Materiales para el instructor Capítulo 1: un mundo de paladines, héroes y delincuentes

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 1: un mundo de paladines, héroes y delincuentes

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 1: Secciones y objetivos

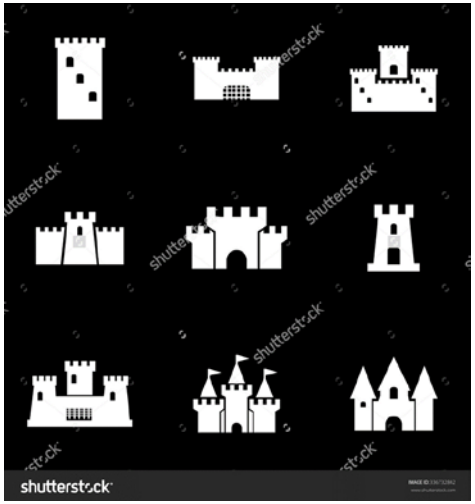
- 1.1 Características del mundo de la ciberseguridad
  - Describa las características comunes que componen el mundo de la ciberseguridad
- 1.2 Delincuentes y profesionales del área de la ciberseguridad
  - Distinga las características de los delincuentes cibernéticos y los héroes
- 1.3 Comparación de las amenazas a la ciberseguridad
  - Compare la manera en que las amenazas a la ciberseguridad afectan a las personas, las empresas y las organizaciones
- 1.4 Factores de crecimiento del delito cibernético
  - Analice las organizaciones y los esfuerzos comprometidos a expandir la fuerza laboral de ciberseguridad

1.1 El mundo de la ciberseguridad

Cisco | Networking Academy®
Mind Wide Open™

Descripción general de los reinos

- Sitios web y poder de los datos
  - Las grandes empresas han sido creadas mediante la recopilación y aprovechamiento del poder de los datos y del análisis de los datos
  - Estas empresas tienen la responsabilidad de proteger estos datos contra el uso indebido y el acceso no autorizado
  - El crecimiento de los datos ha generado importantes oportunidades para los especialistas en ciberseguridad
- Reinos
  - Las empresas grandes y pequeñas han reconocido el poder de los datos masivos y del análisis de datos
  - Organizaciones como Google, LinkedIn y Amazon proporcionan servicios y oportunidades importantes para sus clientes
  - El crecimiento de la recopilación y análisis de los datos presenta grandes riesgos para las personas y la vida moderna si no se toman las precauciones para proteger los datos sensibles contra los delincuentes u otras personas que tienen intención de dañar



Descripción general de los reinos (cont.)

- Los paladines cibernéticos ahora cuentan con la tecnología para hacer un seguimiento de las tendencias mundiales del clima, monitorear los océanos y seguir el movimiento y el comportamiento de las personas, los animales y los objetos en tiempo real.
- Surgieron nuevas tecnologías, como los Sistemas de información geoespaciales (GIS) y el Internet de todo (IdT). Cada uno depende de la recopilación y el análisis de enormes cantidades de datos.
- Esta recopilación de datos en aumento puede ayudar a las personas a ahorrar energía, mejorar las eficiencias y reducir los riesgos de seguridad.

1.2 Los delincuentes cibernéticos contra los profesionales cibernéticos

Cisco | Networking Academy®
Mind Wide Open™

Delincuentes de la ciberseguridad

- **Piratas informáticos**: este grupo de delincuentes penetran en las computadoras o redes para obtener acceso por varios motivos.

  Atacantes de sombrero blanco penetran en las redes o los sistemas informáticos para descubrir las debilidades a fin de mejorar la seguridad de estos sistemas.

  Atacantes de sombrero gris se encuetran entre los atacantes de sombrero blanco y negro. Los atacantes de sombrero gris pueden encontrar una vulnerabilidad y señalarla a los propietarios del sistema si esa acción coincide con su agenda.

  Los atacantes de sombrero negro*:* son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red.

Delincuentes de la ciberseguridad (cont.)

Existen varios tipos de delincuentes. Cada una tiene sus propios motivos:

- **Script kiddies:** adolescentes o aficionados que se limitan principalmente a realizar bromas y actos de vandalismo, tiene pocas habilidades o ninguna, y generalmente usan herramientas existentes o instrucciones que se encuentran en Internet para realizar ataques.
- **Agentes de vulnerabilidad:** hackers de sombrero gris que intentan descubrir los ataques e informarlos a los proveedores, a veces a cambio de premios o recompensas.
- **Hacktivistas:** hackers de sombrero gris que se reúnen y protestan contra diferentes ideas políticas y sociales. Los hacktivistas protestan en público contra las organizaciones o los gobiernos mediante la publicación de artículos, videos, la filtración de información confidencial y la ejecución de ataques de denegación de servicio distribuida.

Delincuentes de la ciberseguridad (cont.)

Existen varios tipos de delincuentes. Cada una tiene sus propios motivos:

- **Delincuentes cibernéticos** hackers de sombrero negro independientes o que trabajan para grandes organizaciones de delito cibernético. Cada año, los delincuentes cibernéticos son responsables de robar miles de millones de dólares de consumidores y empresas.
- **Hackers patrocinados por el estado:** según la perspectiva de una persona, son hackers de sombrero blanco o sombrero negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras. La mayoría de los países del mundo participan en algún tipo de hacking patrocinado por el estado.

Especialistas en ciberseguridad

Frustrar a los delincuentes cibernéticos es una tarea difícil. Las empresas, el gobierno y las organizaciones internacionales han comenzado a tomar medidas coordinadas para limitar o mantener a raya a los delincuentes cibernéticos. Las acciones coordinadas incluyen las siguientes:

- **Base de datos de vulnerabilidad**: la base de datos Vulnerabilidades y Exposiciones Comunes (CVE) nacional es un ejemplo de desarrollo de una base de datos nacional. La base de datos CVE nacional fue desarrollada para proporcionar una base de datos de todas las vulnerabilidades conocidas, qué esté públicamente disponible. http://www.cvedetails.com/
- **Sistemas de advertencia temprana**: el proyecto Honeynet es un ejemplo de la creación de sistemas de advertencia temprana. El proyecto proporciona un HoneyMap que muestra la visualización en tiempo real de los ataques. https://www.honeynet.org/node/960
- **Inteligencia cibernética compartida**: InfraGard es un ejemplo de compartición amplia de la inteligencia en ciberseguridad. El programa InfraGard es una asociación entre el FBI y el sector privado. Los participantes se dedican a compartir información e inteligencia para evitar ciberataques hostiles. https://www.infragard.org/

Especialistas en ciberseguridad (cont.)

- **Estándares ISM**: los estándares ISO 27000 son un ejemplo de estándares de administración de seguridad informática. Los estándares proporcionan un marco para implementar medidas de ciberseguridad en una organización. http://www.27000.org/
- **Nuevas leyes**: se promulgaron las leyes de seguimiento del grupo ISACA en relación con la ciberseguridad. Estas leyes pueden abordar desde la privacidad individual hasta la protección de la propiedad intelectual. Algunos ejemplos de estas leyes incluyen: la Ley de Ciberseguridad, la Ley federal de notificación de violaciones de datos de intercambio y la Ley de confianza y responsabilidad de los datos. http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Herramientas para frustrar el delito cibernético

1.3 Amenazas al reino

Cisco | Networking Academy®
Mind Wide Open™

Amenazas al reino

Ámbitos de las amenazas

- El término paladines cibernéticos se refiere a los innovadores y visionarios que crean el reino cibernético
- Los paladines cibernéticos poseen conocimientos para reconocer la influencia de los datos y aprovechan esos recursos para crear grandes organizaciones, proporcionar servicios y proteger a las personas de los ciberataques
- Los paladines cibernéticos reconocen la amenaza que presentan los datos si se utilizan contra las personas
- Una amenaza a la ciberseguridad es la posibilidad de que ocurra un evento nocivo, como un ataque
- La vulnerabilidad cibernética es una debilidad que hace que un objetivo sea susceptible a un ataque
- Las amenazas cibernéticas son particularmente peligrosas para algunos sectores y el tipo de información que recopilan y que protegen

Ámbitos de las amenazas (cont.)

Los siguientes ejemplos son solo algunas fuentes de datos que pueden provenir de organizaciones establecidas:

- **Información personal**
- **Historias clínicas**
- **Registros educativos**
- **Registros de empleo y financieros**

Ámbitos de las amenazas (cont.)

Los servicios de red como DNS, HTTP y las bases de datos en línea son los objetivos principales para los delincuentes cibernéticos.

- Los delincuentes utilizan herramientas de análisis de paquetes para capturar flujos de datos en una red. Los analizadores de protocolos de paquetes supervisan y registran toda la información que proviene de una red.
- Los delincuentes pueden utilizar además dispositivos falsos, como puntos de acceso a Wi-Fi no seguros.
- La falsificación del paquete (o la inyección de paquetes) interfiere con una comunicación de red establecida mediante la creación de paquetes para que parezca como si fueran parte de una comunicación.

Ámbitos de las amenazas (cont.)

Los sectores del reino incluyen los siguientes:

- Manufactura
  - Controles del sector
  - Automatización
  - SCADA
- Producción energética y distribución
  - Distribución eléctrica y matriz inteligente
  - Petróleo y gas
- Comunicación
  - Teléfono
  - Correo electrónico
  - Mensajería
- Sistemas de transporte
  - Transporte aéreo
  - Ferrocarriles
  - Vehículos de carretera

Ámbitos de las amenazas (cont.)

- A nivel personal, todas las personas necesitan proteger su identidad, sus datos y sus dispositivos informáticos.
- A nivel corporativo, es responsabilidad de los empleados proteger la reputación, los datos y los clientes de la organización.
- A nivel estatal, la seguridad nacional y la seguridad y el bienestar de los ciudadanos están en juego.
- En EE. UU., la Agencia de Seguridad Nacional (NSA) es responsable de las actividades de recopilación y vigilancia de inteligencia.
- Los esfuerzos por proteger la forma de vida de las personas a menudo entran en conflicto con su derecho a la privacidad.

1.4 El lado oscuro de la ciberseguridad

Cisco | Networking Academy®
Mind Wide Open™

La propagación del lado oscuro

Los ataques pueden originarse dentro de una organización o fuera de ella, como se muestra en la figura.

Amenazas de seguridad internas

- Un usuario interno, como un empleado o un partner contratado, puede de manera accidental o intencional
- Las amenazas internas tienen el potencial de causar mayores daños que las amenazas externas porque los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura. Los atacantes internos normalmente tienen conocimiento de la red corporativa, sus recursos y sus datos confidenciales. También pueden tener conocimiento de las contramedidas de seguridad, las políticas y los niveles más altos de privilegios administrativos.

Amenazas de seguridad externas

- Las amenazas externas de los aficionados o de los atacantes expertos pueden explotar las vulnerabilidades en los dispositivos conectados a la red o pueden utilizar la ingeniería social, como trucos, para obtener acceso.
- Los ataques externos aprovechan las debilidades o vulnerabilidades para obtener acceso a los recursos internos.

La propagación del lado oscuro (cont.)

Vulnerabilidades de los dispositivos móviles: en el pasado, los empleados generalmente utilizaban computadoras de la empresa conectadas a una LAN corporativa.

- En la actualidad, los dispositivos móviles como iPhones, smartphones, tablets y miles de otros dispositivos son sustitutos poderosos o agregados de las computadoras tradicionales.
- La gente usa cada vez más estos dispositivos para tener acceso a la información de la empresa. Bring Your Own Device (BYOD) es una tendencia en crecimiento.
- La incapacidad para administrar y actualizar de manera central los dispositivos móviles presenta una amenaza en crecimiento para las organizaciones que permiten el uso de dispositivos móviles de los empleados en sus redes.

La propagación del lado oscuro (cont.)

- **El surgimiento del Internet de las cosas**: el Internet de las cosas (IdC) es el conjunto de tecnologías que permiten la conexión de varios dispositivos a Internet.
- Las tecnologías del IdC permiten que las personas conecten miles de millones de dispositivos a Internet. Estos dispositivos incluyen trabas, motores y dispositivos de entretenimiento, solo por mencionar algunos ejemplos.
- Esta tecnología afecta la cantidad de datos que necesitan protección. Los usuarios acceden a estos dispositivos en forma remota, lo cual aumenta la cantidad de redes que requieren protección.
- Con el surgimiento del IdC, hay muchos más datos que deben administrarse y protegerse. Todas estas conexiones, además de la capacidad y los servicios de almacenamiento expandidos que se ofrecen a través de la nube y la virtualización, han generado el crecimiento exponencial de los datos.

La propagación del lado oscuro (cont.)

Impacto de los datos masivos: los datos masivos son el resultado de los conjuntos de datos que son grandes y complejos, lo que hace que las aplicaciones tradicionales de procesamiento de datos sean inadecuadas. Los datos masivos presentan desafíos y oportunidades según tres dimensiones:

- El volumen o la cantidad de datos
- La velocidad de los datos
- La variedad o el rango de los tipos y fuentes de datos

Existen muchos ejemplos de amenazas de gran envergadura en las noticias. Como resultado, los sistemas empresariales deben realizar cambios drásticos en los diseños de producto de seguridad y las actualizaciones importantes a las tecnologías y las prácticas. Además, los gobiernos y las industrias están introduciendo más regulaciones y obligaciones que requieren una mejor protección de los datos y controles de seguridad para ayudar a proteger los datos masivos.

La sofisticación del lado oscuro

Armas avanzadas

- La Amenaza persistente avanzada (APT) es una amenaza continua a las computadoras que se realizan en el radar contra un objeto específico. Los delincuentes eligen generalmente una APT por motivos políticos o empresariales.
- Los ataques a los algoritmos pueden rastrear los datos de informe propio de un sistema, como la cantidad de energía que utiliza una computadora, y usar esa información para seleccionar los objetivos o para activar alertas falsas. Los ataques a los algoritmos son más taimados porque atacan a los diseños utilizados para mejorar el ahorro de energía, disminuir las fallas del sistema y mejorar las eficiencias.
- Selección inteligente de víctimas. En el pasado, los ataques seleccionaban las opciones más fáciles o las víctimas más vulnerables. Muchos de los ataques más sofisticados se ejecutan sólo si el atacante puede igualar las firmas de la víctima objetivo.

Un alcance más amplio y el efecto cascada

- La administración de identidades federada se refiere a varias empresas que permiten a los usuarios utilizar las mismas credenciales de identificación que obtienen acceso a las redes de todas las empresas del grupo. El objetivo de la administración de identidades federada es compartir la información de identidad automáticamente a través de los límites del castillo.
- La manera más común de proteger la identidad federada es vincular la capacidad de inicio de sesión a un dispositivo autorizado.

La sofisticación del lado oscuro (cont.)

Implicaciones de seguridad

- Existen muchas implicaciones de seguridad relacionadas con el lado oscuro de la ciberseguridad, incluidos los centros de llamadas de emergencia en EE. UU. que son vulnerables a los ciberataques que podrían apagar las redes de 911 y comprometer así la seguridad pública.
- Un ataque de denegación de servicios telefónicos (TDoS) utiliza las llamadas telefónicas a una red telefónica objetivo, lo que condiciona el sistema y evita que las llamadas legítimas pasen.
- Los centros de llamadas 911 de próxima generación son vulnerables porque utilizan los sistemas de voz sobre IP (VoIP) en lugar de líneas fijas tradicionales.

Reconocimiento mejorado de las amenazas a la ciberseguridad

- Las defensas contra los ciberataques al inicio de la era cibernética eran bajas. Un estudiante inteligente de escuela secundara o script kiddie podría tener acceso a los sistemas.
- Ahora, los países de todo el mundo son más conscientes de las amenazas de los ciberataques. La amenaza que presentaron los ciberataques ahora encabezan la lista de las mayores amenazas a la seguridad nacional y económica en la mayoría de los países.

1.5 Creación de más héroes

Cisco | Networking Academy®
Mind Wide Open™

Un marco de fuerza laboral para la ciberseguridad

Cómo abordar la escasez de especialistas en ciberseguridad

- En EE. UU., el Instituto Nacional de Normas y Tecnologías (NIST) creó un marco de trabajo para las empresas y las organizaciones que necesitan profesionales en el área de la ciberseguridad. El marco de trabajo les permite a las empresas identificar los tipos principales de responsabilidades, los cargos y destrezas de la fuerza laboral necesarias.

Siete categorías de paladines en el área de la ciberseguridad

El marco de la fuerza laboral categoriza el trabajo en ciberseguridad en siete categorías.

- **Operar y mantener** incluye proporcionar soporte técnico, administración, y el mantenimiento necesario para garantizar el rendimiento y la seguridad de los sistemas de TI
- **Proteger y defender** incluye la identificación, el análisis y la mitigación de amenazas a los sistemas internos y redes internas
- **Investigar** incluye la investigación de los eventos cibernéticos o los delitos informáticos que involucran a los recursos de TI
- **Recopilar y operar** incluye operaciones especializadas de ataque y engaño, y la recopilación de información sobre ciberseguridad

Un marco de fuerza laboral para la ciberseguridad (cont.)

- **Analizar** incluye la revisión y evaluación altamente especializada de la información entrante de ciberseguridad para determinar si es útil para la inteligencia
- **Supervisión y desarrollo** establece el liderazgo, la administración y la dirección para realizar el trabajo de ciberseguridad de manera eficaz
- **Disponer de manera segura** incluye conceptualización, diseño y creación de sistemas de TI seguros

Dentro de cada categoría, existen varias áreas de especialidad. Las áreas de especialidad luego definen los tipos comunes de trabajo de ciberseguridad.

Comunidades de ciberseguridad en línea

Organizaciones profesionales

- Los especialistas en ciberseguridad deben colaborar a menudo con colegas profesionales. Las organizaciones internacionales de tecnología a menudo patrocinan talleres y conferencias. Visite cada sitio con la clase y analice los recursos disponibles.

Comunidades de ciberseguridad en línea

Competencias y organizaciones estudiantiles de ciberseguridad

- Los especialistas en ciberseguridad deben tener las mismas destrezas que los hackers, especialmente que los hackers de sombrero negro, para ofrecer protección contra los ataques.
- ¿Cómo puede una persona crear y practicar las aptitudes necesarias convertirse en un especialista en ciberseguridad?
- Las competencias de habilidades del estudiante son una excelente manera de desarrollar habilidades y capacidades de conocimiento en ciberseguridad.
- Existen muchas competencias nacionales de habilidades en ciberseguridad disponibles para los estudiantes de ciberseguridad.

SkillsUSA

USCC
US CYBER CHALLENGE

ncl

Certificaciones en ciberseguridad

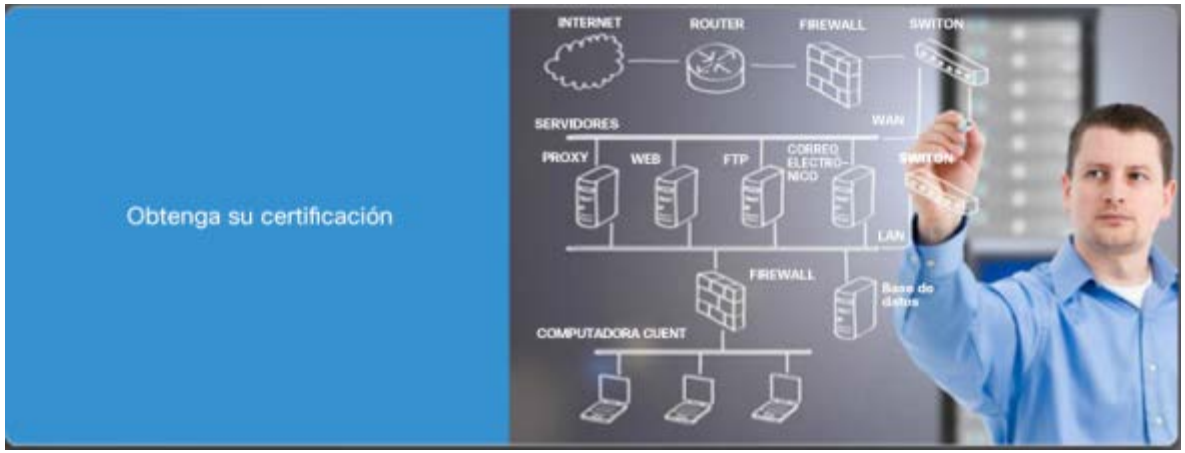
Certificaciones del sector

En un mundo de amenazas a la ciberseguridad, existe una gran necesidad de contar con profesionales expertos y calificados en seguridad de la información. La industria de TI estableció estándares para que los especialistas en ciberseguridad obtengan certificaciones profesionales que proporcionan pruebas de las habilidades y el nivel de conocimiento.

- **CompTIA Security+:** Security+ es un programa de pruebas patrocinado por CompTIA que certifica la competencia de los administradores de TI en la seguridad de la información.
- **EC-Council Certified Ethical Hacker (CEH):** CEH es una certificación de nivel intermediario que afirma que los especialistas en ciberseguridad que poseen esta credencial poseen las habilidades y el conocimiento para varias prácticas de hacking.
- **SANS GIAC Security Essentials (GSEC):** la certificación GSEC es una buena opción como credencial de nivel básico para especialistas en ciberseguridad que pueden demostrar que comprenden la terminología y los conceptos de seguridad, y tienen las habilidades y la experiencia necesarias para puestos “prácticos” en seguridad. El programa SANS GIAC ofrece varias certificaciones adicionales en los campos de administración de la seguridad, informática forense y auditoría.

Certificaciones en ciberseguridad (cont.)

- **(ISC) ^2 profesional certificado en seguridad de los sistemas informáticos (CISSP):** la certificación de CISSP es una certificación neutral para proveedores para los especialistas en ciberseguridad con mucha experiencia técnica y administrativa. También está aprobada formalmente por el Departamento de Defensa (DoD) de EE. UU y es una certificación con reconocimiento global del sector en el campo de la seguridad.
- **Certificación para administradores de seguridad informática (CISM) de ISACA:** los héroes cibernéticos responsables de administrar, desarrollar y supervisar los sistemas de seguridad de la información a nivel empresarial o para aquellos que desarrollan las mejores prácticas de seguridad puedan obtener la certificación CISM.



Certificaciones en ciberseguridad (cont.)

Certificaciones patrocinadas por la empresa: otras credenciales importantes para los especialistas en ciberseguridad son las certificaciones patrocinadas por la empresa. Estas certificaciones miden el conocimiento y la competencia en la instalación, la configuración y el mantenimiento de los productos de los proveedores. Cisco y Microsoft son ejemplos de empresas con certificaciones que prueban el conocimiento de sus productos. Haga clic aquí para explorar la matriz de las certificaciones de Cisco que se muestran en la figura.

Asociado en redes con certificación de Cisco (seguridad CCNA): la certificación de Seguridad CCNA ratifica que un especialista en ciberseguridad cuenta con el conocimiento y las habilidades necesarias para proteger las redes de Cisco.

Certificaciones de Cisco

	Nivel básico	Asociado	Profesional	Experto
Arquitecto				Arquitecto de CCAr
Nube		Nube de CCNA	Nube de CCNP	
Colaboración		Colaboración de CCNA	Colaboración de CCNP	Colaboración de CCIE
Centro de datos		Centro de datos de CCNA	Centro de datos de CCNP	Centro de datos de CCIE
Diseño	CCENT	CCDA	CCDP	CCDE
Seguridad industrial/ Internet de las cosas (IdC)		CCNA industrial		
Routing y switching	CCENT	Routing y switching de CCNA	CCNP Routing & Switching	CCIE Routing y switching
Seguridad	CCENT	Seguridad CCNA (CCNA Security)	Seguridad CCIE (CCIE Security)	Seguridad CCNP (CCNP Security)
Proveedor de servicios		CCNA SP	CCNP SP	CCIE SP
Inalámbrica	CCENT	CCNA inalámbrico	CCNP inalámbrico	CCIE inalámbrico
Otras certificaciones	Técnico certificado			
Especialista	Laboral	Centro de datos	Internet de las cosas	Programabilidad de la red
	Seguridad	Software de sistema operativo	Proveedor de s ervicios	Colaboración

Certificaciones en ciberseguridad (cont.)

Cómo convertirse en un héroe cibernético

Los héroes deben ser capaces de responder a las amenazas tan pronto como ocurran. Esto significa que las horas de trabajo pueden ser poco convencionales. Los héroes cibernéticos también analizan las políticas, las tendencias y la inteligencia para comprender cómo piensan los delincuentes cibernéticos. Muchas veces, esto pueden incluir una gran cantidad de trabajo de detección. Le damos un buen consejo para convertirse en un héroe de ciberseguridad:

- **Estudie**: conozca los aspectos básicos para completar los cursos en TI. Sea un estudiante durante toda su vida. La ciberseguridad es un campo en constante cambio y los especialistas en ciberseguridad deben mantenerse actualizados.
- **Obtenga certificaciones**: las certificaciones patrocinadas por la empresa y el sector, de organizaciones como Microsoft y Cisco demuestran que uno posee los conocimientos necesarios para buscar empleo como especialista en ciberseguridad.
- **Busque pasantías**: la búsqueda de una pasantía en seguridad como estudiante puede traducirse en oportunidades en el futuro.
- **Únase a organizaciones profesionales**: únase a las organizaciones de seguridad informática, asista a reuniones y conferencias y participe en foros y blogs para obtener conocimiento de los expertos.

1.6 Resumen del capítulo

Cisco | Networking Academy®
Mind Wide Open™

Resumen del capítulo

Resumen

- En este capítulo se explicó la estructura del mundo en ciberseguridad y el motivo por el que sigue creciendo con los datos y la información como la divisa preciada.
- Exploró la motivación de los delincuentes cibernéticos.
- Exploró la propagación del lado oscuro debido a las transformaciones técnicas en constante expansión que transcurren en todo el mundo.
- Proporcionó detalles sobre cómo convertirse en un héroe cibernético para ayudar a vencer a los delincuentes cibernéticos que fortalecen el lado oscuro.
- Examinó los recursos disponibles para ayudar a crear más héroes.
- Explicó que los profesionales cibernéticos deben contar con las mismas destrezas que los delincuentes cibernéticos.
- Si desea continuar explorando los conceptos de este capítulo, consulte la página Recursos y actividades adicionales en Recursos para el estudiante.