SECURE INFRASTRUCTURE MANAGEMENT (DEVSECOPS) (EMaCS-02-14)				
DEGREE PROGRAM:		Master in Computer Science for the Human-Centric and Sustainable Industry		
SEMESTER: Second	**TYPE:** Basic	**CREDITS:** 6 ECTS	**WORKLOAD:** 150 hours	**MENTORING:** 3 hours/week
LANGUAGE: English				

OBJECTIVES	
General	Assessing, identifying and analysing techniques for prevention, detection and mitigation of cybersecurity attacks in the context of infrastructure, with strong focus on cloud-driven operations. Management of security issues of infrastructure. Preparing, developing and implementing secure infrastructures for deploying software architectures and code.
Specific	• Be aware of the classification or taxonomy of infrastructure as a service (IaaS) models proposed in the space of DevOps. • Understand the fundamentals of some of the algorithms based on cloud-based infrastructure applied by many companies to their operations: communication protocols, secure data storage, data encryption, etc. • Understand the solutions that IaaS platforms can provide and how they are currently being applied to ensure secure data storage, processing and retrieval, etc. • Obtain sufficient knowledge to implement IaaS-driven services and apply them to real problems, being able to compare these to real-world problems, being able to compare different relevant models. • Recognize the typical characteristics of the optimisation problems that a computer engineer may encounter when securely managing infrastructure: autonomy, stability, security, load balancing, scheduling, etc. • Obtain a general knowledge of the range of solutions provided by IaaS platforms to the above-mentioned problems. To know the advantages and disadvantages of each of these techniques depending on each type of problem. • Be able to use, understand and analyse the results provided by IaaS platforms and its relevant software, as well as to programme some of the management routines of this paradigm

SUSTAINABILITY

- The students will understand that by guaranteeing the security of a computational infrastructure its energy efficiency can be improved and the threats leading to waste of resources can be mitigated.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

- The students will learn how to ensure resilience of infrastructure with respect to disruptions induced by cyber-threats with a focus on understanding the risks generated by continuously evolving threats and the necessity of developing adaptive secure technologies.
- The students will gather skills on implementing strategies to ensure the protection of sensitive data and of users privacy leading to an increase of the trust in using the infrastructures by various communities.

SUBJECT MATTER

Lecture:

- Introduction to DevOps
- Git, GitHub
- Testing
- Docker
- Kubernetes
- Software Development Lifecycle and DevSecOps maturity models
- Static Component Analysis

- Infrastructure as a Code security
- Monitoring and Measurement
- Security through Logs
- Secure application development
- Planning and designing (Jira)

Lab activity:

- Introduction to cloud-driven infrastructures
- Managing AWS infrastructure (1)
- Managing AWS infrastructure (2)
- Managing Azure infrastructure (1)
- Managing Azure infrastructure (2)
- Docker-driven infrastructure security analysis
- Kubernetes-driven infrastructure security analysis
- Managing code security for secure infrastructures (1)
- Managing code security for secure infrastructures (2)
- Log analysis for securing infrastructures (1)
- Log analysis for securing infrastructures (2)

COMPETENCES

C5: PROGRAMMING
C7: PROTECTING PERSONAL DATA AND PRIVACY
C8. PROTECTING HEALTH AND WELL-BEING
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
C17. COMMUNICATING EFFECTIVELY

LEARNING OUTCOMES

Knowledge	• Know how to express thoughts and concerns in manners that a computational machine could implement, deploy and, ultimately, execute. Algorithmic thinking. • Know how to gather relevant information all-in-one place following a logical line-of-thought, for improved clarity of perception and comprehensive instructions for anyone involved in the process being studied/handled.
Skills	• Ability to manage infrastructures in the context of cybersecurity. • Capacity to identify and implement best approaches to securing data in cloud-driven infrastructures. • Ability to assess and develop techniques for secure coding and data practices. • Be able to identify, analyze and implement IaaS-driven software services that follow secure coding practices and protocols.
Attitudes/values	• Weigh the benefits and disadvantages of using infrastructure-as-a-service (IaaS) platforms. • Be willing to accept that some approaches may not be perfect in solving the problem that they aim to address. • Have a disposition to keep learning, to educate oneself and stay informed about IaaS (e.g. to understand socket-driven communication mechanisms over the Internet or other types of networks, to understand how cloud-dependent algorithms work, to comprehend the relevance and importance of developing secure and stable communication protocols between applications, etc.).

	• Be open to engage in collaborative processes to co-design and co-create new products and services based on existing IaaS platforms, to support and enhance the capabilities of human workers on industrials settings, as well as improve services and help making better decisions for the sustainability of operations and respect of the environment.

TEACHING METHODS

Method	Class Workload	Individual Workload	Total
Theoretical Sessions	28	28	56
Laboratory Sessions	14	42	56
Research and writing of an applied project	4	32	36
Written Examinations	2	0	2
TOTAL	**48 hours**	**102 hours**	**150 hours**

EVALUATION

- Project (70%)
- Homework (30%)

PRECONDITIONS

- Basic skills in programming.
- Basic understanding of emulation and virtualization concepts.
- Knowledge of calculus and mathematics at a level of a graduate student (e.g. matrix and vector calculus, Boolean operations, etc.)

DEPARTMENT	Computer Science
LECTURERS	Ciprian Pungilă
LITERATURE	• Abdelkebir, S., Maleh, Y., & Belaissaoui, M. (2017). *An agile framework for its management in organizations: a case study based on DevOps*. Proceedings of the 2Nd International Conference on Computing and Wireless Communication Systems, 67, 1-8. • Bou Ghantous, G., & Gill, A. (2017). *DevOps: concepts, practices, tools, benefits and challenges*. Proceedings PACIS2017, 96. • Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). *DevOps*. IEEE Software, 33(3), 94-100. • Hsu, T. H. C. (2018). *Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps*. Packt Publishing Ltd. • Koskinen, A. (2019). *DevSecOps: building security into the core of DevOps*. Masters Thesis, University of Jyväskylä.