Course guide
270134 - GCS - Cybersecurity Management

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: 2022  ECTS Credits: 6.0  Languages: English

LECTURER
Coordinating lecturer: MANUEL MEDINA LLINÀS - RAUL ROCA CANOVAS
Others: Primer quadrimestre:
        RAUL ROCA CANOVAS - 10

PRIOR SKILLS
Basic knowledge of operating systems, network architectures, information systems architecture.
DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CEE4.2. 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.
CS11. 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.
CS12.1. To demonstrate comprehension and apply the management principles and techniques about quality and technological innovation in the organizations.
CS12.3. To demonstrate knowledge and application capacity of extraction and knowledge management systems.
CS12.4. To demonstrate knowledge and capacity to apply systems based on Internet (e-commerce, e-learning, etc.).
CS12.6. To demonstrate knowledge and capacity to apply decision support and business intelligence systems.
CS12.7. To manage the presence of the organization in Internet.
CS13.1. 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 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.
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.
CT12.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CT13.1. 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

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours small group</td>
<td>30.0</td>
<td>20.00</td>
</tr>
<tr>
<td>Self study</td>
<td>84.0</td>
<td>56.00</td>
</tr>
<tr>
<td>Guided activities</td>
<td>6.0</td>
<td>4.00</td>
</tr>
<tr>
<td>Hours large group</td>
<td>30.0</td>
<td>20.00</td>
</tr>
</tbody>
</table>

**Total learning time:** 150 h

## CONTENTS

### 1. Prevention and Response to cybersecurity incidents

**Description:****

1) Monitoring
2) Information Gathering and cyber-intelligence
3) Incident response: Exchange of information and evidence
4) Cloud computing security
5) Implementation

### 2. Cybersecurity to emerging technologies

**Description:**

1) Federation of identities
2) Blockchain
3) IoT
4) ICS / SCADA
5) Quantum Computing

### 3. Governance of cybersecurity

**Description:**

1) Government: Employees management, BYOD, policies and practices
2) Privacy and identity theft in social networks
3) E-commerce insurance: anti-fraud payment cards, intermediaries.
4) Cybercrime economy
5) Regulations and legislation

**Methodology:**
## Activities

<table>
<thead>
<tr>
<th>Attendance to lectures and bibliographic research work Topic 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> 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. Students will have to make a research of additional information about the topic</td>
</tr>
<tr>
<td><strong>Specific objectives:</strong> 1, 2</td>
</tr>
<tr>
<td><strong>Related competencies:</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Full-or-part-time:</strong> 23h</td>
</tr>
<tr>
<td>Theory classes: 9h</td>
</tr>
<tr>
<td>Practical classes: 5h</td>
</tr>
<tr>
<td>Self study: 9h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test 1: Incident response and prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Control of 15 test questions on the topics presented and debated in class.</td>
</tr>
<tr>
<td><strong>Full-or-part-time:</strong> 7h</td>
</tr>
<tr>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td>Self study: 6h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test 2. Cybersecurity in emerging technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Control of 15 test questions on the topics presented and debated in class.</td>
</tr>
<tr>
<td><strong>Full-or-part-time:</strong> 7h</td>
</tr>
<tr>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td>Self study: 6h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test 3. Cybersecurity Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Control of 15 test questions on the topics presented and debated in class.</td>
</tr>
<tr>
<td><strong>Full-or-part-time:</strong> 7h</td>
</tr>
<tr>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td>Self study: 6h</td>
</tr>
</tbody>
</table>
### 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:** 21h  
Practical classes: 15h  
Guided activities: 6h

### 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:** 23h  
Theory classes: 9h  
Practical classes: 5h  
Self study: 9h

### Attend lectures and write report related to topic 3

**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:** 23h  
Theory classes: 9h  
Practical classes: 5h  
Self study: 9h
GRADING SYSTEM

The final grade of the subject is calculated as:

- 30% research works
- 25% Oral presentations of the work
- 45% Continuous evaluation controls (15% each control)

The transversal competence is evaluated from the research works.

Process details:
There will be 2 or 3 multiple answers choices tests during the course, that will count 45% of the final grade.
The students will have to build groups to collaborate in the preparation of 2 research works, each of which will be both: presented at the classroom (or virtually if needed), and submitted in a written report.
On some of the topics addressed at the lectures, the students will be asked to do write a draft implementation of the concepts described in the lecture, that will be collected at the end of the lecture.

BIBLIOGRAPHY

Basic:
- Diario La Ley.

Complementary: