

MASTER en CIBERGUERRA, NUEVOS ESCENARIOS DE CONFRONTACIÓN



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

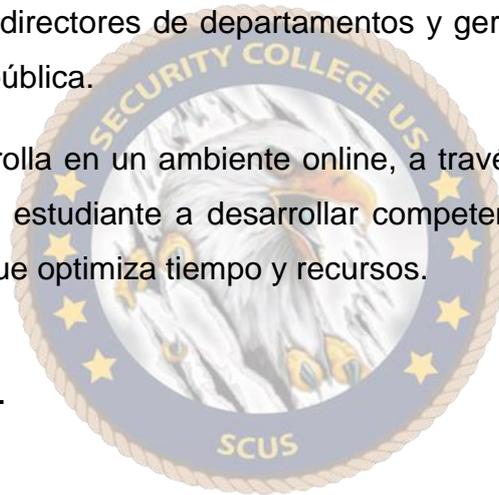


MÁSTER PROFESIONAL CIBERGUERRA NUEVOS ESCENARIOS DE CONFRONTACIÓN.

FUNDAMENTACIÓN

El programa de “**Master en ciberguerra nuevos escenarios de confrontación**” está dirigido a estudiantes y profesionales de la seguridad, ingenieros de sistemas, ingenieros electrónicos, administradores de empresas, estudiantes de geopolítica, relaciones internacionales, auditores, consultores, ex miembros de las fuerzas de seguridad, miembros activos de las Fuerzas Militares y de Policía, directores de departamentos y gerentes de procesos en la empresa privada y pública.

El programa se desarrolla en un ambiente online, a través de nuestro campus virtual, el cual lleva al estudiante a desarrollar competencias en un ambiente totalmente amigable que optimiza tiempo y recursos.



OBJETIVO GENERAL

Objetivos Y Alcance

Conocer la realidad de los riesgos y la necesidad que tienen los Estados para planear y desarrollar operaciones militares en el ciberespacio, lo cual representa grandes retos para la conformación de equipos multidisciplinarios alrededor de las nuevas tecnologías que diariamente avanzan en el área de las TIC'S, las cuales generan escenarios completamente diferentes dado el entorno en el que se conducen estas actividades, entendiendo que los actores, los medios y los métodos son distintos a los ordinarios ya conocidos por los expertos en la defensa de Estado.



Objetivos Específicos:

- Adquirir las habilidades y destrezas necesarias en la identificación de escenarios de ciber guerra.
- Identificar los actores que intervienen en una confrontación a través del ciberespacio.
- Conocer la historia de la ciber guerra desde el nacimiento del internet hasta nuestros días.
- Comprender como el internet de las cosas generan diversidad y riesgos nación.
- Estudiar diferentes procesos de ciber guerra a través de la historia.

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.
- Este Máster tiene un tiempo de duración de 800 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 10, con un 75% mínimo para aprobar.



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

DURACIÓN

800 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 certificación:

MASTER EN CIBERGUERRA NUEVOS ESCENARIOS DE CONFRONTACIÓN.

Duración: 800 horas cronológicas.



ESTRUCTURA DEL MASTER

El máster consta de 14 módulos base de la especialidad, con una duración de 800 horas cronológicas, distribuidos de la siguiente manera:

1. Introducción, generalidades y conceptos básicos. 40
2. Actores que intervienen en el ciberespacio. 80 horas
3. Infraestructuras críticas. 130 horas
4. Ciberarmas desde la resortera hasta la bomba atómica. 80 horas
5. Amenazas persistentes. 30 horas
6. Guerra Asimétrica. 50 horas
7. Cibercrimen, hacking y ciberterrorismo 50 horas.
8. Cibercrimes, y su transnacionalización. 20 horas.
9. Caso de estudio Irán y Estonia. 50 horas.



10. Caso de estudio Estados Unidos Vs China. 50 horas
11. Caso de Estudio Edward Snowden desde la perspectiva ética. 40 horas
12. Espionaje industrial. 40 horas
13. Fragilidad política a través de redes sociales. 20 horas
14. Artículo de investigación. 120 horas.

FICHA TÉCNICA

Duración	: 800 horas cronológicas
Fecha inicio	:
Modalidad	: On-Line (A distancia), a través de nuestro Campus Virtual.
Horarios	: Libre disposición del alumno
Valor	: US \$ 3.500 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



Camilo Parada

Magíster en estudios sociales, especialista en libertad, autoridad y justicia en la teoría política contemporánea, politólogo con énfasis en relaciones internacionales, Sólida formación académica, capacidad argumentativa, destreza organizacional, estructuración de procesos y en análisis prospectivo.

Experiencia en la orientación de procesos académicos a nivel escolar, Universitario y Pos gradual, con implementación de diversas metodologías según el área de conocimiento, los saberes a impartir y la población estudiantil.

Sólidos conocimientos en áreas asociadas a la Historia Política, Procesos Institucionales, Conflictos Sociales y Ambientales, Globalización y Territorio. Aplicaciones metodológicas según el área de conocimiento y el proceso cognitivo a trabajar.



Lic. Rodrigo Cardoso González.

Licenciado en Filosofía y pensamiento político, con maestría en Inteligencia estratégica. Experto en diseño de procesos de análisis estratégicos, desarrollo de capacidades organizacionales y en procesos de toma de decisiones. Ha sido docente internacional en los diplomados de inteligencia prospectiva en Brasil, Chile y Perú. Consultor en la modernización organizacional de la Dirección de Inteligencia y Seguridad Nacional – DIS de Costa Rica. Ha asesorado la creación de centros de prospectiva en la Policía Nacional de Colombia, y la renovación de la educación en la Escuela de Posgrados de Policía y en la Escuela de oficiales de policía. Ha sido docente de la Universidad Javeriana en el curso en dirección estratégica de organizaciones. Docente de la Escuela de Posgrados de Policía, de la Fundación Ingeniería Jurídica y director de proyectos de innovación y capacidades organizacionales del Grupo Innovati



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.



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





CONTACTO INTERNACIONAL



Joany Guerrero
Director del Programa
Decano Facultad de Ciberseguridad
Security College US
iguerrero@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