Guía docente de la asignatura

Asignatura	Seguridad de Redes y Sistemas		
Materia	Complementos de Computación		
Módulo	Tecnologías Específicas		
Titulación	Grado en Ingeniería Informática		
Plan	545	**Código**	46927
Periodo de impartición	1er cuatrimestre	**Tipo/Carácter**	Optativa
Nivel/Ciclo	Grado	**Curso**	3
Créditos ECTS	6		
Lengua en que se imparte	Español		
Profesor/es responsable/s	Arturo González Escribano, Julian Arroyo Álvarez		
Datos de contacto (E-mail, teléfono…)	arturo@infor.uva.es (983423000 Ext. 5613) julian@infor.uva.es (98342300 Ext, 5639)		
Horario de tutorías	Ver horarios de tutoría oficiales de cada profesor en la página web de la UVa		
Departamento	Infomática (ATC,CCIA,LSI)		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La conectividad y facilidad de intercambio de información actuales implican enormes riesgos para la integridad de la información y su trasmisión o difusión, tanto a nivel personal como a nivel institucional. En esta asignatura se aborda una visión global de la ingeniería de seguridad, junto con conocimientos específicos de herramientas y procedimientos.

1.2 Relación con otras materias

Ver apartado 1.3

1.3 Prerrequisitos

Se requieren conocimientos sobre fundamentos de redes. Aunque se tratan de nuevo desde la perspectiva de los planes de seguridad integral, son aconsejables conocimientos básicos de administración de sistemas, así como de fundamentos de criptografía y herramientas relacionadas.

Instrumentalmente son necesarios conocimientos de programación, y manejo del interfaz de comandos en sistemas UNIX.

2. Competencias

2.1 Generales

G3. Capacidad de análisis y síntesis
G4. Capacidad de organizar y planificar
G5. Comunicación oral y escrita en la lengua propia
G9. Resolución de problemas
G10. Toma de decisiones
G11. Capacidad crítica y autocrítica
G14. Responsabilidad y compromiso ético
G16. Capacidad de aplicar los conocimientos en la práctica
G17. Habilidades de investigación
G18. Capacidad de aprender
G19. Capacidad de adaptarse a nuevas situaciones
G20. Capacidad de generar nuevas ideas
G21. Habilidad para trabajar de forma autónoma

2.2 Específicas

IC6: Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos

3. Objetivos

- Conocer los principios metodológicos básicos de la ingeniería de la seguridad y saber aplicarlos a la elaboración de una estrategia de seguridad y protección de información en las organizaciones.
- Identificar los protocolos utilizados para garantizar la seguridad en las comunicaciones en Internet, y elegir el protocolo adecuado para cada caso concreto.
- Saber aplicar sistemas de protección de información basados en criptografía de clave pública y privada en entornos prácticos y realistas.
- Analizar los niveles de seguridad y los posibles ataques de sistemas informáticos en estudios de caso realistas.

4. Bloques temáticos

Bloque 1: Seguridad de Redes y Sistemas

Bloque único

Carga de trabajo en créditos ECTS: 6

a. Contextualización y justificación

Ver apartado 1.1

b. Objetivos de aprendizaje

Ver apartado 3

c. Contenidos

Tema 1. Introducción y fundamentos de ingeniería de seguridad

Tema 2. Técnicas criptográficas en seguridad

Tema 3. Ataques, auditoría y protección

Tema 4. Configuración y explotación de cortafuegos

Tema 5. Seguridad perimetral

d. Métodos docentes

Las actividades presenciales se realizarán por todo el grupo de forma conjunta cuando el espacio en el aula permita cumplir las normas de distanciamiento y seguridad. En caso contrario se utilizará modalidad semipresencial, con un grupo en el aula y otro asistiendo de forma telemática con rotación de los grupos cada semana.

Actividades presenciales

- Aula: Clases magistrales, participativas y expositivas. Aprendizaje basado en problemas.

- Laboratorio: Resolución de problemas y casos prácticos. Aprendizaje basado en problemas. Aprendizaje cooperativo. Estudios de casos. Método de proyectos.
- Seminario: Presentaciones, debate y estudio de casos.

Actividades no presenciales

- Estudio personal, preparación de sesiones y temas de debate.
- Trabajo práctico personal y grupal de explotación de herramientas, montaje y configuración de sistemas.

Herramientas docentes

- Plataforma de e-learning Moodle (Campus virtual de la Uva).
- Herramientas de gestión de máquinas virtuales.

e. Plan de trabajo

Se publicará en la plataforma de docencia virtual.

f. Evaluación

La evaluación se realizará de forma continua, en base a entregables: pequeños ejercicios y proyectos. En la convocatoria extraordinaria se realizará un examen final basado en preguntas cortas y/o ejercicios. El contenido del examen cubrirá la parte teórica, práctica y de laboratorio.

g.1 Bibliografía básica

- *Network Security Essentials: Applications and Standards*. William Stallings. 5ªed. Prentice-Hall 2013
- *Firewalls and Internet Security: Repelling the Wily Hacker.* William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin. 2ªed. Addison-Wesley 2003.

g.2 Bibliografía complementaria

- *Seguridad en Unix y Redes*. Antonio Villalón Huerta. Version 2.1. RedIris, Julio 2002. (versión online y PDF disponible en:

http://www.rediris.es/cert/doc/unixsec/).

h. Recursos necesarios

- Laboratorio de ordenadores del Grado.
  Cuenta con un puesto por alumno. Cada ordenador tiene el software y recursos necesarios para la ejecución de los ejercicios y consultas a través de la red.

- Plataforma de docencia virtual Moodle:
  Campus virtual de la UVa (http://campusvirtual.uva.es/)

i. Temporalización

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque único	6	Primer cuatrimestre

5. Métodos docentes y principios metodológicos

Actividad	Metodología
Clase de teoría	1. Clase magistral participativa 2. Estudio de casos en aula 3. Resolución de problemas
Clase práctica	1. Clase magistral participativa 2. Realización de proyectos guiado por el profesor, que encargará y guiará el trabajo que se realizará de forma individual o en grupos (2/3 alumnos).
Seminarios	1. Talleres de aprendizaje
Tutoría	1. Seguimiento y evaluación de los contenidos teóricos y de los proyectos

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	14	Estudio y trabajo autónomo individual	30
Clases prácticas de aula (A)	14	Preparación de trabajo de laboratorio	30
Laboratorios (L)	28	Elaboración de trabajos	30
Prácticas externas, clínicas o de campo			
Seminarios (S)	2		
Tutorías grupales (TG)			
Evaluación	2		
Total presencial	**60**	**Total no presencial**	**90**

7. Sistema y características de la evaluación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Ejercicios, tareas y/o exámenes parciales	100 %	Evaluación continua en convocatoria ordinaria.
Examen final	100 %	Examen de teoría en convocatoria extraordinaria.

CRITERIOS DE CALIFICACIÓN
• **Convocatoria ordinaria:** Se plantearán durante el desarrollo de la asignatura ejercicios, tareas y/o exámenes parciales según el contenido de cada parte. El resultado de la evaluación en la convocatoria ordinaria será la media ponderada de estas notas de evaluación continua. • **Convocatoria extraordinaria:** Los alumnos que no superen la evaluación en la convocatoria ordinaria se podrán presentar en la convocatoria extraordinaria a un examen final que supondrá el 100 % de la nota final

9. Consideraciones finales