European Commission

MICROGUIDE

Project acronym:

Microguide

Project full title: DEVELOPING GUIDELINES
FOR THE IMPLEMENTATION OF
MICRO-CREDENTIALS IN HIGHER EDUCATION
Project No. 2021-1-ProjectRS01-KA220-HED-000027585
Funding Scheme: Erasmus+


PILOT MICRO-CREDENTIAL 3 – SPAIN

Name of the micro-credential:

Security management of computer systems

Provider:

University of Lleida

Programme level:

Suitable for students of higher education with a degree or master's in computer science or telecommunications.

Link to the EQF:

Level EQF-6, equivalent to MECES-2

Duration:

60 h

Modality:

100% face-to-face

ECTS awarded

6

Justification

In recent years, it has become clear that an Internet presence is necessary for any company or organization. The Internet is a fundamental medium through which you can communicate with partners, customers, and suppliers.

Despite all the advantages it brings, the Internet presence also involves a series of risks. The possibility of being a victim of a cyberattack always exists. For this reason, having expert personnel in managing the security of computer systems is essential.

According to a report by Check Point Research[32], Spanish companies received an average of 1042 attacks per week during 2023. If successful, the impact of these attacks can be harmful in many aspects, such as loss of intellectual property,

32 https://www.itdigitalsecurity.es/actualidad/2024/01/descienden-los-ataques-en-espana-en- 2023-mientras-se-incrementan-en-el-resto-del-mundo

physical damage resulting from the alteration of processes, interruption of daily activity, financial losses, reputational damage, or legal and regulatory penalties.

This micro-credential in cybersecurity aims to provide specific and specialized knowledge to professionals who administer or carry out their activity through services connected to the Internet.

The objective of the training

The course provides extensive training in the security of computer systems connected to the Internet. The training provided will allow us to know the tasks that are in charge of a company's head of cybersecurity, as well as particular knowledge of the technology and tools available to provide security to the teams of an organization.

Learning Outcomes

At the end of the micro-credential, participants will be able to:

- Analyse the nature of the data that form part of an information system and design appropriate technical measures to protect them according to their level of sensitivity.
- Choose the right cryptographic technology to protect an organization's data and communications, including proper key management.
- Securely manage a multi-user machine to avoid/detect both internal and external attacks.
- Securely manage an organization's network to prevent/detect both internal and external attacks.
- Securely configure and use commonly used telematic services.

Access and admission

OThis micro-credential is suitable for students in a higher-level training cycle, university degree, or university master's degree in computer engineering, telecommunications, or related disciplines.

Curriculum structure

1. Regulations and standards (6h)

- The General Data Protection Regulation
- The ISO/IEC 27002 standard

2. System administration (12h)

- User management

- File system security
- Logs management
- Pen testing

3. Fundamentals of cryptography (16h)

- Shared key encryption
- Public key encryption
- Digital signature
- Public key infrastructures

4. Network security (16h)

- Security in wireless networks
- Firewall systems
- Intrusion detection systems
- Virtual private networks

5. Security in telematic services (10h)

- Security in the Web service
- Email security
- Secure remote access

Evaluation methodology

The syllabus is developed with master classes where the teacher explains the theoretical concepts and practical activities.

The evaluation is done by delivering documents showing evidence that the practical activities have been carried out correctly. In addition, it will also be necessary to include texts that demonstrate that the concepts worked on in each activity have been understood.

Teaching staff

The teaching staff must have expertise in the following areas:

- Legislation on data protection and regulations on the secure management of computer systems
- Cryptography
- Operating System Administration
- Network Administration
- Configuration of telematic services

Material resources

This micro-credential needs a classroom that has:

- Blackboard
- Projector
- One computer with a Linux operating system for each student. The student will need to have administration permissions. For this reason, the use of virtual machines is recommended.
- Internet connection

The entire practical activity of the course can be done using free distribution software.