

1. DATOS GENERALES

Asignatura: SEGURIDAD DE SISTEMAS SOFTWARE		Código: 42333	
Tipología: OBLIGATORIA		Créditos ECTS: 6	
Grado: 346 - GRADO EN INGENIERÍA INFORMÁTICA (AB)		Curso académico: 2018-19	
Centro: 604 - ESCUELA SUPERIOR DE INGENIERIA INFORMÁTICA (AB)		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
1.A.10	SISTEMAS INFORMÁTICOS	2478	fernando.cuartero@uclm.es
		Horario de tutoría	
		Martes y miércoles de 10:00 a 12:00 Lunes, de 18:00 a 20:00	

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:

- Auditoría 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
INS1	Capacidad de análisis, síntesis y evaluación.
INS2	Capacidad de organización y planificación.
INS3	Capacidad de gestión de la información.
INS4	Capacidad de resolución de problemas aplicando técnicas de ingeniería.
INS5	Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.
IS5	Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
PER1	Capacidad de trabajo en equipo.
PER2	Capacidad de trabajo en equipo interdisciplinar.
PER4	Capacidad de relación interpersonal.
PER5	Reconocimiento a la diversidad, la igualdad y la multiculturalidad.
SIS1	Razonamiento crítico.
SIS3	Aprendizaje autónomo.
SIS4	Adaptación a nuevas situaciones.
SIS5	Creatividad.
SIS6	Capacidad de liderazgo.
SIS8	Capacidad de iniciativa y espíritu emprendedor.
SIS9	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.	
Conocer las principales técnicas y servicios de seguridad del software.	
Identificar, modelar e integrar los requisitos de seguridad del software en el proceso de su desarrollo.	
Resultados adicionales	
No se han establecido.	

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:** Seguridad en desarrollo de software
 - Tema 3.1:** Introducción
 - Tema 3.2:** Requisitos, Riesgos y servicios. Gestión de seguridad
 - Tema 3.3:** Desarrollo seguro: Metodología Cigital Touchpoints
 - Tema 3.4:** Desarrollo seguro: Metodología Microsoft SDL
 - Tema 3.5:** Desarrollo seguro: Metodología OpenSAMM
- Tema 4:** Técnicas de hacking
- 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, análisis 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	Rec	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Método expositivo/Lección magistral	SIS4 IS1 IS5 INS3	0.84	21	S	N	N	Clases teóricas del temario.
Estudio o preparación de pruebas [AUTÓNOMA]	Autoaprendizaje	SIS4 INS4 IS1 IS5 INS3 PER1	1.6	40	S	S	S	Estudio de los temas de teoría.
Elaboración de informes o trabajos [AUTÓNOMA]	Trabajo en grupo	SIS4 INS4 IS1 IS5 INS3 PER1	1.12	28	S	S	S	Trabajo teórico de la asignatura
Presentación de los trabajos realizados v								

Presentación de trabajos o temas [PRESENCIAL]	Pruebas de evaluación	SIS4 INS3 PER1	0.32	8	S	N	S	debate
Prácticas en aulas de ordenadores [PRESENCIAL]	Prácticas	SIS4 INS4 IS1 IS5 INS3 PER1	1	25	S	N	N	Prácticas de laboratorio
Elaboración de memorias de Prácticas [AUTÓNOMA]	Trabajo en grupo	SIS4 INS3 PER1	0.88	22	S	S	S	Trabajo práctico de la asignatura.
Prueba final [PRESENCIAL]	Pruebas de evaluación	SIS4 INS4 IS1 IS5 INS3 PER1	0.16	4	S	S	S	Prueba final.
Tutorías individuales [PRESENCIAL]	Otra metodología	SIS4 INS4 IS1 IS5 INS3 PER1	0.08	2	S	N	S	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
 Rec: Actividad formativa recuperable

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

Sistema de evaluación	Valoraciones		Descripción
	Estudiante presencial	Estud. semipres.	
Prueba	50.00%	0.00%	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%	0.00%	

Criterios de evaluación de la convocatoria ordinaria:

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.

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

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
Período temporal: 3 semanas	
Grupo 14:	
Inicio del tema: 12-09-2018	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
Período temporal: 4 semanas	

Tema 3 (de 5): Seguridad en desarrollo de software

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
Período temporal: 4 semanas	

Tema 4 (de 5): Técnicas de hacking

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
Período temporal: 2 semanas	

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
Período temporal: 1 semana	
Grupo 14:	
Inicio del tema:	Fin del tema: 20-12-2018

Actividad global

Actividades formativas	Suma horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	21
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
Total horas: 150	

Comentarios generales sobre la planificación:

La asignatura se imparte en tres sesiones semanales de 1,5 horas.

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título	Libro/Revista Población Editorial ISBN	Año	Descripción	Enlace Web	Catálogo biblioteca
Comité ISO	ISO/IEC 27001			Norma ISO 27001. Estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements)	http://www.iso27000.es/	
Gary McGraw	Software Security. Building Security In	Addison- Wesley	978-0321356703	2006		
	Libro electrónico de Seguridad					

Jorge Hamo Aguirre	Informática y Criptología		2006	http://www.criptored.upm.es/guateoria/gt_mu01a.htm
Manuel José Lucena López	Criptografía y Seguridad en Computadores		2010	http://www.di.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto
Microsoft	Microsoft SDL			http://www.microsoft.com/security/sdl/default.aspx
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/
Viega, John	Building secure software : how to avoid security problems	Addison-Wesley	0-201-72152-X 2002	

