Cybersecurity and Data Protection

Academic Year: (2019 / 2020) **Review date: 08-05-2019**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ MANZANO, LORENA

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 2

OBJECTIVES

CB1. Students have proven knowledge in an area of ??study that starts in secundary educatian and it is usually at a level that, although supported by advanced textbooks, also includes some aspects that imply knowledge coming from the forefront of his field of study
CB2. Students know how to apply their knowledge to their work or vocation in a professional manner and that they possess the skills that are usually demonstrated through the elaboration and defense of arguments and the resolution of problems within their area of study
CB3. Students have the ability to gather and interpret relevant data (usually within their area of ??study) to make judgments that include a reflection on relevant issues of social, scientific or ethical nature
CG3. Students should be able to manage, identify, gather and interpret relevant information on issues related to business in the digital age.
CG5. Students should know how to design, plan and align the evolution of technology (systems and information and communication technologies) with respect to the organization of the company and its evolution.
CG6. Students should know how to make judgments that include an ethical reflection on fundamental business and economic issues in the digital age.
CT1. Students should be able to work in multidisciplinary and / or international teams as well as to organize and plan the work taking the right decisions based on the available information, gathering and interpreting relevant data to make judgments and critical thinking within the study area.
CT3. Students should be able to assess the reliability and quality of the information and its sources using such information in an ethical manner, avoiding plagiarism, and in accordance with the academic and professional conventions of the study area.
CE13. Students should understand the advanced information systems, as well as the main technological tools applicable in companies and in business, as well as their needs in security and information protection issues, cryptography, artificial intelligence and big data
RA1. Students should have acquired advanced knowledge and demonstrated an understanding of the theoretical and practical aspects and the methodology of work in the field of business administration and digital technology with a depth that reaches the forefront of knowledge
RA3. Students should have the ability to collect and interpret data and information on which to base their conclusions including, when necessary and relevant, reflection on social, scientific or ethical issues in the field of the digital age company.

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

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. 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 20% of the final exam is passed.

The evaluation of the extraordinary exam follows the same criteria as aforementioned.

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

BASIC BIBLIOGRAPHY

- EU Commission. https://www.eugdpr.org/ General Data Protection Regulation (GDPR), 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