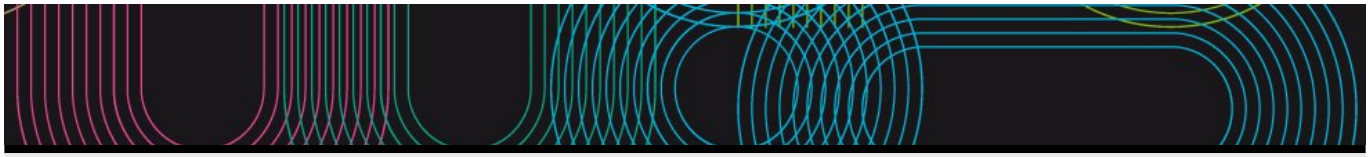

IDENTIFYING DATA				
(*)Seguridade en dispositivos móviles				
Subject	(*)Seguridade en dispositivos móviles			
Code	V05M175V11218			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician English			
Department				
Coordinator	López Bravo, Cristina			
Lecturers	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
E-mail	clbravo@det.uvigo.es			
Web	http://http://moovi.uvigo.gal			
General description	This course presents a general view of security in mobile devices with different characteristics. Based on the study of the architecture of these devices, we will discover their internal operation and which are the main security tools that they include, along with the risks and threats they suffer. We will study how to find, analyze and mitigate the vulnerabilities that affect mobile devices, using forensic analysis tools, secure application development and device management in business environments. The documentation of this course will be in English.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction: Threats and vulnerabilities that affect mobile devices	
Mobile devices architectures	
Security models in mobile devices	
Writing secure Applications	Permissions Packages management Users management APIs
Data security	
Devices security	
Network security	
Vulnerabilities, exploits and malicious applications	
Forensic analysis of mobile operating systems	
Enterprise Mobile Management Systems (EMM)	

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	9	9	18
Practices through ICT	12	12	24
Objective questions exam	2	14	16
Problem and/or exercise solving	0	5	5
Report of practices, practicum and external practices	0	12	12

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Lecturing	The professors of the course present the main theoretical contents related to security in mobile devices. Through this methodology competencies B14 and C14 get developed.
Practices through ICT	Students will complete guided and supervised practices. Through this methodology the competencies C14, D3, D8 and D9 get developed.

Personalized assistance

Methodologies	Description
Practices through ICT	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the lab sessions or during tutorial sessions. Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website. The tutorial sessions could also be agreed with the teacher by appointment.
Lecturing	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the master sessions or during tutorial sessions (also virtually). Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website. The tutorial sessions could also be agreed with the teacher by appointment.

Assessment

	Description	Qualification	Training and Learning Results
Objective questions exam	Short-questions exam on the theoretical and practical contents reviewed throughout the course, both in the lectures and in the laboratory practices. This exam will be done at the end of the term.	40	
Problem and/or exercise solving	Problem-solving tests where students make use of the acquired knowledge, in both theoretical and practical sessions. This test will be carried out throughout the term, with partial deliveries on the dates indicated by teachers.	25	
Report of practices, practicum and external practices	Students will individually fill questionnaires and/or write practice reports, where the right development and understanding of the practice get probed.	35	

Other comments on the Evaluation

ORDINARY EXAM

Following the guidelines of the degree, two evaluation systems will be offered to students attending this course: continuous assessment and global assessment.

Before the end of the fourth week of the course, students must declare if they opt for the continuous assessment or the global assessment. Those who opt for the continuous assessment system may not be listed as "not presented" if they make a delivery or an assessment test after the communication of their decision.

Continuous assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. To pass the course the final grade must be greater or equal to five.

Global assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. In this case, the problem-solving test (troubleshooting) will be done in a single test at the end of the term. To pass the course the final grade must be greater or equal to five.

EXTRAORDINARY EXAM

The assessment will consist in an objective questions exam, a problem-solving exam and delivering the practice reports of all the practices carried out throughout the course.

OTHER COMMENTS

The obtained grades are only valid for the current academic year.

The use of any material during the tests will have to be explicitly authorized.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Sources of information

Basic Bibliography

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

Complementary Bibliography

Joshua Drake, **Android hacker's handbook**, 1, Jonh Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, Jonh Wiley & Sons, 2013

Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013

David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016

Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Recommendations

Other comments

It is recommended to have Linux OS and Java programming skills. It is also recommended, but not indispensable, to have Android programming skills.