Libera Università Internazionale
degli Studi Sociali Guido Carli

LUISS

Syllabus

Academic Year	2021/2022
Program	Data Science and Management
course	Data Privacy and Security
Term	II semester
Year	1
SSD	ING-INF/05 - Sistemi di elaborazione delle informazioni
Credits	6

INSTRUCTIONAL GOALS	The course provides an in-depth understanding of data privacy and security in technology-enabled environments and it focuses on technological solutions, methods and practices for data protection in business organizations and peer to peer networks. This provides students with an understanding of strategic and regulatory issues of data privacy and security in modern organizing as well as an overview of mechanisms for privacy and security assurance in enterprise architectures and projects. Students in this course will not only gain a deep understanding of the design principles for data privacy and security but they will also acquire the practical skills necessary for their successful applications to problems in science and industry.
INTENDED LEARNING OUTCOMES They describe what a learner is expected to know, understand and be able to demonstrate after completion of a learning path.	**Knowledge and understanding**: The course will offer key concepts and methods to plan, design, implement, manage and audit technological and organizational solutions to assure data privacy and security in digital business. In particular, the course will provide a good understanding of the normative, ethical and social issues of data privacy and security and a deep understanding of the strengths and weaknesses of enterprise security architectures. **Applying knowledge and understanding**: On successful completion of this course students will be able to: • Analyze the social and organizational implications of cyber risk in digital ecosystems • Select, design and implement the most appropriate security controls to mitigate risk in business organizations • Apply data analytics tools and techniques to support decision making in incident management and security operations • Design innovative solutions using data-driven analytics and deep learning for situational awareness in security operations. **Making judgements**: Students are expected to be able to reflect on the social and ethical responsibilities of applying digital technologies in enterprise systems development. Throughout the entire course, students will be invited to apply their multidisciplinary knowledge to critically assess realistic scenarios for strategic and tactical decision making. **Communications Skills**: This course will give the students the possibility to acquire and to understand major terms and concepts so as to communicate effectively their ideas, findings, proposals, analysis and critical reasoning in the area of data privacy and security. A special emphasis will be given to oral

	presentations and pitches in project group works, and to writing technical reports and documentation. **Learning skills**: This course will empower students with the capability to learn several analytical tools for maintaining and analyzing data, and to apply them to real-world problems in an independent and critical way. A strong emphasis will be given to the application of the techniques and tools covered in the course to complex business problems that are typical of today's data-driven companies.
Pre-requisites	Basic knowledge of information systems and IT architectures.
Course content	The course will cover the following topics: • Challenges to data privacy and security • Ethical issues • Software vulnerabilities • Cyberattack models • Planning, designing and implementing IT security • Cryptography • Network security • Security operation tools and techniques
Reference Books	Lecture notes, research papers and course material will be made available on the e-learning platform. Recommended reading: RG. Dhillon, Information Security, Text & Cases. Prospect Press 2018
Teaching Methods	The course consists of lectures complemented by teaching cases, practical lab sessions and group project works.
Assessment	There will be a midterm project assignment, a final project and a written exam. In the written exam students are required to demonstrate that: • they have acquired an in-depth understanding of data privacy and security; • they have a good knowledge of the key concepts and methods to plan, design, implement, manage and audit technological and organizational solutions to assure data privacy and security in digital business; • they are able to analyze the social and organizational implications of cyber risk in digital ecosystems; • they are able to select, design and implement the most appropriate security controls to mitigate risk in business organizations; • they understand the social and ethical responsibilities of applying digital technologies in enterprise systems. The written exam will count for 60% of the grade. In the midterm and final projects students are required to demonstrate that they are able to: • apply data analytics tools and techniques to support decision making in incident management and security operations; • design innovative solutions using data-driven analytics and deep learning for situational awareness in security operations; • communicate effectively their ideas, findings, proposals, analysis and critical reasoning. The midterm and the final projects will count for 20% of the grade each. Students that will not take the midterm and final project during the course are required to take an oral exam after the course. . The overall assessment will take into account the level of knowledge and understanding of data privacy and security; the capacity for thinking creatively, analytically and critically; the capacity to design, implement and evaluate solutions in the area of data privacy and security; and the capacity to present effectively findings and conclusions.