Cybersecurity and Data Protection

Academic Year: (2023 / 2024) **Review date: 02/06/2023 09:40:11**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: CALLEJO PINARDO, PATRICIA

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 2

OBJECTIVES

Students should understand the needs of advanced information systems, as well as the main technological tools applicable in companies and in business, regarding security, information protection and cryptography.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to Cybersecurity
a. Principles of cybersecurity
b. Threats, Attacks and Vulnerabilities
c. Security Services and Mechanisms
2. Principles of Protection of Information
a. Encryption of information. Encryption types.
b. Symmetric and asymmetric cryptography
c. Digital signature and certificates
d. Cryptocurrency. Bitcoin, blockchain, etc.
3. Security in the transmission of information.
a. Secure communications protocols. HTTPS and virtual private networks (VPN)
b. Secure Email
4. Management and Administration of Cibersecurity.
a. Information Systems Security Management. ISO / IEC 27000 family
b. Risk Analysis and Management
c. Business Continuity Plans
5. Legal Aspects of Data Protection.
a. The General Data Protection Regulation (GDPR).
b. Supervisory authority
c. Data Protection Officer (DPO).

LEARNING ACTIVITIES AND METHODOLOGY

AF1. THEORETICAL-PRACTICAL CLASSES. They will present the knowledge that students should acquire. They will receive the class notes and will have basic reference documents to facilitate the follow-up of the classes and the development of the subsequent work. Exercises and problems that students may have, will be solved and workshops and evaluation tests will be carried out to develope the necessary skills.
AF2. TUTORIALS. Individualized (individual tutorials) or group (collective tutorials) assistance to students will be provided by the teacher.
AF3. INDIVIDUAL OR GROUP STUDENT WORK.
MD1 THEORETICAL CLASSES. The teacher will present the main concepts of the subject supported by audiovisual media. Also, materials and bibliography are provided to complement the students' learning.
MD2. PRACTICAL CLASSES. Resolution of practical cases, problems, etc. raised by the teacher individually or in groups.
MD3. TUTORIALS. For subjects of 6 credits, 4 hours will be dedicated with 100% of attendance.

ASSESSMENT SYSTEM

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

SE1. Non-continuous evaluation:
Students who do not follow the continuous evaluation should do a final exam composed of questions related to theory and lab assignments/works. Both parts have to be passed separately (50%) to pass the subject. The result of this exam (both parts) corresponds to 100% of the final mark and you should get 50% min. to pass the subject.

SE2. Continuous evaluation:
- Lab assignments/ Works (30%)
- Mid-term exam (30%)
- Final Exam (40%)

Marks are added when 40% of the final exam is passed.

Extraordinary call:
Students who do not pass the subject in the ordinary call will have an extraordinary call to pass it:
1. If the student followed the continuous evaluation: the grade will be the one established in the program of the subject for the ordinary call. However, the student will have the right to be graded only with the grade obtained in the final exam if it is more favorable.
2. If the student did not follow the continuous evaluation: the grade will be the grade obtained in the final exam. However, the teacher may authorize the delivery of the exercises of the continuous evaluation in the extraordinary call, being evaluated in such case in the same way as in the ordinary call.

BASIC BIBLIOGRAPHY

- Comisión EU Reglamento General de Protección de Datos (RGPD), 2018, Comisión EU.

- EU Commission General Data Protection Regulation (GDPR) 2018, EU Commission.

- ISO organization ISO/IEC 27001 Information security management, ISO.

- Peltier, T. R. Information security risk analysis, Auerbach publications., 2010

- Stallings, W. Cryptography and network security: principles and practice (4th edition), Prentice Hall., 2005