ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 24 horas

Seguridad / Certified Indicent Handler CIH

El programa EC-Council Certified Incident Handler (E|CIH) capacita a los estudiantes con los conocimientos, habilidades y capacidades necesarias para prepararse, gestionar y erradicar amenazas y actores maliciosos durante un incidente de seguridad. El curso cubre el proceso completo de manejo y respuesta a incidentes, combinando contenido teórico con laboratorios prácticos diseñados para enseñar procedimientos y técnicas tácticas que permiten planificar, registrar, clasificar, notificar y contener incidentes de manera efectiva. Los participantes aprenden a manejar distintos tipos de incidentes, aplicar metodologías de evaluación de riesgos y comprender las leyes y políticas relevantes relacionadas con la gestión de incidentes. Además, el programa incluye actividades posteriores al incidente, como contención, erradicación, recopilación de evidencias y análisis forense, orientadas a acciones legales, mitigación y prevención de futuros incidentes. E|CIH adopta un enfoque metodológico integral que abarca desde la preparación y planificación del proceso de gestión de incidentes hasta la recuperación de activos organizacionales afectados.

Con más de 95 laboratorios avanzados, 800 herramientas y escenarios prácticos en distintos sistemas operativos, el programa ofrece una formación completa y realista que transforma a los estudiantes en profesionales capaces de manejar incidentes en entornos organizacionales complejos, consolidándose como una de las certificaciones más completas del mercado en manejo y respuesta a incidentes.

Perfil de la audiencia

- ✓ El curso E|CIH está dirigido a profesionales de ciberseguridad de nivel medio a alto que cuenten con un mínimo de tres años de experiencia. También está orientado a individuos del ámbito de la seguridad de la información que deseen fortalecer sus habilidades y conocimientos en el manejo y respuesta a incidentes, así como a personas interesadas en prevenir amenazas cibernéticas dentro de sus organizaciones.

Prerrequisitos

El curso ECIH está diseñado para profesionales de ciberseguridad de nivel medio a senior. Los candidatos con un mínimo de 1 año de experiencia en el ámbito de la ciberseguridad pueden postularse a este programa. También son elegibles las personas con experiencia en seguridad de la información que deseen ampliar sus conocimientos y habilidades en el manejo y respuesta a incidentes.

Módulos

MÓDULO 01: Introducción al manejo y respuesta a incidentes

- Comprender las amenazas a la seguridad de la información y los vectores de ataque
- Explicar diversos marcos de ataque y defensa
- Comprender los conceptos de seguridad de la información
- Comprender los incidentes de seguridad de la información
- Comprender el proceso de gestión de incidentes
- Comprender la automatización y orquestación de la respuesta a incidentes
- Describir diversas mejores prácticas para el manejo y respuesta a incidentes
- Explicar diversos estándares relacionados con el manejo y respuesta a incidentes
- Explicar diversos marcos de ciberseguridad
- Comprender las leyes y el cumplimiento legal sobre manejo de incidentes

MÓDULO 02: Proceso de manejo y respuesta a incidentes

- Comprender el proceso de manejo y respuesta (IH&R)
- Explicar los pasos de preparación para el manejo y respuesta
- Comprender el registro y asignación de incidentes
- Comprender la clasificación (triage) de incidentes
- Explicar el proceso de notificación
- Comprender el proceso de contención
- Describir la recolección de evidencia y el análisis forense
- Explicar el proceso de erradicación
- Comprender el proceso de recuperación
- Describir diversas actividades posteriores al incidente
- Explicar la importancia de las actividades de intercambio de información

MÓDULO 03: Primera respuesta

- Explicar el concepto de primera respuesta
- Comprender el proceso de asegurar y documentar la escena del crimen
- Comprender el proceso de recopilación de evidencia en la escena
- Explicar el proceso para preservar, empaquetar y transportar evidencia

MÓDULO 04: Manejo y respuesta a incidentes de malware

- Comprender el manejo de incidentes de malware
- Explicar la preparación para manejar incidentes de malware
- Comprender la detección de incidentes de malware
- Explicar la contención de incidentes de malware
- Describir cómo realizar análisis de malware
- Comprender la erradicación de incidentes de malware
- Explicar la recuperación tras incidentes de malware
- Comprender el manejo de incidentes de malware – Estudio de caso
- Describir mejores prácticas contra incidentes de malware

MÓDULO 05: Manejo y respuesta a incidentes de seguridad en correo electrónico

- Comprender los incidentes de seguridad en correo electrónico
- Explicar los pasos de preparación para manejarlos
- Comprender la detección y contención de estos incidentes
- Comprender el análisis de incidentes de correo electrónico
- Explicar la erradicación de incidentes
- Comprender el proceso de recuperación
- Comprender el manejo de incidentes – Estudio de caso
- Explicar mejores prácticas contra estos incidentes

MÓDULO 06: Manejo y respuesta a incidentes de seguridad en redes

- Comprender el manejo de incidentes de seguridad en redes
- Prepararse para manejar incidentes de red
- Comprender la detección y validación de incidentes
- Comprender el manejo de incidentes de acceso no autorizado

- Comprender el manejo de incidentes de uso inapropiado
- Comprender el manejo de incidentes de denegación de servicio
- Comprender el manejo de incidentes de seguridad en redes inalámbricas
- Comprender el manejo de incidentes – Estudio de caso
- Describir mejores prácticas contra incidentes de red

MÓDULO 07: Manejo y respuesta a incidentes de seguridad en aplicaciones web

- Comprender el manejo de incidentes en aplicaciones web
- Explicar la preparación para respondER
- Comprender la detección y contención
- Explicar el análisis de incidentes
- Comprender la erradicación
- Explicar la recuperación
- Comprender el manejo – Estudio de caso
- Describir mejores prácticas para asegurar aplicaciones web

MÓDULO 08: Manejo y respuesta a incidentes de seguridad en la nube

- Comprender el manejo de incidentes de seguridad en la nube
- Explicar los pasos involucrados
- Comprender cómo manejar incidentes en Azure
- Comprender cómo manejar incidentes en AWS
- Comprender cómo manejar incidentes en Google Cloud
- Comprender el manejo – Estudio de caso

- Explicar mejores prácticas contra incidentes en la nube

MÓDULO 09: Manejo y respuesta a amenazas internas (Insider Threats)

- Comprender el manejo de amenazas internas
- Explicar los pasos de preparación
- Comprender la detección y contención
- Explicar el análisis
- Comprender la erradicación
- Comprender el proceso de recuperación
- Comprender el manejo – Estudio de caso
- Describir mejores prácticas contra amenazas internas

MÓDULO 10: Manejo y respuesta a incidentes de seguridad en endpoints

- Comprender el manejo de incidentes en endpoints
- Explicar el manejo de incidentes basados en dispositivos móviles
- Explicar el manejo de incidentes basados en IoT
- Explicar el manejo de incidentes basados en OT
- Comprender el manejo – Estudio de caso

Examen de Conocimientos – EC-Council Certified Incident Handler (E|CIH)

El examen oficial del programa EC-Council Certified Incident Handler (E|CIH) evalúa la capacidad del candidato para aplicar de forma práctica los principios, procesos y técnicas de manejo y respuesta a incidentes en escenarios reales. A través de una evaluación estructurada, el examen mide el dominio del proceso completo de IH&R, incluyendo la preparación, detección, contención, erradicación, recuperación, análisis forense y actividades posteriores al incidente. Con un enfoque claro en incidentes modernos —como ataques de malware, seguridad de correo electrónico, ataques web, amenazas internas, incidentes en la nube, endpoints y redes— esta certificación garantiza que el profesional pueda desempeñarse eficazmente como parte de un equipo de respuesta ante incidentes. La evaluación se realiza dentro del ECC Exam Portal, lo que garantiza un entorno seguro y estandarizado. Aprobar este examen valida habilidades esenciales para roles de respuesta, análisis y gestión de incidentes en organizaciones de cualquier sector.

- Código del examen:
  - 212-89
- Duración:
- 3 horas
- Disponibilidad:
  - ECC Exam Portal
- Formato del examen:
  - Opción múltiple (100 preguntas)