Facultad de Ciencias

GUÍA DOCENTE DE LA ASIGNATURA

G678 - Garantía y Seguridad en Sistemas y Redes

Grado en Ingeniería Informática
Optativa. Curso 4

Curso Académico 2015-2016

1. DATOS IDENTIFICATIVOS

Título/s	Grado en Ingeniería Informática	Tipología y Curso	Optativa. Curso 4
Centro	Facultad de Ciencias		
Módulo / materia	MATERIA INGENIERÍA DE COMPUTADORES MENCION EN INGENIERIA DE COMPUTADORES MENCIÓN EN INGENIERÍA DE COMPUTADORES		
Código y denominación	G678 - Garantía y Seguridad en Sistemas y Redes		
Créditos ECTS	6	Cuatrimestre	Cuatrimestral (1)
Web			
Idioma de impartición	Español	Forma de impartición	Presencial

Departamento	DPTO. INGENIERÍA INFORMÁTICA Y ELECTRÓNICA
Profesor responsable	ENRIQUE VALLEJO GUTIERREZ
E-mail	enrique.vallejo@unican.es
Número despacho	Facultad de Ciencias. Planta: + 1. DESPACHO PROFESORES (1108)
Otros profesores	ESTEBAN STAFFORD FERNANDEZ

2. CONOCIMIENTOS PREVIOS

Es imprescindible haber cursado y aprobado las siguientes asignaturas:
- Sistemas Operativos
- Sistemas Informáticos
- Introducción a las Redes de Computadores
- Redes de Computadores y Sistemas Distribuidos

Otras conocimientos importantes.
- Programación en ensamblador
- Programación en lenguaje C
- Programación en PHP
- Servidores Web y protocolo HTTP

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS	
Competencias Genéricas	Nivel
(Comunicación) Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.	3
Capacidad de organización y planificación.	1
Capacidad de resolución de problemas aplicando técnicas de ingeniería.	1
Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.	2
Capacidad de trabajo en equipo.	1
Razonamiento crítico.	1
Aprendizaje autónomo.	2
Adaptación a nuevas situaciones.	1
Tener motivación por la calidad.	3
Poseer una capacidad demostrada para la comunicación oral y escrita así como para hacer presentaciones efectivas en público.	1
Capacidad de comprensión auditiva, lectura, interacción y expresión oral y escrita en Inglés	1
Competencias Específicas	Nivel
Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.	2
Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.	2
Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.	2
Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.	3

3.1 RESULTADOS DE APRENDIZAJE
- Conocer las técnicas básicas de protección y seguridad de que consta el sistema operativo.
- Conocer los aspectos fundamentales de garantía y seguridad en entornos computacionales distinguiendo las vulnerabilidades y ataques más comunes.
- Conocer los aspectos de seguridad a nivel de sistema y red, así como los mecanismos necesarios para cubrirlos: control de usuarios y accesos, permisos, firewalls, seguridad criptográfica, virus, etc.
- Saber manejar las herramientas adecuadas para configurar una red segura.
- Ser capaces de comunicar de forma efectiva, tanto por escrito como oralmente conocimientos, técnicas, resultados e ideas relacionados con el contenido de la materia estudiada.

4. OBJETIVOS

La sociedad actual depende cada vez más en los sistemas de información. Esta dependencia hace que los efectos de un fallo en estos sistemas pueda desencadenar consecuencias muy graves. Es por ello que un Ingeniero Informático debe conocer la manera de asegurar el funcionamiento de los sistemas a su cargo. Para ello debe cuidar tanto su diseño como su puesta en funcionamiento y explotación.

En el transcurso de la asignatura, el alumno deberá alcanzar los siguientes objetivos:

- Conocer las herramientas criptográficas de uso común en seguridad de computadores. Encriptación simiétrica, asimétrica y funciones de resumen (hash).
- Entender los mecanismos de control de acceso y autenticación. Saber evaluar los riesgos de tales mecanismos y proponer medios paliativos.
- Comprender y saber evaluar los riesgos de seguridad más habituales en sistemas informáticos, tanto a nivel de aplicación, sistema o red.
- Saber aplicar medios que mejoren la seguridad en sistemas y redes informáticos. Seleccionando contramedidas de proteccion, detección, contención y recuperación.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES

ACTIVIDADES	HORAS DE LA ASIGNATURA
ACTIVIDADES PRESENCIALES	
HORAS DE CLASE (A)	
- Teoría (TE)	20
- Prácticas en Aula (PA)	10
- Prácticas de Laboratorio (PL)	30
- Horas Clínicas (CL)	
Subtotal horas de clase	60
ACTIVIDADES DE SEGUIMIENTO (B)	
- Tutorías (TU)	7,5
- Evaluación (EV)	7,5
Subtotal actividades de seguimiento	15
Total actividades presenciales (A+B)	75
ACTIVIDADES NO PRESENCIALES	
Trabajo en grupo (TG)	15
Trabajo autónomo (TA)	60
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
Total actividades no presenciales	75
HORAS TOTALES	150

6. ORGANIZACIÓN DOCENTE

	CONTENIDOS	TE	PA	PL	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	Bloque 1: Conceptos Generales 1.1 Introducción 1.2 Herramientas criptográficas 1.3 Autenticación 1.4 Internet Authentication Applications 1.5 Control de Acceso	5,00	3,00	8,00	0,00	2,00	2,00	4,00	16,00	0,00	0,00	1-5
2	Bloque 2: Seguridad en Software 2.1 Código malintencionado 2.2 Denegación de Servicio 2.3 Desbordamiento de Pila 2.4 Programación segura 2.5 Protección de Sistema Operativo 2.6 Estrategias de protección multinivel 2.7 Seguridad en Bases de Datos	8,00	4,00	12,00	0,00	3,00	3,00	6,00	24,00	0,00	0,00	5-11
3	Bloque 3: Seguridad en Red 3.1 Protocolos de Seguridad en Internet 3.2 Detección de Intrusión 3.3 Prevención de intrusion y cortafuegos 3.4 Auditoría de Seguridad 3.5 Seguridad en redes inalámbricas	7,00	3,00	10,00	0,00	2,50	2,50	5,00	20,00	0,00	0,00	11-15
TOTAL DE HORAS		20,00	10,00	30,00	0,00	7,50	7,50	15,00	60,00	0,00	0,00	

Esta organización tiene carácter orientativo.

TE	Horas de teoría
PA	Horas de prácticas en aula
PL	Horas de prácticas de laboratorio
CL	Horas Clínicas
TU	Horas de tutoría
EV	Horas de evaluación
TG	Horas de trabajo en grupo
TA	Horas de trabajo autónomo
TU-NP	Tutorías No Presenciales
EV-NP	Evaluación No Presencial

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Test sobre los contenidos teóricos y prácticos de la asignatura	Evaluación en laboratorio	No	Sí	100,00

Calif. mínima	0,00
Duración	7,5 horas
Fecha realización	A lo largo del curso
Condiciones recuperación	Recuperación mediante un examen final en Junio o Septiembre
Observaciones	Se realizarán seis tests, dos tests por cada uno de los tres bloques temáticos. Cada uno de ellos durará entre 60 y 90 minutos. Los alumnos que no aprueben mediante esta evaluación continua deberán recuperar la asignatura en el examen final de Junio o Septiembre

TOTAL 100,00

Observaciones

Observaciones para alumnos a tiempo parcial

Los alumnos matriculados a tiempo parcial realizarán únicamente el examen final con el 100% de la nota.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

Computer Security: Principles and Practice, 2 ED. W. Stallings, L Brown. ED: Pearson Education Limited.

Complementaria

9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO

10. COMPETENCIAS LINGÜÍSTICAS

☑ Comprensión escrita ☐ Comprensión oral
☐ Expresión escrita ☐ Expresión oral
☐ Asignatura íntegramente desarrollada en inglés

Observaciones
En la asignatura se utilizará material, documentación y software en inglés.