Networking Academy

Fundamentos de Ciberseguridad

Alcance y Secuencia

Versión 3.0

Contenido

Introducción

Cada día, las amenazas a la ciberseguridad crecen en complejidad y escala. En su publicación Informe de riesgos globales (2021), incluso el Foro Económico Mundial incluyó la falla de la seguridad cibernética entre los 5 principales riesgos globales, junto con amenazas como el clima extremo y las enfermedades infecciosas. Al mismo tiempo, las organizaciones de todo el mundo buscan nuevos talentos en ciberseguridad. Sin embargo, debido a una brecha de habilidades, es probable que los 3,5 millones de trabajos de seguridad cibernética previstos en todo el mundo queden sin cubrir para 2025. Los educadores son fundamentales para ayudar a cerrar esta brecha de habilidades al impulsar los viajes profesionales de seguridad cibernética de sus estudiantes. Fundamentos de Ciberseguridad 3.0 ha sido diseñado para ayudar a los educadores a preparar a los estudiantes para que den el primer paso en su trayectoria profesional en ciberseguridad. Después de completar el curso, los estudiantes pueden encontrar puestos de trabajo como Analista de seguridad cibernética junior, Técnico de seguridad cibernética, Soporte de seguridad cibernética, Especialista en seguridad cibernética o Soporte de mesa de ayuda de nivel 1. O bien, pueden continuar su educación hacia roles de trabajo de seguridad cibernética de nivel asociado y profesional con cursos como CyberOps Associate, Network Security, etc.

Público al que está destinado

El curso Fundamentos de Ciberseguridad 3.0 está diseñado para los estudiantes como un punto de partida para las carreras de ciberseguridad. Equipa a los alumnos con habilidades laborales de nivel de entrada en los dominios de tres cursos: seguridad de puntos finales, defensa de redes y administración de amenazas cibernéticas. Estos dominios brindan una experiencia de aprendizaje integrada y completa para un rol de analista de ciberseguridad junior de nivel de entrada. Los temas del curso incluyen amenazas y ataques de ciberseguridad, mitigación de amenazas, vulnerabilidades en protocolos y servicios de red, seguridad de puntos finales de Linux y Windows, medidas y arquitecturas de defensa de red comunes, administración de vulnerabilidades y riesgos, y respuesta a incidentes de ciberseguridad. El curso incluye laboratorios prácticos que utilizan máquinas virtuales, actividades de Packet Tracer y experiencias de laboratorio basadas en la investigación. El curso es apropiado para estudiantes de muchas edades y niveles educativos, principalmente en escuelas secundarias, universidades y ONG que se enfocan en oportunidades de capacitación.

Requisitos

Se espera que los estudiantes tengan las siguientes destrezas:

- Nivel de lectura de escuela secundaria
- Conocimientos básicos de la computadora
- Habilidades básicas de navegación del sistema operativo de la computadora
- Habilidades básicas de uso de Internet
- Conocimiento de redes TCP/IP, incluidos protocolos de red, servicios, procesos y configuración básica de dispositivos de red, como enrutadores y conmutadores.

Coordinación con las certificaciones

Este curso se alinea con los objetivos de certificación de ciberseguridad del Técnico de Soporte Certificado de Cisco (CCST).

Descripción del curso

En este curso, los alumnos desarrollan habilidades de preparación para la fuerza laboral y construyen una base para el éxito en carreras relacionadas con la seguridad cibernética. Con video y soporte de medios interactivos

enriquecidos, los participantes aprenderán y practicarán el conocimiento y las habilidades de ciberseguridad mediante una serie de experiencias prácticas y actividades simuladas que reforzarán el aprendizaje.

Fundamentos de Ciberseguridad enseña conceptos y habilidades integrales de ciberseguridad en el nivel de entrada, desde la mitigación y defensa de amenazas hasta el análisis forense posterior a un incidente. Los estudiantes avanzarán desde conceptos básicos de ciberseguridad hasta experiencias en la evaluación de vulnerabilidades y riesgos más adelante en el plan de estudios.

Fundamentos de Ciberseguridad incluye las siguientes características:

- Este curso consta de tres dominios.
- Los tres dominios se alinean con el conocimiento común, las habilidades y las capacidades requeridas en la fuerza laboral de seguridad cibernética en el nivel de entrada.
- Cada curso se compone de múltiples módulos. Cada módulo consta de varios temas.
- Cada módulo incluye una evaluación interactiva Verifique su Comprensión, una actividad de autoevaluación interactiva o alguna otra forma de evaluar la comprensión, como un cuestionario de opción múltiple, un laboratorio o una actividad de Packet Tracer. Estas evaluaciones están diseñadas para decirles a los alumnos si dominan bien el contenido del módulo o si necesitan repasarlo antes de continuar. Los estudiantes pueden asegurar su nivel de comprensión mucho antes de tomar un cuestionario o examen calificado. Los cuestionarios de verificación de la comprensión no afectan la calificación general del estudiante.
- Los estudiantes aprenden los conceptos básicos de un conjunto integral de habilidades que llevan a cabo los miembros del equipo de ciberseguridad en una amplia gama de organizaciones.
- El lenguaje utilizado para describir los conceptos de ciberseguridad está diseñado para ser entendido fácilmente por los alumnos de todos los niveles, y las actividades interactivas incorporadas ayudan a reforzar la comprensión.
- Las evaluaciones y las actividades prácticas se centran en competencias específicas para aumentar la retención y proporcionar flexibilidad en el curso.
- Las herramientas de aprendizaje multimedia, como los videos, los juegos y los cuestionarios, abordan diversos estilos de aprendizaje y ayudan a estimular el aprendizaje y a promover una mayor retención del conocimiento.
- Las prácticas de laboratorio y las actividades de aprendizaje basadas en la simulación de Cisco® Packet racer ayudan a los alumnos a desarrollar el pensamiento crítico y las destrezas para la resolución de problemas complejos.
- Los exámenes incorporados proporcionan un panorama inmediato que sirve de apoyo a la evaluación del conocimiento y las destrezas adquiridas.
- Las actividades de Cisco Packet Tracer están diseñadas para su uso con la versión más reciente de Packet tracer.

Objetivos del curso

Fundamentos de Ciberseguridad está diseñado para estudiantes que desean comenzar su carrera profesional en ciberseguridad. Fundamentos de Ciberseguridad prepara a los estudiantes para dar su primer paso hacia el nivel de entrada o continuar su educación hacia roles de trabajo de nivel asociado y profesional. Este material del curso lo ayudará a desarrollar las aptitudes necesarias para realizar lo siguiente:

- Explicar cómo los agentes de amenazas ejecutan algunos de los tipos más comunes de ataques cibernéticos.

- Explicar los principios de seguridad de la red.
- Explicar cómo las vulnerabilidades de TCP/IP permiten los ataques a las redes.
- Recomendar medidas para mitigar las amenazas.
- Solucionar problemas de una red inalámbrica.
- Explique cómo se emplean los dispositivos y servicios para reforzar la seguridad de las redes.
- Utilizar herramientas administrativas de Windows.
- Implementar seguridad básica en Linux.
- Evaluar la protección de terminales y los impactos del malware.
- Utilizar las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.
- Explicar métodos para defender la seguridad de las redes.
- Implementar algunos de los diversos aspectos de la defensa de sistemas y redes.
- Configurar el control de acceso local y basado en el servidor.
- Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red.
- Explicar cómo se implementan los firewalls para proporcionar seguridad de red.
- Implementar un firewall de políticas basado en zonas mediante CLI.
- Recomendar requisitos de seguridad en la nube basados en un escenario de nube determinado.
- Determinar las técnicas criptográficas necesarias para garantizar la confidencialidad, la integridad y la autenticidad.
- Explicar cómo las tecnologías de seguridad afectan el monitoreo de la seguridad.
- Utilizar diferentes tipos de registros y registros para almacenar información sobre hosts y la red.
- Explicar el proceso de evaluación de alertas.
- Crear documentos y políticas relacionados con el cumplimiento y la gobernanza de la ciberseguridad.
- Utilizar herramientas para las pruebas de seguridad de la red.
- Evaluar las fuentes de inteligencia de amenazas.
- Explicar cómo se evalúan y administran las vulnerabilidades de los dispositivos finales.
- Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos.
- Utilizar modelos de respuesta ante incidentes y técnicas forenses para investigar incidentes de seguridad.

Requisitos de Equipo

Los laboratorios prácticos requieren computadoras capaces de ejecutar software de virtualización (VirtualBox o UTM) con al menos 4 GB de RAM y 20 GB de espacio libre en disco. Los laboratorios que requieren entornos de red más complejos utilizan la herramienta de simulación de red Packet Tracer. Otras experiencias de aprendizaje requieren una investigación enfocada basada en Internet y la finalización de documentos de laboratorio.

Equipo de laboratorio opcional:

- Host con Microsoft Windows

Software:

- Oracle Virtual Box o UTM
- Archivo OVA de máquina virtual de laboratorio
- Packet Tracer 8.2.1 o superior

Esquema del curso

El primer dominio, Seguridad de Terminales, presenta conceptos fundamentales críticos en ciberseguridad, como ataques comunes y atacantes; amenazas, vulnerabilidades y riesgos; tendencias actuales en ciberseguridad; vulnerabilidades de servicios y protocolos de red, terminales de Windows y Linux; y mitigación de amenazas y defensa. Al final del curso, los estudiantes pueden identificar amenazas comunes y técnicas de mitigación, usar los conceptos de amenaza, vulnerabilidad y riesgo, y adquirir experiencia en el análisis de ataques comunes, operación y seguridad de terminales y malware.

El segundo dominio, Defensa de la Red, introduce conceptos fundamentales críticos en ciberseguridad, como defensa de sistemas y redes, control de acceso, firewalls, seguridad en la nube, aplicaciones de criptografía, datos de seguridad de redes y evaluación de alertas de seguridad. Al final del curso, los estudiantes pueden implementar medidas defensivas y control de acceso, configurar un firewall simulado, usar diferentes tipos de datos de red y evaluar alertas de seguridad.

El tercer dominio, Administración de Amenazas Cibernéticas, presenta conceptos fundamentales críticos en seguridad cibernética, como ética y gobierno, pruebas de seguridad de redes, inteligencia de amenazas, evaluación de vulnerabilidades de puntos finales, administración de riesgos y respuesta posterior a incidentes. Al final del curso, los alumnos estarán preparados para participar en una amplia gama de actividades de administración de amenazas y respuesta a incidentes como miembros de un equipo de operaciones de ciberseguridad.

A continuación se enumeran el conjunto actual de módulos y sus competencias asociadas. Cada módulo es una unidad de aprendizaje integrada que consta de contenido, actividades y evaluaciones que se enfocan en un conjunto específico de competencias. El tamaño del módulo dependerá de la profundidad de los conocimientos y las destrezas necesarias para dominar la competencia.

Tabla 1: Título del Módulo y Objetivo

Título del Módulo / Título del Tema	Objetivo
Dominio Uno: Seguridad de Dispositivos Finales	
Módulo 1: Amenazas, Vulnerabilidades y Ataques a la Ciberseguridad	Explicar cómo los agentes de amenazas ejecutan algunos de los tipos más comunes de ataques cibernéticos.
1.1 Amenazas Comunes	Explicar las amenazas, las vulnerabilidades y los ataques que se producen en los diversos dominios.
1.2 Engaño	Identificar los diferentes métodos de engaño utilizados por los atacantes para engañar a sus víctimas.
1.3 Ciberataques	Describir los ataques de red habituales
1.4 Ataques a Dispositivos Inalámbricos y Móviles	Describir los tipos comunes de ataques de dispositivos móviles e inalámbricos.
1.5 Ataques a las Aplicaciones	Describir los tipos de ataques a aplicaciones.
Módulo 2: Protección de Redes	Explicar los principios de seguridad de la red.
2.1 Estado Actual de los Asuntos	Describir el panorama actual de amenazas contra la seguridad
2.2 ¿Quién está atacando nuestra red?	Explicar cómo han evolucionado las amenazas de red.
Módulo 3: Ataque a los fundamentos	Explicar cómo las vulnerabilidades de TCP/IP permiten los ataques a redes.
3.1 Detalles de la PDU de IP	Explicar la estructura del encabezado IPv4 e IPv6.
3.2: Vulnerabilidades de IP	Explicar cómo las vulnerabilidades de IP permiten los ataques a redes.
3.3 Vulnerabilidades de TCP y UDP	Explicar cómo las vulnerabilidades de TCP y UDP permiten los ataques a redes.
Módulo 4: Atacando lo que Hacemos	Recomendar medidas para mitigar las amenazas.

4.1: Servicios IP	Explicar las vulnerabilidades del servicio IP.
4.2 Servicios Empresariales	Explicar cómo las vulnerabilidades de IP permiten los ataques a redes.
4.3 Mitigando los Ataques de Red Comunes	Recomendar medidas básicas de mitigación de amenazas.
Módulo 5: Dispositivos de comunicación de red inalámbrica	Solucionar problemas de una red inalámbrica.
5.1 Comunicaciones Inalámbricas	Explicar cómo los dispositivos de red inalámbrica permiten la comunicación por redes.
5.2 Amenazas a la WLAN	Describir las amenazas a las WLAN.
5.3 WLAN Seguras	Solucionar problemas de una conexión inalámbrica.
Módulo 6: Infraestructura de Seguridad de Red	Explicar cómo se emplean los dispositivos y servicios para reforzar la seguridad de las redes.
6.1 Dispositivos de Seguridad	Explicar cómo se emplean los dispositivos para reforzar la seguridad de las redes.
6.2 Servicios de Seguridad	Explicar cómo los servicios mejoran la seguridad de las redes.
Módulo 7: El Sistema Operativo Windows	Utilizar herramientas administrativas de Windows.
7.1 Historia de Windows	Describir la historia del sistema operativo Windows.
7.2 Arquitectura y operaciones de Windows	Explicar la arquitectura de Windows y su funcionamiento.
7.3 Configuración y Monitoreo de Windows	Usar herramientas administrativas de Windows para configurar, monitorear y administrar los recursos del sistema.
7.4 Seguridad de Windows	Explicar cómo Windows se puede mantener seguro.
Módulo 8: Descripción General de Linux	Implementar seguridad básica de Linux.
8.1 Conceptos Básicos de Linux	Explicar por qué las funciones de Linux son esenciales para investigación y monitoreo de seguridad de la red.
8.2 Trabajando en el Shell de Linux	Utilizar el shell de Linux para manipular los archivos de texto.
8.3 Servidores y Clientes de Linux	Utilizar la línea de comandos de Linux para identificar los servidores que se ejecutan en una computadora.
8.4 Administración Básica del Servidor	Utilizar comandos para ubicar y monitorear archivos de registro.
8.5 El Sistema de Archivos de Linux	Usar comandos para administrar el sistema de archivos y los permisos de Linux.
8.6 Trabajando con la GUI de Linux	Explicar los componentes básicos de la GUI de Linux.
8.7 Trabajando en un Host de Linux	Utilizar herramientas para detectar malware en un host de Linux.
Módulo 9: Protección de Sistemas y Dispositivos Finales	Evaluar la protección de terminales y los impactos del malware.
9.1 Defensa de Sistemas y Dispositivos	Utilizar procesos y procedimientos para proteger los sistemas.
9.2 Protección Antimalware	Explicar los métodos de mitigación de malware.
9.3 Prevención de Intrusiones Basada en Host	Recomendar medidas de seguridad para terminales.
9.4 Seguridad de las Aplicaciones	Utilizar herramientas de investigación de malware para conocer las características del malware.
Módulo 10: Principios, Prácticas y Procesos de Ciberseguridad	Utilizar las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.
10.1 Las Tres Dimensiones	Utilizar hash para verificar la integridad de los archivos.
10.2 Estados de Datos	Comparar los tres estados de datos.
10.3 Contramedidas de Ciberseguridad	Comparar los tipos de contramedidas de la ciberseguridad.
Dominio Dos: Defensa de la red	
Módulo 11: Comprender la Defensa	Explicar métodos para defender la seguridad de las redes.
11.1 Defensa en Profundidad	Explicar cómo se utiliza la estrategia de defensa en profundidad para proteger las redes.
11.2 Administración de Operaciones de Ciberseguridad	Explicar cómo una organización monitorea las amenazas de ciberseguridad.
11.3 Políticas, Regulaciones y Estándares de Seguridad	Explicar políticas, regulaciones y estándares de seguridad.

Módulo 12: Defensa del Sistema y de la Red	Implementar algunos de los diversos aspectos de la defensa de sistemas y redes.
12.1 Seguridad Física	Explicar cómo se implementan las medidas de seguridad físicas para proteger el equipo de red.
12.2 Seguridad de la aplicación	Explicar cómo aplicar las medidas de seguridad de las aplicaciones.
12.3 Fortalecimiento de la red: Servicios y Protocolos	Explicar cómo fortalecer los servicios y protocolos de red.
12.4 Fortalecimiento de la Red: Segmentación	Explicar cómo la segmentación de la red puede ayudarlo a fortalecerla.
12.5 Fortalecimiento de Dispositivos Inalámbricos y Móviles	Configurar el fortalecimiento y la seguridad del router inalámbrico.
12.6 Resiliencia de Ciberseguridad	Explicar la seguridad física con los dispositivos de IoT.
12.7 Sistemas Integrados y Especializados	Implementar seguridad física con dispositivos de IoT.
Módulo 13: Control de Acceso	Configurar el control de acceso local y basado en el servidor.
13.1 Controles de acceso	Configurar el acceso seguro en un host.
13.2 Conceptos del Control de Acceso	Explicar cómo el control de acceso protege los datos de la red.
13.3 Administración de Cuentas	Explicar la necesidad de la administración de cuentas y las estrategias de control de acceso.
13.4 Uso y funcionamiento de AAA	Configurar la autenticación basada en servidor con TACACS+ y RADIUS.
Módulo 14: Listas de control de acceso	Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red.
14.1 Introducción a las Listas de Control de Acceso	Describir las ACL IPv4 estándar y extendidas.
14.2 Uso de Máscaras de Comodín	Explicar la forma en que las ACL utilizan máscaras de comodín.
14.3 Configurar ACLs	Explicar cómo configurar una ACL.
14.4 Sintaxis de ACL Estándar con Nombre de IPv4	Utilizar números de secuencia para editar listas ACL IPv4 estándar ya existentes.
14.5 Implementar ACL	Implementar ACL.
14.6 Mitigar Ataques con ACL	Utilizar las ACL para mitigar los ataques de red comunes.
14.7 ACL de IPv6	Configurar ACL IPv6 usando la CLI.
Módulo 15: Tecnologías de Firewall	Explicar cómo se implementan los firewalls para proporcionar seguridad de red.
15.1 Redes Seguras con Firewalls	Explicar cómo se utilizan los firewalls para ayudar a proteger las redes.
15.2 Firewalls en el Diseño de Redes	Explicar las consideraciones de diseño para implementar tecnologías de firewall.
Módulo 16: Firewalls de política basados en zonas	Implementar un firewall de políticas basado en zonas mediante CLI.
16.1 Descripción general de ZPF	Explicar cómo se utilizan los firewalls de políticas basadas en zonas para ayudar a proteger una red.
16.2 Operación de ZPF	Explicar el funcionamiento de un firewall de Política Basada en la Zona.
16.3 Configurar una ZPF	Configurar un firewall de política basada en la zona con CLI.
Módulo 17: Seguridad en la Nube	Recomendar requisitos de seguridad en la nube basados en un escenario de nube determinado.
17.1 Virtualización y Computación en la Nube	Describir formas de gestionar las amenazas a la nube pública y privada.
17.2 Los Dominios de Seguridad en la Nube	Explicar los dominios de la seguridad en la nube.
17.3 Seguridad de la Infraestructura en la Nube	Explicar la mitigación de amenazas a la infraestructura de la plataforma en la nube.
17.4 Seguridad de Aplicaciones en la Nube	Recomendar aplicaciones de seguridad en la nube.
17.5 Seguridad de los datos en la nube	Explicar cómo proteger los datos en la nube.
17.6 Protección de máquinas virtuales	Explicar cómo proteger las instancias de máquina virtuales.
Módulo 18: Criptografía	Determinar las técnicas criptográficas necesarias para garantizar la confidencialidad, la integridad y la autenticidad.
18.1 Confidencialidad	Determinar el algoritmo de cifrado que se usará según los requisitos.

18.2 Ocultamiento de datos	Utilizar una técnica para ocultar datos.
18.3 Integridad y autenticidad	Explicar la función de la criptografía para garantizar la integridad y autenticidad de los datos.
18.4 Hash	Explicar cómo utilizar las herramientas de hash.
18.5 Criptografía de llave pública	Utilizar una firma digital.
18.6 Autoridades y sistema de confianza de la PKI	Utilizar el hashing para detectar la interceptación de la red.
18.7 Aplicaciones e impacto de la criptografía	Explicar cómo el uso de cifrado afecta a las operaciones de ciberseguridad.
Módulo 19: Tecnologías y protocolos	Explicar cómo las tecnologías de seguridad afectan el monitoreo de la seguridad.
19.1 Protocolos comunes de monitoreo	Explicar el comportamiento de los protocolos de red comunes en el contexto del monitoreo de la seguridad.
19.2 Tecnologías de seguridad	Explicar cómo afectan las tecnologías de seguridad a la capacidad de supervisar protocolos de red comunes.
Módulo 20: Datos de seguridad de red	Utilizar diferentes tipos de registros y registros para almacenar información sobre hosts y la red.
20.1 Tipos de datos de seguridad	Describir los tipos de datos empleados en el monitoreo de seguridad.
20.2 Registros de terminales	Describir los elementos de un archivo de registro de un terminal.
20.3 Registros de redes	Utilizar diferentes tipos de servicios para recopilar datos de la red.
Módulo 21: Evaluación de alertas	Explicar el proceso de evaluación de las alertas.
21.1 Fuente de alertas	Identificar la estructura de alertas.
21.2: Descripción general de la evaluación de las alertas	Explicar cómo se clasifican las alertas.
Dominio Tres: Administración de Amenazas Cibernéticas	
Módulo 22: Gobernanza y Cumplimiento	Crear documentos y políticas relacionados con el cumplimiento y la gobernanza de la ciberseguridad.
22.1 Gobernanza	Crear documentos de políticas de ciberseguridad.
22.2 La Ética de la Ciberseguridad	Crear un código personal de conducta ética.
22.3 Marco de Trabajo para la Administración de la Seguridad de TI	Evaluar los controles de seguridad.
Módulo 23: Pruebas de Seguridad de la Red	Utilizar herramientas para las pruebas de seguridad de la red.
23.1 Evaluaciones de Seguridad	Utilizar comandos para recopilar información de la red y diagnosticar problemas de conectividad.
23.2 Técnicas de Pruebas de Seguridad de la Red	Describir las técnicas utilizadas en las pruebas de seguridad de la red.
23.3 Herramientas de Pruebas de Seguridad de la Red	Describir las herramientas utilizadas en las pruebas de seguridad de la red.
23.4 Pruebas de penetración	Describir cómo una organización utiliza las pruebas de penetración para evaluar la seguridad del sistema.
Módulo 24: Inteligencia contra Amenazas	Evaluar las fuentes de inteligencia de amenazas.
24.1 Fuentes de información	Evaluar las fuentes de información utilizadas para comunicar las amenazas emergentes a la seguridad de la red.
24.2 Servicios de Inteligencia contra Amenazas	Describir varios servicios de inteligencia contra amenazas.
Módulo 25: Evaluación de vulnerabilidades de terminales	Explicar cómo se evalúan y administran las vulnerabilidades de los dispositivos finales.
25.1 Perfiles de redes y servidores	Explicar el valor de red y los perfiles de servidor.
25.2 Sistema de puntuación de vulnerabilidades comunes (CVSS)	Explicar cómo se utilizan los informes del CVSS para describir las vulnerabilidades de seguridad.
25.3 Administrador de dispositivos de seguridad	Explicar cuán seguras son las técnicas de administración de dispositivos para proteger los datos y activos.
Módulo 26: Gestión de Riesgos y Evaluación de Vulnerabilidad	Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos.
26.1 Administración de riesgos	Explicar la administración de riesgos

26.2 Evaluación de Riesgos	Calcular los Riesgos
26.3 Controles de Seguridad	Evaluar los controles de seguridad según las características de la organización.
Módulo 27: Análisis y respuesta de incidentes e informática forense digital	Utilizar modelos de respuesta ante incidentes y técnicas forenses para investigar incidentes de seguridad.
27.1 Manejo de evidencia y atribución del ataque	Explicar la función de los procesos forenses digitales.
27.2 Cadenas de Eliminación Cibernética	Identificar los pasos proporcionados en la cadena de eliminación cibernética.
27.3 Análisis del modelo de diamante de las intrusiones	Utilizar el Modelo de Diamante del Análisis de Intrusiones para clasificar los eventos de intrusión.
27.4 Respuesta a incidentes	Aplicar los procedimientos de manejo de incidente NIST 800-61r2 para una situación de incidentes determinada.
27.5 Recuperación ante desastres	Utilizar comandos para realizar copias de respaldo de archivos y restaurar operaciones de red.