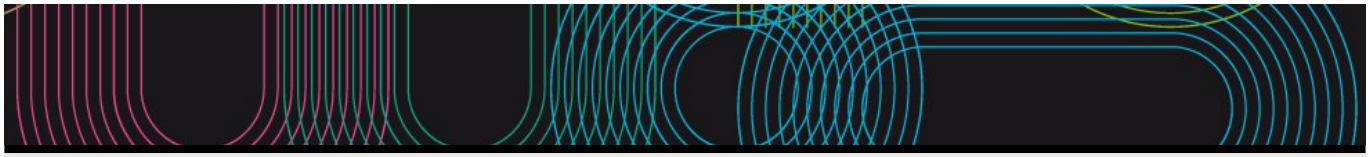

IDENTIFYING DATA				
Management of Information Security				
Subject	Management of Information Security			
Code	V05M175V01101			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	1st	1st
Teaching language	Spanish Galician			
Department				
Coordinator	Caeiro Rodríguez, Manuel			
Lecturers	Caeiro Rodríguez, Manuel Dafonte Vázquez, José Carlos Fernández Vilas, Ana			
E-mail	mcaeiro@det.uvigo.es			
Web	http://faitic.uvigo.es			
General description	This subject introduces the fundamental concepts related to the management of information security (e.g. vulnerability, threat, risk). It is devoted to the study of the methodologies, tools and specifications that deal with risk analysis and the development of information security management systems.			

Competencies	
Code	
A2	Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization.
A3	Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements.
B1	To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area.
B2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.
C5	To design, deploy and operate a security management information system based on a referenced methodology.
C7	To demonstrate ability for doing the security audit of systems, equipment, the risk analysis related to security weaknesses, and for developing de procedures for certification of secure systems.
C13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
D4	Ability to ponder the importance of information security in the economic progress of society.
D5	Ability for oral and written communication in English.

Learning outcomes	
Expected results from this subject	Training and Learning Results
To know the fundamental concepts related to Information Security Management: vulnerability, threat, risk, countermeasure, security policy, security plan	A2 A3 D4 D5
To know the different Information Security Management methodologies, commonly accepted	B1 B2 C5 D5

To know the proper tools to carry out tasks related to risk analysis and security audit, as well as knowing which are the most appropriate for each environment	B1 B2 C7 C13 D5

Contents	
Topic	
Foundations	Basic concepts: confidentiality, integrity, availability, threat, risk, etc. Legal framework of cybersecurity Standardization: standards and specifications Security operations centers
Risk analysis, management and certification	ISO 27005 and ISO 31000 Methodologies and risk analysis tools National Security Strategy
Information Security Management Systems	ISO27000, 27001 and 27002 National Scheme of Evaluation and Certification of Information Technologies Classification of information Training and awareness
Business impact	Cybersecurity roles Typical sequence of an attack Resilience Business continuity management Contingency plan
Security audit	Control objectives Frameworks and standards for the audit Audit of personal data security Delegate of data protection

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	19	29	48
Mentored work	0.5	10	10.5
Laboratory practical	18	57	75
Objective questions exam	1.5	3	4.5
Case studies	3	9	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	Presentation by the faculty of the subject syllabus. This methodology will be used to work on competencies: CE5, CE7, CE13, CT4 and CT5.
Mentored work	Each student individually will carry out a work on one of the topics of the subject to be presented in group A. This methodology will be used to work on competences CG1, CG2, CT4 and CT5.
Laboratory practical	In the lab, guided practices will be developed and practical case studies will be presented. This methodology will be used to work on competencies CB2, CB3, CG1, CG2, CE5, CE7, CE13 and CT5.

Personalized assistance	
Methodologies	**Description**
Lecturing	The teaching staff of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. The doubts will be answered in person or online (during the master's own session, or during the schedule established for the tutorials). The tutoring schedule will be established at the beginning of the course and will be published on the webpage of the subject.
Laboratory practical	The teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. Likewise, the faculty will guide the students during the realization of the tasks assigned to them in the laboratory practices. The doubts will be answered in person (during the internships, or during the scheduled time for tutorials). The tutoring schedule will be established at the beginning of the course and will be published on the website of the subject.

Mentored work	The teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. Likewise, the faculty will guide the students during the realization of the tasks assigned to them in the laboratory practices. The doubts will be answered in person (during the internships, or during the scheduled time for tutorials). The tutoring schedule will be established at the beginning of the course and will be published on the website of the subject.

Assessment

	Description	Qualification	Training and Learning Results		
Mentored work	Each student individually will carry out a work on one of the topics of the subject to be presented in group A.	10	B1 B2		D4 D5
Objective questions exam	Exam of theoretical knowledge and practical development	50	B1 B2	C5 C7 C13	D4 D5
Case studies	Exercises of practical cases on the risk analysis and the realization of security plans	40	A2 A3	C5 C7 C13	D5

Other comments on the Evaluation

Students can decide to be evaluated according to a continuous evaluation model or a single evaluation model. All students who submit the report of the first case study are opting for continuous assessment. Once the students choose the continuous assessment model, their grade can never be "Not Submitted".

The grade will be the result of applying the weighted average between results: (i) written exam (50%) (ii) case studies (40%), and (iii) mentored work (10%).

Written exam: will take place on the dates published in the official calendar.

Practical part:

1- Continuous evaluation model. Reports of 2 case studies and 2 evaluations of the peer reports that will be delivered in the weeks indicated in the document that will be provided to students on the first day of class. One report will be on risk analysis and the other on the development of a security plan (ISMS). Each report will have a weight in the final grade of 15% and each evaluation of 5%. The reports will be developed in a group and all students in the same group will receive the same grade. The evaluations will be carried out individually. It is also necessary to carry out a supervised work on a subject of the subject to be presented in group A.

2- Single evaluation model. Individual delivery of the 2 reports of the two practical cases on the same date of the written exam published in the official calendar. In this case, the evaluation of peer reports will not be carried out and each report will have a weight in the final grade of 25%.

In the second-chance assessment, students will be evaluated using the single evaluation modality.

If plagiarism is detected in any of the assessment tests, the final grade of the subject will be "Suspenso (0)", a fact that will be communicated to the school's management to adopt the appropriate measures.

Sources of information

Basic Bibliography

Campbell, Tony, **Practical Information Security Management: A Complete Guide to Planning and Implementation**, Apress, 2016

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012).**, AENOR, 2015

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices. (ISO 22313:2012).**, AENOR, 2015

UNE-EN ISO, **Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)**, AENOR, 2017

UNE-EN ISO, **Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).**, AENOR, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000:2018)**, ISO/IEC, 2018

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Guidance (ISO/IEC 27003:2017)**, ISO/IEC, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016)**, ISO/IEC, 2016

ISO/IEC, **Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2011)**, ISO/IEC, 2011

Complementary Bibliography

Gómez Fernández, Luis y Fernández Rivero, Pedro Pablo, **Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS**, AENOR, 2015

Fernández Sánchez, Carlos Manuel y Piatiini Velthuis, Mario, **Modelo para el gobierno de las TIC basado en las normas ISO**, AENOR, 2012

ISO, **Risk management -- Principles and guidelines (ISO/IEC 31000:2009)**, ISO, 2009

Alan Calder Steve Watkins, **IT Governance: An International Guide to Data Security and ISO27001/ISO27002**, 5, Kogan Page, 2012

Alan Calder, **Nine Steps to Success - North American edition: An ISO 27001:2013 Implementation Overview**, 1, IT Governance Publishing, 2017

Edward Humphreys, **Implementing the ISO / IEC 27001 ISMS Standard**, 2, Artech House, 2016

Recommendations

Contingency plan

Description

=== EXCEPTIONAL PLANNING ===
Given the uncertain and unpredictable evolution of the health alert caused by COVID-19, the University of Vigo establishes an extraordinary planning that will be activated when the administrations and the institution itself determine it, considering safety, health and responsibility criteria both in distance and blended learning. These already planned measures guarantee, at the required time, the development of teaching in a more agile and effective way, as it is known in advance (or well in advance) by the students and teachers through the standardized tool.

=== ADAPTATION OF THE METHODOLOGIES ===

Presentations for groups A will be provided through Faitic.

In the case of groups B, the teaching staff will be able to establish communication channels with the students through the Remote Campus, Faitic or other tools.

The tutoring sessions will be provided by telematic means (email, Remote Campus, Faitic forums, etc.) by prior appointment.

=== ADAPTATION OF THE TESTS ===

In case of activation of non-face-to-face teaching, no changes will be made in the evaluation model.