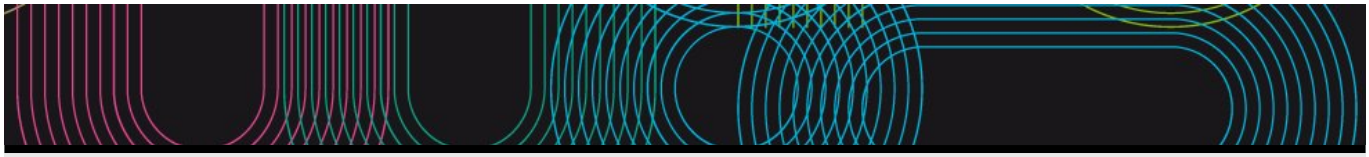

IDENTIFYING DATA				
Security in information systems				
Subject	Security in information systems			
Code	P52M182V01207			
Study programme	Master Universitario en Dirección TIC para la defensa			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	4	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Fernández Gavilanes, Milagros			
Lecturers	Fernández Gavilanes, Milagros Vales Alonso, Javier			
E-mail	mfgavilanes@cud.uvigo.es			
Web	http://campus.defensa.gob.es | https://moovi.uvigo.gal			
General description	The subject of Security in information systems will show the techniques, protocols and architectures related to security that exist at the different levels of implementation of a modern information system, with a particular emphasis on the communications part. The subject will focus on the clear exposition of these problems, and their practical resolution through practical study cases.			

Training and Learning Results	
Code	
A6	CB6 - Possess and understand knowledge that provides a basis or opportunity to be original in the development and / or application of ideas, often in a research context.
A7	CB7 - That students know how to apply the acquired knowledge and their ability to solve problems in new or poorly understood environments within broader (or multidisciplinary) contexts related to their area of study.
A8	CB8 - That students are able to integrate knowledge and face the complexity of formulating judgments based on information that, being incomplete or limited, includes reflections on the social and ethical responsibilities linked to the application of their knowledge and judgments.
A9	CB9 - That students know how to communicate their conclusions and the knowledge and ultimate reasons that support them to a specialized and unspecialized public in a clear and unambiguous way.
A10	CB10 - That students possess the learning skills that allow them to continue studying in a way that will be largely self-directed or autonomous.
B1	CG1 - Possess advanced and highly specialized knowledge and demonstrate a detailed and well-founded understanding of the theoretical and practical aspects dealt with in the different areas of study.
B2	CG2 - Integrate and apply the knowledge acquired, and possess the ability to solve problems in new or imprecisely defined environments, including multidisciplinary contexts related to their field of study.
B7	CG7 - Assess the importance of security aspects in the management of systems and information, identifying security needs, analyzing possible threats and risks and contributing to the definition and evaluation of security criteria and policies.
C18	CISTI4 - Define, analyze and implement security mechanisms throughout the life cycle of information systems.
D4	CT4 - Oral and written communication skills.
D6	CT6 - Properly manage information resources.

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

LO1: Understand the threats and vulnerabilities inherent in software development by showing how software can be made more secure.	A6 A7 A8 A9 A10 B1 B2 B7 C18
LO2: Describe the problems, threats and solutions used at different levels of a communications system/service.	A6 A7 A8 A9 A10 B1 B2 B7 C18
LO3: Describe the modern technical foundations of cryptography on which symmetric key and public key systems are based.	A6 A7 A8 A9 A10 B1 B2 B7 C18
LO4: Study public key infrastructure systems, including in detail how the creation, maintenance, distribution, use, storage and revocation of digital certificates will be addressed.	A6 A7 A8 A9 A10 B1 B2 B7 C18
LO5: Describe new applications and trends in the field of information systems security.	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6

Contents	
Topic	
Topic 1. Introduction to security in information systems.	- Introduction to Data Centres. - Typical structure - Administration of Data Processing Centres
Topic 2. Security in software development.	- sSDLC - Vulnerabilities - Countermeasures
Topic 3. Symmetric key encryption.	- Mathematical principles - Block coders (DES, Triple-DES, AES) - Stream coders (RC4)
Topic 4. Public key cryptography.	- Motivation - Mathematical principles - Diffie-Hellman - RSA - Elliptic Curve Cryptography (ECC)
Topic 5. Digital signatures.	- MAC and Hash systems - MD5 - SHA - HMAC

Topic 6. Key distribution systems and authentication.	- Introduction - Kerberos - X509 - Public key infrastructure (PKI)
Topic 7. Transport and web security.	- Motivation - SSL - TLS - SSH
Topic 8. Security in networks.	- IPSec - Firewalls - VPNs - Cloud systems
Topic 9. Trends in the use of security systems.	- Blockchain - Deep web - Anonymization - Cryptocurrencies - Zero Knowledge Proof Cryptography - Deniable Encryption - White box cryptography - Sharing of secrets - Steganography - Quantum cryptography - Electronic voting

Planning

	Class hours	Hours outside the classroom	Total hours
Autonomous problem solving	0	9	9
Previous studies	0	52	52
Lecturing	8	8	16
Problem solving	3	3	6
Practices through ICT	4	0	4
Seminars	4	0	4
Self-assessment	0	4	4
Presentation	4	0	4
Essay questions exam	1	0	1

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

Methodologies

	Description
Autonomous problem solving	Activity in which students analyze and solve problems and/or exercises related to the subject autonomously.
Previous studies	Search, reading, documentation work and/or autonomous performance of any other activity that the student considers necessary to enable him or her to acquire knowledge and skills related to the subject. It is usually carried out before classes, laboratory practices and/or evaluation tests.
Lecturing	Exposition by a lecturer of the contents of the subject under study, theoretical bases and/or guidelines of a work or exercise that the student has to develop.
Problem solving	Activity in which problems and/or exercises related to the subject are formulated. The student must develop the appropriate and correct solutions by exercising routines, applying formulas or algorithms, applying procedures for transforming the available information and interpreting the results.
Practices through ICT	Activities of application of knowledge in a specific context and acquisition of basic and procedural skills in relation to the subject, through the use of ICTs.
Seminars	Activity focused on work on a specific topic, which allows delving into or complementing the contents of the subject.

Personalized assistance

Methodologies	Description
Lecturing	Given the blended nature of the course, we will distinguish two cases: (1) Attention in the distance phase: it will be carried out through the use of telematic means. Students who wish to do so may pose questions to the teaching staff in forums or by email. They may also arrange individual tutorials with the teacher, which will take place via videoconference. (2) Attention in the face-to-face phase: although the use of telematic mechanisms for student attention is still possible, face-to-face tutoring mechanisms will also be used during this phase.

Problem solving	Given the blended nature of the course, we will distinguish two cases: (1) Attention in the distance phase: it will be carried out through the use of telematic means. Students who wish to do so may pose questions to the teaching staff in forums or by email. They may also arrange individual tutorials with the teacher, which will take place via videoconference. (2) Attention in the face-to-face phase: although the use of telematic mechanisms for student attention is still possible, face-to-face tutoring mechanisms will also be used during this phase.
Practices through ICT	Given the blended nature of the course, we will distinguish two cases: (1) Attention in the distance phase: it will be carried out through the use of telematic means. Students who wish to do so may pose questions to the teaching staff in forums or by email. They may also arrange individual tutorials with the teacher, which will take place via videoconference. (2) Attention in the face-to-face phase: although the use of telematic mechanisms for student attention is still possible, face-to-face tutoring mechanisms will also be used during this phase.
Seminars	Given the blended nature of the course, we will distinguish two cases: (1) Attention in the distance phase: it will be carried out through the use of telematic means. Students who wish to do so may pose questions to the teaching staff in forums or by email. They may also arrange individual tutorials with the teacher, which will take place via videoconference. (2) Attention in the face-to-face phase: although the use of telematic mechanisms for student attention is still possible, face-to-face tutoring mechanisms will also be used during this phase.

Assessment

	Description	Qualification	Training and Learning Results
Practices through ICT	Activities of application of knowledge in a specific context and acquisition of basic and procedural skills in relation to the subject, through the use of ICT. They allow evaluating the knowledge and skills of the student. There will be four deliverable activities (AE1, AE2, AE3 and AE4). The first three will be assessed during the distance learning phase: AE1 and AE2 will cover topic 3, while AE3 will cover topic 4 of the subject. In the case of deliverable AE4 this will be done during the face-to-face phase. Each deliverable will score 10% of the final mark.	40	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4
Self-assessment	Mechanism in which, through a series of questions or activities, it is possible for the student to autonomously assess their degree of acquisition of knowledge and skills on the subject, allowing self-regulation of the personal learning process. A questionnaire (AV) covering topics (1 to 8) will be administered during the distance learning phase.	10	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6
Presentation	Exhibition by the students, individually or in groups, of a topic related to the contents of the subject or the results of a job, exercise, project, etc. Through the presentation you can assess knowledge, skills and attitudes. This exhibition task (T) will be assessed during the face-to-face phase.	20	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6
Essay questions exam	Assessment test that includes open questions and/or exercises on a topic. Students must develop, relate, organize and present the knowledge they have on the subject in an argued response. It can be used to assess knowledge and skills. There will be a written test (PE) at the end of the face-to-face phase, in which all the topics and contents of the subject will be all the subjects and contents of the course (including the contents of the distance and face-to-face contents of the distance and face-to-face phases).	30	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4

Other comments on the Evaluation

If we call MED_CON the average mark for continuous assessment, which is calculated as follows:

MED_CON = 0.1*AE1 + 0.1*AE2+ 0.1*AE3 + 0.1*AE4 + 0.1*AV + 0.2*T + 0.3*PE

A grade of no less than 50% will be required to pass the subject.

In the case of evaluation in an extraordinary call, the student will have the option of redoing (totally or partially) the following evaluation activities:

- Self-assessment activities (test)
- Deliverables (practices)
- Presentations and/or expositions
- Exam

While participation in forums will be integrated into self-assessment activities.

Those activities that the student decides to repeat will be reassessed, losing the note of the previous call. The written test will be done online.

ACADEMIC INTEGRITY:

Students are expected to show adequate ethical behaviour, committing to act honestly. Based on article 42.1 of the *Regulation on the evaluation, qualification and quality of teaching and the student learning process of the University of Vigo*, **any violation of academic integrity in the assessment process, as well as the cooperation in it will result in the assignment of a failing grade to the student (zero) for the entire course in the corresponding assessment opportunity**, regardless of the percentage of importance that the test in question had in the overall continuous assessment and independently of other disciplinary actions that may be applied.

In the event that there is any difference between the guides in Galician/Spanish/English related to the evaluation, what is indicated in the teaching guide in Spanish will always prevail.

Sources of information

Basic Bibliography

William Stallings, **Network Security Essentials. Applications and Standards**, 5, Prentice Hall, 2013

Joshua Davies, **Implementing SSL/TLS. Using Cryptography and PKI**, Wiley, 2011

Complementary Bibliography

Tanenbaum Andrew, Wetherall David, **Computer Networks**, 5, Prentice Hall, 2010

Stuart McClure, Joel Scambray, George Kurtz, **Hacking exposed 7 network security secrets and solution**, 7, McGraw‐Hill, 2012

Recommendations

Subjects that it is recommended to have taken before

Security of the information/P52M182V01106