Public information security management

Academic Year: (2019 / 2020) **Review date: 26/04/2020 20:51:12**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: RIBAGORDA GARNACHO, ARTURO

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

There is not requirement

OBJECTIVES

- Analyze 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.
- Audit the security of an information system, with special emphasis on personal data
- Know the national, European and NATO schemes for classification of information, as well as the protection, maintenance and declassification of this

.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Security of information in the State
2. Introduction to information security.
3. Standardization, homologation, evaluation, certification and accreditation. Legal framework.
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.
10. Audit of the management of security and personal data

LEARNING ACTIVITIES AND METHODOLOGY

The training activities include:
1 Lectures, individual or group tutorials, personal work and student presentations, including theoretical and practical tests and examinations. To facilitate their development students receive class notes in the appropriate web tool and have basic reference texts that allow them to complete and deepen the most important or more fundamental issues.
2nd Practice, individual tutorials and personal work, including tests and examinations. All it aimed at the acquisition of practical skills related to the program for each subject.

ASSESSMENT SYSTEM

% end-of-term-examination/test:	50
% of continuous assessment (assigments, laboratory, practicals…):	50

Questionnaires of theory, practical work: 30%
Midterm Exam (non-releasing) : 20%
Final written exam in which the knowledge, skills and abilities acquired throughout the course will be evaluated globally: 50%. 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.
% end-of-term-examination: 50
% of continuous assessment: 50

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

- 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-ISI/IEC 27001:2014 y su aplicación en el ENS, AENOR, 2015

- null Norma UNE-ISO/IEC 27002:2015, UNE, 2015

- null Norma UNE-ISO/IEC. 27000:2014, UNE, 2014

- null Norma UNE-ISO/IEC. 27001:2014 , UNE, 2014

- A. Ribagorda. Seguridad de la información. Curso Complementos de Formación (2ª edición)., Centro Universitario de la Guardia Civil..

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