Course guide
270134 - GCS - Cybersecurity Management

Last modified: 31/01/2024

Unit in charge:	Barcelona School of Informatics
Teaching unit:	701 - DAC - Department of Computer Architecture.
Degree:	BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2023 **ECTS Credits:** 6.0 **Languages:** English

LECTURER

Coordinating lecturer:	MARC RUIZ RAMÍREZ
Others:	Primer quadrimestre: EVA RODRIGUEZ LUNA - 10 MARC RUIZ RAMÍREZ - 10 Segon quadrimestre: EVA RODRIGUEZ LUNA - 10 MARC RUIZ RAMÍREZ - 10

PRIOR SKILLS

Basic knowledge of operating systems, network architectures, information systems architecture.

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CEC4.2. To demonstrate comprehension, to apply and manage the guarantee and security of computer systems.
CES1.2. To solve integration problems in function of the strategies, standards and available technologies
CES1.3. To identify, evaluate and manage potential risks related to software building which could arise.
CES1.9. To demonstrate the comprehension in management and government of software systems.
CSI1. To demonstrate comprehension and apply the principles and practices of the organization, in a way that they could link the technical and management communities of an organization, and participate actively in the user training.
CSI2.1. To demonstrate comprehension and apply the management principles and techniques about quality and technological innovation in the organizations.
CSI2.3. To demonstrate knowledge and application capacity of extraction and knowledge management systems .
CSI2.4. To demostrate knowledge and capacity to apply systems based on Internet (e-commerce, e-learning, etc.).
CSI2.6. To demonstrate knowledge and capacity to apply decision support and business intelligence systems.
CSI2.7. To manage the presence of the organization in Internet.
CSI3.1. To demonstrate comprehension of the principles of risks evaluation and apply them correctly when elaborating and executing operation plans.
CT2.3. To design, develop, select and evaluate computer applications, systems and services and, at the same time, ensure its reliability, security and quality in function of ethical principles and the current legislation and normative.
CT2.4. To demonstrate knowledge and capacity to apply the needed tools for storage, processing and access to the information system, even if they are web-based systems.
CT2.5. To design and evaluate person-computer interfaces which guarantee the accessibility and usability of computer systems, services and applications.
CT3.3. To be able to find and interpret basic information for evaluating the economic environment of the organization.
CT3.4. To know the basic financial concepts which allow valuing the costs and benefits of a project or different alternatives, monitor a budget, control the cost, etc.
CT3.6. To demonstrate knowledge about the ethical dimension of the company: in general, the social and corporative responsibility and, concretely, the civil and professional responsibilities of the informatics engineer.
CT3.7. To demonstrate knowledge about the normative and regulation of informatics in a national, European and international scope.
CT6.4. To demonstrate knowledge and capacity to apply the characteristics, functionalities and structure of the Distributed Systems and Computer and Internet Networks guaranteeing its use and management, as well as the design and implementation of application based on them.
CT7.1. To demonstrate knowledge about metrics of quality and be able to use them.
CT7.2. To evaluate hardware/software systems in function of a determined criteria of quality.
CT7.3. To determine the factors that affect negatively the security and reliability of a hardware/software system, and minimize its effects.
CT8.1. To identify current and emerging technologies and evaluate if they are applicable, to satisfy the users needs.
CTI2.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CTI3.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.

Generical:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

TEACHING METHODOLOGY

The subject will be lectured based on the organization of a teaching model that will be repeated for each of the proposed subjects:
1. Introduction of cybersecurity problems and existing solutions by the teacher, and in some cases by a guest expert.
2. Complementary presentation by a group of students about a specific aspect related to the subject.
3. Discussion in class about recent publications that explain cybersecurity incidents or trends in specific tools or strategies to address cybersecurity issues related to this topic.
If needed, this discussion, as well as all the lecture presentations, will be implemented online.

LEARNING OBJECTIVES OF THE SUBJECT

1.Know the cybersecurity Market
2.Identify the different cybersecurity problems of companies and know the applicable solutions
3.Work in group and write reports and do presentations in the classroom

STUDY LOAD

Type	Hours	Percentage
Self study	84,0	56.00
Hours small group	30,0	20.00
Guided activities	6,0	4.00
Hours large group	30,0	20.00

Total learning time: 150 h

CONTENTS

Part 1: Cybersecurity management and governance

Description:
1.1) Monitoring

1.2) Information Gathering and Cyber-intelligence

1.3) Incident response: Exchange of information and evidence

1.4) Implementation

1.5) Cybersecurity Governance

1.6) Cybercrime Economy

1.7) Regulations and legislations

Part 2. Cybersecurity to relevant and emerging technologies

Description:
2.1) Cloud Computing

2.2) Identity Federation

2.3) IoT / ICS /SCADA

2.4) e-commerce

2.5) Xarxes socials

2.6) Blockchain

2.7) Intel·ligència Artificial

2.8) Computació i Communicacions Quàntiques

ACTIVITIES

Attendance to lectures and bibliographic research work Topic 1

Description:
Presentation of the problems and solutions of cybersecurity for each one of the subjects of the subject.
The presentation will be based on documentation available on the Internet about the latest trends in each topic 1.
Students will have to make a research of additional information about the topic

Specific objectives:
1, 2

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
CSI1. To demonstrate comprehension and apply the principles and practices of the organization, in a way that they could link the technical and management communities of an organization, and participate actively in the user training.

Full-or-part-time: 47h
Theory classes: 10h
Practical classes: 10h
Self study: 27h

Test Part 1

Description:
Quiz of 20-25 test questions on the topics presented and debated in class.

Specific objectives:
1, 2

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
CSI1. To demonstrate comprehension and apply the principles and practices of the organization, in a way that they could link the technical and management communities of an organization, and participate actively in the user training.

Full-or-part-time: 19h
Guided activities: 1h
Self study: 18h

Attendance lectures and writing report linked to Topic 2

Description:
Same as topic 1

Specific objectives:
1, 2

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
CSI1. To demonstrate comprehension and apply the principles and practices of the organization, in a way that they could link the technical and management communities of an organization, and participate actively in the user training.

Full-or-part-time: 47h
Theory classes: 10h
Practical classes: 10h
Self study: 27h

Test Part 2

Description:
Quiz of 20-25 test questions on the topics presented and debated in class.

Specific objectives:
1, 2

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
CSI1. To demonstrate comprehension and apply the principles and practices of the organization, in a way that they could link the technical and management communities of an organization, and participate actively in the user training.

Full-or-part-time: 19h
Guided activities: 1h
Self study: 18h

Oral Presentation

Description:
Oral presentations in class of the work done in a group by the students

Specific objectives:
1, 3

Related competencies :
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 18h
Theory classes: 8h
Practical classes: 10h

GRADING SYSTEM

The final grade of the subject is calculated as:

· 40% research works (20% each report)
· 20% Oral presentations of the work
· 40% Continuous evaluation controls (20 % each control)

The transversal competence is evaluated from the research works.

Process details:

There will be 2 multiple answers choices tests during the course, that will count 40% of the final grade.

The students will have to build groups of 4 to collaborate in the preparation of 2 research works and 1 oral presentation.

Research works can include a draft implementation of the concepts described in the lecture

BIBLIOGRAPHY

Basic:
- Medina, M.; Molist, M. Cibercrimen: ¡protégete del Bit-Bang!, los ataques en el Ciberespacio a: tu ordenador, tu móvil, tu empresa... aprende de víctimas, expertos y CiberVigilantes. Barcelona: Tibidabo, 2015. ISBN 9788416204823.
- Diario La Ley. Wolters Kluwer,
- Clement, S. MISP: user guide: a threat sharing platform. MISP Threat Sharing, 2018.
- European Union Agency for Network and Information Security. ENISA threat landscape report 2017 15 top cyber-threats and trends. ENISA, 2018. ISBN 9789292042509.

Complementary:
- Medina, Manel; Molist, Merçè. Cibercrimen: ¡protégete del Bit-Bang!, los ataques en el ciberespacio a : tu ordenador, tu móvil, tu empresa ... aprende de victimas, expertos y cibervigilantes. Barcelona: Tibidabo, 2015. ISBN 9788416204823.