EC-COUNCIL



EC-COUNCIL · PROGRAMA DE RESPUESTA A INCIDENTES

EC-Council Certified Incident Handler (E|CIH) v3

Prepárese para detectar, contener y erradicar incidentes de seguridad, y recuperar la operación de forma segura y ordenada

¿Por qué debería asistir?

El programa E|CIH de EC-Council prepara a los participantes con los conocimientos y habilidades para anticiparse, gestionar y erradicar amenazas y actores maliciosos durante un incidente. Cubre el proceso completo de manejo y respuesta a incidentes (IH&R), con laboratorios prácticos que enseñan los procedimientos tácticos para planificar, registrar, clasificar (triage), notificar y contener, además de metodologías de evaluación de riesgos y las leyes y políticas aplicables.

Al finalizar, podrá crear políticas de IH&R y atender incidentes de malware, correo electrónico, red, aplicaciones web, nube, amenazas internas y endpoints, incluidas la contención, la erradicación, la recolección de evidencia y el análisis forense. Con más de 95 laboratorios y 800 herramientas, es una de las certificaciones de IH&R más completas del mercado.

3 días	10	95	800+	50/50
DURACIÓN	MÓDULOS	LABORATORIOS	HERRAMIENTAS	TEORÍA / PRÁCTICA



¿Quién debería participar?

Manejo de incidentes y CSIRT
Manejadores y respondedores de incidentes, analistas, ingenieros y líderes de equipos CSIRT.

SOC y defensa cibernética
Analistas e ingenieros de SOC, consultores de defensa cibernética y analistas de inteligencia de amenazas.

Forense y riesgo
Investigadores forenses digitales, analistas de riesgo y vulnerabilidades, y pentesters.

Profesionales de seguridad
Profesionales de nivel medio y alto, con al menos 3 años de experiencia, que desean fortalecer sus capacidades de IH&R.

Objetivos de aprendizaje

- Comprender las amenazas, vectores de ataque, actores y sus motivaciones, y los marcos Cyber Kill Chain y MITRE ATT&CK
- Dominar los fundamentos de seguridad: evaluación de vulnerabilidades, gestión de riesgos, inteligencia de amenazas, modelado y threat hunting
- Aplicar los fundamentos de la gestión de incidentes, incluida la automatización y orquestación de la respuesta
- Conocer las mejores prácticas, estándares, marcos, leyes y regulaciones aplicables al manejo de incidentes
- Planificar un programa de IH&R en sus nueve etapas, desde la preparación hasta las actividades post-incidente
- Ejecutar la primera respuesta: recolección, documentación, preservación, embalaje y transporte de evidencia
- Manejar de forma sistemática incidentes de malware, correo, red, aplicaciones web, nube, amenazas internas y endpoints
- Usar plantillas, listas de verificación, playbooks y runbooks listos para automatizar la respuesta





Programa del curso

Duración: 3 días

Módulo	Contenido
Módulos 1–3 Día 1	**01 Introducción al manejo y respuesta a incidentes:** amenazas y vectores de ataque, marcos de ataque y defensa, conceptos de seguridad, proceso de gestión de incidentes, automatización y orquestación de la respuesta, estándares, marcos de ciberseguridad, leyes y cumplimiento legal. **02 Proceso de manejo y respuesta a incidentes:** preparación, registro y asignación, triage, notificación, contención, recolección de evidencia y análisis forense, erradicación, recuperación, actividades post-incidente e intercambio de información. **03 Primera respuesta:** concepto de primera respuesta; asegurar y documentar la escena; recolectar, preservar, embalar y transportar la evidencia.
Módulos 4–7 Día 2	**04 Manejo y respuesta a incidentes de malware:** preparación, detección, contención, análisis de malware, erradicación, recuperación, caso de estudio y mejores prácticas. **05 Manejo y respuesta a incidentes de seguridad del correo electrónico:** preparación, detección y contención, análisis, erradicación, recuperación, caso de estudio y mejores prácticas. **06 Manejo y respuesta a incidentes de seguridad de red:** detección y validación; accesos no autorizados, uso inapropiado, denegación de servicio y redes inalámbricas; caso de estudio y mejores prácticas. **07 Manejo y respuesta a incidentes de seguridad en aplicaciones web:** preparación, detección y contención, análisis, erradicación, recuperación, caso de estudio y mejores prácticas para asegurar aplicaciones web.
Módulos 8–10 Día 3	**08 Manejo y respuesta a incidentes de seguridad en la nube:** pasos del manejo de incidentes en la nube; incidentes en Azure, AWS y Google Cloud; caso de estudio y mejores prácticas. **09 Manejo y respuesta a amenazas internas:** preparación, detección y contención, análisis, erradicación, recuperación tras ataques internos, caso de estudio y mejores prácticas. **10 Manejo y respuesta a incidentes de seguridad en endpoints:** incidentes en dispositivos móviles, IoT y OT, y caso de estudio.

Examen

Duración: 3 horas

Título	EC-Council Certified Incident Handler (E|CIH) – Versión 3		
Código	212-89	**N.º de preguntas**	100
Formato	Opción múltiple	**Duración**	3 horas
Aprobación	Según la forma del examen (cert.eccouncil.org/faq)	**Plataforma**	ECC Exam Portal

¿Quién puede aplicar?

- **Experiencia recomendada:** profesionales de ciberseguridad de nivel medio a alto con un mínimo de 3 años de experiencia.
- **También dirigido a:** profesionales de seguridad de la información que desean ampliar sus conocimientos en manejo y respuesta a incidentes, y personas interesadas en prevenir amenazas cibernéticas.

Roles profesionales asociados a E|CIH

Manejador y respondedor de incidentes, consultor o analista de respuesta a incidentes, analista o líder de CSIRT, analista de SOC, consultor de defensa cibernética, investigador forense digital, analista de riesgo y vulnerabilidades, analista de inteligencia de amenazas y pentester.

Información general

- Manual del estudiante de más de 1.600 páginas, más de 780 diapositivas, 125 plantillas, listas de verificación y kits, y más de 10 playbooks y runbooks
- Alineado al 100 % con el marco NICE 2.0 y con CREST Certified Incident Manager (CCIM)
- EC-Council es una organización acreditada ISO/IEC 17024 y reconocida por el DoD 8140/8570