

# Certified Hacking Forensic Investigator

## Descrición

As tecnoloxías dixitais están a cambiar a maneira de facer negocios. Así como as organizacións rapidamente aceptan as tecnoloxías dixitais como as nubes, big data, IoT e outros, o contexto de investigación dixital é máis relevante. O crecente número de ataques cibernéticos e crimes cambiou o rol de investigadores forenses de ADN a Dixitais.

CHFIv9, a última versión do programa foi deseñada por profesionais expertos no manexo de evidencias dentro de investigacións de cibercrimenes. Foi desenvolvido por un panel de investigadores expertos en problemas a investigacións e por profesionais da industria, establecéronse os estándares para as mellores prácticas en investigacións dixitais. Ademais, tamén está dedicado a aumentar o nivel de coñecemento, comprensión e habilidades en ciberseguridad e Investigación.

CHFIv9 presenta unha perspectiva detalladamente metodolóxica respecto das investigacións forenses e análises de evidencias dixitais. Prové as habilidades necesarias para a identificación de Pegadas dixitais e a recompilación de evidencia en caso de persecución penal. A certificación fortifica o nivel de aplicación de coñecementos de quen estea interesado na integridade das redes e investigacións dixitais.

## Obxectivos

O obxectivo da formación é axudarlle a dominar a metodoloxía dun Hacker Forensic Investigator. Os asistentes, unha vez superado o exame correspondente, lograrán obter unha das certificacións de maior interese global: CHFI - Computer Hacking Forensic Investigator.

Ao finalizar este curso, os estudantes serán capaces

de:

- Realizar resposta a incidentes e forenses
- Realizar recompilacións de evidencia electrónica
- Realizar adquisicións forenses dixitais
- Realizar bit- stream Imaging / adquisición dos medios dixitais confiscados durante o proceso de investigación
- Examinar e analizar texto, gráficos, multimedia e imaxes dixitais
- Levar a cabo exames exhaustivos das unidades de disco duro do computador e outros medios de almacenamento de datos electrónicos
- Recuperar información e datos electrónicos de discos duros de computadoras e outros dispositivos de almacenamento de datos
- Seguir estritos datos e procedementos de manexo de probas
- Manter a pista de auditoría (é dicir, a cadea de custodia) e a integridade da evidencia
- Facer traballos de exame técnico, análise e notificación de probas baseadas en computadoras
- Preparar e manter os expedientes
- Utilizar ferramentas forenses e métodos de investigación para atopar datos electrónicos, incluíndo historia de uso da internet, documentos de procesamento de textos, imaxes e outros arquivos
- Reunir información volátil e non volátil de Windows, MAC e Linux

- Recuperar arquivos e particións eliminados en Windows, Mac VOS X e Linux
- Realizar procuras de palabras clave incluíndo o uso de palabras ou frases de destino
- Investigar eventos para evidenciar ameazas ou ataques internos
- Apoiar a xeración de informes de incidentes e outras garantías
- Investigar e analizar todas as actividades de resposta relacionadas con incidentes cibernéticos
- Planificar, coordinar e dirixir as actividades de recuperación e as tarefas de análises de incidentes

Exame incluído:

CHFI 312-49 Certified Hacking Forensic Investigator

### **Dirixido a**

O curso CHFI está destinado a todas as persoas interesadas en investigacións forenses dixitais, avogados/as, consultores/as legais, corpos oficiais: oficiais de policía, axentes federais, defensa e milicia, detectives e investigadores/as, responsables de incidentes e membros de equipo; xerentes de seguridade da información, defensores/as de redes; profesionais, directores/as e xerentes IT; enxeñeiros/as en sistemas e redes, analistas e consultores/as de seguridade.

É necesario ter a capacidade de ler textos técnicos en inglés.

### **Perfil do docente**

---

## Certified Hacking Forensic Investigator

O noso equipo de formación son persoas con máis de 5 anos de experiencia en áreas de alta especialización técnica nos ámbitos de aplicación. Dispoñen das certificacións oficiais do fabricante (neste caso EC Council) para impartir estes cursos.

<b>DURACIÓN</b>	60 horas
<b>PROGRAMA</b>	Programación 2018/19
<b>MATRÍCULA</b>	Gratuíta
<b>METODOLOXÍA</b>	Presencial
<b>TIPO</b>	CURSO
<b>CERTIFICACIÓN OFICIAL</b>	Sí
<b>EXAME CERTIFICACIÓN</b>	CCHFI 312-49 Certified Hacking Forensic Investigator
<b>BENEFICIOS</b>	
<b>HORARIO</b>	De luns a venres de 09:30 a 13:45 horas.
<b>PERIODO INSCRICIÓN</b>	09/05/2019 - 23/05/2019
<b>PROBA DE SELECCIÓN</b>	28/05/2019, 11:00
<b>PERIODO DOCENCIA</b>	11/06/2019 - 28/06/2019
<b>LUGAR DE DOCENCIA</b>	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
<b>Nº PRAZAS</b>	16 (Mínimo 10)

## **Temario**

Módulo 01: A informática forense no mundo actual

Módulo 02: Proceso de investigación na informática forense

Módulo 03: Entendendo os Discos Duros e o Sistema de Ficheiros

Módulo 04: Adquisición e duplicación de datos

Módulo 05: Defensa contra técnicas anti-forense

Módulo 06: Análise forense do Sistema Operativo

Módulo 07: Forense de rede

Módulo 08: Investigación de ataques web

Módulo 09: Forense de Base de datos

Módulo 10: Forense en Cloud

Módulo 11: Forense de Malware

Módulo 12: Investigación de ataques por email

Módulo 13: Forense en dispositivos móbiles

Módulo 14: Redacción e presentación de informes forenses