Public information security management

Academic Year: (2023 / 2024) **Review date: 04-05-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GARCIA CARMONA, ANTONIO

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

There is not requirement

OBJECTIVES

- Identify the threats and vulnerability of an information system and apply the appropriate protection measures.
- Know the organization and structure of cybersecurity in the State.
- Know the de jure or de facto schemes of international, European and national security standardization.
- Manage the security of an information system
- Design a comprehensive information security plan.
- Analyze and manage the risks of a specific installation.
- Prepare a training plan on information security.
- Know the national, European and NATO schemes of information classification, as well as the protection, maintenance and declassification of it and the security measures of the Information Technology systems that handle classified information.

Know the legal framework for information security in Spain and the EU.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Security of information in the State
2. Standardization, homologation, evaluation, certification and accreditation. Legal framework.
3. Introduction to information security.
4. The Information Security Management System. Family ISO 27XXX.
5. The integral security plan for information systems.
6. Risk analysis and management. The MAGERIT method. The PILAR tool
7. Training and awareness plans.
8. Classification of information
9. Legal aspects related to security management.

LEARNING ACTIVITIES AND METHODOLOGY

Training activities include:
Master classes. To facilitate their development, students will receive class presentations in the appropriate web tool and will have basic reference texts that allow them to complete and deepen the most important topics.
Practices, individual or group tutorials and personal work of the student, including tests and exams. All this oriented to the acquisition of practical skills related to the program of the subject.

ASSESSMENT SYSTEM

Theory questionnaires and practical work: 40%
Partial Exam (non-liberatory): 20%
Final written exam in which the knowledge, skills and abilities acquired throughout the course will be evaluated globally: 40%. The completion of this exam is mandatory, being necessary to obtain at least 40% of the maximum possible grade to pass the course.
Final Exam Percentage Weight: 40
Percentage weight of the rest of the evaluation: 60

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

BASIC BIBLIOGRAPHY

- null Autoridad delegada para la protección de la información clasificada. Normas de la Autoridad nacional para la protección de la información clasificada, Ministerio de la Presidencia, 2014
- A. Ribagorda. Seguridad de la información. Curso Complementos de Formación (2ª edición)., Centro Universitario de la Guardia Civil..
- C.M. Fernández Sánchez y M. Piattini Velthuis Modelo para el gobierno de las TIC basado en las normas ISO, AENOR, 2012
- Departamento de Seguridad Nacional Estrategia Nacional de Ciberseguridad, Ministerio de la Presidencia, reacciones con las Cortes e igualdad, 2019
- L. Gómez Fernández; P.P. Fernández Rivero Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS, AENOR, 2015
- null Norma UNE-EN ISO/IEC 27000, UNE, 2019
- null Norma UNE-EN ISO/IEC 27001, UNE, 2017
- null Norma UNE-EN ISO/IEC. 27002, UNE, 2017

BASIC ELECTRONIC RESOURCES

- . ENISA. Publications: http://www.enisa.europa.eu
- . INCIBE. Guías: http://www.incibe.es/CERT/guias_estudios
- . NIST. Special Publication 800-100. Information Security Handbook: A Guide for Managers: https://csrc.nist.gov/publications/detail/sp/800-100/final
- CENTRO CRIPTOLÓGICO NACIONAL . Serie CCN-STIC: https://www.ccn-cert.cni.es/