Seminar I

Academic Year: (2024 / 2025) **Review date: 19-04-2024**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: SANCHEZ MACIAN PEREZ, ALFONSO ALEJANDRO

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Not applicable

OBJECTIVES

Possess and understand knowledge that provides a basis or opportunity to be original in the development and / or application of ideas, often in a research context.

That students know how to apply the knowledge acquired and their ability to solve problems in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of ¿¿study.

That students are able to integrate knowledge and face the complexity of making judgments based on information that, being incomplete or limited, includes reflections on social and ethical responsibilities linked to the application of their knowledge and judgments.

That the students possess the learning skills that allow them to continue studying.

Understand and apply research methods and techniques of cyber attacks to a specific installation.

Conceive, design, implement and maintain a global Cyber ¿¿defense system in a defined context.

Know the technical regulations and the legal dispositions of application in the cybersecurity matter, its implications in the design of systems and in the application of security tools.

Know the current trends in cyberattack techniques and the experiences learned in real cases.

Apply the appropriate services, mechanisms and security protocols in a specific case.

Analyze the risks of the introduction of personal devices in a professional environment. Know and apply the measures to control these risks.

LEARNING RESULTS

Upon the passing of this subject students students should be able to:

Understand new ICT trends, their associated risks, as well as judge the suitability to counteract them from current and developing security services and mechanisms.

Know the legal, Spanish, community and international framework in which Cybersecurity, Cyber Defense and Cyber attack develops.

Design an integral model (legal, physical, administrative-organizational and technical) to protect one (or several) real information system, operating in a certain environment.

To know in the actions of the Judicial Power, the Security Corps and the Armed Forces in the prevention and persecution of cybercriminals, cyberterrorists and cyberespies and the protection of critical

infrastructures.

DESCRIPTION OF CONTENTS: PROGRAMME

The objective is to bring the most pressing problems and solutions in every moment of industry, administration, defense and research to the students. Through the 12 proposed lectures, students can access the experience of 12 professionals of recognized prestige whose professional work is related to cybersecurity in its legal, administrative and managerial and legal facets. On the other hand, the more academic conferences put the students in contact with the state of the art in concepts, protocols, developments and tools in specific subjects related to the cybersecurity.

Therefore, the 12 presentations can fit within any of the subjects of the masters.c topics related to cybersecurity. Therefore, the seminars will be able to fit within any of the subjects of the masters.

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES

Lecturers will give talks open to group discussion, interaction and practices. Lecturers are professionals to be selected from different Cybersecurity related to fields: Administration, Law, Army and Police, and Companies.

Lectures (can be theoretical, practical or theoretical / practical)
Individual student work

TEACHING METHODOLOGIES
The presentations are given with support of computer and audio-visual means and the bibliography is provided to complement the learning of the students.

ASSESSMENT SYSTEM

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

Assistance to the lectures is compulsory.

Assessment will be done based on an essay related to one of the seminars (50%), a final exam (40%) and the participation (10%)