CLOUD SECURITY (EMaCS-02-11)				
DEGREE PROGRAM:		Master in Computer Science for the Human-Centric and Sustainable Industry		
SEMESTER: Second	**TYPE:** Basic	**CREDITS:** 6 ECTS	**WORKLOAD:** 150 hours	**MENTORING:** 4 hours/week
LANGUAGE: English				

OBJECTIVES	
General	The student will gain introductory knowledge of cloud computing platforms and the underlying technologies that enable them, with the aim of explaining and demonstrating the security challenges that arise with their use.
Specific	• Be aware of the security challenges posed by the move to cloud-based software deployments • Understand the architecture of cloud computing systems: AWS, GCP, Azure and the underlying technologies that they employ: software containers, virtual machines, automated deployment tools. • Understand virtual networks, data flows and how to secure them both in transit as well as at rest. • Obtain sufficient knowledge about configuration, resource and identity management in order to be able to present a secure-by-default cloud deployment scenario. • Recognize the most common configuration and management failures that have led to data and security breaches based on past high-profile cases. • Be able to monitor and analyse logs and audit trails for signs of security breaches, as well as how to react when these occur.

SUSTAINABILITY

- The students will understand that robust security practices in the cloud can contribute to optimize the cloud resources usage, thus reducing energy consumption and, consequently, the environmental impact.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

- The students will learn how to provide for users a seamless and secure access to cloud services and will understand that they should prioritize the protection of users, their data, and their overall digital experiences.
- The students will gain skills on how to detect, mitigate, and recover from security incidents, ensuring the resilience of the IT infrastructure and of the organization which uses it.

SUBJECT MATTER

Lecture:

- Cloud technology. Microservices-based architecture.
- Major cloud platforms: AWS, GCP, Azure.
- Cloud deployment pipeline.
- Case study: The Capital One security breach.
- Network security.
- Virtual machine security.
- Software container security.
- Identity and access management.
- Compute resource management and configuration management.
- Data security in transit and at rest.
- Logging, audit trails, and continuous monitoring.
- Security incident detection and response.
- Cloud forensics.

- Security testing.

Lab activity:

- Connecting to public cloud platforms. Deploying applications in the cloud.
- Working with software containers: Docker. Creating, configuring containers and virtual networks.
- Orchestrating containers: docker-compose and Kubernetes.
- Version control for software code. Continuous integration technologies.
- Creating and managing user accounts. Managing secrets in the cloud.
- Data encrypting. Log files analysis and intrusion detection
- Case studies: security breaches in the cloud.

COMPETENCES

C5: PROGRAMMING
C7: PROTECTING PERSONAL DATA AND PRIVACY
C9. REFLECTING ON ETHICAL OUTCOMES
C10: EXPLORATORY AND CRITICAL THINKING
C11: PROBLEM FRAMING
C12: IDENTIFYING NEEDS AND TECHNOLOGICAL RESPONSES
C13: CREATIVELY USING DIGITAL TECHNOLOGIES
C14: SOLVING TECHNICAL PROBLEMS

LEARNING OUTCOMES

Knowledge	• Know about cloud architecture and the technologies underlying it. • Know about the main configuration errors in cloud platforms. • Know about security breaches and their remediation. • Know about the best practices for securing cloud platforms and services.
Skills	• Be able to develop cloud platforms for application launches. • Ability to manage users, roles, and associated secrets. • Be able to understand advanced concepts associated with cloud computing technologies.
Attitudes/values	• Adaptation to new cloud platforms and technologies due to similarities with those presented in the course/lab.

TEACHING METHODS

Method	Class Workload	Individual Workload	Total
Theoretical Sessions	28	28	56
Laboratory Sessions	28	28	56
Research and writing of an applied project	4	32	36
Written Examinations	2	0	2
TOTAL	**62 hours**	**88 hours**	**150 hours**

EVALUATION

- Written Examinations (50%)
- Project (30%)
- Lab assignments/homework (30%)

PRECONDITIONS

- Knowledge on computation systems, databases and computer networks
- Skills on high-level programming languages
- Skills on development and maintenance of computer applications
- Ability to use of the theoretical foundations of computer science

DEPARTMENT	Computer Science
LECTURERS	Dana Petcu, Mario Reja
LITERATURE	• Chris Dotson, Practical cloud security: a guide for secure design and deployment, O'Reilly Media, 1st edition, 2019, ISBN: 1492037516 • Julien Vehent, Securing DevOps: Security in the Cloud, Manning, 1st edition, 2018, ISBN: 1617294136

	• Liz Rice, Container Security: Fundamental Technology Concepts that Protect Containerized Applications, O'Reilly Media, 1st edition, 2020, ISBN: 1492056707 • Nigel Poulton, Docker Deep Dive: Zero to Docker in a single book, Packt Publishing, 2020, ISBN:9781800565135 • Nigel Poulton, The Kubernetes Book: 2023 Edition, independently published, 2023, ISBN:979-8402153776 • Yevgeniy Brikman, Terraform: Up and Running: Writing Infrastructure as Code, O'Reilly Media, 3rd Edition, 2022, ISBN: 1098116747