Course Title	Information Security				
Course Code	IS504				
Course Type	Elective				
Level	Postgraduate				
Year / Semester	1st Year / 2nd Semester				
ECTS	7.5	**Lectures / week**	1	**Laboratories / week**	1
Course Purpose and Objectives	The objectives of the course are: • Provide the fundamentals of Information security. • Present the information threats and attacks and ways to protect the information from such attacks. • Look at specific technical areas of information security such as authentication, access control, denial of service, intrusion detection and prevention systems and, finally cryptographic algorithms. • Concern with management aspects of information security and more specifically on management practices related to risk management. • Discuss the legal and ethical issues that are commonly found in today's organizations. • Introduce computer forensics and how we can find evidence.				
Learning Outcomes	After completing the course the students are expected to: O[1] Explain the challenges and scope of information security; O[2] Identify the common threats faced today; O[3] Describe the access control mechanism used for user authentication and authorization; O[4] Understand the importance of cryptographic algorithms used in information security; O[5] Explain the use of such security tools as firewalls and intrusion prevention systems; O[6] Recognize the importance of physical security and discuss ways to improve physical security of an enterprise;				

	O[7] Ensure infrastructure and network security;
	O[8] Examine and resolve legal and ethical issues;
	O[9] Enhance critical thinking and analysis skills through the use of case studies, research papers and small group exercises.
	O[10] Strengthen research, writing and presentation skills.

Prerequisites	None	**Required**	None
Course Content	1st week: Introduction to Information Security 2nd week: Attacks and Threats 3rd week: Denial of Service Attacks 4th week: Intrusion Detection and Prevention Systems 5th week: Basic Cryptography 6th week: Access Control Fundamentals 7th week: User Authentication 8th week: Physical Security 9th week: Risk Management 10th week: Network Security 11th week: Legal and Ethical Issues in Information Security 12th week: Introduction to Forensics 13th week: Conclusions / Rehearsal		
Teaching Methodology	Mix of lectures, active learning techniques and activities. More precisely: • Lectures • Notes and PowerPoint Presentations in digital format through the electronic platform • Basic textbook(s) and additional bibliography • Assignments • Meetings with the instructor(s) • Discussions in Forums through the electronic platform of real word case studies • Web links • Critical reflection on research article • Peer review on group working and discussion in forum • Educational videos on real world case studies and critical discussion in forum		
Bibliography	Compulsory Bibliography		

- W. Stallings, L. Brown, Computer Security Principles and Practice, 4th edition, 2018, Pearson

- Wenliang Du, Computer & Internet Security: A Hands-on Approach

- Michael E. Whitman, Principles of Information Security, 6th edition, 2018

Additional Bibliography

- Yang, J.; Chen, Y.-L.; Por, L.Y.; Ku, C.S. A Systematic Literature Review of Information Security in Chatbots. Appl. Sci. 2023, 13, 6355. https://doi.org/10.3390/app13116355
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2
-

Assessment	5% Quizzes

20% Projects/Assignments
10% Peer Assessment
5% Oral Presentation
60% Final exams

Assessment methods and mapping with Learning Outcomes

	Percentage	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
Quizzes	5%	√	√			√			√		
Projects / Assignments	20%			√	√		√	√			√
Peer Assessment	10%			√	√		√	√		√	√
Oral Presentation	5%									√	√
Final exam	60%	√	√	√	√	√			√		

Language	English