** Title **

Security, Privacy and Availability of Health Data (SEC4H)

** CFU **

9 CFU

** Learning outcomes **

The student will be able to protect health data by structuring a computer network and by adopting the proper security mechanisms to defend the data against malicious attackers. The student will also able to guarantee that adopted solutions guarantee the privacy of the data according to the GDPR. Lastly, the student will be able to deploy the availability of the data in spite of faults and malicious attacks against availability such as those implemented by ransomware gangs.

** Syllabus **

- Encryption 1 CFU
  - Symmetric
  - Asymmetric
- Risk assessment of ICT networks 2 CFU
  - Application vulnerabilities
  - OS vulnerabilities
  - Structural (System) Vulnerabilities
  - Vulnerability discovery
  - Vulnerability Classification
  - Attacks and Intrusions
  - Attack and defense platforms
- Risk management 3 CFU
  - Gap Analysis
  - Physical and logical segmentation
  - Firewalling
  - Intrusion detection and endpoint protection
  - Patching and patch scheduling
  - Zero trust network vs. VPN
  - Authentication
  - Role-based access control
- Data Availability 1 CFU
  - Ransomware attacks
  - Redundancy
  - Backup
  - Backup Integrity
- Data Confidentiality & Privacy 2 CFU
  - Data encryption at rest
  - Data encryption in transit
  - Data confidentiality in computation
    - Homorphic Encryption
    - Enclaves
    - Hardware support for enclaves
    - Intel Software Guard Extension
  - Side Channel Leaks in Web Applications

- Access log and log integrity
- Least privilege principle
- Privacy and cloud architectures
- Notification constraints

**** Course organization & Assessment****

Lectures: 50% The lectures will introduce the main methodologies to achieve robustness despite faults and adversarial attacks.

Laboratory/practice: 50% some lab activities will consist in the solution of security problems from the real world. Other labs activities will be implemented through a computer lab and will be focused on the configuration and evaluation of security tools such as firewalls, and intrusion detection systems and attack platforms.

Assessment: According to the participation in the discussions of security problems and the results of the computer lab activities.

**** Prerequisites ****

Computer and network programming

Operating System

Programming language and programming environment

Network protocols