COURSE GUIDE 2023/24

Faculty 363 - Faculty of Engineering - Bilbao **Cycle** .

Degree GIIGSI30 - Bachelor's Degree in Computer Engineering in Management and In **Year** Third year

COURSE

26025 - Information System Security Management Systems **Credits, ECTS:** 6

COURSE DESCRIPTION

Information Systems, which may include computer equipment, networks and data carriers, are responsible for working with the sensitive information of any organization. These Information Systems are threatened by risks and threats that may have different origins. We may encounter physical risks such as damage caused by a natural disaster, or by unauthorized access to information; and logical risks generated by a computer attack such as a virus, denial-of-service attacks, etc.

In this subject, the different risks to which the information and the systems that contain it can be subjected will be studied, in order to know them in depth and thus be able to control them and minimize their impact.

COMPETENCIES/LEARNING RESULTS FOR THE SUBJECT

Ability to integrate information and communications technology solutions and business processes to meet the information needs of organizations, allowing them to achieve their objectives effectively and efficiently, thus giving them competitive advantages.

Ability to determine the requirements of the information and communication systems of an organization attending to aspects of security and compliance with regulations and current legislation.

Ability to actively participate in the specification, design, implementation and maintenance of information and communication systems.

Ability to understand and apply the principles of risk assessment and apply them correctly in the development and implementation of action plans.

CONTENIDOS TEÓRICO-PRÁCTICOS

1.- Introduction
This topic will analyze the security risks that an organization faces and study how to evaluate and estimate the impact that these risks may have.

2.- Introduction to encryption
The main purpose of information encryption is its protection. This topic will address the basic ideas about encryption, as well as its history.

3.- Symmetric encryption
Most common algorithms and their applications.

4.- Asymmetric encryption
Most common algorithms and their applications.

5.- Secure communications
Application of encryption in secure communications: certificates, SSH connections, etc.

6.- Bitcoin
Bitcoin is an interesting application of encryption, as well as other concepts such as distributed databases. A basic technical introduction to Bitcoin and its Blockchain will be offered.

7.- Backups
Backups ensure the completeness of the information and its usability in case of loss of the original information. This topic will look at different ways and systems of backing up.

8.- Physical security
There is no point in having an information system protected against all kinds of logical risks, if anyone can physically access and manipulate it. The physical security of information systems and data is essential.

9.- Network Security
Information is rarely isolated on a machine without connection to any network. Taking security measures to protect communication networks is an essential step to secure information.

10.- Security in Web Systems

Every day more and more data is in systems connected to the Web that can be accessed from anywhere on the planet. There are many aspects of security that must be taken into account in the implementation of such systems to prevent unwanted access.

11.- The human factor
Throughout this topic, social engineering and different ways of protecting people's information will be studied, since they are often the weakest link in the information protection chain.

12.- Malware What is malicious code (malware)? How can it be detected and avoided? This topic will look at the main ways to protect yourself from malware and its effects. To do this, we will study what types of malware exist, the characteristics of each of them and their effects on information systems.

13.- Legislation
In the field of computer security it is essential to know the current legislation in this area. This topic will analyze the most important laws that are in force and their effects on information systems.

14.- Computer forensics
In this topic, the procedures for the autopsy of a computer equipment will be studied.

15.- Talks (To be defined)
Talks about Bitcoin, Pentest, etc. by industry experts

TEACHING METHODS

The master classes (M) will be used mainly for the presentation of the theoretical concepts associated with computer security and the resolution of doubts raised by the students. However, in some master classes and in some computer practices (PO) these concepts will be reinforced through the resolution of exercises, either individually or in small groups. It is recommended to use the laptop in class, especially with a GNU/Linux operating system.

PO classes that are not used for the resolution of exercises, will be used to apply the active methodology of Problem-Based Learning. From time to time students will be provided with a series of exercises that they can work on individually or in groups.

In case of confinement, classes and tutorials will be carried out telematically. The evaluation system will continue to adapt the tests for online performance.

TYPES OF TEACHING

Types of teaching	M	S	GA	GL	GO	GCL	TA	TI	GCA
Hours of face-to-face teaching	45				15				
Horas de Actividad No Presencial del Alumno/a	67,5				22,5				

Legend:
M: Lecture-based | S: Seminar | GA: Applied classroom-based groups
GL: Applied laboratory-based groups | GO: Applied computer-based groups | GCL: Applied clinical-based groups
TA: Workshop | TI: Industrial workshop | GCA: Applied fieldwork groups

Evaluation methods

- Continuous evaluation
- End-of-course evaluation

Evaluation tools and percentages of final mark

- Written test, open questions 10%
- Multiple choice test 20%
- Exercises, cases or problem sets 30%
- Teamwork assignments (problem solving, Project design) 40%

ORDINARY EXAMINATION PERIOD: GUIDELINES AND OPTING OUT

In the ordinary call, by default, the students are covered by the continuous evaluation system, although there is the option of taking advantage of the final evaluation indicating it by email, at the latest before the two weeks before the 3rd exam. In the continuous evaluation system, the evaluation will be divided into three parts, each of them with a theoretical and a practical exam, whose grades will average. Each exam will deal with the subject seen in class and the laboratory reports made up to that date and since the previous exam.

In addition, throughout the semester a series of assignments will be carried out that will influence the final grade of the subject to different extents. In the final evaluation system there will be a single theoretical and a practical exam that will correspond to the entire syllabus of the subject. The final grade of the subject will be calculated using the arithmetic average of both exams.

ASSIGNMENT EVALUATION:
The detection of plagiarism anywhere in a work will mean a score of 0 in that work. The works must be written correctly, so at the very moment a third serious spelling mistake is detected, the work will no longer be corrected and its mark will be the one corresponding to the part of it that has been evaluated.

COPY CASES:
If a copy is detected between jobs from two different groups, both jobs will be evaluated with 0. In the case of exams, article 46.2 of the current regulations regarding the evaluation of students will apply.

WAIVER OF THE CALL:
To renounce the call and appear as "Not Presented" in the continuous evaluation mode, it is enough not to sit for the 3rd exam. In the final assessment mode, it is enough not to sit for the final exam.

EXTRAORDINARY EXAMINATION PERIOD: GUIDELINES AND OPTING OUT

Students who do not pass the subject in their ordinary call will have to take a theoretical exam and a practical one in the extraordinary call on the complete syllabus of the subject. Students who have followed the continuous evaluation system will have the possibility to indicate in the exam itself if they want the final grade of the subject to be calculated using only the grades of the exams or if they want the grade of the work carried out throughout the semester to be taken into account.

WAIVER OF THE CALL: In case of not taking the theoretical or practical exam, an assessment of "Not Presented" will be obtained.

MANDATORY MATERIALS

Class notes, support material for teaching in the classroom and laboratories.

BIBLIOGRAFÍA

Basic bibliography

Enciclopedia de la Seguridad Informática, Álvaro Gómez Vieites, RAMA 2006

Detailed bibliography

The governance of privacy. C.J. Bennett y C.D. Raab, Massachussets Institute of Technology Press 2006
Beyond Fear. B. Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World; 2006; Springer
Vigilancia permanente. Edward Snowden. Planeta, 2019
Social Engineering: The Science of Human Hacking. Christopher Hadnagy, Wiley 2018
El pequeño libro rojo del activista en la red. Marta Peirano, Roca 2015
Grokking Bitcoin. Kalle Rosenbaum, Manning 2019

Journals

Auditoría + Seguridad informática
IEEE Security & Privacy

Web sites of interest

Blog de Bruce Schneier sobre seguridad (Accessed 12/05/2022)
https://www.schneier.com/

Agencia Española de Protección de Datos (Accessed 12/05/2022)
http://www.agpd.es

Red temática de criptografía y seguridad de la información (Accessed 12/05/2022)
http://www.criptored.upm.es

Equipo de seguridad de rediris (Accessed 12/05/2022)
http://www.rediris.es/cert/

Instituto nacional de ciberseguridad (Accessed 12/05/2022)
https://www.incibe.es/

Blog sobre seguridad (Accessed 12/05/2022)

https://krebsonsecurity.com

Malware scanner (Accessed 12/05/2022)
https://www.virustotal.com

OBSERVATIONS

If a work is rated with a 0 due to plagiarism, the subject will be suspended in its ordinary call.