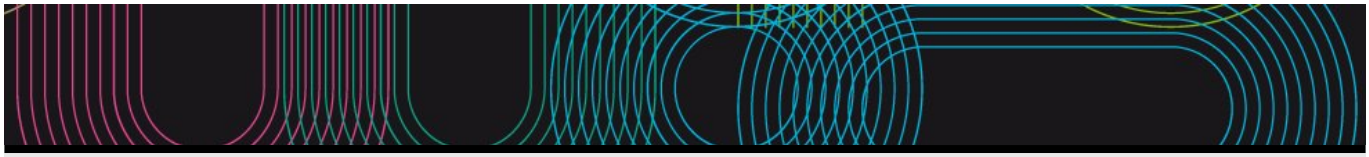

IDENTIFYING DATA				
Security of the information				
Subject	Security of the information			
Code	P52M182V01106			
Study programme	Master Universitario en Dirección TIC para la defensa			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Mandatory	1st	1st
Teaching language	Spanish			
Department				
Coordinator	Rodelgo Lacruz, Miguel			
Lecturers	Rodelgo Lacruz, Miguel			
E-mail	mrodelgo@cud.uvigo.es			
Web	http://moovi.uvigo.gal			
General description	This subject aims to provide students with training in the fundamental concepts of information security: the threats and vulnerabilities posed by new technologies, the most common types of computer attacks and ways to protect against them, the basic uses and applications of cryptography, user authentication methods and permissions management. Classroom lectures will be used for the introduction of theoretical concepts, which will be complemented by laboratory practices.			

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.
B3	CG3 - Direct, plan, coordinate, organize and/or supervise tasks, projects and/or human groups. Work cooperatively in multidisciplinary teams acting, where appropriate, as an integrator of knowledge and lines of work.
B6	CG6 - Be able to make decisions in environments characterized by complexity and uncertainty, evaluating the different existing alternatives in order to select the one with the most favorable expected result, appropriately managing the risk associated with the decision.
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.
C9	CE9 - Manage information security in regulatory, technical and methodological aspects.
D5	CT5 - Autonomous learning and work.

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

LO1 - Relate the terminology and essential concepts, both from a conceptual and technical point of view in the field of information security.	A6 A7 A8 A9 A10 B1 B6 B7 C9 D5
LO2 - Know the threats and vulnerabilities posed by new technologies, the most common types of computer attacks and ways to protect against them.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5
LO3 - Know the fundamentals, applications and uses of modern cryptography.	A6 A7 A8 A9 A10 B1 B7 C9 D5
LO4 - Be able to design and evaluate appropriate measures for user identification and authentication, as well as the management of identities and associated authorizations.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5

Contents	
Topic	
Definitions, concepts and basic principles	- Introduction - Properties of information security - Basic Concepts - Fundamental principles. - New cyber defense scenario
Threats and vulnerabilities	- Malware - Application threats - Network threats - Social engineering
Physical Security	- Environmental Threats - Technical threats - Man-made threats - Damage recovery and backup - Physical and logical security integration
Operational Security	- Human Resources - Systems operation
Cryptographic techniques	- Symmetric cryptography - Asymmetric cryptography - Cryptographic Hash
Identification and authentication	- Introduction: Authentication process, Authentication risk. - Authentication methods: Passwords, Tokens, Biometrics. - Remote authentication - Identity management

Authorization and access control	- Components of access control: Authentication, Authorization and Auditing. - AAA Protocols - Access control policies: DAC, MAC, RBAC, ABAC. - Identity Federation

Planning

	Class hours	Hours outside the classroom	Total hours
Previous studies	0	25	25
Lecturing	8	8	16
Practices through ICT	6	0	6
Seminars	1	0	1
Discussion Forum	0	5	5
Objective questions exam	2	0	2
Essay	0	20	20

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

Methodologies

	Description
Previous studies	Search, reading, documentation work and / or autonomously performing any other activity that the student considers necessary to enable the acquisition of knowledge and skills related to the subject. It is usually carried out prior to classes, laboratory practices and/or evaluation tests.
Lecturing	Presentation by a teacher of the contents of the subject under study, theoretical basis and / or guidelines for a work or exercise that the student has to develop.
Practices through ICT	Activities of knowledge application in a given context and acquisition of basic and procedural skills in relation to the subject, through the use of ICT.
Seminars	Activity focused on a specific topic, which allows to extend or complement the contents of the subject.
Discussion Forum	Activity developed in a virtual environment in which diverse and current topics related to the academic and/or professional field are discussed.

Personalized assistance

Methodologies	Description
Lecturing	It will be carried out through the use of online means. Students who may ask questions to the lecturer in forums or by e-mail. They will also be able to arrange individual tutorials with him, which will be carried out by videoconference.
Practices through ICT	Although it is still possible to use telematic mechanisms for student attention, in this case, face-to-face tutoring mechanisms will also be used.
Seminars	Although it is still possible to use telematic mechanisms for student attention, in this case, face-to-face tutoring mechanisms will also be used.

Assessment

	Description	Qualification	Training and Learning Results
Objective questions exam	A test that assesses knowledge and includes closed questions with different answer alternatives (true or false, multiple choice, item matching, etc.). Students select an answer from a limited number of possibilities. During the distance phase, three scoreable self-assessment questionnaires (P1, P2, and P3) will be conducted that will cover Block I (topics 1 and 2), II (topics 3 and 4), and III (topics 5, 6 and 7), respectively, and a specific questionnaire on social engineering (SE). At the end of the face-to-face phase, a final exam (FE) will be conducted that covers all the theoretical topics and practical contents of the subject.	75	A6 A7 A8 A9 A10 B1 B6 B7 C9 D5
Essay	An essay or document prepared on a topic that must be written according to established rules of style and length. It allows the evaluation of the student's skills, knowledge and, to a lesser extent, attitudes. An essay (E) will be carried out that will be evaluated during the distance phase: the E activity covers Block I (topics 1 and 2).	25	A6 A7 A8 A9 A10 B1 B3 B7 C9 D5

Other comments on the Evaluation

If we denote MED_CON as the average score of continuous assessment, it is calculated as:

MED_CON = 0.1*P1 + 0.1*P2 + 0.1*P3 + 0.05*SE + 0.25*E + 0.4*FE.

To pass the subject, it will be necessary to obtain 50% of the score and at least a 4 out of 10 on the final exam. The continuous assessment grade of students who do not obtain at least a 4 out of 10 on the final exam will be calculated as: MED_CON_FINAL = min(4, MED_CON).

In the event that the student fails to pass the course in the ordinary call, he/she will be entitled to a second evaluation opportunity (extraordinary call) to be held in the distance mode on the dates established for this purpose by the Master's Academic Committee. In this case, the evaluation will consist of a single written test that will account for 100% of the grade, being necessary to obtain at least 50% to pass the course.

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 case of any difference between the Galician/Spanish/English guides related to the evaluation, the Spanish guide will always prevail.

Sources of information

Basic Bibliography

Complementary Bibliography

William, Stallings, **Computer Security: Principles and Practice**, 4ª Ed., Pearson Education India, 2017

White, Gregory, et al., **CompTIA Security+ all-in-one exam guide**, 5ª Ed., McGraw-Hill, Inc., 2018

Centro Criptológico Nacional, **CCN-STIC guides**,

Recommendations

Other comments

It is recommended that students taking this course have a basic knowledge of computer systems and computer networks operation.