



POLITÉCNICA

INTERNATIONAL
CAMPUS OF
EXCELLENCE

COORDINATION PROCESS OF
LEARNING ACTIVITIES
PR/CL/001



E.T.S. de Ingenieros
Informáticos

ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

103000590 - Computer Security

DEGREE PROGRAMME

10AK - Master Universitario En Software Y Sistemas

ACADEMIC YEAR & SEMESTER

2022/23 - Semester 1

Index

Learning guide

1. Description.....	1
2. Faculty.....	1
3. Prior knowledge recommended to take the subject.....	2
4. Skills and learning outcomes	3
5. Brief description of the subject and syllabus.....	4
6. Schedule.....	5
7. Activities and assessment criteria.....	7
8. Teaching resources.....	9
9. Other information.....	10

1. Description

1.1. Subject details

Name of the subject	103000590 - Computer Security
No of credits	4 ECTS
Type	Optional
Academic year of the programme	First year
Semester of tuition	Semester 1
Tuition period	September-January
Tuition languages	English
Degree programme	10AK - Master Universitario en Software y Sistemas
Centre	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Academic year	2022-23

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Julio Mariño Carballo	D-2308	julio.marino@upm.es	Tu - 15:00 - 17:00 W - 12:30 - 13:30 Th - 15:00 - 17:00 F - 12:30 - 13:30 Please get in touch with the instructor to get an appointment in order to check his availability.

Manuel Carro Liñares (Subject coordinator)	2303	manuel.carro@upm.es	F - 15:00 - 19:00 Please send an e-mail to set up an appointment before going to the instructor's office.
---	------	---------------------	--

* The tutoring schedule is indicative and subject to possible changes. Please check tutoring times with the faculty member in charge.

2.3. External faculty

Name and surname	Email	Institution
Pedro Moreno	pedro.moreno@imdea.org	IMDEA Software Institute
Juan Caballero	Juan.caballero@imdea.org	IMDEA Software Institute
Marco Guarnieri	marco.guarnieri@imdea.org	IMDEA Software Institute
Dario Fiore	Dario.Fiore@imdea.org	IMDEA Software Institute
Ignacio Cascudo	ignacio.cascudo@imdea.org	IMDEA Software Institute
Srdjan Matic	srdjan.matic@imdea.org	IMDEA Software Institute

3. Prior knowledge recommended to take the subject

3.1. Recommended (passed) subjects

The subject - recommended (passed), are not defined.

3.2. Other recommended learning outcomes

- An undergraduate level course on computer security is desired but not required. Some demonstrable knowledge on the basic principles of computer security is necessary.

4. Skills and learning outcomes *

4.1. Skills to be learned

CEM8 - Aplicar los fundamentos teóricos y matemáticos adecuados al procesamiento y análisis de funciones y datos de diversa naturaleza, y evaluar y diseñar los métodos relacionados para su aplicación en dominios prácticos

CG1 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CG13 - Apreciación de los límites del conocimiento actual y de la aplicación práctica de la tecnología más reciente.

CG4 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG7 - Especificación y realización de tareas informáticas complejas, poco definidas o no familiares

CG8 - Planteamiento y resolución de problemas también en áreas nuevas y emergentes de su disciplina

CG9 - Aplicación de los métodos de resolución de problemas más recientes o innovadores y que puedan implicar el uso de otras disciplinas

CGI20 - Adquirir conocimientos científicos avanzados del campo de la informática que le permitan generar nuevas ideas dentro de una línea de investigación.

CGI23 - Capacidad de leer y comprender publicaciones dentro de su ámbito de estudio/investigación, así como su catalogación y valor científico

4.2. Learning outcomes

RA13 - Select and apply optimization methods to specific problems

RA12 - Be familiar with examples of real applications and research trends and lines

RA15 - Knowledge of techniques for proving code correctness

RA112 - Identify computer security threats and decide the best proactive and reactive measures against them

* The Learning Guides should reflect the Skills and Learning Outcomes in the same way as indicated in the Degree Verification Memory. For this reason, they have not been translated into English and appear in Spanish.

5. Brief description of the subject and syllabus

5.1. Brief description of the subject

This course gives students a general view of Computer Security. Lectures are divided in independent blocks which provide basic concepts in Computer Security, such as cryptography, software security, information access control, communication network security, or privacy. Each block includes a theory part to give students the basic concepts and a practical exercise to demonstrate and fix the presented concepts. The particular order and length of the topics in the blocks will depend on the schedule of the instructors.

5.2. Syllabus

1. Software Security
2. Physical Security
3. Cryptography
4. Network security

6. Schedule

6.1. Subject schedule*

Week	Classroom activities	Laboratory activities	Distant / On-line	Assessment activities
1	Introduction to Computer Security Duration: 02:00 Lecture			
2	Software security Duration: 02:00 Lecture			
3	Software security Duration: 02:00 Lecture			
4	Software security Duration: 02:00 Lecture			
5	Software security Duration: 02:00 Lecture			Practical problem / exercise on Software Security Individual work Continuous assessment Not Presential Duration: 04:00
6	Physical security Duration: 02:00 Lecture			
7	Physical security Duration: 02:00 Lecture			
8	Physical security Duration: 02:00 Lecture			Practical problem / exercise on Physical Security Individual work Continuous assessment Not Presential Duration: 04:00
9	Cryptography Duration: 02:00 Lecture			
10	Cryptography Duration: 02:00 Lecture			
11	Cryptography Duration: 02:00 Lecture			
12	Cryptography Duration: 02:00 Lecture			Practical problem / exercise on Cryptography Individual work Continuous assessment Not Presential Duration: 04:00

13	Network security Duration: 02:00 Lecture			
14	Network security Duration: 02:00 Lecture			
15	Network security Duration: 02:00 Lecture			Practical problem / exercise on Network Security Individual work Continuous assessment Not Presential Duration: 04:00
16				
17				Global exam Written test Final examination Presential Duration: 02:00

Depending on the programme study plan, total values will be calculated according to the ECTS credit unit as 26/27 hours of student face-to-face contact and independent study time.

* The schedule is based on an a priori planning of the subject; it might be modified during the academic year, especially considering the COVID19 evolution.

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
5	Practical problem / exercise on Software Security	Individual work	No Presential	04:00	25%	2 / 10	CG4 CG8 CG9 CG1 CG7 CG13 CGI20 CGI23
8	Practical problem / exercise on Physical Security	Individual work	No Presential	04:00	25%	2 / 10	CG4 CG8 CG9 CG1 CG7 CG13 CGI20 CGI23
12	Practical problem / exercise on Cryptography	Individual work	No Presential	04:00	25%	2 / 10	CG4 CG8 CG9 CG1 CG7 CG13 CGI20 CEM8 CGI23
15	Practical problem / exercise on Network Security	Individual work	No Presential	04:00	25%	2 / 10	CG4 CG8 CG9 CG1 CG7 CG13 CGI20 CGI23

7.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Global exam	Written test	Face-to-face	02:00	100%	5 / 10	CG4 CG8 CG9 CG1 CG7 CG13 CGI20 CEM8 CGI23

7.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Comprehensive exam	Written test	Face-to-face	02:00	100%	5 / 10	CG8 CG1 CG7 CG13 CGI20 CEM8 CG9 CGI23

7.2. Assessment criteria

- No mandatory activities are necessary to pass via the global exams.
- The minimum grade to pass the course is 5 over 10 (either when it is calculated as the weighted sum of individual homework or when it is the grade of a single comprehensive exam).
- The topics covered in each homework assignment can be tested separately in the final exam. A student only needs to make the exercises corresponding to homework assignments that s/he failed either in the regular and extraordinary global exams.
- The global exams, both regular and extraordinary, will be made in person.
- Copying from any source (either textbooks, the Internet, another student, or any other source) with or without the permission of the author of the source, as well as other types of academic fraud, can lead to a 'fail' grade in the course and / or being reported to the academic authorities, who will decide whether to take additional authoritative measures. In particular, in case of non-ethical or fraudulent behavior, the Law 3/2022 of February 24th will be applied, as well as the corresponding UPM regulations. Article 12 and 14 of Law 3/2022 states that a serious fault may mean, among other outcomes, failing the corresponding sitting.
- There are no learning blocks whose earned grades can be carried over to future academic courses.
- Failure to deliver the homework at the time and in the form stated by the instructor(s) may result in a failure for that exercise.
- Active participation in the course can be taken into account to fine-tune the student's final grade.

8. Teaching resources

8.1. Teaching resources for the subject

Name	Type	Notes
Various	Others	Will be decided based on the selected topics.

9. Other information

9.1. Other information about the subject