UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura: GESTIÓN DE AUDITORÍA Y SEGURIDAD
Código: 310608
Tipología: OBLIGATORIA
Créditos ECTS: 6
Grado: 2358 - MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA (AB)
Curso académico: 2019-20
Centro: 604 - E.S. DE INGENIERIA INFORMATICA ALBACETE
Grupo(s): 10 11
Curso: 1
Duración: Primer cuatrimestre
Lengua principal de impartición: Español
Segunda lengua:
Uso docente de otras lenguas:
English Friendly: S
Página web: https://campusvirtual.uclm.es/login/index.php
Bilingüe: N

Profesor: **ENRIQUE ARIAS ANTUNEZ** - Grupo(s): **10 11**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
Agrupación Politécnica/ Desp. 0.A.8	SISTEMAS INFORMÁTICOS	2497	enrique.arias@uclm.es	The tutoring schedule will be at the Computing Systems Dept. web site: http://www.dsi.uclm.es/pers.php?codpers=earias

Profesor: **JOSE LUIS MARTINEZ MARTINEZ** - Grupo(s): **10 11**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
ESII-1.C.11	SISTEMAS INFORMÁTICOS	2294	joseluis.martinez@uclm.es	Publicada en la página de la ESII. Se atenderá cualquier día y hora previa cita a través del mail

2. REQUISITOS PREVIOS

No se han establecido.

3. JUSTIFICACIÓN EN EL PLAN DE ESTUDIOS, RELACIÓN CON OTRAS ASIGNATURAS Y CON LA PROFESIÓN

Esta asignatura pertenece a la materia de "Calidad y Seguridad", y ofrece al alumno una amplia visión de los conceptos de auditoría y seguridad, así como el papel que estos conceptos juegan en los sistemas de información de las empresas.

Mediante **Gestión de Auditoría y Seguridad** se pretende dar conocer los aspectos relativos a la auditoría y seguridad de los sistemas y tecnologías de información, contemplando tanto los aspectos legislativos como los normativos, entre otras dimensiones.

En la profesión de Ingeniería Informática, las competencias relativas con la gestión de la auditoría y seguridad son de las más demandadas y reconocidas, desde el gobierno y gobernanza de las TI, hasta la creación y gestión de Sistemas de Gestión de la Seguridad de la Información (SGSI), la realización de análisis y gestión de riesgos, así como análisis de su impacto en las empresas.

La puesta en marcha de departamentos de auditoría y gestión de la seguridad (Control Interno), así como afrontar otros retos en temas emergentes de gestión de la auditoría y la seguridad relativa a ciberseguridad, infraestructuras críticas, planes de contingencia y recuperación ante desastres, también son actividades clave para esta profesión.

4. COMPETENCIAS DE LA TITULACIÓN QUE LA ASIGNATURA CONTRIBUYE A ALCANZAR

Competencias propias de la asignatura

Código	Descripción
CE06	Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.
INS03	Capacidad de gestión de la información.
INS04	Capacidad de resolución de problemas aplicando técnicas de ingeniería.
INS05	Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.
PER01	Capacidad de trabajo en equipo.
PER02	Capacidad de trabajo en equipo interdisciplinar.
PER04	Capacidad de relación interpersonal.
PER05	Reconocimiento a la diversidad, la igualdad y la multiculturalidad.
SIS01	Razonamiento crítico.
SIS02	Compromiso ético.
SIS03	Aprendizaje autónomo.
SIS09	Tener motivación por la calidad.
UCLM02	Capacidad para utilizar las Tecnologías de la Información y la Comunicación.
UCLM04	Compromiso ético y deontología profesional.

5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

Resultados de aprendizaje propios de la asignatura

Descripción

Evaluar y certificar la seguridad de los sistemas software en base a las normas y estándares existentes, así como a los modelos de madurez de la seguridad más adecuados.

Planificar, poner en marcha y explotar departamentos responsables de las tareas de auditoría, seguridad y gestión de la calidad en las empresas.

Realizar auditorías de la dirección de informática en base a las normas y estándares existentes.

Realizar auditorías de seguridad de los sistemas en base a las normas y estándares existentes.

6. TEMARIO

Tema 1: Introducción a la Gestión de la Auditoría y la Seguridad
Tema 2: Introducción a la Seguridad y Auditoría de los Sistemas de Información
Tema 2.1 Introducción a la Auditorí
Tema 3: Áreas de la Auditoría
Tema 4: Introducción al Gobierno de las TI
Tema 5: Ciclo de vida de Sistemas de Información
Tema 6: Implementación de Sistemas y Operaciones
Tema 7: Continuidad de Negocio y Recuperación ante Desastres
Tema 8: Introducción al Sistema de Gestión de Seguridad de la Información (SGSI)
Tema 9: Conceptos básicos de análisis forense
Tema 10: Forense de red y de RAM.
Tema 11: Análisis forense de Malware
Tema 12: Detección de amenazas en IoT
Tema 13: Prácticas
Tema 13.1 Práctica 1: Plan de Continuidad de Negocio y Recuperación ante Desastres
Tema 13.2 Práctica 2: Fase Plan del SGSI
Tema 13.3 Práctica 3: Gestión del riesgo
Tema 13.4 Práctica 4: Fases Do, Check y Act del SGSI
Tema 13.5 Práctica 5: Forense de red y RAM. Casos prácticos.
Tema 13.6 Práctica 6: Herramientas para el Análisis Forense de Malware
Tema 13.7 Práctica 7: Aplicación del Procesamiento de Eventos Complejos a la Detección de Amenazas en IoT

7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas (para títulos anteriores a RD 822/2021)	ECTS	Horas	Ev	Ob	Rec	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Combinación de métodos	CE06 INS03 INS04 INS05 SIS01 SIS02 SIS09 UCLM04	1.6	40	S	S	S	Esta actividad se desarrolla durante el espacio de tiempo dedicado a teoría exponiendo los conceptos fundamentales que serán objeto de los exámenes finales. Los alumnos semipresenciales la realizarán bien por videoconferencia, o visionando las grabaciones de la clase a posteriori.
Prácticas de laboratorio [PRESENCIAL]	Aprendizaje orientado a proyectos	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	0.8	20	S	S	S	Las prácticas de laboratorio se organizan según temario en el laboratorio. Tanto presenciales como semipresenciales han de realizar todas las prácticas, y por tanto,enviar los informes pertinentes y realizar el examen de prácticas.
Tutorías individuales [PRESENCIAL]		SIS01 SIS02 SIS09 UCLM04	0.3	7.5	N	-	-	Esta actividad se realiza de manera presencial en el despacho del tutor y de manera semipresencial a través de videoconferencia por tutoría digital.
Otra actividad no presencial [AUTÓNOMA]	Aprendizaje basado en problemas (ABP)	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	1.5	37.5	N	-	-	Resolución de problemas y preparación de casos: Esta actividad se realiza fuera de aula y/o laboratorio que consiste en repaso de documentación adicional necesaria para la marcha correcta del grupo grande. Se suele basar en los recursos adicionales proporcionados por el profesor a través de la plataforma Campus Virtual. Además, se han de analizar y estudiar de manera individual normativas como LOPD para comentar en el foro.
Estudio o preparación de pruebas [AUTÓNOMA]	Trabajo autónomo	CE06 INS03 INS04 INS05 PER01 PER02 PER04 PER05 SIS01 SIS02 SIS03 SIS09 UCLM02 UCLM04	1.8	45	N	-	-	PLAB Preparación de prácticas de laboratorio: Previo al desarrollo de las prácticas, los alumnos han de repasar los estándares internacionales en las que estas se basan, así como el funcionamiento de las herramientas que se utilizarán

								para la realización de las mismas.
				Total:	**6**	**150**		
				Créditos totales de trabajo presencial: 2.7				**Horas totales de trabajo presencial: 67.5**
				Créditos totales de trabajo autónomo: 3.3				**Horas totales de trabajo autónomo: 82.5**

Ev: Actividad formativa evaluable
Ob: Actividad formativa de superación obligatoria
Rec: Actividad formativa recuperable

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

	Valoraciones		
Sistema de evaluación	**Estudiante presencial**	**Estud. semipres.**	**Descripción**
Prueba final	50.00%	50.00%	(ESC) A mitad de la asignatura tendrá lugar un examen parcial (Examen parcial I) con una puntuación de 3 puntos. Al final de la asignatura habrá un examen parcial (Examen parcial II) que tendrá una puntuación de 2 puntos.
Presentación oral de temas	10.00%	10.00%	(PRES) En el trascurso del cuatrimestre se realizará un trabajo en grupo o de manera individual sobre ciertos aspectos jurídicos. Para este trabajo no será necesaria la presentación de una memoria, pero sí de realizar una exposición en clase. Este trabajo no tendrá puntuación, será una actividad formativa. Al final de la asignatura se realizará una presentación del SGSI y será sumativa por pares.
Práctico	25.00%	25.00%	(LAB) Las prácticas relativas a auditoría de sistemas IoT se valorarán hasta 2,5 puntos. Éstas se evaluarán con la supervisión del alumno en el laboratorio.
Elaboración de trabajos teóricos	15.00%	15.00%	(INF) Las prácticas de gestión de riesgo se evaluarán con la presentación informes de prácticas. En particular se presentará un informe de la práctica 1, y otro al final de las prácticas 2-4, recogiendo el trabajo realizado durante las mismas. El primer informe tendrá un valor de 0,5 puntos y el segundo de 1 punto.
Total:	**100.00%**	**100.00%**	

Criterios de evaluación de la convocatoria ordinaria:
La nota se divide en 4 puntos relativos a las prácticas, 5 puntos de teoría y 1 punto de presentación.

.- De los 4 puntos de prácticas hay que sacar al menos 2 puntos repartidos de las siguiente manera: 1 de la primera parte de la asignatura y 1 de la segunda parte de la asignatura. las prácticas no son recuperables. Sí lo son las entregas (Elaboración de trabajos teóricos)
.- De los 5 puntos de teoría hay que sacar al menos 2.5 puntos. En la convocatoria ordinaria se realizará un parcial de la primera y otro de la segunda parte de la asignatura, y en la convocatoria ordinaria el estudiante que no se ha presentado a los parciales, ha suspendido alguno o quiere subir nota puede hacerlo en dicha convocatoria. Por tanto, los puntos de teoría son recuperables
.- El último punto se refiere a la presentación de trabajo hay que obtener un mínimo de 0,5 puntos.

Para superar la asignatura, entre todo, hay que sumar al menos 5 puntos.

La nota superada en cada parte se guardará hasta la convocatoria especial de finalizacion, si el alumno decide presentarse a extraordinaria o finalización bien para mejorar la nota o bien para recuperar las partes que le quedan.

Particularidades de la convocatoria extraordinaria:
No se guardarán los parciales, por lo que en el caso de teoría se pueden recuperar los 5 puntos de teoría.

Particularidades de la convocatoria especial de finalización:
No se guardarán los parciales, por lo que en el caso de teoría se pueden recuperar los 5 puntos de teoría.

9. SECUENCIA DE TRABAJO, CALENDARIO, HITOS IMPORTANTES E INVERSIÓN TEMPORAL

No asignables a temas

Horas	**Suma horas**
Tutorías individuales [PRESENCIAL][]	7.5
Otra actividad no presencial [AUTÓNOMA][Aprendizaje basado en problemas (ABP)]	6.5
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	90

Comentarios generales sobre la planificación: La planificación podría varias en función de la dinámica del propio grupo. Los cambios serán consensuados por todos los agentes implicados y notificados en la plataforma virtual de manera pertinente y siempre por adelantado.

Tema 1 (de 13): Introducción a la Gestión de la Auditoría y la Seguridad

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	1

Periodo temporal: Semana 1
Comentario: .

Tema 2 (de 13): Introducción a la Seguridad y Auditoría de los Sistemas de Información

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	5

Periodo temporal: Semanas 1 y 2

Tema 3 (de 13): Áreas de la Auditoría

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	1.5
Periodo temporal: Semanas 2	

Tema 4 (de 13): Introducción al Gobierno de las TI	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	.5
Periodo temporal: Semana 2	

Tema 5 (de 13): Ciclo de vida de Sistemas de Información	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 3	

Tema 6 (de 13): Implementación de Sistemas y Operaciones	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 3	

Tema 7 (de 13): Continuidad de Negocio y Recuperación ante Desastres	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 6	

Tema 8 (de 13): Introducción al Sistema de Gestión de Seguridad de la Información (SGSI)	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 5	

Tema 9 (de 13): Conceptos básicos de análisis forense	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	4
Periodo temporal: Semana 11	

Tema 10 (de 13): Forense de red y de RAM.	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 11	

Tema 11 (de 13): Análisis forense de Malware	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 13	

Tema 12 (de 13): Detección de amenazas en IoT	
Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2
Periodo temporal: Semana 14	

Tema 13 (de 13): Prácticas	
Actividades formativas	**Horas**
Prácticas de laboratorio [PRESENCIAL][Aprendizaje orientado a proyectos]	14
Otra actividad no presencial [AUTÓNOMA][Aprendizaje basado en problemas (ABP)]	6
Periodo temporal: Semana 6-14	

Actividad global	
Actividades formativas	**Suma horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	26
Prácticas de laboratorio [PRESENCIAL][Aprendizaje orientado a proyectos]	14
Tutorías individuales [PRESENCIAL][]	7.5
Otra actividad no presencial [AUTÓNOMA][Aprendizaje basado en problemas (ABP)]	12.5
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	90
Total horas:	150

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título/Enlace Web	Editorial	Población	ISBN	Año	Descripción
	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
	www.nist.gov					National Institute of Standards and Technology

					MAGERIT versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) http://www.coso.org/
DEL PESO NAVARRO, EMILIO / DEL PESO, MAR / PIATTINI VELTHUIS, MARIO G	AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.	RA-MA	978-84-7897-849-6	2008	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 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
	Ataques en redes de datos IPv4 e				

Juan Luis García Rambla	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