Data protection & cybersecurity

Academic Year: (2022 / 2023) **Review date: 26-05-2022**

Department assigned to the subject: Computer Science and Engineering Department, Telematic Engineering Department

Coordinating teacher: CALLEJO PINARDO, PATRICIA

Type: Compulsory ECTS Credits : 6.0

Year : 2 Semester : 2

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to Cybersecurity
2. Principles of Data Protection
3. Privacy in Big Data
4. Security management and government
5. Legal aspects of data protection

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.
AF8: WORKSHOPS AND LABORATORIES
AF9: FINAL EXAM. In which the knowledge, skills and abilities acquired throughout the course will be assessed globally.
MD1: CLASS THEORY. Exhibitions in the teacher's class with support of computer and audiovisual media, in which the main concepts of the subject are developed and materials and bibliography are provided to complement the students' learning.
MD2: PRACTICES. Resolution of practical cases, problems, etc. raised by the teacher individually or in groups.
MD3: TUTORIALS. Individualized assistance (individual tutorials) or group (collective tutorials) to students by the teacher.
MD6: LABORATORY PRACTICES. Applied / experimental teaching to workshops and laboratories under the supervision of a tutor.

ASSESSMENT SYSTEM

E2: FINAL EXAMINATION In which the knowledge, skills and abilities acquired throughout the course will be assessed globally.
E1: PARTIAL EXAM.
CE: CONTINUOUS EVALUATION. Labs and presentations throughout the course will be evaluated.
CE=Lab ABE+Lab Pilar+MAGERIT Presentations+Extra.
Extra=exercise on Statistical Disclosure Control + participation in DoS and Business continuity + participation in regular classes and in the forum with questions and comments.
E1, E2, Lab ABE, Lab Pilar, MAGERIT Presentations and the Extra are each of them evaluated over 10 points.

A minimum mark of 4 is required in E2 to pass the course.

FM: Final Mark= 0.4*E2+0.6*(E1+CE)/4

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

BASIC BIBLIOGRAPHY

- Alfred J. Menezes , Jonathan Katz , Paul C. van Oorschot , Scott A. Vanstone Handbook of Applied Cryptography (Discrete Mathematics and Its Applications), CRC Press, 1996
- Josep Domingo-Ferrer, David Sánchez, Jordi Soria-Comas Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections, Morgan & Claypool Publishers , 2017

BASIC ELECTRONIC RESOURCES

- Miguel A. Amutio, Javier Candau, Pepe Mañas . MAGERIT ¿ version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method: https://administracionelectronica.gob.es/pae_Home/dam/jcr:80b16a91-75b1-432d-ab23-844a12aab5fc/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf