Risk analisys and systems certification

Academic Year: (2020 / 2021) **Review date: 27-04-2017**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: RUBIO MANSO, JOSE MARIA

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 1

OBJECTIVES

BASIC COMPETENCES

- To be able to link knowledges and face the complexity of judging from incomplete or limited information to include their own reflexions over ethical and social responsibilities in the application of their knowledge (CB8).
- To communicate their conclusions, knowledge and reasoning to non specialized audience in a clear way (CB9).
- To continue their self learning to keep updated in their field of studies (CB10).

GENERAL COMPETENCES

- To know the technical and legal frameworkin cibersecurity, their implications in system design and in the usage of security tools (CG4).
- To develop, deploy and maintain Information Security Management Systems (ISMS) (CG5).

SPECIFIC COMPETENCES

- To know the basic facts the requirements and the procedure of secure systems (CE9).

LEARNING OUTCOMES:

* Develop a risk analysis for an organization to use as a basis for managing the resulting risks, with a clear identification of the asumable risk threshold.
* Know the main criteria (specifically Commons Criteria) and the corresponding evaluation and certification methodologies of security and their implications in the secure architecture development.
* Know the Evaluation and Certification national Schema (Esquema Nacional de Evaluación y Certificación) of Information Technologies, the requirements, and the functions of the evaluation and certification laboratories and Certification Organizations, as well as the implications and extents of the mutual recognition agreements of certifications.

DESCRIPTION OF CONTENTS: PROGRAMME

Risk analysis and system certification:

1. Risk analysis and management
1.1. Concepts
1.2. Standards. UNE/ISO 31000 and 27005. ENS. PCI-DSS
1.3. Methodologies and tools. MAGERIT/PILAR
1.4. Risk Mitigation. Control selection.

2. Evaluation and certification of products and systems.
2.1. Introduction and concepts
2.2. ISO/IEC 15408. Common Criteria. Other criteria.
2.3. Protection profiles
2.4. Evaluation methodologies. ISO/IEC 18045
2.5. Mutual acceptance of certificates

3. National legislation. Orden PRE 2740/2007.
3.1. National legislation. Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
3.2. Evaluation laboratories. Acreditation

3.3. National Certification Body.

LEARNING ACTIVITIES AND METHODOLOGY

Learning activities willl consist of theoretical and practical lectures, tutoring, team working and individual work of the student.

METHODOLOGY

-The teacher will lecture using slides and practical demos to illustrate the students on the concepts. Bibliographic and further material will be provided to the students to go deepr into practical aspects.
- The students will critically review given texts provided by the teacher.
Some specialized press articles and manuals will be given for class discussion or self study
- The students will present contents related to the subject, under the supervision of the teacher, to promote the discussion and constructive criticism
- Students will perform personal or group assignments and deliver the documentation for evaluation, or class discussion.

ASSESSMENT SYSTEM

The assessment system includes:

1. Continuous assessment (60% of the final mark) of the student comprises of one or more of the following methods:
   1.1. Written tests (40%).
   1.2. Individual or collective practical works and reports assigned by the lecturer (15%)
   1.3. Participation in the debates organized throughout the semester (5%).

2. Final exam (40% of the final mark) assessing the knowledge and skills acquired during the course.

For the extraordinary exam there are three cases:

a) Keep the grade obtained during the term in the continuous assessment process and sit an exam for the remaining 40% of the final grade; or

b) Students who have not followed the continuous assessment process will sit an exam for 100% of the final grade. This exam may have questions related to all activities done during the course.

c) Students who have followed the continuous assessment process can request being marked using the procedure discussed in b).

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

BASIC BIBLIOGRAPHY

- null NORMA ISO/IEC 15408-1, ISO, 2009
- null NORMA ISO/IEC 15408-2, ISO, 2008
- null NORMA ISO/IEC 15408-3, ISO, 2005
- null NORMA ISO/IEC 18405, ISO, 2005
- null NORMA ISO/IEC 27005, AENOR, 2008
- null NORMA UNE-ISO 31000, AENOR, 2010
- null NORMA UNE-ISO/IEC 27000, AENOR, 2014
- null NORMA UNE-ISO/IEC 27001, AENOR, 2014
- null NORMA UNE-ISO/IEC 27002, 2015, AENOR

ADDITIONAL BIBLIOGRAPHY

- Debra S. Herrmann Using the Common Criteria for IT Security Evaluation, CRC Press, 2002
- Marquina Llivisaca, Edgar Geovanny Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT, EAE, 2012

BASIC ELECTRONIC RESOURCES

- . ISO Freely Available Standards: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- . MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WMqje_JRKnQ
- . Herramienta PILAR: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html
- . Esquema Nacional de Seguridad (ENS): https://administracionelectronica.gob.es/ctt/ens#.WMqkBvJRKnQ
- . PCI Security Standards Council: https://es.pcisecuritystandards.org/minisite/en/
- . Portal Common Criteria: https://www.commoncriteriaportal.org/
- . Esquema Nacional de Evaluación y Certificación de la Seguridad de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_evaluacion_y_certificacion_de_la_seguridad/pae_Seguridad_Evaluacion_Esquema_Nacional.html?comentarioContenido=0#.WMqk3PJRKnQ