Seminar II

Academic Year: (2023 / 2024) **Review date: 21-04-2023**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: ALMENARES MENDOZA, FLORINA

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 2

OBJECTIVES

This subject will contribute to the following basic general (CG1, CG3, CG4) and specific (CE1, CE2, CE3 y CE7) competences:

- To know and understand knowledges that can give a opportunity to achieve original developments in a research context.

- To be able to apply acquired knowledge and their capacity of problem solving in new or less known environments, within the wider (even disciplinary) contexts related to their field of study.

- To be able to link knowledges and face the complexity of judging from incomplete or limited information to include their own reflections over ethical and social responsibilities in the application of their knowledge.

- To continue their self learning to keep updated in their field of studies.

- To understand and apply methods and techniques of cyberattacks to a given site under test.

- To conceive, design, deploy and maintain a Cyberdefense Global System in a given context.

- To know the technical and legal framework in cybersecurity, their implications in system design and in the usage of security tools.

- To know the actual trends in cyberattacks and the experiences leant from real cases.

- To apply the services, mechanisms and security protocols in a given case.

- To analyze the risks of introducing personal devices in a professional environment. To know and apply the controls for such risks.

LEARNING OUTCOMES

- Knowledge of the trends in information technologies, their associated risks, and to judge on the security services and mechanism suitability for avoiding such risks.

- Knowledge about the legal framework related to Cybersecurity.

- Capability to design an integral model (legal, physical, administrative and technical) to protect a real system operating under a known environment.

- Knowledge about professional activities of the Law and Military forces in the prevention and prosecution of cyber-(delinquents, terrorists, spies) and about critical infrastructure protection.

DESCRIPTION OF CONTENTS: PROGRAMME

The objective is to have a closer view of problems and solutions from the industry, administration, defense and research to the students. Different lectures will give the students the opportunity of hearing and discussing with experienced professionals involved in some of the diferent aspects of the Cibersecurity: legal, administrative or management . Besides some academic lectures can provide the students with the state of the art in concepts, protocols, developments and tools in different fields

related to Cibersecurity. Seminars can be a powerful tool that can relate to any of the Master subjects.

LEARNING ACTIVITIES AND METHODOLOGY

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.

In addition, readings related to topic of the talks are recommended.

ASSESSMENT SYSTEM

Assistance at the lectures is mandatory.

Students will deliver a written essay of their choice out of the lectures. The evaluation will be made from assistance (10%), the written essay (50%), and a final exam (40%).

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