

National Course Plan

Centro Superior de Formación Europa Sur (Cesur), Spain



Co-funded by
the European Union

Contents

1. Summary	3
2. Training setting.....	3
3. Learner Journey(s).....	4
3.1 The Comprehensive Cybersecurity Proficiency Assessment	4
3.2 BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY	5
Advanced (Hare) learning journey	6
4. Conclusion.....	6

MECyS is funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA).

Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



1. Summary

The Spanish Training Prototypes are tailored for prospective educators in vocational and business education, as well as learners enrolled in the Spanish dual system. Furthermore, we extend our course offerings to relevant personnel in Micro and Small Enterprises (MSEs).

The course content will be adapted to suit the distinctive needs of each cohort. For students, fundamental content will be provided, recognizing their position at the commencement of their vocational journey. Teacher trainees will receive an in-depth exploration of the conceptual framework and pedagogical recommendations across various learner pathways. MSE staff will access specialized insights focusing on Cybersafety, encompassing cybersecurity and data protection.

The training format for teacher trainees and students will predominantly feature on-site workshops, incorporating a blend of online and printed materials. Where viable, an emphasis will be placed on game-based and other interactive methodologies. To facilitate the engagement of MSE staff, the approach will be crafted to be as asynchronous, and internet based as practicable.

2. Training setting

Vocational students in MSEs can be considered as a primary target group, as it is highly extended in fact, 27% enter vocational education with the aim in mind to enter university.

The initial target demographic is VET students, specifically those preparing for employment in IT. These aspiring computer scientists are in the process of acquiring the skills necessary to develop a job in the IT field, including those working part-time in small companies while pursuing their studies.

The training will consist of 4 hours of master class and 1h of quiz before and 1h after to show the knowledge acquired before and after the course.

Considering the diverse degrees of digital integration observed among Micro and Small Enterprises (MSEs) spanning different sectors, a clear necessity emerges for enhanced digital proficiency and heightened consciousness surrounding cybersecurity. It's anticipated that the proficiencies concerning digital aptitude, cybersecurity awareness, and data safeguarding within this demographic will be multifaceted. As a result, the MECyS programme is meticulously crafted to address an intermediate skill level, thereby fostering inclusivity for participants possessing a spectrum of competencies. Acknowledging the constraints posed by time commitments and potential forthcoming financial limitations, the course is strategically

designed to provide adaptability, ensuring it can cater to the specific requirements of the Spanish target audience.

3. Learner Journey(s)

3.1 THE COMPREHENSIVE CYBERSECURITY PROFICIENCY ASSESSMENT

The Comprehensive Cybersecurity Proficiency Assessment is designed to evaluate an individual's knowledge, skills, and abilities in various aspects of cybersecurity. This assessment aims to provide a comprehensive understanding of the participant's cybersecurity proficiency across multiple domains.

The test is structured into several sections, each focusing on key areas of cybersecurity, such as Cybersecurity Fundamentals: This section assesses the candidate's understanding of basic cybersecurity concepts, terminology, and principles. Questions may cover topics such as confidentiality, integrity, availability, encryption, and authentication.

Network Security: Participants will be tested on their knowledge of network security principles, protocols, and best practices. This includes topics such as firewalls, intrusion detection systems, VPNs, secure configurations, and network segmentation.

Secure Software Development: Participants will be assessed on their understanding of secure software development practices, including secure coding principles, common vulnerabilities (e.g., injection attacks, cross-site scripting), and secure development life cycle methodologies.

Incident Response and Disaster Recovery: This section focuses on the candidate's knowledge of incident response procedures, incident handling techniques, and disaster recovery planning. Questions may cover incident classification, escalation procedures, containment measures, and recovery strategies.

Security Awareness and Training: Participants will be assessed on their awareness of common cybersecurity threats, social engineering tactics, and the importance of security awareness training for end users.

The assessment may include a combination of multiple-choice questions, scenario-based questions, and hands-on exercises to evaluate both theoretical knowledge and practical skills. Each section will be weighted based on its importance in the cybersecurity domain, and participants will receive a detailed score report highlighting their strengths and areas for improvement.

The Comprehensive Cybersecurity Proficiency Assessment is suitable for individuals seeking to assess their cybersecurity skills, as well as organizations looking to evaluate the competency of their cybersecurity professionals. It provides valuable insights into an individual's readiness to address cybersecurity challenges in today's dynamic threat landscape.

Cybersecurity Fundamentals: This section assesses the candidate's understanding of basic cybersecurity concepts, terminology, and principles. Questions may cover topics such as confidentiality, integrity, availability, encryption, and authentication.

3.2 BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY

What?

Basic Cybersecurity Fundamentals: Covering the foundational principles of cybersecurity, including the importance of strong passwords, secure online behaviour, and an introduction to common threats.

Introduction to Data Protection: Providing an overview of data protection laws and the significance of responsibly handling and securing sensitive information.

Understanding Phishing and Malware: Exploring common types of phishing attacks, malware, and practical tips for recognizing and avoiding them.

Network Security Basics: Introduction to securing networks, including Wi-Fi security and protecting against unauthorized access.

How?

Utilize interactive presentations, real-world examples, and practical exercises to introduce key cybersecurity concepts.

Incorporate case studies, legal frameworks, and interactive discussions to emphasize the significance of data protection.

Why?

The beginner level content focuses on establishing a solid foundation in cybersecurity for individuals with limited prior knowledge. These fundamental concepts are essential for building a baseline understanding of cybersecurity risks and best practices. By covering basic principles, cyber hygiene, and introductory topics, the course ensures that participants develop a strong understanding of essential cybersecurity concepts before moving to more advanced content.

ADVANCED (HARE) LEARNING JOURNEY

What?

Cloud Security: Exploring the challenges and best practices for securing data and operations in cloud environments, considering the specific needs of small enterprises and startups.

Advanced Threats and Cyber Attacks: In-depth examination of sophisticated cyber threats, understanding the tactics of hackers, and strategies for defending against advanced attacks.

How?

Combine theoretical lectures with hands-on labs, case studies, and discussions on real-world network security scenarios.

Engage in hands-on labs, live demonstrations, and collaborative discussions on advanced threat scenarios.

Why?

The expert level content is designed for participants with a strong foundation in cybersecurity and professional experience in the field. This content provides a deeper dive into advanced topics, focusing on strategic cybersecurity management, incident response, and specialized areas like cloud security. By addressing the complex challenges faced by small enterprises and startups, the course equips participants with the expertise needed to implement comprehensive cybersecurity measures within their organizations.

4. Conclusion

In summary, the MECyS (Micro and Small Enterprises Cybersecurity) project emerges as a pivotal endeavor aimed at addressing the intricate tapestry of digitalization across diverse Micro and Small Enterprises (MSEs) operating within various sectors. This project stands as a beacon, illuminating the pressing need for bolstered digital competencies and heightened cybersecurity consciousness within this vital economic sector.

Upon scrutinizing the digital landscape inhabited by MSEs, it becomes evident that their levels of digital integration vary significantly. While some may boast advanced technological infrastructures and adeptness in navigating digital realms, others may still be in the nascent stages of digital adoption, grappling with the complexities and vulnerabilities inherent in the digital sphere. It is within this context that the MECyS project finds its *raison d'être* – to bridge the digital divide, equip MSEs with requisite digital skills, and fortify their cyber defences against an ever-evolving threat landscape.

The demographic of MSEs presents a rich mosaic of competencies, ranging from fledgling entrepreneurs taking their first steps into the digital world to seasoned veterans seeking to fortify their cyber fortifications. Consequently, the MECyS project is meticulously architected to cater to this diverse spectrum of proficiency levels. Through a judicious blend of foundational principles and advanced techniques, the project endeavors to empower VET students, specifically those preparing for employment in IT, fostering inclusivity and ensuring that participants with varying degrees of digital acumen find value and relevance in the course offerings.

Furthermore, the MECyS project operates within the pragmatic confines of real-world constraints, acknowledging the temporal limitations and potential financial constraints that often beset MSEs. In cognizance of these challenges, the project is imbued with a spirit of flexibility, designed to bend and adapt to the unique circumstances of the Spanish target group. Whether it be accommodating busy schedules or navigating budgetary constraints, the MECyS project strives to provide a tailored approach, ensuring accessibility and efficacy in its delivery mechanisms.

The finalized English version of the Spanish National Course Plan was to basically align the Course Plans of the MECyS partners. Further developments will be done in the Spanish version.



MECyS

Micro - Enterprise Cybersecurity

mecys.eu



Co-funded by
the European Union