UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura: SEGURIDAD DE SISTEMAS SOFTWARE
Código: 42333
Tipología: OPTATIVA
Créditos ECTS: 6
Grado: 406 - GRADO EN INGENIERÍA INFORMÁTICA (AB)_20
Curso académico: 2021-22
Centro: 604 - E.S. DE INGENIERÍA INFORMÁTICA ALBACETE
Grupo(s): 14
Curso: 4
Duración: Primer cuatrimestre
Lengua principal de impartición: Español
Segunda lengua: Inglés
Uso docente de otras lenguas:
English Friendly: N
Página web: http://campusvirtual.uclm.es
Bilingüe: N

Profesor: **FERNANDO CUARTERO GOMEZ** - Grupo(s): **14**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
1.A.10	SISTEMAS INFORMÁTICOS	2478	fernando.cuartero@uclm.es	Lunes, 10-12 Miercoles, 10-12 Jueves, 10-12

2. REQUISITOS PREVIOS

Esta asignatura se apoya en las competencias y contenidos adquiridos en las asignaturas del módulo de Formación Básica y del módulo Común a la Rama Informática.

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

La conectividad, extensibilidad y complejidad del software actual, así como la responsabilidad social del mismo, reflejan la necesidad de los contenidos que se imparten en esta asignatura.

Tiene relación con las siguientes asignaturas:

Auditoria de sistemas de información

Fundamentos de programación I y II

Ingeniería del Software

Procesos de Ingeniería del Software

Administración de Bases de Datos

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

Competencias propias de la asignatura

Código	Descripción
INS01	Capacidad de análisis, síntesis y evaluación.
INS02	Capacidad de organización y planificación.
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.
IS05	Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
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.
SIS03	Aprendizaje autónomo.
SIS04	Adaptación a nuevas situaciones.
SIS05	Creatividad.
SIS06	Capacidad de liderazgo.
SIS08	Capacidad de iniciativa y espíritu emprendedor.
SIS09	Tener motivación por la calidad.

5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

Resultados de aprendizaje propios de la asignatura

Descripción

Conocer las normas, estándares y legislación más relevante sobre seguridad del software.

Identificar, modelar e integrar los requisitos de seguridad del software en el proceso de su desarrollo.

Conocer las principales técnicas y criterios para analizar, diseñar y estructurar software.

6. TEMARIO

Tema 1: Introducción a la seguridad de sistemas software

- **Tema 1.1** Definiciones y conceptos. Fundamentos de seguridad
- **Tema 1.2** Evolución histórica.
- **Tema 1.3** Seguridad a distintos niveles. Riesgos, gestión, normas.
- **Tema 1.4** Principios de diseño y desarrollo de software seguro. Seguridad organizativa.

Tema 2: Seguridad en los sistemas de información.

- **Tema 2.1** Introducción
- **Tema 2.2** Definiciones y conceptos
- **Tema 2.3** Sistemas de cifrado
- **Tema 2.4** Aplicaciones de cifrado en el diseño de software seguro

Tema 3: Técnicas de hacking

- **Tema 3.1** Desbordamiento. Buffer, enteros.
- **Tema 3.2** Inyección SQL
- **Tema 3.3** X scripting
- **Tema 3.4** Otras

Tema 4: Seguridad en desarrollo de software

- **Tema 4.1** Introducción
- **Tema 4.2** Requisitos, Riesgos y servicios. Gestión de seguridad
- **Tema 4.3** Desarrollo seguro: Metodología Cigital Touchpoints
- **Tema 4.4** Desarrollo seguro: Metodología Microsoft SDL
- **Tema 4.5** Desarrollo seguro: Metodología OpenSAMM

Tema 5: Certificación, normas y estándares para la seguridad

COMENTARIOS ADICIONALES SOBRE EL TEMARIO

En las sesiones de laboratorio, se tiene previsto conocer varias herramientas de análisis y captura de requisitos de seguridad, análsis de amenazas, de gestión de riesgos y se plantearán varios casos de estudio sobre los que trabajar con las herramientas

7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas	ECTS	Horas	Ev	Ob	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Método expositivo/Lección magistral	INS01 INS03 INS05 SIS04	0.84	21	S	N	Clases teóricas del temario.
Estudio o preparación de pruebas [AUTÓNOMA]	Autoaprendizaje	INS03 INS04 IS05 PER01 SIS03 SIS04	1.6	40	S	S	Estudio de los temas de teoría.
Elaboración de informes o trabajos [AUTÓNOMA]	Trabajo en grupo	INS03 INS04 IS05 PER01 PER02 PER04 PER05 SIS01	1.12	28	S	S	Trabajo teórico de la asignatura
Presentación de trabajos o temas [PRESENCIAL]	Pruebas de evaluación	INS03 PER01 PER02 SIS04 SIS05	0.32	8	S	N	Presentación de los trabajos realizados y debate
Prácticas en aulas de ordenadores [PRESENCIAL]	Prácticas	INS03 INS04 IS05 PER01 SIS04	1	25	S	N	Prácticas de laboratorio
Elaboración de memorias de Prácticas [AUTÓNOMA]	Trabajo en grupo	INS03 PER01 SIS04	0.88	22	S	S	Trabajo práctico de la asignatura.
Prueba final [PRESENCIAL]	Pruebas de evaluación	INS03 INS04 IS05 SIS04	0.16	4	S	S	Prueba final.
Tutorías individuales [PRESENCIAL]	Otra metodología	INS02 INS03 IS05 PER04 SIS04	0.08	2	S	N	Tutorías para resolver dudas.
		Total:	**6**	**150**			
Créditos totales de trabajo presencial: 2.4							**Horas totales de trabajo presencial: 60**
Créditos totales de trabajo autónomo: 3.6							**Horas totales de trabajo autónomo: 90**

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
Prueba final	0.00%	50.00%	Recuperación de los contenidos no superados en la evaluación contínua.
Prueba	50.00%	50.00%	Se realizarán exámenes parciales, y en caso necesario, un a prueba final de la asignatura. (ESC)
Elaboración de trabajos teóricos	20.00%	0.00%	Trabajos relacionados con la temática de la asignatura. (INF)
Actividades de autoevaluación y coevaluación	20.00%	0.00%	Realización de prácticas de laboratorio, incluida la memoria de prácticas. (LAB)
Presentación oral de temas	10.00%	0.00%	Exposición oral de trabajos individuales o de grupo. (PRES)
Total:	**100.00%**	**100.00%**	

** En **Evaluación no continua** se deben definir los porcentajes de evaluación según lo dispuesto en el art. 6 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. 13.2) 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:

Prueba escrita, con un peso del 50%.
Trabajos prácticos, bien individuales o en equipo: 20%.
Será requisito obligado la entrega de los trabajos de prácticas, con un peso del 20%.
se realizarán exposiciones orales de temas, incluidos los trabajos y memoria de prácticas.
Todas las actividades de evaluación podrán hacerse en modalidad no presencial.

Evaluación no continua:

Consistirá en una prueba evaluable que englobe, tanto la prueba escrita de la evaluación contínua, como los contenidos realizados en las prácticas y los trabajos desarrollados.

Particularidades de la convocatoria extraordinaria:

Prueba escrita para valoración de conocimientos teóricos y prácticos.
Será requisito obligado la entrega de los trabajos de prácticas.

Particularidades de la convocatoria especial de finalización:

Prueba escrita para valoración de conocimientos teóricos y prácticos.
Será requisito obligado la entrega de los trabajos de prácticas.

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

No asignables a temas

Horas	**Suma horas**
Presentación de trabajos o temas [PRESENCIAL][Pruebas de evaluación]	8
Prueba final [PRESENCIAL][Pruebas de evaluación]	4
Tutorías individuales [PRESENCIAL][Otra metodología]	2

Comentarios generales sobre la planificación: La asignatura se imparte en tres sesiones semanales de 1,5 horas.

Tema 1 (de 5): Introducción a la seguridad de sistemas software

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	6
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	7
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	7

Periodo temporal: 3 semanas

Grupo 14:

Inicio del tema: 06-09-2021 **Fin del tema:**

Tema 2 (de 5): Seguridad en los sistemas de información.

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	6
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	11
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	9
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	7
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo en grupo]	8

Periodo temporal: 4 semanas

Grupo 14:

Inicio del tema: 04-10-2021 **Fin del tema:**

Tema 3 (de 5): Técnicas de hacking

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	7
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	13
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	8
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	8
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo en grupo]	9

Periodo temporal: 2 semanas

Grupo 14:

Inicio del tema: 25-10-2021 **Fin del tema:**

Tema 4 (de 5): Seguridad en desarrollo de software

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	1
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	7
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	9
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	2
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo en grupo]	4

Periodo temporal: 4 semanas

Grupo 14:

Inicio del tema: 08-11-2021 **Fin del tema:**

Tema 5 (de 5): Certificación, normas y estándares para la seguridad

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	1
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	2
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	2
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	1
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo en grupo]	1

Periodo temporal: 1 semana

Grupo 14:

Inicio del tema: 13-12-2021 **Fin del tema:** 20-12-2021

Actividad global

Actividades formativas	Suma horas
Estudio o preparación de pruebas [AUTÓNOMA][Autoaprendizaje]	40
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	28
Presentación de trabajos o temas [PRESENCIAL][Pruebas de evaluación]	8
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	25
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo en grupo]	22
Prueba final [PRESENCIAL][Pruebas de evaluación]	4
Tutorías individuales [PRESENCIAL][Otra metodología]	2
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	21
Total horas:	150

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título/Enlace Web	Editorial	Población	ISBN	Año	Descripción
Comité ISO	ISO/IEC 27001 http://www.iso27000.es/					Norma ISO 27001. Estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements)
Gary McGraw	Software Security. Building Security In	Addison-Wesley		978-0321356703	2006	
Jorge Ramió Aguirre	Libro electrónico de Seguridad Informática y Criptología http://www.criptored.upm.es/guiateoria/gt_m001a.htm				2006	
Manuel José Lucena López	Criptografía y Seguridad en Computadores http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto				2010	
Microsoft	Microsoft SDL http://www.microsoft.com/security/sdl/default.aspx					Metodología de desarrollo de software SDL
Neil Daswani, Christoph Kern y Anita Kesavan	Foundations of security. What every programmer needs to know	Apress			2007	
Open SAMM	Open SAMM http://www.opensamm.org/					Metodología de desarrollo de software seguro Open SAMM
Viega, John	Building secure software : how to avoid security problems	Addison-Wesley		0-201-72152-X	2002	