



Curso de Desarrollo
Seguro basado en OWASP
Top 10



Greenetics Cybersecurity Academy

A decorative graphic in the top-left corner consisting of several hexagons in shades of green and grey, with a magnifying glass icon positioned over one of them.

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 DESARROLLO SEGURO BASADO EN OWASP TOP 10

- ◇ El curso de DESARROLLO SEGURO BASADO EN OWASP TOP 10 está orientado a toda persona que esté interesada en iniciarse en el mundo del desarrollo de software de manera segura, y que desee comprender las técnicas y herramientas básicas que utilizan los hackers actualmente para realizar un ataque, para así mismo implementar protecciones a nivel de código que puedan controlar o mitigar estos ataques.
- ◇ Durante las clases se realizarán ataques reales contra equipos y sistemas informáticos. Se atacará protocolos conocidos, servidores, aplicaciones web, evadiendo sistemas de defensa en punto final, entre otros.
- ◇ Este curso se enfoca en Desarrollo de Software Seguro, es decir, se estudian las metodologías de cómo crear software siguiendo buenas prácticas de referentes a nivel mundial. Además para ejemplos prácticos y casos de estudio se utilizará el Lenguaje de Programación web PHP.





Estructura del Curso



Objetivo General

Proporcionar conocimientos teóricos y prácticos con la finalidad de adquirir las habilidades necesarias para desarrollar aplicaciones web seguras basado en el OWASP Top 10 con el fin de mejorar la seguridad y evitar posibles ataques futuros.

En este curso aprenderás a:

Entender los fundamentos de Hacking y los diferentes tipos de hacking.

Dominar técnicas y usos del footprinting.

Entender el funcionamiento de los robots utilizados por Google y otros buscadores

Crear un laboratorio de hacking y desarrollo seguro desde cero.

Aprender el manejo de sistemas operativos utilizados para hacking.

Entender términos relacionados con networking.

Dominar técnicas de búsqueda de información en fuentes abiertas y cerradas.

Aprender a escanear, enumerar, y hackear sistemas de computación.

Utilizar las herramientas básicas de los hackers

Implementar las prácticas de desarrollo de software en aplicaciones web

Comprender el Proyecto de OWASP Top 10 y las vulnerabilidades más críticas.



Aval Internacional

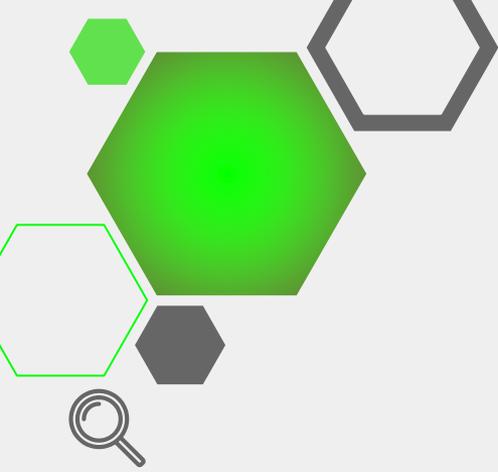
- ◇ Este curso es tipo certificación avalado internacionalmente por el **CERT Cyberseg** (Centro de Respuestas a Incidentes de Seguridad Informática de Guatemala, certificado por FIRST, OEA, ITU, Universidad Cernegie Mellon; con presencia y liderazgo internacional)





CONTENIDOS





MÓDULO 1. GENERAL

- ◇ Introducción al curso
- ◇ Contenido del curso
- ◇ Metodología del curso
- ◇ Advertencia del curso
- ◇ Requerimientos del curso

MÓDULO 2. PERSPECTIVA DE ATACANTE

- ◇ Laboratorios
- ◇ Virtualización y sistemas operativos para Hacking y Desarrollo
- ◇ Manejo de Sistema Operativo orientado a Hacking
- ◇ Principios de Networking





MÓDULO 3. DESARROLLO SEGURO

- ◇ Introducción al Pentesting
- ◇ Recolección de Información
- ◇ Análisis de Vulnerabilidades
- ◇ Metodologías de Desarrollo de Software Seguro
- ◇ Guías de Desarrollo de Software Seguro
- ◇ Buenas Prácticas de Desarrollo Seguro
- ◇ Prácticas de Laboratorio y Análisis



INSTRUCTOR

◇ Ing. Galoget Latorre, Ingeniero en Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional (EPN). Fundador & CEO del Grupo de Investigación en Software Libre y Seguridad Informática Hackem Research Group.

Investigador y colaborador en Proyectos Internet of Things (IoT) con Technische Universiteit Delft (TU Delft) (Países Bajos) y Technische Universität München (TUM) (Alemania).

Ex-Presidente IEEE Computer Society [EPN], Líder OWASP Ecuador [EPN], Embajador del Proyecto Fedora GNU Linux & Mozilla en Ecuador. Miembro ISACA Ecuador y Criptored.

Docente/Instructor en el Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN).





Dirigido a

- ◇ Personas que quieren iniciarse en el mundo de la Ciberseguridad.
- ◇ Estudiantes técnicos que desean especializarse en Ciberseguridad.
- ◇ Profesionales y estudiantes técnicos vinculados a las áreas informáticas, redes de computadoras, bases de datos y telecomunicaciones.
- ◇ Administradores de redes de computadoras en general, y específicamente quienes tienen a su cargo un servidor Linux o Windows.
- ◇ Profesionales de Tecnología y otras áreas con interés en gestionar las áreas de Seguridad de la Información.





Metodología

Este curso se enfoca en Desarrollo de Software Seguro, es decir, se estudian las metodologías de cómo crear software siguiendo buenas prácticas de referentes a nivel mundial. Además para ejemplos prácticos y casos de estudio se utilizará el Lenguaje de Programación web PHP.

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

27 y 28 de Abril
2019

Sábado y
Domingo
8am a 5pm

Modalidad
Presencial





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 personas),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA
- www.greenetics.com.ec, sección de Inscripciones.





Incluye

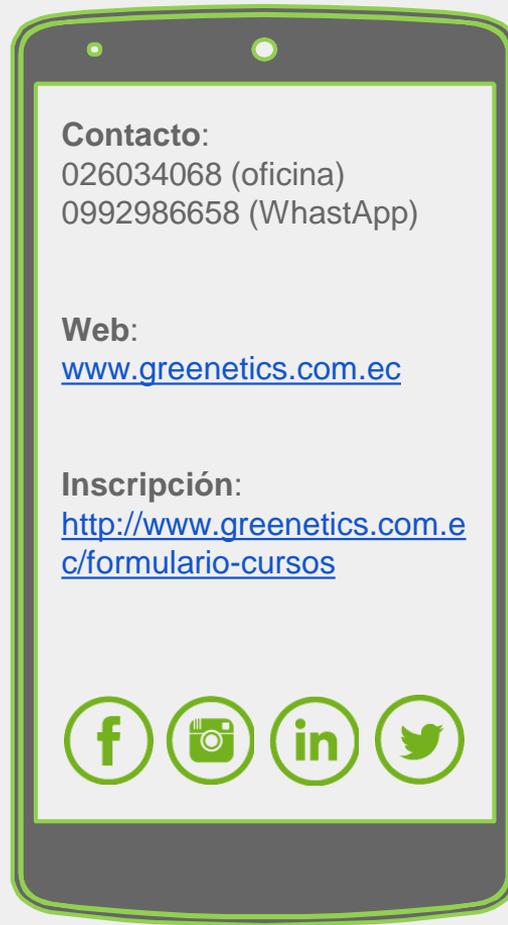
- ◇ Material exclusivo y de uso confidencial.
- ◇ Un computador por participante (Curso Calendarizado).
- ◇ Refrigerios, almuerzos (Curso Calendarizado).
- ◇ **Certificado de aprobación del curso por 16 horas de duración**
- ◇ Certificado avalado por **CERT-CYBERSEG (Guatemala)**.
- ◇ Este curso se enfoca en Desarrollo de Software Seguro, es decir, se estudian las metodologías de cómo crear software siguiendo buenas prácticas de referentes a nivel mundial. Además para ejemplos prácticos y casos de estudio se utilizará el Lenguaje de Programación web PHP.



Contacto

Dirección del Curso:

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





Derechos Reservados

Se encuentra prohibida la copia y/o reproducción o en cualquier modo la explotación de este material sin la previa autorización legal escrita de la empresa GREENETICS SOLUCIONES S.A.

Sin embargo, usted podrá bajar el material a su computadora personal para uso exclusivamente personal o educacional y no comercial limitado a una copia por página.

De igual forma se prohíbe la publicación de este material en medios digitales y páginas web ajenas a la marca GREENETICS SOLUCIONES S.A.

