Cyber security management and administration

Academic Year: (2019 / 2020) **Review date: 25-04-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: RIBAGORDA GARNACHO, ARTURO

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Not apply

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. In regard to the master plan of information technology of an organization, its security plan and given the available human resources, technological resources and so on, develop an information security plan.
3. Develop a business continuity plan given the maximum available recovery time.
4. Develop a security awareness and training plan regarding the organization structure.
5. Develop and maintain an information classification system.
6. Learn about the working of the Security Operations Centers, as well as their mutual relations and norms for the exchange of security incidents information.
7. Learn about the legal provisions concerning cibersecurity and its applications in the design of secure systems.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction and basic concepts. Normalization, evaluation, certification and accreditation. Institutes for standards. Legal framework.
2. Security management information system. ISO/IEC standards. Series 27XXX. UNEISO/IEC 27000: 2014, UNE-EN ISO/IEC 27001:2017, UNE-EN ISO/IEC 27002:2017. Certifiable standards of the series.
3. Security plans.
4. Training and awareness.
5. Information classification.
6. Business continuity plan. UNE-EN-ISO 22301:2015 and UNE-ISO 22313:2013.
7. Cibersecurity operation centers.
8. Cibersecurity strategies and legal framework.
9. Security auditing. Audit frameworks and standards. Audit of personal data. Evidences. Analysis. Audit report.

LEARNING ACTIVITIES AND METHODOLOGY

TRAINING ACTIVITIES
Theoretical lessons.
Theoretical-practical lessons.
Tutoring
Group work
Individual 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 extent 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 45% of the note, a partial examination (not liberatory) another 15%, 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).

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	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-ISI/IEC 27001:2014 y su aplicación en el ENS, AENOR.
- NORMA UNE-ISO/IEC 27000:2014, AENOR, 2014
- NORMA UNE-ISO/IEC 27001:2014, AENOR, 2014
- NORMA UNE-ISO/IEC 27002:2015, AENOR, 2015

BASIC ELECTRONIC RESOURCES

- ENISA . Publications: www.enisa.europa.eu/publications
- INCIBE . Guías: www.incibe.es/CERT/guias_estudios
- NIST . Special Publications (800 Series): csrc.nist.gov/publications/PubsSPs.html