Technologies Applied to Security II

Academic Year: (2024 / 2025) **Review date: 03-06-2024**

Department assigned to the subject: null

Coordinating teacher:

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 1

SKILLS AND LEARNING OUTCOMES

K3-To have the scientific and technical knowledge necessary to face the technological and telecommunications challenges related to security, and to know the capabilities provided by new technologies, adapting to their evolution and application in the performance of their duties.
K4-Have the forensic science skills necessary to lead forensic teams and conduct forensic reports related to crime.
K7-Know the main procedures and technologies applied to defence and the main trends in their development.
S2-Solve problems, analyse and synthesise information to evaluate and make judgements with agility, initiative and creativity, identifying opportunities for improvement and adapting to complex situations related to defence and public security.
S4-Apply statistical knowledge in the analysis of crime and its security implications at national and international level
S7-To be agile in the digital environment, including the legal and ethical dimension, and to understand the fundamentals of process analysis and modelling, data governance and information for decision making.
C1-Demonstrate the ability to exercise leadership and assume command, adapting to each situation and paying permanent attention to safety and compliance with the rules and measures established to guarantee the integrity of personnel, installations, equipment, systems, material and documentation, in accordance with the regulations in force.
C3-To analyse and draw conclusions from experiences based on case studies in which the engagement of public safety professionals with the citizens they serve has been particularly relevant.
C4-Design and carry out tasks or projects using creativity and curiosity to contribute value with an entrepreneurial attitude, reasoning with arguments and being able to deliberate on their validity by subjecting one's own and external convictions to debate.
C6-Solving complex situations in the field of security through the application of scientific-technological knowledge and tools.

DESCRIPTION OF CONTENTS: PROGRAMME

Introduction to cybersecurity. Cryptographic mechanisms and protocols. Authentication. Access control. Network security. Software security. Vulnerabilities. Malware. Privacy and cybersecurity regulation.

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