greenetics

Certificación en Gestión de Incidentes de Seguridad Informática

Certificación GRCIH – Greenetics Certified Incident Handler

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.

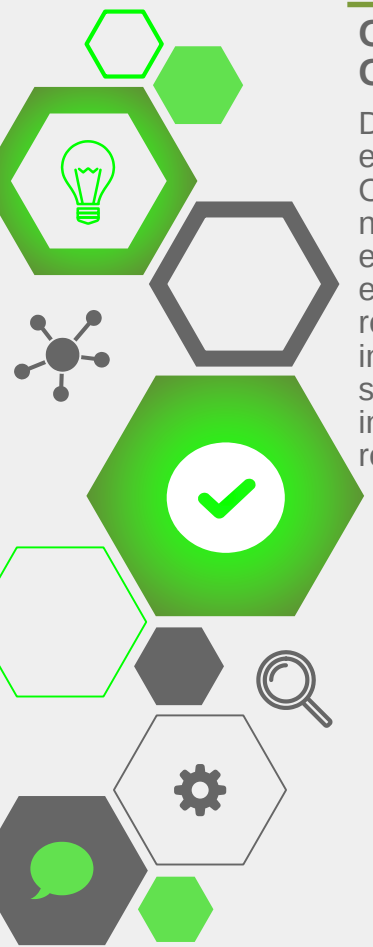
En Greenetics, nuestro objetivo es proporcionar sistemas seguros. Con las medidas necesarias, su empresa puede crecer más rápido y operar de manera más eficaz y, al mismo tiempo, preservar tanto la seguridad como la protección de los datos.

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

CERTIFICACIÓN DE MANEJO Y GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

- Los incidentes de seguridad se han producido en organizaciones de todo tamaño, ubicación geográfica y actividad. Es una cuestión de tiempo que un incidente se produzca afectando a los recursos de información de una organización grande o pequeña.
- Todos los estándares de Seguridad de la Información y marcos referenciales internacionales de Seguridad establecen la necesidad de tener la capacidad de manejar los incidentes de seguridad. Para ello, hay que iniciar por entender qué es un incidente y cuáles son las formas de manejarlo, los recursos tanto humanos como técnicos que son necesarios para mitigar su impacto y las herramientas que pudieran ser útiles para equipar a un grupo de respuesta a incidentes de seguridad de la información.
- Es necesario aplicar criterios antes, durante y después de un incidente para que el impacto que éste genere no quede fuera de control.

Estructura del Curso



Objetivo General

Dar a conocer los elementos que una Organización necesitaría para establecer un equipo de respuesta a incidentes de seguridad de la información y sus recursos asociados.

Objetivos Específicos

El participante al culminar el curso estará en capacidad de:

- Conocer los principales estándares de la industria que serían relevantes para el Manejo de Incidentes.
- Establecer la necesidad de una estrategia y recursos para manejo de incidentes en la Organización.
- Establecer los criterios para organizar un equipo de respuesta a Incidentes para la Organización.
- Identificar el perfil de los usuarios que compondrían el Equipo de Respuesta a Incidentes.
- Identificar los principales procesos y procedimientos necesarios para el Manejo de Incidentes de Seguridad.
- Conocer las estrategias de respuesta a incidentes aplicables.
- Revisar las estrategias de comunicación de los incidentes.
- Conocer las herramientas informáticas que se puede usar para la respuesta a incidentes.

Certificación

- Este curso es tipo certificación de 40 horas de duración 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 (4H)

- Estándares existentes
  - SEI CERT
  - NIST
  - ISO 27035
- Necesidad de una organización de Respuesta a Incidentes
- Incidentes en el mundo real
- Taller: Análisis de Archivos de bitácora (Log Files)

MÓDULO 2. ORGANIZANDO UN EQUIPO DE RESPUESTA A INCIDENTES (4H)

- Eventos e Incidentes
- Necesidad de Respuesta a Incidentes
- Política de Respuesta a Incidentes
- Creación de Planes y Procedimientos
- Estructura del Equipo de Respuesta a Incidentes
- Servicios del Equipo de Respuesta a Incidentes
- Taller: Análisis de Artefactos
- Taller: Buscando y encontrando información en DNS

MÓDULO 3. MANEJO DE INCIDENTES (16H)

- Preparación
- Detección y Análisis
- Contención, Erradicación y Recuperación
- Actividades Post-Incidente
- Lista de Verificación de Manejo de Incidentes
- Taller: Reconocimiento con Probes & Scans
- Taller: Ataques al Email
- Taller: Código Malicioso

MÓDULO 4. COORDINACIÓN Y DIVULGACIÓN DE INFORMACIÓN (4H)

- Coordinación
- Técnicas de Divulgación de Información
- Divulgación Granular Información
- Taller: Distributed Denial of Service Attacks (DDoS)
- Taller: Incidentes de alto impacto

MÓDULO 5. HERRAMIENTAS DE MANEJO DE INCIDENTES (4H)

- Sandbox
- RTIR
- Splunk
- Nagios
- Alien vault

Instructores

- Ing. Ramón E. Valdez, cuenta con 10 años de experiencia en proyectos de Seguridad de la Información y las siguientes certificaciones de la Industria: CERT Certified Security Incident Handler; ISO27001 Lead Auditor; Certified | Ethical Hacker; ITIL Foundations. Además tiene experiencia como instructor y facilitador por muchos años desde la época universitaria en diferentes ámbitos e instituciones.

- Instructor de Apoyo

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

Dirigido a

- Personas responsables del área de Seguridad de la Información
- Personal responsable de las áreas de Seguridad Informática o Seguridad de la Información.
- Responsables de Respuesta a Incidentes de Seguridad.
- Oficiales de Seguridad de la Información.
- Personas responsables del área de Seguridad de la Información.
- Profesionales de Tecnología y otras áreas con interés en manejo de Incidentes de Seguridad de la Información.

Requisitos del Participante

Conocimientos de Seguridad de la Información

Conocimientos de Tecnologías de Información

Deseable conocimientos en:

- Administración de Sistemas
- Redes y comunicaciones informáticas

Conocimientos de Tecnologías de Seguridad Informática

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)

Bibliografía

- CICHONSKI - Paul, MILLAR; Tom, GRANCE; Tim, SCARFONE. Karen.Computer Security. Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. US Departament of Commerce. August 2012
- INTERNATIONAL STANDARD ISO/IEC 27035 Information technology — Security techniques — Information security incident management. ISO Geneva, Switzerland 2011
- KRAUSZ - Michael, Managing Information Security Breaches Studies from real life. IT Governance Publishing. Cambridgeshire, 2010
- VINCENT Jesse, SPIER Robert, ROLSKY Dave, CHAMBERLAIN Darren, FOLEY Richard, RT Essentials. O'Reilly Media. Sebastopol, US, 2005

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.

Recursos software para el curso

Se utilizará las siguientes herramientas:

- Virtualbox
- Sandbox
- RT-IR
- Splunk
- Nagios

Fechas y Horarios

7, 8, 14 y 15 de Septiembre 2018

Horario Intensivo de 8am a 5pm

Modalidad Presencial

Inversión

Profesionales:
USD 580,00 + IVA

Descuento para Estudiantes:
USD 500,00 + IVA

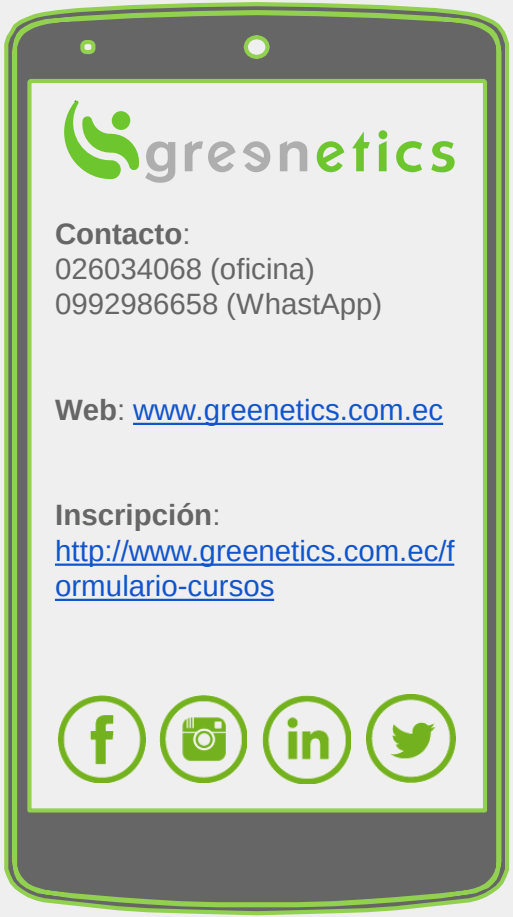
- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA
- Paypal por medio de nuestra página web www.greenetics.com.ec, sección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

Incluye

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

- **Certificación GRCIH – Greenetics Certified Incident Handler.**
- **Certificado de aprobación del curso por 40 horas de duración (40 créditos académicos CGRE)**
- 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.