

Academic Year: ( 2023 / 2024 )

Review date: 28-04-2023

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 2

**REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)**

not applicable

**OBJECTIVES****BASIC COMPETENCES:**

Form professionals with the ability to integrate knowledge and form judgments from incomplete or inaccurate information.

Form professionals with the ability to communicate thoughts and judgments and give reasons accordingly.

Form professionals with the ability to study and learn autonomously.

**LEARNING RESULTS:**

1. Develop, deploy and maintain an Information Security Management System (ISMS).
2. Know the methodologies for evaluating systems and products and their certification procedures.
3. Know the legal framework of cybersecurity.

**DESCRIPTION OF CONTENTS: PROGRAMME**

1. Information security in the State. National cybersecurity scheme. National cybersecurity strategy. Main actors of cybersecurity in Spain and their competences: CCN / CNI; INCIBE; MCCD; CNPIC, etc. Cybercrime in Spain.
2. Standardization, evaluation, certification and accreditation. Standardization institutions. Legal framework.
3. Information security management systems. ISO / IEC standards. 27XXX series. UNE-ISO / IEC 27000: 2019, UNE-EN ISO / IEC 27001: 2017, UNE-EN ISO / IEC 27002: 2017. Security audit.
4. Evaluation and certification of products and systems.
5. Legal framework of cybersecurity.

**LEARNING ACTIVITIES AND METHODOLOGY****TRAINING ACTIVITIES**

Theoretical lessons.

Theoretical-practical lessons.

Tutoring

Group work

**TEACHING METHODOLOGIES**

Class lectures with computer and audiovisual resources. Main concepts of the subject will be presented together with additional bibliography.

Critical reading of recommended text: press articles, reports, tutorials and/or academic articles. They will be used for class discussions or to extend and consolidate taught concepts.

Class presentations and discussions under the supervision of the teacher based on topics related to the subject, as well as case studies.

**ASSESSMENT SYSTEM**

The assessment mission is to know the degree of compliance with the learning objectives, so all the student's work, individually or collectively will be assessed through continuous assessment of their activities through exercises and tests, practical work and other activities academic training described above.

A formative evaluation will be conducted through continuous feedback, which allows the student to assess what knows and what is expected of him. The final grade will take into account individual

student activities and team activities. The activities carried out during the course, individual or group, will involve 40% of the note, a partial examination (not liberatory) another 20%, while the individual final exam constitute the remaining 40%. In any case, conducting final exam is compulsory, being necessary to obtain at least 40% of the maximum possible score in this test to pass the course.

For the extraordinary call, you can give three situations according to the student:

- a) You have followed the process of continuous evaluation and want to keep note of this. In this case, the test will have the same percentage value in the ordinary call, and the final grade for the course will consider the note of the continuous assessment and the grade obtained in the final exam.
- b) has not followed the process of continuous evaluation. In this case, you have the right to conduct an examination with a value of 100% of the total course grade. This review may contain questions relevant to the activities carried out during the course.
- c) Has followed the continuous evaluation process, but want to be qualified in the resit in the same conditions as in paragraph b).

<b>% end-of-term-examination:</b>	40
<b>% of continuous assessment (assignments, laboratory, practicals...):</b>	60

#### BASIC BIBLIOGRAPHY

- C.M. Fernández Sánchez y M. Piattini Velthuis Modelo para el gobierno de las TIC basado en las normas ISO, AENOR, 2012
- L. Gómez Fernández; P.P. Fernández Rivero Como implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el ENS, AENOR.
- UNE 27000, UNE, 2019
- UNE EN-ISO/IEC UNE-ISO/IEC 27001:2017, UNE.
- UNE EN-ISO/IEC UNE EN-ISO/IEC 27000:2019, UNE.
- UNE EN-ISO/IEC 27001:2017, UNE.
- UNE EN-ISO/IEC 27001:2017, UNE.
- UNE EN-ISO/IEC UNE EN-ISO/IEC 27002:2017, UNE.

#### BASIC ELECTRONIC RESOURCES

- CCN/CNI . Serie CCN-STIC: <https://www.ccn-cert.cni.es/>
- ENISA . Publications: [www.enisa.europa.eu/publications](http://www.enisa.europa.eu/publications)
- INCIBE . Guías: [www.incibe.es/CERT/guias\\_estudios](http://www.incibe.es/CERT/guias_estudios)
- NIST . Special Publications (800 Series): [csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)