UniversidadeVigo

Subject Guide 2020 / 2021

IDENTIFYING DATA

Security Auditing and Management

Subject	Security Auditing and Management			
Code	O06M132V03203			
Study programme	(*)Máster Universitario en Enxeñaría Informática			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Méndez Reboredo, José Ramón			
Lecturers	Méndez Reboredo, José Ramón			
E-mail	moncho.mendez@uvigo.es			
Web	http://moovi.uvigo.gal			
General description	This course will review aspects of security including: physical security, network security, SS.OO. and services, application development security. It will also introduce Information Security Management Systems (ISMS): regulations and standards. Risk analysis, countermeasures, contingency plans and disaster recovery. Technical security audits and ISMS certification audits. Given the current nature of the topics, it may be necessary to use materials written in English and/or tools with a user interface in English. Translated with www.DeepL.com/Translator (free version) Besides this, the subject shows Information Security Management Systems (ISMS/ SGSI in spanish): rules and standard. Analysis of risks, countermeasures, contingency plans and disaster recovery. Technical security audits and ISMS certification audits. Given the novelty of the subject, the usage of materials written in English or the use of tools with English interfaces could be necessary.			

Competencies

Code	
A3	(CB8) That the students are able to integrate knowledges and confront to the complexity to formulate trials from an information that, being incomplete or limited, includes reflections on the social and ethical responsibilities linked to the application of his knowledges and trials.
B2	Ability to manage works and install computer systems, complying with current regulations and ensuring the quality of service.
B3	Ability to direct, schedule and supervise multidisciplinary teams
B7	Ability to start, direct and manage computer equipment manufacturing projects, guaranteeing safety for people and goods, the final quality of products and their approval
B9	Ability to understand and apply ethical responsibility, legislation and professional ethics of the activity of the profession of Computer Engineer
C7	
D2	Capacity for the dirección of teams and organizations
D3	Capacity of leadership
D5	Capacity of work in team
D6	Skills of relations interpersonales
D7	Capacity of reasoning crítico and creativity
D8	Responsibility and commitment ético in the desempeñor of the professional activity

D9	Respect and promoción of the human rights, the principles democráticos, the principles of equality between men and women, of solidarity, of universal accessibility and diseñor for all
D10	Orientation to quality and continuous improvement
D13	Capacity to integrate knowledges and enfrentarse to the complexity to formulate trials from an información incomplete

Learning outcomes

Expected results from this subject	Training and Learning Results
RA01: Know and know how to apply the tools, techniques, procedures and good practices available to ensure the security of information at various levels where it is necessary: physical security, network security and OS and security in the development of applications.	A3 B2 B3 B7 C7 D2 D5 D6 D7 D8 D10 D13
RA02: Knowing and understanding about Information Security regulations and standards, risk analysis methodologies and methodologies for conducting security audits.	A3 B2 B3 B7 C7 D2 D3 D5 D6 D7 D8 D10 D13
RA03: Ability to design and implement preventive measures, security policies and contingency plans based on the identification of security risks and vulnerabilities of computer systems	A3 B2 B3 B7 B9 C7 D2 D3 D5 D6 D7 D8 D9 D10 D13
RA04: Ability to design an organization's information security management system (ISMS), identify, define and implement its security controls, plan its implementation and manage its maintenance and improvement.	A3 B2 B3 B7 C7 D2 D3 D5 D6 D7 D8 D10 D13

RA05: To be able to design and execute security audits in the organizations, including those oriented to certification, according to the existing methodologies and good practices.	A3 B2 B3 B7 B9 C7 D2 D3 D5 D6 D7 D8 D9 D10 D13

Contents

Topic	
1. Security issues	1.1 Physical security 1.2 Network security, SS.OO. and services 1.3 Security in application development
2. Information Security Management Systems (ISMS)	2.1 Regulations and standards 2.2 Risk analysis, countermeasures, contingency plans and disaster recovery 2.3 Technical security audits 2.4 ISMS Certification Audits

Planning

	Class hours	Hours outside the classroom	Total hours
Laboratory practical	10.5	0	10.5
Lecturing	20.5	14	34.5
Objective questions exam	1	17	18
Problem and/or exercise solving	16	71	87

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

Methodologies

	Description
Laboratory practical	There will be practical activities, guided laboratory sessions, problem-solving seminars, etc. in groups, under the direction of a teacher. Pre- and post-lab and seminar activities may be included to help achieve the proposed objectives. Activities aimed at developing projects, case studies, reports, etc. will be particularly encouraged. Also, evaluation activities can be organized in these sessions.
Lecturing	Different activities will be used in the classroom, aimed at the whole group or at small groups. Mainly, lectures will be given to develop the fundamental contents of the subject and to achieve the active participation of the students, short individual or group activities will be carried out to apply the concepts exposed and to solve problems. In the proposed activities, the acquisition of knowledge and its application in the professional and research field of Computer Science will be promoted.

Personalized assistance

Tests	**Description**
Problem and/or exercise solving	Problems are posed some time before the end of the class so that students can come up with solutions (and support can be provided). The implementation of the solution is done autonomously until the next day of class. At the beginning of the next class, the students still have some time to finish the activity and be able to solve last minute technical questions.

Assessment

	Description	Qualification	Training and Learning Results
Objective questions exam	Examination. The dates are given in the section on other comments and second call. Learning outcomes RA01 and RA02 are assessed	50	B2 C7 D10 B7

Problem and/or exercise solving	The activities that the student will develop in a non-presential way will be oriented mainly to the acquisition of knowledge in the professional and research field of Computer Science, and to the development of the projects and works requested, either individually or in group. The performance of practical activities in the laboratory will be evaluated. They will be held in the course of the face-to-face sessions. Learning outcomes RA01, RA02, RA03, RA04 and RA05 will be evaluated.	50	A3	B2 B3 B7 B9	C7	D2 D3 D5 D6 D7 D8 D9 D10 D13

Other comments on the Evaluation

EVALUATION CRITERIA FOR ASSISTANTS 1st EDITION OF EVALUATION REPORTS

Students who regularly attend the class will have grades for "Problem solving and/or exercises" which will consist of different practical exercises that will be done in a group or individually during the course of the class and in a non-presential way. Students who have not passed (or completed) up to two of these problems may optionally make up for them through a specific practical test of the exercise or exercises to be made up. When the number of exercises to be made up exceeds two, the student must take the practical test for the entire "Problem solving and/or exercise" subject.

The practice test for the entire "Problem Solving and/or Exercise" subject will be taken on the official examination date just after the "Objective Question Test".

To pass the course, a student must have an average of 5 out of 10 points between the theory test (Objective Test) and the corresponding practical evaluation ("Problem Solving and/or Exercises" or the practical test for the entire "Problem Solving and/or Exercises" course).

ASSESSMENT CRITERIA FOR NON-ASSISTANTS

The evaluation for non-assistants will be equivalent to the evaluation for assistants when the student has been absent from more than two "Problem solving and/or exercise" tests. Therefore, the student must take the "Objective Question Test" and the corresponding evaluation of the practical test for the entire "Problem Solving and/or Exercise" subject. This test will be individual and includes the performance of exercises similar to those performed by the attending students. The dates are listed below. Learning outcomes: RA01, RA02, RA03, RA04 and RA05.

To pass the subject, a student must have an average of 5 points or more out of 10 among all the tests.

EVALUATION CRITERIA FOR THE 2ND EDITION OF EVALUATION REPORTS AND THE END OF DEGREE CALL

The same evaluation system applied to the first edition of the minutes will be used, keeping the qualification of the "Problem solving and/or exercises".

EVALUATION REPORTS FILLING

The grade to be recorded will be the average result between the Examination of objective questions and the "Problem solving and/or exercise" or practical test of the "Problem solving and/or exercise" subject.

EVALUATION DATES

The schedule of assessment tests officially approved by the Xunta de Centro of the ESEI is published on the website http://www.esei.uvigo.es.

Sources of information

Basic Bibliography

Inteco, **Guía SGSI de INTECO-CERT (https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf)**,

ISO27000.es, **El portal de ISO 27001 en español. Gestión de Seguridad de la Información**,

Complementary Bibliography

LUIS GOMEZ FERNANDEZ, **CÓMO IMPLANTAR UN SGSI SEGÚN UNE-ISO/IEC 27001:2014 Y SU APLICACI ON EN EL ESQUEMA NACIONAL DE SEGURIDAD**, 9788481439083, 1, AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERT, 2015

DAVID ROLDAN MARTINEZ; JOSE MANUEL HUIDOBRO MOYA, **SEGURIDAD EN REDES Y SISTEMAS INFORMATICOS**, 978-8428329170, 1, EDICIONES PARANINFO, 2005

CHRIS MCNAB, **SEGURIDAD DE REDES**, 9788441524026, 2, ANAYA MULTIMEDIA, 2008

Recommendations

Other comments

The student must be able to use the tools of the Internet to obtain information (search engines, forums, etc.).

It is recommended to have typing skills for this and other subjects.

Contingency plan

Description

=== PLANNED EXCEPTIONAL MEASURES ===
In view of the uncertain and unpredictable evolution of the health alert caused by the COVID-19, the University of Vigo has established an extraordinary planning that will be activated at the time when the administrations and the institution itself determine it in accordance with safety, health and responsibility criteria, and guaranteeing teaching in a non-presential or partially presential scenario. These measures, already planned, guarantee the development of teaching in a more agile and effective way when they are known beforehand (or well in advance) by students and teachers through the standardized and institutionalized tool of teaching guides.

=== SCENARIO 1: MIXED TEACHING
In the case of an exceptional situation in which the full capacity of the classrooms where teaching is given cannot be used, a mixed teaching will be carried out, in which part of the students will be able to attend the classes in person, while another part of the students will be able to follow the classes online through the Remote Campus.

In this situation, the methodologies and evaluation systems will be maintained. Evaluations will be done in person (e.g. by requesting larger classrooms). If this is not possible, they will be carried out through the Remote Campus, Faitic and/or other services of the University of Vigo. In this case, students will be informed sufficiently in advance.

Tutorials will preferably be done online. In order to be able to organize the tutorials better, students must inform the teaching staff of their wish to do so beforehand by e-mail.

=== SCENARIO 2: NON-PRESENTIAL TEACHING ===
In the case of an exceptional situation in which it is not possible to teach in person, classes will be given online through the Remote Campus.

In such a situation, the methodologies and evaluation systems will be maintained. Evaluations will be carried out through the Remote Campus, Faitic and/or other services of the Universidade de Vigo. These changes will be communicated to the students with sufficient notice.

Regarding the tutorials, they will be done online and, in order to make a better organization, students must communicate to the faculty their desire to perform a tutorial in advance through an email.

In exceptional cases where a student justifies the existence of a situation that prevents him/her from following the subject in a normal way (e.g. connectivity problems, conciliation problems, etc.), he/she may agree with the teaching staff to adapt the dates of the assessment tests, as well as the means of taking them. In any case, the assessment systems will be maintained.