Seminario II

Curso Académico: (2023 / 2024) **Fecha de revisión: 21-04-2023**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: ALMENARES MENDOZA, FLORINA

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

OBJETIVOS

El objetivo de esta asignatura es acercar los problemas y soluciones más acuciantes de la industria, administración, defensa e investigación a los estudiantes. Por lo que al terminar el curso los estudiantes serán capaces de alcanzar las siguientes competencias generales (CG1, CG3, CG4) y específicas (CE1, CE2, CE3 y CE7), junto con otras asignaturas:

- Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación o temáticas recientes.

- Aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

- Integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

- Poseer las habilidades de aprendizaje que les permitan continuar estudiando.

- Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

- Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido.

- Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

- Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.

- Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.

- Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.

En cuanto a los resultados de aprendizaje, a la superación de esta asignatura los estudiantes deberán ser capaces de:

- Comprender las nuevas tendencias de las TIC, sus riesgos asociados, así como juzgar la idoneidad para contrarrestarlos de los servicios y mecanismos de seguridad actuales y en desarrollo.

- Conocer el marco legal, español, comunitario e internacional en el que desenvuelve la Ciberseguridad, Ciberdefensa y Ciberataque.

- Diseñar un modelo integral (legal, físico, administrativo-organizativo y técnico) de protección un (o varios) sistema de información real, operando en un cierto entorno.

- Conocer en las actuaciones del Poder Judicial, los Cuerpos de Seguridad y las Fuerzas Armadas en la prevención y persecución de ciberdelincuentes, ciberterroristas y ciberespías y la protección de las infraestructuras críticas.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

A través de los distintos seminarios o talleres que se propongan los estudiantes podrán tener acceso a la experiencia de profesionales de reconocido prestigio (de la industria, administración, defensa e/o investigación) cuya labor profesional está relacionada con la Ciberseguridad en sus facetas legales, administrativas y de gestión y legales. Por otra parte, los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Clases magistrales abiertas al diálogo y a la discusión en grupo, además de clases teórico-prácticas, realizadas por diversos profesionales del campo de la ciberseguridad: Administración, Fuerzas de seguridad, Judicial, Empresas.

Además, se recomienda la lectura de textos y bibliografía complementaria sobre la temática de los seminarios.

SISTEMA DE EVALUACIÓN

La asistencia a los seminarios es obligatoria.

La evaluación se realizará a partir de un trabajo escrito a elegir entre las ponencias (50%), un examen final (40%) y la participación (10%).

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60