

Academic Year: (2022 / 2023)

Review date: 20-05-2022

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 0

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

No specific requirements are in place

OBJECTIVES**BASIC SKILLS**

CB8 Students must be able to integrate knowledge and face the complexity of making judgments from information that, incomplete or limited, includes reflections on social and ethical responsibilities linked to the application of their knowledge and judgments

CB9 Students must know how to communicate their conclusions and the latest knowledge and reasons that support them to specialized and non-specialized audiences in a clear and unambiguous manner

CB10 Students must have the learning skills that allow them to continue studying in a way that will be largely self-directed or autonomous.

GENERAL COMPETENCES

CG1 Understand the impact of new digital environments on libraries, archives and other documentation services, as well as the role of information and documentation professionals and experts in this technological and social context.

CG2 Identify lines of technological innovation in libraries and archives and documentation centers, and undertake possible projects for their development. The

CG5 Recognize the growing importance of teamwork in the world of work and demonstrate adaptability and integration in different work environments, maintaining relationships and communication flows.

CG8 To value the rigorous and well-done work, in planning, organizing and developing one's own activities, demonstrating initiative, creativity and sense of responsibility, maintaining interest throughout the process, and feeling personal satisfaction with the results achieved.

CG9 Integrate knowledge, make judgments and communicate their conclusions, as well as the latest knowledge and reasons that support them, to specialized and non-specialized audiences in a clear and unambiguous way.

CG10 Recognize the need for continuous adaptation to different jobs in different productive sectors, and technological and organizational innovations related to the profession, showing interest in incorporating new techniques, processes, tools and techniques into the profession's own activities. technologies.

SPECIFIC COMPETENCES

CE1 To know and analyze the current state and future prospects of technological progress and their application in libraries and archives.

CE5 Examine the main security problems of network information, as well as the knowledge of the protection systems existing in this digital environment

LEARNING OUTCOMES

This subject focuses on training students in the various technical and legal aspects of the resources that determine the tools to support information tasks and documentaries. A crucial aspect of training is that students acquire the skills necessary for the implementation of digital document management projects (EDRMS). To this end, the student will be given the necessary skills to plan, analyze and manage the implementation of an appropriate solution to typical scenarios within the framework of digital continuity and access to information in networks. He will be trained in basic skills to evaluate different technological alternatives for the creation of EDRMS ensuring their access by users and authorized institutions.

The student after passing the subject must:

Know and understand the objectives of information security and the threats and vulnerabilities of information systems.

Know and understand the problems of authentication and integrity of the electronic document and the tools to guarantee them.
Know and apply the legal regime of administrative transparency and public information.
Understand and apply the legal regime of information and documentation in public organizations on storage media.

DESCRIPTION OF CONTENTS: PROGRAMME

The primary objective for students is to recognise IT security as an unavoidable aspect of digital information and its supporting systems. Subordinated to this overall goal, the student will be able to identify the dimensions of IT security (confidentiality, integrity and availability), threats (technical or physical) that digital information is exposed to and to know and use the main tools to protect it.

The program is divided into five main sections:

PART ONE: Students will discuss the dimensions of security (confidentiality, integrity, availability), emphasising their relative importance according to specific environments and introduce specific security measures for each one of them. The different types of threats and the vulnerabilities of IT systems will be described.

PART TWO: We analyse the problems of conservation over a long time and safe destruction of electronic documents.

PART THREE: We consider data encryption as an essential tool for security, exploring various systems and their intended uses.

PART FOUR: Signature and digital certificates as a basic tool to guarantee integrity together with document authenticity and non-repudiation.

PART FIVE: We will present the security problems arising in IT systems accessed via computer networks as well as the specific protection mechanisms.

Thus, the detailed program is as follows:

1. Introduction to digital document security
 - 1.1 - Security goals
 - 1.2 - Security mechanisms: legal, administrative, physical and technical protections
 - 1.3.- Malware
 - 1.4.- IT security. Vulnerabilities.
2. Electronic documents: Resiliency and removal
 - 2.1 - Resiliency techniques. Use of hash functions
 - 2.2 - Secure removal
 - 2.3.- Legal / administrative storage conditions for documents containing personal data
3. Data Encryption
 - 3.1 - Introduction to data hiding techniques
 - 3.2 - Cryptosystem scheme
 - 3.3.- Secret- and public-key encryption
 - 3.4.- Encryption in Microsoft Office, PDF and other user apps
 - 3.5.- Specific encryption software
4. Digital signature and user authentication
 - 4.1.- Introduction to digital signature. Differences with handwritten one
 - 4.2. Timestamping
 - 4.3.- Digital Certificates. Types
 - 4.4 - Certification Authorities. Examples. The DNI-e
 - 4.5.- Certificate revocation
 - 4.6.- User Authentication
5. Computer Network Security
 - 5.1 - Threats to computer networks.
 - 5.2.- Secure connection protocols with servers. TLS/SSL

LEARNING ACTIVITIES AND METHODOLOGY

TRAINING ACTIVITIES OF THE STUDY PLAN RELATED TO SUBJECTS

AF1 Individual work to study theoretical-practical materials (40 h)

AF3 Theoretical-practical classes (3 h)

AF4 Tutorials

AF5 Group work (47 h)

TEACHING METHODOLOGIES

MD1 Lectures with support of computer and audiovisual media, in which the main concepts of the subject are developed and the bibliography is provided to complement the students' learning.

MD3 Resolution of practical cases, problems, etc. raised by the teacher individually or in a group

MD5 Preparation of individual and group work and reports

MD6 Reading of theoretical and practical teaching materials

Office hours will be published in Aula Global, the corporate e-learning platform. There will be two time frames, one for physical attendance and another one for online attendance. In any case, this should be requested by e-mail sufficiently in advance. Apart from these time frames, students may request office hours in other time frames, upon availability of the lecturer

ASSESSMENT SYSTEM

SE2 Individual or group work done during the course

SE4 Exam or Final Work *

* The final exam or work will be done in face-to-face mode, at Carlos III University or at a university-sponsored center that guarantees the student's identity, and must pass it in order to be able to approve the corresponding subject.

1. Ordinary sitting

Theoretical Essay(s).

- It/they represent/s 25% of the final mark

- Compulsory

- Exclusively in groups, unless otherwise stated at the beginning of the subject

Practical assignment(s).

- It/they represent/s 25% of the final mark

- Compulsory

- Exclusively in groups, unless otherwise stated at the beginning of the subject

Final practical Work.

- It represents 25% of the final mark

- Compulsory

- Individual

Final exam

- It represents 25% of the final mark

- Theoretical / Practical

- Compulsory and individual

In order to pass the subject, the following two conditions apply:

- Pass mark: 5.0

- All assignments must be handed in.

2. Extraordinary sitting

In the extraordinary sitting, the following rules apply:

a. The exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept. The exam pass mark will again be 5.0 marks out of 10. If the final practical work was passed, it will not be necessary to repeat it.

b. If the assignments were not handed in in the ordinary sitting, students will be allowed to prepare them (potentially with a different scope). They will follow the same marking scheme as in the ordinary

sitting.

% end-of-term-examination:	50
% of continuous assessment (assignments, laboratory, practicals...):	50

BASIC BIBLIOGRAPHY

- Paar, C.; Pelzl, J. Understanding Cryptography, Springer, 2010
- Ronald L. Mendell Document Security: Protecting Physical and Electronic Content., Charles C Thomas Pub Ltd, 2007

ADDITIONAL BIBLIOGRAPHY

- Charlie Kaufman, Radia Perlman, Mike Speciner Network Security: Private Communication in a Public World (Chap. 2), Prentice Hall, Second edition (2002)
- Christoph Paar, Jan Pelzl Understanding cryptography (Chap. 1 & 6), Springer-verlag, 2010

BASIC ELECTRONIC RESOURCES

- Adobe, Inc. . A primer document on electronic document security:
http://www.adobe.com/security/pdfs/acrobat_lifecycle_security_wp.pdf
- Different contributors . Intypedia -- information security encyclopedia (Chap. 1, 2 and 3): <http://www.intypedia.com>