Seminario I

Curso Académico: (2023 / 2024) **Fecha de revisión: 21-09-2023**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: SANCHEZ MACIAN PEREZ, ALFONSO ALEJANDRO

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No procede

OBJETIVOS

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.

Que los estudiantes sepan 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.

Que los estudiantes sean capaces de 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.

Que los estudiantes posean 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.

RESULTADOS DEL APRENDIZAJE

A la superación de esta materia los estudiantes 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

El objetivo es acercar los problemas y soluciones más acuciantes en cada momento de la industria, administración, defensa e investigación a los alumnos. A través de las 12 conferencias propuestas los alumnos pueden tener acceso a la experiencia de 12 profesionales de reconocido prestigio cuya labor profesional está relacionada con la Ciberseguridad en sus facetas legales, administrativas y de gestión y legales. Por otra parte, las conferencias más académicas ponen 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, las 12 ponencias pueden encuadrarse dentro de cualquiera de las materias del máster.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS

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.

Conferencias (pueden ser teóricas, práticas o teórico/prácticas)
Trabajo individual del estudiante

METODOLOGÍAS DOCENTES
Las ponencias se imparten con soporte de medios informáticos y audiovisuales y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.

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