Guía docente de la asignatura. Curso 15-16

Asignatura	GARANTÍA Y SEGURIDAD DE LA INFORMACIÓN		
Materia	TECNOLOGÍAS DE LA INFORMACIÓN		
Módulo	TECNOLOGÍAS ESPECÍFICAS		
Titulación	GRADO EN INGENIERÍA INFORMÁTICA		
Plan	545	**Código**	46935
Periodo de impartición	1º CUATRIMESTRE	**Tipo/Carácter**	Obligatoria (Mención TI) Optativa (Mención CO)
Nivel/Ciclo	Grado	**Curso**	3
Créditos ECTS	6		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Carmen Hernández Díez; Joaquín Adiego Rodríguez		
Datos de contacto (E-mail, teléfono…)	Teléfono: 983 423000 ext. 5609 e-mail: chernan@infor.uva.es	Teléfono: 983 423000 ext. 5646 e-mail: jadiego@infor.uva.es	
Horario de tutorías	Véase www.uva.es → Docencia → Grados → Grado en Ingeniería Informática → Tutorías		
Departamento	INFORMATICA (ATC, CCIA, LSI)		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La Ingeniería de la Seguridad se ocupa del desarrollo de sistemas que se mantengan fiables frente a errores, usos maliciosos o mala fortuna. Como disciplina, se centra en el estudio de los métodos, procesos y herramientas necesarios para diseñar, implementar y probar sistemas completos y para adaptar los sistemas existentes a entornos que evolucionan.

En un entorno digital como el que nos movemos, el graduado en Ingeniería Informática, con un perfil profesional orientado a la gestión de las Tecnologías de la Información, debe contar con una formación sólida en los aspectos fundamentales de ingeniería de la seguridad.

La asignatura pretende cubrir tanto los aspectos conceptuales más básicos del ámbito de la seguridad como los aspectos metodológicos relacionados con la garantía y protección de la información. Las técnicas relacionadas con la protección de recursos y las técnicas de identificación segura de usuarios y control de acceso forman parte central de los contenidos de esta asignatura.

1.2 Relación con otras materias

Se recomienda que los alumnos hayan superado las competencias básicas de las asignaturas Fundamentos de Redes y Fundamentos de Computadoras.

1.3 Prerrequisitos

No existen prerrequisitos específicos dentro de la materia.

2. Competencias

Esta asignatura pertenece a la materia Tecnologías de la Información y, por tanto, participa en el desarrollo de las competencias generales y transversales de dicha materia. De acuerdo a la memoria de verificación del título (publicado en https://www.inf.uva.es/grado-en-ingenieria-informatica), estas competencias son las siguientes (ver descripciones de los códigos en dicho documento):

Competencias Generales: G01, G02, G03, G04, G06, G08, G09, G10.

Competencias Transversales: CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT10, CT11, CT12, CT13, CT14, CT15, CT16, CT17.

Competencias Específicas: TI1, TI2, TI3, TI4, TI5, TI6, TI7.

3. Objetivos

Código	Descripción
RA01	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos.
RA02	Analizar las necesidades de garantía de la información en un sistema informático.
RA03	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

4. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	30	Estudio y trabajo autónomo individual	50
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	40
Laboratorios (L)	24		
Prácticas externas, clínicas o de campo			
Seminarios (S)	6		
Tutorías grupales (TG)			
Evaluación (fuera del periodo oficial de exámenes)			
Total presencial	**60**	**Total no presencial**	**90**

5. Bloques temáticos

Bloque 1: Fundamentos de Seguridad de la Información

Carga de trabajo en créditos ECTS: 1,2

a. Contextualización y justificación

En este primer bloque se analizan las diferentes facetas de la ingeniería de la seguridad y se introducen los conceptos y objetivos básicos de la seguridad y de la garantía de la información. Se presentan los doce principios básicos de seguridad introducidos ya hace más de tres décadas por Saltzer y Schroeder en un artículo de referencia en el área.

b. Objetivos de aprendizaje

Código	Descripción
RA01	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos.
RA02	Analizar las necesidades de garantía de la información en un sistema informático.

c. Contenidos

TEMA 1: Visión panorámica

TEMA 2: Conceptos básicos de seguridad de la información

TEMA 3: Principios básicos de seguridad

d. Métodos docentes

Ver Anexo: Métodos docentes

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 7 de esta guía.

g. Bibliografía básica

- Charles P. PFleeger, Security in Computing, 4th. ed., Prentice-Hall, 1997. ISBN 0-13-239077-9.
- Stuart Jacobs, *Engineering Information Security*. IEEE Press, 2011. ISBN 978-0-470-56512-4.

h. Bibliografía complementaria

- Ross Anderson, Security Engineering, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.
- David Basin, Patrick Schaller y Michael Schläpfer, Applied Information Security. Springer, 2011. ISBN 978-3-642-24473-5.
- William Stallings, Network and Internetwork Security. Prentice Hall, 1995. ISBN 0-02-415483-0.

- J.H. Saltzer y M.D. Schroeder, The Protection of Information in Computer Systems. Proceedings of the IEEE, volume 63, pag. 1278-1308, 1975.

i. Recursos necesarios

Libros de texto, presentaciones audiovisuales, material disponible en el aula virtual de la asignatura.

Bloque 2: Protección y Garantía de la Información

Carga de trabajo en créditos ECTS: 3,2

a. Contextualización y justificación

En este bloque, que constituye la parte central de la asignatura, se analizan los diferentes mecanismos de protección frente a problemas de seguridad: la protección de recursos (información) y la protección de acceso (usuarios), que incluye los problemas de autenticación e identificación segura.

La protección de acceso se presenta de forma ascendente por niveles, desde el entorno físico al nivel de aplicación. En cada uno de ellos se analizarán las alternativas que se han ido desarrollando para proporcionar mecanismos de protección que garanticen la fiabilidad de los sistemas y de la información.

La protección de la información no protegida usando técnicas criptográficas se aborda en la segunda parte de este bloque.

b. Objetivos de aprendizaje

Código	Descripción
RA02	Analizar las necesidades de garantía de la información en un sistema informático.
RA03	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios.

c. Contenidos

TEMA 1: Protección de acceso

TEMA 2: Fundamentos de criptografía

TEMA 3: Protección de datos

TEMA 4: Privacidad

TEMA 5: Modelado de seguridad

d. Métodos docentes

Ver Anexo: Métodos docentes

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 7 de esta guía.

g. Bibliografía básica

- Charles P. PFleeger, Security in Computing, 4th. ed., Prentice-Hall, 1997. ISBN 0-13-239077-9.
- Stuart Jacobs, *Engineering Information Security*. IEEE Press, 2011. ISBN 978-0-470-56512-4.

h. Bibliografía complementaria

- Ross Anderson, Security Engineering, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.

- David Basin, Patrick Schaller y Michael Schläpfer, Applied Information Security. Springer, 2011. ISBN 978-3-642-24473-5.
- William Stallings, Network and Internetwork Security. Prentice Hall, 1995. ISBN 0-02-415483-0.

i. Recursos necesarios

Libros de texto, presentaciones audiovisuales, material disponible en el aula virtual de la asignatura.

Bloque 3: Gestión de la seguridad de la información

Carga de trabajo en créditos ECTS: 1,6

a. Contextualización y justificación

La asignatura termina con un bloque íntegramente dedicado a los aspectos metodológicos y de planificación de ingeniería de la seguridad, con especial atención a las normas y estándares que se aplican en este dominio.

Desde un enfoque práctico, se analizarán los aspectos clave relacionados con el diseño de políticas de seguridad y los aspectos metodológicos para asegurar un diseño, despliegue, evaluación y mantenimiento de soluciones de seguridad correctas y conformes con los estándares de mercado.

b. Objetivos de aprendizaje

Código	Descripción
RA01	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos
RA02	Analizar las necesidades de garantía de la información en un sistema informático.
RA03	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

c. Contenidos

TEMA 1: Proceso de ingeniería de la seguridad

TEMA 2: Diseño de políticas de seguridad

TEMA 3: Metodología de trabajo en ingeniería de seguridad

d. Métodos docentes

Ver Anexo: Métodos docentes

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 7 de esta guía.

g. Bibliografía básica

- Stuart Jacobs, Engineering Information Security. IEEE Press, 2011. ISBN 978-0-470-56512-4.
- Ross Anderson, Security Engineering, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.

h. Bibliografía complementaria

- Charles P. PFleeger, Security in Computing, 4th. ed., Prentice-Hall, 1997. ISBN 0-13-239077-9.
- David Basin, Patrick Schaller y Michael Schläpfer, Applied Information Security. Springer, 2011. ISBN 978-3-642-24473-5.

i. Recursos necesarios

Libros de texto, presentaciones audiovisuales, material disponible en el aula virtual de la asignatura.

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Fundamentos de Seguridad de la Información	1,2 ECTS	Semanas 1 a 3
Bloque 2: Protección y Garantía de la Información	3,2 ECTS	Semanas 4 a 11
Bloque 3: Gestión de la seguridad de la Información	1,6 ECTS	Semanas 12 a 15

7. Sistema de calificaciones – Tabla resumen

Entre los instrumentos que se contemplan para valorar la consecución de los resultados de aprendizaje se incluyen los siguientes elementos: Cuestionarios de teoría, entregas de ejercicios prácticos, desarrollo documental de un proyecto práctico de seguridad y la subsiguiente presentación pública del proyecto desarrollado.

Se propondrá una prueba de competencias teóricas (Examen de teoría) como viene siendo habitual que habrá que superar satisfactoriamente para superar la asignatura, si bien su peso en la nota final en la convocatoria ordinaria es del 30%.

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Entrega trabajos del bloque 1	15%	Correspondiente al bloque 1.
Entrega trabajos del bloque 2	15%	Correspondiente al bloque 2.
Entrega trabajos del bloque 3	15%	Correspondiente al bloque 3.
Proyecto práctico de seguridad	25%	Informe del desarrollo del proyecto y defensa oral del mismo.
Examen final escrito	30%	Periodo de exámenes

CRITERIOS DE CALIFICACIÓN

Para superar la asignatura en la convocatoria ordinaria deben cumplirse todas las condiciones siguientes:

- Superar satisfactoriamente la parte práctica, es decir obtener al menos el 50% de la máxima calificación en la parte práctica (entregas ejercicios + proyecto práctico + presentación).
- Superar satisfactoriamente la parte teórica, en concreto obtener al menos el 40% de la máxima calificación.
- Obtener al menos una calificación final de 5,0.

Convocatoria extraordinaria:

- El examen de teoría representará el 100% de la calificación final y constará de dos partes: una teórica, con un peso del 60% y otra práctica con un peso del 40%. La parte práctica podrá compensarse con el aprobado de la parte práctica de la convocatoria ordinaria.
- Obtener al menos una calificación final de 5,0 en el examen de teoría.

8. Anexo: Métodos docentes

Actividad	Metodología
Clase de teoría	• Clase magistral participativa • Estudio de casos en aula • Resolución de problemas
Clase práctica	• Realización de proyectos guiados por la profesora, que encargará y guiará el trabajo que se realizará en grupos (3 alumnos), siguiendo un enfoque colaborativo.
Tutoría	• Evaluación de los contenidos teóricos y de los proyectos.

9. Anexo: Cronograma de actividades previstas

El cronograma detallado se elaborará y difundirá a través de entornos de calendario/agenda que permitirán a todos los alumnos tener constancia de las fechas y horas detalladas de cada actividad, en base al horario de la asignatura y a la planificación general.

En caso de producirse algún cambio, se comunicará adecuadamente a través de las plataformas de soporte para el curso.

Información completa en Campus Virtual de la UVa.