Risk Analysis in Cybersecurity

Academic Year: (2022 / 2023) **Review date: 29-06-2021**

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 framework in 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

- Starting from the inventory of assets of an organization apply some of the existing methodologies to perform the risk analysis and know how to transmit the results to the organization (CE9).

LEARNING OUTCOMES:

*Develop a risk analysis for an organization that allows the identification and evaluation of them.

DESCRIPTION OF CONTENTS: PROGRAMME

Introduction and general concepts on Risk Analysis.
1.1 Concepts: assets, threats, vulnerabilities, safeguards...
1.1.1 Qualitative and quantitative analysis.
1.1.2 Static and dynamic analysis.
1.2 Advanced aspects.
1.2.1 Threat modeling and categorization (STRIDE, DREAD, CAPEC). Web Site Threats (WASC).
1.2.2 Vulnerability Assessment and Penetration Tests (VAPT).
Risk Analysis Methodologies.
2.1 ISACA(COSO), CRAMM, EBIOS, PCI-DSS, NIST SP-800...
2.1 ISO-27005. MAGERIT.
Current and future application environments.
3.1 Cloud Computing.
3.2 Big Data - AI.
3.3 Internet Of Things (IoT).
3.4 Mobile environments (Wireles, Smartphones, ...).

LEARNING ACTIVITIES AND METHODOLOGY

Learning activities will 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. Individual or collective practical works and reports assigned by the lecturer (50%)
   1.2. Participation in the debates organized throughout the semester (10%).

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

- AENOR NORMA ISO/IEC 27005, AENOR, 2008
- Adam. Shostack Threat modeling : designing for security, John Wiley and Sons, 2014
- John R. Vacca Cyber Security and IT Infrastructure Protection, Syngress, 2013

ADDITIONAL BIBLIOGRAPHY

- Gibson, Darril Managing Risk in Information Systems (2nd Edition), Jones & Bartlett Learning, 2014
- Gregory Allen Threat assessment and risk analysis : an applied approach, Butterworth Heinemann, 2016
- Marquina Llivisaca, Edgar Geovanny Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT, EAE, 2012
- Uceda Vélez, Tony ; Morana, Marco M.Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis, John Wiley & Sons Inc, 2015

BASIC ELECTRONIC RESOURCES

- CCN . PILAR : https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html
- CSAE (MAP) . MAGERIT v.3: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WMqje_J
- CVE . Common Vulnerabilities and Exposures: https://cve.mitre.org/
- NVD . National Vulnerability Database: https://nvd.nist.gov/vuln
- OWASP . The OWASP¿ Foundation: https://www.owasp.org/index.php/Main_Page