Universidade Vigo

IDENTIFYING DATA

Security management and risk analysis

Subject	Security management and risk analysis			
Code	P52M182V01107			
Study programme	Master Universitario en Dirección TIC para la defensa			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	4	Mandatory	1st	1st
Teaching language	Spanish			
Department				
Coordinator	Fernández Gavilanes, Milagros			
Lecturers	Fernández Gavilanes, Milagros López Román, Iago			
E-mail	mfgavilanes@cud.uvigo.es			
Web	http://campus.defensa.gob.es | https://moovi.uvigo.gal			
General description	The Security Management and Risk Analysis course aims to provide students with an overview of Information Security Management Systems (ISMS), describing the fundamentals of the existing standards for the certification of an ISMS, and paying special attention to risk analysis and management methodologies, as well as security incident response plans.			

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.
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.
D6	CT6 - Properly manage information resources.

Expected results from this subject

Expected results from this subject	Training and Learning Results

LO1: Understand the concept of Risk Management and assess its importance in ICT Systems.	A6 A7 A8 A9 A10 B1 B2 B6 B7 C9 D6
LO2: Understand the characteristics of the ISMS certification process.	A9 A10 B1 B7 C9 D6
LO3: Study the methodologies and tools available to analyse and manage risks.	A7 A10 B1 B3 B6 B7 C9 D6
LO4: To be familiar with MINISDEF's information security policy and management and the recommendations issued by the CCN.	A10 B7 C9 D6
LO5: Assess the scope and methodology to be followed in ICT system security audits.	A7 A8 A9 A10 B2 B6 B7 C9 D6
LO6: Understand how to carry out proper security incident management.	A7 A8 A10 B2 B6 B7 C9 D6

Contents	
Topic	
Topic 1: Introduction to Information Security Management.	- The strategic importance of information and digital assets. - The information security management process. - Definition of security policies, plans, and procedures. - Information Security Professionals: competencies, training, and certifications.
Topic 2: Risk Analysis and Management - The process of risk identification, analysis, and evaluation.	- Review of major vulnerabilities and types of attacks on computer systems. - Risk treatment. - MAGERIT methodology. - The model proposed by ISO 31000.
Topic 3: Information Security Management System.	- Characteristics of an ISMS (Information Security Management System). - Security certifications and standards: ISO 27001 and ENS. - Information security policy and management in MINISDEF. - STIC regulations of CCN.
Topic 4: Security Audits and Incident Response.	- The information security audit process. - Security incident management.

Topic 5: The importance of the human factor in information security.	- Aspects to consider regarding the human factor and security. - Social Engineering techniques. - Phishing attacks. - Definition of policies for safe and acceptable use of computer resources.

Planning

	Class hours	Hours outside the classroom	Total hours
Autonomous problem solving	0	5	5
Previous studies	0	55	55
Lecturing	16	8	24
Problem solving	2	2	4
Discussion Forum	0	5	5
Self-assessment	0	3	3
Presentation	3	0	3
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 analyse and solve problems and/or exercises related to the subject independently.
Previous studies	Research, reading, documentation work and/or autonomous performance of any other activity that the student considers necessary to enable him/her to acquire knowledge and skills related to the subject. This is usually carried out prior to classes, laboratory practicals and/or assessment tests.
Lecturing	Presentation by a teacher of the contents of the subject under study, theoretical bases and/or guidelines for a project 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 appropriate and correct solutions by exercising routines, applying formulas or algorithms, applying procedures for transforming the available information and interpreting the results.
Discussion Forum	An activity carried out in a virtual environment in which a variety of current topics related to the academic and/or professional sphere are debated.

Personalized assistance

Methodologies	Description
Lecturing	There are two methods of personalised attention: (1) Attention in the distance phase: this will be carried out through the use of telematic means. Students who wish to do so may ask the lecturers questions in forums or by e-mail. They will also be able to arrange individual tutorials with the lecturer, which will be carried out by videoconference. (2) Attention in the face-to-face phase: although it is still possible to use telematic mechanisms for student attention, during this phase face-to-face tutoring mechanisms will also be used.
Problem solving	There are two methods of personalised attention: (1) Attention in the distance phase: this will be carried out through the use of telematic means. Students who wish to do so may ask the lecturers questions in forums or by e-mail. They will also be able to arrange individual tutorials with the lecturer, which will be carried out by videoconference. (2) Attention in the face-to-face phase: although it is still possible to use telematic mechanisms for student attention, during this phase face-to-face tutoring mechanisms will also be used.

Assessment

	Description	Qualification	Training and Learning Results		
Discussion Forum	An activity carried out in a virtual environment in which a variety of current topics related to the academic and/or professional sphere are debated. It allows the assessment of skills, knowledge and, to a lesser extent, attitudes of the learner. A forum activity (F) will be carried out and assessed during the distance phase: activity F will cover topic 1 of the subject.	10	A6 A7 A10	C9	D6
Self-assessment	Mechanism in which, by means of a series of questions or activities, the student is able to autonomously assess his/her degree of acquisition of knowledge and skills on the subject, allowing self-regulation of the personal learning process. A questionnaire (AV) covering subjects 1, 2 and 3 will be carried out during the distance learning phase.	30	B1	C9	D6

Presentation	Presentation by the students, individually or in groups, of a topic related to the contents of the subject or the results of a work, exercise, project, etc. Through the presentation, knowledge, skills and attitudes can be assessed. This presentation work (P) will be assessed during the face-to-face phase and will cover topics 1 and 2.	30	A7 A8 A9 A10	B1 B2 B3 B6 B7	C9	D6
Essay questions exam	Assessment test which includes open questions and/or exercises on a topic. Students must develop, relate, organise and present their knowledge of the subject in a reasoned response. It can be used to assess knowledge and skills. A written test (PE) will be held at the end of the face-to-face phase, in which topics (1-5) of the subject will be assessed.	30	A10	B1	C9	D6

Other comments on the Evaluation

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

MED_CON = 0.1*F + 0.3*AV + 0.3*P + 0.3*PE

In order to pass the course, it will be necessary to achieve a grade of 50% or higher in all the evaluations of the course.

In the event that the student does not manage to pass the subject in the ordinary call, he/she will have the right to a second opportunity for assessment (extraordinary call) which will be carried out in distance mode on the dates established for this purpose by the Master's Academic Committee. The assessment process in the extraordinary call will be by means of a final exam.

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

Fernández, C. Manuel., Piattini, M., y Peso, E., **Auditoría Informática: Un enfoque práctico**, 2, Ra-Ma, 2000

Merino Bada, C. y Cañizares Sales, R., **Implantación de un sistema de gestión de seguridad de la información según ISO 27001**, 1, Fundación Confemetal, 2011

Talabis, M. y Martin, J., **Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis**, 1, Syngress, 2012

Tipton, H. F. and Micki K., **Information Security Management Handbook**, 5, Auerbach Publications, 2004

Recommendations

Subjects that are recommended to be taken simultaneously

Information systems/P52M182V01105