UNIVERSIDAD DE CASTILLA - LA MANCHA
GUÍA DOCENTE

1. General information

Course: SECURITY OF SOFTWARE SYSTEMS
Type: ELECTIVE
Degree: 407 - DEGREE PROGRAMME IN COMPUTER SCIENCE ENGINEERING
Center: 108 - SCHOOL OF COMPUTER SCIENCE OF C. REAL
Year: 4
Main language: Spanish
Use of additional languages:
Web site: https://campusvirtual.uclm.es

Code: 42333
ECTS credits: 6
Academic year: 2020-21
Group(s): 20
Duration: First semester
Second language:
English Friendly: Y
Bilingual: N

Lecturer: **DAVID GARCIA ROSADO** - Group(s): **20**

Building/Office	Department	Phone number	Email	Office hours
Fermín Caballero/2.15	TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN	+34926052105	david.grosado@uclm.es	Available on https://esi.uclm.es/categories/profesorado-y-tutorias

2. Pre-Requisites

This subject is based on the competences and contents acquired in the subjects of the Basic Training module and the Common to the Computer Branch module.

Software Engineering I.
Software Engineering II.
Databases.
Requirements Engineering.

3. Justification in the curriculum, relation to other subjects and to the profession

The connectivity, extensibility and complexity of the current software, as well as its social responsibility, reflect the need for the contents taught in this subject.

It is related to the following subjects:

Audit of information systems
Programming principles I and II.
Software Engineering.
Software Engineering Processes.

4. Degree competences achieved in this course

Course competences

Code	Description
INS01	Analysis, synthesis, and assessment skills.
INS02	Organising and planning skills.
INS03	Ability to manage information and data.
INS04	Problem solving skills by the application of engineering techniques.
INS05	Argumentative skills to logically justify and explain decisions and opinions.
IS05	Ability to detect, assess, and manage potential risks which may occur.
PER01	Team work abilities.
PER02	Ability to work in multidisciplinary teams.
PER04	Interpersonal relationship skills.
PER05	Acknowledgement of human diversity, equal rights, and cultural variety.
SIS01	Critical thinking.
SIS03	Autonomous learning.
SIS04	Adaptation to new scenarios.
SIS05	Creativity.
SIS06	Leadership skills.
SIS08	Initiative and entrepreneurial abilities.
SIS09	Care for quality.

5. Objectives or Learning Outcomes

Course learning outcomes

Description

Knowledge of the most relevant norms, standards and legislation regarding software security.

Knowledge of the main software security techniques and services.

Ability to identify, model and integrate software security requirements into the software development process.

6. Units / Contents

Unit 1: Fundamentals of Security
Unit 2: Introduction to Cryptography
Unit 3: Security Requirements and Security Design
Unit 4: Security Analysis and Testing
Unit 5: Security Risk Analysis and Management
Unit 6: Ethical and Legal Aspects of Security

ADDITIONAL COMMENTS, REMARKS

In the laboratory sessions, several tools of the Kali Linux environment, analysis and capture of security requirements, risk management and code analysis and testing are planned, and several case studies will be presented on which to work with the tools.

7. Activities, Units/Modules and Methodology

Training Activity	Methodology	Related Competences (only degrees before RD 822/2021)	ECTS	Hours	As	Com	Description
Class Attendance (theory) [ON-SITE]	Lectures	INS01 INS02 INS04 INS05 IS05 SIS01 SIS09	0.6	15	N	-	Teaching of the subject matter by lecturer (MAG)
Individual tutoring sessions [ON-SITE]		INS01 INS02 INS04 INS05 SIS09	0.18	4.5	N	-	Individual or small group tutoring in lecturer¿s office, classroom or laboratory (TUT)
Study and Exam Preparation [OFF-SITE]	Self-study	INS01 INS02 INS04 INS05 IS05 SIS03 SIS08 SIS09	1.8	45	N	-	Self-study (EST)
Other off-site activity [OFF-SITE]	Practical or hands-on activities	INS01 INS02 INS03 INS04 INS05 IS05 PER01 PER02 PER04 PER05 SIS03 SIS04 SIS05 SIS06 SIS08 SIS09	0.9	22.5	N	-	Lab practical preparation (PLAB)
Problem solving and/or case studies [ON-SITE]	Project/Problem Based Learning (PBL)	INS01 INS02 INS04 INS05 IS05 PER01 PER02 PER04 PER05 SIS01 SIS03 SIS04 SIS05 SIS06 SIS08 SIS09	0.6	15	Y	N	Worked example problems and cases resolution by the lecturer and the students (PRO)
Writing of reports or projects [OFF-SITE]	Self-study	INS01 INS02 INS04 INS05 IS05 PER01 PER02 PER04 PER05 SIS01 SIS03 SIS04 SIS05 SIS06 SIS08 SIS09	0.9	22.5	Y	N	Preparation of essays on topics proposed by lecturer (RES)
Laboratory practice or sessions [ON-SITE]	Practical or hands-on activities	INS01 INS02 INS03 INS04 INS05 IS05 PER01 PER02 PER04 PER05 SIS04 SIS05 SIS06 SIS08 SIS09	0.72	18	Y	Y	Realization of practicals in laboratory /computing room (LAB)
Final test [ON-SITE]	Assessment tests	INS01 INS02 INS04 INS05 IS05	0.3	7.5	Y	Y	Final test of the complete syllabus of the subject (EVA)
Total:			**6**	**150**			
Total credits of in-class work: 2.4				**Total class time hours: 60**			
Total credits of out of class work: 3.6				**Total hours of out of class work: 90**			

As: Assessable training activity
Com: Training activity of compulsory overcoming (It will be essential to overcome both continuous and non-continuous assessment).

8. Evaluation criteria and Grading System

Evaluation System	Continuous assessment	Non-continuous evaluation*	Description
Final test	40.00%	40.00%	Compulsory activity that can be retaken (rescheduling) to be carried out within the planned exam dates of the final exam call (convocatoria ordinaria).
Theoretical papers assessment	15.00%	15.00%	Non-compulsory activity that can be retaken. To be carried out before end of teaching period
Laboratory sessions	30.00%	30.00%	Compulsory activity that can be retaken. To be carried out during lab sessions
Assessment of active participation	15.00%	15.00%	Non-compulsory activity that can be retaken. To be carried out during the theory/lab sessions in the case of continuous evaluation students. The non-continuous evaluation students will have an alternative evaluation system for this activity.
Total:	**100.00%**	**100.00%**	

According to art. 4 of the UCLM Student Evaluation Regulations, it must be provided to students who cannot regularly attend face-to-face training activities the passing of the subject, having the right (art. 12.2) to be globally graded, in 2 annual calls per subject , an ordinary and an extraordinary one (evaluating 100% of the competences).

Evaluation criteria for the final exam:

Continuous assessment:

In compulsory activities, a minimum mark of 40% is required in order to pass that activity and have the possibility to therefore pass the entire subject. The evaluation of the activities will be global and therefore must be quantified by means of a single mark. If the activity consists of several sections, each section may be evaluated separately provided students are informed in writing of this evaluation criterion at the beginning of the academic year. In the case of the activities that may be retaken (i.e., rescheduling), an alternative activity or test will be offered in the resit/retake exam call (convocatoria extraordinaria).

The final exam will be common for all the theory/laboratory groups of the subject and will be evaluated by the lecturers of the subject in a serial way, i.e., each part of the final exam will be evaluated by the same lecturer for all the students.

A student is considered to pass the subject if she/he obtains a minimum of 50 points out of 100, taking into account the points obtained in all the evaluable activities, and also has passed all the compulsory activities.

For students who do not pass the subject in the final exam call (convocatoria ordinaria), the marks of activities already passed will be conserved for the resit/retake exam call (convocatoria extraordinaria). In the case of the passed recoverable activities, the student will have the opportunity to receive an alternative evaluation of those activities in the resit/retake exam call and, in that case, the final grade of the activity will correspond to the latter grade obtained.

The mark of the passed activities in any call, except for the final exam, will be conserved for the subsequent academic year at the request of the student, provided that mark is equal or greater than 50% and that the activities and evaluation criteria of the subject remain unchanged prior to the beginning of that academic year.

The failure of a student to attend the final exam will automatically result in her/him receiving a "Failure to attend" (no presentado). If the student has not passed any compulsory evaluation activity, the maximum final grade will be 40%.

Non-continuous evaluation:

Students who are unable to attend training activities on a regular basis may apply at the beginning of the semester for the non-continuous assessment mode. Similarly, if a student who is undergoing continuous assessment incurs any circumstance that prevents her/him from regularly attending the classroom-based training activities, she/he may renounce the accumulated mark in continuous assessment and apply for the non-continuous assessment mode. In this case, a notification by the student must be given before the date scheduled for the tests in the ordinary call, in accordance with a deadline that will be informed at the beginning of the semester.

Students who take the non-continuous assessment mode will be globally graded, in 2 annual calls per subject, an ordinary and an extraordinary one (evaluating 100% of the competences), through the assessment systems indicated in the column "Non-continuous assessment".

In the "non-continuous assessment" mode, it is not compulsory to keep the mark obtained by the student in the activities or tests (progress test or partial test) taken in the continuous assessment mode.

Specifications for the resit/retake exam:

Evaluation tests will be conducted for all recoverable activities.

Specifications for the second resit / retake exam:

Same characteristics as the resit/retake exam call.

9. Assignments, course calendar and important dates	
Not related to the syllabus/contents	
Hours	hours
General comments about the planning: The subject is taught in 3 x 1,5 hour sessions per week	

10. Bibliography and Sources

Author(s)	Title/Link	Publishing house	Citv	ISBN	Year	Description
JAVIER AREITIO Bertolín	SEGURIDAD DE LA INFORMACIÓN. Redes, Informática y Sistemas de Información	Paraninfo		978-84-9732-502-8	2008	
Aguilera López, Purificación	Seguridad informática	Editex		978-84-9771-657-4	2010	
Stallings, William	Computer security : principles and practice	Prentice Hall		978-0-13-513711-6	2008	
Viega, John	Building secure software : how to avoid security problems the right way	Addison-Wesley		0-201-72152-X	2002	