greenetics

Certificación Oficial de Seguridad de la Información

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 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

- La necesidad de profesionales de Seguridad de la Información está en pleno crecimiento. Es necesario que quien va a cubrir el rol del responsable interno de la Seguridad de la Información comprenda plenamente el ámbito y el alcance de sus responsabilidades.

- Se revisará no solo el perfil del Oficial y su formación profesional sino también el enfoque necesario de parte del mismo para el cumplimiento de objetivos de Seguridad de la Información en la Organización.

Estructura del Curso

Objetivo General

Dar a conocer cuál es el rol del Oficial de Seguridad de la Información como responsable de la Seguridad en una Organización y afirmar al Oficial de Seguridad con los mejores criterios sobre sus responsabilidades y enfoque en el trabajo cotidiano.

Objetivos Específicos

El participante al culminar el curso estará en capacidad de:

- Establecer cuál podría ser la misión del Oficial de Seguridad de la Información dentro de la Organización.
- Establecer cuáles podrían ser los objetivos del Oficial de Seguridad de la Información dentro de la Organización.
- Establecer cuáles podrían ser las responsabilidades del Oficial de Seguridad de la Información dentro de la Organización.
- Revisar las posibles alternativas de la ubicación jerárquica en el contexto de la Organización.
- Identificar cuál sería la formación académica deseable del Oficial de Seguridad de la Información.
- Conocer las principales certificaciones profesionales de la industria que serían relevantes para el OSI.
- Conocer los principios de Seguridad de la Información y riesgos como la línea base necesaria para establecer una estrategia de Seguridad de la Información en una Organización.
- Conocer diferentes enfoques de las estrategias de Seguridad de la Información para una Organización.

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)

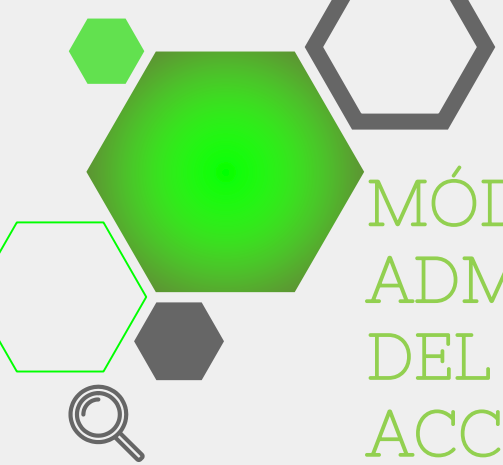
CONTENIDOS

MÓDULO 1. INTRODUCCIÓN

- Misión del Oficial de Seguridad de la Información dentro de la Organización.
- Objetivos del Oficial de Seguridad de la Información dentro de la Organización.
- Responsabilidades y competencias del Oficial de Seguridad de la Información dentro de la Organización.
- Alternativas de la ubicación jerárquica en el contexto de la Organización.
- Formación académica y características personales del Oficial de Seguridad de la Información.
- Certificaciones profesionales de la industria relevantes.

MÓDULO 2: ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN (10 horas)

- Gobierno y Gestión de Seguridad de la Información
- Gestión de Riesgos de SI
- Taller de Análisis de Riesgo
- Programa de Seguridad de la Información
- Clasificación Información
- Controles de Seguridad (tipos y clases)
- Políticas y Procedimientos de Seguridad de la Información
- Seguridad Administrativa (segregación de funciones, rotación, NDAs, etc.)
- Seguridad en Data Center

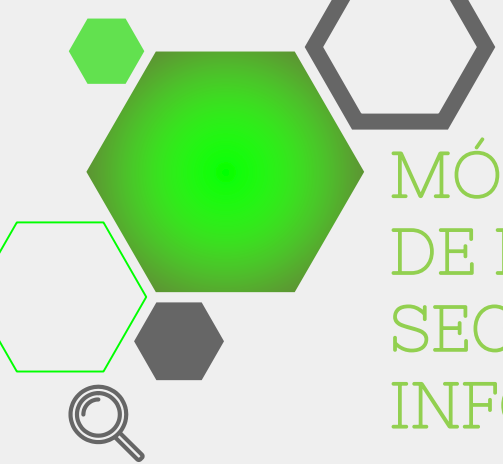


MÓDULO 3: ADMINISTRACIÓN DEL CONTROL DE ACCESO LÓGICO

- AAA (Autenticación, Autorización, y Responsabilidad)
- Menor Privilegio y Necesidad de Conocer
- Modelos de Control de Acceso
- Protocolos de Control de Acceso
- Tecnologías de Control de Acceso (Single Sign-On, Gestión de Identidades, Kerberos)

MÓDULO 4: SEGURIDAD EN OPERACIONES DE TI

- Gestión de Activos (Gestión de configuración y gestión de cambios)
- SLAs (Acuerdos de Nivel de Servicio)
- Tolerancia a Fallas
- Gestión de Backups
- Arreglo redundante de discos independientes (RAID)



MÓDULO 5: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Delitos informáticos
- Aspectos legales de una investigación (tratado de evidencia y cadena de custodia)
- Informática Forense
- Peritaje informático en Ecuador
- Privacidad y regulaciones
- Respuesta a incidentes de Seguridad de Información (Preparación, detección, contención, erradicación, recuperación. Lecciones aprendidas)
- Taller de gestión de incidentes

MÓDULO 6: GESTIÓN DE SEGURIDAD EN REDES Y COMUNICACIONES

- Arquitectura y Diseño de Redes
- Seguridad en protocolos y dispositivos de Red (repetidores, switches, routers, firewalls, IDPS, Endpoint)
- Seguridad en Comunicaciones (Protocolos de Autenticación)
- VPN (PPP, IPSec, SSL y TLS)
- Seguridad en VoIP
- Seguridad en Wireless
- Seguridad en RFID
- Seguridad en Acceso Remoto

MÓDULO 7: SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE

- Conceptos de Programación (compiladores, intérpretes, bytecodes, etc.)
- Análisis de vulnerabilidades
- Técnicas de prueba
- Vulnerabilidades de Software, Testeo y Aseguramiento (Inyecciones SQL, OS, RFI, XSS, CSRF, etc.)
- Los riesgos OWASP de seguridad en el desarrollo de software.
- Taller de análisis de vulnerabilidades.
- Actividades de Seguridad en el SDLC (Risk Management, Defensa en profundidad, BSIMM, Integración en los métodos de desarrollo).

MÓDULO 8: CONTINUIDAD DEL NEGOCIO

- ISO 22301 Continuidad de Negocio
- Plan de Continuidad del Negocio y Recuperación de Desastres
- BIA (Análisis de Impacto al Negocio)
- Estrategias de continuidad (RPO, RTO, MDT, etc.)
- Estrategias de Recuperación (sitio redundante, hot site, warm site, cold site, etc.)
- Pruebas de recuperación
- Entrenamiento

MÓDULO 9: AUDITORIA DE SEGURIDAD DE INFORMACIÓN

- Auditorías (CobIT, ISO 27001, PCI-DSS)
- Evaluaciones de Seguridad de Información
- Evidencia de Auditoria de Seguridad de Información (Tipos)
- Recolección de Información
- Hallazgos de Auditoria de Seguridad de Información

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.

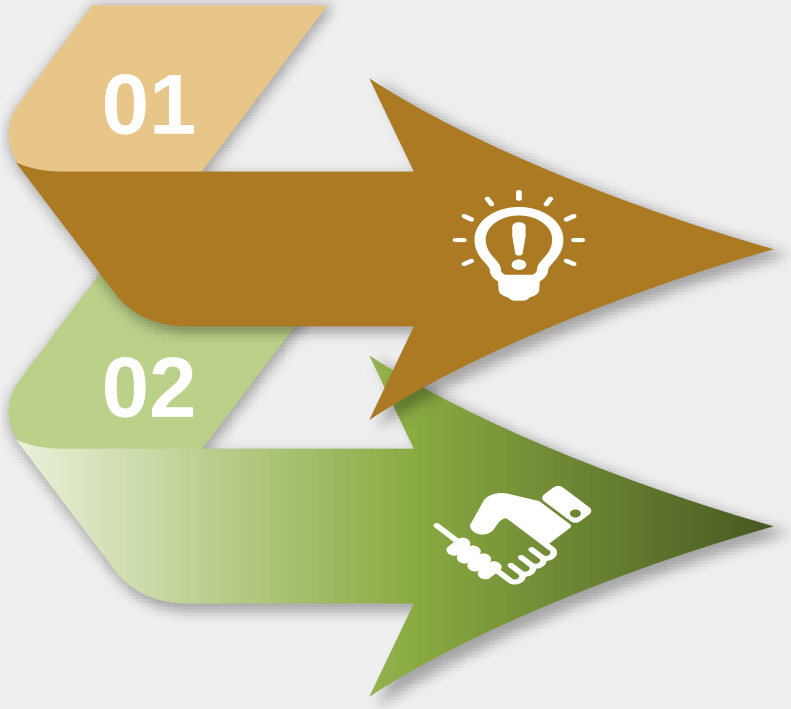
- Ing. José María Gómez de la Torre, CEH. Incident Handler, ENSA, Ingeniero en Telecomunicaciones de la Escuela Politécnica del Ejército, Máster en Dirección de Empresas de la Universidad Andina Simón Bolívar.

- 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 Cyberseguridad para el sector público y privado. Ganador de varios juegos de Guerra Cibernética a nivel internacional.

Dirigido a

- Directores de la Organización
- Gerentes de Sistema e Infraestructura
- Personal responsable de las áreas de Seguridad Informática o Seguridad de la Información.
- Profesionales de Tecnología y otras áreas con interés en gestionar las áreas de Seguridad de la Información.
- Oficiales de Seguridad de la Información designados.
- Personas responsables del área de Seguridad Informática
- Personas responsables del área de Seguridad de la Información

Requisitos del Participante



Conocimientos básicos de Tecnologías de Información.
Interés en ampliar conocimientos en otras áreas de una organización.

Deseable conocimientos en:
Gestión Organizacional
Gestión de Riesgos
Gestión de Tecnologías

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

- KOUNS, Barry L. KOUNS Jake. The Chief Information Security Officer. Insights, tools and survival skills. IT Governance Publishing, Cambridgeshire 2011

- KOVACICH, Gerald L. The Information Systems Security Officer’s Guide. Establishing and Managing a Cyber Security Program. Third Edition. Elsevier. Amsterdam 2016

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

2019

Fin de Semana 8am a 5pm

Modalidad Presencial 40 horas académicas

Inversión

Profesionales:
USD 580,00 + IVA

Descuento para Estudiantes:
USD 500,00 + IVA

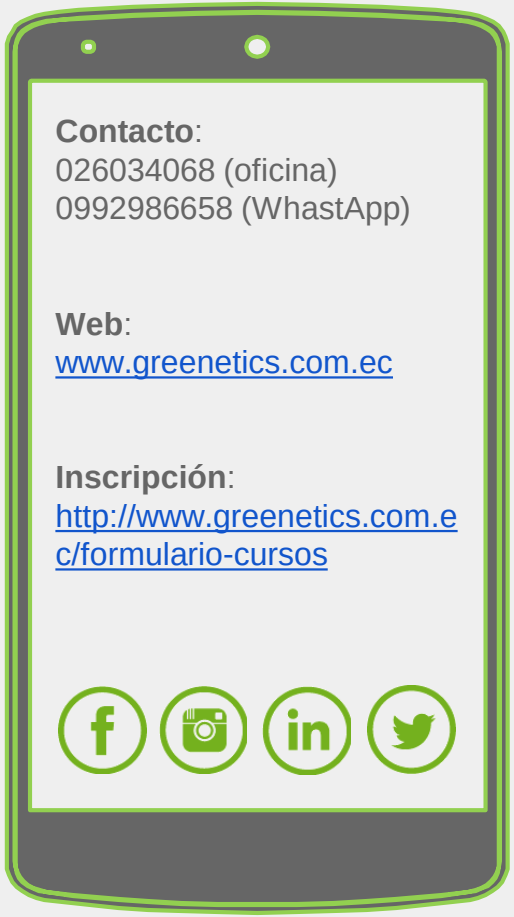
- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA
- Paypal por medio de nuestra página web www.greenetics.com.ec, sección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

Incluye

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

- **Certificado de aprobación del curso por 40 horas de duración (40 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.