Proyecto/Guía docente de la asignatura Adaptada a la Nueva Normalidad

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**	3º (Mención TI) 4º (Mención CO)
Créditos ECTS	6		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Valentín Cardeñoso Payo Amador Aparicio de la Fuente		
Datos de contacto (E-mail, teléfono…)	Teléfono: 983 18 5601 e-mail: valen@infor.uva.es	Teléfono: 983 42 36 70 e-mail: amador@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

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 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.

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[1] estas competencias son las siguientes (ver descripciones de los códigos en dicho documento):

Competencias Generales: CG1, CG2, CG3, CG4, CG6, CG8, CG9, CG10.

CG1	Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas para este grado, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.
CG2	Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas para el grado.
CG3	Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
CG4	Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas para el grado.
CG6	Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas para el grado.
CG8	Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
CG9	Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.
CG10	Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática, de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas para el grado.

1 https://www.inf.uva.es/grado-en-ingenieria-informatica

Competencias Específicas: TI7, SI2

TI7	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
SI2	Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

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 políticas, modelos y gestores de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

4. Bloques temáticos

Bloque 1: Fundamentos de Seguridad de la Información

Carga de trabajo en créditos ECTS: 0,4

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

PRÁCTICA 1: Configuración de laboratorio virtual de seguridad.

d. Métodos docentes

Ver apartado 6 de esta guía.

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 8 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: 3,6

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.

En la protección de acceso, 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: Estándares de seguridad

TEMA 2: Protección de acceso

TEMA 3: Criptografía

PRÁCTICA 2: Servicios de red y control de acceso remoto

PRÁCTICA 3: Protección criptográfica

PRÁCTICA 4: Certificados y Firma Digital

d. Métodos docentes

Ver apartado 6 de esta guía.

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 8 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: 2

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

PROYECTO: Análisis de Riesgos – Plan de Seguridad

PRÁCTICA 4: Competición SEGURIDAD

d. Métodos docentes

Ver apartado 6 de esta guía

e. Plan de trabajo

Ver Anexo: Cronograma de Actividades Previstas.

f. Evaluación

Ver apartado 8 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.

5. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Fundamentos de Seguridad de la Información	0,4 ECTS	Semanas 1
Bloque 2: Protección y Garantía de la Información	3,6 ECTS	Semanas 2 a 10
Bloque 3: Gestión de la seguridad de la Información	2 ECTS	Semanas 11 a 15

6. Métodos docentes y principios metodológicos

Se utilizarán los siguientes métodos docentes:

- **Clase teórica** para la exposición de los contenidos y el planteamiento de los aspectos clave sobre los que deberán trabajar los alumnos. Para conseguir esta participación, se encargará a los alumnos tareas individuales o grupales, que tienen el fin de ayudar a preparar las sesiones teóricas.
- **Estudios de caso** en los que se revisarán diversos ejemplos de relativos al tema que se esté trabajando, que serán analizados y desarrollados por los estudiantes.
- **Prácticas de laboratorio** realizadas en parejas o en grupo, supervisadas en el laboratorio por el profesor correspondiente, según las indicaciones que se darán en los enunciados de cada práctica.

7. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	30	Estudio y trabajo autónomo individual	60
Laboratorios (L)	24	Estudio y trabajo autónomo grupal	30
Evaluación	6		
Total presencial	**60**	**Total no presencial**	**90**

8. Sistema y características de la evaluación

Convocatoria ordinaria

INSTRUMENTO/PROCEDIMIENTO	PESO	OBSERVACIONES
(E) Entregas supuestos prácticos	30%	Entregas periódicas de ejercicios prácticos, en el periodo ordinario
(P) Competición SEGURIDAD	10%	Entregas periódicas de ejercicios prácticos
(C) Cuestionarios de evaluación parcial de conocimientos	15%	Dos cuestionarios, a realizar en las semanas 4 y 10 del curso, aprox.
(S) Proyecto práctico de seguridad	30%	Informe del desarrollo del proyecto y defensa oral del mismo
(PE) Prueba escrita	15%	Periodo de exámenes

Convocatoria extraordinaria

INSTRUMENTO/PROCEDIMIENTO	PESO	OBSERVACIONES
(E') Entregas supuestos prácticos	30%	Entregas periódicas de ejercicios prácticos, en el periodo ordinario
(S') Proyecto práctico de seguridad	30%	Informe del desarrollo del proyecto y defensa oral del mismo, en el periodo extraordinario
(PE') Prueba escrita	40%	Periodo de exámenes de la convocatoria extraordinaria

CRITERIOS DE CALIFICACIÓN

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

- La calificación final de la asignatura en la convocatoria ordinaria se obtendrá mediante la suma de las calificaciones obtenidas en los diferentes apartados: (E) + (P) + (C) + (S) + (PE)
- Se debe obtener al menos una calificación final de 5,0 y al menos de 4,0 en los apartados (C) + (PE) y (E) + (P) + (S)

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

- Para la parte (E'): Si el estudiante ha realizado y entregado los trabajos a desarrollar en el laboratorio a lo largo del curso, podrá conservar esa nota o mejorarla revisando los aspectos que le señale el profesor. Aquellos alumnos que no hayan realizado estos trabajos previamente, obtendrán la calificación de 0 puntos en este apartado.
- Para la parte (S'): Si el estudiante ha realizado y entregado el Proyecto práctico de seguridad, podrá conservar esa nota o mejorarla revisando los aspectos que le señale el profesor. Aquellos alumnos que no hayan realizado este trabajo previamente, tendrán que presentarlo y defenderlo oralmente en la fecha que se determine en el periodo extraordinario.
- La calificación final de la asignatura en la convocatoria extraordinaria se obtendrá mediante la suma de las calificaciones obtenidas en los diferentes apartados: (E') + (S') + (PE')
- Se debe obtener al menos una calificación final de 5,0.

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.