



# UNIVERSIDAD DE CASTILLA - LA MANCHA

## GUÍA DOCENTE

### 1. DATOS GENERALES

**Asignatura:** SEGURIDAD EN SISTEMAS INFORMÁTICOS

**Tipología:** OBLIGATORIA

**Grado:** 346 - GRADO EN INGENIERÍA INFORMÁTICA (AB)

**Centro:** 604 - ESCUELA SUPERIOR DE INGENIERIA INFORMATICA (AB)

**Curso:** 4

**Lengua principal de impartición:** Español

**Uso docente de otras lenguas:** Inglés para alumnos extranjeros

**Página web:** <https://esiiab.uclm.es/asig.php?codasig=42357&curso=2018-19>

**Código:** 42357

**Créditos ECTS:** 6

**Curso académico:** 2018-19

**Grupo(s):** 13

**Duración:** Primer cuatrimestre

**Segunda lengua:** Inglés

**English Friendly:** S

**Bilingüe:** N

Profesor: JOSE LUIS MARTINEZ MARTINEZ - Grupo(s): 13				
Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
ESII-1.C.11	SISTEMAS INFORMÁTICOS	2294	joseluis.martinez@uclm.es	
Profesor: JOSE MIGUEL VILLALON MILLAN - Grupo(s): 13				
Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
ESII-1.C.5	SISTEMAS INFORMÁTICOS	2384	josemiguel.villalon@uclm.es	

### 2. REQUISITOS PREVIOS

Asignatura obligatoria para la Materia de Tecnología Específica de Tecnologías de la Información, es aconsejable haber cursado los módulos de Formación Básica y el módulo Común a la Rama de Informática (Módulos I y II). Se recomienda por tanto tener claros los conceptos básicos de redes de interconexión y configuración de dispositivos en red (Redes I y Redes II), y conceptos de programación y sistemas operativos.

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

Esta asignatura se integra en la materia de Tecnologías y Sistemas de Información del plan de estudios.

La seguridad informática es una competencia común a todos los planes de Ingeniería Informática, recogida en el Libro Blanco y en todas las recomendaciones curriculares de IEEE/ACM.

La seguridad es una competencia específica, pero afecta a todas las materias del plan de estudios. El principio del eslabón más débil establece que un sistema informático es tan seguro como su punto más vulnerable. Esto se traduce necesariamente en un asignatura multidisciplinar, donde se consideran aspectos de muy bajo nivel y aspectos de muy alto nivel. El Ingeniero Informático debe ser consciente de la pluralidad de problemas que afectan a la seguridad, para poder tomar las decisiones adecuadas de diseño, operación o mantenimiento.

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

#### Competencias propias de la asignatura

Código	Descripción
INS2	Capacidad de organización y planificación.
INS5	Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.
PER2	Capacidad de trabajo en equipo interdisciplinar.
SIS1	Razonamiento crítico.
SIS3	Aprendizaje autónomo.
SIS4	Adaptación a nuevas situaciones.
SIS5	Creatividad.
TI7	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

### 5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

#### Resultados de aprendizaje propios de la asignatura

Descripción

Configurar redes seguras empleando firewalls y redes privadas virtuales.

Conocer las últimas técnicas en seguridad en las transacciones, así como la legislación vigente en cuanto a protección de datos.

Diseñar planes de seguridad y contingencia en Centros de Procesos de Datos (CPD's).

Gestionar la seguridad en sistemas informáticos.

Identificar vulnerabilidades del sistema informático, analizar y clasificar ataques.

Utilizar técnicas de codificación y criptografía para proteger la información.

### 6. TEMARIO

#### Tema 1: Introducción

**Tema 1.1** Presentación de la Asignatura

**Tema 1.2** Introducción a la Seguridad Informática y de la Información

#### Tema 2: Hacking Ético

**Tema 2.1** Footprinting & Open Source Intelligence

Tema 2.2 Fingerprinting & Enumeration

Tema 2.3 Ataques de Acceso

Tema 2.4 Congreso NavajaNegra

Tema 2.5 Ataques a Redes de Datos e Ingeniería Social

Tema 2.6 Explotación de Vulnerabilidades

### Tema 3: Auditoría Web

Tema 3.1 OWASP y Proxy Web

Tema 3.2 XSS

Tema 3.3 CSRF+LFI+RFI+CLI

Tema 3.4 SQLi

Tema 3.5 Blind SQLi y automatización

### Tema 4: Fortificación

Tema 4.1 Securitización del router y servicios

Tema 4.2 AAA

Tema 4.3 Cortafuegos Avanzados

Tema 4.4 IPTables y Snort

## 7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas	ECTS	Horas	Ev	Ob	Rec	Descripción	
Enseñanza presencial (Teoría) [PRESENCIAL]	Combinación de métodos	TI7	0.96	24	S	N	S		
Enseñanza presencial (Prácticas) [PRESENCIAL]	Prácticas	TI7	1.2	30	S	N	S	Desarrollo de las prácticas de laboratorio	
Presentación de trabajos o temas [PRESENCIAL]	Trabajo en grupo	INS2 INS5 PER2 SIS1 SIS3 SIS4 SIS5	0.12	3	S	N	N	Exposición en clase de un trabajo relacionado con la asignatura	
Prueba final [PRESENCIAL]	Pruebas de evaluación	INS5 SIS1	0.2	5	S	S	S	Examen final teórico y práctico	
Elaboración de informes o trabajos [AUTÓNOMA]	Trabajo en grupo	INS2 INS5 PER2 SIS1 SIS3 SIS4 SIS5	0.8	20	S	N	S	Trabajo autónomo para el desarrollo del trabajo de la asignatura	
Estudio o preparación de pruebas [AUTÓNOMA]	Trabajo autónomo	INS2 INS5 PER2 SIS1 SIS3 SIS4 SIS5 TI7	2.56	64	S	N	S	Estudio y preparación de las diferentes pruebas tanto online como presenciales (examen final)	
Pruebas on-line [AUTÓNOMA]	Pruebas de evaluación	INS2 SIS4	0.16	4	S	N	S	Realización de test de cada tema y práctica	
<b>Total:</b>			<b>6</b>	<b>150</b>					
<b>Créditos totales de trabajo presencial: 2.48</b>								<b>Horas totales de trabajo presencial: 62</b>	
<b>Créditos totales de trabajo autónomo: 3.52</b>								<b>Horas totales de trabajo autónomo: 88</b>	

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.	
Trabajo	10.00%	0.00%	Elaboración de un trabajo y su exposición pública sobre un tema propuesto por el profesor. Corresponde, "PRES" de la memoria de grado.
Pruebas de progreso	20.00%	0.00%	Se realizarán tests vía moodle para realizar una evaluación continua del contenido teórico de la asignatura. Corresponde con la categoría "ESC" de la memoria de grado.
Pruebas de progreso	20.00%	0.00%	Se realizarán tests vía moodle como evaluación continua de las prácticas de laboratorio. Corresponde con la categoría "INF" de la memoria de grado.
Prueba final	25.00%	0.00%	Prueba final correspondiente a la parte de teoría. Corresponde con la categoría "ESC" de la memoria de grado.
Prueba final	25.00%	0.00%	Prueba final práctica en el laboratorio que corresponde con la categoría "LAB" de la memoria de grado.
<b>Total:</b>	<b>100.00%</b>	<b>0.00%</b>	

### Criterios de evaluación de la convocatoria ordinaria:

[MODALIDAD CON EVALUACIÓN CONTÍNUA]

-Teoría:

- Examen Final Teórico: 25% (Nota mínima: 4 puntos. Compensable con los test de la evaluación continua)

-Prácticas:

- Examen de Final Práctico de Laboratorio: 25% (Nota mínima: 4 puntos. Compensable con los test de la evaluación continua)

-Evaluación Continua:

Test Evaluables: 40% Se realizarán test de 10 preguntas V/F al final de cada sub-tema.

- Trabajo:

- Trabajo práctico defendido en clase: 10%

[MODALIDAD SIN EVALUACIÓN CONTÍNUA]

- Teoría:
- Examen Final: 50% (Nota mínima: 4 puntos. Compensable con la parte de prácticas)
- Prácticas:
- Examen Final de Prácticas: 50% (Nota mínima: 4 puntos. Compensable con la parte de teoría)

En ambas modalidades se guarda cada parte para la convocatoria extraordinaria si se supera el 5

El alumno que no supere todas las pruebas mínimas exigidas (nota mínima de 4 tanto en el examen de teoría Y prácticas) en la asignatura aparecerá como suspenso y tendrá una nota final correspondiente a la nota media entre el examen de teoría y prácticas. En caso de que la media de aprobado, tendrá una nota de suspenso, 4.

**Particularidades de la convocatoria extraordinaria:**

En la convocatoria extraordinaria solo se podrá recuperar el examen final de teoría y el caso práctico en el laboratorio, las notas de los test y de los trabajos se mantienen de la ordinaria. Si el alumno lo desea, puede presentarse según el formato CON O SIN MODALIDAD EVALUACIÓN CONTÍNUA, es decir, con o sin tener en cuenta los resultados de la evaluación continua

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

Igual que la extraordinaria

9. SECUENCIA DE TRABAJO, CALENDARIO, HITOS IMPORTANTES E INVERSIÓN TEMPORAL	
<b>No asignables a temas</b>	
<b>Horas</b>	<b>Suma horas</b>
Presentación de trabajos o temas [PRESENCIAL][Trabajo en grupo]	3
Prueba final [PRESENCIAL][Pruebas de evaluación]	5
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	20
Pruebas on-line [AUTÓNOMA][Pruebas de evaluación]	4
<p><b>Comentarios generales sobre la planificación:</b> Esta planificación es ORIENTATIVA, pudiendo variar a lo largo del periodo lectivo en función de las necesidades docentes, festividades, o por cualquier otra causa imprevista. La planificación semanal de la asignatura podrá encontrarse de forma detallada y actualizada en la plataforma Campus Virtual (Moodle). Las actividades de evaluación o recuperación de clases podrían planificarse, excepcionalmente, en horario de tarde La asignatura se imparte en tres sesiones semanales de 1,5 horas.</p>	
<b>Tema 1 (de 4): Introducción</b>	
<b>Actividades formativas</b>	<b>Horas</b>
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	4
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	2
<b>Tema 2 (de 4): Hacking Ético</b>	
<b>Actividades formativas</b>	<b>Horas</b>
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	6
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	10
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	24
<b>Tema 3 (de 4): Auditoría Web</b>	
<b>Actividades formativas</b>	<b>Horas</b>
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	8
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	12
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	24
<b>Tema 4 (de 4): Fortificación</b>	
<b>Actividades formativas</b>	<b>Horas</b>
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	6
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	8
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	14
<b>Actividad global</b>	
<b>Actividades formativas</b>	<b>Suma horas</b>
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	24
Enseñanza presencial (Prácticas) [PRESENCIAL][Prácticas]	30
Presentación de trabajos o temas [PRESENCIAL][Trabajo en grupo]	3
Prueba final [PRESENCIAL][Pruebas de evaluación]	5
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo en grupo]	20
Estudio o preparación de pruebas [AUTÓNOMA][Trabajo autónomo]	64
Pruebas on-line [AUTÓNOMA][Pruebas de evaluación]	4
<b>Total horas: 150</b>	

10. BIBLIOGRAFÍA, RECURSOS					
Autor/es	Título/Enlace Web	Editorial	Población ISBN	Año	Descripción
Catherine Paquet	Implementing Cisco IOS Network Security	Cisco Press		2009	
Fundamentos de Seguridad en Redes	Fundamentos de Seguridad en Redes	Cisco Press		2008	
Kurose, J., Ross, K.	Redes de Computadores. Un enfoque descendente basado en Internet	Pearson Education		2003	
Michael Walkings, Kevin Wallace	CCNA Security Official Exam Certification Guide	Cisco Press		2008	
William Stallings	Computer security. Principles and	Pearson International		2008	

William Stallings	Practice Fundamentos de seguridad en redes	Edition Pearson Prentice Hall	2003
varios	Colección Pack Completa  <a href="http://Oxword.com/es/">http://Oxword.com/es/</a> Estándares de la serie ISO/IEC <a href="http://www.aenor.es">www.aenor.es</a> , <a href="http://www.iso.org">www.iso.org</a> y <a href="http://www.iso27000.es">www.iso27000.es</a>	Oxword	Colección de varios ejemplares