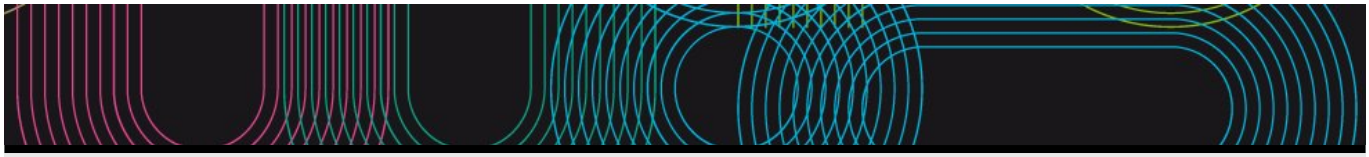

IDENTIFYING DATA				
Security Auditing and Management				
Subject	Security Auditing and Management			
Code	O06M132V03203			
Study programme	Máster Universitario en Ingeniería Informática			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
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.			

Training and Learning Results	
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	Ability to design, develop, manage and evaluate security assurance certification mechanisms for information processing and access in a local or distributed processing system.
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

Expected results from this subject	
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
Laboratory practice	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	Different activities will be used in the classroom, aimed at the whole group or small groups. Mainly, lectures will be held to develop the fundamental contents of the subject and to achieve the active participation of students, short individual or group activities will be carried out to apply the concepts presented and solve problems. The proposed activities will promote the acquisition of knowledge and its application in the professional and research field of Computer Science. Attendance at these sessions is not mandatory.
Lecturing	Practical activities, guided laboratory sessions, problem-solving seminars, etc. will be carried out in groups, under the guidance of a lecturer. Activities prior to and after the laboratory and seminar sessions may be included to help achieve the proposed objectives. Activities aimed at the development of projects, practical cases, reports, etc. will be especially encouraged. In addition, assessment activities may be organised in these sessions. Attendance at these sessions is not mandatory.

Personalized assistance	
Tests	**Description**
Laboratory practice	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	40	B2 C7 D10 B7

Laboratory practice	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.	60	A3	B2 B3 B7 B9	C7	D2 D3 D5 D6 D7 D8 D9 D10 D13

Other comments on the Evaluation

CONTINUOUS EVALUATION SYSTEM

The continuous evaluation system consists of two parts: (*i*) the exam of objective questions and (*ii*) the laboratory practices.

(i). Objective questions exam
This is an exam that will take place on the date scheduled in the final exam calendar of the center. It will consist of short or multiple-choice questions and will serve to evaluate the theoretical knowledge acquired by the student.
Methodology(es) applied: Examination of objective questions.
% Grading: 40%.
Minimum %: To pass the subject the student must obtain a grade between the two tests of the subject higher than 5 out of 10.
Competences assessed: B2, B7, C7 and D10.
Assessed outcomes: R01 and R02.

(ii). Laboratory practice
Consists of the delivery of all the laboratory practices proposed throughout the course.
Methodology(es) applied: Laboratory practicals.
% Grade: 60% in total (around 15% each of them).
Minimum %: To pass the subject the student must obtain a grade between the two tests of the subject higher than 5 out of 10.
Competences assessed: A3, B2, B3, B7, B9, C7, D2, D3, D5, D6, D7, D8, D9, D10 and D13.
Assessed outcomes: R01, R02, R03, R04 and R05.

A student who submits any of the laboratory practicals is understood to be under the continuous evaluation procedure described above.
If a student does not submit any of the tests, he/she will be assigned a grade of 0 in it.

GLOBAL EVALUATION SYSTEM

When a student does not present any of the laboratory practices, it will be understood that he/she chooses the global evaluation modality.

In the same way as in the previous case, the global evaluation system consists of two parts: (*i*) the exam of objective questions and (*ii*) the laboratory practicals.

(i). Objective questions exam
This is an exam that will be held on the date scheduled in the final examination calendar of the center. It will consist of short or multiple-choice questions and will serve to evaluate the theoretical knowledge acquired by the student.
Methodology(s) applied: Examination of objective questions.
Grading %: 40%.
Minimum %: To pass the subject the student must obtain a grade between the two tests of the subject higher than 5 out of 10.
Competences assessed: B2, B7, C7 and D10.
Assessed outcomes: R01 and R02.

(ii). Laboratory practice
It is assumed that the student does not attend regularly to the practical sessions and/or does not make the corresponding deliveries so he/she will have to take an exam that will be held after (and on the same day) the exam of objective questions where the acquisition of the practical knowledge of the subject will be evaluated.
Methodology(ies) applied: Examination of laboratory practices.
% Grading: 60% in total (3-4 practices at 25-33% each).
Minimum %: To pass the subject the student must obtain a grade between the two tests of the subject higher than 5 out of

10.
Competences assessed: A3, B2, B3, B7, B9, C7, D2, D3, D5, D6, D7, D8, D9, D10 and D13.
Assessed outcomes: R01, R02, R03, R04 and R05.

EVALUATION CRITERIA FOR THE EXTRAORDINARY AND END-OF-COURSE EXAMS

The continuous and global evaluation systems described above will be used. For these exams, the grades of the parts passed in the common exam will be kept.

GRADING PROCESS

In any case, the grade that will appear in the minutes will be the weighted mean of the grades recorded in the exam of objective questions and in the laboratory practice.

EVALUATION DATES

The official exam dates for the different exams, officially approved by the ESEI's Xunta de Centro, are published on the ESEI's web page (https://esei.uvigo.es).

USE OF MOBILE DEVICES

All students are reminded of the prohibition of the use of mobile devices during the evaluation tests. In particular, Article 13.2.d) of the University Student Statute, regarding the duties of university students, establishes the duty to refrain from "the use of or cooperation in fraudulent procedures in evaluation tests, in the work carried out or in official university documents".

QUERY/REQUEST FOR TUTORIALS

Tutorials can be consulted through the faculty member's personal page, accessible through the address https://esei.uvigo.es/docencia/profesorado/.

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). Último acceso 08/07/2022**,

ISO27000.es, **El portal de ISO 27001 en español. Gestión de Seguridad de la Información (https://www.iso27000.es). Último acceso 08/07/2022**,

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**, 978-84-8143-900-7, 1, AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERT, 2015

DAVID ROLDAN MARTINEZ; JOSE MANUEL HUIDOBRO MOYA, **SEGURIDAD EN REDES Y SISTEMAS INFORMATICOS**, 9788428329170, 1, EDICIONES PARANINFO, 2005

CHRIS MCNAB, **SEGURIDAD DE REDES**, ‎978-8441517516, 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.