270134 - GCS - Cybersecurity Management

Coordinating unit: 270 - FIB - Barcelona School of Informatics
Teaching unit: 701 - AC - Department of Computer Architecture
Academic year: 2018
Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
ECTS credits: 6
Teaching languages: Catalan

Teaching staff

Coordinator: - Manel Medina Llinàs (medina@ac.upc.edu)
Others: - Antonio Rodriguez I Garcia (antonio.rodriguez.g@fib.upc.edu)

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.
CSI1.1. To demonstrate comprehension and apply the management principles and techniques about quality and technological innovation in the organizations.
CSI1.2. To demonstrate knowledge and application capacity of extraction and knowledge management systems.
CSI1.4. To demonstrate knowledge and capacity to apply systems based on Internet (e-commerce, e-learning, etc.).
CSI1.6. To demonstrate knowledge and capacity to apply decision support and business intelligence systems.

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.
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.

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.

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>Total learning time: 150h</th>
<th>Theory classes: 60h</th>
<th>40.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical classes: 0h</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>Laboratory classes: 0h</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>Guided activities: 6h</td>
<td>4.00%</td>
<td></td>
</tr>
<tr>
<td>Self study: 84h</td>
<td>56.00%</td>
<td></td>
</tr>
</tbody>
</table>
### 1. Prevention and Response to cybersecurity incidents

**Degree competences to which the content contributes:**

**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

**Degree competences to which the content contributes:**

**Description:**
1. Federation of identities
2. Blockchain
3. IoT
4. ICS / SCADA
5. Quantum Computing

### 3. Governance of cybersecurity

**Degree competences to which the content contributes:**

**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:**
## Planning of activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Hours</th>
<th>Description</th>
<th>Specific objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attendance to lectures and bibliographic research work Topic 1</strong></td>
<td>23h</td>
<td>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>
<td>1, 2</td>
</tr>
<tr>
<td><strong>Test 1: Incident response and prevention</strong></td>
<td>7h</td>
<td>Control of 15 test questions on the topics presented and debated in class.</td>
<td></td>
</tr>
<tr>
<td><strong>Test 2. Cybersecurity in emerging technologies</strong></td>
<td>7h</td>
<td>Control of 15 test questions on the topics presented and debated in class.</td>
<td></td>
</tr>
<tr>
<td><strong>Test 3. Cybersecurity Governance</strong></td>
<td>7h</td>
<td>Control of 15 test questions on the topics presented and debated in class.</td>
<td></td>
</tr>
<tr>
<td><strong>Oral Presentation</strong></td>
<td>21h</td>
<td>Oral presentations in class of the work done in a group by the students</td>
<td></td>
</tr>
</tbody>
</table>

### Hours
- **Theory classes**: 9h
- **Practical classes**: 5h
- **Laboratory classes**: 0h
- **Guided activities**: 0h
- **Self study**: 9h
- **Guided activities**: 1h
- **Self study**: 6h
- **Guided activities**: 1h
- **Self study**: 6h
- **Guided activities**: 1h
- **Self study**: 6h
- **Theory classes**: 0h
- **Practical classes**: 15h
- **Laboratory classes**: 0h
- **Guided activities**: 6h
- **Self study**: 0h
### Specific objectives:

1, 3

| Attendance lectures and writing report linked to Topic 2 | Hours: 23h  
Theory classes: 9h  
Practical classes: 5h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 9h |
|--------------------------------------------------------|---------------|
| **Description:**  
Same as topic 1 | **Specific objectives:**  
1, 2 |

| Attend lectures and write report related to topic 3 | Hours: 23h  
Theory classes: 9h  
Practical classes: 5h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 9h |
|----------------------------------------------------|---------------|
| **Description:**  
Same as topic 1 | **Specific objectives:**  
1, 2 |

### Qualification 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.
Bibliography

Basic:


PENTEO. Big Data analytics. 2018.


Complementary: