# UNIVERSIDAD DE CASTILLA - LA MANCHA

# GUÍA DOCENTE

## 1. DATOS GENERALES

| | | | |
|---|---|---|---|
| **Asignatura:** | GESTIÓN DE AUDITORÍA Y SEGURIDAD | **Código:** | 310608 |
| **Tipología:** | OBLIGATORIA | **Créditos ECTS:** | 6 |
| **Grado:** | 2361 - MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA (AB) (2020) | **Curso académico:** | 2023-24 |
| **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 | https://www.esiiab.uclm.es/pers.php?codpers=earias&idmenup=pers&curso=2023-24 |

## 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: Auditoría de los Sistemas de Información**
**Tema 2: Introducción al Gobierno de las Tecnologías y Sistemas de Información**
**Tema 3: Seguridad de los Sistemas de Información**
**Tema 4: Seguridad de TI en la Organización**
**Tema 5: Gestión de Riesgos**
**Tema 6: Continuidad de Negocio**
**Tema 7: Ciberseguridad**

## COMENTARIOS ADICIONALES SOBRE EL TEMARIO

El orden del temario podrá sufrir modificaciones en función de la disponibilidad del profesor visitante.

## 7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

| Actividad formativa | Metodología | Competencias relacionadas (para títulos anteriores a RD 822/2021) | ECTS | Horas | Ev | Ob | Descripción |
|---|---|---|---|---|---|---|---|
| Enseñanza presencial (Teoría) [PRESENCIAL] | Combinación de métodos | CE06 INS03 INS04 INS05 SIS01 SIS02 SIS09 UCLM04 | 1.6 | 40 | N | - | 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 | 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. Las prácticas se recuperan haciendo las prácticas. Se realizarán un total de 3 prácticas de una duración aproximada de 30h. 2 de ellas versarán sobre la implementación de un Sistema de Gestión de Seguridad de la Información y la otra sobre cuestiones relativas a la ciberseguridad. Para la realización de las 2 primeras prácticas se requiere que el alumno repase los estándares que se pondrá a sus disposición en Campus Virtual. En la práctica relacionada con ciberseguridad, no se requiere un conocimiento previo puesto que se ven en los seminarios asociados a dichas 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 (Será imprescindible su superación tanto en evaluación continua como no continua)

## 8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

| Sistema de evaluación | Evaluacion continua | Evaluación no continua* | Descripción |
|---|---|---|---|
| Práctico | 25.00% | 25.00% | (LAB)<br>Las prácticas relativas a ciberseguridad se valorarán hasta 2,5 puntos. Éstas se evaluarán con la supervisión del alumno en el laboratorio. |
| Elaboración de trabajos teóricos | 25.00% | 25.00% | (INF)<br>Las prácticas de SGSI se evaluarán con la presentación informes de prácticas. |
| Prueba final | 40.00% | 40.00% | (ESC)<br>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 1 puntos. T |
| Presentación oral de temas | 10.00% | 10.00% | (PRES) A lo largo del cuatrimestre se realizará un trabajo en grupo o individual sobre la implantación de un Sistema de Gestión de la Seguridad de la Información que se realiza de forma práctica (3 prácticas). Para este trabajo, se presentará en clase el SGSI implantado, en particular las prácticas 2 y 3, y se evaluará su informe en el apartado "evaluación de trabajos teóricos". |
| **Total:** | **100.00%** | **100.00%** | |

** En **Evaluación no continua** se deben definir los porcentajes de evaluación según lo dispuesto en el art. 4 del Reglamento de Evaluación del Estudiante de la UCLM, que establece que debe facilitarse a los estudiantes que no puedan asistir regularmente a las actividades formativas presenciales la superación de la asignatura, teniendo derecho (art. 12.2) a ser calificado globalmente, en 2 convocatorias anuales por asignatura, una ordinaria y otra extraordinaria (evaluándose el 100% de las competencias).*

**Criterios de evaluación de la convocatoria ordinaria:**

**Evaluación continua:**

Las prácticas se evaluarán de forma continua presentando las correspondientes memorias (prácticas 1 a 4) o por observación (prácticas 1 y 4).
El examen de teoría y la presentación se harán al final del cuatrimestre. El examen de teoría se realizará en la convocatoria ordinaria o extraordinaria siendo la complicidad para asistir presencialmente. La presentación podrá realizarse de forma presencial o por Equipos.

Para aprobar la asignatura son aplicables las siguientes limitaciones:
1.- Cada alumno tiene que preparar una pregunta por lección en una Wiki.
2.- Se debe obtener una puntuación superior a 1,5 puntos en el examen de teoría.
3.- Se debe conseguir una puntuación superior a 3 puntos sumando las puntuaciones en prácticas + informe + presentación.
4.- Una vez obtenidas las puntuaciones mínimas, se suman directamente el resto de puntuaciones.

Si un alumno ha completado el 50% de las actividades evaluables o, en todo caso, ha finalizado el periodo de clase, será considerado en evaluación continua sin posibilidad de cambiar la modalidad de evaluación.

Si se prueba que en cualquiera de los apartados ha evaluar ha habido copia, se suspenderá la convocatoria completa.

**Evaluación no continua:**

Aquellos alumnos que decidan seguir la modalidad no continua podrán enviar las memorias de prácticas al final del curso.
La presentación y el examen de teoría tienen evaluación no continua.
Para aprobar la asignatura se aplican las siguientes restricciones
1.- Cada alumno tiene que preparar una pregunta por lección en una Wiki.
2.- Se debe obtener una puntuación superior a 1,5 puntos en el examen de teoría.
3.- Se debe conseguir una puntuación superior a 3 puntos sumando las puntuaciones en prácticas + informe + presentación.
4.- Una vez obtenidas las puntuaciones mínimas, se suman directamente el resto de puntuaciones.

Recuerde que, si un alumno ha completado el 50% de las actividades evaluables o, si en algún caso, ha finalizado el periodo de clase, será considerado en evaluación continua sin posibilidad de cambiar la modalidad de evaluación.

Si se prueba que en cualquiera de los apartados ha evaluar ha habido copia, se suspenderá la convocatoria completa.

**Particularidades de la convocatoria extraordinaria:**

Igual que en la evaluación no continua de la convocatoria ordinaria

**Particularidades de la convocatoria especial de finalización:**

Igual que en la evaluación no continua de la convocatoria ordinaria

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

**No asignables a temas**

| Horas | Suma horas |
|---|---|
| Prácticas de laboratorio [PRESENCIAL][Aprendizaje orientado a proyectos] | 20 |
| Tutorías individuales [PRESENCIAL][] | 7.5 |
| Otra actividad no presencial [AUTÓNOMA][Aprendizaje basado en problemas (ABP)] | 37.5 |
| Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo] | 45 |

**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 7): Auditoría de los Sistemas de Información | |
|---|---|
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 5 |
| **Periodo temporal:** Semanas 2 | |
| **Tema 2 (de 7): Introducción al Gobierno de las Tecnologías y Sistemas de Información** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 2 |
| **Periodo temporal:** Semana 2 | |
| **Tema 3 (de 7): Seguridad de los Sistemas de Información** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 5 |
| **Periodo temporal:** Semana 3 | |
| **Tema 4 (de 7): Seguridad de TI en la Organización** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 3 |
| **Periodo temporal:** Semana 3 | |
| **Tema 5 (de 7): Gestión de Riesgos** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 8 |
| **Periodo temporal:** Semana 6 | |
| **Tema 6 (de 7): Continuidad de Negocio** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 5 |
| **Periodo temporal:** Semana 5 | |
| **Tema 7 (de 7): Ciberseguridad** | |
| **Actividades formativas** | **Horas** |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 12 |
| **Periodo temporal:** Semana 11 | |
| **Actividad global** | |
| **Actividades formativas** | **Suma horas** |
| Prácticas de laboratorio [PRESENCIAL][Aprendizaje orientado a proyectos] | 20 |
| Tutorías individuales [PRESENCIAL][] | 7.5 |
| Otra actividad no presencial [AUTÓNOMA][Aprendizaje basado en problemas (ABP)] | 37.5 |
| Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo] | 45 |
| Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos] | 40 |
| **Total horas:** | 150 |

## 10. BIBLIOGRAFÍA, RECURSOS

| Autor/es | Título/Enlace Web | Editorial | Población | ISBN | Año | Descripción |
|---|---|---|---|---|---|---|
| | 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 |
| | | | | | | 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 |

| | | | | | |
|---|---|---|---|---|---|
| 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 | 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 | | | | |
| 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 |