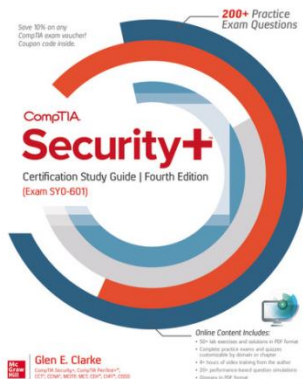


Security+: Contenido

Guía de estudio de certificación CompTIA Security+, cuarta edición (examen SYO-601), 4ª edición

Escribe el [primera revisión](#)

Por [Glen E. Clarke](#)



TIEMPO PARA COMPLETAR:
26h 52m

TEMAS:
[CompTIA Seguridad+](#)

PUBLICADO POR:
[McGraw-Hill](#)

FECHA DE PUBLICACIÓN:
Septiembre 2021

LONGITUD DE IMPRESIÓN:
944 páginas

1 Conceptos básicos y terminología de redes

[Descripción de los dispositivos de red y el cableado](#)

[Mirando los dispositivos de red](#)

[Descripción del cableado de red](#)

[Ejercicio 1-1: Revisión de componentes de red](#)

[Descripción de TCP/IP](#)

[Revisión del direccionamiento IP](#)

[Ejercicio 1-2: Descripción de direcciones válidas](#)

[Descripción de los protocolos TCP/IP](#)

[Ejercicio 1-3: Visualización de la información del protocolo con Wireshark](#)

[Descripción de los protocolos de capa de aplicación](#)

[Descripción de IPv6](#)

[Ejercicio 1-4: Identificación de protocolos en TCP/IP](#)

[Prácticas recomendadas de seguridad de red](#)

[Uso del dispositivo](#)

[Uso de cables y protocolos](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[2 Introducción a la terminología de seguridad](#)

[Objetivos de la seguridad de la información](#)

[Confidencialidad](#)

[Integridad](#)

[Disponibilidad](#)

[Responsabilidad](#)

[Ejercicio 2-1: Escenarios de la CIA](#)

[Descripción de la autenticación y la autorización](#)

[Identificación y autenticación](#)

[Autorización](#)

[Comprender los principios y la terminología de seguridad](#)

[Tipos de seguridad](#)

[Privilegios mínimos, separación de funciones y rotación de funciones](#)

[Concepto de necesidad de saber](#)

[Seguridad en capas y diversidad de defensa](#)

[Due Care y Due Diligence](#)

[Vulnerabilidad y exploit](#)

[Actores de amenazas](#)

[Vectores de amenaza](#)

[Fuentes de inteligencia de amenazas](#)

[Fuentes de investigación](#)

[Analizar los roles y responsabilidades de seguridad](#)

[Propietario del sistema y propietario de los datos](#)

[Controlador de datos y procesador de datos](#)

[Administrador del sistema](#)

[Usuario](#)

[Usuario privilegiado](#)

[Usuario Ejecutivo](#)

[Roles y responsabilidades de los datos](#)

[Oficial de Seguridad](#)

[Ejercicio 2-2: Terminología de seguridad](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[3 Políticas y estándares de seguridad](#)

[Introducción a las políticas de seguridad](#)

[Estructura de una política](#)

[Identificación de tipos de directivas](#)

[Políticas generales de seguridad](#)

[Políticas que afectan a los usuarios](#)

[Políticas que afectan a la gestión de personal](#)

[Políticas que afectan a los administradores](#)

[Ejercicio 3-1: Revisión de una directiva de seguridad](#)

[Políticas que afectan a la administración](#)

[Otras políticas populares](#)

[Políticas de Recursos Humanos](#)

[Política de Contratación](#)

[Política de terminación](#)

[Vacaciones obligatorias](#)

[Políticas de recursos humanos relacionadas con la seguridad](#)

[Ejercicio 3-2: Creación de una directiva de seguridad](#)

[Educación y sensibilización de los usuarios](#)

[Capacitación general y capacitación basada en roles](#)

[Hábitos de usuario](#)

[Nuevas amenazas y tendencias de seguridad](#)

[Uso de Redes Sociales y Programas P2P](#)

[Métricas de capacitación y seguimiento](#)

[Ejercicio 3-3: Diseño de un programa de capacitación](#)

[Importancia de las políticas para la seguridad de la organización](#)

[Conceptos de privacidad y datos confidenciales](#)

[Regulaciones y Estándares](#)

[Regulaciones, Estándares y Legislación](#)

[Marcos y guías de seguridad](#)

[Guías de configuración de Benchmark/Secure](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[4 tipos de ataques](#)

[Entendiendo la Ingeniería Social](#)

[Visión general de la ingeniería social](#)

[Ataques populares de ingeniería social](#)

[Ataques físicos](#)

[Inteligencia Artificial Adversarial](#)

[Ataques a la cadena de suministro](#)

[Ataques basados en la nube frente a ataques locales](#)

[Razones para la eficacia](#)

[Prevención de ataques de ingeniería social](#)

[Identificación de ataques de red](#)

[Ataques de red populares](#)

[Ejercicio 4-1: Envenenamiento de DNS después de explotar usando Kali Linux](#)

[Ejercicio 4-2: Realización de un análisis de puertos](#)

[Otros ataques de red](#)

[Ejecución de código malicioso o script](#)

[Prevención de ataques de red](#)

[Mirando los ataques de contraseña](#)

[Tipos de ataques de contraseña](#)

[Ataques y conceptos criptográficos](#)

[Ataques en línea frente a ataques fuera de línea](#)

[Otros términos de ataque de contraseña](#)

[Prevención de ataques de contraseña](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[5 Vulnerabilidades y amenazas](#)

[Problemas de seguridad con vulnerabilidades](#)

[Razones para sistemas vulnerables](#)

[Comprender el impacto de las vulnerabilidades](#)

[Problemas comunes de seguridad y salida del dispositivo](#)

[Ejercicio 5-1: Control de medios extraíbles](#)

[Vulnerabilidades basadas en la nube frente a vulnerabilidades locales](#)

[Identificación de amenazas físicas](#)

[Husmeando](#)

[Robo y pérdida de activos](#)

[Fallo humano](#)

[Sabotaje](#)

[Mirando el software malicioso](#)

[Escalada de privilegios](#)

[Virus](#)

[Otro software malicioso](#)

[Protección contra software malicioso](#)

[Amenazas contra el hardware](#)

[Configuración del BIOS](#)

[Dispositivos USB](#)

[Teléfonos inteligentes y tabletas](#)

[Ejercicio 5-2: Explotación de un dispositivo Bluetooth](#)

[Almacenamiento extraíble](#)

[Almacenamiento conectado en red](#)

[PBX](#)

[Riesgos de seguridad con sistemas integrados y especializados](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

6 Mitigación de las amenazas a la seguridad

Descripción del endurecimiento del sistema operativo

Desinstalar software innecesario

Deshabilitar servicios innecesarios

Ejercicio 6-1: Deshabilitar el servicio Servicios de Escritorio remoto

Proteja las interfaces y aplicaciones de administración

Deshabilitar cuentas innecesarias

Administración de parches

Protección con contraseña

Endurecimiento del registro

Cifrado de disco

Procedimientos de endurecimiento del sistema

Endurecimiento de la seguridad de la red

Ejercicio 6-2: Endurecimiento de un conmutador de red

Herramientas para el endurecimiento del sistema

Ejercicio 6-3: Creación de una plantilla de seguridad

Postura de seguridad e informes

Prácticas recomendadas de endurecimiento del servidor

Todos los servidores

Servidores HTTP

Servidores DNS

Ejercicio 6-4: Limitar las transferencias de zona DNS

[Servidores DHCP](#)

[Servidores SMTP y servidores FTP](#)

[Estrategias comunes de mitigación](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[7 Implementación de la seguridad basada en host](#)

[Soluciones de seguridad de host y aplicaciones](#)

[Protección de endpoints](#)

[Integridad del arranque](#)

[Base de datos](#)

[Implementación de firewalls basados en host y HIDS](#)

[Firewalls basados en host](#)

[Ejercicio 7-1: Configuración de TCP Wrappers en Linux](#)

[IDS basado en host e IPS basado en host](#)

[Protección contra el malware](#)

[Administración de parches](#)

[Uso de software antivirus y antispam](#)

[Spyware y Adware](#)

[Filtros de phishing y bloqueadores de ventanas emergentes](#)

[Ejercicio 7-2: Prueba manual de un sitio web para phishing](#)

[Practicar buenos hábitos](#)

[Seguridad de dispositivos y seguridad de datos](#)

[Seguridad de hardware](#)

[Seguridad de dispositivos móviles](#)

[Seguridad de los datos](#)

[Ejercicio 7-3: Configuración de permisos en Windows 10](#)

[Seguridad de las aplicaciones y preocupaciones BYOD](#)

[Diseño seguro del sistema](#)

[Implementación de ensayo seguro](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[8 Protección de la infraestructura de red](#)

[Descripción de los cortafuegos](#)

[Cortafuegos](#)

[Uso de IPTables como firewall](#)

[Ejercicio 8-1: Configuración de IPTables en Linux](#)

[Uso de las funciones de firewall en un enrutador doméstico](#)

[NAT y redes ad hoc](#)

[Servidores proxy](#)

[Routers y ACL](#)

[Otros dispositivos y tecnologías de seguridad](#)

[Uso de sistemas de detección de intrusos](#)

[Descripción general de IDS](#)

[Ejercicio 8-2: Uso de Snort: un IDS basado en red](#)

[Engaño y interrupción](#)

[Analizadores de protocolos](#)

[Principios de diseño y administración de redes](#)

[Segmentación de red](#)

[Conmutadores de red](#)

[Traducción de direcciones de red](#)

[Control de acceso a la red](#)

[Protección de datos](#)

[Soberanía de los datos](#)

[Puerta de enlace de correo](#)

[Cifrado de comunicación de red](#)

[Consideraciones sobre la API](#)

[Principios de administración de redes](#)

[Consideraciones sobre la conectividad empresarial](#)

[Colocación de dispositivos de seguridad y dispositivos de red](#)

[Gestión de la configuración](#)

[Protección de dispositivos](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[9 Redes inalámbricas y seguridad](#)

[Descripción de las redes inalámbricas](#)

[Normas](#)

[Canales](#)

[Tipos de antenas](#)

[Autenticación y cifrado](#)

[Protección de una red inalámbrica](#)

[Prácticas recomendadas de seguridad](#)

[Vulnerabilidades con redes inalámbricas](#)

[Ejercicio 9-1: Cracking WEP con Kali Linux](#)

[Consideraciones de instalación](#)

[Configuración de una red inalámbrica](#)

[Configuración del punto de acceso](#)

[Configuración del cliente](#)

[Otras tecnologías inalámbricas](#)

[Infrarrojo](#)

[Bluetooth](#)

[Comunicación de campo cercano](#)

[RFID](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[10 Autenticación](#)

[Identificación de modelos de autenticación](#)

[Terminología de autenticación](#)

[Métodos y tecnologías de autenticación](#)

[Factores y atributos de autenticación multifactor](#)

[Ejercicio 10-1: Configuración de MFA en Outlook Web Mail](#)

[Administración de autenticación](#)

[Inicio de sesión único](#)

[Requisitos en la nube frente a los requisitos locales](#)

[Protocolos de autenticación](#)

[Protocolos de autenticación de Windows](#)

[Protocolos comunes de autenticación](#)

[Servicios de autenticación](#)

[Implementación de la autenticación](#)

[Cuentas de usuario](#)

[Fichas](#)

[Mirando la biometría](#)

[Autenticación basada en certificados](#)

[Servicios de autenticación/federación basados en notificaciones](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de auto comprobación](#)

[11 Autorización y control de acceso](#)

[Introducción al control de acceso](#)

[Tipos de controles de seguridad](#)

[Negación implícita](#)

[Revisión de los principios de seguridad/conceptos generales](#)

[Esquemas de control de acceso](#)

[Control de acceso discrecional](#)

[Control de acceso obligatorio](#)

[Control de acceso basado en roles](#)

[Ejercicio 11-1: Asignación de un usuario al rol sysadmin](#)

[Control de acceso basado en reglas](#)

[Control de acceso basado en grupos](#)

[Control de acceso basado en atributos](#)

[Otras herramientas de control de acceso](#)

[Implementación del control de acceso](#)

[Identidades](#)

[Tipos de cuenta](#)

[Uso de grupos de seguridad](#)

[Ejercicio 11-2: Configuración de grupos de seguridad y asignación de permisos](#)

[Derechos y privilegios](#)

[Ejercicio 11-3: Modificación de derechos de usuario en un sistema Windows](#)

[Seguridad del sistema de archivos y seguridad de la impresora](#)

[Listas de control de acceso](#)

[Directivas de grupo](#)

[Ejercicio 11-4: Configuración de directivas de contraseñas a través de directivas de grupo](#)

[Seguridad de la base de datos](#)

[Ejercicio 11-5: Cifrado de información confidencial en la base de datos](#)

[Restricciones de la cuenta](#)

[Aplicación de la directiva de cuentas](#)

[Supervisión del acceso a la cuenta](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[12 Introducción a la criptografía](#)

[Introducción a los servicios de criptografía](#)

[Comprender la criptografía](#)

[Algoritmos y claves](#)

[Ejercicio 12-1: Cifrado de datos con el cifrado César](#)

[Otros términos de criptografía](#)

[Cifrado simétrico](#)

[Conceptos de cifrado simétrico](#)

[Algoritmos de cifrado simétrico](#)

[Ejercicio 12-2: Cifrado de datos con el algoritmo AES](#)

[Cifrado asimétrico](#)

[Conceptos de cifrado asimétrico](#)

[Algoritmos de cifrado asimétrico](#)

[Criptografía cuántica](#)

[Intercambio de claves en banda frente a intercambio de claves fuera de banda](#)

[Descripción del hash](#)

[Conceptos de hash](#)

[Algoritmos hash](#)

[Ejercicio 12-3: Generación de hashes para verificar la integridad](#)

[Identificación de los usos del cifrado](#)

[Casos de uso comunes](#)

[Comprender las limitaciones](#)

[Cifrado de datos](#)

[Cifrado de la comunicación](#)

[Entendiendo la esteganografía](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[13 Administración de una infraestructura de clave pública](#)

[Introducción a la infraestructura de clave pública](#)

[Descripción de la terminología de PKI](#)

[Autoridad de Certificación y Autoridad de Registro](#)

[Depósito](#)

[Administración de una infraestructura de clave pública](#)

[Ciclo de vida del certificado](#)

[Listas de revocación de certificados y OCSP](#)

[Otros términos de PKI](#)

[Implementación de una infraestructura de clave pública](#)

[Cómo funciona SSL/TLS](#)

[Cómo funcionan las firmas digitales](#)

[Creación de una PKI](#)

[Ejercicio 13-1: Instalación de una entidad emisora de certificados](#)

[Ejercicio 13-2: Habilitación de SSL para un sitio web](#)

[Administración de una PKI](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

14 Seguridad física

Elegir una ubicación comercial

Preocupaciones de las instalaciones

Iluminación y ventanas

Puertas, ventanas y paredes

Preocupaciones de seguridad

Controles de acceso físico

Ejercicio 14-1: Obtener acceso a un sistema sin seguridad física

Esgrima y Personal

Bloqueos de hardware/Tipos de bloqueo

Sistemas de acceso

Otros controles de seguridad física

Listas y registros de acceso físico

Videovigilancia

Tipos de sensores

Implementación de controles ambientales

Comprender hvac

Blindaje

Extinción de incendios

Resumen de la certificación

✓ Simulacro de dos minutos

Preguntas y respuestas

[Respuestas de autocomprobación](#)

[15 Ataques a aplicaciones y seguridad](#)

[Descripción de los ataques a las aplicaciones](#)

[Recorrido de directorios](#)

[Ejercicio 15-1: Explotación de un servidor web IIS con Directory Traversal](#)

[Ataques de inyección](#)

[Ejercicio 15-2: Ataques de inyección SQL](#)

[Ataques de desbordamiento de búfer](#)

[Secuencias de comandos entre sitios](#)

[Falsificación de solicitudes entre sitios](#)

[Pasar el Hash](#)

[Escalada de privilegios](#)

[SSL Stripping](#)

[Manipulación y refactorización de controladores](#)

[Otros ataques a aplicaciones](#)

[Por qué existen vulnerabilidades en las aplicaciones](#)

[Conceptos de desarrollo seguro de aplicaciones](#)

[Conceptos de codificación segura](#)

[Entornos de aplicaciones](#)

[Técnicas de codificación segura](#)

[Marcos de aplicaciones y secuencias de comandos](#)

[Implementar la seguridad de host y aplicaciones](#)

[Seguridad del host](#)

[Seguridad de las aplicaciones](#)

[Calidad y pruebas del código](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[16 Virtualización y seguridad en la nube](#)

[Virtualización y seguridad de virtualización](#)

[Introducción a la virtualización](#)

[Beneficios de la virtualización](#)

[Hipervisor](#)

[Problemas de seguridad con la virtualización](#)

[Conceptos de computación en la nube](#)

[Descripción general de la computación en la nube](#)

[Consideraciones sobre la computación en la nube](#)

[Resiliencia y automatización](#)

[Características de la nube](#)

[Soluciones de ciberseguridad para la nube](#)

[Controles de seguridad en la nube](#)

[Soluciones de seguridad en la nube](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[17 Análisis de riesgos](#)

[Introducción al Análisis de Riesgos](#)

[Visión general del análisis de riesgos](#)

[Proceso de análisis de riesgos](#)

[Herramientas para ayudar a analizar el riesgo](#)

[Riesgo con Cloud Computing y Terceros](#)

[Tipos de evaluación de riesgos](#)

[Cualitativo](#)

[Ejercicio 17-1: Realización de un análisis cualitativo de riesgos](#)

[Cuantitativo](#)

[Ejercicio 17-2: Realización de un análisis cuantitativo de riesgos](#)

[Estrategias de mitigación de riesgos](#)

[Ejercicio 17-3: Identificación de técnicas de mitigación](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

18 Recuperación ante desastres y continuidad del negocio

[Introducción a la continuidad del negocio y la recuperación ante desastres](#)

[Introducción a la Continuidad del Negocio](#)

[Comprender la recuperación ante desastres](#)

[Copia de seguridad y restauración de datos: conceptos de copia de seguridad](#)

[Medios de destino de copia de seguridad](#)

[Consideraciones de seguridad con cintas](#)

[Tipos de copias de seguridad](#)

[Programación de copias de seguridad](#)

[Ejercicio 18-1: Copia de seguridad y restauración de datos en un servidor Windows Server](#)

[Consideraciones geográficas](#)

[Implementación de la tolerancia a fallos](#)

[Introducción a la redundancia](#)

[No persistencia y diversidad](#)

[Descripción de RAID](#)

[Ejercicio 18-2: Configuración de RAID 0 en un sistema Windows](#)

[Ejercicio 18-3: Creación de un volumen reflejado en un servidor Windows Server](#)

[Ejercicio 18-4: Creación de un volumen RAID 5 en un servidor Windows](#)

[Descripción de la alta disponibilidad](#)

[Clústeres de conmutación por error](#)

[Equilibrio de carga de red](#)

[Hardware redundante](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[19 Comprensión de la supervisión y la auditoría](#)

[Introducción a la supervisión](#)

[Herramientas de monitoreo](#)

[Comandos útiles del sistema](#)

[SNMP](#)

[Monitor de rendimiento](#)

[Analizador de protocolos y Sniffer](#)

[Ejercicio 19-1: Supervisión del tráfico de red con Wireshark](#)

[Descripción de Syslog](#)

[Información de seguridad y gestión de eventos](#)

[Trabajar con SOAR](#)

[Implementación del registro y la auditoría](#)

[Descripción de la auditoría](#)

[Ejercicio 19-2: Implementación de auditorías en Windows](#)

[Descripción del registro](#)

[Ejercicio 19-3: Configuración del registro en IIS](#)

[Ejercicio 19-4: Configuración de Firewall de Windows](#)

[Áreas populares para auditar](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)

[20 evaluaciones y auditorías de seguridad](#)

[Comprender los tipos de evaluaciones](#)

[Tipos de evaluación](#)

[Técnicas de evaluación](#)

[Realización de una evaluación de seguridad](#)

[Caza de amenazas](#)

[Análisis de vulnerabilidades](#)

[Ejercicio 20-1: Búsqueda manual de CVE para vulnerabilidades de Windows 10](#)

[Realización de una prueba de penetración](#)

[Consideraciones y técnicas utilizadas en una prueba de penetración](#)

[Comprender el proceso de piratería](#)

[Ejercicio 20-2: Creación de perfiles de una organización](#)

[Ejercicio 20-3: Uso de un escáner de puertos](#)

[Pasos para realizar una prueba de penetración](#)

[Realización de una evaluación de vulnerabilidades](#)

[Ejercicio 20-4: Realización de un análisis de vulnerabilidades con Nessus](#)

[Herramientas utilizadas para evaluar la seguridad](#)

[Herramientas fundamentales](#)

[Reconocimiento y descubrimiento de redes](#)

[Manipulación de archivos](#)

[Entornos de shell y script](#)

[Captura y reproducción de paquetes](#)

[Otras herramientas comunes](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autoevaluación](#)

[21 Respuesta a incidentes e informática forense](#)

[Trabajar con evidencia](#)

[Admisibilidad](#)

[Tipos de evidencia](#)

[Recopilación de pruebas](#)

[Recopilación de evidencia digital](#)

[Comprender el proceso](#)

[Dónde encontrar evidencia](#)

[Herramientas utilizadas](#)

[Ejercicio 21-1: Uso de FTK Imager para capturar una imagen de la unidad de un sospechoso](#)

[Ejercicio 21-2: Uso de FTK Imager para crear una imagen del contenido de la memoria](#)

[Ejercicio 21-3: Uso de FTK Imager para localizar archivos eliminados](#)

[Ejercicio 21-4: Uso de la autopsia para investigar el disco local](#)

[Ejercicio 21-5: Uso de FTK Imager para ver encabezados de archivo](#)

[Ejercicio 21-6: Realización de análisis forenses de teléfonos celulares](#)

[Ejercicio 21-7: Mirar los metadatos exif](#)

[Local vs. Nube](#)

[Mirando la respuesta a incidentes](#)

[Equipo de Respuesta a Incidentes](#)

[Plan de respuesta a incidentes](#)

[Proceso de respuesta a incidentes](#)

[Primeros respondedores](#)

[Control de daños y pérdidas](#)

[Ejercicios](#)

[Políticas y procedimientos para la respuesta a incidentes](#)

[Fuentes de datos para apoyar una investigación](#)

[Técnicas de mitigación como respuesta a un incidente](#)

[Resumen de la certificación](#)

[✓ Simulacro de dos minutos](#)

[Preguntas y respuestas](#)

[Respuestas de autocomprobación](#)