UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. General information

Course: AUDIT AND SECURITY MANAGEMENT
Code: 310608
Type: CORE COURSE
ECTS credits: 6
Degree: 2361 - MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA (AB) (2020)
Academic year: 2022-23
Center: 604 - SCHOOL OF COMPUTER SCIENCE AND ENGINEERING (AB)
Group(s): 10 11
Year: 1
Duration: First quarter
Main language: Spanish
Second language:
Use of additional languages:
English Friendly: Y
Web site:
Bilingual: N

Lecturer: **ENRIQUE ARIAS ANTUNEZ** - Group(s): **10 11**

Building/Office	Department	Phone number	Email	Office hours
Agrupación Politécnica/ Desp. 0.A.8		2497	enrique.arias@uclm.es	https://www.esiiab.uclm.es/pers.php?codpers=earias&idmenup=pers&curso=2022-23

2. Pre-Requisites

Not established

3. Justification in the curriculum, relation to other subjects and to the profession

This course belongs to the "Quality and Safety" subject, and offers the student a wide vision of the concepts of audit and security, as well as the role that these concepts play in companies' information systems.
Through Audit and Security Management, the aim is to make known the aspects related to the audit and security of information systems and technologies, considering both legislative and regulatory aspects, among other dimensions.
In the Computer Engineering profession, the competencies related to audit and security management are among the most demanded and recognized, from IT governance and management, to the creation and management of Information Security (ISMS), carrying out risk analysis and management, as well as analysis of its impact on companies.
The implementation of audit and security management departments (Internal Control), as well as facing other challenges in emerging audit and security management issues related to cybersecurity, critical infrastructure, contingency plans and disaster recovery are also key activities for this profession.

4. Degree competences achieved in this course

Course competences

Code	Description
CE06	Ability to secure, manage, audit and certify the quality of developments, processes, systems, services, applications and computing products.
INS03	Ability to manage information and data.
INS04	Problem solving skills by the application of engineering techniques.
INS05	Argumentative skills to logically justify and explain decisions and opinions.
PER01	Team work abilities.
PER02	Ability to work in multidisciplinary teams.
PER04	Interpersonal relationship skills.
PER05	Acknowledgement of human diversity, equal rights and cultural variety.
SIS01	Critical thinking.
SIS02	Ethical commitments.
SIS03	Autonomous learning.
SIS09	Care for quality.
UCLM02	Ability to use Information and Communication Technologies.
UCLM04	Professional ethics.

5. Objectives or Learning Outcomes

Course learning outcomes

Description
Assess and certify the security of the system software based on the existing rules and standards, as well as the most appropriate security maturity models
Plan, implement and operate departments responsible for the audit, safety and quality control tasks in companies
Perform an IT management audit based on existing rules and standards
Perform a system security audit based on the existing rules and standards

6. Units / Contents

Unit 1: Information Systems Audit
Unit 2: IT Governance
Unit 3: Information Systems Security

Unit 4: TI Security in the Organization
Unit 5: Risk Management
Unit 6: Business Continuity
Unit 7: Cybersecurity

ADDITIONAL COMMENTS, REMARKS

The order of the agenda may be changed depending on the availability of the visiting professor

7. Activities, Units/Modules and Methodology

Training Activity	Methodology	Related Competences	ECTS	Hours	As	Com	Description
Class Attendance (theory) [ON-SITE]	Combination of methods	CE06 INS03 INS04 INS05 SIS01 SIS02 SIS09 UCLM04	1.6	40	N	-	This activity is developed during the time dedicated to theory exposing the fundamental concepts that will be the object of the final exams. The students will do it either by videoconference or by watching the recordings of the class afterwards.
Laboratory practice or sessions [ON-SITE]	Projects based learning	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	0.8	20	Y	Y	TThe laboratory practicals are organised according to the syllabus in the laboratory. Both face-to-face and blended learning students have to do all the practicals and, therefore, send the relevant reports. The practicals are made up by doing the practicals. A total of 6 practicals of approximately 30 hours will be carried out. 4 of them will deal with the implementation of an Information Security Management System and the other 2 with cybersecurity issues. In order to carry out the first 4 practicals, students are required to review the standards that will be made available to them on the Virtual Campus. In the practices related to cybersecurity, no prior knowledge is required since they are seen in the seminars associated with these practices.
Individual tutoring sessions [ON-SITE]		SIS01 SIS02 SIS09 UCLM04	0.3	7.5	N	-	This activity is carried out in a face-to-face manner in the tutor's office and in a blended manner by video conferencing through digital tutoring.
Other off-site activity [OFF-SITE]	Project/Problem Based Learning (PBL)	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	1.5	37.5	N	-	Problem solving and case preparation: This activity takes place outside the classroom and/or laboratory and consists of reviewing additional documentation necessary for the correct functioning of the large group. It is usually based on the additional resources provided by the teacher through the Virtual Campus platform. In addition, regulations such as the LOPD must be analysed and studied individually in order to comment on the forum.
Study and Exam Preparation [OFF-SITE]	Self-study	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	1.8	45	N	-	PLAB Preparation of laboratory practices: Before the development of the practices, the students have to review the international standards on which they are based, as well as the operation of the tools that will be used to carry them out.
		Total:	**6**	**150**			
		Total credits of in-class work: 2.7					**Total class time hours: 67.5**
		Total credits of out of class work: 3.3					**Total hours of out of class work: 82.5**

As: Assessable training activity
Com: Training activity of compulsory overcoming (It will be essential to overcome both continuous and non-continuous assessment).

8. Evaluation criteria and Grading System

Evaluation System	Continuous assessment	Non-continuous evaluation*	Description
Practical exam	25.00%	25.00%	(LAB) Practical work related to cybersecurity shall be assessed up to 2,5 points. These will be assessed under the supervision of the student in the laboratory.

Theoretical papers assessment	25.00%	25.00%	(INF) ISMS practices will be assessed by the submission of practice reports.
Final test	40.00%	40.00%	(ESC) In the middle of the course there will be a mid-term exam (Mid-term exam I) with a grade of 3 points. At the end of the course there will be a partial exam (Partial Exam II) with a mark of 1 point.
Oral presentations assessment	10.00%	10.00%	(PRES) Over the course of the term, a group or individual project will be carried out on the implementation of an Information Security Management System that is carried out in a practical manner (3 practices). For this work, the implemented ISMS will be presented, in particular practices 2 and 3, in class and its report will be evaluated in the section "theoretical papers assessment".
Total:	**100.00%**	**100.00%**	

According to art. 4 of the UCLM Student Evaluation Regulations, it must be provided to students who cannot regularly attend face-to-face training activities the passing of the subject, having the right (art. 12.2) to be globally graded, in 2 annual calls per subject , an ordinary and an extraordinary one (evaluating 100% of the competences).

Evaluation criteria for the final exam:

Continuous assessment:

Practices will be evaluated in a continuous manner presenting the corresponding reports (practices 1 to 4) or by observation (practices 1 and 4).
Theory exam and presentation will be done at the end of term. The theory exam will be done at the ordinary or extraordinary call being complusoty to attend face-to-face. The presentation could be done face-to-face or by Teams.

To pass the subject the followin constrains are applicable:
1.- Each student has to prepare a question per lesson on a Wiki.
2.- A score higher than 1,5 points must be obtained in the theory exam.
3.- A score higher than 3 points must be achieved adding the scores in practices + report + presentation.
4.- Once the minimum scores are got, then the rest of scores are directly added.

If a student has completed 50% of assessable activities or, if in any case, the class period has ended, he/she will be considered in continuous assessment without the possibility of changing the assessment modality.

If it is proved that any of the sections have been copied, the entire call will be suspended.

Non-continuous evaluation:

For those students that decide to follow the non-continuoud modality could send the reports of practices at the end of the course.
Presentation and theory exam have non-continuous evaluation.
To pass the subject the followin constrains are applicable:
1.- Each student has to prepare a question per lesson on a Wiki.
2.- A score higher than 1,5 points must be obtained in the theory exam.
3.- A score higher than 3 points must be achieved adding the scores in practices + report + presentation.
4.- Once the minimum scores are got, then the rest of scores are directly added.

Remeber that, if a student has completed 50% of assessable activities or, if in any case, the class period has ended, he/she will be considered in continuous assessment without the possibility of changing the assessment modality.

If it is proved that any of the sections have been copied, the entire call will be suspended.

Specifications for the resit/retake exam:

Same as for the non-continuous evaluation of the ordinary call

Specifications for the second resit / retake exam:

Same as for the non-continuous evaluation of the ordinary call

9. Assignments, course calendar and important dates

Not related to the syllabus/contents	
Hours	**hours**
Laboratory practice or sessions [PRESENCIAL][Projects based learning]	20
Individual tutoring sessions [PRESENCIAL][]	7.5
Other off-site activity [AUTÓNOMA][Project/Problem Based Learning (PBL)]	37.5
Study and Exam Preparation [AUTÓNOMA][Self-study]	45
Unit 1 (de 7): Information Systems Audit	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	5
Unit 2 (de 7): IT Governance	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	2
Unit 3 (de 7): Information Systems Security	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	5
Unit 4 (de 7): TI Security in the Organization	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	3
Unit 5 (de 7): Risk Management	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	8

Unit 6 (de 7): Business Continuity	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	5
Unit 7 (de 7): Cybersecurity	
Activities	**Hours**
Class Attendance (theory) [PRESENCIAL][Combination of methods]	12
Global activity	
Activities	**hours**
Laboratory practice or sessions [PRESENCIAL][Projects based learning]	20
Individual tutoring sessions [PRESENCIAL][]	7.5
Other off-site activity [AUTÓNOMA][Project/Problem Based Learning (PBL)]	37.5
Study and Exam Preparation [AUTÓNOMA][Self-study]	45
Class Attendance (theory) [PRESENCIAL][Combination of methods]	40
Total horas:	150

10. Bibliography and Sources

Author(s)	Title/Link	Publishing house	Citv	ISBN	Year	Description
	www.nist.gov					National Institute of Standards and Technology
	https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/					MAGERIT versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
	http://www.coso.org/					The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
	www.iso27000.es					Página web dedicada a la normativa ISO27000
	www.isaca.org					Information Systems Audit and Control Association
	www.bsigroup.es					BSI Group
	www.aenor.es					Asociación Española de Normalización
DEL PESO NAVARRO, EMILIO /						En la actualidad nadie duda que la información se ha convertido en uno de los activos principales de las empresas, representando las tecnologías y los sistemas relacionados con la información su principal ventaja estratégica. Las organizaciones invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información y en la adquisición y desarrollo de tecnologías que les ofrezcan la mayor productividad y calidad posibles. Es por eso que los temas relativos a la auditoría de las tecnologías y los sistemas de información (TSI) cobran cada vez más relevancia a nivel mundial. Esta obra presenta de forma clara y precisa los conceptos fundamentales sobre control interno y auditoría de TSI, ofrece un tratamiento sistemático de

DEL PESO, MAR / PIATTINI VELTHUIS, MARIO G	AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.	RA-MA	978-84-7897-849-6	2008	las técnicas y métodos del auditor informático, aborda los aspectos organizativos, jurídicos y deontológicos asociados a la auditoría de TSI, expone en profundidad las principales áreas de la auditoría de TSI: física, seguridad, explotación, bases de datos, redes, técnica de sistemas, dirección, aplicaciones, etc.; y proporciona pautas y experiencias que ayuden al auditor en sus tareas. Colaboran en el libro más de veinte autores, entre los que se encuentran profesores de universidad y profesionales de reconocido prestigio en el mundo de la auditoría de TSI, reuniendo algunos de ellos las dos cualidades, lo que aporta un gran valor añadido a la obra al ofrecer perspectivas y experiencias muy variadas sobre prácticamente todos los aspectos relacionados con este tema.
	http://www.ra-ma.es/libros/AUDITORIA-DE-TECNOLOGIAS-Y-SISTEMAS-DE-INFORMACION/338/978-84-7897-849-6				
Juan Luis García Rambla	Ataques en redes de datos IPv4 e IPv6	0xword	978-84-617-9278-8	2017	
Daniel Echevarri Montoya	Hacking con Python	0xword	978-84-606-5559-6	2017	
David Puente Castro	Linux Exploiting. Técnicas de explotación de vulnerabilidades en Linux para la creación de exploits	0xword	978-84-616-4218-2	2017	
Pablo González, Germán Sánchez y Jose Miguel Soriano.	Pentesting con Kali Linux Rolling Release 2017	0xword	978-84-608-3207-2	2017	
	OWASP Internet of Things Project				
	https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project				
Pablo González Pérez y Chema Alonso	Metasploit para Pentesters.	0xword	978-84-617-1516-9	2017	
Michael Sikorski and Andrew Honig	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	No Starch Press	978-1593272906	2012	
	Seguridad IoT en Sanidad				
	https://apisa.com.es/wp-content/uploads/2018/05/Seguridad-IoT-en-Sanidad-Estamos-Preparados.pdf				
David Cannon	CISA ® Certified Information Systems Auditor ® Study Guide	Wiley Publising Inc.	978-0-470-61010-7	2011	