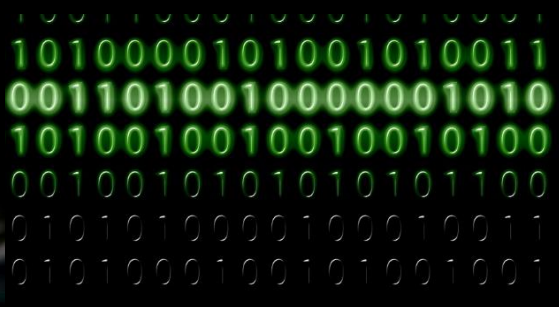
DIPLOMADO
AMENAZAS INFORMÁTICAS EN LA CADENA DE SUMINISTRO



Programa Internacional AVALADO por el
Security College US, de los Estados Unidos de Norteamérica www.securitycollege.us

Security College US
Facultad de Ciberseguridad

info@securitycollege.us Teléfono/WhatsApp +1 301 448 9715

DIPLOMADO EN AMENAZAS
INFORMÁTICAS EN LA CADENA DE SUMINSTRO

FUNDAMENTACIÓN

El diplomado de amenazas informáticas en la cadena de suministro es un programa académico dirigido a profesionales del área de la seguridad, asesores, consultores y especialistas en la gestión de los riesgos para la empresa privada y sectores de la administración pública. Así mismo está pensado para nuestros miembros de las Fuerzas Militares retirados y activos que están pensando en su preparación profesional, con el ánimo de adaptar la experiencia y conocimiento adquirido durante el desarrollo de actividades propias de los organismos de seguridad del Estado para que pueda ser utilizado en la empresa privada en la gestión del riesgo integral.

OBJETIVO GENERAL

Objetivos Y Alcance

Ofrecer al profesional de la seguridad, la capacitación adecuada en los aspectos más relevantes de la Seguridad de la Información en la cadena de suministro y cadena logística, para su fortalecimiento profesional y su posterior aplicabilidad en el entorno empresarial o militar.

Objetivos Específicos:

- Adquirir las habilidades y destrezas necesarias en la aplicación de las diferentes tecnologías de Seguridad de la información.
- Identificar las amenazas y vulnerabilidades en los sistemas de información e implementar las medidas adecuadas para prevenir los diferentes tipos de ataques informáticos que puedan impactar positiva o negativamente una empresa.
- Adquirir los conocimientos para realizar un efectivo proceso de gestión de riesgos.
- Conocer la metodología para diseñar un plan estratégico de mitigación.

- Ofrecer una formación integral acorde a las necesidades del mercado con la visión global de las grandes compañías, dando a los estudiantes conocimientos prácticos y relevantes para su futuro profesional en el campo de la seguridad integral.

METODOLOGIA

- El estudio es llevado de manera online. Al formalizar el alumno su matrícula se le envía a su correo electrónico los datos de acceso al aula virtual, en la cual se encontraran con el siguiente material:
- Módulos en formato PDF.
- Videos explicativos de cada documento expuesto en el curso.
- Videos explicativos de cada taller práctico.
- Ejercicios guiados para la puesta en práctica en casos reales.
- Software utilizado en el programa.
- Este diplomado tiene un tiempo de duración de 180 horas en el cual deberá cumplir los módulos y las evaluaciones dentro del aula virtual. Un curso 80% practico.

EVALUACION

Se realizará una evaluación al término de cada unidad temática tratada y al final del curso cada alumno responderá en forma individual una pauta de evaluación en la que constatará los conocimientos adquiridos y las habilidades desarrolladas y la presentación de un proyecto final. Las evaluaciones se realizaran en una escala de notas del 1 al 100, con un 75% mínimo para aprobar.

Las evaluaciones se realizaran dentro del aula virtual, siempre y cuando no exista o se determine otra forma o medio para medir los conocimientos adquiridos.

DURACIÓN

400 horas cronológicas.

CERTIFICACION

Al cumplir con los créditos académicos y terminar el programa académico con las notas mínimas exigidas en cada módulo, el Security College US, conferirá a quienes cumplan con todas las exigencias del Plan de Estudios, la siguiente certicación:

DIPLOMADO EN AMENAZAS INFORMATICAS EN LA CADENA DE SUMINISTRO

Duración: 400 horas cronológicas.

ESTRUCTURA DEL PROGRAMA

El diplomado consta de 12 módulos base de la especialidad, con una duración de 400 horas cronológicas, distribuidos de la siguiente manera:

1. Introducción. 20 horas
2. Cadena de suministro. 40 horas
3. Identificación de riesgos asociados a la cadena de suministro. 30 horas
4. Principios básicos de la información. 30 horas
5. El cibercrimen, el delincuente informático, delitos informáticos, la evidencia digital, la cadena de custodia. 30 horas
6. Herramientas para la protección. 40 horas
7. Hacking ético, generalidades. 30 horas
8. Técnicas hacking que utilizan los delincuentes informáticos. 50 horas
9. Ransonware, impacto y prevención. 10 horas
10. Análisis de vulnerabilidades. 40 horas
11. Conceptos de la norma ISO 27001 30 horas
12. Trabajo de investigación. 50 horas

FICHA TÉCNICA

Duración : 400 horas cronológicas

Fecha inicio :

Modalidad : On-Line (A distancia), a través de nuestro Campus Virtual.

Horarios : Libre disposición del alumno

Valor : US $ 1.500 dólares.

CUERPO DOCENTE

Director del Programa

Joany Guerrero Herrera

Magister en Inteligencia Estratégica, Gerente en la seguridad y Analista sociopolítico, profesional en Ciencias Militares, Master en seguridad de la información, consultor en seguridad privada mediante Res. 20151400056437 de 23-09-2015, especialista en investigación e información electrónica, Inteligencia Militar manejo de informática, especialista en seguridad de información y seguridad de la información corporativa, docente universitario para instituciones de educación superior militar, decano de la facultad de Ciberseguridad del Security College US.

Profesores

Jorge Bohórquez Cubillos

Mayor de la reserva activa del Ejército Nacional de Colombia, Profesional en Ciencias Militares y Especialista en administración de recursos militares. Auditor Interno en Sistemas integrados de Calidad (ISO 9001, ISO 14001, OHSAS 18001SST), con 31 años de experiencia en la administración de recursos humanos, logísticos y operacionales, amplio conocimiento en planeamiento estratégico, gestión del riesgo, manejo de crisis, toma de decisiones y evaluación de sistemas de seguridad y vigilancia, incluyendo el sector Oíl & Gas.

Ingeniero Richard Oliveros

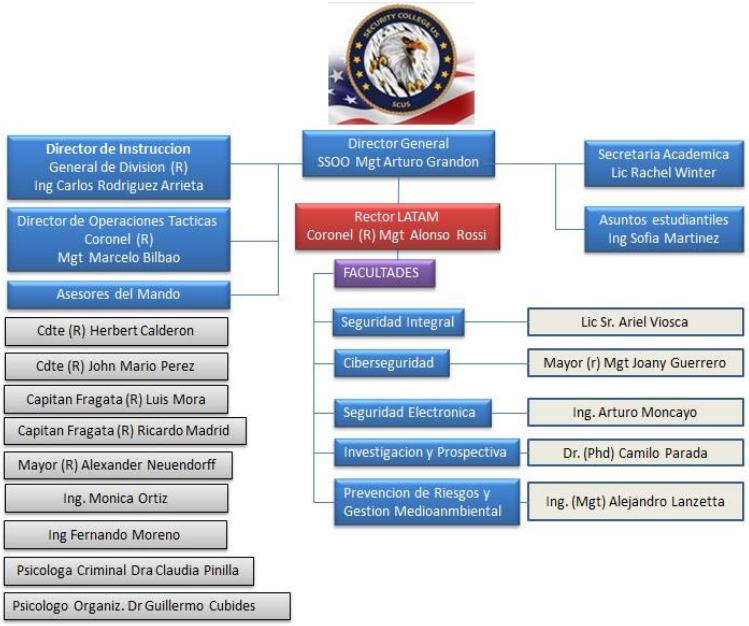
Perfil gerencial con conocimiento técnico y estructurado en ciberdefensa y ciberguerra, conocimientos sólidos en control reputacional online, manejo de marcas digitales y reacción ante desprestigios en web. Ingeniero electrónico con conocimientos en auditorías internas en seguridad de

la información, certificado en ISO27001, Hacking ético, certificado en test de intrusión, configuración de políticas y vpn en firewalls gamma, estructuración y puesta en marcha de pruebas en proyectos de software basados TDD (Siglas en inglés, Desarrollo guiado por pruebas). Analista senior de seguridad en compañías multinacionales del sector financiero, Bancario y de desarrollo de software; testing de software y aplicaciones web, diseñador de casos de usos y pruebas unitarias, implementador de herramientas de gestión de bugs, manejos de versiones, gestor y diseñador de SGSI acopladas a la medida de la Compañía. Ingeniero de implementación de seguridad electrónica, manejo de biométricos, cámaras de seguridad y control de acceso.

Alam Yessid Cáceres Cáceres

Ingeniero de sistemas, ethical hacking pentester, especialista en seguridad de la información, programador php, Delphi, comunity manager, 12 años de experiencia en desarrollo de herramientas para Ciberdefensa, asesor líder en operaciones de inteligencia.

Diagrama esquematico de la NUEVA forma de Capacitar y Supervisar por Internet



CONTACTO INTERNACIONAL

Joany Guerrero
Director del Programa
Decano Facultad de Ciberseguridad
Security College US
jguerrero@securitycollege.us
WhatsApp **+57 316 5479295**

Arturo Grandon
General Director
Security College US
agrandon@securitycollege.us
Telephone/WhatsApp **+1-301-448-9715 EEUU**

SECURITY COLLEGE US: Alma Mater de la Seguridad

www.securitycollege.us