UBA
Universidad de Buenos Aires

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

Dictamen CONEAU Nº 501/19 a efectos de reconocimiento oficial y validez nacional de título.
Reconocimiento oficial y validez nacional de título, Resolución Nº RESOL-2020-198-APN-MECCYT

DATOS GENERALES DEL POSGRADO

Director: Roberto Uzal
Sede del Posgrado: Facultad de Ciencias Económicas
Denominación del título:
Magíster de la Universidad de Buenos Aires en Ciberdefensa y Ciberseguridad
Duración aproximada: 2 años

Informes e inscripción:
Facultad de Ciencias Económicas
Av. Córdoba 2122
Ciudad Autónoma de Buenos Aires (C1120AAQ)
Teléfono: (+54 11) 5285-7100
E-mail:
maestrias.enap@economicas.uba.ar
Web:
www.posgrado.economicas.uba.ar

DESCRIPCIÓN DEL POSGRADO

Objetivos generales:

- Complementar la formación de agentes gubernamentales y de ejecutivos empresariales mediante una sólida formación conceptual y una intensa capacitación instrumental en ciberdefensa y en ciberseguridad, de manera de posibilitar su actuación en casos de cibercrimen, especialmente en los casos de cibercrimen Organizado Transnacional, ciberespionaje, Activismo Hacker, ciberterrorismo y también en los casos de ciberagresiones entre estados naciones.

Objetivos específicos:

- Capacitar a agentes gubernamentales y a ejecutivos empresariales en el diseño e implementación de arquitecturas de hardware / software significativamente robustas y destacable resiliencia a todo tipo de ciberagresiones;
- capacitar a agentes gubernamentales y a ejecutivos empresariales en el diseño, construcción, implantación y mantenimiento de Sistemas de Detección de ciberintrusiones (“Intrusion Detection Systems” - IDS);
- formar a agentes gubernamentales y a ejecutivos empresariales en la detección y mitigación de cibervulnerabilidades;
- capacitar a agentes gubernamentales y a ejecutivos empresariales en el desarrollo de software seguro;
- formar a agentes gubernamentales y a ejecutivos empresariales en la detección de la circulación de malware en las redes teleinformática;
- formar a agentes gubernamentales y a ejecutivos empresariales para que puedan colaborar con significativa eficacia, en la preservación de la Infraestructura Crítica frente a diversos tipos de ciberagresiones;
- capacitar a agentes gubernamentales y a ejecutivos empresariales en “backtracing” y resolver el “Problema de la Atribución” (identificar al ciberagresor con una alta probabilidad de certeza y una muy baja probabilidad de falsos positivos);
- capacitar a agentes gubernamentales y a ejecutivos empresariales para generar elementos probatorios acerca del ciberataque y del ciberatacante con una solvencia forense reconocida por los tribunales internacionales;
- posibilitar que nuestro país pueda efectivamente ejercer los derechos que derivan del Artículo 51 de la Carta de las Naciones Unidas;
- capacitar a agentes gubernamentales y a ejecutivos empresariales para formar parte de CERT (Computer Emergency Response Team) y para liderar dichos equipos;
- formar agentes gubernamentales y ejecutivos empresariales para desempeñarse en posiciones de liderazgo en diversos tipos de emprendimientos en el contexto de la ciberdefensa y de la ciberseguridad.

Requisitos de admisión:
Graduado de la Universidad de Buenos Aires con título de grado correspondiente a una carrera de cuatro (4) años de duración como mínimo, o graduado de otras universidades argentinas con título de grado correspondiente a una carrera de cuatro (4) años de duración como mínimo, o graduado de universidades extranjeras que hayan completado, al menos, un plan de estudios de dos mil seiscientas (2.600) horas reloj o hasta una formación equivalente a master de nivel I, o egresado de estudios de nivel superior no universitario de cuatro (4) años de duración como mínimo y además completar los prerrequisitos que determine la Comisión de Maestría, a fin de asegurar que su formación resulte compatible con las exigencias del posgrado al que aspira.
Aquellas personas que cuenten con antecedentes de investigación o profesionales relevantes podrán ser admitidas excepcionalmente con la recomendación de la Comisión de Maestría y con la aprobación del Consejo Directivo de la Facultad.

Régimen de estudios:
Teórico. Práctico.
Requisitos para la graduación:
Aprobar la totalidad de las asignaturas correspondientes al plan de estudios.
Aprobar y defender el Trabajo Final de Maestría.

Reglamentación:
Resolución del Consejo Superior de la UBA Nº 7743/17.

PLAN DE ESTUDIOS

Cursos de formación general
- Tecnología de la información, ética y normativa jurídica
- Introducción al gerenciamiento innovador (entrepreneurship)
- Introducción a los paradigmas de programación
- Tecnología de la información

Cursos fundamentales de Ciberdefensa / Ciberseguridad
- Introducción a la criptología
- Evolución de la tecnología militar hasta el enfoque “Network-Centric Warfare”
- Tecnología de redes I
- Malware I

Fundamentos y gerenciamiento de la Ciberdefensa y de la Ciberseguridad
- Ciberataques masivos a sistemas de información
- Cursos específicos aspectos operativos de Ciberdefensa y Ciberseguridad
- Principios y enfoques de diseño de software seguro
- Proyecto sobre principios y enfoques de diseño de software seguro
- Teoría organizacional y psicología organizacional
- Diseño y desarrollo de la “Data Exchange Layer” en ambientes de gobierno
- Data Mining – Data warehousing - Big Data
- Tecnología de redes II
- Seguridad en redes de computadoras
- Malware II
- Talleres de Investigación Supervisada y/o Tutoriales en Aspectos Operativos de Ciberdefensa y Ciberseguridad