Computer systems audit and certification

Academic Year: (2020 / 2021) **Review date: 26-08-2019**

Department assigned to the subject:

Coordinating teacher: RIBAGORDA GARNACHO, ARTURO

Type: Compulsory ECTS Credits : 6.0

Year : 1 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Not applicable

OBJECTIVES

The student must acquire a number of generic skills, knowledge, skills and attitudes, which are described below:

Generic transversal competences:

- Capacity of analysis and synthesis,
- Capacity of organization,
- Capacity of abstraction and deduction,
- Troubleshooting,
- Teamwork,
- Ability to apply knowledge to practice.

Attitude competences:

- Capacity to generate new ideas (creativity),
- Critical attitude with regard to current methodologies,
- Concern for the quality of programmes and information systems,
- Motivation to achieve new goals,
- Interest to investigate and seek solutions to new problems encountered in audits and certification of information systems

Specific competences of the module:

- Ability to secure, manage, audit and certify development quality, processes, systems, services, applications and software products.
- Ability to design, develop, manage and evaluate mechanisms for certification and safety of local or distributed information systems.
- Ability to apply the principles, regulations and standardization.
- Ability to plan, design and implement audit processes and certification of software systems.

Learning outcomes:

- Knowledge of the methodologies of evaluation and certification of systems and products of T.I.
- Knowledge of international agreements on mutual recognition of safety certification and its requirements
- Knowledge of national, European and international norms and standards related to the security of information systems, mainly the standards of the ISO / IEC 27000 family
- Ability to analyze and evaluate, for its application to a specific system, various audit methodologies.
- Ability to carry out an audit of the quality of developments, processes, systems, services, applications and computer products, and their security.
- Ability to perform an audit in accordance with current legislation on treatments and systems containing personal data.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Standardization, evaluation, certification and accreditation. Legal framework.
2. IT Audit and consulting.
3. Standardization of ISMS (ISMS). 27xxx family. Study of the UNE-ISO / IEC 27000, 27001, 27002.
4. Audit of distributed systems and networks. Audit cybersecurity.
5. Audit of treatments and systems subject to legal compliance
6. Certification of systems and products T.I.

LEARNING ACTIVITIES AND METHODOLOGY

Magisterial lectures.

- Dedicated to the teaching of specific matter-oriented skills. To facilitate the task students will receive class notes and have basic reference documentation, to enable them to further elaborate on those topics which are of most interest. In addition, students will have access to current regulations, standards and legal provisions, in audit and certification of software systems.

Individual or in group practices.

- Among other activities, students might perform audits of certain components, systems and networks, to then draw conclusions and develop the corresponding reports. They will also carry out the compliance audit of the data protection legislation in real or anonymized fictitious systems. Similarly, given a specific IT field, students shall identify the de facto standards or law governing relevant security matters. Finally, they will carry out audit work of the quality of a computer system.

Supervised activities.

- Participating in the resolution of practical exercises and case studies. Among other activities, the students will perform the analysis and critical commentary of reports issued by the data control Spanish authority (or other regional and autonomical regulators). Similarly, given a specific IT field, students will have to identify those de facto standards or law governing matters, commenting on the relevant aspects of this normalization. Finally, students will also carry out audits on the quality or on the security of a computer system.

Student personal work:

- Geared especially to the acquisition of the capacity for self-organization and planning of individual work and learning process.

ASSESSMENT SYSTEM

The evaluation system is designed to establish the degree of fulfilment of the learning objectives. All aspects of the students¿ work are evaluated, individually or collectively, through continuous review of the academic training activities described above. A formative assessment allows for continuous feedback, allowing students to assess their achievements and what it is expected from them. The activities carried out during the course, individual or in groups, will be 60% of the mark, while the individual final exam will provide the remaining 40%.

Attending the final exam is compulsory, and the student should get at least 40% of the maximum marks in the exam to be able to pass the unit.

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)

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

BASIC BIBLIOGRAPHY

- AENOR UNE-ISO/IEC 27000:2014. UNE-EN ISO/IEC 27001:2017. UNE-EN ISO/IEC 27002:2017., AENOR, 2014 Y 2015 (según se indica)
- ISACA CISA Review Manual (Certified Information Systems Auditor), ISACA.
- ISACA CISM (Certified Information Security Manager), ISACA.
- ISACA ISACA (Information Systems Audit and Control Association) COBIT , www.isaca.org .
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model., ISO/IEC , July 2009
- JTC1. ISO/IEC ISO/IEC 27007: 2011. Guidelines for information security management systems auditing, ISO/IEC, 2011
- PIATTINI, Mario y otros. Auditoría de Tecnologías y Sistemas de Información., RA-MA. , Madrid, 2008