.UBAeconómicas posgrado

ENAP Escuela de Negocios y Administración Pública

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

CONTENIDOS MÍNIMOS

ASIGNATURAS - FORMACIÓN GENERAL

- **Tecnología de la Información, ética y normativa jurídica**

Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen desde un enfoque de la Tecnología de la Información. Contramedidas tecnológicas posibles frente al Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen. La importancia de la Ética en los equipos que enfrentan a las Ciber Agresiones mencionadas. Introducción a la normativa jurídica, nacional e internacional, relacionada con el Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen.

- **Introducción al gerenciamiento innovador (entrepreneurship)**

La importancia de la Gestión Orientada a la Calidad en las contramedidas ante el Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen. Gestión de Proyectos destinados a enfrentar el Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen. Proyectos de implantación de los conceptos y herramientas asociados a la familia de estándares ISO 27000. Aplicación del enfoque "Cuadro de Mando Integral" en un contexto de Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen. Creatividad e Innovación al enfrentar al Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Guerra y Ciber Crimen.

- **Introducción a los Paradigmas de Programación**

Paradigma Prescriptivo y Paradigma Declarativo. Paradigma Declarativo Funcional y Paradigma Declarativo Lógico. Lenguajes de Primera, Segunda, Tercera y Cuarta Generación. El Paradigma de Orientación a Objetos. Desarrollo de ejemplos de programas desarrollados con lenguajes comprendidos en los diversos Paradigmas. Utilización de los distintos Paradigmas de Programación en Ciberdefensa y Ciberseguridad.

- **Tecnología de la Información (orientación Ciberdefensa y Ciberseguridad)**

Evolución de la tecnología del Hardware. Panorama actual, Evolución de los lenguajes de Programación. Evolución del Software de Base (Sistemas Operativos y Gestores de Bases de Datos). Estado actual. Los Sistemas de Información. El Planeamiento Estratégico de los Sistemas de Información como sub conjunto de la Estrategia Organizacional. Análisis de los contenidos de este módulo desde una perspectiva de Ciberdefensa y Ciberseguridad.

ASIGNATURAS FUNDAMENTALES - CIBERDEFENSA y CIBERSEGURIDAD

- **Introducción a la Criptología**

Antecedentes históricos. Fundamentos matemáticos. Criptografía simétrica, DES, TDES, Funciones de Flujo. Funciones Hash. Criptografía asimétrica. RSA. Esquema de cifrado. Esquema de firma digital. Aspectos importantes CCE. Otras herramientas criptográficas. Criptografía Visual. Dinero Electrónico. Certificados Digitales. Infraestructura de claves públicas. Comercio Electrónico. Protocolos de seguridad.

- **Evolución de la Tecnología Militar hasta el enfoque "Network-Centric Warfare"**

Inicio de los conflictos militares en los Pueblos de la Mesopotamia. El Dominio Terrestre de los Conflictos Militares. Evolución de la Tecnología en el Dominio Terrestre. El impacto de la utilización en amplitud del Dominio Marítimo en los Conflictos Militares sobre todo a partir de las Guerras Médicas. Evolución de la Tecnología en el Dominio Marítimo. El Dominio o Contexto Aéreo en los Conflictos Militares a partir de la Primera Guerra Mundial. Evolución de la Tecnología en el Dominio o Espacio Aéreo. Los Conflictos Militares en el Espacio Exterior. Ejemplos desde la Guerra Fría hasta nuestros días. El Ciberespacio como Dominio de los Conflictos Militares. Evolución en los últimos quince años.

- **Tecnología de Redes I**

Uso de las Redes de Computadoras. Hardware de Redes. Software de Redes. Modelos de Referencia. Estandarización de las Redes. La Capa Física. La Capa de Enlace de Datos. La Capa de Red. La Capa de Transporte. La Capa de Aplicación.

- **Malware I**

Introducción general a los Virus Informáticos. Características y funcionalidades de los Gusanos o Worms. Arquitectura general y funcionalidades de los Gusanos o Worms. Características y funcionalidades de Spyware. Ejemplos de Spyware. Distintos niveles de sofisticación del Spyware. Adware; analogía y diferencias con el Spyware. Scareware; finalidad, arquitectura y funcionalidad. Trojanos y backdoors. Naturaleza, Arquitectura y funcionalidad. Rootkits entendido como modificaciones maliciosas en el Sistema Operativo. Botnet: Conformación y distintos usos de las redes de computadores zombis.

- **Fundamentos y Gerenciamiento de la Ciberdefensa y de la Ciberseguridad**

El Planeamiento Estratégico de la Ciberdefensa y de la Ciberseguridad. La formación y el entrenamiento de los Recursos Humanos en Ciberdefensa y Ciberseguridad. El Gerenciamiento de la Ciberseguridad de la Infraestructura Crítica. El Gerenciamiento de la Ciber Disuasión. Principios y Sistemas de Gestión - COBIT, ITIL, ISO 27000 (análisis de casos prácticos).

- **Ciber Ataques masivos a Sistemas de Información**

Características de los Ciber Ataques Masivos a Sistemas de Información. La detección de las primeras fases de Ciber Ataques Masivos a Sistemas de Información. La Defensa ante Ciber Ataques Masivos – Roles de la Ciberdefensa y de la Ciberseguridad. La utilización del enfoque Análisis de Flujos de Redes en los casos de Ciber Ataques Masivos a Sistemas de Información. El "Problema de la Atribución" en los casos de Ciber Ataques Masivos a Sistemas de Información

ASIGNATURAS ESPECÍFICAS - ASPECTOS OPERATIVOS DE CIBERDEFENSA Y CIBERSEGURIDAD

- **Principios y enfoques de Diseño de Software Seguro**

Balance entre requerimientos funcionales y no funcionales, detección de fallas, recuperación, integridad, validación y verificación. Estudio comparativo de las metodologías para desarrollar software seguro: Correctness by Construction (CbyC), Security Development Lifecycle (SDL), Cigital Touchpoints, Common Criteria, Comprehensive, Lightweight Application Security Process (CLASP) y TSP-Secure.

- **Proyecto sobre Principios y enfoques de Diseño de Software Seguro**

Elaboración de un proyecto de diseño de Software Seguro utilizando un enfoque metodológico específico seleccionado a tal fin.

- **Teoría Organizacional y Psicología Organizacional**

Teoría organizacional vista como la naturaleza, propósitos, estructuras y diseños organizacionales; el Comportamiento Organizacional entendido como el conjunto de actos reales y virtuales llevados a cabo por las personas en el rol de miembros de una organización. Pautas culturales y productivas tangibles (hábitats, productos y tecnologías) e intangibles (cultura organizacional. servicios, marcas, conocimiento y know how. Psicología organizacional vista como el conjunto de factores psicológicos relativos al comportamiento organizacional. Incluye el estudio de las aptitudes, factores de personalidad, actitudes, motivos, intenciones, procesos decisorios, metas, satisfacción, salud y autorrealización laboral. Rol de los líderes y gerentes en una organización.

- **Diseño y Desarrollo de la "Data Exchange Layer" en ambientes de Gobierno**

"Data exchange" como proceso que toma datos estructurados según un esquema "fuente" y los convierte en datos estructurados en un esquema "destino" (target schema) asegurando que la representación o contenidos no varíen respecto del significado de dichos datos en el esquema "fuente". "Data exchange" en ambiente de gobierno. Uso de datos compartidos entre las diversas áreas de gobierno sin pérdida de sus contenidos semánticos, Diseño de la "Data Exchange Layer" como desafío de Ciber Seguridad. Las Ciber Vulnerabilidades de la "Data Exchange Layer" en ambiente de gobierno. La mitigación de dichas vulnerabilidades.

- **Data Mining - Datawarehousing - Big Data**

Data Mining o minería de datos. Extracción de información significativa de grandes Bases de Datos o Data Warehouses. Obtención de información asociada a la "Inteligencia del Negocio". Tendencias y Correlaciones. Optimización del Proceso de Toma de Decisiones. Data Warehouse como almacenamiento de los datos orientados a la transacción. Data Warehouse como conjunto de estructuras de datos organizadas específicamente para consultas y despliegues específicos. Big Data o datos masivos como proceso de recolección de grandes cantidades de datos. Análisis para encontrar información implícita, patrones recurrentes, nuevas correlaciones. Big Data como respuesta al agotamiento de los medios tradicionales de almacenamiento.

- **Tecnología de Redes II**

World Wide Web. Arquitectura. Documentos web estáticos. Documentos web dinámicos. HTTP: Protocolo de Transferencia de Hipertexto. Web inalámbrica. Audio digital. Audio de flujo continuo. Radio en Internet. Voz sobre IP. Video. Compresión de Video. Video bajo demanda.

- **Seguridad en Redes de Computadoras**

Seguridad en la comunicación: Ipsec. Firewalls. Redes privadas virtuales. Seguridad inalámbrica. Protocolos de autenticación. Seguridad en Correo Electrónico. Seguridad en la Web.

- **Malware II**

Arquitectura de un esquema de Denegación de Servicios Distribuida. Malware tipo Stuxnet. Arquitectura. Funcionalidades. Análisis del caso Natanz. Malware de tipo modular Shamoon - Disttrack. Arquitectura. Funcionalidades. Caso de Saudi Aranco Oil Company. Análisis. Análisis integral del malware tipo modular Flame.

TALLERES DE INVESTIGACIÓN SUPERVISADA Y/O TUTORIALES EN ASPECTOS OPERATIVOS DE CIBERDEFENSA Y CIBERSEGURIDAD (preparatorios para el Trabajo Final)

La aplicación de los conceptos y enfoques de la Metodología de la Investigación constituyen la esencia de la componente "Investigación Supervisada" de este módulo. Los tutoriales disponibles (asociados a los Talleres de Investigación) serán definidos por la Dirección de la Maestría para cada una de las cohortes correspondientes a la Orientación "Aspectos Operativos de la Ciberdefensa y Ciberseguridad". Se pondrá énfasis en la redacción de Informes correspondientes a los trabajos de Investigación Científica y se alentará la elaboración de publicaciones y/o presentaciones en congresos y jornadas.

- **Talleres de Investigación Supervisada**

Estos talleres están incluidos en las 160 hs de los Talleres de Investigación Supervisada.
El objetivo primordial del taller es el de dotar a los futuros egresados de las herramientas y el apoyo que les permitan elaborar el Proyecto de Trabajo Final de Maestría.

Una vez aprobados los Talleres de Investigación Supervisada (asociados a los Talleres de Investigación), continuarán con la elaboración del Trabajo Final junto al Director de Trabajo Final.

- **Trabajo Final de Maestría**

Se espera que los Trabajos Finales de Maestría consistan en una investigación empírica que se realizará a partir de datos recolectados por el maestrando o del tratamiento original de datos secundarios de acuerdo a las pautas del método científico. El diagnóstico así elaborado puede dar lugar a la elaboración de propuestas de mejora, cambio o intervención

Dado que se espera que egresen "investigadores del Ciberespacio", los maestrandos deberán elaborar un trabajo final que deberá tener un enfoque multidisciplinar, escrito e individual según las siguientes opciones:
a) Con forma de Tesis ("Problema, Solución Propuesta al Problema seleccionado como Objeto de Estudio y Sustento de la pertinencia, relevancia y originalidad de la Solución Propuesta). Deberán ser evidentes i) el estudio crítico de información / conocimiento relevante centrado en el Problema ii) la correcta aplicación de los conceptos y herramientas de la Metodología de la Investigación Científica.
b) Con forma de Proyecto Profesional Innovador en Ciberdefensa y/o Ciberseguridad de evidente originalidad y gran relevancia.