Course Title	Cybersecurity Architecture and Operations				
Course Code	CYS645				
Course Type	Compulsory				
Level	Master (2^{nd} cycle)				
Year / Semester	1^{st} Year/2^{nd} Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify the various components of a comprehensive cybersecurity architecture within an organization. • Describe and classify controls that meet specific control objectives and to treat identified risks. • Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc. • Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover. • Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others. • Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control. • Evaluate and select appropriate architectural and operational options according to the organizational risk environment.				
Prerequisites	None	Co-requisites	CYS600		
Course Content	Introduction: Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication.				

Processes: User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others.

Phases: Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover.

Identify: Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process.

Protect: Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening.

Detect: Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicatiors of compromise (IOC).

Respond: Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls.

Recover: Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes.

Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations.

DevSecOps: Core principles and benefits of DevSecOps, challenges of traditional software development and how DevSecOps addresses them, Integrating Security into CI/CD Pipelines, implementing security checkpoints in continuous integration and continuous deployment (CI/CD) pipelines, Incorporating security testing, code analysis, and vulnerability scanning, Secure Code Practices, Threat Modeling in DevSecOps. Overview of popular DevSecOps tools and frameworks.
Hands-on experience with selected tools for vulnerability assessment and security automation.

Embedded Systems Security: basics of embedded systems and their applications, Identifying the security challenges specific to embedded devices, Embedded Systems Architecture, Exploring the architecture of embedded systems and potential vulnerabilities, Analyzing common attack vectors against embedded devices, Secure Boot and Firmware Protection, Implementing secure boot mechanisms to ensure the integrity of firmware, Exploring techniques for protecting firmware from

	unauthorized modifications, Communication Security in Embedded Systems, Integrating security into the embedded system development lifecycle, Performing security testing, including penetration testing and code reviews. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.
Teaching Methodology	E-Learning
Bibliography	*Santos, O., Developing Cybersecurity Programs and Policies. Pearson.* *“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)* *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker* *ISO/IEC 27002 - Information security, Cybersecurity and privacy protection – Information Security controls*
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English