Information security and technological risk management

Academic Year: (2019 / 2020) **Review date: 22-04-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ MANZANO, LORENA

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None

OBJECTIVES

The following goals are defined in terms of the Learning Outcomes, according to the level for Masters, defined in RD 1027/2011, 15th July.
With regard to KNOWLEDGE ACQUISITION, at the end of the course the student will be able to:
1a. Know and understand the objectives of IT security.
1b. Know and understand the threats and vulnerabilities of information systems.
1c. Know and understand how Big Data analytics may help to address the introduced threats.
1d. Know and understand in detail the application of Big Data analytics techniques to assess the level of risk of an IT system.
With regard to SKILLS ATTAINMENT, students will be able to:
2a. Identify vulnerabilities and threats on digital information systems.
2b. Investigate the main threats and vulnerabilities of information stored or processed in a system in a particular environment.
2c. Find and select appropriate Big Data analytics techniques to protect an IT system, taking into account the legal framework.
2d. Apply Big Data analytics techniques to determine the risk level of a given IT system.
2e. Investigate and develop technical essays on security issues in new environments subject of study.
2f. Take responsibility in a professional environment for tasks related to the research, evaluation and implementation of Big data techniques for security and risk assessment.
With regard to ATTITUDES, after completing the course students should have:
3a. A critical attitude within the field of Big data analytics for security.
3b. A cooperative and team work attitude to obtain the documentation and data needed to analyze and assess the risks of particular IT systems.
3c. A positive attitude to teamwork to coordinate the different points of view (legal, operational, procedural) of the actors involved in the protection of IT systems.
The primary objective for students is to learn how to apply Big Data analytics mechanisms for IT security and privacy purposes. Subordinated to this overall goal, the student will be able to choose the most suitable technique considering the goals (e.g. protecting a given system, reacting against an incident, assessing the risk level) and the existing restrictions (e.g. available data, legal issues, organizational aspects).

DESCRIPTION OF CONTENTS: PROGRAMME

The programme is divided into five main sections:

1.Introduction to big data & security
Information security concepts are introduced, defining those which are especially relevant in the context of Big Data and corporative systems.

2.Security information sources
Tools and techniques to collect and manage security data will be presented. In this way, the security of a network could be monitorized to detect threats.

3.Security data analysis.
SIEMs are introduced as a tool to manage security events at a large scale. The use of SIEM will be linked to security information sources previously learnt. Besides, the relevance of logs management will be described.

4.Security data visualization.
Tools and techniques for the efficient visualization of security data will be explained, together with existing risks in high scale corporative networks.

5. Privacy preservation in big data and legal aspects.
Cryptographic primitives to design privacy-preserving and secure protocols in distributed environments will be described. Recent advances for privacy preserving data analysis, data sanitization and retrieval will be discussed as well. Finally, privacy rules and policies linked to Big Data management will be introduced, emphasizing those related to corporative environments.

LEARNING ACTIVITIES AND METHODOLOGY

Teaching methodology will include:

(1) theoretical lectures and teaching material. To facilitate their development students will receive class notes and other documents in the web tool along with relevant basic texts. (1.5 ECTS)
(2) A practical approach encouraging research and further discussion of real case studies of processes and practices on IT security (1.5 ECTS)

Lectures are aimed mainly at achieving knowledge objectives while practical and problem solving seek to develop attitudes and skills.

ASSESSMENT SYSTEM

Students will be evaluated by the list of descriptors (1a-1d), (2a-2f) , (3a,3c) defined as targets regarding the acquisition of knowledge, skills attainment and attitudes of this subject.
The assessment may be continuous assessment or non-continuous assessment:

Ordinary sitting - continuous assessment:
· End of term examination (40% of the final mark)
- A minimum grade of 5.0 is mandatory to pass the subject
· Periodical assignments (60% of the final mark)
A set of individual or in-groups assignments will be proposed. All of them have to be handed-in. Otherwise, non-continuous assessment applies.

Ordinary sitting - non-continuous assessment:
· End of term examination (100% of the final mark)
- A maximum grade of 6.0 may be achieved (i.e. 100% = 6.0)
- At least 5.0 marks must be achieved to pass the subject.
- The exam contains specific parts regarding the competences that have been addressed in the assignments.

Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.
b. Otherwise, students will have an exam counting for 100% of the final mark. The teacher may allow fulfilling the periodical assignments. In this case, the terms and conditions of the ordinary sitting would apply.
c. Even if the student did follow the continuous assessment, he/she has the right to be assessed considering only the mark from the final exam if it is more favourable to him/her.

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

BASIC BIBLIOGRAPHY

- James R. Kalyvas; Michael R. Overly Big Data, CRC Press, 2015

- Matt Bishop Computer Security: Art and Science, Addison-Weley, 2003

- Petra Saskia Bayerl; Andrew Staniforth; Richard Hill; Hamid R. Arabnia; Gregory B. Saathoff; Babak Akhgar Application of Big Data for National Security, Butterworth-Heinemann, 2010
- Terence Craig; Mary E. Ludloff Privacy and Big Data, O'Reilly Media, 2011

- Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. Information security in big data: privacy and data mining, IEEE Access, 2014

ADDITIONAL BIBLIOGRAPHY

- Mark Talabis; Robert McPherson; I Miyamoto; Jason Martin Information Security Analytics, Syngress, 2013

- Mark Van Rijmenam Think Bigger, AMACOM, 2014

- Mohamed Gaber; Sherif Sakr Large Scale and Big Data, CRC Press, 2013

BASIC ELECTRONIC RESOURCES

- VVAA . Big data analysis, how to turn big data into big money, Ch. 7: https://www.safaribooksonline.com/library/view/big-data-analytics/9781118239049/xhtml/Chapter07.html