greenetics

Certificación en Análisis Forense Informático

Greenetics Cybersecurity Academy

Es la primera academia de Seguridad Informática/Hacking Ético del país certificada por **CERT (Centro de Respuesta a Incidentes de Seguridad Informática).** Únete y conviértete en un Ethical Hacker desde cero o incrementa tus conocimientos en el mundo de la ciberseguridad. Nuestra compañía se complace en brindar todas las facilidades para entregarle un servicio de calidad y oportuno.

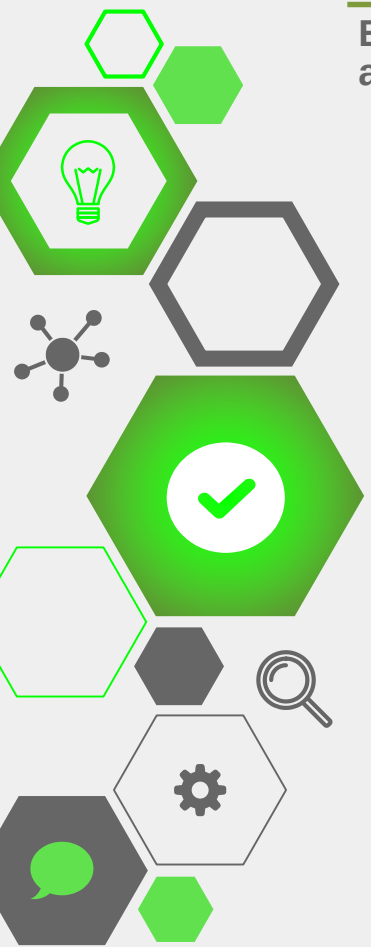
En Greenetics, nuestro objetivo es proporcionar sistemas seguros. Con las medidas necesarias, su empresa puede crecer más rápido y operar de manera más eficaz y, al mismo tiempo, preservar tanto la seguridad como la protección de los datos.

Auditoría de Sistemas	Informática Forense	Consultoría en Seguridad
Centro de respuesta de incidentes	Seguridad (Outsourcing)	Seguridad Perimetral
Capacitación Certificaciones	SGSI	Pentesting

CURSO DE ANÁLISIS FORENSE INFORMÁTICO

- El curso de **INFORMÁTICA FORENSE** está orientado a toda persona que esté interesada en comprender las técnicas, herramientas y procedimientos necesarios para realizar un análisis forense manteniendo la denominada “cadena de custodia”.
- Los contenidos inician con una introducción al mundo del análisis forense, posteriormente se analizan los procedimientos adecuados para realizar un análisis forense y finalmente se realizaran análisis forense sobre PCs y dispositivos móviles.

Estructura del Curso



En este curso aprenderás a:

- Comprender el campo de acción de un Analista Forense
- Entender el caso en el que aplicar los análisis proactivo y reactivo en forensia
- Realizar un análisis forense sobre dispositivos extraíbles de almacenamiento
- Entender los sistemas de ficheros usados en cada tipo de Sistema Operativo
- Extraer información forense de RAM Slacks, ficheros de intercambio, paginación y almacenamiento en cache
- Recolección de datos “in situ” en Sistemas Operativos Windows y Linux
- Manejar la evidencia de acuerdo a una cadena de custodia válida para un proceso judicial
- Manejar herramientas para análisis forense
- Realizar recuperación de datos y búsqueda de evidencia
- Realizar un análisis forense sobre dispositivos móviles
- Conocer cómo hacer un análisis forense

Certificación

- Este curso es tipo certificación avalado internacionalmente por el **CERT Cyberseg** (Centro de Respuestas a Incidentes de Seguridad Informática de Guatemala, certificado por FIRST, OEA, ITU, Universidad Cernegie Mellon; con presencia y liderazgo internacional)

CONTENIDOS

MÓDULO 1. INTRODUCCIÓN A LA INFORMÁTICA FORENSE

- Concepto de Informática Forense
- Campos de acción del Análisis Forense Informático
- Tipos de casos aplicables
- Aspectos jurídicos a tener en cuenta en el Análisis Forense Informático
- Tipos de Análisis Forense Informático (reactivo, proactivo)
- El Análisis Forense sobre dispositivos de almacenamiento
- Herramientas existentes
- Valor probatorio de evidencia en Informática Forense ante un ente judicial
- La utilización de sitios Web indispensables para trabajar en Seguridad Informática

MÓDULO 2. SISTEMAS DE FICHEROS

- Sistemas Operativos y sus sistemas de ficheros
- Sistemas de ficheros FAT
- Formas de almacenarse los datos
- Sistema de ficheros NTFS
- Sistemas ext3, ext4, reiser, hfs
- RAM Slack
- Ficheros de intercambio y paginación
- Almacenamiento de caché

MÓDULO 3: IDENTIFICACIÓN DE CASOS Y PRESERVACIÓN DE EVIDENCIAS

- Ejemplo de Delito Informático (Phishing)
- Recolección de data *in situ*
  - En Sistemas Operativos Linux
  - En Sistemas Operativos Windows
- Datos críticos a obtener en el caso
- Obtención de “palabras clave”
- La Cadena de Custodia y cómo establecerla
- Funciones hash
- Marco Tecnológico Pericial
  - Acceso a la evidencia
  - Identificación y registro
  - Autenticación, duplicación y resguardo de la evidencia
  - Detección, recolección y registro de indicios probatorios
  - Análisis e interpretación de los indicios probatorios. Reconstrucción y simulación del incidente
  - Cotejo, correlación de datos y conclusiones
- Herramientas de software y hardware

MÓDULO 4: RECUPERACIÓN DE DATOS Y BÚSQUEDA DE EVIDENCIA

- Herramientas para recuperación de datos
- Búsqueda y recuperación de datos borrados o perdidos
- Elementos no alocados
- Clasificación del material obtenido
- Recuperación de correos electrónicos
- Ficheros protegidos con contraseñas
- Cómo romper o crackear contraseñas
- Recuperación de caché de navegación
- Acceso al fichero de paginación
- Recuperación de claves del registro
- Detección de programas instalados y desinstalados
- Detección de dispositivos de almacenamiento que fueron conectados al computador para sustraer información
- Prácticas paso a paso de recuperación de datos
- Realización de un Informe Pericial
  - La Imparcialidad
  - Presentación de evidencias obtenidas
  - Simplicidad del informe
  - Construyendo el anexo de pruebas recabadas
  - Realizar un informe consistente frente a un posible contra peritaje

MÓDULO 5: ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES

- Por qué hacer Análisis Forense a un dispositivo móvil
- Adquiriendo la evidencia digital
- Análisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de Texto, Notas, Calendario de Eventos, Navegación, Mapas, Preferencias del Sistema, Logs, Aplicaciones, Información eliminada
- Análisis con Herramientas libres o gratuitas
- Análisis con Herramientas comerciales
- Recomendaciones adicionales para la entrega del informe

INSTRUCTORES

- Ing. Marco Rivadeneira, MBA, GCEH, GFI, Ingeniero en Electrónica y Redes de la Universidad Politécnica del Ecuador y Máster en Dirección de Empresas de la Universidad Complutense de Madrid – España. Ex Coordinador Nacional del *Computer Emergency Response Team* del Ecuador - ECUCERT, experto consultor de Ciberseguridad para el sector público y privado. Conferencista a nivel Nacional e Internacional en temas de Ciberseguridad. Ganador de varios juegos de Guerra Cibernética a nivel internacional.

- Ing. Diego Guacho. Ingeniero en Electrónica y Redes de la Universidad Politécnica del Ecuador. Experto en seguridad informática del CERT Nacional del Ecuador. Analista Forense de Seguridad, experto consultor de Cyberseguridad para el sector público y privado. Ganador de varios juegos de Guerra Cibernética a nivel internacional.
- **Apoyo**: Ing. Óscar Acevedo, CEO. CISA, CEH. CEO Cyberseg (Guatemala) Remoto – virtual. Director y fundador del *Computer Emergency Response Team* de Guatemala.

Requisitos:

- El alumno deberá tener conocimientos medios de redes, sistemas operativos, seguridad informática en infraestructura IT y Ethical Hacking.

Metodología

Luego de una exposición de los contenidos de cada capítulo, se llevará a cabo talleres participativos en grupos de trabajo para encontrar soluciones a escenarios planteados por el instructor promoviendo de esa forma la aplicación práctica de los conocimientos impartidos.

Evaluación

Se tomará en cuenta parámetros como:

- Participación en clase
- Presentación de resultados individuales o grupales
- Evaluación final online (Se deberá superar el 70% de la calificación total para la emisión de la certificación)

Recursos didácticos para el curso

Se dispondrá del contenido del curso en presentaciones y documentos con información complementaria actualizada y material para los talleres.

Recursos hardware para el curso

Se proveerá de los siguientes elementos de hardware y comunicaciones:

- Una estación de trabajo para cada estudiante con Windows 10 capacidad de operar máquinas virtuales.
- Interconexión de red entre las estaciones.
- Conexión a Internet controlada.
- Un servidor de mayor capacidad para colocar las máquinas virtuales comunes para los estudiantes.

Fechas y Horarios

Del 3 al y 7 de Septiembre

6pm a 9pm

Modalidad Presencial
20 horas académicas

Inversión

Profesionales:
USD 280,00 + IVA

Descuento para Estudiantes:
USD 230,00 + IVA

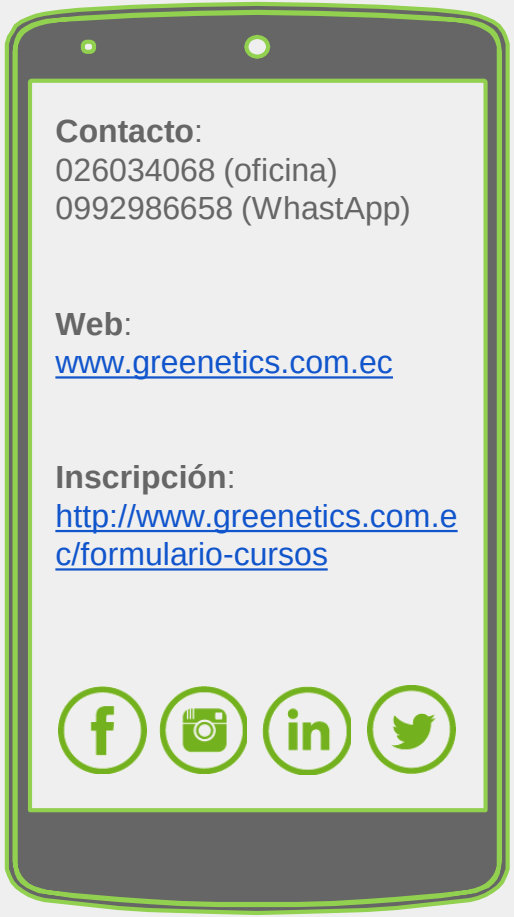
- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA
- Paypal por medio de nuestra página web www.greenetics.com.ec, sección de Inscripciones.

Incluye

- Material exclusivo y de uso confidencial.
- Un computador por participante (Curso Calendarizado).
- Refrigerios, almuerzos (Curso Calendarizado).

- **Certificado de aprobación del curso por 20 horas de duración (20 créditos académicos)**
- Certificado avalado por **CERT-CYBERSEG** (**Guatemala**).
- Contenidos, programa e instructores reconocidos por el **Ministerio de Trabajo**
- Empresa y Capacitadores certificados por la **Secretaría Técnica de Capacitación y Formación Profesional del Ecuador.**

Contacto



Dirección del Curso:
Av. Shyris N34-328 y Av. Portugal, Ed. SMERALD of 803. Junto a la sede de Alianza PAÍS.