

Certified Cybercrime Forensic Investigator (CCFI)



➤ Descripción del curso

Este curso está diseñado para darle al estudiante las herramientas y los conocimientos básicos para iniciarse en el mundo Forense Informático. Busca que el estudiante entienda con detalle cómo identificar las posibles fallas de seguridad, como se generan, como encontrar evidencia de brechas de seguridad, ataques, estrategias para el manejo de evidencia.

En este escenario, el curso ofrece la Metodología Forense y un marco conceptual de análisis que oriente a los alumnos ante una situación en la que se encuentre comprometida la seguridad informática de una organización, nuestro CCFI tendrán los elementos necesarios para abordar posibles situaciones de fraude realizados a través de computadoras, sabrá identificar evidencia digital relevante y presentar una aproximación desde la perspectiva legal en conjunto con las especificaciones técnicas que reviste el hecho.

Este curso forma parte de los créditos obligatorios en la Ruta de la Certified Master Security Engineer (CMSE)

➤ Forma de Evaluación

Nuestro proceso de certificación consta de dos fases.

Fase I: Examen en Línea (1010V2-GLC). El estudiante deberá contestar diversas pregunta teórico/prácticas de manejos de diferentes escenarios para la aplicación Forense.

Fase II: Examen práctico. Se le otorgara al estudiante acceso a un servidor virtual a través de internet, que contara con las herramientas para el análisis y procedimiento que se exigirán en la entrega del informe, del cual se llenara en línea a medida que avanza en las etapas descrita en la documentación, al finalizar la documentación se le entregara a los jueces que analizaran cada unas las pautas respondida por el estudiante. Al finalizar el informe durante un periodo de evaluación aproximado de 24 Horas se entrega los resultados y se procedera la entrega del certificado a través del correo internacional.

La puntuación mínima para la aprobación de cada Fase deberá ser de 700 / 1000 Puntos.

➤ A quien va dirigido

Profesionales de la seguridad de Negocios, Administradores de Sistemas, Profesionales Legales, Entidades Bancarias, Seguros y otros profesionales.

➤ Examen de Certificación

La certificación CCFI representa un esquema diferente en las certificaciones actuales ya que el el proceso de examen se divide en 2 partes:

1. Examen en línea 1010V2-GLC

2. Desarrollo de proyecto Forense.

➤ Duración

5 días



➤ Contenido del curso

Modulo 1: El Lenguaje del Cybercrimen

- Crecimiento del cybercrimen
 - Abusos y usos indebidos de redes
-

Modulo 2: Los Hackers

- Modus operandi, motivos y tecnología
 - Caracterización de los penetradores de cybercrimenes (SKRAM)
 - Herramientas y métodos aplicados
-

Modulo 3: Investigando un Cybercrimen

- Definición de lo que es un cybercrimen
 - Modelo de Investigación
 - Proceso de Investigación Forense
 - Herramientas Forenses
 - Análisis de cada elemento en un escenario Forense
-

Modulo 4: Adquisición Y Duplicación de datos

- Técnicas de adquisición de datos
 - Duplicación de discos bit a bit
 - Creación de imágenes de disco
 - Recuperación de datos y particiones eliminados
-

Modulo 5: Introducción a la Criptografía

- Conceptos generales de criptografía
 - Algoritmos de encriptación
 - Cracking de claves de archivos protegidos a nivel sistema operativo y aplicaciones
 - Esteganografía
-

Modulo 6: Análisis de Logs

- Huellas de hackeo
 - Registros de intento de intusión
 - Firewall Analyzer: Analizando los registros
-

Modulo 7: Evidencia Digital en Redes

- Análisis del Tráfico de red
- Análisis de Logs
- Network Intrusion Detection
- Registros y datos a través del modelo OSI
- Análisis de Incidentes en Seguridad en Redes

Modulo 8: Evidencia de ataques Web

- Los tipos de ataques Web
 - CrossSite Scripting (XSS)
 - Crosssite Request Forgery (CSRF)
 - Análisis de un ataque CSRF
 - Rastreo de ip
 - Analizando vulnerabilidades de un servicio web
-

Modulo 9: Análisis de Correos Electrónicos

- Funcionamiento de un cliente y servidor de correo
 - Rastreo de un email
 - Recuperación de emails borrados o Almacenes corruptos
-

Modulo 10: Análisis Forense de Móviles Y Pda

- Introducción
 - Pasos de PDA Forense
 - Métodos de Investigación
 - Herramientas utilizadas
-

Modulo 11: Presentación de la Evidencias

- Normas para la presentación de Evidencias
 - Armado de Líneas de Sucesos
-

Modulo 12: Consideraciones Legales

- Leyes internacionales sobre los cybercrimenes
 - El discurso probatorio en informática
 - Aplicaciones en distintos Países
-

Modulo 13: Direcciones Futuras

- Digital Evidence Response Team
- Preparación Forense de Redes
- Análisis Forense en sistemas inalámbricos
- Anonimato y seguimiento
- Retos y problemáticas legales

Calle Roberto H. Todd 656 Tercer Piso
Santurce, Puerto Rico, 00907

Tel.: (787) 620-5656 - Fax: (787) 722-1273

Email: info@glccorp.com - www.glccorp.com