Temarios Cyber Security

Preparado para:

Clientes

28 de mayo de 2021

Versión 1.2

Preparado por:

Rubén Guerrero

Director de Unidad de Negocios

rguerrero@compueducacion.mx

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

Contenido

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

Resumen Ejecutivo

El grupo EC Council se compone de varias entidades que ayudan a servir el mismo objetivo, que es la de crear un cyber mundo mejor, más seguro a través de la sensibilización y la educación. Nuestras entidades incluyen Consejo Internacional de Consultores de Comercio Electrónico (EC-Council), iClass, EC-Council Universidad, EC-Council Global Services y el EC-Council Conferencias y Eventos.

EC-Council crea contenido (los materiales del curso y los exámenes) y certificación entregado a través de nuestro canal de centros autorizados de capacitación que consta de más de 700 socios que representan a más de 2.000 ubicaciones físicas en más de 145 países de todo el mundo. Somos el dueño y desarrollador de la mundialmente famosa Certified Ethical Hacker (CEH), la Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) y programas de Licencia de Penetration Tester (LPT)(Master).

iClass es un programa de entrenamiento para certificación directa de EC-Council. iClass ofrece cursos de certificación EC-Council a través de diversas metodologías de capacitación: presencial en las instalaciones del cliente, entrega sincrónica a través de live, online y presencial y asincrónicamente a través de nuestra plataforma de video streaming. Los videos del curso iClass también pueden descargarse en un dispositivo móvil, como un iPad, y también se pueden enviar a la ubicación del cliente.

Un Vistazo de EC-Council

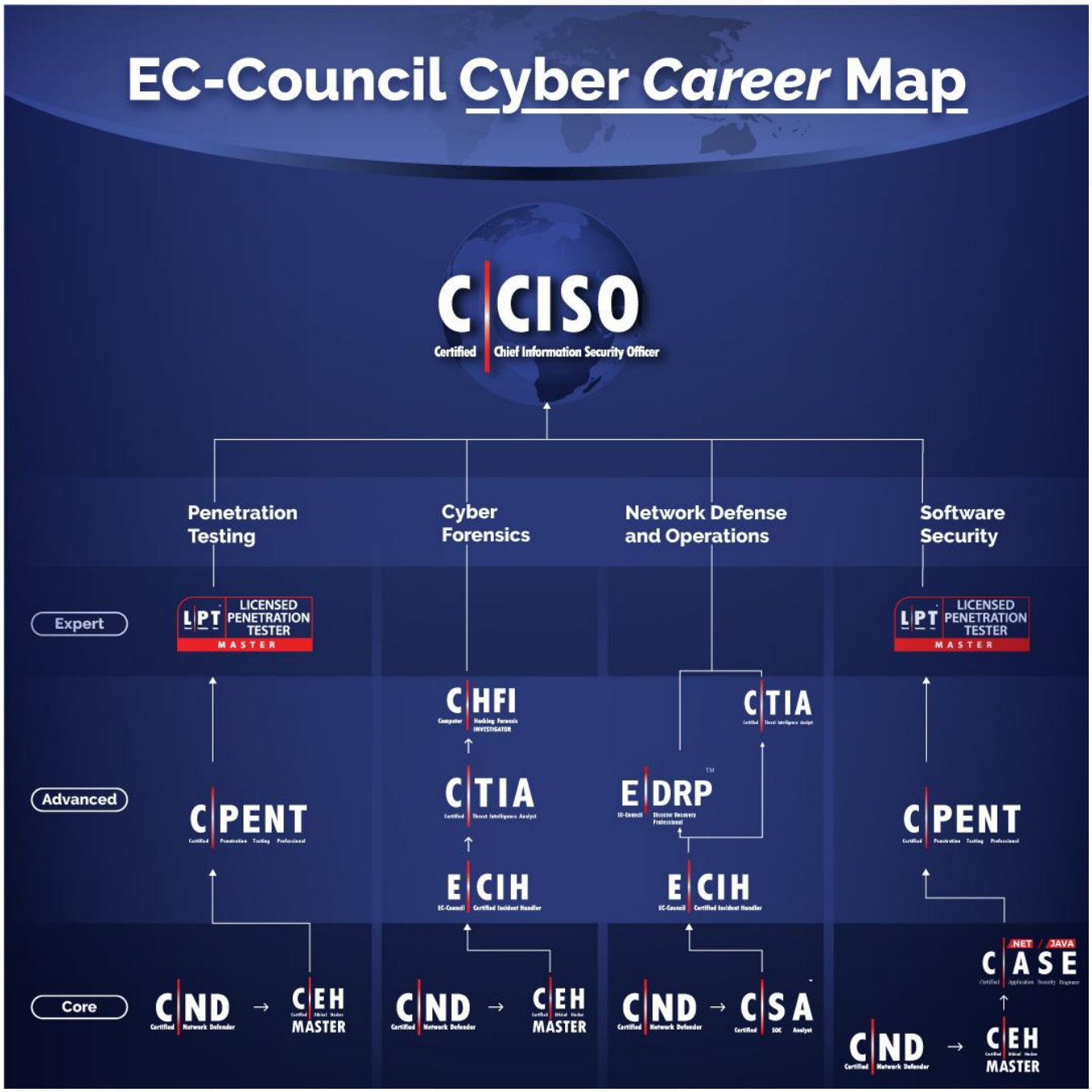
EC-Council Group es una institución multidisciplinaria de servicios profesionales mundiales de seguridad de la información.

EC-Council Group es una organización dedicada a la seguridad de la información que aspira a crear conocimientos, facilitar la innovación, la ejecución de la investigación, desarrollo, aplicación y nutrir los expertos en la materia con el fin de proporcionar habilidades únicas y conocimientos especializados en materia de seguridad cibernética.

Algunas de las mejores organizaciones de todo el mundo como el US Army, US Navy, DoD, el FBI, Microsoft, IBM, y las Naciones Unidas han confiado en EC-Council para desarrollar y mejorar su infraestructura de seguridad.

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García



Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

1 CEH v11: Certified Ethical Hacker (Ingles/Español)

CEH proporciona una comprensión profunda de las fases de piratería ética, varios vectores de ataque y contramedidas preventivas. Te enseñará cómo los hackers piensan y actúan maliciosamente para que estará mejor posicionado para configurar su infraestructura de seguridad y defender futuros ataques.

Comprender las debilidades y vulnerabilidades del sistema ayuda a las organizaciones a fortalecer sus controles de seguridad del sistema para minimizar el riesgo de un incidente.

CEH fue construido para incorporar un entorno práctico y un proceso sistemático en todos los dominios y metodología de piratería ética, dándole la oportunidad de trabajar para demostrar los conocimientos y habilidades necesarias para realizar el trabajo de un hacker ético. Usted tendrá una postura completamente diferente hacia las responsabilidades y medidas necesarias para estar seguro.

En su 11ª versión, CEH continúa evolucionando con los últimos sistemas operativos, herramientas, tácticas, exploits, y tecnologías. Aquí están algunas actualizaciones más importantes del CEH v11:

- Incorporación de Parrot Security OS
- Reasignado al marco NIST/NICE
- Módulos mejorados de seguridad en la nube, IoT y OT
    - Amenazas basadas en la nube
    - Amenazas de IoT
    - Ataques de Tecnología Operativa (OT)
- Análisis de malware moderno
- Cubriendo las últimas amenazas - Malware sin archivos
- Nuevos diseños de laboratorio y sistemas operativos
- Aumento del tiempo de laboratorio y el enfoque práctico
- Biblioteca de herramientas más completa de la industria

CEH v11 es el único curso en versión Inglés o Español (solo en el curso video streaming. Los materiales, laboratorios y examen existen solo en versión Inglés)

1.1 Resultados Clave

- Introducción exhaustiva al Ethical Hacker
- Exposición a vectores de amenazas y contramedidas
- Aborda el hackeo a las áreas emergentes de IoT, cloud y móviles
- Te prepara para combatir el malware, troyanos, puertas traseras, y más
- Le habilita para hackear mediante el dispositivo móvil

1.2 Temario

- Introducción al Ethical Hacking
- Footprinting y reconocimiento
- Escaneo de redes

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Enumeración
- Análisis de Vulnerabilidad
- Hackeo del sistema
- Amenazas de Malware
- Sniffing
- La ingeniería social
- Denegación de servicio
- El secuestro de sesiones
- Evasión de IDS, cortafuegos y Honeypots
- Hackeo de Servidores Web
- Hackeo de aplicaciones Web
- Inyección SQL
- Hackeo de redes inalámbricas
- Hackeo de plataformas móviles
- IoT & OT Hacking
- Cloud Computing
- Criptografía

1.3 Información del Examen

Título del Examen: Certified Ethical Hacker (ANSI)

- Código de examen: 312-50 (ECC), Examen 312-50 (VUE)
- Número de preguntas: 125
- Duración: 4 horas
- Disponibilidad: ECC Exam Portal, VUE
- Formato de Prueba: Opción múltiple
- Puntuación: Consulte https://cert.eccouncil.org/faq.html

Título del Examen: Certified Ethical Hacker (PRACTICAL)

- Número de Retos Prácticos: 20
- Duración: 6 horas
- Disponibilidad: ASPEN - iLabs
- Formato de Prueba: iLabs Cyber Range
- Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

2 CHFI:Computer Hacking Forensic Investigator

CHFI es un curso integral que cubre los principales escenarios de investigación forense, que permitirán a los estudiantes adquirir experiencia en la práctica.

El programa proporciona una sólida base de conocimientos de los principales conceptos y prácticas en el análisis forense digital dominios pertinentes para las organizaciones de hoy en día. Además, CHFI proporciona un sólido conocimiento en los dominios de análisis forense digital.

2.1 Resultados Clave

- Amplio proceso de investigación forense.
- Análisis forense de sistemas de archivos, sistemas operativos, redes y bases de datos, sitios web y sistemas de correo electrónico.
- Técnicas para investigar sobre cloud, malware y dispositivos móviles.
- Adquisición de datos y análisis, así como las técnicas anti-forense.
- profundo conocimiento de la cadena de custodia, el informe forense y la presentación.

2.2 Temario

- La informática forense en el mundo de hoy
- Proceso de investigación informática forense
- Comprensión de discos duros y sistemas de archivos
- Adquisición de datos y duplicación
- Derrotando Técnicas Anti-Forensics
- Forensia del Sistema Operativo
- Forensia de Red
- Investigando ataques Web
- Análisis Forense de la Base de Datos
- Forensia de la Nube
- Análisis forense del Malware
- Investigando crímenes de correo electrónico
- Forensia de Moviles
- Redacción y presentación del informe forense

2.3 Información del Examen

- Título del examen: Computer Hacking Forensic Investigator
- Código del examen: examen 312-49
- Número de preguntas: 150
- Duración: 4 horas
- Disponibilidad: Portal de Examen de ECC
- Formato de Prueba: Opción múltiple
- Puntuación: consulte Https://cert. eccouncil.org/faq.html

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

3 CBP: Certified Blockchain Professional

Blockchain, la piedra angular de una estrategia de descentralización, es una base de datos distribuída que es replicada a través de múltiples nodos para habilitar un inmutable, permanente, transparente y seguro registro de transacciones. Esencialmente, Blockchain un **sistema de validación de transacciones de datos y almacenamiento de datos auto-regulado**.

El curso **C|BP** provee una visión general profunda **100% a la mano** de la tecnología Blockchain y su implementación en el mundo real.

La certificación **C|BP** consiste de tres áreas del conocimiento y competencias en tecnología Blockchain: **Desarrollo**, **Implementación** y **Estrategia**.

Durante el curso, el estudiante no solo estará expuesto múltiples conceptos de implementación Blockchain, sino también estará inmerso en una guía única para desarrollo Blockchain sostenible y escalable con el uso de libros contables resistentes al quantum.

3.1 Resultados Clave

- Profundo entendimiento de la criptografía y cryptomonedas, libros contables distribuidos, descentralización y contratos inteligentes.
- Habilidad para construir poderosas y altamente seguras aplicaciones descentralizadas utilizando Ethereum para crear contratos inteligentes y facilitar transacciones “in-app” confiables.
- Habilidad para proveer soluciones innovadoras para resolver la adopción de la industria y los problemas de escalabilidad.

3.2 Temario

- Introduction: Blockchain technology
- Crypto assets
- Blockchain mining
- Bitcoin
- Sustainable Blockchain
- Open source business bockchain frameworks
- Hyperledger
- Ethereum
- Decentralized Applications (DApps)
- AI & Blockchain
- Impacto on Industry
- Industry use cases
- IoT & Blockchain
- Blockchain Project Implementation
- Scalable Blockchain
- Security in Blockchain (Secure Blockchain)
- Blockchain as a Service (BaaS)

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Open Research Problems in Blockchain

3.3 Información del Examen

- Título del examen: The Certified Blockchain Professional
- Código de examen: IIB-503
- Número de preguntas: 100
- Duración: 3 horas
- Disponibilidad: Portal Examen de ECC
- Formato de Prueba: Opción múltiple

4 CND v2: Certified Network Defender

¡El único programa de defensa de red del equipo azul!

La ciberseguridad domina ahora las prioridades de cada empresa que se esfuerza por adaptarse a un mundo post-COVID. Obligados a ir a distancia, las identidades y dispositivos de sus trabajadores son el nuevo perímetro de seguridad.

De hecho, la ciberseguridad para las empresas es ahora tan crítica como el propio acceso a Internet.

El único programa construido para el experimento más grande del mundo de trabajo en casa!

Estudios e informes de noticias han demostrado que los atacantes cibernéticos se apresuran a atacar a las nuevas, desprotegidas y amenazadas áreas sin protección, creadas cuando millones de empleados comenzaron a trabajar desde casa.

Proporcionar seguridad de red a un ecosistema distribuido sin precedentes en este mundo pospandémico, es la prueba de ácido de cada equipo de defensa de red.

El programa Certified Network Defender v2 ha sido actualizado y cargado con munición para ayudar a los “Blue Team” a defenderse y ganar la guerra contra las brechas de red. Los individuos y las corporaciones que buscan fortalecer sus habilidades de defensa de la red, encontrarán CND v2 un “deber tener” por 5 razones:

- Un solo programa integral de defensa de la red construido para incorporar habilidades seguras de red - Proteger, Detectar, Responder y Predecir.
- Mapas a NICE 2.0 Framework
- Viene repleto de las últimas herramientas, tecnologías y técnicas
- Implementa un enfoque práctico para el aprendizaje
- Diseñado con un enfoque mejorado en la predicción de amenazas, continuidad del negocio y recuperación ante desastres

4.1 Resultados Clave

- Conocimientos sobre cómo proteger, detectar y responder a los ataques de red.
- Fundamentos de defensa de la red.
- La aplicación de los controles de seguridad de la red perimetral, protocolos, electrodomésticos, Secure IDS, VPN y configuración del firewall.
- Intríncsecos de la firma del tráfico de red, análisis y escaneo de vulnerabilidades.

4.2 Temario

- Ataques de red y estrategias de defensa
- Seguridad de la red administrativa
- Seguridad técnica de la red
- Seguridad perimetral de la red

- Endpoint Security-Sistemas Windows
- Sistemas Endpoint Security-Linux
- Endpoint Security- Dispositivos móviles
- Dispositivos endpoint security-ioT
- Seguridad de la aplicación administrativa
- Seguridad de datos
- Seguridad de red virtual empresarial
- Seguridad de la red de Enterprise Cloud
- Seguridad de red inalámbrica empresarial
- Monitoreo y análisis de tráfico de red
- Monitoreo y análisis de registros de red
- Respuesta a incidentes e investigación forense
- Continuidad del negocio y recuperación ante desastres
- Anticipación del riesgo con gestión de riesgos
- Evaluación de amenazas con análisis de superficie de ataque
- Predicción de amenazas con inteligencia de amenazas cibernéticas

4.3 Información del Examen

- Título del Examen: Certified Network Defender
- Código de examen: 312-38
- Número de preguntas: 100
- Duración: 4 horas
- Disponibilidad: Portal Examen de ECC
- Formato de Prueba: Opción múltiple
- Puntuación: Consulte
- Puntuación: Consulte https://cert.eccouncil.org/faq.html

5 CPENT: Certified Penetration Testing Professional

El programa Certified Penetration Tester (CPENT) de EC-Council le enseña cómo realizar una prueba de penetración efectiva en un entorno de red empresarial que debe ser atacado, explotado, evadido y defendido. Si sólo ha estado trabajando en redes planas, la gama de práctica en vivo de CPENT le enseñará a llevar sus habilidades al siguiente nivel enseñándole cómo hacer pentesting en sistemas de IoT, en sistemas OT, cómo escribir sus propios exploits, construir sus propias herramientas, llevar a cabo la explotación de binarios avanzada, doble pivote para acceder a redes ocultas, y también personalizar scripts / exploits para entrar en los segmentos más íntimos de la red.

El corazón del programa CPENT es tratar de ayudarle a dominar sus habilidades de pentesting mediante su utilización en nuestros cyber range en vivo.

Los rangos CPENT fueron diseñados para ser dinámicos, con el fin de darle un programa de entrenamiento en un mundo real, por lo que así como los objetivos y la tecnología continúan cambiando en las redes en vivo, tanto la práctica CPENT como los rangos de exámenes, imitarán esta realidad a medida que nuestro equipo de ingenieros continúe añadiendo objetivos y defensas a lo largo de la vida útil del curso CPENT.

5.1 Resultados Clave

- 100% alineado con el framework NICE.
- Programa de pruebas de penetración 100% basado en metodología.
- Combina enfoques manuales y automatizados de pruebas de penetración.
- Diseñado con las prácticas de pruebas de penetración más comunes ofrecidas por los mejores proveedores de servicios.
- Mapas a todos los portales de trabajo principales. Título del rol: Penetration Tester & Security Analyst.
- Proporciona una guía sólida de escritura de informes.
- Ofrece una experiencia en el mundo real a través de un rango de pruebas de penetración avanzada.
- Proporciona a los candidatos una prueba de pluma estándar para su uso en el campo.

5.2 Temario

- Módulo 01: Introducción a las pruebas de penetración
- Módulo 02: Pruebas de penetración de alcance y participación
- Módulo 03: Inteligencia de código abierto (OSINT)
- Módulo 04: Pruebas de penetración de ingeniería social
- Módulo 05: Pruebas de penetración de red – Externa
- Módulo 06: Pruebas de penetración de red– Interno
- Módulo 07: Pruebas de penetración de red – Dispositivos perimetrales
- Módulo 08: Pruebas de penetración de aplicaciones web
- Módulo 09: Pruebas de penetración inalámbrica
- Módulo 10: Pruebas de penetración de IoT
- Módulo 11: Pruebas de penetración OT/SCADA
- Módulo 12: Pruebas de penetración en la nube
- Módulo 13: Análisis binario y explotación
- Módulo 14: Informar sobre las acciones de escritura y post-pruebas

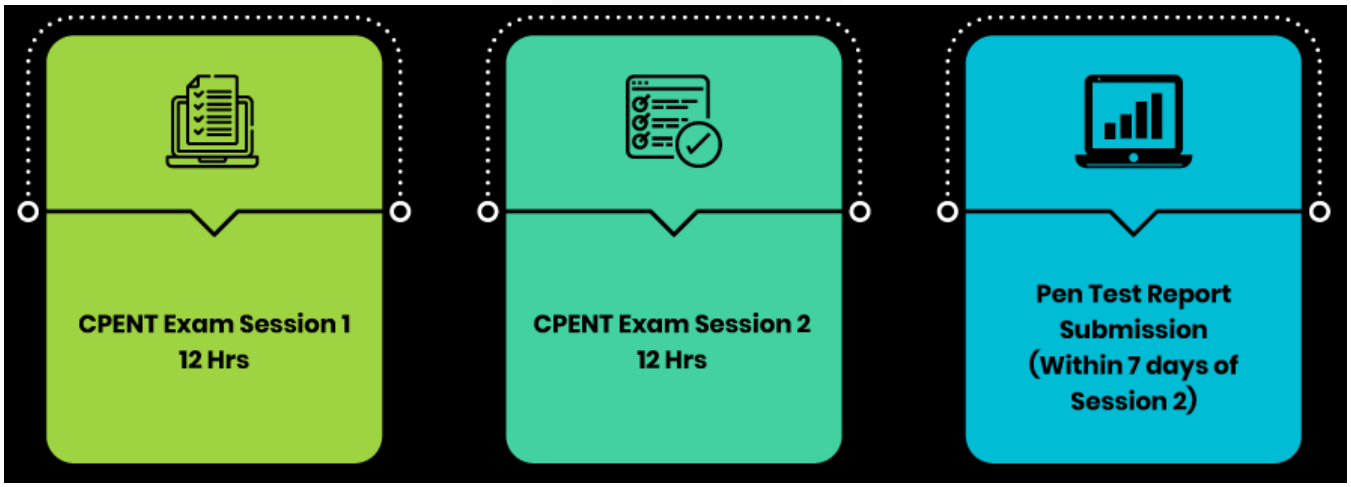
Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

5.3 Información del Examen

Características del examen:

- ¡Elige tu desafío! ¡Dos sesiones de 12 horas o un solo examen de 24 horas!
- Especialistas de EC-Council monitorean durante todo el examen; hacer trampa no es una opción.
- Logra un score de al menos un 70% y conviértete en un CPENT.
- ¡Consigue al menos el score de 90% y gana la muy respetada designación LPT (Master) adicional!
- Puntuación: Consulte https://cert.eccouncil.org/faq.html



Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

6 EDRP: EC-Council Disaster Recovery Professional

El curso de EDRP identifica vulnerabilidades y toma contramedidas apropiadas para prevenir y mitigar los riesgos de fracaso de una organización. También proporciona una base profesional de networking en curso de recuperación ante desastres principios, incluida la preparación de un plan de recuperación de desastres, evaluación de riesgos en la empresa, desarrollo de políticas y procedimientos, la comprensión de las funciones y relaciones de los diversos miembros de la organización, la ejecución de un plan, y recuperarse de un desastre.

6.1 Resultados Clave

- Introducción a la gestión de riesgos, continuidad del negocio y recuperación ante desastres.
- Gestión de desastres y emergencias, y la normativa aplicable.
- El proceso de planificación de recuperación ante desastres, la preparación, la recuperación de los sistemas e instalaciones.
- Respuesta a Incidentes y enlace con los servicios públicos y los órganos reguladores.
- Exposición a diversos servicios de gobierno y otras entidades.

6.2 Temario

- Introducción a la recuperación ante desastres y continuidad de negocio
- Gestión de la continuidad del negocio (BCM)
- Evaluación de riesgos
- Análisis de impacto en el negocio (BIA)
- Planificación de la continuidad del negocio (BCP)
- Estrategias de copia de seguridad de datos
- Estrategias de recuperación de datos
- Recuperación de desastres
- Virtualization-Based System Recovery
- Recuperación de sistemas centralizados y descentralizados
- Proceso de Planificación de recuperación de desastres
- Pruebas BCP, mantenimiento y formación

6.3 Información del Examen

Título del Examen: EC-Council Disaster Recovery Professional
Código de examen: 312-76
Número de preguntas: 150
Duración: 4 horas
Disponibilidad: Portal Examen ECC
Formato de Prueba: Opción múltiple
Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

7 CCISO: Certified Chief Information Security Officer

La Certificación C|CISO es un programa líder de la industria que reconoce la experiencia del mundo real necesaria para triunfar en los más altos niveles ejecutivos de la seguridad de la información. Reuniendo todos los componentes necesarios para una posición de nivel C, el programa C|CISO combina gestión de auditoría, la gobernanza, los controles, la gestión del capital humano, el desarrollo del programa estratégico y la pericia financiera vital para un líder exitoso es el programa. El programa de capacitación de C|CISO puede ser la clave para una transición exitosa a los rangos más altos de la gestión de la seguridad de la información.

7.1 Resultados Clave

- Establece la función del CISO y modelos de gestión
- Los conceptos básicos de los controles de seguridad de la información, gestión de riesgos y cumplimiento
- Crea fundación para el liderazgo a través de la planificación estratégica, la gestión de programas y la gestión de proveedores

7.2 Dominio

- Gobernanza y Administración de Riesgos
- Controles en Seguridad de Información, Cumplimientos y Gestión de Auditoría
- Administración y Operación del Programa de Seguridad
- Competencias Principales en Seguridad de la Información
- Planeación Estratégica, Finanzas, Provisionamiento y Gestión de Proveedores

7.3 Información del Examen

- Número de preguntas: 150
- Duración: 2,5 horas
- Formato de Prueba: elección múltiple

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

8 ECIHv2: EC-Council Certified Incident Handler

El programa EC-Council Certified Incident Handler está diseñado para proporcionar las habilidades fundamentales para manejar y responder a los incidentes de seguridad informática en un sistema de información. El curso aborda varios principios y técnicas subyacentes para detectar y responder a las amenazas de seguridad informática actuales y emergentes. Los estudiantes aprenderán cómo manejar varios tipos de incidentes, metodologías de evaluación de riesgos y varias leyes y políticas relacionadas con el manejo de incidentes. Después de asistir al curso, podrán crear políticas de manejo y respuesta a incidentes y lidiar con varios tipos de incidentes de seguridad informática.

8.1 Resultados Clave

- Principios, procesos y técnicas para detectar y responder a amenazas de seguridad/ infracciones
- Enlace con órganos jurídicos y reglamentarios
- Aprender a manejar incidentes y realizar evaluaciones
- Cubrir diversos incidentes como código malicioso, ataques a la red, y los ataques internos

8.2 Temario

Módulo 1: Introducción al manejo y Respuesta a Incidentes
Módulo 2: Proceso de Respuesta y Manejo de Incidentes
Módulo 3: Lectura Forense y Primeras Respuestas
Módulo 4: Manejo y respuesta de incidentes de código malicioso
Módulo 5: Manejo y respuesta de Incidentes de seguridad de correo electrónico
Módulo 6: Manejo y respuesta de Incidentes de seguridad de red
Módulo 7: Manejo y respuesta de Incidentes de seguridad de las aplicaciones Web
Módulo 8: Manejo y respuesta de Incidentes en la seguridad de la nube
Módulo 9: Manejo y respuesta de amenazas de intrusos

8.3 Información del Examen

- Título del examen: EC-Council Certified Incident Handler
- Código de examen: 212-89
- Número de preguntas: 100
- Duración: 3 horas
- Disponibilidad: Portal Examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

9 CSCU: Certified Secured Computer User

El propósito del programa de capacitación CSCU es proporcionar a los estudiantes los conocimientos y habilidades necesarios para proteger sus activos de información. Esta clase sumergirá a los estudiantes en un entorno interactivo en el que adquirirán una comprensión fundamental de varias amenazas de seguridad de la red y las computadoras, como el robo de identidad, el fraude con tarjetas de crédito, las estafas de phishing bancario en línea, virus y puertas traseras, correos electrónicos falsos, delincuentes sexuales que acechan en línea, pérdida de Información confidencial, ataques de piratería e ingeniería social. Más importante aún, las habilidades aprendidas de la clase ayudan a los estudiantes a tomar los pasos necesarios para mitigar su exposición a la seguridad.

9.1 Resultados Clave

- Fundamentos de diversas amenazas de seguridad informática y de redes
- Comprensión del robo de identidad, phishing, malware, ingeniería social, y fraudes financieros
- Aprender a salvaguardar el móvil, medios de comunicación y protección de datos
- Protección de ordenadores, cuentas y perfiles de redes sociales como usuario
- Comprender los incidentes de seguridad y presentación de informes

9.2 Temario

Módulo 1: Introducción a la seguridad de datos
Módulo 2: Seguridad de los sistemas operativos
Módulo 3: Malware y antivirus
Módulo 4: Seguridad en Internet
Módulo 5: La seguridad en los sitios de redes sociales
Módulo 6: Proteger las comunicaciones por correo electrónico
Módulo 7: Proteger los dispositivos móviles
Módulo 8: Asegurar la nube
Módulo 9: Asegurar conexiones de red
Módulo 10: Copia de seguridad de datos y recuperación ante desastres.

9.3 Información del Examen

- Título del examen: Certified Secure Computer User
- Código de examen: 112-12
- Número de preguntas: 50
- Duración: 2 horas
- Disponibilidad: Portal Examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

10 CTIA: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) está diseñado y desarrollado en colaboración con expertos en inteligencia de amenazas y ciberseguridad de todo el mundo para ayudar a las organizaciones a identificar y mitigar los riesgos empresariales mediante la conversión de amenazas internas y externas desconocidas en amenazas conocidas. Es un programa integral a nivel de especialistas que enseña un enfoque estructurado para desarrollar una inteligencia de amenazas efectiva.

En el panorama de amenazas en constante cambio, C | TIA es un programa esencial para aquellos que enfrentan las amenazas cibernéticas a diario. Las organizaciones de hoy exigen un analista de inteligencia de amenazas de ciberseguridad de nivel profesional que pueda extraer la inteligencia de los datos mediante la implementación de varias estrategias avanzadas. Dichos programas de nivel profesional solo se pueden lograr cuando el núcleo del currículo se asigna y cumple con los marcos de inteligencia de amenazas publicados por el gobierno y la industria.

C|TIA es un programa impulsado por el método que utiliza un enfoque integral, que abarca los conceptos de la planificación del proyecto de inteligencia de amenazas para la construcción de un informe para difundir Threat Intelligence. Estos conceptos son sumamente esenciales mientras se construye la inteligencia de amenaza efectiva y, cuando se utiliza correctamente, puede asegurar a las organizaciones de futuras amenazas o ataques. Este programa se ocupa de todas las fases involucradas en el ciclo de vida de inteligencia de amenazas, con esta atención a un enfoque realista y futurista hace que C|TIA sea uno de los más completas certificaciones de Threat Intelligence en el mercado hoy en día. Este programa proporciona el sólido conocimiento profesional que se requiere para una carrera en la inteligencia de amenazas y mejora tus habilidades como analista de inteligencia de amenazas, aumentando tu empleabilidad. Es deseado por la mayoría de los ingenieros de seguridad cibernética, analistas y profesionales de todo el mundo y es respetado por las autoridades de contratación.

10.1 Resultados Clave

- Habilita a los individuos y a las organizaciones con la capacidad de preparar y ejecutar un programa de inteligencia de amenazas que permita el conocimiento basado en la evidencia y proporcione consejos viables sobre las actuales amenazas desconocidas.
- Asegurar que las organizaciones tengan la capacidad predictiva en lugar de simplemente medidas proactivas más allá del mecanismo de defensa activa.
- Empodera a los profesionales de la seguridad de la información con los conocimientos para desarrollar un programa profesional, sistemático y repetible de inteligencia contra amenazas en la vida real.
- Diferenciará Threat Intelligence Professionals de otros profesionales de la seguridad de la información
- Proporcionar una habilidad invaluable de una estructurada inteligencia de amenazas para mejorar las aptitudes y aumentar su empleabilidad

10.2 Temario

- Introducción a Threat Intelligence
- Las amenazas cibernéticas y la metodología Kill Chain
- Requisitos, planificación, dirección, y revision
- La recopilación y procesamiento de datos
- Análisis de Datos
- Los informes de inteligencia y difusión

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

10.3 Información del Examen

- Título del examen: Certified Threat Intelligence Analyst
- Código de examen: 312-85
- Número de preguntas: 50
- Duración: 2 horas
- Disponibilidad: Portal de examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

11 ECESv2: EC-Council Certified Encryption Specialist

El programa EC-Council Certified Encryption Specialist (ECES) introduce a los profesionales y estudiantes al campo de la criptografía. Los participantes aprenderán los cimientos de la criptografía simétrica y clave moderna incluyendo los detalles de algoritmos como Feistel Functions, DES y AES.

ECES proporciona las habilidades necesarias para realizar un despliegue eficaz de tecnologías de cifrado. Es un curso completo que abarca varios algoritmos, los conceptos clave detrás de esos algoritmos, aplicaciones de la criptografía de varias maneras y la realización de criptoanálisis

11.1 Resultados Clave

- Tipos de estándares de cifrado y sus diferencias
- Cómo seleccionar el mejor estándar para su organización?
- Cómo mejorar su conocimiento en Pentesting en cifrado?
- Implementación correcta e incorrecta de tecnologías de encriptación
- Errores comunes cometidos en implementación de tecnologías de cifrado
- Mejores prácticas cuando implemente tecnologías de cifrado
- Desarrollar habilidades para proteger los datos críticos en organizaciones con encriptación
- Desarrollar una comprensión profunda de los algoritmos esenciales de criptografía y sus aplicaciones
- Tome decisiones informadas sobre la aplicación de tecnologías de cifrado
- Ahorre tiempo y costo evitando errores comunes al implementar tecnologías de cifrado de manera eficaz
- Desarrollar conocimientos laborales de criptoanálisis

11.2 Temario

- Módulo 01: Introducción e Historia de la Criptografía
  - ¿Qué es la criptografía?
  - Historia de la criptografía
  - Sustitución mono-alfabeto (César Cifrado,
  - Cifrado Atbash, Cifrado Affine, Cifrado ROT13)
  - Sustitución multibebeto (disco de cifrado, Vigenère Cipher, Cifrado Playfair, cifrado ADFGVX)
  - Sustitución homofónica
  - Cifrados nulos y de libros
  - Cifrados de vallas ferroviarias
  - La máquina Enigma
  - CrypTool
- Módulo 02: Criptografía Simétrica y “Hashes”
  - Criptografía simétrica
  - Teoría de la información
  - Principio de Kerckhoffs
  - Sustitución y transposición
  - Matemáticas binarias
  - Cifrado de bloques frente a cifrado de corriente
  - Algoritmos simétricos de cifrado de bloques (Feistel Function, DES, 3DES, AES, Blowfish, Serpent, Twofish, Skipjack, IDEA, CAST, TEA, SHARK)
  - Métodos de algoritmo simétrico

- Cifrados de flujo simétricos (RC4, FISH, PIKE)
- Función Hash (Hash – Sal, MD5, MD6, SHA, FORK-256, RIPEMD-160, GOST, Tiger)
- CryptoBench

- Módulo 03: Teoría de Números y Criptografía Asimétrica
  - Cifrado asimétrico
  - Datos de números básicos
  - Teorema del Cumpleaños
  - Generador de números aleatorios
  - Diffie-Hellman
  - Rivest Shamir Adleman (RSA)
  - Menezes–Qu-Vanstone
  - Digital Signature Algorithm
  - Elliptic Curve
  - Elgamal
  - CrypTool
- Módulo 04: Aplicaciones de Criptografía
  - FIPS Standards
  - Firmas Digitals
  - Certificados Digitales
  - Public Key Infrastructure (PKI)
  - Digital Certificate Management
  - Trust Models
  - Certificados y Servidores Web
  - Autenticación (PAP, S-PAP, CHAP, Kerberos)
  - Pretty Good Privacy (PGP)
  - Encripción Wi-Fi
  - SSL y TLS
  - Virtual Private Network (VPN)
  - Archivos de Encripción
  - BitLocker
  - Disk Encryption Software: VeraCrypt
  - Errores de Criptología Comúnes
  - Steganography
  - Steganalysis
  - Herramientas de Detección Steganography
  - National Security Agency y Cryptografía
  - Cifrado inquebrantable
- Módulo 04: Criptoanálisis
  - Breaking Ciphers
  - Cryptanalysis
  - Frequency Analysis
  - Kasiski
  - Cracking Modern Cryptography
  - Linear Cryptanalysis
  - Differential Cryptanalysis
  - Integral Cryptanalysis
  - Cryptanalysis Resources
  - Cryptanalysis Success
  - Rainbow Tables

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Password Cracking

11.3 Información del Examen

- Título del examen: EC-Council Certified Encryption Specialist
- Código de examen: 212-81
- Número de preguntas: 50
- Duración: 2 horas
- Disponibilidad: Portal de examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

12 CSA: Certified SOC Analyst

El programa CSA Certified SOC Analyst es el primer paso para integrarse a un Centro de Operaciones en Seguridad (SOC). Esta ingeniado para el actual y el futuro aspirante a Analista SOC Tier I y Tier II para obtener las competencias en el desempeño nivel introducción y nivel intermedio de operaciones.

CSA es un programa de entrenamiento y credencialización que ayuda al candidato a adquirir habilidades técnicas en demanda y por tendencia mediante una instrucción por los mejores y más experimentados entrenadores en la industria. El programa se enfoca en crear nuevas oportunidades de carrera a través de un extenso y meticuloso conocimiento con capacidades de nivel avanzado para contribuir dinámicamente a un equipo SOC.

Siendo un programa intenso de tres días, abarca minuciosamente los fundamentos de las operaciones SOC, antes de retransmitir el conocimiento de la gestión de log y correlación, despliegue de SIEM, detección avanzada de incidentes y respuesta incidente. Además, el candidato aprenderá a gestionar varios procesos de SOC y colaborará con el CSIRT en el momento de la necesidad.

12.1 Componentes críticos

- 100% Cumplimiento con el marco tecnológico de NICE 2.0
- Destaca en el extremo-a-extremo del flujo de trabajo del SOC
- Aprenda detectar incidencias con SIEM
- Detección de incidencias mejorada con Threat Intelligence
- Crear el entendimiento del despliegue SIEM
- Promueve el aprendizaje práctico
- El entorno de laboratorio simula un entorno en tiempo real
- Obtenga más información con material de referencia adicional

12.2 Temario

- Módulo 1 - Operaciones y gestión de la seguridad
- Módulo 2 - Comprensión de las amenazas cibernéticas, IoCs y metodología de ataque
- Módulo 3 - Los incidentes, Eventos y registro
- Módulo 4 - Detección de incidentes de seguridad de la información y administración de eventos (SIEM)
- Módulo 5 - Detección de incidencias mejorada con Threat Intelligence
- Módulo 6 - Respuesta a incidentes

12.3 Información del Examen

Detalles de Examen

El examen de la CSA está diseñado para poner a prueba y validar en un candidato la comprensión global de los trabajos y tareas necesarias como analista del SOC. Validando así su comprensión global de un completo flujo de trabajo del SOC.

- Título del examen: Certified SOC Analyst

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Código de examen: 312-39
- Número de preguntas: 100
- Duración: 3 horas
- Disponibilidad: Portal de examen ECC (please visit https://www.eccexam.com)
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Requerimiento de elegibilidad de examen

El programa CSA requiere un candidato que tenga 1 año de experiencia laboral en la administración de la red / dominio de seguridad y deberá ser capaz de proporcionar pruebas de la misma, validados a través del proceso de solicitud, a menos que el candidato asista a la formación oficial.

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

13 CASE JAVA

La credencial CASE pone a prueba las habilidades y conocimientos críticos de seguridad requeridos a lo largo de un ciclo de vida de desarrollo de software típico (SDLC), centrándose en la importancia de la implementación de metodologías y prácticas seguras en el entorno operativo inseguro de hoy.

El programa de capacitación certificado por CASE se desarrolla simultáneamente para preparar a los profesionales de software con las capacidades necesarias que esperan los empleadores y la academia a nivel mundial. Está diseñado para ser un curso práctico y completo de seguridad de aplicaciones que ayudará a los profesionales de software a crear aplicaciones seguras.

El programa de capacitación abarca actividades de seguridad involucrados en todas las fases del ciclo de vida de desarrollo de software (SDLC): Planear, crear, probar e implementar una aplicación.

A diferencia de otros cursos de seguridad de la aplicación, CASE va más allá de las directrices sobre prácticas de codificación seguras e incluye el requisito de recopilar seguro, robusto diseño de la aplicación, y manejo de las cuestiones de seguridad en el post-desarrollo las fases del desarrollo de aplicaciones.

13.1 Resultados Clave

- La seguridad más allá de codificación segura - desafiando la mentalidad tradicional donde la aplicación segura significa codificación segura
- Pruebas de desarrollo de aplicaciones seguras y de acreditación en todas las fases del SDLC
- El programa CASE mapea a muchas áreas de especialidad en la “Categoría de Provisión Segura” EN EL NICE Frame 2.0
- Incluye técnicas tales como las Técnicas de Validación de Entradas, prácticas de codificación de Defensa, autenticaciones y autorizaciones, ataques criptográficos, técnicas de control de errores, y la gestión de sesiones técnicas, entre muchos otros.

13.2 Temario

- Comprensión Application Security, amenazas y ataques
- Recopilación de requisitos de seguridad
- Secure Application Diseño y Arquitectura
- Prácticas de codificación seguras para la validación de entrada
- Prácticas de codificación seguras para la autenticación y autorización
- Prácticas de codificación seguras para criptografía
- Prácticas de codificación seguras para la gestión de sesiones
- Prácticas de codificación seguras para la Gestión de Errores
- Estáticos y dinámicos de la aplicación de pruebas de seguridad (SAST & DAST)
- Implementación segura y mantenimiento

13.3 Información del Examen

- Título del examen: Certified Application Security Engineer (Java)

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Código de examen: 312-96
- Número de preguntas: 50
- Duración: 2 horas
- Disponibilidad: Portal Examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

14 CASE.NET

La credencial CASE pone a prueba las habilidades y conocimientos críticos de seguridad requeridos a lo largo de un ciclo de vida de desarrollo de software típico (SDLC), centrándose en la importancia de la implementación de metodologías y prácticas seguras en el entorno operativo inseguro de hoy.

El programa de capacitación certificado por CASE se desarrolla simultáneamente para preparar a los profesionales de software con las capacidades necesarias que esperan los empleadores y la academia a nivel mundial. Está diseñado para ser un curso práctico y completo de seguridad de aplicaciones que ayudará a los profesionales de software a crear aplicaciones seguras.

El programa de capacitación abarca actividades de seguridad involucrados en todas las fases del ciclo de vida de desarrollo de software (SDLC): Planear, crear, probar e implementar una aplicación.

14.1 Resultados Clave

- Asegurar que la seguridad de la aplicación no es solo una idea sino algo más importante.
- Asienta las bases requeridas por los desarrolladores de aplicaciones y organizaciones de desarrollo para producir aplicaciones seguras con mayor estabilidad y menos riesgos de seguridad para el consumidor.
- Asegurar que las organizaciones reduzcan el riesgo de perder millones debido a compromisos de seguridad que puedan surgir en cada paso del proceso de desarrollo de aplicaciones.
- Ayuda a los individuos a desarrollar el hábito de dar importancia a la seguridad inviolable de su puesto de trabajo en el centro de descargas de SDLC, por lo tanto, la apertura de seguridad como el dominio principal para testers, desarrolladores, administradores de red, etc.

14.2 Temario

- Entendiendo Application Security, Amenazas y Ataques
- Recopilación de Requerimientos de Seguridad
- Diseño y Arquitectura de Secure Application
- Prácticas de codificación seguras para la validación de entrada
- Prácticas de codificación seguras para la autenticación y autorización
- Prácticas de codificación seguras para criptografía
- Prácticas de codificación seguras para la gestión de sesiones
- Prácticas de codificación seguras para la Gestión de Errores
- Pruebas de Seguridad de Apicaciones Estáticas y Dinámicas (SAST & DAST)
- Implementación y mantenimiento seguro

14.3 Información del Examen

- Título del Examen: Certified Application Security Engineer (.NET)
- Código de examen: 312-95
- Número de preguntas: 50
- Duración: 2 horas

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

- Disponibilidad: Portal Examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

15 LPT: Licensed Penetration Testing

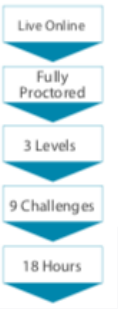
La credencia LPT (Master) esta desarrolladá en colaboración con las PYME y profesionales de todo el mundo después de un minucioso trabajo por roles, trabajo por tareas y un gap análisis de habilidades.

El examen práctico LPT (Maestro) es la culminación del track completo de Seguridad de la información de EC Council desde el programa CEH hasta ECSA. El examen LPT (Master) cubre el ajuste de habilidades, técnicas de análisis y redacción de informes, necesarios para ser un verdadero profesional en pruebas de penetración.

15.1 Resultados Clave

- Maestría en habilidades de Pruebas de Penetración
- Capacidad para llevar a cabo la metodología de forma repetible
- Compromiso con el código de ética
- Capacidad para presentar resultados analizados mediante reportes estructurados

15.2 Información del Examen



Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

16 Breake-The-Code Challenge

- BTC lleva Gamification al siguiente nivel, repleto de 24 increíbles desafíos de hacking (en esteroides!), a través de 4 niveles de complejidad que cubren 18 vectores de ataque, incluyendo el ¡OWASP Top 10!

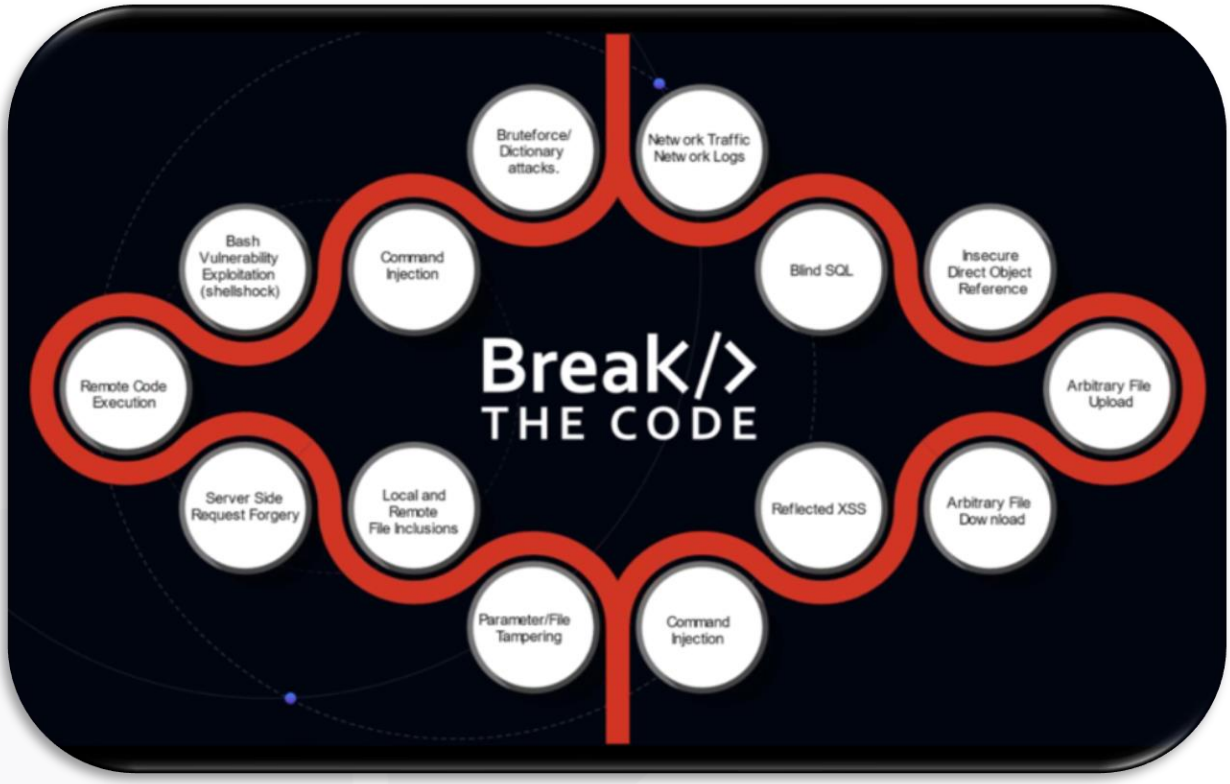
- Cubre vulnerabilidades que van desde un script básico entre sitios hasta pivotando, dando acceso en última instancia a todo el servidor.

- Algunas de las vulnerabilidades cubiertas son XSS, SQLi, IDoR y Ejecución remota de código.

- Los estudiantes están obligados a poseer habilidades y procedimientos variados para capturar la bandera de cada vulnerabilidad en diferentes niveles.

- Viene con una interfaz de usuario interactiva, a la que los alumnos se conectan a través de una VPN para acceder
- Aplicaciones.

- Contiene un sistema de puntuación dinámico que rastrea los niveles de ascenso de un alumno, con competidores
- viendo esto en el panel del portal.



Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

17 CodeRed

¿Qué es **CodeRed**? Una plataforma de autoaprendizaje de ciberseguridad a prueba de futuro de EC-Council para el aprendizaje continuo.

CodeRed llena el vacío de capacitación en ciberseguridad al ofrecer ofertas atractivas para diferentes segmentos.

	Individuals	Organizations	Academia
PRO	Total Access to the Entire Library of World Class Cybersecurity Education Content		
Box Bundles	Smaller selections of content that are • Affordable • Bite Sized • Topic Specific	Customized Learning Bundle • Industry Specific • Organization Specific	Customized Learning Bundle • Curriculum Specific • Organization Specific
Micro-degree	Deep dive into a topic and be awarded an EC Council Certificate		
Enterprise		Holistic platform enabling organizations to successfully deliver and monitor cybersecurity upskilling of employees	Holistic platform enabling institutions to successfully deliver and monitor a cybersecurity curriculum
Wholesale		Host specific , customized CodeRed content on internal LMS or on-prem LMS	

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

17.1 CodeRed Pro

Una biblioteca de clase mundial de temas de ciberseguridad Expertos en Ciberseguridad:

	Breadth	Relevance	Measurement
Individuals	Access library of world Class Cybersecurity programs that you can trust which means you will always learn from the best.	A constantly expanding library mapped to learning domains that allow you learn from a full spectrum of topics to be a competent professional	A customized dashboard means you can keep track of your learning and stay focused on your goals
Organizations	Provide your team the learning across multiple domains that they need so that they can maintain your organizational security	A constantly expanding library mapped to learning domains that allow your entire team to learn from a full spectrum of tools to be effective	Measure the learning of your staff through a dedicated dashboard so that you can ensure that everyone is up to speed
Academia	Augment your Cybersecurity Curriculum by providing your institution access to the full library and make sure they keep abreast with the latest trends	A constantly expanding library mapped to learning domains that allow your students to learn from full spectrum of topics that they can explore	Measure the learning of your students through a dedicated dashboard so that you can ensure that everyone is up to speed

17.2 CodeRed Microdegree

Vías de aprendizaje integrales para promover la práctica aprendizaje basado en vídeo con laboratorios simulados prácticos:

Individuals

Deep dive into a specialized topic so you can become an expert and get assessed to earn an EC-Council qualification which recognizes you as an expert

Live
200 Hours of learning spanned over 114 videos, 150 labs and 300 assessments

Releasing Q2, 21
200 Hours of learning spanned over 150 videos, 110 labs and 300 assessments

Live
200 Hours of learning spanned over 75 videos, 55 labs and 300 assessments

Releasing Q2, 21
200 Hours of learning spanned over 60 videos, 200 labs and 300 assessments

18 Duración de los Cursos

La duración del curso viene reflejada en Horas. Los días de duración dependerán del tiempo dedicado por el participante al estudio.

Item	Producto	Duración del Curso
1	CEH/CHFI/CND/EDRP/CPENT	40 Hrs
2	CCISO	32 Hrs
3	CASE JAVA/CASE.NET/ECIH v2/CTIA/CSA	24 Hrs
4	ECESv2	20 Hrs
5	CSCU	16 Hrs
6	LPT	Only Master Certification Exam

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García

19 Qué incluyen los Cursos

Un curso de OnLine de Cyber Security incluye:

- Instructor-lead, Curso Electrónico Oficial basado en Streaming Video Training Modules – Acceso por 1 Año.
- Material Oficial EC-Council (e-Courseware) – Acceso por 1 año
- Plataforma de Laboratorios Virtuales (iLabs) – Acceso por 6 Meses (Excepto CCISO y CSCU)
- Voucher para Examen de Certificación - Válido por 1 Año (Excepto APT)
- Certificado de Participación

Notas Importantes a Considerar:

- CSCU y/o CCISO No incluyen **iLabs**.
- El Curso APT es un entrenamiento para el examen LPT, por lo mismo, no incluye voucher de examen.
- ECSS (Certified Security Specialist) no está disponible en la plataforma **iLearn**.

Oficina CDMX
Plaza Polanco, Jaime Balmes No. 11.
Edificio B Piso 7
Col. Los Morales Polanco

Oficina Monterrey
Av. Bosques del Valle #106, Local 3
Col. Bosques del Valle, C.P. 66250,
San Pedro Garza García