



# UNIVERSITÀ DI PAVIA

Anno Accademico 2018/2019

## INFORMATION SECURITY

<b>Anno immatricolazione</b>	2017/2018
<b>Anno offerta</b>	2018/2019
<b>Normativa</b>	DM270
<b>SSD</b>	ING-INF/05 (SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI)
<b>Dipartimento</b>	DIPARTIMENTO DI INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE
<b>Corso di studio</b>	COMPUTER ENGINEERING
<b>Curriculum</b>	Computer Science and Multimedia
<b>Anno di corso</b>	2°
<b>Periodo didattico</b>	Primo Semestre (01/10/2018 - 18/01/2019)
<b>Crediti</b>	6
<b>Ore</b>	45 ore di attività frontale
<b>Lingua insegnamento</b>	English
<b>Tipo esame</b>	SCRITTO E ORALE CONGIUNTI
<b>Docente</b>	BARILI ANTONIO (titolare) - 6 CFU
<b>Prerequisiti</b>	Good knowledge of operating systems, networking and data base technologies.
<b>Obiettivi formativi</b>	Knowledge of information security techniques. Ability to assess the security level of some common software systems and to design improvement actions.
<b>Programma e contenuti</b>	<p>Introduction Security vs. Safety. Physical security. Information security: privacy, availability, integrity, authenticity. Information security threats and countermeasures.</p> <p>Basic Information Theory and Cryptography Introduction to information theory and cryptography. Historical development. Symmetric and asymmetric ciphers. Hashing functions</p>

and MACs. Pseudo-Random Number Generators. Digital certificates. Cryptanalysis.

#### Digital Signature

Digital documents and digital signatures. Creation, preservation and validation of digital documents. Digital documents as court evidence. Public key infrastructures. Italian and EU laws concerning digital signatures.

#### Copyright Protection

Introduction to copyright law. Software and database protection. Audio, video and picture protection. Digital rights management (DRM). Watermarking and steganography.

#### Communication Protection

Information communication and diffusion. Synchronous and asynchronous communication. E-mail. The Web as an information diffusion media. Communication privacy protection. Threats to the freedom and privacy of communications and countermeasures. Phishing.

#### Systems and Networks Protection

Access control: authentication, authorization and accounting. Physical and logical information protection. Networks protection. Firewalls. Threats to systems and communication networks. Malware.

#### Incident Response e Digital Forensics

Incident detection and response. System audit and log analysis. Intrusion Detection Systems. Introduction to digital forensics.

#### Metodi didattici

Lectures (hours/year in lecture theatre): 45  
Practical class (hours/year in lecture theatre): 0  
Practicals / Workshops (hours/year in lecture theatre): 0

#### Testi di riferimento

Lecture notes and online references provided by the instructor.

#### Modalità verifica apprendimento

Written test.

#### Altre informazioni

Written test.

#### Obiettivi Agenda 2030 per lo sviluppo sostenibile

[Sfidi e obiettivi di sviluppo sostenibile](#)