



EC-Council



E | CIH

EC-Council Certified Incident Handler

**Prepárese para manejar y responder
a incidentes de seguridad**

EC-COUNCIL

MANEJADOR DE INCIDENTES CERTIFICADO V2

LA
NATURALEZA
CRÍTICA DEL
MANEJO
RAPIDO A
INCIDENTES

“

Una reacción organizada y cuidadosa ante un incidente puede significar la diferencia entre una completa recuperación y desastre total.

-Symantec

POR QUÉ EL MANEJO DE INCIDENTES ES OBLIGATORIO PARA CADA ORGANIZACIÓN

Para identificar un ataque malicioso

214 DÍAS

Para contener y recuperarse de un ataque

77 DÍAS

Las organizaciones no tener un plan de respuesta a incidentes

77 DÍAS

74% de l rango-
empleadores
califican que
difícilmente
contratan a su
IH calificado y
Personal R
Como muy alto.

DOS DE LAS 10 PRINCIPALES MEDIDAS DE AHORRO DECOSTES EN CASO DE VIOLACIÓN DE DATOS

Ahorro de costos promedio con empleados deseguridad capacitados

\$9.30

Ahorro de costos promedio con un equipo derespuesta a incidentes

\$14por registro

¿ESTÁ SU ORGANIZACIÓN PREPARADA PARA MANEJAR EL PRÓXIMO INCIDENTE DE FORMA EFICAZ Y EFICIENTE?

Prepárese para manejar y responder a incidentes de seguridad

Esta última iteración del programa de Manejo Certificado de Incidentes (E|CIH) de EC-Council ha sido diseñada y desarrollada en colaboración con profesionales de ciberseguridad y manejo de respuesta a incidentes en todo el mundo.

Es un programa integral de nivel especializado que imparte el conocimiento y las habilidades que las organizaciones necesitan para manejar de manera efectiva las consecuencias posteriores a la filtración al reducir el impacto del incidente, tanto desde una perspectiva financiera como reputacional.

APRENDA HABILIDADES DE MANEJO DE INCIDENTES DEL MUNDO REAL

Después de un desarrollo riguroso, que incluyó un análisis de tareas de trabajo (JTA) cuidadoso relacionado con el manejo de incidentes y los trabajos de primeros respondedores de incidentes, EC-Council desarrolló un programa de capacitación intensivo de 3 días altamente interactivo, integral, basado en estándares y certificación que brinda un enfoque estructurado para aprender los requisitos de respuesta y manejo de incidentes del mundo real.

NO SOLO DETECTAR SINO GESTIONAR INCIDENTES DE SEGURIDAD

Las organizaciones están bajo constante ataque y con el conocimiento y las habilidades que se encuentran en el programa E|CIH, los profesionales ahora no solo pueden detectar incidentes, sino también gestionarlos rápidamente y responder de manera holística a estos incidentes.

MAPAS A LOS MARCOS DE LA INDUSTRIA

Los profesionales interesados en seguir el manejo y la respuesta a incidentes como una carrera requieren una capacitación integral que no solo imparta conceptos sino que también les permita experimentar escenarios reales. El programa E|CIH incluye aprendizaje práctico entregado a través de laboratorios dentro del programa de capacitación. La verdadera empleabilidad después de obtener una certificación solo se puede lograr cuando el núcleo de los planes de estudios se corresponde y cumple con los marcos de respuesta e incidentes publicados por el gobierno y la industria.

PROGRAMA IMPULSADO POR MÉTODOS

E|CIH es un programa basado en métodos que utiliza un enfoque holístico para cubrir amplios conceptos relacionados con el manejo y la respuesta a incidentes de la organización, desde la preparación y planificación del proceso de respuesta al manejo de incidentes hasta la recuperación de los activos de la organización después de un incidente de seguridad. Estos conceptos son esenciales para manejar y responder a incidentes de seguridad para proteger a las organizaciones de futuras amenazas o ataques.

APRENDA TODAS LAS ETAPAS DEL MANEJO DE INCIDENTES

Este programa aborda todas las etapas involucradas en el manejo de incidentes y el proceso de respuesta para mejorar sus habilidades como manejador y respondedor de incidentes, aumentando su empleabilidad. Este enfoque convierte a E|CIH en una de las certificaciones relacionadas con el manejo y la respuesta a incidentes más completas del mercado actual.

PIENSE EN LA EMPLEABILIDAD GLOBAL

Las habilidades que se enseñan en el programa E|CIH de EC-Council son deseadas por los profesionales de ciberseguridad de todo el mundo y son respetadas por los empleadores.

Las organizaciones buscan manejadores de incidentes profesionales y personal de respuesta que pueda preparar políticas y planes de seguridad para abordar incidentes con eficacia en escenarios con limitaciones de tiempo para reducir el impacto de los incidentes.

E|CIH ES UNO DE LOS MEJORES PROGRAMAS DE MANEJO DE INCIDENTES

Obtenga acceso a laboratorios nuevos y avanzados:

¡El programa E|CIH viene con acceso a más de 50 laboratorios, 800 herramientas y 4 sistemas operativos!

Cumple con los principales marcos de la industria:

100% de quejas con el marco NICE 2.0 y el marco CREST.

Plantillas completas disponibles:

Una gran variedad de plantillas, listas de verificación y hojas de trucos.

E|CIH TAMBIÉN CUBRE UNA GRAN VARIEDAD DE INCIDENTES DE SEGURIDAD

<p>Incidentes de malware</p> <p>Orientación de detecciones de malware las empresas aumentaron en un 270 por ciento</p>	<p>Incidentes de seguridad en la nube</p> <p>Se lanzaron 681 millones de ciberataques contra la nube clientes en 2018</p>	<p>Incidentes de seguridad del correo electrónico</p> <p>9 de cada 10 infecciones intentos durante todo el año fueron</p>
<p>Seguridad de aplicaciones web incidentes</p> <p>El 3,6% de los sitios web sufrieron ataques a aplicaciones web</p>	<p>Incidentes de seguridad de la red</p> <p>El 21,2% de los dispositivos fueron expuesto a amenazas de red en el 1er mes, ascendiendo a 43,7% después de 4 meses</p>	<p>Amenazas internas</p> <p>\$ 8.76 millones es el promedio costo anual de información privilegiada amenazas</p>



PÚBLICO OBJETIVO DE E|CIH

No existe una organización que esté realmente a salvo de un ciberataque. Un administrador de incidentes con las habilidades adecuadas para el manejo de incidentes puede ayudar a reducir el impacto de una infracción.

Las habilidades de manejo de incidentes que se enseñan en E|CIH son complementarias a los roles de trabajo a continuación, así como a muchos otros trabajos de seguridad cibernética:

Penetración Probadores	Vulnerabilidad Evaluación Auditores	Evaluación de riesgos Administradores	Red Administradores
Solicitud Seguridad Ingenieros	Ciberforense Investigadores/ Analista y SOC Analista	Sistema Administradores/ Ingenieros	cortafuegos Administradores y Gerentes Red /TI Gerentes

E|CIH es un programa de nivel especializado que atiende a profesionales de ciberseguridad de nivel medio a alto. Para aumentar sus posibilidades de éxito, se recomienda que tenga al menos 1 año de experiencia en el dominio de la ciberseguridad.

Los miembros de E|CIH son profesionales de seguridad ambiciosos que trabajan en organizaciones de Fortune 500 a nivel mundial.

DURACIÓN SUGERIDA DEL CURSO

3 DÍAS

24 HORAS TIEMPO TOTAL DE CLASE

Certificación:

El examen E|CIH se puede intentar después de completar el curso oficial E|CIH impartido por cualquier Centro de Capacitación Autorizado (ATC) del ECCouncil o directamente por el EC- Council. Los candidatos que aprueben con éxito el examen recibirán el certificado E|CIH y los privilegios de membresía. Se requiere que los miembros se adhieran a las políticas de la Política de Educación Continua de EC-Council.

DETALLES DEL EXAMEN

<p>TÍTULO DEL EXAMEN</p> <p>Certificado por el Consejo de la CE Manejador de incidentes</p>	<p>CÓDIGO DE EXAMEN</p> <p>212-89</p>	<p>NÚMERO DE PREGUNTAS</p> <p>100</p>
<p>DURACIÓN</p> <p>3 horas</p>	<p>EXAMEN DISPONIBILIDAD</p> <p>Consejo CE portal de examen</p>	<p>FORMATO DE PRUEBA</p> <p>Múltiple Elección</p>

CRITERIO DE ELEGIBILIDAD

Para ser elegible para rendir el examen E|CIH, el candidato debe:

Asista a la capacitación oficial de E|CIH a través de cualquiera de los Centros de capacitación autorizados (ATC) de EC-Council o asista a la capacitación en línea en vivo de EC-Council a través de iWeek o únase a nuestro programa de autoaprendizaje a través de iLearn (consulte <https://iclass.eccouncil.org>).

Los candidatos con un mínimo de 1 año de experiencia laboral en el dominio que deseen postularse para realizar el examen directamente sin asistir a la capacitación deben pagar la tarifa de solicitud de elegibilidad de USD 100. Esta tarifa está incluida en su tarifa de capacitación si decide asistir a la capacitación.

Cláusula: Requisitos de edad y políticas relativas a los menores

El requisito de edad para asistir a la capacitación o al examen está restringido a cualquier candidato quee esté permitido por su país de origen/residencia.

Si el candidato es menor de edad según lo permitido por su país de origen/residencia, no es elegible para asistir a la capacitación oficial ni para intentar el examen de certificación a menos que proporcione un consentimiento por escrito al centro de capacitación acreditado/EC-Council. /indemnización de su padre/tutor legal y una carta de respaldo de su institución de educación superior. Solo se considerarán candidatos de una institución de educación superior acreditada a nivel nacional.



E|CIH ESTÁ DISEÑADO PARA REMEDIAR LAS AMENAZAS CIBERNÉTICAS MODERNAS

Cumple al 100 % con la publicación especial NICE 800-181 Cybersecurity Workforce Framework

Cubre los fundamentos de los problemas clave en el mundo de la seguridad de la información, incluidos los conceptos básicos de la piratería ética, los controles de seguridad de la información, las leyes relevantes y los procedimientos estándar.

100% compatible con los marcos CREST

E|CIH asigna el 100 por ciento al marco del Administrador de incidentes certificado por CREST (CCIM). Se enfoca en mantener un estándar apropiado para la respuesta a incidentes que determina el camino de la investigación en base a una considerable experiencia en el manejo de incidentes del mundo real y la información pertinente disponible. E|CIH se asigna a los exámenes de nivel de certificación CREST que están diseñados para establecer el punto de referencia para los manejadores de incidentes de alto nivel. Al obtener la certificación E|CIH, las personas son reconocidas mundialmente como manejadores de incidentes certificados.

Diseñado en base a un análisis integral de tareas laborales de toda la industria

E|CIH fue desarrollado por expertos en la materia y profesionales en el dominio de respuesta y manejo de incidentes mediante la realización de un riguroso análisis de tareas laborales en toda la industria. El programa se diseñó después de realizar un análisis intensivo de todas las combinaciones posibles de tareas, conocimientos, habilidades y capacidades (TKSA) de las publicaciones de trabajo relevantes de varias empresas multinacionales en todo el mundo. Este mapeo y análisis integrales sincronizan el programa E|CIH con los criterios de requisitos de trabajo del manejador de incidentes de toda la industria, abriendo la puerta de oportunidades a los titulares de la certificación E|CIH en varias organizaciones multinacionales.

Se enfoca en una aproximación de la estructura para realizar el proceso de respuesta y manejo de incidentes

El programa E|CIH se centra en un enfoque estructurado para realizar el proceso de manejo y respuesta a incidentes (IH&R). El proceso de IH&R incluye etapas como manejo de incidentes y preparación de respuesta, validación y priorización de incidentes, escalamiento y notificación de incidentes, recopilación y análisis de evidencia forense, contención de incidentes, recuperación de sistemas y erradicación de incidentes. Este proceso sistemático de manejo y respuesta a incidentes crea conciencia entre los que responden a incidentes para saber cómo responder a varios tipos de incidentes de seguridad.

Centrarse en desarrollar habilidades para manejar diferentes tipos de incidentes de ciberseguridad.

Este programa demuestra el proceso completo de IH&R de manera sistemática para varios tipos de incidentes de ciberseguridad, incluidos incidentes de malware, incidentes de seguridad de correo electrónico, incidentes de seguridad de redes, incidentes de seguridad de aplicaciones web, incidentes de inseguridad en la nube e incidentes relacionados con amenazas internas. Al cubrir el proceso de IH&R de extremo a extremo para todos estos tipos de incidentes de seguridad, E|CIH es un programa excepcional para los administradores de incidentes actuales y futuros.

Énfasis en la preparación forense y los procedimientos de primera respuesta.

Toda organización debe estar bien preparada para responder a cualquier incidente de seguridad. Es crucial que un manejador de incidentes responda de manera rápida, efectiva y eficiente para manejar, contener y mitigar el incidente. Esta primera respuesta requiere un conjunto de reglas estrictas y precisas que un respondedor de incidentes debe seguir para tratar el incidente de manera adecuada. Si hay alguna falta de preparación forense o de un proceso de primera respuesta, el incidente puede causar un daño desastroso a la organización. El programa E|CIH se centra en cómo una organización debe prepararse para abordar cualquier tipo de incidente cibernético junto con los pasos que debe realizar un socorrista para registrar o tratar el incidente.

Programa práctico.

E|CIH viene integrado con laboratorios para que los estudiantes puedan practicar las habilidades que aprenden. De hecho, más del 40 por ciento del tiempo de clase se dedica al aprendizaje práctico a través de los laboratorios del EC-Council. La relación teoría-práctica para el programa E|CIH es de 60:40, lo que proporciona a los estudiantes una experiencia práctica utilizando las últimas herramientas, técnicas, metodologías, marcos de respuesta y manejo de incidentes en diferentes plataformas operativas que requieren los manejadores de incidentes para manejar y responder eficazmente a diversas amenazas e incidentes organizacionales.

El entorno de laboratorio simula un entorno en tiempo real

El entorno de laboratorio de E|CIH consta de los sistemas operativos más recientes y con parches, incluidos Windows 10, Windows Server 2016, Ubuntu Linux y OSSIM para realizar laboratorios. El entorno de laboratorio simula una situación en tiempo real para los manejadores de incidentes, brindando a los estudiantes habilidades que pueden aplicar de inmediato para proteger sus respectivas organizaciones.

Énfasis en los estándares y leyes de manejo de incidentes.

Los profesionales de manejo de incidentes están obligados a operar bajo ciertas reglas y regulaciones bien definidas. El programa E|CIH cubre varios estándares, leyes y políticas de ciberseguridad e IH&R, lo que permite a los profesionales de manejo de incidentes alinear su proceso de manejo de incidentes de acuerdo con los estándares de la industria.

Enorme inventario de plantillas de manejo de incidentes, listas de verificación y hojas de trucos

El programa acompaña a más de cien plantillas de manejo de incidentes, listas de verificación y hojas de trucos para una planificación eficaz de la respuesta a incidentes, lo que ayuda a manejar un incidente de manera efectiva. Esta vasta colección de material de documentación permite que un manejador de incidentes implemente la documentación relacionada con incidentes requerida en su organización. Las plantillas también ayudan a los manejadores de incidentes a redactar informes completos basados en la audiencia objetiva y los incidentes.



ESQUEMA DEL CURSO

<p>Introducción a Manejo de incidentes y Respuesta</p>	<p>Manejo de incidentes Y Procesos De Respuesta</p>	<p>Forense preparación y Primera respuesta</p>
<p>Manejo y Respondiendo al Malware incidentes</p>	<p>Manejo y Respondiendo al correo electrónico Incidentes de seguridad</p>	<p>Manejo y respuesta a la seguridad de la red incidentes</p>
<p>Manejo y respuesta a la aplicación web Incidentes de seguridad</p>	<p>Manejo y Respondiendo a la nube Incidentes de seguridad</p>	<p>Manejo y Respondiendo a Insider amenazas</p>

OBJETIVOS DE APRENDIZAJE DEL PROGRAMA E | CIH

- Comprender los problemas clave que asolan el mundo de la seguridad de la información
- Aprenda a combatir diferentes tipos de amenazas de ciberseguridad, vectores de ataque, actores de amenazas y sus motivos.
- Aprenda los fundamentos de la gestión de incidentes, incluidos los signos y costos de un incidente
- Comprender los fundamentos de la gestión de vulnerabilidades, la evaluación de amenazas, la gestión de riesgos, la automatización y orquestación de respuestas a incidentes.
- Domine todas las mejores prácticas, estándares, marcos de seguridad cibernética, leyes, actos, regulaciones de manejo y respuesta a incidentes.
- Decodificar los diversos pasos involucrados en la planificación de un programa de respuesta y manejo de incidentes
- Obtenga una comprensión de los fundamentos de la informática forense y la preparación forense.
- Comprender la importancia del procedimiento de primera respuesta, incluida la recopilación de pruebas, el embalaje, el transporte, el almacenamiento, la adquisición de datos, la recopilación de pruebas volátiles, estáticas y el análisis de pruebas.
- Comprender las técnicas antiforenses utilizadas por los atacantes para encontrar encubrimientos de incidentes de ciberseguridad.
- Aplicar las técnicas correctas a diferentes tipos de incidentes de ciberseguridad de manera sistemática, incluidos incidentes de malware, incidentes de seguridad de correo electrónico, incidentes de seguridad de redes, incidentes de seguridad de aplicaciones web, incidentes de seguridad en la nube e incidentes relacionados con amenazas internas.



EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx
Siguenos en nuestras redes

