tarjetas de crédito, identificaciones fiscales y las credenciales de autenticación.
Falta de control de acceso a nivel de función	Cuando no se verifican los derechos de acceso de nivel de la función, los atacantes pueden falsificar las solicitudes para acceder a la funcionalidad sin autorización.
Falsificación de petición en sitios cruzados (del inglés Cross-Site Request Forgery, CSRF)	Un ataque CSRF se produce cuando un atacante obliga al navegador del usuario a enviar peticiones HTTP falsificadas, incluyendo las “cookies” de sesión. Esto permite a un atacante engañar a las víctimas para realizar operaciones en sitios web ilegítimos.
Uso de componentes con vulnerabilidades conocidas	Ciertos componentes, tales como bibliotecas, marcos y otros módulos de software generalmente se ejecutan con privilegios completos. Los atacantes pueden explotar un componente vulnerable para acceder a datos o hacerse cargo de un servidor.
Redireccionamientos y reenvíos no validados	Las aplicaciones Web con frecuencia re-direccinan o re-envían a los usuarios a otras páginas. Cuando se utilizan datos no confiables para determinar el destino, un atacante puede redirigir las víctimas a sitios de phishing o malware.

Los controles de aplicación son controles sobre las funciones de entrada, procesamiento y salida de datos. Incluyen métodos para ayudar a asegurar la precisión, completud, validez, verificabilidad y consistencia, logrando así la integridad y confiabilidad de los datos.

Los controles de aplicación pueden consistir en pruebas de edición; totales; conciliaciones e identificación; así como la notificación de datos incorrectos, faltantes o excepciones. Los controles automatizados deben estar acoplados con procedimientos manuales para asegurar la investigación adecuada de las excepciones. La implementación de estos controles ayuda a asegurar la integridad del sistema, que las funciones relacionadas del sistema operan como se pretende y que la información contenida en el sistema es relevante, confiable, segura y está disponible cuando se le necesita. Los controles de aplicación incluyen:

- Cortafuegos (firewalls)
- Programas de cifrado
- Programas contra software malintencionado (anti-malware)
- Programas de detección/eliminación de spyware
- Autenticación biométrica

Para reducir los riesgos de seguridad de aplicaciones, OWASP recomienda lo siguiente:

- Definir los requisitos de seguridad de la aplicación.
- Utilizar buenas prácticas de arquitectura de seguridad de aplicación desde el comienzo del diseño de la aplicación.
- Implementar controles de seguridad fuertes y utilizables.
- Integrar la seguridad en el ciclo de vida del desarrollo.
- Estar al día sobre vulnerabilidades de aplicaciones.

Pruebas

La fase de pruebas del SDLC incluye:

- Verificar y validar que un programa, subsistema o aplicación, y los controles de seguridad diseñados, realizan las funciones para las que han sido diseñados
- Determinar si las unidades que se están probando, operan sin ningún mal funcionamiento o efectos adversos sobre otros componentes del sistema
- Una variedad de metodologías de desarrollo y requisitos organizacionales para proporcionar una amplia gama de planes o niveles de prueba

Desde una perspectiva de seguridad, esto debería incluir pruebas de vulnerabilidad y control.

Proceso de revisión

Los procesos de revisión de código pueden abarcar desde procesos informales hasta procesos muy formales, equipos de revisión o inspecciones de código. La seguridad debería estar integrada como parte de cualquier proceso de revisión.

SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

Los entornos de desarrollo y pruebas son relativamente abiertos y con frecuencia tienen un menor número de controles de acceso, debido a la naturaleza colaborativa del proceso de desarrollo. Es importante separar los entornos de desarrollo, prueba y producción, para minimizar la posibilidad de un compromiso o una mala configuración sean introducidos o arrastrados a través del proceso.

Se deberían usar diferentes controles de acceso (credenciales) en los diferentes entornos.

Además, si los datos de producción se utilizan en el entorno de prueba, la información privada o de identificación personal debe ser mezclada, de modo que la información confidencial no sea dada a conocer inadvertidamente.

Desarrollo Ágil

La metodología Ágil permite gestionar proyectos, incluido el desarrollo de software, de manera más flexible. Se han reportado múltiples beneficios derivados del uso de metodologías ágiles frente al tradicional desarrollo en cascada; sin embargo, no ha sido adoptado de manera regular en el mundo de la seguridad. En lugar de llevar a cabo test de penetración y otras medidas de seguridad en fases tempranas del proceso, éstas se aplican cerca de su finalización, haciéndola más difícil efectuar cambios como respuesta a dichos tests. Esto puede derivar en el uso de métodos alternativos (workarounds) y el desarrollo de parches destinados a llegar a una fecha límite de lanzamiento, lo cual es diagonalmente opuesto a una visión más razonada y segura de las soluciones.

La metodología ágil, por el contrario, ofrece oportunidades para reevaluar el proyecto desde el propio proyecto, permitiendo muchas oportunidades para realizar test desde fases tempranas. Este enfoque permite adaptar la planificación a los resultados de los tests y así poder desarrollar soluciones más maduras en vez de arreglar con urgencia problemas desconocidos.

Desarrollo y Operaciones TI (DevOps)⁶⁶

DevOps combina los conceptos de desarrollo ágil, infraestructuras ágiles y operaciones flexibles, para permitir el lanzamiento rápido y continuo de versiones y la mejora continua en la creación de valor en las TI. La corriente DevOps se originó debido a la frustración de grupos de TI con herramientas y procesos disfuncionales y deficientes, con el objetivo de lograr que el desarrollo de software y las operaciones fueran más eficientes y menos costosas.

⁶⁶ ISACA, *DevOps Overview*, EE.UU., 2015, www.isaca.org/dev-ops

Los DevOps dividen los proyectos grandes en entregables más pequeños y en múltiples desarrollos, lo que facilita la gestión desde el diseño hasta la puesta en marcha y las operaciones. Los desarrollos frecuentes e iterativos pueden ser orquestados para ser movidos en bloque entre diversos grupos hasta su puesta en producción, minimizando así el riesgo de disruptores. Los pequeños despliegues son más sencillos de depurar a lo largo del proceso de desarrollo y permanecen estables tras su puesta en producción.

A continuación se indican algunos beneficios relativos al rendimiento del negocio en el uso de metodologías DevOps son:

- Reduce el tiempo de comercialización
- Retorno de versión más rápido
- Alto rendimiento
- Mejora de la calidad
- Satisfacción del cliente
- Reducción de la complejidad de las TI
- Mejora del rendimiento del proveedor y de los partners de negocio
- Reducción de las amenazas debidas al factor humano

Los posibles desafíos en el uso de metodologías DevOps incluyen:

- Tener una idea equivocada sobre lo que significa DevOps
- Pensar que los asuntos relativos al cumplimiento y la seguridad no conciernen DevOps
- Necesidad de automatización
- Falta de habilidades
- Cultura de la organización
- Miedo al cambio
- Mentalidad cerrada

AMENAZAS ADICIONALES

Es importante para el profesional de la seguridad de la información reconocer que hay muchas fuentes de asesoramiento en materia de seguridad, de mejores prácticas y de recomendaciones. El hecho que una amenaza no aparezca en una lista “top” de un año en concreto no significa que pueda olvidarse de ella.

Otras amenazas de seguridad a tener en cuenta son:

- **Canal encubierto (covert channel)**—Medio para transferir de forma ilícita información entre sistemas que usan la infraestructura existente. Los canales encubiertos son ataques simples y sigilosos que a menudo pasan desapercibidos.
- **Condición de carrera (race condition)**—Según Rouse, “una situación indeseable que se produce cuando un dispositivo o sistema intenta realizar dos o más operaciones al mismo tiempo, pero debido a la naturaleza del dispositivo o sistema, las operaciones deben realizarse en la secuencia correcta con el fin de hacerse correctamente”.⁶⁷ Las condiciones de carrera varían; sin embargo, estas vulnerabilidades ofrecen oportunidades para accesos a la red no autorizados.
- **Ataque orientado a retorno**—Técnica utilizada frecuentemente para explotar las vulnerabilidades de corrupción de memoria. En pocas palabras, permite a un atacante ejecutar código a pesar de los avances tecnológicos tales como pilas (stacks) no ejecutables y montículos (heaps) no ejecutables. Las vulnerabilidades de corrupción de memoria se producen “cuando un programa privilegiado está obligado a corromper su propio espacio de memoria, de manera que las áreas de memoria corrompidas tienen un impacto en el funcionamiento seguro del programa”.⁶⁸
- **Esteganografía**—El arte o la práctica de ocultar un mensaje, imagen o archivo dentro de otro mensaje, imagen o archivo. Los archivos multimedia son ideales debido a su gran tamaño.

⁶⁷ Rouse, Margaret, “Race Condition,” Septiembre 2005, <http://searchstorage.techtarget.com/definition/race-condition>

⁶⁸ Herath, Nishad, “The State of Return Oriented Programming in Contemporary Exploits,” Security Intelligence, 3 Marzo 2014, <http://securityintelligence.com/return-oriented-programming-rop-contemporary-exploits/#.VFkNEBa9bD0>

TEMA 7—SEGURIDAD DE LOS DATOS

Las bases de datos pueden ser protegidas individualmente con controles similares a las protecciones aplicadas a nivel del sistema. Los controles específicos que se pueden aplicar en el nivel de base de datos incluyen:

- Autenticación y autorización de acceso
- Controles de acceso que limiten o controlen los tipos de datos accesibles y qué tipos de accesos se permiten (como sólo lectura, lectura y escritura, o borrado).
- Monitorización de registro y otras transacciones
- Controles de cifrado e integridad
- Copias de seguridad

Los controles que se utilizan para proteger las bases de datos deben ser diseñados conjuntamente con los controles del sistema y las aplicaciones, formando otra capa de protección en un esquema de defensa en profundidad.

CLASIFICACIÓN DE DATOS

La información usada por una organización puede tener un valor e importancia variables. Por ejemplo, alguna información puede ser pública y requiere una protección mínima, mientras que otra información, como la información de seguridad nacional, salud u otro tipo de información personal o secretos comerciales, podría acarrear un daño significativo para la organización en caso de que fuera publicada, borrada o modificada accidentalmente.

Es importante que la organización comprenda la sensibilidad de la información y clasifique los datos en función de su confidencialidad y el impacto de la publicación o pérdida de la información.

La clasificación de datos funciona mediante el etiquetado de los datos con los metadatos basados en una taxonomía de clasificación. Esto permite que los datos se puedan encontrar de forma rápida y eficiente, reduce los costes relativos al almacenamiento y las copias de seguridad, y ayuda a asignar y maximizar los recursos. El número de niveles de clasificación debe mantenerse al mínimo. Deben ser designaciones simples que asignan diferentes grados de sensibilidad y criticidad.

La clasificación de datos debe ser definida en una política de clasificación de los datos que proporcione la definición de las diferentes clases de información y cómo cada clase de información debe ser manejada y protegida. Además, el esquema de clasificación debe expresar la asociación de los datos y de sus procesos de apoyo al negocio.

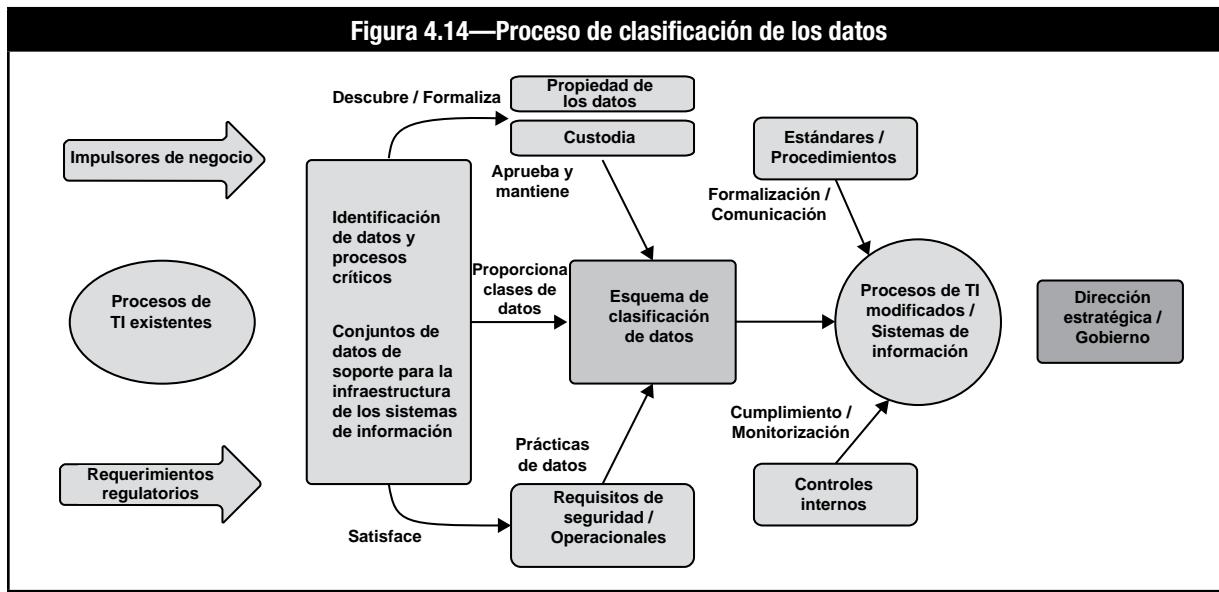
En algunos casos, las regulaciones locales pueden afectar a la clasificación y manejo de los datos, tales como los controlados por leyes de protección de datos. Por ejemplo, la Ley Sarbanes-Oxley de Estados Unidos define qué registros de datos deben almacenarse y por cuánto tiempo.

La información también puede necesitar ser reclasificada en base a los cambios en su importancia. Por ejemplo, antes del lanzamiento de un producto, los detalles del diseño, precios y otros datos pueden ser confidenciales y necesitan una protección significativa; sin embargo, después de la presentación del producto, esta información puede llegar a ser pública y no requiere el mismo nivel de protección.

PROPIETARIOS DE LOS DATOS

Otra consideración importante para la seguridad de los datos es definir el propietario de los datos. A pesar de que TI aplica los controles de seguridad y vigilancia de los datos empresariales, los datos no pertenecen a TI. La información del negocio pertenece en última instancia al responsable de los procesos del negocio. El propietario es generalmente responsable de establecer la clasificación de los datos y, por lo tanto, del nivel de protección requerido. El propietario de los datos puede ser un individuo que crea los datos o una entidad organizacional que actúa como custodio de la información. El proceso de clasificación de los datos se muestra en la **figura 4.14**.

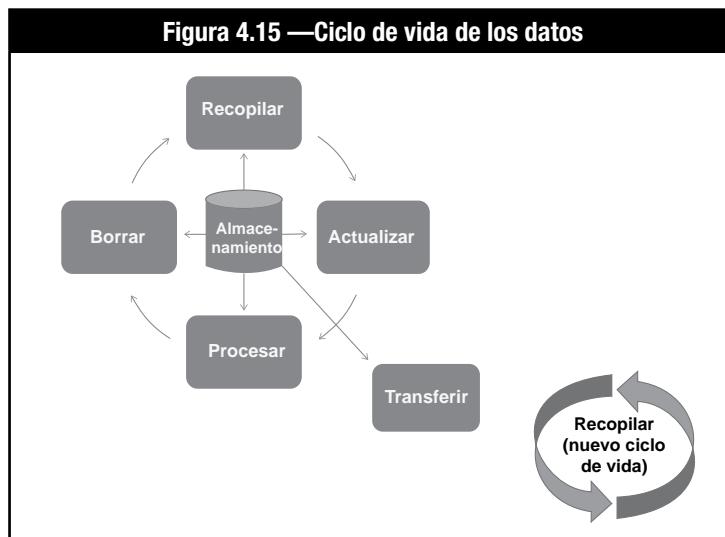
Figura 4.14—Proceso de clasificación de los datos



Al clasificar los datos, se deben considerar los siguientes requisitos:

- **Acceso y autenticación**—Determinar los requisitos de acceso, incluyendo la definición de perfiles de usuarios, criterios de aprobación de acceso y procedimientos de validación.
- **Confidencialidad**—Determinar donde se almacenan los datos confidenciales y cómo se transmiten.
- **Privacidad**—Usar controles para alertar a un usuario afectado de que su información está a punto de ser utilizada.
- **Disponibilidad**—Determinar las tolerancias en el tiempo de actividad (uptime) y el tiempo de inactividad (downtime) para los diferentes tipos de datos.
- **Propiedad y distribución**—Establecer procedimientos para proteger los datos ante copia y distribución no autorizada.
- **Integridad**—Proteger los datos de cambios no autorizados mediante los procedimientos de control de cambios, y la monitorización y detección automática de cambios y manipulaciones no autorizadas.
- **Retención de datos**—Determinar los períodos de retención y preservar versiones específicas de software, hardware, credenciales de autenticación y claves de cifrado, para asegurar la disponibilidad.
- **Auditabilidad**—Mantener un registro de acceso, autorizaciones, cambios y transacciones.

Después de la asignación de la clasificación de datos, se pueden establecer controles de seguridad tales como cifrado, autenticación y registro. Las medidas de seguridad deben aumentar a medida que el nivel de confidencialidad o criticidad de los datos aumenta. El ciclo de vida completo de datos se muestra en la **figura 4.15**.



SEGURIDAD DE BASES DE DATOS

La seguridad de bases de datos comprende un amplio rango de controles de seguridad de la información para proteger las bases de datos de una organización. La seguridad de bases de datos es fundamental, ya que contienen información crítica y sensible necesaria para la gestión de negocio. Las bases de datos son vulnerables a riesgos, incluyendo:

- Actividades no autorizadas por parte de usuarios autorizados
- Infección o interacción con malware
- Problemas de espacio
- Daño físico
- Fallos de diseño
- Corrupción de datos

La seguridad de bases de datos se alcanza mediante las siguientes medidas:⁶⁹

- Cifrado de la información sensible en la base de datos
- Hacer uso de las vistas para restringir la información disponible al usuario
- Securizar los protocolos de comunicación con la base de datos
- Control de accesos basados en contenidos que restrinjan el acceso a registros sensibles
- Restringir el acceso con rol de administrador
- Indexado eficiente para mejorar las peticiones de datos
- Copias de seguridad de las bases de datos
- Copias de seguridad de los diarios de transacciones (remote journaling)
- Integridad referencial
- Integridad de entidad
- Validación de la entrada de datos
- Campos de datos definidos (esquemas)
- Acceso por red restringido o segregado

⁶⁹ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

SECCIÓN 4—EVALUACIÓN DE CONOCIMIENTOS

1. Ponga los pasos de la fase de pruebas de penetración en el orden correcto.
 - A. Ataque
 - B. Descubrimiento
 - C. Presentación de informes
 - D. Planificación

2. El fortalecimiento de la seguridad del sistema debe aplicar el principio de _____ o _____.
 - A. Gobierno corporativo, cumplimiento
 - B. Menor privilegio, control de acceso
 - C. Inspección de estado, acceso remoto
 - D. Evaluación de vulnerabilidades, mitigación del riesgo

3. Seleccione todas las opciones que apliquen. ¿Cuáles de las áreas funcionales siguientes son consideradas de gestión de red, de acuerdo con la norma ISO?
 - A. Gestión de contabilidad
 - B. Gestión de fallas
 - C. Gestión de firewalls
 - D. Gestión del rendimiento
 - E. Gestión de la seguridad

4. La virtualización consiste en:
 - A. la creación de una capa entre los controles de acceso físico y lógico.
 - B. múltiples sistemas operativos que coexisten en el mismo servidor, aislados unos de otros.
 - C. el uso simultáneo del modo kernel y del modo de usuario.
 - D. interrogación DNS, consultas WHOIS y búsqueda (sniffing) en la red

5. La gestión de las vulnerabilidades comienza con la enumeración de los activos de ciberseguridad y sus respectivas ubicaciones, lo que se puede lograr a través de:
 - A. escaneo (Scanning) de vulnerabilidad.
 - B. prueba de penetración.
 - C. el mantenimiento de un inventario de activos.
 - D. el uso de herramientas de línea de comandos.

Ver respuestas en el Anexo C.



CYBERSECURITY NEXUS

Sección 5:

Respuesta a Incidentes

Los temas tratados en esta sección incluyen:

1. Evento vs. Incidente
2. Respuesta a incidentes de seguridad
3. Investigaciones, retenciones legales y preservación
4. Informática Forense
5. Planes de recuperación de desastres y de continuidad del negocio

Página dejada en blanco intencionadamente

TEMA 1—EVENTO VS. INCIDENTE

Todas las organizaciones necesitan hacer un esfuerzo significativo para protegerse a sí mismos y para prevenir ciberataques de tal manera que éstos no causen daños o interrupciones. Sin embargo, los controles de seguridad no son perfectos y no pueden eliminar por completo todos los riesgos; por lo tanto, es importante que las organizaciones estén preparadas y sean capaces de detectar y gestionar los potenciales problemas de ciberseguridad.

EVENTO VS. INCIDENTE

Es importante distinguir entre evento y un incidente debido a que los dos términos se utilizan a menudo como sinónimos, a pesar de que tienen diferentes significados. Un evento es cualquier cambio, error o interrupción dentro de una infraestructura de TI como puede ser un fallo del sistema, un error de disco o que un usuario olvide su contraseña. El Instituto Nacional de Normas y Tecnología (NIST) define un evento como “cualquier ocurrencia observable en un sistema o red.”⁷⁰

Si bien hay un acuerdo general en lo que es un evento, hay una mayor variedad en la definición de un incidente. NIST define un incidente como “una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.” Otra definición de uso común es “El intento o éxito en el acceso no autorizado, uso, revelación, modificación o pérdida de información o la interferencia con las operaciones de red o de sistemas”. Muchas organizaciones definen un incidente como la actividad de un agente de amenaza humana. Otros podrían incluir cualquier cosa disruptiva, incluyendo un mandato judicial para el descubrimiento de la información electrónica o la disruptión debida a un desastre natural.

Independientemente de la definición exacta utilizada por una organización en particular, es importante distinguir entre los eventos que se manejan en el curso normal de los negocios y los incidentes que requieren la experiencia en seguridad e investigación para gestionarlos.

TIPOS DE INCIDENTES

Un incidente de ciberseguridad es un evento adverso que afecta negativamente a la confidencialidad, integridad y disponibilidad de los datos. Los incidentes de ciberseguridad pueden ser involuntarios, como el que alguien olvide activar una lista de acceso en un router, o intencionales, como un ataque dirigido por un hacker. Estos eventos también se pueden clasificar como técnicos o físicos. Los incidentes técnicos incluyen virus, malware, ataques de denegación de servicio (DoS) y fallos del sistema. Los incidentes físicos pueden incluir ingeniería social y la pérdida o robo de ordenadores portátiles o dispositivos móviles.

⁷⁰ Instituto Nacional de Normas y Tecnología (NIST), *Publicación Especial 800-61 Revision 2, Computer Security Incident Handling Guide*, EEUU, Agosto 2012

Hay muchos tipos de incidentes relacionados con la ciberseguridad, y nuevos tipos de incidentes emergen frecuentemente. El US-CERT proporciona un conjunto de términos y sus relaciones desarrollados a partir del NIST SP 800-61 Revision 2, tal y como muestra la **figura 5.1**.

Figura 5.1—Taxonomía de los vectores de ataque		
Vector de ataque	Descripción	Ejemplo
Desconocido	La causa del ataque no está definida.	Esta opción es aceptable si la causa (vector) es desconocida antes del informe inicial. El vector de ataque puede ser actualizado en posteriores reportes.
Desgaste	Un tipo de ataque que hace uso de métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios	La denegación de servicio pretende impedir o denegar el acceso a una aplicación; se trata de fuerza bruta contra un mecanismo de autenticación, como contraseñas o firmas digitales
Web	Un ataque realizado desde una página web o una aplicación basada en web.	Los ataques XSS se emplean para robar credenciales o redireccionar a un sitio que explota alguna vulnerabilidad del navegador para instalar malware
Correo electrónico/Phishing	Ataque realizado mediante correo electrónico o ficheros adjuntos	Exploit enmascarado como documento adjunto o un enlace a un sitio malicioso contenido en el cuerpo del correo electrónico
Medios externos/removibles	Un ataque realizado desde dispositivos externos o periféricos	Código malicioso que se distribuye en un sistema desde una memoria externa infectada
Impersonar/Spoofing	Ataque que implica el reemplazo de servicios o contenidos legales por otros maliciosos	Los ataques de suplantación, hombre en el medio, puntos de acceso inalámbricos hostiles e inyección SQL implican impersonar.
Uso inadecuado	Incidente resultante de la violación, por parte de un usuario autorizado, de las políticas de una organización acerca del uso aceptable, excluyendo las categorías anteriormente descritas	La instalación, por parte de usuarios, de aplicaciones para compartir ficheros o la realización de actividades ilegales en un sistema son las principales causas de pérdida de datos sensibles.
Pérdida o robo de equipamiento	La pérdida o robo de un dispositivo o medio usado por una organización	Teléfonos móviles o portátiles mal ubicados
Otra fuente	Un método de ataque que no encaja en ningún otro vector	

Fuente: US-CERT, "Attack Vectors Taxonomy," US-CERT Federal Incident Notification Guidelines, EEUU,
<https://www.us-cert.gov/incident-notification-guidelines>

La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) proporciona una taxonomía para los incidentes, que se muestra en la **figura 5.2**.

Figura 5.2—Taxonomía de la Red Europea CSIRT		
Clase de incidente (campo de entrada obligatorio)	Tipo de incidente (campo de entrada opcional pero deseable)	Descripción/Ejemplos
Contenido abusivo	Spam	Correo electrónico masivo no solicitado, lo que significa que el receptor no ha permitido de manera verificable que el correo electrónico le sea enviado, y que ese mensaje se ha enviado como parte de una colección de mensajes muy grandes, todos con igual contenido
	Discurso dañino	Desacreditación o discriminación de una persona (p.e., ciber acoso, racism o amenazas contra uno o varios individuos)
	Infantil/Sexual/Violencia	Pornografía infantil, exaltación de la violencia, etc.
Código malicioso	Virus	Software que se incluye o instala intencionadamente en un sistema con fines dañinos. Normalmente, se necesita cierta interacción con el usuario para activar el código.
	Gusano	
	Troyano	
	Spyware	
	Marcador	
	Rootkit	

Figura 5.2—Taxonomía de la Red Europea CSIRT (cont.)

Clase de incidente (campo de entrada obligatorio)	Tipo de incidente (campo de entrada opcional pero deseable)	Descripción/Ejemplos
Recolectar información	Escaneo	Ataques que envían peticiones a un sistema para descubrir puntos débiles. Esto también incluye algunos tipos de procedimientos de test para recopilar información acerca de los hosts, los servicios y las cuentas. Ejemplos: fingerd, interrogación DNS, ICMP, SMTP (EXPN, RCPT, etc.).
	Sniffing	Observar y almacenar el tráfico de red (wiretapping)
	Ingeniería social	Recolectar información proveniente de personas de manera no técnica (p.e., engaños, trucos, sobornos o amenazas)
Intentos de intrusión	Explotar vulnerabilidades conocidas	Un intento de comprometer un sistema o de interrumpir un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado como un nombre CVE (p.e., desbordamiento de buffer, puertas traseras, XSS, etc.).
	Intentos de acceso	Múltiples intentos de acceso (adivinar/romper contraseñas, fuerza bruta)
	Firma de un nuevo ataque	Un intento utilizando un exploit desconocido
Intrusiones	Compromiso de una cuenta privilegiada	Comprometer con éxito un sistema o una aplicación (servicio). Esto puede haber sido causado remotamente por una vulnerabilidad conocida o desconocida, pero también por un acceso local no autorizado. También incluye formar parte de una Botnet (red de computadoras infectadas con código malicioso).
	Compromiso de una cuenta no privilegiada	Comprometer con éxito un sistema o una aplicación (servicio). Esto puede haber sido causado remotamente por una vulnerabilidad conocida o desconocida, pero también por un acceso local no autorizado. También incluye formar parte de una Botnet (red de computadoras infectadas con código malicioso).
	Compromiso de una aplicación	
	Bot	
Disponibilidad	DoS	Mediante este tipo de ataque, un sistema es bombardeado con tal cantidad de paquetes que las operaciones que estaba realizando se retrasan llegando incluso a colapsarse. Ejemplos de DoS son inundación de ICMP o SYN, ataques de derribo y bombardeo de correos. Los ataques de DDoS habitualmente están basados en DoS desde redes de robots, aunque también existen otros escenarios, como los de amplificación DNS.
	DDoS	
	Sabotaje	
	Apagón (sin ser voluntario)	
Seguridad del contenido de la información	Acceso no autorizado a la información	Además del abuso local en datos y sistemas, la seguridad de la información puede peligrar por el compromiso de una cuenta o aplicación. Del mismo modo, son posibles los ataques que interceptan y acceden a la información durante la transmisión (wiretapping, spoofing o hijacking). La causa también puede ser fallo humano, de configuración o de software.
	Modificación no autorizada de la información	
Fraude	Uso no autorizado de recursos	Usar recursos con propósitos no autorizados incluye campañas con fines lucrativos (p.e., emplear el correo electrónico para participar en cadenas de correo provechosas o esquemas piramidales)
	Copyright	Vender o instalar copias comerciales de software sin licencia u otros materiales con derechos de autor (Warez)
	Atacantes que suplantan/secuestran identidades	Tipos de ataques en los que una entidad ilegítima toma la identidad de otra para obtener algún beneficio
	Phishing	Enmascararse como otra entidad con el fin de persuadir al usuario a que revele credenciales privadas.
Vulnerable	Abiertos al abuso	Solucionadores abiertos, impresoras accesibles a todo el mundo, vulnerabilidades aparentes desde Nessus, etc, escaneos, virus, firmas sin actualizar, etc.
Otra fuente	Todos los incidentes que no encajen en ninguna otra categoría deben ser incluidos en esta clase.	Si aumenta el número de incidentes pertenecientes a esta categoría, es un indicador de que el esquema de clasificación debe ser revisado.
Prueba	Destinado a la prueba	Destinado a la prueba.

Fuente: ENISA, Existing taxonomies, www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

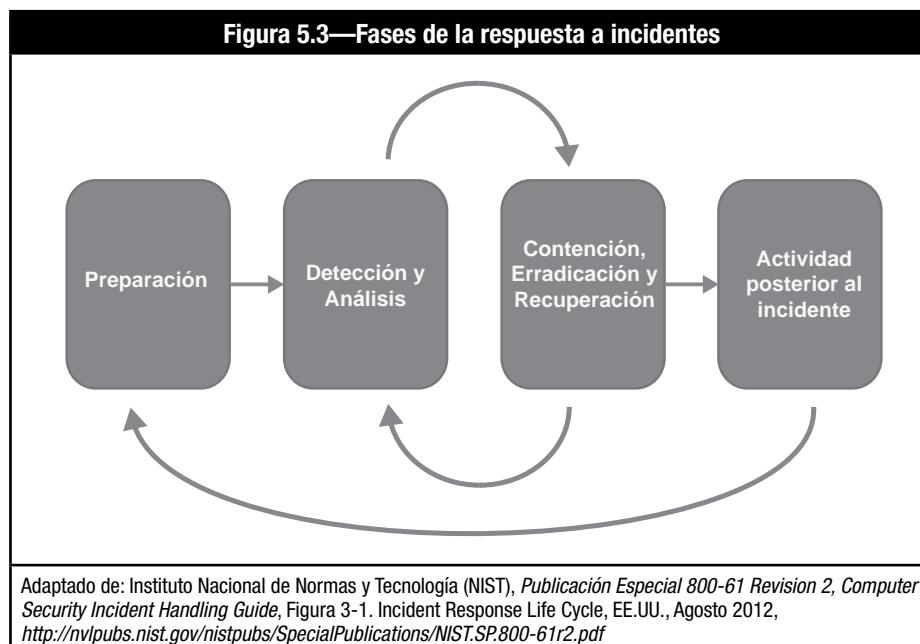
Página dejada en blanco intencionadamente

TEMA 2—RESPUESTA A INCIDENTES DE SEGURIDAD

¿QUÉ ES LA RESPUESTA A INCIDENTES?

La respuesta a incidentes es un programa formal que prepara una entidad para un incidente. Las fases de respuesta a incidentes se muestran en la **figura 5.3**. La respuesta a incidentes generalmente incluye:

1. **Preparación** para establecer los roles, responsabilidades y planes de cómo será manejado un incidente
2. Capacidades de **detección y análisis** para identificar incidentes tan pronto como sea posible y evaluar eficazmente la naturaleza del incidente
3. Capacidad de **investigación** si se requiere la identificación de un adversario
4. Procedimientos de **mitigación y recuperación** para contener el incidente, reducir las pérdidas y volver las operaciones a la normalidad
5. **Análisis posterior al incidente** para determinar las acciones correctivas que prevengan los incidentes similares en el futuro



¿POR QUÉ NECESITAMOS DE LA RESPUESTA A INCIDENTES?

Esperar hasta que ocurra un incidente para averiguar qué hacer es una llamada al desastre. Una planificación e implementación adecuada de la respuesta a incidentes permite a una organización responder a un incidente de una manera sistemática, que sea más eficaz y oportuna. Las organizaciones que no planifican para un incidente de ciberseguridad sufrirán mayores pérdidas durante un período más largo de tiempo. La tendencia actual muestra un aumento en las ocurrencias de incidentes. Estos ataques son cada vez más sofisticados y se traducen en pérdidas crecientes.

Además, muchos reglamentos nacionales y normas internacionales exigen el desarrollo de las capacidades de respuesta a incidentes. El cumplimiento de normativas proporciona requisitos estrictos en políticas de seguridad y respuesta a incidentes.

ELEMENTOS DE UN PLAN DE RESPUESTA A INCIDENTES (IRP)⁷¹

Un enfoque común para el desarrollo de un IRP es un modelo de respuesta a incidentes de seis fases que incluye preparación, identificación, contención, erradicación, restauración y seguimiento:

- **Preparación**—Esta fase prepara a una organización para desarrollar un IRP antes de que ocurra un incidente. Una preparación suficiente facilita una ejecución sin problemas. Las actividades en esta fase incluyen:
 - Establecer un enfoque para manejar incidentes
 - Establecer una política y advertencias en los sistemas de información para disuadir intrusos y permitir la recopilación de información
 - Establecer un plan de comunicación con las partes interesadas

⁷¹ ISACA, *Manual de Preparación al Examen CISM 15^a edición*, EE.UU., 2016

- Desarrollar criterios sobre cuándo reportar un incidente a las autoridades
 - Desarrollar un proceso para activar al equipo de gestión de incidentes
 - Establecer una ubicación segura para ejecutar el IRP
 - Asegurar la disponibilidad de los equipos necesarios
- **Identificación**—Esta fase tiene como propósito verificar si ha ocurrido un incidente y encontrar más detalles del mismo. Se pueden desarrollar reportes de posibles incidentes de fuentes como sistemas de información, usuarios finales u otras organizaciones. No todos los reportes corresponden a incidentes válidos, ya que podría tratarse de falsas alarmas o podrían no considerarse incidentes. Las actividades en esta fase incluyen:
- Asignar la propiedad de un incidente real o posible a un administrador de incidentes
 - Verificar que los reportes o eventos reúnan los requisitos para considerarse incidentes
 - Establecer una cadena de custodia durante la identificación cuando se manejan posibles evidencias
 - Determinar la gravedad de un incidente y escalarlo según sea necesario
- **Contención**—Después de que se ha identificado y confirmado un incidente, el grupo de gestión de incidentes (del inglés Incident Management Team, IMT) se activa y se comparte la información del administrador de incidentes. El equipo llevará a cabo entonces una evaluación detallada y se pondrá en contacto con el propietario del sistema o el gerente de negocio de los sistemas/activos de información afectados a fin de coordinar las acciones que se tomarán. La acción que se tome en esta fase tendrá el propósito de limitar la exposición. Las actividades en esta fase incluyen:
- Activar el IMT/IRT para contener el incidente
 - Notificar a las partes interesadas pertinentes que se hayan visto afectadas por el incidente
 - Obtener un acuerdo sobre las acciones tomadas que pudieran afectar la disponibilidad del servicio o el riesgo del proceso de contención
 - Involucrar a los representantes de TI y miembros de equipo virtuales correspondientes para implementar procedimientos de contención
 - Obtener y mantener evidencia
 - Documentar y generar respaldos de las acciones tomadas a partir de esta fase
 - Controlar y gestionar los comunicados enviados al público por parte del equipo de relaciones públicas
- **Erradicación**—Cuando se han aplicado medidas de contención, se debe determinar la causa raíz del incidente y erradicarla. La erradicación se puede llevar a cabo de varias formas: restableciendo respaldos para alcanzar un estado limpio del sistema, eliminando la causa raíz, mejorando las defensas y llevando a cabo análisis de vulnerabilidad para encontrar otros posibles daños que podrían derivarse de la misma causa raíz. Las actividades en esta fase incluyen:
- Determinar las señales y las causas de incidentes
 - Localizar la versión más reciente de respaldos o soluciones alternativas
 - Eliminar la causa raíz. En caso de infección por gusano o virus, se puede eliminar mediante la aplicación de parches apropiados y software de antivirus actualizado.
 - Mejorar las defensas mediante la implementación de técnicas de protección
 - Realizar análisis de vulnerabilidades para encontrar nuevas vulnerabilidades que haya introducido la causa raíz
- **Recuperación**—Esta fase asegura que los sistemas o servicios afectados son restaurados de acuerdo a una condición especificada en los objetivos de entrega del servicio (SDO) o un plan de continuidad del negocio (BCP). La limitación de tiempo hasta esta fase se documenta en el objetivo de tiempo de recuperación (RTO). Las actividades en esta fase incluyen:
- Restablecer las operaciones, tal como se definió en el SDO
 - Validar que las acciones tomadas sobre los sistemas restablecidos hayan sido exitosas
 - Involucrar a los propietarios del sistema en las pruebas que se lleven a cabo sobre el sistema
 - Facilitar a los propietarios del sistema la declaración de operación normal
- **Lecciones aprendidas**—Al final del proceso de respuesta a incidentes, siempre se debe elaborar un reporte para compartir lo que sucedió, las medidas que se tomaron y los resultados obtenidos después de que se ejecutó el plan. Parte del reporte debe incluir las lecciones aprendidas que brindan al IMT y a otras partes interesadas puntos de aprendizaje valiosos de lo que se pudo haber hecho mejor. Estas lecciones deben desarrollarse en un plan para mejorar la capacidad de gestión de incidentes y la documentación del IRP. Las actividades en esta fase incluyen:
- Redactar el informe del incidente
 - Analizar los problemas encontrados durante los esfuerzos de respuesta a incidentes
 - Proponer mejoras con base en los problemas encontrados
 - Presentar el informe a las partes interesadas pertinentes

TEMA 3—INVESTIGACIONES, RETENCIONES LEGALES Y PRESERVACIÓN

INVESTIGACIONES

Las investigaciones de incidentes de ciberseguridad incluyen la recopilación y análisis de las evidencias con el objetivo de identificar al autor de un ataque o del uso o acceso no autorizado. Esto puede solaparse con el análisis técnico utilizado en la respuesta a incidentes -aunque ambos procesos estén claramente separados- donde el objetivo es entender la naturaleza del ataque, lo que sucedió y cómo ocurrió.

Los objetivos de una investigación pueden entrar en conflicto con los objetivos de respuesta a incidentes. Las investigaciones pueden requerir que el ataque o acceso autorizado continúe mientras se analiza y se recoge la evidencia, mientras que la recuperación puede destruir pruebas o impedir una mayor investigación. La gerencia de la organización debe ser una parte integral de la toma de decisiones entre la investigación y remediación.

Las investigaciones pueden llevarse a cabo debido a una actividad criminal (como se define por las leyes gubernamentales y la legislación), violaciones de los contratos o violaciones de las políticas de la organización. Los investigadores de ciberseguridad también pueden ayudar en otros tipos de investigaciones donde se utilizaron ordenadores o redes en la realización de otros delitos, tales como el acoso donde se utilizó correo electrónico.

Una investigación puede llevarse a cabo en su totalidad con recursos internos o puede ser llevada a cabo a través de una combinación de recursos internos, proveedores de servicios y órganos policiales o reguladores.

PRESERVACIÓN DE EVIDENCIAS

Es muy importante preservar las evidencias en cualquier situación. La mayoría de las organizaciones no están bien equipadas para tratar con intrusos y crímenes electrónicos desde una perspectiva operativa y de procedimientos y responden a este tipo de eventos únicamente cuando ha ocurrido una intrusión y el riesgo se ha hecho realidad. La evidencia pierde su integridad y valor para efecto de los procedimientos legales si no ha sido conservada correctamente ni sujeta a una cadena de custodia bien documentada. Esto ocurre cuando el incidente se maneja inapropiadamente y la intrusión es tratada en forma ad hoc.

La evidencia de un delito informático existe en forma de archivos de logs, marcas de tiempo de archivos, contenido de la memoria, etc. Otras fuentes incluyen el historial del navegador, listas de contactos, cookies, documentos, archivos ocultos, imágenes, metadatos, archivos temporales y vídeos. Si bien no es del todo explicativa, ayuda a proporcionar un contexto para el profesional de ciberseguridad en cuanto a la cantidad de información que está disponible para los contestatarios. La capacidad de localizar y capturar evidencias depende del tipo de datos, habilidades y experiencia de los investigadores y de las herramientas.

Reiniciar el sistema o acceder a los archivos podría dar lugar a que tales pruebas se pierdan, sean corrompidas o sobreescritas. Por lo tanto, uno de los primeros pasos a tomar debe ser copiar una o más imágenes del sistema atacado. El contenido de la memoria debe también ser copiado a un archivo antes de reiniciar el sistema. Cualquier otro análisis posterior debe realizarse sobre una imagen del sistema y sobre copias del repositorio de memoria, no en el sistema original en cuestión.

Además de proteger las evidencias, también es importante preservar la cadena de custodia. La **cadena de custodia** es un término que se refiere a documentar en detalle cómo se maneja y se mantiene la evidencia, incluyendo su propiedad, transferencia y modificación. Esto es necesario para satisfacer los requerimientos legales que exigen un alto nivel de confianza respecto a la integridad de las evidencias.

Para que la evidencia sea admisible en un tribunal de justicia, es necesario mantener con precisión y cronológicamente la cadena de custodia. La cadena de evidencia contiene esencialmente información respecto a:

- Las personas que han tenido acceso (cronológicamente) a la evidencia
- Los procedimientos que se siguieron para trabajar con la evidencia (como duplicación de disco, colocado de memoria virtual)
- Garantías de que el análisis se basa en copias que son idénticas a la evidencia original (podrían ser la documentación, sumas de comprobación o marcas de tiempo)

REQUERIMIENTOS LEGALES

Las investigaciones han definido con claridad los requerimientos legales y estos varían de un país a otro. Únicamente los investigadores capacitados que trabajan con un asesor legal deben realizar investigaciones. Algunas de las cuestiones legales que podrían aplicarse incluyen:

- Recopilación de pruebas y almacenamiento
- Cadena de custodia de las evidencias
- Buscar o monitorizar comunicaciones
- Entrevistas o interrogatorios
- Participación en la aplicación de la ley
- Reglamentos laborales, sindicales y de privacidad

Estas y otras consideraciones legales evolucionan cuando se aplican al ciberespacio y varían, a veces significativamente, de una jurisdicción a otra. No realizar una investigación conforme a los requerimientos legales correspondientes pueden acarrear responsabilidades penales o civiles por el investigador y la organización o puede dar lugar a una incapacidad para emprender acciones legales.

Muchos ataques son de alcance internacional, y navegar por los diferentes (y a veces conflictivos) problemas legales puede ser un reto, añadiendo complejidad a las investigaciones de ciberseguridad. En algunos países, a las personas y las organizaciones privadas no se les permite llevar a cabo investigaciones y requieren de la intervención de autoridades policiales.

TEMA 4—ANÁLISIS FORENSE

Por definición, el análisis forense digital es “el proceso de identificar, preservar, analizar y presentar evidencias digitales en una forma que sea aceptable en cualquier proceso legal (es decir, un tribunal).”⁷² La informática forense incluye actividades que involucran la exploración y aplicación de métodos para recolectar, procesar, interpretar y usar evidencias digitales que ayuden a sustanciar si ha ocurrido un incidente, como por ejemplo:

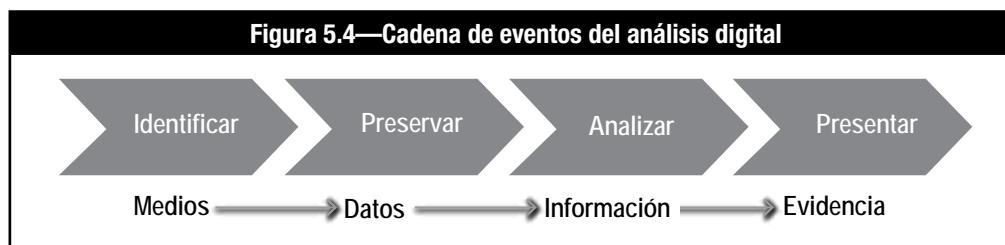
- Proveer validación de que un ataque en efecto ocurrió
- Recolectar evidencias digitales que puedan ser usadas posteriormente en procesos judiciales

Cualquier documento electrónico o dato puede usarse como evidenciadigital, a condición de que haya suficientes garantías, manuales o electrónicas de que el contenido de las evidencias digitales están en su estado original y no han sido alteradas ni modificadas durante el proceso de recolección y análisis.

Es importante usar las mejores prácticas especificadas por la industria, herramientas probadas y la debida diligencia para proveer garantía razonable de la calidad de las evidencias. También es importante demostrar integridad y confiabilidad de la evidenciapara que ésta sea aceptable por parte de las autoridades. Por ejemplo, si el auditor de los Sistemas de Información reinicia una computadora sospechosa de contener información almacenada que podría representar una evidencia en un juicio, el auditor no puede negar después que escribieron datos en el disco duro porque la secuencia de arranque (boot) escribe un registro en el disco. Por esta razón se utilizan herramientas especializadas para realizar copias auténticas del disco, que luego serán utilizadas en la investigación.

Hay cuatro consideraciones principales en la cadena de eventos en lo que respecta a las pruebas de análisis forense digital (**figura 5.4**):

- **Identificar**—Se refiere a la identificación del tipo de información que está disponible y que podría constituir una evidencia de un incidente.
- **Preservar**—Se refiere a la práctica de recuperación de información identificada y que se preserva como evidencia. La práctica generalmente incluye la obtención de imágenes de medios originales en presencia de una tercera parte independiente. El proceso también requiere ser capaz de documentar la cadena de custodia para que pueda establecerse en un tribunal de justicia.
- **Analizar**—Implica extraer, procesar e interpretar las evidencias. Los datos extraídos podrían ser datos binarios incomprendibles, que deben ser procesados y convertidos en un formato legible para las personas. Por lo tanto, la interpretación requiere profundos conocimientos de cómo se integran las distintas partes. El análisis se debe realizar utilizando una imagen del medio de almacenamiento, no el original.
- **Presentar**—Implica una presentación a las diferencias audiencias, tales como gerentes, abogados, tribunales, etc.



La aceptación de las evidencias depende de la forma en la que se lleva a cabo la presentación (debe ser convincente), de las certificaciones del presentador y la credibilidad del proceso utilizado para conservar y analizar las evidencias. El profesional del aseguramiento debe tener en cuenta los elementos clave del análisis forense informático durante la planificación de la auditoría. Estos elementos clave se describen en las secciones siguientes.

PROTECCIÓN DE DATOS

Para prevenir que la información buscada sea alterada, deben aplicarse todas las medidas. Es importante establecer protocolos específicos para informar a las partes apropiadas que se buscará evidencia electrónica y para no destruirla de ninguna manera. La infraestructura y los procesos para respuesta y manejo de incidentes deben estar instalados para permitir una respuesta efectiva y una investigación forense si ocurriera un evento o un incidente.

⁷² McKemmish, D. Rodney; *Computer and Intrusion Forensics*, Artech House, EE.UU., 2003

ADQUISICIÓN DE DATOS

Toda la información y los datos requeridos deben ser transferidos a una ubicación controlada; esto incluye todos los tipos de medios de almacenamiento electrónicos, como por ejemplo las unidades de disco fijo y otros tipos de medios removibles. Cada dispositivo debe ser revisado para asegurar que está protegido contra escritura. Esto se puede conseguir mediante el uso de un dispositivo conocido como un bloqueador de escritura. También es posible obtener datos e información de los testigos o partes relacionadas mediante declaraciones grabadas. Por medio de datos volátiles, los investigadores pueden determinar lo que está sucediendo en un momento en un sistema. Este tipo de datos incluye puertos abiertos, archivos abiertos, procesos activos, logons de usuario, y otros datos presentes en RAM. Esta información se pierde cuando se apaga el ordenador.

GENERACIÓN DE IMÁGENES

La generación de imágenes es un proceso que permite obtener una copia bit a bit de datos para evitar el daño de datos o información originales cuando se pueden realizar múltiples análisis. El proceso de generación de imágenes se hace para obtener datos residuales, como los archivos borrados, fragmentos de archivos borrados y otra información presente, desde el disco para su análisis. Esto es posible porque la generación de imágenes duplica la superficie del disco, sector por sector. Con herramientas apropiadas, a veces es posible recuperar la información destruida (borrada incluso por reformateo) desde la superficie del disco.

EXTRACCIÓN

Este proceso consiste en la identificación y selección de los datos del conjunto de datos copiados. Este proceso debe incluir estándares de calidad, integridad y confiabilidad. El proceso de extracción incluye software usado y medios en los que se hizo la imagen. El proceso de extracción podría incluir diferentes fuentes tales como logs de sistema, logs de firewall, logs de sistema de detección de intrusos (IDS), pistas de auditoría e información de gestión de red.

ENTREVISTAS

Las entrevistas se utilizan para obtener indicadores o relaciones anteriores, incluyendo números de teléfono, direcciones IP y los nombres de las personas, a partir de datos extraídos.

CONVERSIÓN DE DATOS A TEXTO CLARO / NORMALIZACIÓN

Este proceso convierte la información extraída a un formato que puede ser entendido por los investigadores. Incluye la conversión de datos hexadecimales o binarios en caracteres legibles o en un formato adecuado para las herramientas de análisis de datos. Es posible crear relaciones de datos por extrapolación, utilizando técnicas tales como la fusión, correlación, graficado, mapeo o cronológico, que podrían ser utilizados en la construcción de la hipótesis de la investigación.

PRESENTACIÓN DE INFORMES

La información obtenida del análisis forense tiene un valor limitado cuando no se recoge y se informa de la manera adecuada. Un informe debe indicar por qué se revisó el sistema, cómo se revisaron los datos del ordenador y qué conclusiones se hicieron a partir de este análisis. El informe debe alcanzar los siguientes objetivos:⁷³

- Describir con precisión los detalles de un incidente.
- Ser comprensible para los encargados de tomar decisiones.
- Ser capaz de resistir al escrutinio legal.
- Ser inequívoco y no estar abierto a una interpretación errónea.
- Ser fácilmente referenciado.
- Contener toda la información necesaria para explicar las conclusiones alcanzadas.
- Ofrecer conclusiones, opiniones o recomendaciones válidas cuando sea necesario.
- Ser creado en el momento oportuno.

El informe también debe identificar la organización, los informes de muestra y las restricciones en la circulación (si existen) e incluir reservas o certificaciones que el profesional de aseguramiento tiene con respecto a la asignación.

⁷³ Mandia, Kevin; Matt Pepe, Chris Prosise, *Incident Response & Computer Forensics*, 2^a edición, McGraw Hill/Osborne, EE.UU., 2003

ANÁLISIS DE TRÁFICO DE RED

El análisis de tráfico de red identifica patrones en las comunicaciones de red. El análisis de tráfico no necesita tener el contenido real de la comunicación, pero analiza dónde se está llevando a cabo el tráfico, cuándo y por cuánto tiempo ocurren las comunicaciones y el tamaño de la información transferida.

El análisis de tráfico puede utilizarse de forma proactiva para identificar posibles anomalías en las comunicaciones o durante la respuesta a incidentes para desarrollar huellas que identifican diferentes ataques o las actividades de los diferentes individuos.

ANÁLISIS DE ARCHIVOS DE REGISTRO

Se han desarrollado muchos tipos de herramientas para ayudar a reducir la cantidad de información contenida en los registros de auditoría, y para identificar la información útil de los datos en bruto (raw data). En la mayoría de los sistemas, el software de pistas de auditoría puede crear grandes archivos, que pueden ser extremadamente difíciles de analizar manualmente. La diferencia entre los datos no utilizados de las pistas de auditoría y una revisión efectiva podría ser el uso de herramientas automatizadas. Algunos de los tipos de herramientas incluyen:

- **Herramientas de reducción de auditoría**—Estos son preprocesadores diseñados para reducir el volumen de registros de auditoría para facilitar la revisión manual. Antes de una revisión de seguridad, estas herramientas pueden eliminar muchos registros de auditoría que se sabe tienen poca importancia para la seguridad. (Esto por sí solo puede reducir a la mitad el número de registros de las pistas de auditoría). Estas herramientas generalmente eliminan registros generados por clases específicas de eventos; por ejemplo, los registros generados por copias de seguridad nocturnas pueden ser eliminados.
- **Herramientas de detección de tendencia/varianza**—Éstas buscan anomalías en el comportamiento del usuario o del sistema. Es posible construir procesadores más sofisticados que monitorizan las tendencias del uso y detecten las variaciones mayores. Por ejemplo, si un usuario se conecta de forma habitual a las 09:00, pero lo hace a las 04:30 una mañana, esto puede indicar un problema de seguridad que es posible que necesite ser investigado.
- **Herramientas de detección de firma de ataques**—Estas herramientas buscan una firma de ataque, que es una secuencia específica de eventos indicativa de un intento de acceso no autorizado. Un ejemplo sencillo sería la repetición de intentos de inicio de sesión fallidos.

HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL

Las herramientas forenses se pueden clasificar en cuatro categorías:

- **Ordenador**—Examina los medios digitales no volátiles. Debido a la cantidad de herramientas en el mercado, no vamos a discutir herramientas específicas. Los vendedores basan sus herramientas en diferentes plataformas (es decir, Windows, Linux, etc.). La mayoría son propietarias; sin embargo, existen opciones de código abierto. Del mismo modo, algunos se limitan al cumplimiento de la ley y/o las agencias gubernamentales. En última instancia, los requerimientos del negocio determinarán la selección.
- **Memoria**—Se utiliza para adquirir y analizar la memoria volátil.
- **Dispositivo móvil**—Consiste tanto de los componentes de software como de hardware. Debido a la gran cantidad de dispositivos, los fabricantes y alcance previsto, no vamos a discutir herramientas específicas. Los cables desempeñan una función similar a los bloqueadores de escritura para la informática forense.
- **Red**—Monitorización y análisis del tráfico de red. Las opciones van desde las herramientas de línea de comandos anteriormente mencionados hasta infraestructura más compleja de inspección de paquetes.

Además, es posible encontrar varias aplicaciones de soporte que pueden ser usadas. Un ejemplo es el software de virtualización VMware®—que permite a los usuarios ejecutar múltiples instancias de sistemas operativos en un servidor o PC físico.

CRONOGRAMAS

Los cronogramas son gráficos cronológicos donde los acontecimientos relacionados con un incidente pueden ser mapeados para buscar relaciones en casos complejos. Los cronogramas pueden proporcionar una visualización simplificada para su presentación a la gerencia y otras audiencias no técnicas.

ANTI ANÁLISIS FORENSE

Los programadores desarrollan herramientas anti-análisis forense para que sea difícil o imposible para los investigadores recuperar información durante una investigación. Hay muchas maneras en que se puede ocultar información.

Tácticas, técnicas y procedimientos (TTPS) anti-forenses incluyen:

- Borrar de forma segura los datos
- Sobrescribir metadatos
- Prevenir la creación de datos
- Cifrado de los datos
- Cifrado de los protocolos de red
- Ocultar datos en el espacio de inactividad o en otros lugares no asignados
- Ocultar datos o archivos dentro de otro archivo (esteganografía)

TEMA 5—PLANES DE RECUPERACIÓN DE DESASTRES Y DE CONTINUIDAD DEL NEGOCIO

Los desastres son interrupciones que causan que recursos de información críticos queden no operativos durante un período, afectando de manera adversa las operaciones organizacionales. La interrupción podría durar desde unos pocos minutos a varios meses, dependiendo del grado del daño causado al recurso de información. Es importante conocer que, ante situaciones de desastre, es necesario desplegar esfuerzos de recuperación para restaurar el estado operacional.

Un desastre puede ser causado por desastres naturales, tales como terremotos, inundaciones, tornados e incendios, o puede ser causado por eventos provocados por los seres humanos, tales como atentados terroristas, ataques de hackers, virus o errores humanos. Muchas interrupciones comienzan como incidentes menores. Normalmente, si la organización posee un centro de soporte (help desk) o un centro de servicio, éste actuará como el sistema de advertencia temprana para reconocer las primeras señales de una interrupción inminente. A menudo, tales interrupciones (por ejemplo, un rendimiento de la base de datos que desmejora gradualmente) pasan desapercibidas. Hasta que estallan estos “desastres progresivos” (la base de datos se detiene), sólo causan quejas esporádicas de parte de los usuarios.

Desastres relacionados con la ciberseguridad pueden ocurrir cuando una interrupción en el servicio se debe a un mal funcionamiento del sistema, la eliminación accidental de archivos, el lanzamiento de aplicaciones no probadas, la pérdida de copias de seguridad, ataques de denegación de servicio, intrusiones o virus. Estos eventos pueden requerir acciones para recuperar el estado operacional a fin de reanudar el servicio. Las acciones pueden necesitar del restablecimiento del hardware, software o archivos de datos.

CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN DE DESASTRES

El propósito del plan de continuidad de negocio (BCP)/plan de recuperación de desastres (DRP) es permitir al negocio seguir ofreciendo servicios críticos en el caso de una interrupción y sobrevivir a una interrupción desastrosa a las actividades. La planificación y asignación de recursos de forma rigurosa es necesaria para planificarse adecuadamente frente a tal evento.

El BCP tiene en cuenta:

- Las operaciones críticas necesarias para la supervivencia de la organización
- Los medios humanos o materiales que ayudan a esas operaciones críticas.
- La preparación previa al desastre que cubre la gestión de respuesta a incidentes para hacer frente a todas las incidencias relevantes que afectan a los procesos de negocio
- Procedimientos de evacuación
- Procedimientos para declarar un desastre (procedimientos de escalado)
- Circunstancias bajo las cuales debe declararse un desastre (Nota: No todas las interrupciones son desastres, pero un pequeño incidente que no se aborde de manera oportuna o adecuada puede dar lugar a un desastre. Por ejemplo, un ataque de virus no reconocido y contenido a tiempo puede dejar indisponible toda la infraestructura de TI.)
- La identificación clara de las responsabilidades en el plan
- La identificación clara de las personas responsables de cada función del plan
- La identificación clara de la información sobre el contrato
- La explicación paso a paso del proceso de recuperación
- La identificación clara de los diferentes recursos que se requieren para la operación de la recuperación y la continuidad de la organización

El BCP es principalmente responsabilidad de la alta dirección, ya que se encargan de la protección de los activos y la viabilidad de la organización, tal y como se define en la política del BCP/DRP. En general, las unidades de negocio y soporte siguen el BCP para ofrecer un nivel de funcionalidad reducido pero suficiente en las operaciones de negocio inmediatamente después de enfrentar una interrupción, mientras ocurre la recuperación.

Dependiendo de la complejidad de la organización, puede haber uno o más planes para abordar los diversos aspectos del BCP y del DRP. Estos planes no necesariamente tienen que integrarse en un único plan. Sin embargo, cada uno tiene que ser coherente con los otros planes para tener una estrategia viable de BCP.

Aun cuando procesos similares de la misma organización se manejen en una ubicación geográfica diferente, las soluciones de BCP y DRP pueden ser diferentes para escenarios diferentes. Las soluciones pueden ser diferentes debido a requerimientos contractuales (por ejemplo, la misma organización está procesando una transacción en línea para un cliente y el back office está procesando una transacción para otro cliente). Una solución del BCP para el servicio en línea será significativamente diferente de una para el procesamiento de back office.

ANÁLISIS DE IMPACTO EN EL NEGOCIO

El primer paso en la preparación de un nuevo BCP es identificar los procesos de negocio de importancia estratégica, aquellos procesos clave que son responsables del crecimiento del negocio y de la consecución de las metas del negocio. Lo ideal es que el BCP/DRP sea respaldado por una política ejecutiva formal que establezca el objetivo general de la organización en lo que respecta a la recuperación y asigne atribuciones a las personas que participan en el desarrollo, las pruebas y el mantenimiento de los planes.

Basado en los procesos clave, un proceso de análisis de impacto en el negocio (BIA) debe comenzar determinando plazos, prioridades, recursos e interdependencias que apoyan los procesos clave. El riesgo del negocio es directamente proporcional al impacto en la organización y la probabilidad de ocurrencia de la amenaza percibida. Por lo tanto, el resultado del BIA debe ser la identificación de lo siguiente:

- Los recursos humanos, los datos, los elementos de la infraestructura y otros recursos (incluyendo los proporcionados por terceros) que respaldan los procesos clave
- Una lista de las posibles vulnerabilidades, es decir, los peligros o amenazas para la organización
- La probabilidad estimada de que ocurran estas amenazas
- La eficiencia y eficacia de los controles existentes de mitigación de riesgos (contramedidas para afrontar riesgos)

La información se recoge para el BIA de diferentes partes de la organización que poseen procesos/aplicaciones clave. Para evaluar el impacto de tiempo improductivo para un proceso/aplicación particular, se desarrollan los niveles de impacto (por ejemplo, alto, medio, bajo) y, para cada proceso, el impacto se estima en tiempo (horas, días, semanas). El mismo enfoque se usa al estimar el impacto de la pérdida de datos. Si es necesario, el impacto financiero puede estimarse utilizando las mismas técnicas, asignando el valor financiero a los niveles de impacto. Además, los datos del BIA se pueden recolectar en las ventanas de tiempo necesarias para suministrar recursos vitales—cuánto tiempo puede funcionar la organización si se daña un suministro o cuándo llegó el reemplazo.

El BIA debe responder a tres preguntas importantes:

1. ¿Cuáles son los diferentes procesos del negocio?
2. ¿Cuáles son los recursos de información críticos relacionados con los procesos del negocio críticos de una organización?
3. ¿Cuál es el período de tiempo de recuperación crítico para recursos de información en el cual los procesos del negocio se deben reanudar antes de sufrir pérdidas significativas o inaceptables?

La fuente principal de información usada en un BCP es el BIA, que identifica las líneas de tiempo críticas para servicios y productos asociados con la creación de valor y tolerancia de riesgos para el negocio. El BIA también establece el Objetivo de punto de recuperación (PRO) y el Objetivo de tiempo de recuperación (RTO) para un proceso, lo que respectivamente define cuantos datos pueden ser perdidos en una recuperación y con cuanta rapidez se debe realizar dicha recuperación. Debido a que el BCP está basado en el BIA, el profesional de riesgo debe revisar el proceso empleado para determinar el BIA y validar que es preciso y que considera todos los factores de riesgo. En organizaciones que han adoptado un Sistema de gestión de la continuidad del negocio (BCMS: del inglés Business Continuity Management System), el profesional de riesgos se puede beneficiar si tiene acceso directo al BCP para revisar y referenciar en el contexto de gestión de riesgos.⁷⁴

CONSIDERACIONES EN LA CADENA DE SUMINISTRO

NIST define la cadena de suministro de la tecnología de la información y comunicación (ICT) como “un ecosistema complejo, distribuido a nivel mundial e interconectado, que tiene diversas rutas geográficas, y se compone de múltiples niveles de externalización.” Este entorno es interdependiente de entidades públicas y privadas para el desarrollo, la integración y la entrega de productos y servicios de ICT.⁷⁵

La complejidad de las cadenas de suministro y el impacto requiere una concienciación persistente de riesgo y consideración. Los factores más importantes que contribuyen a la fragilidad de las cadenas de suministro son económicos, ambientales, geopolíticos y tecnológicos.⁷⁶

⁷⁴ ISACA, *Manual de Preparación al Examen CRISC 6^a edición*, EE.UU., 2015

⁷⁵ Boyens, Jon; Celia Paulsen; Rama Moorthy; Nadya Bartol; *NIST SP 800-161, 2nd draft: Supply Chain Risk Management Practices for Federal Information Systems and Organization*, NIST, EE.UU., 2014

⁷⁶ Rodrigue, Jean-Paul; “Risk in Global Supply Chains,” https://people.hofstra.edu/geotrans/eng/ch9en/conc9en/supply_chain_risks.html

Ya se trate de la rápida adopción de software de código abierto, de la manipulación de hardware físico o de desastres naturales que dejen los centros de datos indisponibles, las cadenas de suministro requieren la gestión de riesgos. Un ejemplo de esto fue descrito de la siguiente manera en un artículo en la revista Forbes: Las inundaciones en Tailandia provocaron una escasez significativa en el mercado de discos duros, lo que costó millones de dólares en pérdidas a conocidos fabricantes de electrónica.⁷⁷

Los productos o servicios fabricados en cualquier lugar pueden contener vulnerabilidades que pueden presentar oportunidades para los compromisos relacionados con la cadena de suministro de las ICT. Es especialmente importante considerar el riesgo de la cadena de suministro desde el desarrollo del sistema, para incluir la investigación y el desarrollo (R&D) a través de la vida útil, y en última instancia el retiro/eliminación de los productos.

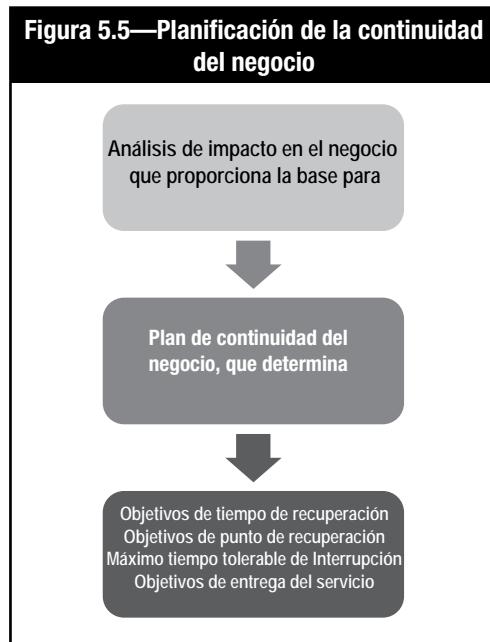
PLANIFICACIÓN DE CONTINUIDAD DEL NEGOCIO DE SI

En el caso del BCP de SI, el enfoque es el mismo que en el BCP con la excepción de que la continuidad del procesamiento de los SI está amenazada. El procesamiento de los SI es de importancia estratégica, es un componente crítico porque la mayoría de los procesos clave de negocios dependen de la disponibilidad de los componentes y los datos de la infraestructura de sistemas clave.

El BCP SI debe estar alineado con la estrategia de la organización. La criticidad de los diferentes sistemas de aplicaciones de la organización depende de la naturaleza del negocio, así como del valor de cada aplicación para el negocio.

El valor de cada aplicación para el negocio es directamente proporcional al rol que desempeña el sistema de información en el apoyo a la estrategia de la organización. Los componentes del sistema de información (entre ellos los componentes de la infraestructura tecnológica) se asocian posteriormente con las aplicaciones (por ejemplo, el valor de una computadora o una red depende de la importancia del sistema de aplicaciones que la utiliza).

Por lo tanto, el BCP/DRP del sistema de información es un componente principal de la estrategia general de continuidad del negocio y recuperación en caso de desastre de una organización. Si el plan de los SI es un plan separado, debe ser consistente con y apoyar el BCP corporativo. Ver la **figura 5.5**.



⁷⁷ Culp, Steve, "Supply Chain Risk a Hidden Liability for Many Companies," *Forbes*, 8 Octubre 2012, www.forbes.com/sites/steveculp/2012/10/08/supply-chain-risk-a-hidden-liability-for-many-companies

CONCEPTOS DE RECUPERACIÓN

La recuperación de datos es el proceso de restauración de datos que han sido perdidos, borrados accidentalmente, dañados o se han vuelto inaccesibles por alguna razón. Los procesos de recuperación varían en función del tipo y la cantidad de datos perdidos, del método de copia de seguridad propia y de los medios de respaldo. El DRP de una organización debe proporcionar la estrategia de cómo se recuperarán los datos y asignar responsabilidades de recuperación.

PROCEDIMIENTOS DE COPIAS DE SEGURIDAD

Los procedimientos de copias de seguridad se utilizan para copiar archivos en un segundo medio como puede ser un disco, una cinta o en la nube. Los archivos de copias de seguridad deben mantenerse en una ubicación fuera del sitio. Las copias de seguridad suelen ser automatizadas utilizando comandos del sistema operativo o programas de copias de seguridad. La mayoría de los programas de copias de seguridad comprimen los datos de modo que las copias de seguridad requieren menos medios de almacenamiento.

Hay tres tipos de copias de seguridad de datos: completos, incrementales y diferenciales. Los respaldos completos proporcionan una copia completa de todos los archivos seleccionados en el sistema, independientemente de si fue respaldada recientemente. Este es el método de copia de seguridad más lento pero el método más rápido para la restauración de datos. Las copias de seguridad incrementales copian todos los archivos que han cambiado desde que se hizo la última copia de seguridad, independientemente de si la última copia de seguridad era una copia de seguridad completa o incremental. Este es el método de copia de seguridad más rápido, pero el método más lento para la restauración de datos. Las copias de seguridad diferenciales sólo copian los archivos que han cambiado desde la última copia de seguridad completa. El archivo crece hasta que se realice la siguiente copia de seguridad completa.

SECCIÓN 5—EVALUACIÓN DE CONOCIMIENTOS

1. Organice los pasos del proceso de respuesta a incidentes en el orden correcto.
 - A. Mitigación y recuperación
 - B. Investigación
 - C. Análisis posterior al incidente
 - D. Preparación
 - E. Detección y análisis
2. ¿Qué elemento de un plan de respuesta a incidentes implica la obtención y preservación de la evidencia?
 - A. Preparación
 - B. Identificación
 - C. Contención
 - D. Erradicación
3. Seleccione tres. La cadena de custodia contiene información sobre:
 - A. objetivo de la recuperación de desastres, recursos y personal.
 - B. quién tuvo acceso a las pruebas, en orden cronológico.
 - C. reglamentos laborales, sindicales y de privacidad.
 - D. prueba de que el análisis se hizo con base en copias idénticas a la evidencia original.
 - E. los procedimientos que se siguieron al trabajar con la evidencia.
4. El NIST define un(a) _____ como “una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.”
 - A. Desastre
 - B. Evento
 - C. Amenaza
 - D. Incidente
5. Seleccione todas las opciones que apliquen. Un análisis de impacto en el negocio (BIA) debe identificar:
 - A. las circunstancias en que debe ser declarado un desastre.
 - B. la probabilidad estimada de que las amenazas identificadas ocurran en realidad.
 - C. la eficiencia y la eficacia de los controles existentes de mitigación de riesgos.
 - D. una lista de vulnerabilidades, peligros y / o amenazas potenciales.
 - E. los tipos de copias de seguridad de datos (completa, incremental y diferencial) que se utilizarán.

Ver respuestas en el Anexo C.

Página dejada en blanco intencionadamente



CYBERSECURITY NEXUS

Sección 6:

Implicaciones de seguridad y adopción de la tecnología evolutiva

Los temas tratados en esta sección incluyen:

1. Panorama actual de amenazas
2. Amenazas persistentes avanzadas (APT)
3. Tecnología móvil—vulnerabilidades, amenazas y riesgos
4. Consumerización de TI y dispositivos móviles
5. La nube y la colaboración digital

Página dejada en blanco intencionadamente

TEMA 1—PANORAMA ACTUAL DE AMENAZAS

Un panorama de amenazas, al que también llamamos entornos de amenazas, es un conjunto de amenazas. El panorama de la ciberseguridad está cambiando constantemente y evolucionando a medida que se desarrollan nuevas tecnologías y los ciberataques y herramientas se vuelven más sofisticadas. El panorama de amenazas desarrollado por la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) se muestra en la **figura 6.1**. Las corporaciones se vuelven más y más dependientes de las tecnologías digitales, que son susceptibles de ser afectadas por riesgos de ciberseguridad. La computación en la nube, las redes sociales y la informática móvil están cambiando como las organizaciones usan y comparten la información; proveen mayores niveles de acceso y conectividad, que crean aperturas más grandes para los ciberdelincuentes.

Figura 6.1—ENISA Panorama de amenazas 2015		
Mayores amenazas de 2015	Tendencias evaluadas en 2015	Cambio en el ranking
1. Software malintencionado (malware)	↑	→
2. Ataques basados en la web	↑	→
3. Ataques de aplicaciones web	↑	→
4. Botnets	↓	→
5. Denegación de servicio	↑	→
6. Daño físico/robo/pérdida	→	↑
7. Amenaza interna (maliciosa, accidental)	↑	↑
8. Phishing	→	↓
9. Spam	↓	↓
10. Exploit kits	↑	↓
11. Brecha en la seguridad de datos	→	↓
12. Robo de identidad	→	↑
13. Fuga de información	↑	↓
14. Ransomware	↑	↑
15. Ciber espionaje	↑	↓
Leyenda: Tendencias: ↑ Ha subido, → Estable, ↓ Ha bajado Ranking: ↑ Aumentando, → Igual, ↓ Bajando		
Fuente: ENISA, ENISA Threat Landscape 2015, Grecia, 2016		

Las motivaciones de los ciber criminales suelen abarcar una, o varias, de las siguientes:

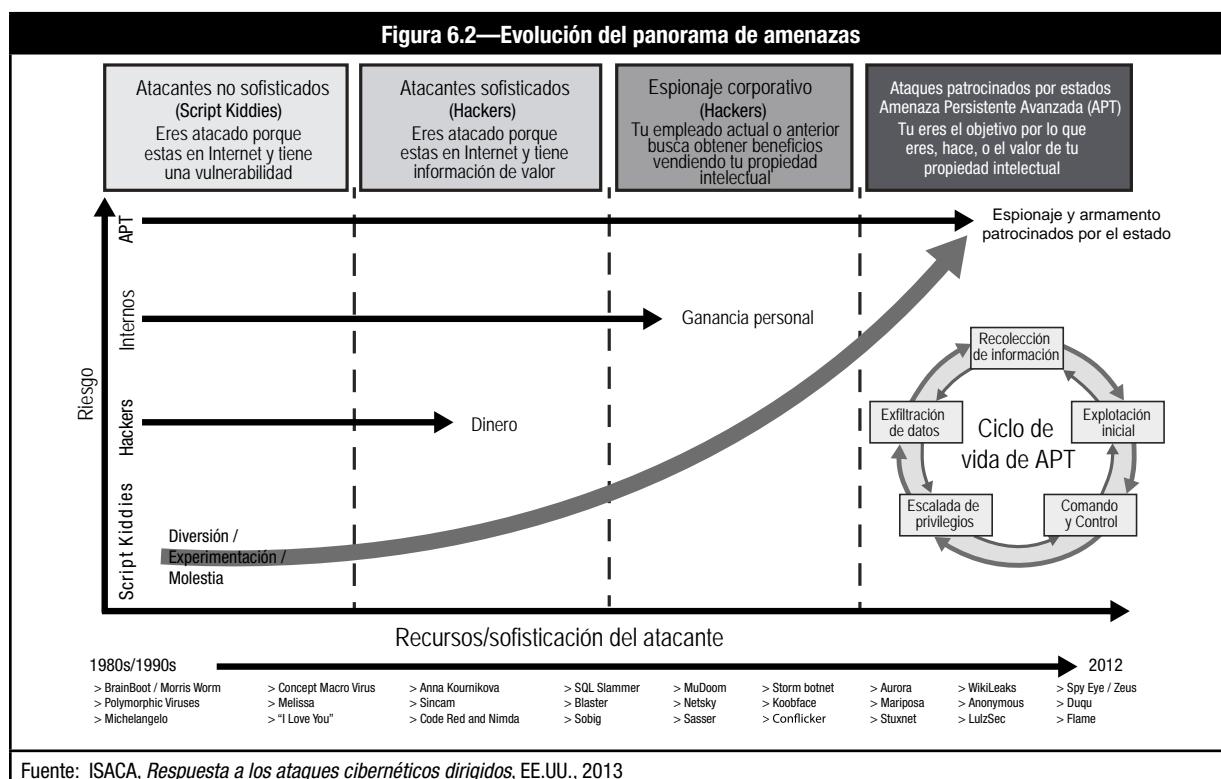
- Beneficios financieros
- Propiedad Intelectual (espionaje)
- Política (activismo)

Las tendencias más recientes en el panorama de las ciberamenazas son:

- Las amenazas son más sofisticadas en cuanto a sus ataques y al uso de herramientas.
- Los patrones de ataque se están dirigiendo a los dispositivos móviles. Esto es especialmente preocupante en el caso de los móviles y otros pequeños dispositivos digitales que están interconectados y que, a menudo, tienen controles de seguridad bastante pobres.
- Muchas naciones han adquirido la capacidad de infiltrarse tanto en objetivos gubernamentales y privados (ciber guerra).
- Como resultado de la computación en la nube han aparecido grandes concentraciones de datos en un número limitado de instalaciones, que han pasado a convertirse en objetivos para posibles atacantes.
- Las redes sociales se han convertido en el canal principal para comunicarse, adquirir conocimientos, marketing, y difusión de información. Los atacantes pueden hacer un mal uso de las redes sociales para obtener datos personales y generar desinformación
- Big Data (macrodatos) hace referencia a las cantidades ingentes de datos estructurados o no y a la utilización de grandes infraestructuras, aplicaciones, servicios web y dispositivos. La popularidad del Big Data como un activo propicia la posibilidad de brechas en de Big Data.

TEMA 2—AMENAZAS PERSISTENTES AVANZADAS

Las amenazas persistentes avanzadas (APTs) son un fenómeno relativamente nuevo para muchas organizaciones. Aunque los motivos detrás de ellas no son totalmente nuevos, el grado de planificación de los recursos empleados y las técnicas utilizadas en los ataques APT no tienen precedentes. Estas amenazas requieren un grado de vigilancia y un conjunto de contramedidas que están por encima y van más allá de los utilizados habitualmente para contrarrestar las amenazas de seguridad habituales provenientes de los hackers, virus o spammers.⁷⁸ La figura 6.2 muestra la evolución del panorama de amenazas.



DEFINIENDO LAS AMENAZAS PERSISTENTES AVANZADAS (APTS)

Hay que tener en cuenta que no existe un acuerdo generalizado en la definición de qué es una APT. Muchos expertos no lo consideran algo nuevo. Algunos lo ven únicamente como la última evolución de las técnicas de ataque que se han desarrollado a lo largo de los años. Otros afirman que el término es engañoso, puntualizando que muchos ataques considerados APTs no son especialmente inteligentes o nuevos. Unos pocos los definen en sus propios términos, como por ejemplo un ataque que es gestionado de forma profesional; un ataque que sigue un *modus operandi* particular; un ataque lanzado por un servicio de inteligencia extranjero; o un ataque que está dirigido y persigue a una empresa específica de forma implacable.

De hecho, todas estas descripciones son válidas. Definir las características de una APT es muy simple: Una **APT** es una amenaza específica que está compuesta de varios vectores de ataque complejos y que permanece oculta (sin ser detectada) durante un periodo de tiempo prolongado. Es un ataque sofisticado, dirigido a un objetivo específico que reaparece tras la víctima. A diferencia de otros muchos actos criminales, no es fácilmente desviado por una respuesta defensiva determinada. Un ejemplo de APT es el phishing de ingeniería social “spear phishing”, en el que se utilizan técnicas de ingeniería social para enmascararse (hacerse pasar por) alguien en quien confiamos, con el fin de obtener información importante, como la contraseña de la víctima.

⁷⁸ ISACA, *Amenazas persistentes avanzadas: Cómo gestionar el riesgo para su negocio*, EE.UU., 2013

CARACTERÍSTICAS DE LAS APTs

Los ataques de este tipo son muy diferentes de aquellos que pueden haber experimentado las empresas en el pasado. La mayoría de las organizaciones se han enfrentado en algún momento con uno o más ataques oportunistas de criminales de poca monta, hackers u otros bromistas. La mayoría de los ataques APT parten de fuentes más siniestras. Son a menudo el resultado del trabajo de equipos profesionales que son empleados por grupos del crimen organizado, determinados activistas o gobiernos. Esto significa que están probablemente bien planeados, son sofisticados, cuentan con recursos suficientes y son potencialmente más dañinos.

Los ataques APT varían su enfoque considerablemente, aunque comparten las siguientes características:

- **Bien documentados**—Los agentes APT investigan a fondo sus objetivos, planifican el uso de sus recursos y anticipan las posibles contramedidas.
- **Sofisticados**—Los ataques APT son diseñados habitualmente para explotar múltiples vulnerabilidades en un ataque único. Utilizan un extenso marco de módulos de ataque diseñados para realizar tareas automatizadas y dirigidas a múltiples plataformas.
- **Son sigilosos**—Ataques de APT a menudo no se detectan a lo largo de meses e incluso años. Estos ataques no están publicitados previamente y se camuflan usando técnicas de ofuscación u ocultamiento que están fuera de cualquier alcance.
- **Persistentes**—Los ataques APT son proyectos a largo plazo con un enfoque en el reconocimiento. Si un ataque es bloqueado con éxito, los autores responden con nuevos ataques. Además, siempre están rastreando métodos o información para el lanzamiento de ataques futuros.

OBJETIVOS DE APT

Las APTs atacan compañías de todos los tamaños en todos los sectores de la industria y todas las regiones geográficas que tengan activos de alto valor. Todos los empleados, independientemente de su antigüedad, desde los auxiliares administrativos a los altos ejecutivos, pueden ser elegidos como objetivo de un ataque phishing de ingeniería social (spear-phishing). Las pequeñas compañías y contratistas pueden ser atacadas al ser proveedores de servicios de una víctima elegida. Pueden ser seleccionadas como objetivos personas que sean consideradas como un potencial puente para obtener acceso al objetivo final.

Ninguna industria con secretos valiosos o cualquier otro recurso que pueda ofrecer una ventaja comercial que pueda ser copiada o quebrantada por medio del espionaje están a salvo de un ataque APT. Ninguna empresa que controle transferencias de dinero, procesos de información de tarjetas de crédito o almaceñe información identificable personal sobre individuos puede ser protegida de ataques criminales. Tampoco lo está aquella que proporcione o sostenga una importante infraestructura nacional crítica puesto que no son inmunes a las intrusiones de los ciber atacantes.

Los ataques APT a menudo abarcan organizaciones intermediarias que proporcionan servicios a empresas objetivo. Los proveedores intermediarios pueden ser percibidos por un atacante como el vínculo más débil de grandes compañías y departamentos gubernamentales ya que, normalmente, están menos protegidos. No importa lo efectivo que sea el perímetro externo de seguridad de la compañía, carece de valor si no se extiende a la cadena de suministro.

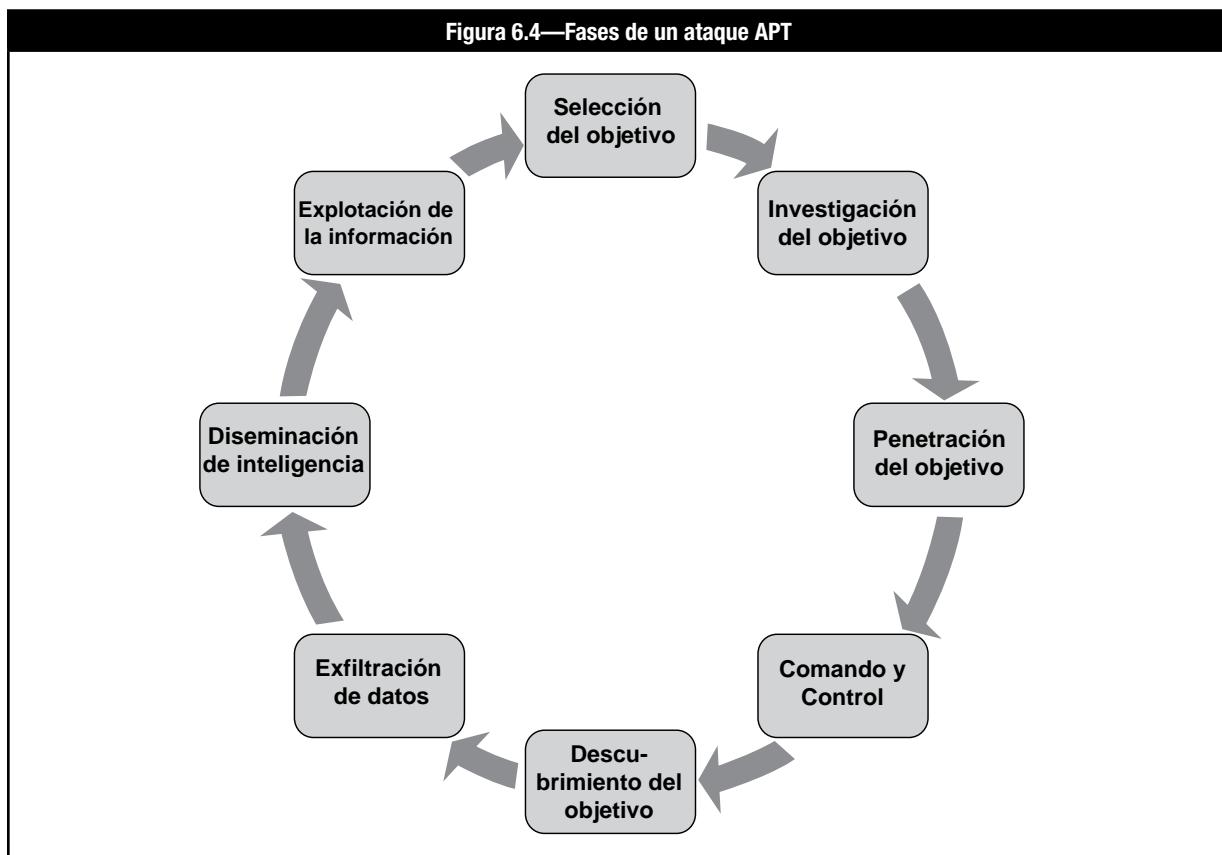
La **figura 6.3** enumera los actores principales detrás de una amenaza APT. Establece sus objetivos y el impacto empresarial potencial de sus ataques.

Figura 6.3—Tipos e impactos de APT

Amenaza	Lo que buscan	Impacto en el negocio
Agencias de inteligencia	Secretos políticos, de defensa o comerciales	Pérdida de secretos comerciales o ventaja competitiva comercial
Grupos criminales	Transferencias de dinero, oportunidades de extorsión, información personal de identidad o cualquier secreto para su venta posterior potencial	Pérdida financiera, fuga de datos de clientes a gran escala o pérdida de secretos comerciales
Grupos terroristas	Producción de terror generalizado a través de la muerte, destrucción y alteración	Pérdida de la producción y servicios, irregularidades del mercado de valores y riesgo potencial para la vida humana
Grupos activistas	Información confidencial o interrupción de los servicios	Importantes fugas de datos o pérdida de servicio
Fuerzas armadas	Inteligencia o posicionamiento de apoyo a futuros ataques contra la infraestructura nacional crítica	Graves daños a las instalaciones en caso de un conflicto militar

FASES DE UN ATAQUE APT

Aunque no existan dos ataques APT que sean idénticos, normalmente tienen un ciclo de vida similar, tal y como se muestra en la **figura 6.4**. Empiezan recogiendo información, que incluye seleccionar y estudiar sus objetivos, planear el ataque y recoger y analizar la información obtenida de una primera infiltración. El atacante entonces establece el comando y control, recogiendo la información del objetivo. Esta información se transmite a la localización del atacante para ser diseminada o explotada.



Página dejada en blanco intencionadamente

TEMA 3—TECNOLOGÍA MÓVIL—VULNERABILIDADES, AMENAZAS Y RIESGOS

La seguridad para la tecnología móvil es una función del riesgo asociado con su uso. A pesar de sus aspectos positivos o negativos, los equipos de seguridad deben de lidiar con el riesgo común a todos los dispositivos y aplicaciones móviles.

APLICACIONES MÓVILES

Similar a la lista discutida en el tema 6 de la sección 4, OWASP proporciona las 10 principales vulnerabilidades de seguridad móvil que deben ser abordadas por los equipos de seguridad cuando se trate de móviles y aplicaciones (**figura 6.5**)



RIESGO FÍSICO

Los dispositivos móviles suelen ser pequeños, por definición. Son fáciles de perder (o de ser robados), especialmente en sitios públicos. Esto incrementa el riesgo físico en general, ya que los teléfonos inteligentes suelen ser vistos como un objetivo interesante para los ladrones. Como los usuarios dependen cada vez más de sus dispositivos móviles, es probable que su pérdida o robo creen condiciones disruptivas y podrían dejar a los empleados sin poder trabajar por períodos de tiempo prolongados.

Las consecuencias de seguridad de la pérdida del dispositivo son más serias. Por ejemplo, información desprotegida y en tránsito, como listado de llamadas, mensajes o información del calendario, podrían verse comprometidas, permitiendo a los atacantes recolectar grandes cantidades de información. Con propósitos criminales, los perpetradores pueden ser capaces de recuperar la información que haya sido eliminada y el historial de uso del dispositivo móvil.

El robo de identidad supone un riesgo adicional, que puede ocurrir como resultado de la obtención y el análisis de un dispositivo móvil robado o perdido. Muchos sistemas operativos (SO) emergentes para dispositivos inteligentes requieren el enlace a una cuenta de usuario con el proveedor, lo que aumenta el riesgo de perder la identidad digital junto con el dispositivo actual.

El vínculo entre el dispositivo y la cuenta está sujeto, en ocasiones, a un riesgo aún mayor cuando se ofrecen servicios de valor añadido como una extensión a la cuenta de usuario existente. Algunos SO ofrecen un almacenamiento “seguro” para la información importante del usuario que abarca desde información personal hasta almacenamiento automático de tarjetas de crédito y funciones de pago. El riesgo de confiar una información tan sensible a un dispositivo móvil (“todo en un mismo lugar”) no debería de descuidarse.

Desde un punto de vista de gestión de seguridad, varios intentos se han llevado a cabo para prevenir, o al menos mitigar, la amenaza de la pérdida o robo de un dispositivo:

- Localización del dispositivo basado en el seguimiento de la antena (celda) a la que se conecta
- Capacidad remota de eliminación de los datos y apagado
- Capacidad de bloqueo remoto de la tarjeta SIM

Mientras estos servicios proporcionan cierto grado de seguridad, siguen dejando una ventana de exposición para que los atacantes analicen el dispositivo, probablemente utilizando herramientas analíticas para sortear las características del SO. Esta amenaza es particularmente significativa porque la imposición de contraseñas seguras o el cifrado en los dispositivos móviles pueden estar restringidos debido a limitaciones del SO.

RIESGO ORGANIZACIONAL

Como con otras muchas tecnologías, los dispositivos móviles se han introducido rápidamente en las empresas a todos los niveles. Están disponibles para la mayoría de los usuarios, bien porque son proporcionados por la compañía o por programas BYOD. En términos de datos, información y conocimientos que existen en la empresa, muchos usuarios tienen acceso privilegiado que a menudo se replica en sus dispositivos móviles.

Aunque los entornos corporativos de PCs han sido objetivo de medidas endurecedoras y protectoras durante muchos años, los dispositivos móviles y sus comparativamente pobres mecanismos de seguridad son más difíciles de gestionar y controlar. A modo de ejemplo, la gerencia (C-suite) y la alta dirección a menudo son usuarios intensos de móviles, y cualquier compromiso a sus dispositivos que tenga éxito puede causar un daño importante de modo seguro.

Otro riesgo organizativo importante aparece de la creciente complejidad y la diversidad de los dispositivos móviles comunes. Mientras que los primeros dispositivos móviles no requerían más que los conocimientos básicos sobre cómo usar un teclado, los teléfonos inteligentes ofrecen todo, desde telefonía básica a aplicaciones complejas. Incluso para usuarios experimentados, este nivel de complejidad puede ser un desafío, y muchos dispositivos móviles están pensados para llevar al usuario a cometer errores humanos y problemas de seguridad causados por el usuario. Ejemplos como la itinerancia de datos involuntaria o el seguimiento involuntario vía GPS demuestran cuántos usuarios no entienden las amplias funciones de sus dispositivos.

Al mismo tiempo, la rápida aparición de nuevas generaciones de hardware requiere de una constante adaptación por parte de los usuarios y de las empresas. Los comparativamente largos ciclos de administración de sistemas que se encuentran en las empresas más grandes, pueden suponer un problema cuando los dispositivos móviles se renuevan, aproximadamente, cada dos años. Igualmente, la vida útil de los SO de los móviles y las aplicaciones es cada vez más corta.

El riesgo resultante para los usuarios se agrava por el hecho que son pocas las empresas que ofrecen, formación formal o informal sobre el uso de los dispositivos móviles. Los usuarios son literalmente abandonados a su suerte cuando se trata de adaptarse y usar nuevas tecnologías y nuevos servicios.

RIESGO TÉCNICO

Monitorización de actividades y Recuperación de datos

En general, los dispositivos móviles utilizan SO basados en servicios con la capacidad de hacer funcionar varios servicios a la vez. Mientras que las primeras variantes de los SO eran bastante transparentes y controlables en términos de actividad, las versiones más recientes muestran una tendencia a “simplificar” la interfaz de usuario restringiendo la capacidad del usuario de cambiar la configuración de bajo nivel. Sin embargo, monitorizar e influenciar la actividad es la función principal del spyware y malware, de la misma manera que lo es la recuperación de datos encubiertos. La información puede ser interceptada en tiempo real mientras está siendo generada en el dispositivo. Ejemplos incluyen mandar cada e-mail enviado desde el dispositivo a una dirección oculta de un tercero, permitir a un atacante escuchar una llamada telefónica o simplemente activar la grabación por el micrófono. La información almacenada como listas de contactos o emails guardados también puede ser recuperada. La **figura 6.6** muestra una perspectiva de los objetivos y sus correspondientes riesgos.

Figura 6.6—Riesgo de Monitorización de actividad y Recuperación de datos⁷⁹

Objetivo	Riesgo
Mensajería	Ataques genéricos de texto SMS, transmisión de mensajes MMS cuyo texto y contenido ha sido enriquecido
	Recuperación de contenidos de correo electrónico en línea y fuera de línea
	Inserción del comandos de servicio a través de mensajes de broadcast celular SMS
	Ejecución de código arbitrario a través de SMS/MMS
	Habilitación de ML para mensajes SMS o correo electrónico
	Reorientar o ataques de phishing por habilitación de HTML en mensajes SMS o correo electrónico
Audio	Iniciación de llamada encubierta , grabación de llamadas
	Habilitar la grabación a través del micrófono
Imágenes/Video	Recuperación de las fotografías y videos , por ejemplo, a través de la práctica de piggybacking de la funcionalidad de "compartir" presente habitualmente en la mayoría de las aplicaciones móviles
	Tomar y compartir fotos o videos encubiertos, incluyendo el borrado sin rastro de dicho material
Geolocalización	Monitorización y recuperación de datos de posicionamiento GPS, incluyendo la fecha y hora
Datos estáticos	Recuperación de lista de contactos, calendario, tareas, notas
Historial	Monitorización y recuperación de todos los archivos históricos en el dispositivo o en la tarjeta SIM (llamadas, SMS, navegación, información de entrada, contraseñas almacenadas, etc.)
Almacenamiento	Ataques genéricos en el dispositivo de almacenamiento (disco duro o disco de estado sólido [SSD]) y los datos replicados allí

En la práctica, el riesgo ya se ha materializado en la mayoría de las plataformas de dispositivos móviles y SO.

Junto con los ataques a la conectividad, el riesgo de monitorizar / influenciar la actividad y la recuperación de datos encubiertos es importante.

CONECTIVIDAD DE RED NO AUTORIZADA

La mayoría de spyware o malware – una vez implantados en un dispositivo móvil – necesita uno o más canales para comunicarse con el atacante. Mientras el malware “durmiente” puede tener un periodo de latencia y permanecer inactivo durante semanas o meses, la información recogida necesitará ser transmitida en algún momento del dispositivo móvil a otro destino.

De forma similar, la función de comando y control encontrada habitualmente en los malware requiere una conexión directa entre el dispositivo móvil y el atacante, especialmente cuando los comandos y las acciones deben de ser ejecutadas y monitorizadas en tiempo real (ej. Escuchas secretas o toma de fotografías encubierta). La **figura 6.7** muestra los vectores más comunes para la conectividad de red no autorizada y el riesgo típico que se desprende de ellos.

Figura 6.7—Riesgo de conectividad no autorizada⁸⁰

Vector	Riesgo
Email	Transmisión de datos cuya complejidad varía entre baja a alta (incluyendo archivos de gran tamaño)
SMS	Transmisión de datos simples, instalaciones de comando y control limitadas (comando de servicio)
HTTP get/post	Vector de ataque genérico para la conectividad, comando y control basado en el navegador
Socket TCP/UDP	Vector de ataque de bajo nivel para la transmisión de datos sencillos a complejos
Exfiltración DNS	Vector de ataque de bajo nivel para la transmisión de datos cuya complejidad varía entre baja a alta, cuyas posibilidades de detección son lentas pero difíciles
Bluetooth	Transmisión de datos cuya complejidad varía entre baja a alta, instalación de comando y control basado en el perfil, vector de ataque genérico para las proximidades
WLAN/WiMAX	Vector de ataque genérico para comando y control completo del objetivo, equivalente a la red cableada

⁷⁹ ISACA, *Securing Mobile Devices*, EE.UU., 2012

⁸⁰ Ibid

Estos vectores de conectividad pueden ser usados de forma combinada, por ejemplo cuando se utiliza la funcionalidad de comando y control basada en el navegador por medio de Bluetooth en un escenario de proximidad. Un importante punto a tener en cuenta es el relativo anonimato de los vectores de conectividad, especialmente en Bluetooth y WLAN/WiMAX. El riesgo de ataques ad-hoc en dispositivos móviles es significativamente superior cuando la conectividad anónima es proporcionada por terceros, por ejemplo, en salas de aeropuertos o cafeterías.

SUPLANTACIÓN DE LA VISTA WEB / INTERFAZ DE USUARIO (UI)

Mientras la mayoría de los dispositivos móviles admiten todos los protocolos pertinentes del navegador, la presentación al usuario se modifica por el proveedor del servicio móvil. Esto se hace principalmente para optimizar la visión en pantallas pequeñas. Sin embargo, las páginas web que se ven en dispositivos típicos (pequeños) normalmente muestran contenido “traducido”, incluyendo modificaciones en el código subyacente.

En la suplantación de la interfaz de usuario, las aplicaciones maliciosas presentan una UI que suplanta el dispositivo nativo o la de una aplicación legítima. Cuando la víctima suministra las credenciales de autenticación, se trasmiten al atacante. Esto conduce a ataques de suplantación que son similares al phishing genérico.

Las típicas aplicaciones de vista web permiten ataques a nivel de proxy (phishing de credenciales mientras se hace proxy a una web legítima) y a nivel de presentación (sitios web falsos presentados a través de la vista web móvil). Este tipo de riesgo es frecuente en aplicaciones bancarias donde varios casos de malware han sido documentados. Debido al atractivo que tiene la información de pago y las credenciales de usuarios, es probable que los riesgos de la vista web y suplantación aumenten en un futuro.

FUGA DE DATOS CONFIDENCIALES

Con la aparición de nuevos patrones de trabajo y con la necesidad de descentralizar la disponibilidad de la información, los dispositivos móviles normalmente almacenan grandes cantidades de datos e información confidenciales. Por ejemplo, presentaciones confidenciales y hojas de cálculo son frecuentemente mostradas directamente desde un dispositivo móvil inteligente en vez de utilizar un ordenador portátil.

La cantidad de espacio almacenado encontrado en muchos dispositivos está creciendo y, de media, casi cualquier dispositivo será pronto capaz de almacenar varios gigabytes de información. Esto incrementa el riesgo de fuga de datos, especialmente cuando los dispositivos móviles almacenan información copiada de redes corporativas. Este es el caso habitual de las aplicaciones de email y calendario estándar que replican automáticamente emails con adjuntos, o de los SO móviles que ofrecen la opción de replicar directorios elegidos entre el dispositivo móvil y el dispositivo de sobremesa. La **figura 6.8** muestra la información y su posible riesgo.

Figura 6.8—Riesgo de fuga de datos confidenciales ⁸¹	
Tipo de información	Riesgo
Identidad	Identidad de equipo móvil Internacional (IMEI), ID de fabricante del dispositivo, información de usuario personalizada
	Estadísticas de liberación de hardware/firmware y software, también revelar lo conocido debilidades o exploits (Código para explotar debilidades) potenciales de día cero
Credenciales	Nombres de usuario y contraseñas, pulsaciones de teclado
	Tokens de autorización, certificados (S/MIME, PGP, etc.)
Archivos de localización	Coordenadas GPS, seguimiento de movimiento, inferencia de lugar/conducta
	Todos los archivos almacenados a nivel del sistema operativo/sistema de archivos

La fuga de datos confidenciales puede pasar inadvertida o puede ocurrir a través de ataques de canal lateral. Incluso una aplicación legítima puede tener fallos en el uso del dispositivo. Como resultado, la información y la autenticación de las credenciales pueden estar expuestas a terceros. Dependiendo de la naturaleza de la información que se haya filtrado, puede surgir un riesgo adicional.

Los dispositivos móviles proporcionan una imagen bastante detallada de lo que sus usuarios hacen, dónde están y cuáles son sus preferencias. Los ataques de canal lateral que se prolongan durante largos períodos de tiempo pueden permitir crear un perfil de usuario detallado en términos de movimientos, comportamientos y hábitos privados/empresariales. Los usuarios que se consideren en riesgo pueden llegar a necesitar protección física adicional.

⁸¹ Ibid

La fuga de datos confidenciales que permite predecir el patrón de comportamiento y las actividades de los usuarios está aumentando ya que muchos usuarios prefieren establecer sus dispositivos en modo “siempre encendido” para así beneficiarse de servicios legítimos como pueden ser los sistemas de navegación o puntos de interés locales.

ALMACENAMIENTO NO SEGURO DE DATOS CONFIDENCIALES

Mientras que la mayoría de los SO móviles ofrecen servicios de protección como el almacenamiento encriptado, muchas aplicaciones almacenan datos confidenciales como credenciales o tokens en texto plano. Es más, la información almacenada por el usuario a menudo se replica sin cifrar, y muchos archivos estándar como las presentaciones y las hojas de cálculo de Microsoft Office® se almacenan sin cifrar para permitir un acceso rápido y cómodo.

Otro riesgo asociado al almacenamiento no seguro de datos confidenciales es la utilización de servicios en la nube pública con fines de almacenamiento. Muchos proveedores de dispositivos móviles han introducido servicios en la nube que ofrecen una forma conveniente de almacenar, compartir y gestionar la información en una nube pública. Sin embargo, estos servicios están dirigidos a consumidores privados, y las funcionalidades de seguridad normalmente no servirán para necesidades corporativas.

Este riesgo tiene otra dimensión: cuando los datos y la información son almacenados o replicados en nubes públicas, los términos y condiciones normalmente descartan cualquier tipo de obligación o responsabilidad, pidiendo al usuario que haga sus propios ajustes de seguridad. En un contexto organizativo, estas limitaciones pueden incrementar el riesgo de almacenar datos confidenciales, especialmente en los escenarios de BYOD.

TRANSMISIÓN NO SEGURA DE DATOS CONFIDENCIALES

Los dispositivos móviles dependen predominantemente de la transmisión inalámbrica de datos, excepto en aquellos pocos casos donde están físicamente conectados al ordenador. Como ya se ha señalado anteriormente, estas transmisiones generan un riesgo de conexión a la red no autorizada, especialmente cuando se utiliza Red de área local inalámbrica (WLAN)/ Interoperabilidad mundial para acceso de microondas (WiMAX) o Bluetooth de corto alcance. Como nuevo protocolo de transmisión, la comunicación de corto alcance (NFC) aumenta el riesgo a muy corta distancia, por ejemplo, cuando se transmiten datos de pago a una distancia de varios centímetros.

Aunque los datos en reposo están protegidos mediante cifrado y otros medios, la transmisión no siempre está cifrada. Es probable que los usuarios de dispositivos móviles utilicen frecuentemente redes públicas no seguras, y el gran número de ataques conocidos en WLAN y Bluetooth supone un riesgo importante.

El reconocimiento automático de redes, una característica típica de los SO móviles, puede conectarnos a una WLAN disponible en los alrededores, memorizando el Identificador del conjunto de servicios (SSID) y los canales. Para muchos proveedores importantes de redes públicas WLAN, estos SSIDs son idénticos en todo el mundo. Esto es intencionado y conveniente; aun así, el riesgo de un ataque malicioso similar aumenta con el uso de nombres genéricos que el dispositivo móvil normalmente aceptará sin necesidad de verificarlos.

Aunque muchas empresas han implementado soluciones de Redes virtuales privadas (VPN) para sus usuarios, puede que éstas no funcionen en dispositivos móviles que son utilizados tanto para transacciones profesionales como personales. Dada la complejidad relativa de configurar y activar la VPN en dispositivos móviles, los usuarios pueden desactivar la transmisión de datos protegida para acceder a otro servicio que no soporte VPN. Incluso para instalaciones de VPN de canal distribuido – ofreciendo una VPN a la empresa mientras se mantiene el enlace abierto a la red pública – el riesgo de un ataque en el origen sigue siendo alto.

DIRIGIDO POR VULNERABILIDADES

Al contrario que los ordenadores portátiles o de sobremesa, los dispositivos móviles sólo ofrecen aplicaciones rudimentarias para el trabajo de oficina. En muchos casos, el tamaño del dispositivo reduce su capacidad de visualización y edición. Como consecuencia, las aplicaciones de procesador de texto típico, hojas de cálculo y presentaciones en dispositivos móviles tienden a ser optimizadas para permitir la apertura y lectura, en lugar de permitir la edición de la información que contiene. Asimismo, formatos de documentos populares como el formato de documentos portables (PDF) de Adobe® se implementan, más o menos, como una solución de sólo lectura diseñada para una lectura rápida en lugar de procesamiento a gran escala.

Al mismo tiempo, se está convirtiendo en una práctica común insertar contenido activo en documentos y archivos PDF. Éstos pueden ser hipervínculos completos, enlaces abreviados o documentos y macros embebidos. Esto se conoce como un vector de ataque para el malware y otros exploits.

La naturaleza restrictiva de las aplicaciones para los dispositivos móviles conduce a un mayor riesgo dirigido por los ataques porque estas aplicaciones pueden no reconocer enlaces malformados y omitir las advertencias habituales que los usuarios podrían esperar de las versiones de escritorio de Microsoft Office o las aplicaciones de PDF.

En la práctica, estas vulnerabilidades crean riesgos y un número de amenazas para el usuario final, por ejemplo, la inserción de material ilegal, la inadvertencia del uso de servicios “Premium” vía SMS/MMS o pasar por alto los mecanismos de doble factor de autenticación.

TEMA 4—CONSUMERIZACIÓN DE TI Y DISPOSITIVOS MÓVILES

CONSUMERIZACIÓN DE TI

Los dispositivos móviles tienen un impacto profundo en la forma en la que se llevan a cabo los negocios y en los patrones de comportamiento de la sociedad. Han aumentado mucho la productividad y la flexibilidad en el trabajo, hasta el punto en el que los individuos se encuentran en condiciones de trabajar desde cualquier lugar en cualquier momento. Asimismo, la potencia de cálculo de los dispositivos inteligentes les ha permitido reemplazar los PCs y portátiles para muchas aplicaciones de empresa.

Tanto los fabricantes como los proveedores de servicios han creado tanto nuevos dispositivos como nuevos modelos de negocio como los pagos móviles o las suscripciones de descargas usando un modelo de pago por uso. Simultáneamente, la masificación del consumo de dispositivos móviles ha relegado a las empresas, por lo menos en algunos casos, a seguidores en lugar de líderes de opinión en cuanto a qué dispositivos se utilizan y cómo se utilizan.

Los impactos del uso de dispositivos móviles pueden englobarse en dos amplias categorías:

- El hardware en sí mismo ha sido desarrollado a un nivel en el que la potencia de cálculo y el almacenaje son prácticamente equivalentes al hardware de PC. De conformidad con la ley de Moore, un teléfono inteligente típico representa el equivalente de lo que solía ser una máquina de gama media hace una década.
- Nuevos servicios móviles han creado nuevos modelos de negocio que están cambiando las estructuras organizativas y la sociedad en su conjunto.

La consumerización no está limitada a los dispositivos. • Nuevas aplicaciones y servicios gratuitos proporcionan mejores experiencias de usuario para cosas como tomar notas, video conferencias, correo electrónico y almacenamiento en la nube, que sus respectivas partes aprobadas por la empresa. En lugar de contar con dispositivos y software proporcionados por la empresa, los empleados están utilizando sus propias soluciones que se ajusten mejor a su estilo de vida, sus necesidades y preferencias.

BYOD

La movilidad en general, y la accesibilidad desde cualquier ubicación han mejorado las prácticas de negocio y han permitido a las empresas centrarse en sus actividades primordiales mientras reducen la cantidad de espacio utilizado de oficinas. Para los empleados, los dispositivos móviles han traído una mayor flexibilidad, por ejemplo, en los programas de BYOD.

La idea de utilizar dispositivos móviles de propiedad privada rápidamente se ha afianzado como un concepto, y muchas empresas se están enfrentando a un nuevo obstáculo: cuando la compra y el aprovisionamiento centralizado de dispositivos móviles es lento o engorroso, muchos usuarios han creado la expectativa de conectar sus propias unidades para lograr productividad de una forma rápida y pragmática.

La desventaja evidente es la proliferación de dispositivos con conocidos (o desconocidos) riesgos de seguridad, y el desafío formidable de gestionar la seguridad del dispositivo frente a desafíos desconocidos. Sin embargo, como las formas de trabajo están cambiando, hay signos claros que BYOD se está convirtiendo en un importante factor de motivación laboral, ya que los empleados no están dispuestos a aceptar restricciones tecnológicas.

Mientras que BYOD puede parecer un facilitador, también ha traído un número de nuevas áreas de riesgos y amenazas asociadas. Estos deben ser equilibrados con las ventajas del uso de dispositivos móviles, teniendo en cuenta las necesidades de seguridad tanto de la persona como de la empresa. Por lo tanto, la gestión de la seguridad debería de abordar tanto el potencial innovador como los riesgos y amenazas del uso de los dispositivos flexibles porque es improbable que las restricciones o prohibiciones de determinados tipos de dispositivos sea efectivo incluso a medio plazo. En efecto, el hecho de que algunas empresas hayan intentado prohibir ciertos dispositivos ha permitido que la tecnología prohibida se haya hecho un hueco en el panorama empresarial – especialmente si esa tecnología está ya ampliamente aceptada por los usuarios privados. Como resultado, las empresas con perspectivas restrictivas sobre dispositivos innovadores siempre estarán detrás de la curva de la amenaza y así expuestas a un riesgo innecesario. Los pros y contras de BYOD se encuentran numerados en la **figura 6.9**.

Figura 6.9—Pros y Contras del BYOD	
Pros	Contras
<ul style="list-style-type: none"> • El coste se traslada al usuario • Satisfacción del trabajador • Actualizaciones de hardware más frecuentes • Tecnología innovadora con las últimas características y capacidades 	<ul style="list-style-type: none"> • Pérdida de control de TI • Riesgo de seguridad conocido o desconocido • Política de uso aceptable más difícil de implementar • Cumplimiento y propiedad de los datos no claros

INTERNET DE LAS COSAS (IOT)⁸²

El Internet de las cosas (del inglés Internet of Things, IoT) se refiere a objetos físicos que tienen embebida una red y elementos de cómputo, y que comunican con otros objetos en la red. Las definiciones de IoT varían en función del concepto de camino de la comunicación. Algunas definiciones establecen que los dispositivos de IoT se comunican a través internet, otras que los dispositivos de IoT se comunican zona través de la red, que puede ser o no Internet.

Esta creciente interconexión de las “cosas” está compuesta de objetos que tienen la capacidad de comunicarse de nuevas maneras – entre ellos, con los propietarios o operadores, con los fabricantes o con otros – para hacer la vida de la gente y de las empresas más sencilla, eficiente y competitiva.

La tendencia del IoT es transformadora desde el punto de vista de la empresa. El valor de la empresa y la competitividad operacional se pueden derivar a medidas que las empresas capitalizan en estas nuevas capacidades para obtener un mayor y mejor valor de negocio de los dispositivos adquiridos. Adicionalmente, las empresas pueden competir más eficientemente en el mercado a medida que proveen estas características en los productos que venden y a medida que también las incorporan en los servicios que ofrecen.

Sin embargo, con el valor adicional viene el riesgo adicional. Aunque el riesgo específico depende del uso, algunas de las áreas de riesgo que los usuarios de IoT deben considerar son:

- Riesgo del negocio:
 - Salud y seguridad en el trabajo
 - Cumplimiento regulatorio
 - Privacidad de usuario
 - Costes inesperados
- Riesgo operacional:
 - Acceso inapropiado a la funcionalidad
 - Uso en segundo plano (shadow usage)
 - Rendimiento
- Riesgo técnico:
 - Vulnerabilidades de dispositivo
 - Actualizaciones de dispositivo
 - Gestión de dispositivo

⁸² ISACA, *Internet of Things: Risk and Value Considerations*, EE.UU., 2015

La **figura 6.10** ilustra algunos puntos a considerar relativos a IoT.

Figura 6.10—Acciones IoT: qué hacer (Dos) y qué evitar (Don'ts)	
Dos	Don'ts
<ul style="list-style-type: none"> • Preparar un modelo de amenaza. • Evaluar el valor de la empresa. • Evaluar de forma holística y gestionar el riesgo. • Equilibrio entre riesgo y beneficio. • Notificar a las partes interesadas del uso previsto. • Participar de forma temprana con los equipos de negocio. • Reunir a las partes interesadas para asegurar la participación y una planificación completa. • Buscar puntos de integración con las protecciones de seguridad y operación existentes. • Examinar y documentar la información que se recoge y transmite por los dispositivos para analizar posibles impactos en la privacidad. • Discutir con las partes interesadas relevantes cuándo, cómo y con quién esta información se compartirá y bajo qué circunstancias. 	<ul style="list-style-type: none"> • Desarrollar rápidamente sin consultar a la empresa u otras partes interesadas. • Ignorar los requisitos de la política existente, tales como la seguridad y la privacidad. • Ignorar los mandatos regulatorios. • Asumir que los proveedores (hardware, software, middleware y otros) tienen conocimiento del uso que se quiere hacer de los dispositivos y de los requisitos de seguridad. • Ignorar los ataques o las vulnerabilidades específicas del dispositivo. • No tener en cuenta las consideraciones de privacidad o “ocultar” los datos que se recogen / transmiten de los usuarios finales.

MACRODATOS

Big data (macrodatos) es un término técnico y de marketing que hace referencia a un activo valioso de la empresa, es decir, la información. Representa una tendencia en tecnología que lidera el camino hacia un nuevo enfoque en el entendimiento del mundo y la toma de decisiones de negocio. Estas decisiones se toman en función de cantidades muy grandes de datos complejos, estructurados y no estructurados (por ejemplo, tweets, videos, transacciones comerciales) que se han vuelto difíciles de procesar mediante la utilización de herramientas básicas de bases de datos y herramientas de gestión de almacenes de datos ("data warehouse"). La gestión y el procesamiento del conjunto de datos cada vez mayor requieren la ejecución de software especializado en múltiples servidores. Para algunas empresas, los grandes conjuntos de datos se cuentan en cientos de gigabytes; para otras, en terabytes o incluso en petabytes, con una tasa de crecimiento y cambio frecuente y rápido (en algunos casos, casi en tiempo real). Esencialmente el término big data se refiere a conjuntos de datos que son demasiado grandes o que cambian demasiado rápido como para ser analizados mediante técnicas tradicionales de bases de datos relacionales o multidimensionales, o herramientas de software comúnmente utilizadas para capturar, administrar y procesar los datos en una ventana de tiempo razonable.⁸³

Este cambio en las capacidades analíticas de trabajo con macrodatos puede introducir riesgos técnicos y de operación y las organizaciones deben entender los riesgos en los que pueden incurrir a través de la adopción o no adopción de estas capacidades.

Los riesgos técnicos y operacionales deben considerar que ciertos elementos de datos pueden ser gobernados por reguladores o requerimientos contractuales y que esos elementos de datos pueden necesitar ser centralizados en un lugar (o al menos ser accesibles de forma centralizada) para que los datos puedan ser analizados. En algunos casos esta centralización puede acarrear riesgos técnicos.⁸⁴ Por ejemplo:⁸⁵

- **Riesgo técnico amplificado**—Si un usuario no autorizado obtuviera acceso a repositorios centralizados, pondría en peligro la totalidad de esos datos en lugar de un subconjunto de los mismos.
- **Privacidad (recogida de datos)**—Técnicas analíticas que pueden impactar en la privacidad; por ejemplo, individuos cuyos datos están siendo analizados pueden sentir que la información revelada sobre ellos es demasiado intrusiva.
- **Privacidad (re-identificación)**—Del mismo modo, cuando los datos se agregan, la información semi anónima o información que no es información identificable individualmente puede volverse no anónima o identificable en el proceso.

⁸³ ISACA, *Big Data: Impacts & Benefits*, EE.UU, 2013, www.isaca.org/Knowledge-Center/Research/Documents/Big-Data_whp_Eng_0413.pdf

⁸⁴ ISACA, *Generating Value from Big Data Analytics*, EE.UU., 2014, www.isaca.org/Knowledge-Center/Research/Documents/Generating-Value-from-Big-Data-Analytics_whp_Eng_0114.pdf

⁸⁵ *Ibid.*

INTELIGENCIA ARTIFICIAL

La inteligencia artificial (IA) es el desarrollo de sistemas de computación avanzados que pueden simular capacidades humanas tales como el análisis. Esta tecnología emergente hará posible que equipos de seguridad manejen de forma precisa y eficiente grandes cantidades de datos complejos y los analicen para nuevas amenazas.

Los esquemas de detección de la IA serán capaces de tratar las amenazas comunes, mientras que también investigarán anomalías para detectar rápidamente las nuevas amenazas en constante evolución. Además, en vez de que los analistas de seguridad tengan que presentar enormes cantidades de datos brutos, la tecnología IA puede presentar la información en vistas más prácticas y adaptarse de forma rápida a los nuevos métodos de ataque.

TEMA 5—LA NUBE Y LA COLABORACIÓN DIGITAL

Según el NIST y la Cloud Security Alliance (CSA), la computación en la nube se define como un “modelo para permitir convenientemente, el acceso a la red bajo demanda a un conjunto compartido de recursos informáticos configurables (ej. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser provisionados y liberados con un mínimo esfuerzo de gestión o interacción por parte del proveedor del servicio.”⁸⁶

La computación en la nube ofrece a las empresas una forma de ahorrar en gasto de capital asociado a los métodos tradicionales de gestión de las TI. Las plataformas comunes que se ofrecen en la nube incluyen Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS). La virtualización y las arquitecturas orientadas al servicio (SOAs) actúan como factores clave en estos escenarios. Aunque parezca atractivo, la computación en la nube no deja de tener su propio conjunto de riesgos, el primero y más importante de los cuales siendo la seguridad de la información que se confía a los proveedores de la nube.⁸⁶

Al igual que ocurre con cualquier contrato con un tercero, es importante para las organizaciones asegurar que sus proveedores de nube tienen sistemas de seguridad equivalentes o mejores a los que utiliza la propia organización. Muchos de los proveedores de nube están certificados en la ISO 27001 o FIPS 140-2. Además, las organizaciones pueden solicitar auditorías del proveedor de la nube. Las auditorias de seguridad deberían cubrir las instalaciones, redes, hardware y sistemas operativos dentro de la infraestructura de la nube.

RIESGO DE LA COMPUTACIÓN EN LA NUBE

El reto para la computación en la nube es proteger la información dentro de nubes públicas y privadas así como asegurar el gobierno, la gestión del riesgo y el cumplimiento en todo el entorno integrado. El NIST remarca los siguientes riesgos principales de seguridad de la infraestructura de la nube:

- **Pérdida de gobierno**—El cliente generalmente cede cierto nivel de control al proveedor de la nube, esto puede afectar a la seguridad, especialmente si los acuerdos de nivel de servicio (SLA) dejan una brecha en las defensas de seguridad.
- **Bloqueo**—Puede ser complicado para un cliente cambiar de un proveedor a otro, lo cual genera dependencia a un proveedor de la nube en particular para la prestación del servicio.
- **Fallos en el aislamiento**—Una característica de la computación en la nube son los recursos compartidos. Aunque no es común, el fallo de los mecanismos que separan el almacenamiento, la memoria, el enrutamiento y la reputación entre los diferentes clientes puede generar riesgos.
- **Cumplimiento**—Migrar a la nube puede representar un riesgo para que la organización obtenga una determinada certificación en caso de que el proveedor no pueda proporcionar evidencias de cumplimiento.
- **Compromiso de la interfaz de gestión**—La interfaz de gestión de clientes puede plantear un riesgo mayor en el caso que se acceda a ella a través de Internet y facilite el acceso a un conjunto más amplio de recursos.
- **Protección de datos**—Puede ser difícil para los clientes verificar los procedimientos de gestión de datos del proveedor de la nube.
- **Eliminación incompleta o insegura de datos**—Debido a los múltiples contratos de arrendamientos y la reutilización de los recursos de hardware, hay un mayor riesgo que la información no sea eliminada completamente, adecuadamente o de una manera oportuna.
- **Infiltrado malicioso**—Los arquitectos de la nube tienen funciones de alto riesgo. Un infiltrado malicioso puede causar daño a un nivel muy alto.

Este riesgo puede llevar a diferentes eventos de amenaza. La CSA ha identificado en la siguiente lista las mayores amenazas a la computación en la nube:⁸⁷

1. Brecha en la seguridad de datos
2. Pérdida de datos
3. Secuestro de cuentas
4. Interfaces de programación de aplicaciones (APIs) no seguras
5. Denegación de servicio (DoS)
6. Infiltrados maliciosos
7. Abuso de los servicios en la nube
8. Diligencia debida insuficiente
9. Problemas derivados de compartir tecnología

⁸⁶ ISACA, *Top Business/Technology Issues Survey Results*, EE.UU., 2014,

⁸⁷ Cloud Security Alliance (CSA), *The Notorious Nine: Cloud Computing Top Threats in 2013*, 2013

RIESGO DE APLICACIÓN EN LA NUBE

En la implementación y adaptación de las estrategias basadas en la nube, las empresas tienden a incluir ofertas SaaS, extendiéndolo a veces a procedimientos de negocio críticos y a las aplicaciones relacionadas. A pesar del hecho que estas ofertas de servicios pueden traer ventajas al negocio, generan vulnerabilidades del flujo de datos que pueden ser explotadas por el ciber crimen y la ciber guerra. El riesgo resultante se ve agravado por el hecho que muchos vendedores y proveedores de hardware (de dispositivos móviles), suministran servicios en la nube gratuitos para reforzar la lealtad del usuario. Esto es a menudo el caso de la sincronización de datos, el manejo de tipos de archivo populares tales como música o fotografías, e información personal como email y entradas del calendario.

La capa de aplicación en el entorno de TI en general es especialmente susceptible a ataques de día-cero, como lo demuestran muchos ejemplos prácticos. Incluso los grandes proveedores de software actualizan y parchean frecuentemente sus aplicaciones, pero nuevos vectores de ataque que utilizan estas aplicaciones aparecen a diario. En términos de ciber crimen y ciber guerra, el mercado de los ataques de día cero está muy vivo, y el lapso de tiempo que transcurre desde el descubrimiento hasta el reconocimiento y el remedio se hace cada vez más grande.

Asimismo, la propagación de malware complejo ha ido creciendo en los últimos años. Desde una perspectiva del ciber crimen y la ciber guerra, los últimos ejemplos de malware muestran un nivel de sofisticación y persistencia más alto que las versiones básicas utilizadas por atacantes oportunistas. Mientras que los proveedores de software son rápidos a la hora de abordar malware en términos de reconocimiento y eliminación, existe un riesgo residual significativo de malware que se puede hacer persistente en las empresas objetivo.

Los ataques de malware secundarios—donde las APTs hacen uso del malware sencillo ya instalado—a menudo tienen éxito cuando las condiciones del entorno son propicias para el error del usuario o cuando hay falta de vigilancia, por ejemplo en el hogar del usuario o cuando el usuario está viajando. En la práctica, la eliminación del malware primario (proceso bastante simple) a menudo disipa cualquier sospecha y hace que los usuarios y los administradores de seguridad se dejen llevar por un falso sentimiento de seguridad. El malware que es secundario y muy complejo puede haberse infiltrado en el sistema previamente, presentando como cebo un conocido y simple malware primario.

BENEFICIOS DE LA COMPUTACIÓN EN LA NUBE

Aunque la computación en la nube es atractiva para los atacantes debido a la masiva concentración de información, las defensas de la nube pueden ser más robustas, escalables y rentables. ENISA proporciona los siguientes beneficios de seguridad más importantes de la computación en la nube:

- **Impulso de mercado**—Puesto que la seguridad es una de las mayores prioridades para la mayoría de los clientes de la nube, los proveedores de la nube tienen una motivación importante para incrementar y mejorar sus prácticas de seguridad.
- **Escalabilidad**—La tecnología en la nube permite una rápida reasignación de los recursos, tales como filtrado, organización del tráfico, autenticación y cifrado y medidas defensivas.
- **Rentabilidad**—Todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. La concentración de recursos proporciona perímetros físicos y controles de acceso físico más baratos y facilita y abarata la aplicación de muchos procesos de seguridad.
- **Actualización oportuna y eficaz**—Las actualizaciones pueden ser desplegadas rápidamente a través de una plataforma homogénea.
- **Auditoría y evidencia**—La computación en la nube puede proporcionar imágenes forenses de máquinas virtuales, lo que implica un tiempo de inactividad menor para las investigaciones forenses.

Aunque existen muchos beneficios de la computación en la nube, también existe riesgo. La **figura 6.11** lista los beneficios y riesgos de la computación en la nube.

Figura 6.11—Beneficios y riesgos de la computación en la nube	
Beneficios	Riesgo
<ul style="list-style-type: none"> ● Impulso de mercado para el cloud ● Escalabilidad ● Implementación rentable ● Actualización oportuna y eficaz ● Capacidades de auditoría y evidencia 	<ul style="list-style-type: none"> ● Pérdida de gobierno ● Bloqueado a un proveedor ● Fallos en el aislamiento ● Cumplimiento ● Protección de datos ● Compromiso de la interfaz de gestión de clientes ● Eliminación de datos inseguros o incompletos ● Infiltrado malicioso

MEDIOS SOCIALES⁸⁸

La tecnología de las redes sociales implica la creación y divulgación de contenido a través de las redes sociales mediante Internet. Las diferencias entre las redes sociales y los medios tradicionales están definidas por el nivel de interacción e interactividad disponible para el consumidor. Por ejemplo, un espectador puede mirar las noticias en televisión sin mecanismos de retroalimentación interactiva, mientras que las herramientas de las redes sociales permiten a los consumidores comentar, debatir e incluso distribuir las noticias. El uso de las redes sociales creó plataformas de comunicación altamente efectivas donde cualquier usuario, prácticamente en cualquier lugar del mundo, puede crear contenido libremente y divulgar esta información en tiempo real a la audiencia mundial que varía en tamaño de algunas a literalmente millones de personas.

Existen varios tipos de herramientas de redes sociales: blogs (por ejemplo, WordPress), sitios que comparten imágenes y videos (por ejemplo, Flickr y YouTube), interacciones sociales (por ejemplo, Facebook) y redes profesionales (por ejemplo, LinkedIn). El vínculo común entre todas las formas de redes sociales es que el contenido es proporcionado y administrado por usuarios individuales que aprovechan las herramientas y plataformas que proveen los sitios de las redes sociales.

Las empresas usan las redes sociales para aumentar el reconocimiento de la marca, las ventas, los ingresos y la satisfacción del cliente; sin embargo, existe un riesgo asociado a su uso. Se dividen en empresas con presencia en las redes sociales corporativas y empresas cuyos empleados utilizan las redes sociales.

El riesgo asociado a una presencia en las redes sociales corporativas incluye:

- Introducción de virus/software malintencionado (malware) a la red de organización
- Información errónea o engañosa publicada a través de una presencia corporativa fraudulenta o secuestrada
- Derechos de contenido poco claros o indefinidos de la información difundida en los sitios de las redes sociales
- Insatisfacción del cliente debido a las faltas expectativas de respuesta de calidad o respuesta
- Mala administración de las comunicaciones electrónicas que puede verse afectada por las regulaciones de retención o la exhibición de documentos electrónicos

Riesgos asociados al uso de medios sociales por parte del empleado incluyen:

- Uso de cuentas personales para comunicar información relacionada con el trabajo
- Difusión de imágenes o información por parte de los empleados que los vinculan a la empresa
- Uso excesivo de redes sociales por parte de los empleados en el lugar de trabajo
- Acceso a las redes sociales por parte de los empleados a través de dispositivos móviles proporcionados por la empresa (teléfonos inteligentes, tabletas)

⁸⁸ ISACA, *Manual de Preparación al Examen CISA 26^a edición*, EE.UU., 2015

Página dejada en blanco intencionadamente

SECCIÓN 6—EVALUACIÓN DE CONOCIMIENTOS

1. _____ se define como “un modelo que permite un acceso conveniente, por demanda y a través de la red, a un conjunto compartido de recursos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con mínima administración o interacción con el proveedor del servicio”.
 - A. Software como servicio (SaaS)
 - B. Computación en la nube
 - C. Macrodatos
 - D. Plataforma como servicio (PaaS)
2. Seleccione todas las opciones que apliquen. ¿Cuál de las siguientes afirmaciones sobre las amenazas persistentes avanzadas (APT) son verdaderas?
 - A. Las APT normalmente se originan a partir de fuentes tales como grupos del crimen organizado, activistas o gobiernos.
 - B. Las APT usan técnicas de ofuscación que las ayudan a permanecer sin ser descubiertas durante meses o incluso años.
 - C. Las APT suelen ser proyectos a largo plazo y con múltiples fases, enfocados en el reconocimiento.
 - D. El ciclo de ataque de la APT comienza con la penetración del objetivo y la recolección de información sensible.
 - E. Aunque a menudo se asocian con las APT, las agencias de inteligencia rara vez son las autoras de los ataques APT.
3. ¿Cuáles de las siguientes respuestas son beneficios para el BYOD?
 - A. La política de uso aceptable es más fácil de implementar.
 - B. Transferencia del costo al usuario.
 - C. La satisfacción del trabajador aumenta.
 - D. El riesgo de seguridad es conocido por el usuario.
4. Escoja tres. ¿Qué tipos de riesgo se asocian normalmente con los dispositivos móviles?
 - A. Riesgo organizacional
 - B. Riesgo de cumplimiento
 - C. Riesgo técnico
 - D. Riesgo físico
 - E. Riesgo transaccional
5. ¿Qué tres elementos del panorama de amenazas actual han proporcionado mayores niveles de acceso y conectividad, y por lo tanto han aumentado las oportunidades para el delito cibernético?
 - A. La mensajería de texto, la tecnología Bluetooth y las tarjetas SIM
 - B. Las aplicaciones Web, los botnets y el malware primario
 - C. Las ganancias financieras, la propiedad intelectual y la política
 - D. La computación en la nube, las redes sociales y la computación móvil

Ver respuestas en el Anexo C.

Página dejada en blanco intencionadamente



Apendices

Anexo A—Declaraciones de conocimientos

Anexo B—Glosario

Anexo C—Respuestas de la Evaluación de conocimientos

Página dejada en blanco intencionadamente

ANEXO A—DECLARACIONES DE CONOCIMIENTOS

DOMINIO 1: CONCEPTOS DE CIBERSEGURIDAD

- 1.1 Conocimiento de los principios de ciberseguridad utilizados para gestionar el riesgo relacionado con el uso, procesamiento, almacenamiento y transmisión de información o de datos
- 1.2 Conocimiento de la gestión de la seguridad
- 1.3 Conocimiento de los procesos de gestión del riesgo, incluyendo las etapas y métodos para la evaluación del riesgo
- 1.4 Conocimiento de los agentes de amenaza (por ejemplo, “script kiddies”, los no patrocinados por estados-nación, y los patrocinados por estados-nación)
- 1.5 Conocimiento de las funciones o roles de la ciberseguridad
- 1.6 Conocimiento de tácticas, técnicas y procedimientos (TTP) comunes del adversario.
- 1.7 Conocimiento de leyes, políticas, procedimientos y requisitos de gobierno relevantes
- 1.8 Conocimiento de los controles de ciberseguridad

DOMINIO 2: PRINCIPIOS DE ARQUITECTURAS DE CIBERSEGURIDAD

- 2.1 Conocimiento de los procesos de diseño de la red, de manera que incluya la comprensión de los objetivos de seguridad, los objetivos operacionales y las compensaciones
- 2.2 Conocimiento de los métodos, herramientas y técnicas de diseño de sistemas de seguridad
- 2.3 Conocimiento de acceso a la red, la gestión de identidades y de accesos
- 2.4 Conocimiento de principios y métodos de seguridad de la tecnología de la información (TI) (por ejemplo, firewalls, zonas desmilitarizadas, cifrado)
- 2.5 Conocimiento de los conceptos de arquitectura de seguridad de la red, incluyendo la topología, protocolos, componentes y principios (por ejemplo, aplicación de la defensa en profundidad)
- 2.6 Conocimiento de los conceptos y la metodología de análisis de malware
- 2.7 Conocimiento de metodologías y técnicas de detección de intrusos, y técnicas para detectar intrusiones basadas en hosts y la red por medio de las tecnologías de detección de intrusión
- 2.8 Conocimiento de los principios de defensa en profundidad y la arquitectura de seguridad de la red
- 2.9 Conocimiento de los algoritmos de cifrado (por ejemplo, Seguridad IP [IPSEC], Estándar de Encriptación Avanzada [AES], Encapsulación enrutada genérica “Generic Routing Encapsulation” [GRE])
- 2.10 Conocimiento de criptografía
- 2.11 Conocimiento de metodologías de cifrado
- 2.12 Conocimiento de cómo fluye el tráfico a través de la red (es decir, transmisión y encapsulación de datos)
- 2.13 Conocimiento de los protocolos de red (por ejemplo, Protocolo de Control de Transmisión y Protocolo de Internet [TCP/IP], Protocolo de Configuración Dinámica del Host [DHCP]), y los servicios de directorio (por ejemplo, el Sistema de Nombres de Dominio [DNS])

DOMINIO 3: SEGURIDAD DE LA RED, SISTEMAS, APLICACIONES Y DATOS

- 3.1 Conocimiento de herramientas de evaluación de vulnerabilidades, incluyendo herramientas de código abierto, y sus capacidades
- 3.2 Conocimiento básico de administración de sistemas, redes y técnicas para fortalecimiento de la seguridad del sistema operativo
- 3.3 Conocimiento de riesgo asociado con virtualizaciones
- 3.4 Conocimiento de las pruebas de penetración
- 3.5 Conocimiento de los principios de gestión de sistemas de red, incluyendo modelos, métodos (por ejemplo, supervisión de rendimiento extremo a extremo) y herramientas
- 3.6 Conocimiento de tecnologías de acceso remoto
- 3.7 Conocimiento de la línea de comandos de UNIX
- 3.8 Conocimiento de amenazas de seguridad y vulnerabilidades de los sistemas y las aplicaciones
- 3.9 Conocimiento de los principios de gestión del ciclo de vida del sistema, incluyendo la seguridad y la usabilidad del software
- 3.10 Conocimiento de requerimientos locales especializados de los sistemas (por ejemplo, sistemas de infraestructura crítica que no pueden emplear la tecnología de la información estándar [TT]) para la seguridad, el rendimiento y la confiabilidad
- 3.11 Conocimiento de amenazas de seguridad y vulnerabilidades de los sistemas y las aplicaciones (por ejemplo, desbordamiento de búfer, código móvil, cross-site scripting, Lenguaje Procedural / Lenguaje de consultas estructuradas [PL/SQL] e inyecciones, condiciones de carrera, canal encubierto, repetición, ataques orientados a retorno, código malicioso)
- 3.12 Conocimiento de la dinámica social de los atacantes informáticos en un contexto global
- 3.13 Conocimiento de técnicas de gestión de configuración segura

- 3.14 Conocimiento de las capacidades y aplicaciones de equipos de red, incluyendo hubs, routers, switches, bridges, servidores, medios de transmisión y hardware relacionado
- 3.15 Conocimiento de los métodos de comunicación, principios y conceptos que soportan la infraestructura de red
- 3.16 Conocimiento de los protocolos de red comunes (por ejemplo, Protocolo de Control de Transmisión/Protocolo de Internet [TCP/IP]) y servicios comunes (por ejemplo, web, correo electrónico, sistema de nombres de dominio [DNS]) y cómo interactúan para proporcionar comunicaciones de red
- 3.17 Conocimiento de los diferentes tipos de redes de comunicación (por ejemplo, red de área local [LAN], red de área amplia [WAN], red de área metropolitana [MAN], red de área local inalámbrica [WLAN], red de área amplia inalámbrica [WWAN])
- 3.18 Conocimiento de las tecnologías de virtualización, y el desarrollo y mantenimiento de la máquina virtual
- 3.19 Conocimiento de seguridad de las aplicaciones (por ejemplo, el ciclo de vida de desarrollo del sistema [SDLC], vulnerabilidades, las mejores prácticas)
- 3.20 Conocimiento de evaluación de la amenaza de riesgo

DOMINIO 4: RESPUESTA A INCIDENTES

- 4.1 Conocimiento de las categorías de incidentes para respuestas
- 4.2 Conocimiento de la continuidad de negocio / recuperación de desastres
- 4.3 Conocimiento de respuesta a incidentes y metodologías de manejo
- 4.4 Conocimiento de herramientas de correlación de eventos de seguridad
- 4.5 Conocimiento de los procesos de incautación y aseguramiento de evidencia digital (por ejemplo, la cadena de custodia)
- 4.6 Conocimiento de los tipos de datos digitales forenses
- 4.7 Conocimiento de los conceptos básicos y las prácticas de procesamiento de datos forenses digitales
- 4.8 Conocimiento de las tácticas, técnicas y procedimientos (TTPS) anti-forenses
- 4.9 Conocimiento de la configuración de herramientas forense comunes y de aplicaciones de soporte (por ejemplo, VMware®, Wireshark®)
- 4.10 Conocimiento de los métodos de análisis de tráfico de red
- 4.11 Conocimiento de qué archivos del sistema (por ejemplo, archivos de log, archivos de registro, archivos de configuración) contienen información relevante, y dónde encontrar dichos archivos del sistema

DOMINIO 5: SEGURIDAD DE LA TECNOLOGÍA EN EVOLUCIÓN

- 5.1 Conocimiento de las tecnologías emergentes, y de sus problemas de seguridad, riesgos y vulnerabilidades asociados
- 5.2 Conocimiento de riesgos asociados con la computación móvil
- 5.3 Conocimiento de los conceptos de computación en la nube, relacionados con los datos y la colaboración
- 5.4 Conocimiento de riesgo de trasladar las aplicaciones y la infraestructura a la nube
- 5.5 Conocimiento de los riesgos asociados con la externalización (outsourcing)
- 5.6 Conocimiento de los procesos y prácticas de la gestión de riesgo de la cadena de suministro

ANEXO B—GLOSARIO

A

Acceso lógico—Habilidad para interactuar con los recursos informáticos concedidos mediante la identificación, autenticación y autorización.

Acceso Wi-Fi protegido (WPA)—Clase de sistemas usada para proteger las redes informáticas inalámbricas (Wi-Fi). WPA fue creado en respuesta a varias deficiencias graves que los investigadores encontraron en el sistema anterior, Privacidad equivalente al cableado (WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue pensado como una medida intermedia para ocupar el lugar de WEP mientras se preparaba 802.11i. WPA está diseñado para funcionar con todas las tarjetas de interfaz de red inalámbrica, pero no necesariamente con puntos de acceso inalámbricos de primera generación. WPA2 implementa la norma completa, pero no funciona con algunas tarjetas de red más antiguas. Ambos proporcionan buena seguridad con dos problemas significativos. En primer lugar, se debe activar WPA o WPA2 y seleccionar en lugar de WEP; WEP normalmente se presenta como la primera opción de seguridad en la mayoría de las instrucciones de instalación. En segundo lugar, en el modo “personal”, que es la opción más habitual para hogares y oficinas pequeñas, se requiere una frase de paso que, para asegurar una seguridad total, debe ser más larga que las contraseñas habituales de seis a ocho caracteres y que los usuarios aprenden a usar.

Acceso Wi-Fi protegido II (WPA2)—Protocolo de seguridad inalámbrica que soporta los estándares de cifrado 802.11i para proporcionar mayor seguridad. Este protocolo utiliza el Estándar de Encriptación Avanzada (AES) y el protocolo de integridad de clave temporal (TKIP) para un cifrado fuerte.

Acción de recuperación—Ejecución de una respuesta o de una tarea según un procedimiento escrito.

Aceptación del riesgo—Si el riesgo está dentro del margen de tolerancia al riesgo de la empresa o si el costo de mitigar el riesgo es mayor que la pérdida potencial, la empresa puede asumir el riesgo y asimilar las pérdidas.

Activo intangible—Un activo que no es de naturaleza física. Ejemplos incluyen: propiedad intelectual (patentes, marcas, derechos de autor, procesos), la buena voluntad y el reconocimiento de marca.

Activos—Bien de valor tangible o intangible que vale la pena proteger, incluyendo a las personas, la información, la infraestructura, las finanzas y la reputación.

Activos tangibles—Cualquier activo que tenga forma física.

Acuerdo de nivel de servicio (SLA)—Acuerdo, preferiblemente documentado, entre un proveedor de servicios y el (los) cliente(s) / usuario(s) que define objetivos mínimos de rendimiento para un servicio y cómo será medido.

Acuerdo recíproco—Acuerdo de procesamiento de emergencia entre dos o más empresas con aplicaciones y equipos similares. Por lo general, los participantes de un acuerdo recíproco prometen proporcionar tiempo de procesamiento entre sí cuando se presenta una emergencia.

Adversario—Agente de la amenaza.

Adware—Paquete de software que automáticamente reproduce, muestra o descarga material publicitario en un ordenador después de que el software esté instalado en él o mientras se esté utilizando la aplicación. En la mayoría de los casos, ésto se hace sin que el usuario haya sido notificado o sin su consentimiento. El término adware también puede referirse al software que muestra publicidad, ya sea con o sin el consentimiento del usuario; estos programas muestran anuncios como una alternativa a las tarifas por registro de shareware. Éstos se clasifican como adware en el sentido de publicidad soportada por software, pero no como spyware. De esta manera, el Adware no funciona subrepticiamente o induciendo a error al usuario, y proporciona al usuario un servicio específico.

Agente de amenaza—Métodos y cosas usadas para explotar una vulnerabilidad. Algunos ejemplos son la determinación, la capacidad, la motivación y los recursos.

Algoritmo de cifrado—Función o cálculo basado en las matemáticas que cifra / descifra información.

Algoritmo de resumen del mensaje—Los algoritmos de resumen de mensaje son SHA1, MD2, MD4 y MD5. Estos algoritmos son funciones unidireccionales a diferencia de los algoritmos de cifrado de claves públicas y privadas. Todos los algoritmos de resumen toman un mensaje de longitud arbitraria y producen un resumen de mensaje de 128 bits.

Alojamiento web—Negocio que consiste en proporcionar el equipo y los servicios necesarios para albergar y mantener archivos para uno o más sitios web y proporcionar conexiones rápidas a Internet para esos sitios. La mayoría de los alojamientos web son “compartidos”, lo que significa que los sitios web de varias compañías están en el mismo servidor para compartir / reducir los costos.

Amenaza—Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de una manera que pueda dañarlo. Causa potencial de un incidente no deseado (ISO/IEC 13335).

Amenaza persistente avanzada APT—Un adversario que posee un nivel de experiencia avanzado y una cantidad significativa de recursos, que le permiten crear oportunidades para lograr sus objetivos usando múltiples vectores de ataque (NIST SP800-61).

La APT:

1. Persigue sus objetivos reiteradamente a lo largo de un período prolongado de tiempo
2. Se adapta a los esfuerzos de los defensores para resistirlos
3. Está decidido a mantener el nivel necesario de interacción para ejecutar sus objetivos

Análisis de amenazas—Evaluación del tipo, alcance y naturaleza de los eventos o acciones que pueden resultar en consecuencias adversas; identificación de las amenazas que existen contra los activos de la empresa. El análisis de amenazas suele definir el nivel de amenaza y la probabilidad de que ésta se materialice.

Análisis de causa raíz—Proceso de diagnóstico para establecer los orígenes de los eventos, que pueden ser utilizados para aprender de las consecuencias, típicamente de errores y problemas.

Análisis de criticidad—Análisis para evaluar los recursos o funciones del negocio para identificar su importancia para la empresa, y el impacto si una función no se puede completar o un recurso no está disponible.

Análisis de impacto—Estudio para priorizar la criticidad de los recursos de información para la empresa basado en los costos (o consecuencias) de eventos adversos. En un análisis del impacto se identifican amenazas a los activos y se determinan pérdidas de negocio potenciales para diferentes períodos de tiempo. Esta evaluación se utiliza para justificar el grado de protección que se requiere y los tiempos de recuperación. Este análisis es la base para establecer la estrategia de recuperación.

Análisis de tráfico de la red—Identifica patrones en las comunicaciones de red. El análisis de tráfico no necesita tener el contenido real de la comunicación, pero analiza dónde se está llevando a cabo el tráfico, cuándo y por cuánto tiempo ocurren las comunicaciones y el tamaño de la información transferida.

Análisis de vulnerabilidades—Proceso de identificación y clasificación de vulnerabilidades.

Análisis del impacto en el negocio (BIA)—Evaluación de la criticidad y sensibilidad de los activos de información. Ejercicio que determina el impacto de perder el apoyo de cualquier recurso para una empresa, establece el escalado de esa pérdida a lo largo del tiempo, identifica los recursos mínimos necesarios para la recuperación , y se prioriza la recuperación de los procesos y al sistema de soporte. Este proceso también incluye hacer frente a la pérdida de ingresos, gastos inesperados, problemas legales (cumplimiento normativo o contractual), procesos interdependientes y la pérdida de la reputación pública o la confianza pública.

Análisis forense—Proceso de recolección, evaluación, clasificación y documentación de evidencia digital para ayudar en la identificación de un delincuente y el método de compromiso.

Analógico—Una señal de transmisión que varía continuamente en amplitud y tiempo y se genera en forma de ondas. Las señales analógicas se utilizan en telecomunicaciones.

Ancho de banda—Rango entre las frecuencias transmisibles más altas y más bajas. Equivale a la capacidad de transmisión de una línea de electrónica y se expresa en bytes por segundo o hercios (ciclos por segundo).

Anti-malware—Una tecnología ampliamente utilizada para prevenir, detectar y eliminar muchas categorías de malware, incluyendo virus, gusanos, troyanos, keyloggers, plug-ins de explorador maliciosos, adware y spyware.

Aprovisionamiento de usuarios—Proceso para crear, modificar, desactivar y eliminar cuentas de usuario y sus perfiles a través de la infraestructura de TI y aplicaciones de negocio.

Archivos de firma de virus—Archivo de patrones de virus que se comparan con los archivos existentes para determinar si están infectadas con un virus o un gusano.

Arquitectura—Descripción del diseño subyacente fundamental de los componentes del sistema de negocio, o de un elemento del sistema de negocio (por ejemplo, la tecnología), las relaciones entre ellos, y la manera en la que soportan los objetivos de la empresa.

Arquitectura de ciber seguridad—Describe la estructura, componentes y topología (conexiones y la disposición en plano) de los controles de seguridad dentro de la infraestructura de TI de una empresa. La arquitectura de seguridad muestra cómo la defensa en profundidad se implementa, cómo se vinculan las capas de control y es esencial para el diseño e implementación de los controles de seguridad en cualquier entorno complejo.

Ataque de “hombre en el medio”—Estrategia de ataque en la que el atacante intercepta el flujo de comunicación entre dos partes del sistema víctima y luego reemplaza el tráfico entre los dos componentes con el propio, asumiendo con el tiempo el control de la comunicación.

Ataque de denegación de servicio (DoS)—Asalto a un servicio desde un único origen que lo desborda con un número tan alto de solicitudes que supera sus capacidades, con el resultado de una parada total del servicio o una operación a una velocidad significativamente reducida.

Ataque de fuerza bruta—Ataque mediante el cual se intentan todas las combinaciones posibles de contraseñas o claves de cifrado hasta dar con la correcta.

Ataque de paquetes fragmentados en miniatura (Miniature fragment attack)—Mediante este método, un atacante fragmenta el paquete IP en unos más pequeños y los envía a través del firewall, con la esperanza de que sólo la primera secuencia de paquetes fragmentados será examinada, permitiendo al resto pasar sin revisión.

Ataque—Ocurrencia real de un evento adverso.

Ataques ROP (Ataques orientados al retorno)—Técnica de explotación en la que el atacante utiliza el control de la pila de llamadas para ejecutar de forma indirecta instrucciones máquina seleccionadas, inmediatamente antes de la instrucción de retorno en subrutinas dentro del mismo código de programa existente.

Atenuación—Reducción de la intensidad de la señal durante la transmisión.

Autenticación—Acto de verificar la identidad de un usuario y la elegibilidad del usuario para acceder a la información computarizada. La autenticación está diseñada para proteger contra actividades de inicio de sesión fraudulentas. También puede hacer referencia a la verificación de la exactitud de un dato.

Autenticación basada en un único factor (SFA)—Proceso de autenticación que requiere sólo el ID de usuario y una contraseña para permitir el acceso.

Autenticación de dos factores—Uso de dos mecanismos independientes para la autenticación (por ejemplo, una tarjeta inteligente y una contraseña), normalmente la combinación de algo que se sabe, que es o que se tiene.

Autenticación multifactorial / de múltiples factores—Combinación de uno o más métodos de autenticación, como un dispositivo token o una contraseña (o número de identificación personal [PIN] o dispositivo token y biométrico).

Autenticidad—Autoría indiscutible.

Autoridad de asignación de números de Internet (IANA)—Responsable de la coordinación global de la raíz del DNS, direccionamiento IP y otros recursos de protocolo de Internet.

Autoridad de certificación (CA)—Tercera parte de confianza que da servicio a infraestructuras o empresas de autenticación y entidades registradoras y les emite certificados.

Autoridad de registro (RA)—Institución individual que valida la prueba de identidad y propiedad de un par de claves de una entidad.

B

Base de datos—Colección almacenada de los datos relacionados necesarios para las empresas y los individuos para satisfacer sus requerimientos de procesamiento y recuperación de la información.

Bastión—Sistema fuertemente fortificado contra ataques.

Biometría—Técnica de seguridad que verifica la identidad de un individuo mediante el análisis de un atributo físico único, como una huella de la mano.

Bitácora (Log)—Para registrar los detalles de la información o eventos en un sistema de registro organizado, por lo general secuenciado en el orden en que ocurrieron.

Bloqueador de escritura—Dispositivo que permite la adquisición de información en una unidad sin crear la posibilidad de dañar accidentalmente la unidad.

Botnet (Red de computadoras infectadas con código malicioso)—Término derivado de “robot network” (red de robots); es una red numerosa, automatizada y distribuida de ordenadores previamente comprometidos que pueden ser controlados simultáneamente para lanzar ataques a gran escala, tales como un ataque de denegación de servicios a víctimas seleccionadas.

Bridges—Dispositivos de la capa de enlace de datos desarrollados a principios de los años 1980 para conectar redes de área local (LANs) o crear dos segmentos de red LAN o red de área amplia (WAN) separados de un único segmento para reducir los dominios de colisión. Los bridges actúan como dispositivos de almacenamiento y envío en el proceso de envío de tramas hacia su destino. Ello se logra mediante el análisis de la cabecera MAC de un paquete de datos, que representa la dirección de hardware de un NIC.

Broadcast (difusión)—Método usado para distribuir la información a varios destinatarios de forma simultánea.

Búsqueda—Proceso por el cual los datos que atraviesan una red son capturados o monitoreados.

C

Caballos de Troya / Troyanos—Código malicioso o dañino intencionalmente oculto dentro de un programa de ordenador autorizado. A diferencia de los virus, no se replican, pero pueden ser igualmente destructivos para una computadora.

Cadena de custodia—Principio legal con respecto a la validez e integridad de la evidencia. Requiere responsabilidad por cualquier cosa que se utilice como evidencia en un proceso legal, con el fin de asegurar que puede rendir cuentas desde el momento en que se obtuvo hasta que se presentó en el tribunal. Incluye documentación sobre quién tuvo acceso a la evidencia y cuándo, así como la capacidad de identificar la evidencia como el elemento exacto que se recuperó o probó. La falta de control sobre la evidencia puede conducir a su desacreditación. La cadena de custodia depende de la capacidad para verificar que la evidencia no pudo haber sido alterada. Esto se logra sellando la evidencia para que no se pueda cambiar, y proporcionando un registro documental de la custodia para probar que la evidencia estuvo, en todo momento, bajo estricto control y no sujeta a manipulación.

Capa de aplicación—En el modelo de comunicaciones de Interconexión de Sistemas Abiertos (OSI), la capa de aplicación proporciona servicios para un programa de aplicación para asegurar que se puede establecer una comunicación efectiva con otro programa de aplicación en una red. La capa de aplicación no es la aplicación que está haciendo la comunicación; una capa de servicio es la que proporciona estos servicios.

Capa de conector seguro (SSL)—Protocolo que se utiliza para transmitir documentos privados a través de Internet. El protocolo SSL utiliza una clave privada para cifrar los datos que se van a transferir a través de la conexión SSL.

Cebó de atracción (Honeypot)—Servidor configurado especialmente, también conocido como un servidor señuelo, diseñado para atraer y controlar los intrusos de tal manera que sus acciones no afecten a los sistemas de producción. También conocido como “Servidor señuelo.”

Certificado digital—Pieza de información, una forma digitalizada de firma, que proporciona la autenticidad del remitente, la integridad del mensaje y el no repudio. Se genera una firma digital mediante la clave privada del remitente o la aplicación de una función de hash unidireccional.

Checksum—Valor matemático que se asigna a un archivo y se utiliza para “probar” el archivo en una fecha posterior para verificar que los datos contenidos en el archivo no se han modificado maliciosamente. Un checksum criptográfico se crea ejecutando una serie complicada de operaciones matemáticas (conocida como algoritmo criptográfico) que transforma los datos del archivo en una cadena fija de dígitos llamada valor hash, que se usa a continuación como checksum. Si no conoce cuál es el algoritmo criptográfico que se usó para crear el valor hash, es altamente improbable que una persona no autorizada pueda cambiar los datos sin cambiar inadvertidamente el correspondiente checksum. Los checksum criptográficos se usan en la transmisión de datos y almacenamiento de datos. Los checksum criptográficos también se conocen como códigos de autenticación de mensajes, valores de verificación de integridad, códigos de detección de modificación o códigos de integridad de mensajes.

Ciber espionaje—Actividades realizadas en nombre de la seguridad, los negocios, la política o la tecnología para encontrar información que debería permanecer secreta. No es inherentemente militar.

Ciber guerra—Actividades apoyadas por organizaciones militares con el propósito de amenazar la supervivencia y el bienestar de una sociedad/entidad extranjera.

Ciber policía—Investigador de actividades relacionadas con la delincuencia informática.

Ciber seguridad—Protección de activos de información abordando las amenazas a la información procesada, almacenada y transportada por los sistemas de la información interconectados.

Ciclo de Vida del Desarrollo de Sistemas (SDLC)—Fases desplegadas en el desarrollo o la adquisición de un sistema de software. SDLC es un enfoque utilizado para planificar, diseñar, desarrollar, probar e implementar un sistema de aplicación o una modificación importante de un sistema de aplicación. Fases típicas de SDLC incluyen el estudio de viabilidad, estudio de requerimientos, definición de requerimientos, diseño detallado, programación, pruebas, instalación y revisión posterior a la implementación, pero no las actividades de entrega de servicios o beneficios.

Cifrado de bloques—Algoritmo público que opera en texto claro en bloques (cadenas o grupos) de bits.

Cifrado de clave pública—Sistema criptográfico que utiliza dos claves: una clave pública, que es conocida por todos, y una clave privada o secreta (la segunda), que sólo es conocida por el destinatario del mensaje. Ver también clave asimétrica.

Cifrado de clave simétrica—Sistema en el que una clave diferente (o conjunto de claves) es utilizada por cada pareja de personas o entes, para asegurar que nadie más puede leer sus mensajes. La misma clave se utiliza para el cifrado y descifrado. Ver también sistema de cifrado de clave privada.

Cifrado (Cipher)—Algoritmo para realizar el cifrado.

Cifrado (Encryption)—Proceso de tomar un mensaje no cifrado (texto plano), aplicarle una función matemática (algoritmo de cifrado con una clave) y producir un mensaje cifrado (texto cifrado).

Clasificación de datos—Asignación de un nivel de sensibilidad a los datos (o información) que resulta en la especificación de controles para cada nivel de clasificación. Los niveles de sensibilidad de datos se asignan de acuerdo a categorías predefinidas a medida que los datos se crean, modifican, mejoran, almacenan o transmiten. El nivel de clasificación es un indicador del valor o importancia de los datos para la empresa.

Clave asimétrica (clave pública)—Técnica de cifrado en la que diferentes claves criptográficas se utilizan para cifrar y descifrar un mensaje. Ver Cifrado de clave pública.

Clave de cifrado—Pieza de información, en forma digitalizada, utilizada por un algoritmo de cifrado para convertir texto plano en texto cifrado.

Clave de descifrado—Pieza digital de información utilizada para recuperar texto plano descifrando el correspondiente texto cifrado.

Código de autenticación de mensajes—Checksum estándar del Instituto Nacional Estadounidense de Estándares (ANSI) que se genera utilizando el Estándar de Encriptación de Datos (DES).

Colisión—Situación que se produce cuando dos o más demandas se realizan simultáneamente en un equipo que puede manejar sólo una en un determinado instante (Estándar Federal 1037C).

Comercio electrónico—Procesos a través de los cuales las empresas hacen negocios de manera electrónica con sus clientes, proveedores y otros socios comerciales externos, usando Internet como tecnología habilitadora. El comercio electrónico abarca tanto el modelo de comercio electrónico de empresa a empresa (B2B) como el de empresa a consumidor (B2C), pero no incluye los métodos de comercio electrónico que no están en Internet basados en redes privadas, tales como el intercambio electrónico de datos (EDI) y la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT).

Compartimentación—Proceso para la protección de los activos de muy alto valor, o en entornos donde la confianza es un problema. El acceso a un activo requiere de dos o más procesos, controles o individuos.

Computación en la nube—Acceso a red cómodo y bajo demanda a un conjunto compartido de recursos que pueden ser rápidamente aprovisionados y entregados con un esfuerzo mínimo de gestión o de interacción con el proveedor de servicios.

Comunicaciones entrantes en la red (Ingress)—Comunicaciones de la red que entran.

Comunicaciones salientes de la red (Egress)—Comunicaciones de la red que salen.

Concentrador—Punto de conexión común para los dispositivos en una red, los concentradores se utilizan para conectar segmentos de una red de área local (LAN). Un concentrador contiene múltiples puertos. Cuando un paquete llega a un puerto, se copia a los otros puertos para que todos los segmentos de la LAN puedan ver todos los paquetes.

Concentrador de Red privada virtual (VPN)—Sistema utilizado para establecer túneles VPN y manejar un gran número de conexiones simultáneas. Este sistema proporciona servicios de autenticación, autorización servicios de contabilización.

Confidencialidad—Preservar restricciones autorizadas en el acceso y la divulgación, incluyendo medios para la protección de la privacidad y la propiedad de la información.

Comutación de paquetes—Proceso de transmisión de mensajes en piezas convenientes que se pueden volver a ensamblar en el destino.

Consumerización—Nuevo modelo en el que las tecnologías emergentes son adoptadas en primer lugar por el mercado de consumo y se extienden más adelante a la empresa.

Contención—Medidas adoptadas para limitar la exposición después de haber identificado y confirmado un incidente.

Contramedidas—Cualquier proceso que reduce directamente una amenaza o vulnerabilidad.

Contraseña—Cadena de caracteres, generalmente protegida mediante encriptación, que autentica a un usuario de una computadora en un sistema informático.

Control—Medio mediante el cual se gestiona el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales , que pueden ser de carácter administrativo, técnico, de gestión, o jurídico. También se utiliza como sinónimo de salvaguarda o de contramedida.

Control de acceso discrecional (DAC)—Medio de restringir el acceso a objetos en función de la identidad de los sujetos y / o grupos a los que pertenecen. Los controles son discretionarios en el sentido de que un individuo con un cierto permiso de acceso es capaz de pasar ese permiso (quizás indirectamente) a cualquier otro individuo.

Control de acceso obligatorio (MAC)—Medio para restringir el acceso a los datos basados en distintos grados de requisitos de seguridad para la información contenida en los objetos y las correspondientes credenciales de seguridad de los usuarios o programas que actúen en su nombre.

Controles de acceso lógico—Políticas, procedimientos, estructura organizativa y controles de acceso electrónicos diseñados para restringir el acceso al software y a los archivos de datos.

Cortafuego humano—Persona preparada para actuar como una defensa de capa de red a través de la educación y la sensibilización

Cortafuegos (Firewall)—Sistema o combinación de sistemas que establece un límite entre dos o más redes, formando típicamente una barrera entre un entorno seguro y un entorno abierto como Internet.

Costo total de propiedad (TCO)—Incluye el costo original del equipo computacional más el costo de: software, hardware y actualizaciones de software, mantenimiento, soporte técnico, capacitación y algunas actividades realizadas por los usuarios.

Criptografía—Arte de diseñar, analizar y atacar esquemas criptográficos.

Criptografía de curva elíptica (ECC)—Algoritmo que combina la geometría plana con el álgebra para lograr una autenticación más fuerte con claves más pequeñas en comparación con los métodos tradicionales, como RSA, que utilizan principalmente la factorización algebraica Las claves más pequeñas son más adecuadas para dispositivos móviles.

Criptosistema—Pareja de algoritmos que utilizan una clave y convierten el texto plano en texto cifrado y viceversa.

Criticidad—La importancia de un activo o una función particular para la empresa, y el impacto si ese activo o función no está disponible.

Cronogramas—Gráficos de tiempo donde los acontecimientos relacionados con un incidente pueden ser asociados para buscar relaciones en casos complejos. Los cronogramas pueden proporcionar una visualización simplificada para su presentación a la administración y otras audiencias no técnicas.

Cross-site scripting (XSS)—Tipo de inyección en el cual scripts (secuencias de comandos) maliciosos se inyectan en los sitios web benignos y de confianza. Los ataques de Cross-site scripting (XSS) ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Los defectos que permiten que estos ataques tengan éxito son bastante generalizados y se producen en cualquier lugar de una aplicación web que utiliza la entrada de un usuario dentro de la salida generada sin validar o codificarlo. (OWASP)

Cumplimiento—Adhesión y capacidad de demostrar la adhesión a los requisitos obligatorios definidos por leyes y reglamentos, así como los requisitos voluntarios que resultan de las obligaciones contractuales y las políticas internas.

Custodio de datos—Individuo(s) y departamento(s) responsable(s) del almacenamiento y salvaguarda de datos informatizados.

D

Datos volátiles—Datos que cambian con frecuencia y se pueden perder cuando la alimentación eléctrica del sistema está apagado.

Debido cuidado—Nivel de cuidado esperado por parte de una persona razonable de competencia similar y bajo las condiciones similares.

Defensa en profundidad horizontal—Controls are placed in various places in the path to access an asset.

Defensa en profundidad vertical—Controles colocados en diferentes capas del sistema - hardware, sistema operativo, las aplicaciones, bases de datos o nivel del usuario.

Defensa en profundidad—Práctica consistente en establecer capas de defensa para proporcionar mayor protección. La defensa en profundidad incrementa la seguridad al aumentar el esfuerzo que se necesita en un ataque. Esta estrategia coloca múltiples barreras entre un atacante y los recursos de información y computación de una empresa.

Derechos de acceso—Los permisos o privilegios concedidos a usuarios, programas o estaciones de trabajo para crear, cambiar, eliminar o ver los datos y archivos dentro de un sistema, tal y como están definidas por las reglas establecidas por los propietarios de los datos y la política de seguridad de la información.

Desastre—Evento desastroso repentino, imprevisto que provoca un gran daño o pérdida. Cualquier evento que crea una incapacidad a una parte de una organización para proporcionar funciones críticas del negocio durante un cierto período de tiempo predeterminado. Términos similares son interrupción del negocio, corte y catástrofe.

El período en el que la gestión de la empresa decide desviar la forma normal de producción y lanza su plan de recuperación de desastres (DRP). Por lo general indica el comienzo de un movimiento desde una ubicación principal a una ubicación alternativa.

Desbordamiento de búfer—Ocurre cuando un programa o proceso intenta almacenar en una memoria intermedia (área de almacenamiento temporal de datos) más datos de los que se tenía la intención de contener. Puesto que los buffers son creados para contener una cantidad limitada de datos, la información adicional que tiene que ir a alguna parte—puede desbordar hacia buffers adyacentes, corrompiendo o sobrescribiendo los datos válidos contenidos. Aunque puede ocurrir accidentalmente por error de programación, el desbordamiento de búfer es un tipo cada vez más común de ataque a la seguridad en la integridad de los datos. En los ataques de desbordamiento de búfer, los datos adicionales pueden contener códigos diseñados para activar acciones específicas, resultando en el envío de nuevas instrucciones a la computadora atacada que podrían, por ejemplo, dañar los archivos del usuario, cambiar los datos, o divulgar información confidencial. Se dice que los ataques de desbordamiento de búfer han surgido porque el lenguaje de programación C proporcionó el marco, y las malas prácticas de programación proporcionaron la vulnerabilidad.

Descentralización—Proceso de distribución del procesamiento informático a diferentes lugares dentro de una empresa.

Descifrado—Técnica utilizada para recuperar el texto plano original del texto cifrado de modo que sea inteligible para el lector. El descifrado es un proceso inverso al cifrado.

Detección de intrusiones—Proceso de seguimiento de los eventos que ocurren en un sistema informático o red para detectar signos de acceso no autorizado o un ataque.

Diligencia debida—Realización de aquellas acciones que son consideradas generalmente como prudentes, responsables y necesarias para llevar a cabo una investigación, revisión y/o análisis exhaustivo y objetivo.

Dirección IP—Número binario único utilizado para identificar los dispositivos en una red TCP/IP.

Direcciones de control de acceso al medio (MAC)—Identificador único asignado a las interfaces de red para las comunicaciones en el segmento físico de red.

Disponibilidad—Garantizar el acceso y uso de la información de una forma oportuna y fiable.

Dispositivo móvil—Dispositivo informático pequeño, de mano, que tiene típicamente una pantalla con entrada táctil y / o un mini teclado, y un peso menor a dos libras.

Documentos de cumplimiento—Políticas, estándares y procedimientos que documentan las acciones que se requieren o prohíben. Las violaciones pueden estar sujetas a acciones disciplinarias.

E

Encabezado de autenticación IP (Authentication header – AH)—Protocolo utilizado para proporcionar integridad y autenticación del origen de los datos sin conexión para datagramas IP (en lo sucesivo denominado simplemente “integridad”) y para proporcionar protección contra las repeticiones. (RFC 4302). AH asegura la integridad de los datos con un checksum que un código de autenticación de mensaje, tal como MD5, genera. Para asegurar la autenticación del origen de los datos, AH incluye una clave secreta compartida en el algoritmo que se utiliza para la autenticación. Para garantizar la protección frente a la repetición, AH utiliza un campo de número de secuencia dentro de la cabecera de autenticación IP.

Encabezado MAC—Representa la dirección de hardware de un controlador de interfaz de red (NIC) en el interior de un paquete de datos.

Encapsulado de carga útil de seguridad (ESP)—Protocolo, que está diseñado para proporcionar una combinación de servicios de seguridad en IPv4 e IPv6. ESP se puede utilizar para proporcionar confidencialidad, autenticación del origen de datos, integridad sin conexión, un servicio anti reproducción (una forma de integridad de secuencia parcial), y (limitada) confidencialidad del flujo de tráfico (RFC 4303). La cabecera ESP se inserta después de la cabecera IP y antes de la cabecera del protocolo de la siguiente capa (medio de transporte) o antes de una cabecera IP encapsulada (modo túnel).

Enmascaramiento—Técnica informática para bloquear la visualización de la información sensible, como contraseñas, en un ordenador o un reporte.

Enrutador (router)—Dispositivo de red que puede enviar (enrutar) paquetes de datos de una Red de área local (LAN) o Red de área amplia (WAN) a otra, basado en direccionar en la capa de red (capa 3) en el modelo de interconexión de sistemas abiertos (OSI). Las redes conectadas por routers pueden usar protocolos de red diferentes o similares. Los enruteadores generalmente son capaces de filtrar paquetes en base a parámetros tales como direcciones de origen, direcciones de destino, protocolos y aplicaciones de red (puertos).

Enumeración y Clasificación de Patrón Común de Ataque (CAPEC)—Catálogo de patrones de ataque como “un mecanismo de abstracción para ayudar a describir cómo se ejecuta un ataque contra los sistemas o redes vulnerables”, publicado por la Corporación MITRE.

Equipo de respuesta a emergencias informáticas (CERT)—Grupo de personas integradas en la empresa con líneas claras de cómo reportar y responsabilidades de apoyo para dar soporte en caso de emergencia en los sistemas de información. Este grupo actuará como un control correctivo eficaz, y deberá actuar además como punto de contacto único para todos los incidentes y asuntos relacionados con los sistemas de información.

Erradicación—Cuando se han desplegado medidas de contención después de que ocurra un incidente, la causa raíz del incidente debe ser identificada y eliminada de la red. Los métodos de erradicación incluyen: restauración de copias de seguridad para lograr un estado limpio del sistema, eliminar la causa raíz, mejorar las defensas y realizar análisis de vulnerabilidades para encontrar otros daños potenciales desde la misma causa raíz.

Escaneo de puertos—Acto de descubrimiento en un sistema para identificar los puertos abiertos.

Escaneo de vulnerabilidades—Proceso automatizado para identificar de forma proactiva las debilidades de seguridad en una red o sistema individual.

Escuchas o lectura ilegal de mensajes (Eavesdropping)—Escuchar una comunicación privada sin permiso.

Especificación de enrutamiento en la fuente—Técnica de transmisión en la que el remitente de un paquete puede especificar la ruta que el paquete debe seguir a través de la red.

Estándar de Encriptación Avanzada (AES)—Algoritmo público que soporta claves cuyo tamaño está comprendido entre 128 y 256 bits.

Estándar de encriptación de datos (DES)—Algoritmo para codificar datos binarios. Se trata de un sistema criptográfico de clave secreta publicado por la Agencia Nacional de Normas (NBS), el antecesor del Instituto Nacional de Normas y Tecnología de EE.UU. (NIST). DES y sus variantes han sido sustituidas por el Estándar de Encriptación Avanzada (AES).

Ethernet—Protocolo y esquema de red popular que utiliza una topología de bus y acceso múltiple con escucha de portadora y detección de colisiones (CSMA / CD) para evitar fallos de la red o colisiones cuando dos dispositivos intentan acceder al mismo tiempo a la red.

Evaluación del riesgo—Proceso utilizado para identificar y evaluar los riesgos y sus efectos potenciales. Las evaluaciones de riesgo son utilizadas para identificar aquellos ítems o áreas que presentan la exposición, la vulnerabilidad o el riesgo más alto para la empresa y que deben ser incluidos en el plan de auditoría anual de SI. Las evaluaciones de riesgo también se utilizan para gestionar la entrega del proyecto y el riesgo de beneficios del proyecto.

Evento—Algo que sucede en un lugar y/o tiempo específico.

Evento de amenaza—Cualquier evento durante el cual un elemento / actor de la amenaza actúa contra un activo de una manera que tiene el potencial de causar daño directamente.

Evidencia—Información que aprueba o desaprueba un problema determinado. La información que un auditor recoge en el transcurso de la realización de una auditoría de SI; es relevante si se refiere a los objetivos de la auditoría y tiene una relación lógica con los hallazgos y conclusiones que utiliza para apoyarse.

Evitar los riesgos—Proceso por el cual se evita sistemáticamente el riesgo, lo que constituye una forma de gestión del riesgo.

Exfiltración del sistema de nombres de dominio (DNS)—Tunelización sobre el DNS para obtener acceso a la red. Es un vector de ataque de bajo nivel para la transmisión de datos simple y compleja, lenta pero difícil de detectar.

Exploit de día cero—Vulnerabilidad que se explota antes de que el creador/proveedor del software sea consciente de su existencia.

Exploit—Uso completo de una vulnerabilidad en beneficio de un atacante.

Extensiones multipropósito seguras de correo de internet (S / MIME)—Proporciona servicios criptográficos de seguridad para las aplicaciones de mensajería electrónica: autenticación, integridad de mensajes y no repudio del origen de los mensajes (usando firmas digitales) y la privacidad y seguridad de los datos (usando cifrado) para proporcionar una forma consistente para enviar y recibir datos MIME (RFC 2311).

Externalización—Acuerdo formal con un tercero para realizar actividades de Seguridad de la Información (SI) u otra función de negocios para una empresa.

F

Filtrado de contenido—Controlar el acceso a una red mediante el análisis de los contenidos de los paquetes entrantes y salientes ya sea dejándoles pasar o negándoles la entrada en base a una lista de reglas. Difiere del filtrado de paquetes en el sentido que analiza los datos en el paquete en lugar de los atributos del paquete en sí (por ejemplo, dirección IP de origen / destino, banderas de protocolo de control de transmisión [TCP]).

Filtrado de paquetes—Control de acceso a una red mediante el análisis de los atributos de los paquetes entrantes y salientes, permitiéndoles el paso, o bien negándose, en función de una lista de reglas.

Firma digital—Pieza de información, una forma digitalizada de firma, que proporciona la autenticidad del remitente, la integridad del mensaje y el no repudio. Se genera una firma digital mediante la clave privada del remitente o la aplicación de una función de hash unidireccional.

Fortalecer la seguridad del sistema—Proceso consistente en eliminar la mayor cantidad posible de riesgos de seguridad mediante la eliminación de todos los programas de software que no sean esenciales, protocolos, servicios y utilidades del sistema.

Fuerza bruta—Clase de algoritmos que intentan repetidamente todas las combinaciones posibles hasta dar con una solución.

Fuga de datos—Desviar o filtrar información transmitiendo archivos del ordenador o robando informes y cintas del ordenador.

Función hash—Algoritmo que asigna o traduce un conjunto de bits a otro (generalmente más pequeño), de modo que un mensaje produce el mismo resultado cada vez que el algoritmo se ejecuta utilizando el mismo mensaje como entrada. Desde el punto de vista computacional es inviable que un mensaje sea derivado o reconstituido desde el resultado producido por el algoritmo o que se encuentren dos mensajes diferentes que produzcan el mismo resultado hash utilizando el mismo algoritmo.

Función Hashing—Usar una función hash (algoritmo) para crear el valor del hash o suma de comprobación que valida la integridad del mensaje.

G

Gateway (Pasarela)—Dispositivo (router, firewall) en una red que sirve como entrada a otra red.

Generación de imágenes (imaging)—Proceso que permite obtener una copia bit a bit de los datos para evitar el daño de los datos o información originales cuando se pueden realizar múltiples análisis. El proceso de generación de imágenes se hace para obtener datos residuales, como los archivos borrados, fragmentos de archivos borrados y otra información presente, desde el disco para su análisis. Esto es posible porque la generación de imágenes duplica la superficie del disco, sector por sector.

Gerente de seguridad (CSO)—Persona que por lo general es responsable de todos los asuntos de seguridad, tanto físicos como digitales, en una empresa.

Gerente de seguridad de la información (CISO)—Persona encargada de la seguridad de la información dentro de la empresa.

Gestión de la configuración—Control de cambios a un conjunto de elementos de configuración a lo largo del ciclo de vida del sistema.

Gestión de parches—Área de la administración de sistemas que contempla la adquisición, las pruebas y la instalación de múltiples parches (cambios de código) en un sistema informático gestionado, con el objetivo de mantener el software actualizado y a menudo para hacer frente a riesgos de seguridad. La gestión de parches incluye las siguientes tareas: mantener el conocimiento actualizado de los parches disponibles; decidir qué parches son apropiadas para cada tipo de sistemas; garantizar que los parches están instalados correctamente; prueba de sistemas después de la instalación; y documentar todos los procedimientos asociados, tales como configuraciones específicas requeridas. Hay una serie de productos disponibles para automatizar las tareas de gestión de parches. Los parches a veces son ineficaces y a veces pueden causar más problemas que los que corren. Los expertos en gestión de parches sugieren que los administradores de sistemas tomen medidas sencillas para evitar problemas, tales como la ejecución de copias de seguridad y pruebas de parches en los sistemas no críticos antes de la instalación. La gestión de parches puede considerarse como parte de la gestión de cambios.

Gestión de riesgos—Actividades coordinadas para dirigir y controlar una empresa con respecto al riesgo. En el estándar internacional, el término “control” se utiliza como sinónimo de “medida”. (Guía ISO/IEC 73:2002)

Uno de los objetivos del gobierno. Implica reconocer los riesgos; evaluar el impacto y la probabilidad de ocurrencia del riesgo; y el desarrollo de estrategias, tales como evitar el riesgo, reducir el efecto negativo de los riesgos y/o transferir el riesgo, para gestionarlo en el contexto del apetito de riesgo de la empresa. (COBIT 5)

Gobierno—Asegura que se evalúen las necesidades, condiciones y opciones de las partes interesadas para determinar objetivos equilibrados y acordados, determinando la dirección a través de la priorización y la toma de decisiones, y monitoreando el desempeño y cumplimiento en relación con la dirección y los objetivos acordados. Las condiciones pueden incluir el costo de capital, de las tasas internacionales de cambio, etc. Las opciones pueden incluir el cambio de fabricación a otros lugares, subcontratar porciones de la empresa a terceros, la selección de una combinación de productos de muchas opciones disponibles, etc.

Gobierno de TI—Responsabilidad de los ejecutivos y el consejo de administración; consiste en el liderazgo, estructuras organizacionales y procesos que aseguran que la TI de la empresa sostiene y extiende las estrategias y objetivos de la empresa.

Gobierno, Gestión de Riesgo y Cumplimiento (GRC)—Término de negocios usado para agrupar las tres disciplinas relacionadas entre sí y que son responsables de la protección de los activos y las operaciones.

Gusano—Ataque programado de red, en el que un programa auto-replicante no se adhiere a otros programas, sino que se extiende de forma independiente de la acción de los usuarios.

H

Hacker—Individuo que intenta obtener acceso no autorizado a un sistema informático.

I

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)—Pronunciado I E cubo; es una organización compuesta por ingenieros, científicos y estudiantes. Más conocida por el desarrollo de normas para la industria de la computación y la electrónica.

IEEE 802.11—Familia de especificaciones desarrolladas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para la tecnología de red de área local inalámbrica (WLAN). 802.11 especifica una interfaz sobre el aire entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos.

Impacto—Magnitud de pérdida resultante de una amenaza que explota una vulnerabilidad.

Incertidumbre—Dificultad de predecir un resultado debido al conocimiento limitado de todos los componentes.

Incidente—Cualquier evento que no es parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción, o una reducción en la calidad de dicho servicio.

Indicador clave de riesgo (KRI)—Subconjunto de indicadores de riesgo que son altamente relevantes y poseen una alta probabilidad de predecir o indicar el riesgo importante. Véase también Indicador de Riesgo.

Informática Forense digital—Proceso de identificar, preservar, analizar y presentar evidencia digital de una manera que es legalmente aceptable en cualquier procedimiento legal

Informática forense—Aplicación del método científico a los medios digitales para establecer información objetiva para la revisión judicial. Este proceso a menudo implica la investigación de los sistemas informáticos para determinar si son o han sido utilizados para actividades ilegales o no autorizadas. Como disciplina, combina elementos legales y ciencias de la computación para recopilar y analizar datos de los sistemas de información (por ejemplo, ordenadores personales, redes, comunicaciones inalámbricas y dispositivos de almacenamiento digital) de una manera que es admisible como prueba en un tribunal de justicia.

Infraestructura como un servicio (IaaS)—Ofrece la capacidad de proveer procesamiento, almacenamiento, redes y otros recursos de computación fundamentales, permitiendo al cliente implementar y ejecutar software arbitrario, que puede incluir sistemas operativos (SO) y aplicaciones.

Infraestructura crítica—Sistemas cuya incapacidad o destrucción tendría un efecto debilitador en la seguridad económica de una empresa, comunidad o nación.

Infraestructura de clave pública (PKI)—Serie de procesos y tecnologías que permiten asociar claves criptográficas con la entidad para la cual se emitieron esas claves.

Ingeniería social—Ataque basado en engañar a los usuarios o administradores en la ubicación objetivo, para que revelen información confidencial o sensible.

Ingestión—Proceso para convertir la información extraída a un formato que puede ser entendido por los investigadores. Ver también Normalización.

Inspección a nivel del estado—Arquitectura de firewall que rastrea cada conexión que atraviesa todas las interfaces del firewall y asegura que sean válidas.

Instalaciones alternativas—Ubicaciones e infraestructuras desde las cuales se ejecutan los procesos de emergencia o de respaldo, cuando las ubicaciones principales no están disponibles o están destruidas; incluye otros edificios, oficinas o centros de procesamiento de datos.

Instituto Nacional de Normas y Tecnología (NIST)—Desarrolla pruebas, métodos de prueba, datos de referencia, implementación de pruebas de concepto, y análisis técnico para fomentar el desarrollo y uso productivo de las tecnologías de la información. NIST es una entidad del gobierno estadounidense que crea normas obligatorias que son seguidas por las agencias federales y aquéllos que hacen negocios con ellas.

Integridad—Protección contra la modificación o destrucción de información inapropiada, incluye garantizar el no repudio y la autenticidad de la información.

Intercambio inter-redes de paquetes/Intercambio secuenciado de paquetes (IPX/SPX)—IPX es la capa 3, protocolo de red, del modelo de interconexión de sistemas abiertos (OSI); SPX es un protocolo de transporte de capa. La capa SPX está encima de la capa IPX y proporciona servicios orientados a la conexión entre dos nodos en la red.

Interrogación—Se utiliza para obtener indicadores o relaciones anteriores, incluyendo números de teléfono, direcciones IP y los nombres de las personas, a partir de datos extraídos.

Intruso—Individuo o grupo que obtiene acceso a la red y a sus recursos sin permiso.

Investigación—Recogida y análisis de las evidencias con el objetivo de identificar al autor de un ataque o el uso o acceso no autorizado.

Inyección—Término general para tipos de ataque que consisten en inyectar código que es interpretado / ejecutado por la aplicación a continuación (OWASP).

Inyección de SQL—Se trata del resultado provocado por la falla de una aplicación para validar adecuadamente la entrada de datos. Cuando los procesos de entrada de datos especialmente diseñadas con la sintaxis de SQL se utilizan sin la validación adecuada como parte de las consultas SQL, es posible obtener información de la base de datos de una manera que no ha sido prevista durante la fase de diseño de la aplicación. (MITRE)

K

Keylogger—Software utilizado para registrar todas las pulsaciones de teclado en un ordenador.

L

Latencia—Tiempo que lleva un retraso en un sistema y una red para responder. Más específicamente, la latencia del sistema es el tiempo que un sistema toma para recuperar datos. La latencia de red es el tiempo que tarda un paquete para viajar desde el origen hasta el destino final.

Límite—Controles lógicos y físicos para definir un perímetro entre la organización y el mundo exterior.

Lineamiento—Descripción de una manera particular de lograr algo que es menos prescriptiva que un procedimiento.

Lista de control de acceso (ACL)—Tabla computarizada interna de las reglas de acceso relacionadas con los niveles de acceso al ordenador permitidos para usuarios y terminales de ordenador. También se conoce como tablas de control de acceso.

Lista de revocación de certificados (CRL)—Instrumento para controlar la validez en el tiempo de los certificados para los cuales la autoridad de certificación (CA) tiene responsabilidad. La CRL detalla los certificados digitales que ya no son válidos. El intervalo de tiempo entre dos actualizaciones es muy crítico y es también un riesgo en la verificación de los certificados digitales.

Localizador uniforme de recursos (URL)—Cadena de caracteres que forman una dirección web.

Longitud de la clave—Tamaño de la clave de cifrado medido en bits.

M

Mainframe—Equipo de alta velocidad y grandes dimensiones, da soporte a numerosas estaciones de trabajo o periféricos.

Mecanismo de ataque—Un método utilizado para entregar el exploit. A menos que el atacante esté llevando a cabo personalmente el ataque, el mecanismo de ataque puede implicar un exploit, que entrega el payload al objetivo.

Medición de los resultados—Muestra las consecuencias de las acciones tomadas previamente; a menudo referido como un indicador de retraso. La medición de resultados se enfoca frecuentemente en los resultados al final de un período de tiempo y en describir el desempeño histórico. También se le conoce como un indicador clave de objetivo (KGI) y se utiliza para indicar si se han cumplido los objetivos. Se puede medir sólo después del hecho y, por lo tanto, se le llama “indicador de retraso.”

Medios extraíbles—Cualquier tipo de dispositivo de almacenamiento que puede ser extraído del sistema mientras está en uso.

Métricas de seguridad—Estándar de medición utilizado en la gestión de actividades relacionadas con la seguridad.

Mitigación del riesgo—Gestión de riesgos a través de la utilización de contramedidas y controles.

Modelo de interconexión de sistemas abiertos (OSI)—Modelo para el diseño de una red. El modelo de interconexión de sistemas abiertos (OSI) define grupos de funcionalidades requeridos para interconectar computadoras en capas. Cada capa implementa un protocolo estándar para implementar su funcionalidad. Hay siete capas en el modelo OSI.

Modo de túnel—Se utiliza el modo de túnel para proteger el tráfico entre diferentes redes cuando el tráfico tiene que viajar a través de redes intermedias o no confiables. El modo de túnel encapsula todo el paquete IP con un encabezado AH o ESP y un encabezado IP adicional.

Modo de usuario—Se utiliza para la ejecución de actividades normales del sistema.

Modo Kernel—Se utiliza para la ejecución de instrucciones privilegiadas para el funcionamiento interno del sistema. En el modo kernel, no hay protecciones de errores o actividades maliciosas y todas las partes del sistema y la memoria son accesibles.

Monitorización no intrusiva—Uso de sondas o trazas transportadas para conformar la información, monitorizar el tráfico e identificar vulnerabilidades.

N

No repudio—Aseguramiento de que un ente no puede negar a posteriori los datos que originó; provisión de pruebas de la integridad y origen de los datos que puede ser verificado por terceros. Una firma digital puede proporcionar el no repudio.

Normalización—Eliminación de los datos redundantes.

Número de identificación personal (PIN)—Tipo de contraseña (por ejemplo, un número secreto asignado a una persona) que, junto con algunos medios de identificación de la persona, sirve para verificar la autenticidad del individuo. Los PINs han sido adoptados por las instituciones financieras como el principal medio de verificación de los clientes en un sistema de transferencia electrónica de fondos (EFT).

Número primo—Número natural mayor que 1 que sólo puede ser dividido por 1 y por sí mismo.

0

Objetivo de punto de recuperación (RPO)—Determinado en base a la pérdida aceptable de datos en caso de una interrupción de las operaciones. Indica el punto más temprano en el tiempo que es aceptable para recuperar los datos. El RPO cuantifica eficazmente la cantidad permisible de pérdida de datos en caso de interrupción.

Objetivo de tiempo de recuperación (RTO)—Cantidad de tiempo permitido para la recuperación de una función de negocio o un recurso después tras la materialización de un desastre.

Objetivo—Persona o activo seleccionado como el objetivo de un ataque.

Objetivos de entrega del servicio (SDO)—Directamente relacionado con las necesidades del negocio, SDOes el nivel de servicios que se debe alcanzar durante el modo de proceso alternativo hasta que se restablezca la situación normal.

Ofuscación—Codificación de mensaje para que no pueda ser leído—Acto deliberado de crear código fuente o código máquina que es difícil de entender para los seres humanos.

Organización internacional para la estandarización (ISO)—El mayor desarrollador del mundo de Estándares Internacionales voluntarios.

P

Paquete—Unidad de datos que es enrutada desde la fuente al destino en una red de commutación de paquetes. Un paquete contiene información de enrutamiento y de datos. El Protocolo de Control de Transmisión / Protocolo de Internet (TCP / IP) es un tipo de red de commutación de paquetes.

Parche—Reparaciones de los errores y vulnerabilidades de programación de software.

Payload—Parte que contiene los datos fundamentales en una transmisión. En el software malintencionado, hace referencia a la sección que contiene los datos / código dañino.

Perímetro de seguridad—Límite que define el área de interés de la seguridad y la cobertura de la política de seguridad.

Phishing—Tipo de ataque de correo electrónico (e-mail) que intenta convencer a un usuario de que el emisor es genuino, pero con la intención de obtener información para su uso en ingeniería social. Los ataques de phishing pueden disimularse haciéndose pasar por una organización de lotería que avisa al destinatario o al usuario de un banco acerca de un gran premio; en cualquier caso, la intención es obtener los detalles de la cuenta y el número de identificación personal (PIN). Ataques alternativos pueden buscar obtener información de negocio aparentemente inocua, que se puede utilizar en otra forma de ataque activo.

Pista de auditoría—Pista visible de evidencia que permite rastrear la información contenida en las declaraciones o informes hacia la fuente de entrada original.

Plan de continuidad del negocio (BCP)—Plan utilizado por una empresa para responder a la interrupción de los procesos críticos de negocio. Depende del plan de contingencia para la restauración de los sistemas críticos

Plan de recuperación de desastres (DRP)—Conjunto de recursos humanos, físicos, técnicos y de procedimiento para recuperar, dentro de un tiempo y costo definidos, una actividad interrumpida por una emergencia o desastre.

Plan de respuesta a incidentes—Componente operacional de una gestión de incidentes. El plan incluye procedimientos documentados y lineamientos para la definición de la criticidad de los incidentes, los procesos de presentación de informes y escalado, y los procedimientos de recuperación.

Plataforma como servicio (PaaS)—Ofrece la capacidad de desplegar en la infraestructura de la nube aplicaciones —creadas o— adquiridas por el cliente, que son producidas utilizando lenguajes de programación y herramientas soportadas por el proveedor.

Política—Generalmente, un documento que registra un principio de alto nivel o curso de acción que se ha decidido. El propósito que se persigue es influir y guiar la toma de decisiones presentes y futuras para estar alineados con la filosofía, objetivos y planes estratégicos establecidos por los equipos de gestión de la empresa.

Además del contenido de las políticas, éstas deben describir las consecuencias de no cumplir con la política, los medios para manejar las excepciones, y la manera en la que se comprobará y medirá el cumplimiento de la política.

Política de monitorización—Reglas que describen o delinean la forma en que la información acerca del uso de computadoras, redes, aplicaciones y la información debe ser capturada e interpretada.

Política de uso aceptable—Política que establece un acuerdo entre los usuarios y la empresa y define, para todas las partes, los rangos de uso que están aprobados antes de obtener acceso a una red o a Internet.

Prevención de intrusiones—Enfoque preventivo para la seguridad de la red utilizado para identificar las amenazas potenciales y responder a ellas para detenerlas o al menos limitar el daño o la disruptión.

Principio de mínimo privilegio / acceso—Controles utilizados para permitir el acceso con el mínimo privilegio necesario para completar una tarea.

Privacidad—Libertad frente a la intrusión o divulgación de información personal no autorizada. Explorar—Inspeccionar una red o sistema para encontrar los puntos débiles.

Privacidad equivalente al cableado (WEP)—Esquema que forma parte del estándar de red inalámbrica IEEE 802.11 con el objetivo de securizar redes inalámbricas IEEE 802.11 (también conocidas como redes Wi-Fi). Debido a que una red inalámbrica transmite mensajes a través de radio, es particularmente susceptible escuchas. WEP fue pensado para proporcionar un nivel de confidencialidad comparable al de una red cableada tradicional (en particular, no protege a los usuarios de la red entre sí), de ahí su nombre. Varias debilidades graves fueron identificadas por criptoanalistas, y WEP fue reemplazado por el acceso protegido Wi-Fi (WPA) en 2003, y luego en el 2004 por el estándar IEEE 802.11i completo (también conocido como WPA2). A pesar de las debilidades, WEP proporciona un nivel de seguridad que puede disuadir la escucha ocasional.

Probabilidad—Probabilidad de que suceda algo.

Procedimiento—Documento que contiene una descripción detallada de los pasos necesarios para llevar a cabo operaciones específicas en conformidad con los estándares aplicables. Los procedimientos se definen como parte de los procesos.

Proceso alternativo—Proceso automático o manual diseñado y creado para continuar los procesos de negocio críticos desde el punto de falla hasta el regreso a la normalidad.

Programa de seguridad de la información—Combinación global de medidas técnicas, operacionales y de procedimiento y estructuras de gestión implementadas para proporcionar la confidencialidad, integridad y disponibilidad de la información en base a los requerimientos del negocio y el análisis de riesgos.

Propiedad intelectual—Activo intangible que pertenece a una empresa para su uso exclusivo. Ejemplos incluyen: patentes, derechos de autor, marcas registradas, ideas y secretos comerciales.

Propietario de los datos—Persona(s), normalmente un gerente o director, responsable(s) de la integridad, informes precisos y uso de datos informatizados.

Protección—Práctica, procedimiento o mecanismo que reduce el riesgo.

Proteger contra escritura—Uso de hardware o software para evitar que los datos sean sobrescritos o eliminados.

Protocolo—Reglas según las cuales una red opera y controla el flujo y la prioridad de las transmisiones.

Protocolo de Control de Transmisión (TCP)—Protocolo de Internet orientado a conexión que soporta conexiones de transferencia de datos fiables. Los paquetes de datos se verifican mediante checksums y se retransmiten si se han perdido o dañado. La aplicación no participa en la validación de la transferencia.

Protocolo de Control de Transmisión / Protocolo de Internet (TCP / IP)—Proporciona la base que hace posible Internet; un conjunto de protocolos de comunicación que abarcan el acceso al medio, el transporte de paquetes, la comunicación de sesión, la transferencia de archivos, el correo electrónico (e-mail), la emulación de terminal, el acceso remoto a archivos y la gestión de redes.

Protocolo de datagrama de usuario (UDP)—Protocolo de Internet no orientado a conexión que está diseñado pensando en la eficiencia y velocidad de la red a expensas de la fiabilidad. Una petición de datos por el cliente es atendida enviando paquetes sin pruebas para verificar si realmente llegan al destino, o si fueron dañados durante el transporte. Corresponde a la aplicación determinar estos factores y solicitar retransmisiones.

Protocolo de Internet (IP)—Especifica el formato de los paquetes y el esquema de direccionamiento.

Protocolo de mensajes de control de Internet (ICMP)—Conjunto de protocolos que permiten a los sistemas comunicar información sobre el estado de los servicios en otros sistemas. Por ejemplo, ICMP se utiliza para determinar cuándo los sistemas están levantados, los tamaños máximos de paquetes en los enlaces, si un host/red/ puerto de destino está disponible. Los hackers suelen utilizar (abusar) de ICMP para determinar información sobre el sitio remoto.

Protocolo de transferencia de archivos (FTP)—Protocolo utilizado para transferir archivos a través de un Protocolo de Control de Transmisión/Protocolo de Internet (TCP / IP) de una red (Internet, UNIX, etc.).

Protocolo de transferencia de hipertexto (HTTP)—Protocolo de comunicación utilizado para conectar los servidores a la World Wide Web. Su función principal es establecer una conexión con un servidor web y transmitir lenguaje de marcado de hipertexto (Hypertext markup language-HTML), lenguaje de marcado extensible (Extensible markup language-XML) u otras páginas a los navegadores clientes.

Protocolo de transferencia de noticias en red (NNTP)—Se usa para la distribución, consulta, recuperación y publicación de artículos de noticias de red (Netnews) utilizando un mecanismo fiable basado en el flujo. Para clientes lectores de noticias, NNTP permite la recuperación de artículos de noticias que se almacenan en una base de datos central, dando a los suscriptores la posibilidad de seleccionar sólo aquellos artículos que desean leer (RFC 3977).

Protocolo seguro de transferencia de hipertexto (HTTPS)—Protocolo de capa de aplicación, HTTPS transmite mensajes individuales o páginas de forma segura entre un cliente web y el servidor mediante el establecimiento de una conexión de tipo SSL.

Protocolo simple de transporte de correos (SMTP)—Protocolo estándar de correo electrónico (e-mail) en Internet.

Proveedor de servicio de Internet (ISP)—Tercera parte que proporciona a personas y empresas acceso a Internet y a una variedad de otros servicios relacionados con Internet.

Proyecto abierto de seguridad de aplicaciones web (OWASP)—Comunidad abierta dedicada a habilitar a las organizaciones para concebir, desarrollar, adquirir, operar y mantener aplicaciones fiables.

Prueba de penetración—Prueba en vivo de la eficacia de las defensas de seguridad a través de la imitación de las acciones de los atacantes en la vida real.

Puerta trasera—Medio a través del cual se recupera el acceso a un sistema comprometido mediante la instalación de software o la configuración de software existente que permitir el acceso remoto en las condiciones definidas por el atacante.

Puerto (número de puerto)—Proceso o aplicación- elemento de software específico que sirve como punto final de la comunicación para los protocolos de capa de transporte IP (UDP y TCP).

Puertos conocidos—0 al 1023: Controlados y asignados por la Autoridad de Números Asignados de Internet (IANA), y en la mayoría de los sistemas puede ser utilizado sólo por los procesos del sistema (o raíz) o por los programas ejecutados por usuarios con privilegios. Los puertos asignados utilizan la primera parte de los posibles números de puerto. Inicialmente, estos puertos asignados estaban en el rango 0-255. Actualmente, la gama de puertos asignados gestionados por la IANA se ha ampliado al rango 0-1023.

Puertos dinámicos—Puertos dinámicos y/o privados - 49152 a 65535. No listados por IANA debido a su naturaleza dinámica.

Puertos registrados—1024 al 49151: Enumerados por la IANA, en la mayoría de los sistemas pueden ser utilizados por procesos o programas ordinarios ejecutados por usuarios comunes.

R

Recuperación—Fase en el plan de respuesta a incidentes que asegura que los sistemas o servicios afectados son restaurados de acuerdo a una condición especificada en los objetivos de entrega del servicios (SDO) o un plan de continuidad del negocio (BCP).

Red de área amplia (WAN)—Red de computadoras que conecta diferentes lugares remotos que pueden ir desde las distancias cortas, como un piso o edificio, hasta las transmisiones extremadamente largas que abarcan una gran región o varios países.

Red de área local (LAN)—Red de comunicación que sirve para varios usuarios dentro de un área geográfica específica. Una LAN de computadoras personales funciona como un sistema de procesamiento distribuido en el que cada equipo de la red hace su propio procesamiento y gestiona algunos de sus datos. Los datos compartidos se guardan en un servidor de archivos que funciona como unidad remota de disco para todos los usuarios de la red.

Red de área local inalámbrica (WLAN)—Dos o más sistemas en red que utilizan un método de distribución inalámbrica.

Red de área local virtual (VLAN)—Segmentación lógica de una LAN en diferentes dominios de difusión. Se establece configurando puertos en un conmutador, de modo que los dispositivos conectados con estos puertos puedan comunicarse como si estuvieran conectados al mismo segmento físico de red, a pesar de que están ubicadas en segmentos de LAN diferentes. Una VLAN se basa en conexiones lógicas en vez de físicas.

Red de área metropolitana (MAN)—Red de datos destinada a servir un área del tamaño de una gran ciudad.

Red privada virtual (VPN)—Red privada segura que utiliza la infraestructura pública de telecomunicaciones para transmitir datos. En comparación con un sistema mucho más costoso de líneas propias o alquiladas que sólo pueden ser utilizadas por una compañía, las VPN son utilizadas por empresas tanto para extranets como para áreas amplias de Intranets. Utilizando cifrado y autenticación, una VPN cifra todos los datos que pasan entre dos puntos de Internet, manteniendo la privacidad y la seguridad.

Red telefónica pública comutada (PSTN)—Sistema de comunicaciones que establece un canal dedicado (o circuito) entre dos puntos mientras dure la transmisión.

Reducción del riesgo—Aplicación de controles o contramedidas para reducir la probabilidad del impacto de un riesgo a un nivel dentro del rango de tolerancia al riesgo de la organización.

Regulaciones—Reglas o leyes definidas y forzadas por una autoridad para regular la conducta.

Remediación—Después de que las vulnerabilidades han sido identificadas y evaluadas, una remediación apropiada puede llevarse a cabo para mitigar o eliminar la vulnerabilidad.

Repetición / retransmisión—Habilidad de copiar un mensaje o flujo de mensajes entre dos partes y repetir (retransmitir) a una o más de las partes.

Repetidores—Dispositivo de capa física que se regenera y propaga señales eléctricas entre dos segmentos de red. Los repetidores reciben señales de un segmento de red y amplifican (regeneran) la señal para compensar las señales (analógicas o digitales) distorsionadas por la pérdida de transmisión debido a la reducción de la intensidad de la señal durante la transmisión (por ejemplo, atenuación).

Requerimientos legales—Leyes creadas por las instituciones gubernamentales.

Requerimientos regulatorios—Reglas o leyes que regulan la conducta y que la empresa debe obedecer para estar en cumplimiento.

Resiliencia—Capacidad de un sistema o red para resistir a fallas o para recuperarse rápidamente frente a cualquier interrupción, generalmente con mínimos efectos.

Responsabilidad—La capacidad de relacionar una actividad o evento dado con su parte responsable.

Respuesta a incidentes—Respuesta de una empresa ante un desastre u otro evento significativo que pueda afectar considerablemente a la empresa, su gente o su capacidad para funcionar de manera productiva. Una respuesta a incidentes puede incluir la evacuación de una instalación, iniciar un plan de recuperación ante desastres (DRP), realizar una evaluación de daños y cualquier otra medida necesaria para que una empresa vuelva a un estado más estable.

Respuesta pasiva—Alternativa de respuesta en la detección de intrusiones, en la cual el sistema simplemente reporta y registra el problema detectado, confiando al usuario en la toma de una acción posterior.

Resumen del mensaje—Versión más pequeña extrapolada del mensaje original creado usando un algoritmo de resumen de mensaje.

Retención de datos—Se refiere a las políticas que gobiernan la gestión de datos y registros para el cumplimiento de los requisitos de archivado de datos, tanto internos, legales como regulatorios.

Retorno de la inversión (ROI)—Medida de la eficiencia y del desempeño operativo, calculada en su forma más simple, dividiendo los ingresos netos por la inversión total en el período considerado.

Riesgo—La combinación de la probabilidad de un evento y sus consecuencias (ISO / IEC 73).

Riesgo inherente—Nivel de riesgo o exposición sin tener en cuenta las acciones que la dirección ha tomado o puede tomar (por ejemplo, la implementación de los controles).

Riesgo residual—Riesgo que permanece después de que la dirección haya implementado una respuesta al riesgo

Rootkit—Suite de software diseñada para ayudar a un intruso a obtener acceso administrativo no autorizado a un sistema informático.

RSA—Sistema de cifrado de clave pública desarrollado por R. Rivest, A. Shamir y L. Adleman utilizado para el cifrado y para firmas digitales. El RSA tiene dos claves diferentes, la clave de cifrado pública y la clave secreta de descifrado. La fortaleza de RSA depende de la dificultad de la factorización del número primo. Para aplicaciones con alto nivel de seguridad, el número de bits de clave de descifrado debe ser mayor que 512 bits.

Ruta de acceso—Ruta lógica que un usuario final usa para acceder a la información computarizada. Típicamente incluye una ruta a través del sistema operativo, software de telecomunicaciones, software de aplicación seleccionado y el sistema de control de acceso.

S

Secuestro (Hijacking)—Explotación de una sesión de red válida para fines no autorizados.

Secure Shell (SSH)—Protocolo de red que utiliza la criptografía para proteger la comunicación, el inicio de sesión por línea de comando remota y la ejecución remota de comandos entre dos ordenadores conectados en red.

Segmentación—Proceso consistente en agrupar lógicamente los activos, recursos y aplicaciones de red, en áreas compartimentadas que no tienen confianza las unas con las otras.

Segmentación de redes—Técnica común para implementar la seguridad de redes consistente en segmentar la red de la organización en zonas separadas que se pueden controlar, monitorear y proteger de forma separada.

Segregación de funciones (SoD)—Control interno básico que previene o detecta errores e irregularidades mediante la asignación a individuos diferentes de responsabilidades relativas al inicio y registro de transacciones y la custodia de los activos. La segregación de funciones se utiliza comúnmente en grandes organizaciones de TI, para que ninguna persona esté en condiciones de introducir código malicioso o fraudulento sin ser detectado.

Seguridad como un servicio (SecaaS)—Próxima generación de servicios de seguridad gestionados dedicados a la entrega, a través de Internet, de servicios especializados de seguridad de la información.

Seguridad de la capa de transporte (TLS)—Protocolo que proporciona privacidad en las comunicaciones a través de Internet. El protocolo permite que las aplicaciones cliente-servidor puedan comunicarse de una manera diseñada para prevenir el espionaje, la manipulación o la falsificación de mensajes (RFC 2246).

El protocolo TLS se compone de dos capas: el Protocolo de Registro TLS y el Protocolo Handshake TLS. El Protocolo de Registro TLS proporciona seguridad de conexión con método de cifrado como el estándar de Encriptación de datos (DES). El Protocolo de Registro TLS también se puede utilizar sin cifrado. El Protocolo de Handshake TLS permite que el servidor y el cliente se autentiquen mutuamente y negocien un algoritmo de cifrado y claves criptográficas antes del intercambio de datos.

Seguridad de la información—Garantiza que dentro de la empresa, la información esté protegida frente a usuarios no autorizados (confidencialidad), la modificación indebida (integridad), y la imposibilidad de acceso cuando sea necesario (disponibilidad).

Seguridad IP (IpSec)—Conjunto de protocolos desarrollados por el Grupo de trabajo de ingeniería de Internet (IETF) para apoyar el intercambio seguro de paquetes.

Sensibilidad—Medida del impacto que la divulgación indebida de información puede tener en una empresa.

Servicio de acceso remoto (RAS)—Se refiere a cualquier combinación de hardware y software para permitir el acceso remoto a herramientas o información que normalmente residen en una red o en dispositivos de TI.

Originalmente acuñado por Microsoft cuando se refiere a sus herramientas de acceso remoto incorporadas en NT, RAS era un servicio proporcionado por Windows NT que permitió que la mayoría de los servicios disponibles en una red, fueran accesibles a través de un enlace de módem. A lo largo de los años, muchos proveedores han provisto soluciones de hardware y software para obtener acceso remoto a diversos tipos de información en red. En realidad, la mayoría de los enrutadores modernos incluyen una capacidad básica de RAS que se puede habilitar para cualquier interfaz de marcado.

Servicio telefónico normal (POTS)—Sistema de telecomunicaciones por cable.

Servidor de retransmisión / intermediador de correo—Servidor de correo electrónico (e-mail) que retransmite mensajes de modo que ni el remitente ni el destinatario sean usuarios locales.

Servidor proxy—Servidor que actúa en nombre de un usuario. Los proxies típicos aceptan una conexión de un usuario, toman la decisión en cuanto a si se permite que el usuario o dirección IP utilicen el proxy, tal vez realizan una autenticación adicional, y completan la conexión al destino remoto en nombre del usuario.

Servidor web—Utilizando el modelo cliente-servidor y el protocolo de transferencia de hipertexto de la World Wide Web (HTTP), un servidor web es un programa de software que sirve páginas web a los usuarios.

Sistema básico de entrada y salida de red (NetBIOS)—Programa que permite a las aplicaciones en distintas computadoras comunicarse dentro de una red de área local (LAN).

Sistema de detección de intrusiones (IDS)—Inspecciona la actividad de la red y del servidor para identificar patrones sospechosos que pueden indicar un ataque a la red o al sistema.

Sistema de nombres de dominio (DNS)—Base de datos jerárquica que se distribuye a través de Internet que permite que los nombres se resuelvan en direcciones IP (y viceversa) para localizar servicios como servidores web y de correo electrónico.

Sistema de prevención de intrusiones (IPS)—Sistema diseñado no sólo para detectar ataques, sino también para prevenir que se vean afectados por los ataques los servidores víctimas.

Sistema operativo—Programa maestro de control que se ejecuta en una computadora y actúa como un planificador y controlador de tráfico.

Sistemas de control de supervisión y adquisición de datos (SCADA)—Sistemas utilizados para controlar y supervisar los procesos industriales, de fabricación e instalaciones utilitarias.

Sistemas de información (SI)—Combinación de las actividades estratégicas, gerenciales y operativas involucradas en la recolección, el procesamiento, el almacenamiento, la distribución y el uso de la información y sus tecnologías relacionadas.

Los sistemas de información se diferencian de la tecnología de información (TI) en que un sistema de información tiene un componente de TI que interactúa con los componentes del proceso.

Sistemas heredados / históricos—Sistemas informáticos anticuados.

Sitio espejo—Sitio alternativo que contiene la misma información que el original. Los sitios espejo se establecen como centros de respaldo y recuperación de desastres y para equilibrar la carga de tráfico para numerosas solicitudes de descarga. Estos sitios espejos se colocan a menudo en diferentes lugares a lo largo de Internet.

Sitio móvil—Uso de una instalación móvil / temporal que tiene como objetivo la reanudación del negocio. La instalación por lo general puede ser entregada en cualquier sitio y puede albergar tecnologías de información y personal.

Sitio redundante—Estrategia de recuperación que implica la duplicación de los componentes claves de TI, incluidos los datos u otros procesos claves del negocio, para que una rápida recuperación puede tener lugar.

Situación de alerta—Punto en un procedimiento de emergencia cuando el tiempo transcurrido alcanza un umbral y la interrupción no se ha resuelto. La empresa que entra en una situación de alerta inicia una serie de pasos de escalado.

Software antivirus—Software de aplicación usado en múltiples puntos de una arquitectura TI. Está diseñado para detectar y eliminar potencialmente códigos de virus antes de que hagan daño y reparar o poner en cuarentena los archivos que ya han sido infectados.

Software como servicio (SaaS)—Ofrece la capacidad de utilizar las aplicaciones del proveedor para que su ejecución en la infraestructura de la nube. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, el correo electrónico basado en la web).

Software de rotura de contraseñas—Herramienta que pone a prueba la fortaleza de las contraseñas de usuario mediante la búsqueda de contraseñas fáciles de adivinar. Intenta repetidamente palabras de diccionarios expresamente elaborados para dicho propósito, y a menudo generan miles (y en algunos casos incluso millones) de combinaciones de caracteres, números y símbolos.

Software gratuito (Freeware)—Software disponible de forma gratuita.

Software maligno de petición de rescate (Ransomware)—Software maligno que restringe el acceso a los sistemas comprometidos hasta que una petición de rescate haya sido satisfecha.

Software malintencionado (malware)—Nombre corto para software malintencionado. Software diseñado para infiltrar, dañar u obtener información de un sistema computacional sin el consentimiento del propietario. El software malintencionado es comúnmente usado para incluir los virus informáticos, gusanos, troyanos, spyware y adware. El spyware se utiliza generalmente para fines de marketing y, como tal, no es malicioso, aunque es generalmente no deseado. El spyware puede, sin embargo, utilizarse para recopilar información para el robo de identidad u otros fines claramente ilícitos.

Spam—Mensajes generados por computadora, enviados como publicidad no solicitada.

Spear Phishing / Phishing de Ingeniería Social—Ataque de phishing, donde se utilizan técnicas de ingeniería social para hacerse pasar por un ente fiable para obtener información importante, como contraseñas de la víctima.

Spoofing—Falsificación de la dirección de envío de una transmisión con el fin de ganar acceso ilegalmente a un sistema seguro.

Spoofing de paquetes IP (Internet Protocol)—Ataque que usa los paquetes cuyas direcciones de paquetes de Internet (IP) de origen (fuente) han sido falsificadas. Esta técnica explota las aplicaciones que utilizan la autenticación basada en direcciones IP. Esta técnica también puede permitir a un usuario no autorizado obtener acceso de administrador al sistema de destino.

Spyware (Software Espía)—Software cuyo objetivo es vigilar las acciones de un usuario de un ordenador (por ejemplo, sitios web visitados) y reportar estas acciones a un tercero, sin el consentimiento del dueño de la máquina o usuario legítimo. Una forma de spyware especialmente malintencionada es el software que monitorea el uso del teclado para obtener contraseñas o reunir si no información confidencial como números de tarjeta de crédito, que transmite después a un tercero malintencionado. El término ha pasado a referirse también, de una forma más amplia, al software que altera la operación del ordenador en beneficio de un tercero.

Suplantación de interface de usuario—Puede ser un anuncio emergente que suplanta a un diálogo del sistema, un anuncio que se hace pasar por una advertencia del sistema, o un anuncio que se hace pasar por una interfaz de usuario de la aplicación en un dispositivo móvil.

Switches (Comutadores)—Por lo general asociados a un dispositivo de capa de enlace de datos, los switches habilitan segmentos de red de área local (LAN) que serán creados e interconectados, lo cual tiene el beneficio adicional de reducir los dominios de colisión en las redes basadas en Ethernet.

Switches de capa 2—Dispositivos de nivel de enlace de datos que pueden dividir e interconectar segmentos de la red y ayudar a reducir los dominios de colisión en las redes basadas en Ethernet.

Switches de capa 3 y 4—Comutadores con capacidades de operación en la capa 3 y la capa 4 del modelo de interconexión de sistemas abiertos (OSI). Estos comutadores miran el protocolo de red del paquete de entrada, por ejemplo, IP, y luego comparan la dirección IP de destino con la lista de direcciones de sus tablas, para calcular activamente la mejor forma de enviar un paquete a su destino.

Switches de capa 4-7—Usados para equilibrar la carga entre grupos de servidores. También conocidos como comutadores de contenidos, comutadores de servicios de contenidos, comutadores web o comutadores de aplicación.

T

Tarjeta de interfaz de red (NIC)—Tarjeta de comunicación que, cuando se inserta en una computadora, le permite comunicarse con otras computadoras de una red. La mayoría de las NIC están diseñadas para un tipo particular de red o protocolo.

Tarjeta inteligente—Dispositivo electrónico pequeño que contiene memoria electrónica y, posiblemente, un circuito integrado embebido. Las tarjetas inteligentes pueden utilizarse para diferentes propósitos como el almacenamiento de certificados digitales o dinero digital, o pueden utilizarse como un token para autenticar usuarios.

Telnet—Protocolo de red utilizado para permitir el acceso remoto a un equipo servidor. Los comandos tecleados se ejecutan en el servidor remoto.

Texto cifrado—Información generada por un algoritmo de cifrado para proteger el texto plano y que es ininteligible para el lector no autorizado.

Texto claro—Datos que no están cifrados. También conocido como texto plano.

Token—Dispositivo que se utiliza para autenticar a un usuario, generalmente además de un nombre de usuario y contraseña. Un token suele ser un dispositivo del tamaño de una tarjeta de crédito que muestra un número pseudo aleatorio que cambia en cuestión de minutos.

Tolerancia al riesgo—Nivel de variación aceptable que la administración está dispuesta a permitir para un riesgo particular cualquiera, dentro de la consecución de los objetivos de una empresa.

Topología—Diseño físico que muestra cómo las computadoras están conectadas entre sí. Algunos ejemplos de topología incluyen el anillo, la estrella y el bus.

Total de comprobación (hash total)—Total de cualquier campo de datos numéricos en un documento o archivo informático. Este total es verificado con el total de un control del mismo campo para facilitar la precisión del procesamiento.

Traducción de dirección de red (NAT)—Metodología de modificación de la información de la dirección de red en las cabeceras de los paquetes de datagramas cuando están en tránsito a través de un dispositivo de enrutamiento de tráfico, con el fin de asociar un espacio de dirección IP a otro.

Trae tu propio dispositivo (BYOD)—Política de una empresa utilizada para permitir la integración parcial o total de los dispositivos móviles propiedad del usuario para propósitos del negocio.

Transacción electrónica segura (SET)—Estándar que asegurará que la tarjeta de crédito y la información de la orden de pago asociada viajen de forma segura entre las distintas partes involucradas en Internet.

Transferencia del riesgo—Proceso de asignación del riesgo a otra empresa, por lo general a través de la compra de una póliza de seguro o por la externalización del servicio.

Tratamiento de riesgos—Proceso de selección y ejecución de medidas para modificar el riesgo (Guía ISO / IEC 73: 2002).

Triple DES (3DES)—Cifrado en bloque creado a partir del estándar de cifrado de datos (DES) mediante su aplicación llevada a cabo tres veces.

Túnel—Caminos que siguen los paquetes encapsulados, en una red privada virtual de Internet (VPN).

V

Valor—Valor relativo o importancia de una inversión para una empresa, tal y como lo perciben sus grupos de interés, expresada como beneficios del ciclo de vida total neto de los costos relacionados, ajustado para el riesgo y (en el caso del valor financiero) el valor temporal del dinero.

Vector de amenaza—Camino o ruta utilizada por el adversario para obtener acceso al objetivo.

Vector de ataque—Camino o ruta utilizado por el adversario para obtener acceso al objetivo (activo). Hay dos tipos de vectores de ataque: de entrada (Ingress) y de salida (Egress) (también conocido como exfiltración de datos).

Ventana de interrupción aceptable—Período máximo de tiempo en el que un sistema puede estar indisponible antes de poner en peligro la consecución de los objetivos de negocio de la empresa.

Virtualización—Proceso que consiste en agregar una “aplicación invitada” y datos en un “servidor virtual”, reconociendo que la aplicación invitada se apartará del servidor físico de la compañía.

Virus—Programa con la capacidad de reproducirse mediante la modificación de otros programas para incluir una copia de sí mismo. Un virus puede contener código destructivo que puede penetrar múltiples programas, archivos de datos o dispositivos en un sistema y propagarse a través de múltiples sistemas en una red.

Voz sobre IP (VoIP)—También llamada telefonía IP, telefonía de Internet y teléfono de banda amplia, es una tecnología que permite mantener una conversación de voz a través de Internet u otra red dedicada sobre el Protocolo de Internet (IP) en lugar de líneas de transmisión de voz dedicadas.

Vulnerabilidad—Debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer el sistema a amenazas adversas provenientes de eventos de amenaza.

W

Warm site—Similar al hot site pero no equipado totalmente con todo el hardware necesario para la recuperación.

Z

Zona desmilitarizada (DMZ)—Segmento de red protegido (por firewall) que actúa como una zona de amortiguación entre una red de confianza y una sin confianza. Una DMZ se utiliza normalmente para alojar sistemas como servidores web que deben ser accesibles tanto desde las redes internas como desde Internet.

ANEXO C—RESPUESTAS DE LA EVALUACIÓN DE CONOCIMIENTOS

SECCIÓN 1—EVALUACIÓN DE CONOCIMIENTOS (P. 21)

1. Tres controles comunes que se utilizan para proteger la disponibilidad de información son:
 - A. **redundancia, copias de seguridad y controles de acceso.**
 - B. cifrado, permisos de archivos y controles de acceso.
 - C. controles de acceso, archivos de registros (logs) y firmas digitales.
 - D. hashes, archivos de registros (logs) y las copias de seguridad
2. Seleccione todas las opciones que apliquen. El gobierno corporativo tiene varios objetivos, entre ellos:
 - A. **proporcionar orientación estratégica.**
 - B. **asegurar que se cumplen los objetivos.**
 - C. **verificar que los recursos de la organización se están utilizando adecuadamente.**
 - D. dirigir y monitorizar las actividades de seguridad.
 - E. **asegurar que el riesgo se gestiona correctamente.**
3. Escoja tres. De acuerdo con el marco de referencia del NIST, cuáles de las siguientes se consideran funciones clave necesarias para la protección de activos digitales?
 - A. Cifrar
 - B. **Proteger**
 - C. Investigar
 - D. **Recuperar**
 - E. **Identificar**
4. ¿Cuál de las siguientes es la mejor definición de la ciberseguridad?
 - A. El proceso por el cual una organización gestiona el riesgo de la ciberseguridad a un nivel aceptable
 - B. La protección de la información contra el acceso no autorizado o divulgación
 - C. La protección de los documentos en papel, digitales y la propiedad intelectual, y las comunicaciones verbales o visuales
 - D. **La protección de los activos de información, mediante el tratamiento de las amenazas a la información procesada, almacenada o transportada por sistemas de información conectados a través de redes**
5. ¿Cuál de los siguientes roles de ciberseguridad es responsable de gestionar los incidentes y su remediación?
 - A. Consejo de dirección
 - B. Comité Ejecutivo
 - C. **Gestión de la seguridad**
 - D. Profesionales de la ciberseguridad

SECCIÓN 2—EVALUACIÓN DE CONOCIMIENTOS (P. 48)

1. El deber principal de la ciberseguridad es identificar, mitigar y gestionar el **ciberriesgo** a los activos digitales de una organización.
2. Una **amenaza** es cualquier cosa capaz de actuar contra un activo, de una manera que puede causar daño.
3. Un **activo** es algo valioso que merece protección.
4. Una **vulnerabilidad** es una debilidad en el diseño, implementación, operación o controles internos de un proceso, que podría ser aprovechada para violar la seguridad del sistema.
5. El camino o ruta utilizada para obtener acceso al activo objetivo se conoce como un **vector de ataque**.
6. En un ataque, el contenedor que entrega el exploit al objetivo se llama **payload**.
7. Las **políticas** comunican actividades y conductas requeridas y prohibidas.
8. Un **rootkit** es un tipo de malware que oculta la existencia de otro malware, mediante la modificación del sistema operativo subyacente.
9. Los **procedimientos** proporcionan detalles sobre cómo cumplir con las políticas y normas.
10. Las **directrices** proporcionan una guía general y recomendaciones sobre qué hacer en situaciones específicas.

11. El **malware**, también conocido como código malicioso, es el software diseñado para obtener acceso a los sistemas informáticos objetivo, robar información o interrumpir las operaciones computacionales.
12. Las **normas** se utilizan para interpretar las políticas en situaciones específicas.
13. Los **parches** son soluciones a los errores de programación de software y codificación.
14. La **gestión de identidades** incluye muchos componentes, tales como los servicios de directorio, servicios de autenticación y autorización, y las capacidades de gestión de usuarios, tales como el aprovisionamiento y desaproporcionamiento.

SECCIÓN 3—EVALUACIÓN DE CONOCIMIENTOS (P. 83)

1. Seleccione todas las opciones que apliquen. El perímetro de Internet debería:
 - A. **detectar y bloquear el tráfico de los puntos finales internos infectados.**
 - B. **eliminar las amenazas como el spam de correo electrónico, virus y gusanos.**
 - C. formatear, cifrar y comprimir los datos.
 - D. **controlar el tráfico de usuarios con destino internet.**
 - E. **monitorizar la actividad dañina en los puertos de red internos y externos.**
2. La capa de _____ del modelo OSI asegura que los datos se transfieren de forma fiable en la secuencia correcta, y la capa de _____ coordina y gestiona las conexiones de usuario.
 - A. Presentación, enlace de datos
 - B. **Transporte, sesión**
 - C. Física, aplicación
 - D. Enlace de datos, red
3. Escoja tres. Los beneficios clave del sistema DMZ son:
 - A. las DMZs se basan en conexiones lógicas en vez de físicas.
 - B. **un intruso debe penetrar tres dispositivos separados.**
 - C. **las direcciones de red privadas no se dan a conocer en Internet.**
 - D. excelente rendimiento y escalabilidad, a medida que aumenta el uso de Internet.
 - E. **los sistemas internos no tienen acceso directo a Internet.**
4. ¿Cuál de las siguientes define mejor el papel del cifrado dentro de un programa global de ciberseguridad?
 - A. El cifrado es el principal medio para asegurar los activos digitales.
 - B. El cifrado depende de secretos compartidos, y por lo tanto es un medio de control poco fiable.
 - C. Los elementos de cifrado de un programa deben ser manejados por un criptógrafo de terceros.
 - D. **El cifrado es una forma esencial, pero incompleta, de control de acceso.**
5. El número y tipos de capas necesarias para la defensa en profundidad son una función de:
 - A. **valor del activo, la criticidad, la fiabilidad de cada control y el grado de exposición.**
 - B. agentes de amenaza, gobierno corporativo, cumplimiento y la política de dispositivos móviles.
 - C. configuración de red, controles de navegación, interfaz de usuario y tráfico en la VPN.
 - D. el aislamiento, la segmentación, los controles internos y los controles externos.

SECCIÓN 4—EVALUACIÓN DE CONOCIMIENTOS (P. 118)

1. Ponga los pasos de la fase de pruebas de penetración en el orden correcto.
 - D. **Planificación**
 - B. **Descubrimiento**
 - A. **Ataque**
 - C. **Presentación de informes**

2. El fortalecimiento de la seguridad del sistema debe aplicar el principio de _____ o _____.
 - A. Gobierno corporativo, cumplimiento
 - B. Menor privilegio, control de acceso**
 - C. Inspección de estado, acceso remoto
 - D. Evaluación de vulnerabilidades, mitigación del riesgo
3. Seleccione todas las opciones que apliquen. ¿Cuáles de las áreas funcionales siguientes son consideradas de gestión de red, de acuerdo con la norma ISO?
 - A. Gestión de contabilidad**
 - B. Gestión de fallas**
 - C. Gestión de firewalls
 - D. Gestión del rendimiento**
 - E. Gestión de la seguridad**
4. La virtualización consiste en:
 - A. la creación de una capa entre los controles de acceso físico y lógico.
 - B. múltiples sistemas operativos que coexisten en el mismo servidor, aislados unos de otros.**
 - C. el uso simultáneo del modo kernel y del modo de usuario.
 - D. interrogación DNS, consultas WHOIS y búsqueda (sniffing) en la red
5. La gestión de las vulnerabilidades comienza con la enumeración de los activos de ciberseguridad y sus respectivas ubicaciones, lo que se puede lograr a través de:
 - A. escaneo (Scanning) de vulnerabilidad.
 - B. prueba de penetración.
 - C. el mantenimiento de un inventario de activos.**
 - D. el uso de herramientas de línea de comandos.

SECCIÓN 5—EVALUACIÓN DE CONOCIMIENTOS (P. 137)

1. Organice los pasos del proceso de respuesta a incidentes en el orden correcto.
 - D. Preparación**
 - E. Detección y análisis**
 - B. Investigación**
 - A. Mitigación y recuperación**
 - C. Análisis posterior al incidente**
2. ¿Qué elemento de un plan de respuesta a incidentes implica la obtención y preservación de la evidencia?
 - A. Preparación
 - B. Identificación
 - C. Contención**
 - D. Erradicación
3. Seleccione tres. La cadena de custodia contiene información sobre:
 - A. objetivo de la recuperación de desastres, recursos y personal.
 - B. quién tuvo acceso a las pruebas, en orden cronológico.**
 - C. reglamentos laborales, sindicales y de privacidad.
 - D. prueba de que el análisis se hizo con base en copias idénticas a la evidencia original.**
 - E. los procedimientos que se siguieron al trabajar con la evidencia.**

4. El NIST define un(a) como “una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.”
- A. Desastre
 - B. Evento
 - C. Amenaza
 - D. Incidente**
5. Seleccione todas las opciones que apliquen. Un análisis de impacto en el negocio (BIA) debe identificar:
- A. las circunstancias en que debe ser declarado un desastre.
 - B. la probabilidad estimada de que las amenazas identificadas ocurran en realidad.**
 - C. la eficiencia y la eficacia de los controles existentes de mitigación de riesgos.**
 - D. una lista de vulnerabilidades, peligros y / o amenazas potenciales.**
 - E. los tipos de copias de seguridad de datos (completa, incremental y diferencial) que se utilizarán.

SECCIÓN 6—EVALUACIÓN DE CONOCIMIENTOS (P. 161)

1. _____ se define como “un modelo que permite un acceso conveniente, por demanda y a través de la red, a un conjunto compartido de recursos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con mínima administración o interacción con el proveedor del servicio”.
- A. Software como servicio (SaaS)
 - B. Computación en la nube**
 - C. Macrodatos
 - D. Plataforma como servicio (PaaS)
2. Seleccione todas las opciones que apliquen. ¿Cuál de las siguientes afirmaciones sobre las amenazas persistentes avanzadas (APT) son verdaderas?
- A. Las APT normalmente se originan a partir de fuentes tales como grupos del crimen organizado, activistas o gobiernos.**
 - B. Las APT usan técnicas de ofuscación que las ayudan a permanecer sin ser descubiertas durante meses o incluso años.**
 - C. Las APT suelen ser proyectos a largo plazo y con múltiples fases, enfocados en el reconocimiento.**
 - D. El ciclo de ataque de la APT comienza con la penetración del objetivo y la recolección de información sensible.
 - E. Aunque a menudo se asocian con las APT, las agencias de inteligencia rara vez son las autoras de los ataques APT.
3. ¿Cuáles de las siguientes respuestas son beneficios para el BYOD?
- A. La política de uso aceptable es más fácil de implementar.
 - B. Transferencia del costo al usuario.**
 - C. La satisfacción del trabajador aumenta.**
 - D. El riesgo de seguridad es conocido por el usuario.
4. Escoja tres. ¿Qué tipos de riesgo se asocian normalmente con los dispositivos móviles?
- A. Riesgo organizacional**
 - B. Riesgo de cumplimiento
 - C. Riesgo técnico**
 - D. Riesgo físico**
 - E. Riesgo transaccional
5. ¿Qué tres elementos del panorama de amenazas actual han proporcionado mayores niveles de acceso y conectividad, y por lo tanto han aumentado las oportunidades para el delito cibernético?
- A. La mensajería de texto, la tecnología Bluetooth y las tarjetas SIM
 - B. Las aplicaciones Web, los botnets y el malware primario
 - C. Las ganancias financieras, la propiedad intelectual y la política
 - D. La computación en la nube, las redes sociales y la computación móvil**