DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Master Universitario en INGENIERÍA INFORMÁTICA por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería Informática
Asignatura:	INGENIERÍA DE SEGURIDAD
Código:	203
Tipo:	Optativa
Materia:	ESPECIALIDAD EN CIBERSEGURIDAD
Módulo:	COMPLEMENTOS EN TECNOLOGÍAS INFORMÁTICAS
Experimentalidad:	
Idioma en el que se imparte:	Español
Curso:	2
Semestre:	1
Nº Créditos	4,5
Nº Horas de dedicación del estudiante:	112,5
Nº Horas presenciales:	33,8
Tamaño del Grupo Grande:	
Tamaño del Grupo Reducido:	
Página web de la asignatura:	

EQUIPO DOCENTE

Departamento: LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

Área: LENGUAJES Y SISTEMAS INFORMÁTICOS

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: ANTONIO MAÑA GOMEZ	amana@uma.es	952137142	3.2.16 - E.T.S.I. INFORMÁTICA	

RECOMENDACIONES Y ORIENTACIONES

Esta asignatura se centra en los roles de Ingeniero y Arquitecto de seguridad. Es recomendable que los alumnos posean conocimientos básicos de programación, ingeniería del software y de requisitos.

CONTEXTO

Esta asignatura se enmarca en el grupo de asignaturas optativas de la especialidad de Ciberseguridad del Master Universitario en Ingeniería Informática. En conjunto, dichas asignaturas proporcionan un corpus de conocimientos que dotarán a los estudiantes de la formación necesaria para poder incorporarse al mercado laboral en puestos de responsabilidad en ciberseguridad. En particular, esta asignatura proporciona la formación necesaria para poder afrontar los puestos de Ingeniero y Arquitecto de Ciberseguridad.

COMPETENCIAS

1 Competencias generales y básicas.

Competencias básicas

1.1 CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

1.2 CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

1.3 CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

Competencias generales

1.1 CG1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.

1.2 CG2 - Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio.

1.5 CG5 - Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la ingeniería en Informática siguiendo criterios de calidad y medioambientales.

1.8 CG8 - Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos.

2 Competencias específicas.

2 Competencias específicas.

2.1 ETI1 - Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.

2.4 ETI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

2.9 ETI9 - Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios, sistemas inteligentes y sistemas basados en el conocimiento.

CONTENIDOS DE LA ASIGNATURA

Fundamentos

1. Fundamentos de Ingeniería de Sistemas Software Seguros

- El problema de la ingeniería de seguridad
- Estado de la seguridad del software
- Partes interesadas y puntos de vista
- Conceptos básicos de ingeniería de seguridad
- Fundamentos de la especificación de seguridad
- Enmarcando el problema en los nuevos paradigmas informáticos

2. Procesos y está para una ingeniería y desarrollo de sistemas seguros

- Caracterización de procesos de ingeniería de seguridad
- Enfoques basados en el riesgo
- Enfoques basados en amenazas
- Enfoques basados en propiedades
- Enfoques basados en patrones
- Enfoques basados en modelos
- Estándares relacionados con la Ingeniería de Seguridad y Privacidad

Ingeniería de Sistemas Seguros

3. Análisis y especificación de requisitos de seguridad

- Comprender la naturaleza de los requisitos de seguridad
- Aspectos funcionales y no funcionales de los requisitos de seguridad. Relación con otros requisitos.
- Metodologías y herramientas de obtención de requisitos de seguridad
- Requisitos de seguridad, enfoques de especificación y herramientas
- La importancia de la trazabilidad en los requisitos de seguridad

4. Modelado y diseño de sistemas de software seguro

- Enfoques de modelado para diferentes aspectos de seguridad
- Integración de la Ingeniería de Seguridad en la Ingeniería de Sistemas
- Metodologías y herramientas para representar elementos (requisitos, restricciones, -soluciones, ...) de seguridad
- Procesamiento automatizado de modelos de seguridad
- Evaluación de los diseños de seguridad. Enfoques y herramientas

5. Trazabilidad y documentacio¿n de sistemas software seguros

- La naturaleza interrelacionada e interactiva del diseño de sistemas seguros
- Enfoques y herramientas para documentar sistemas seguros
- Trazabilidad basada en modelos. De los requisitos de seguridad a la evaluación y la certificación de seguridad
- Cumplimiento y certificación. Diseño-para-certificación

ACTIVIDADES FORMATIVAS

Actividades presenciales

Actividades presenciales

Actividades expositivas

Lección magistral

Actividades prácticas en instalaciones específicas

Prácticas en laboratorio

ACTIVIDADES DE EVALUACIÓN

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

Esta asignatura tiene como objetivo fundamental dotar al alumno de los conocimientos y competencias necesarios para ser capaz de enfrentarse a las tareas de ingeniería de sistemas seguros.
En concreto, al finalizar este curso los alumnos habrán adquirido conocimientos y habilidades para identificar y documentar requisitos de seguridad, comprender las infraestructuras necesarias para cumplir esos requisitos, identificar y gestionar las amenazas y riesgos del sistema en cuestión, diseñar sistemas que hagan compatibles los requisitos de negocio y los de seguridad, seleccionar e integrar soluciones de seguridad teniendo en cuenta aspectos tanto técnicos como personales, organizativos, financieros, etc., evaluar diseños de seguridad, demostrar cumplimiento de requisitos y restricciones.
Además, la asignatura proporciona bases para abordar la seguridad de forma integral: esto es, teniendo en cuenta roles, partes interesadas, aspectos técnicos y no técnicos (por ejemplo, humano, de regulaciones, legales, etc.), y cubriendo el ciclo de vida completo de los sistemas a proteger.
Finalmente, indicar que en esta asignatura se considera fundamental que los alumnos refuercen su competencia en trabajo en grupo, dado que la inmensa mayoría de los desarrollos profesionales de sistemas de información se realizan en equipo, y los de seguridad no son una excepción.
Para conseguir todo ello, en esta asignatura se combinará un enfoque basado en conferencias para los contenidos introductorios y teóricos, con una metodología de Aprendizaje Basado en Proyectos (PBL) para asegurar que los estudiantes refuercen el contenido teórico al aplicarlo en un proyecto realista. Los estudiantes trabajarán en grupos siguiendo las prácticas de la industria. Los proyectos que servirán de marco para la asignatura han sido cuidadosamente definidos para introducir y resaltar las necesidades que los contenidos teóricos resuelven al alumno. El calendario y la agenda de los contenidos teóricos se han adaptado para que coincida con los puntos en el desarrollo del proyecto en el que los alumnos se enfrentan a esas necesidades y luego les proporcionan una solución, proporcionando al alumno la visión del contexto y la utilidad del contenidos teóricos, y para asegurar que los encuentren útiles para su trabajo futuro.

PROCEDIMIENTO DE EVALUACIÓN

Por su naturaleza, y por estar enfocada al Aprendizaje Cooperativo y Basado en Proyectos, la asignatura se evalúa preferentemente mediante evaluación continua. La evaluación continua se realizará por los siguientes medios:
- Proyecto personalizado práctico y seguimiento continuo. Se usarán para evaluar aquellos resultados o partes de los mismos que por su naturaleza conlleven una aplicación práctica y desarrollo en grupo.
- Seguimiento continuo e informes de progreso. Se usarán para evaluar el trabajo individual de los estudiantes en cada grupo.
- Pruebas escritas. Se usarán para evaluar los resultados o partes de los mismos relacionados con conocimientos teóricos.

*** Procedimiento de evaluación para la primera convocatoria ordinaria:
- (85%) Nota de la evaluación continua.
- (15%) Examen teórico en las aulas de informática.

***Procedimiento de evaluación para la segunda convocatoria ordinaria:
En esta convocatoria los estudiantes pueden elegir si desean o no mantener su nota de evaluación continua, que será ponderada convenientemente. Tal elección se hará explícita al seleccionar el examen (teórico o teórico-práctico) que realicen.
Estudiantes que desean mantener su nota de evaluación continua:
- (70%) Nota de la evaluación continua.
- (30%) Examen teórico en las aulas de informática.

Estudiantes que no desean mantener su nota de evaluación continua:
- (100%) Examen teórico-práctico en las aulas de informática.

***Procedimiento de evaluación para las convocatorias extraordinarias:
- (100%) Examen teórico-práctico en las aulas de informática.

*** Evaluación de estudiantes a tiempo parcial y deportistas de élite. Estos estudiantes pueden optar a ser evaluados como los demás alumnos si lo desean, pero en todas las convocatorias pueden optar, previa comunicación al profesor) por la siguiente evaluación:
- (100%) Examen teórico-práctico en las aulas de informática más entrega de un trabajo amplio.

Obtención de Matrícula de Honor:
- Sólo para alumnos con calificación global por encima de 9 sobre 10.
- Realización de un supuesto práctico o trabajo profundo sobre un tema de especial interés.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Cyber Security Policy Guidebook. Jennifer L. Bayuk (Wiley)

Cybersecurity Exposed: The Cyber House Rules. Raef Meeuwisse (Cyber Simplicity)

Security Engineering: A Guide to Building Dependable Distributed Systems. Ross J. Anderson (Wiley)

Security Patterns: Integrating Security and Systems Engineering. Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad

Security Policies and Implementation Issues (Jones & Bartlett Learning Information Systems Security & Assurance). Robert Johnson (Jones & Bartlett Learning)

Security Requirements Engineering: Designing Secure Socio-Technical Systems. Fabiano Dalpiaz, Paolo Giorgini, Paolo Giorgini (The MIT Press)

Security Strategy: From Requirements to Reality. Bill Stackpole, Eric Oksendahl (Auerbach)

Complementaria

Certified Chief Information Security Officer (CCISO) Secrets To Acing The Exam and Successful Finding And Landing Your Next Certified Chief Information Security Officer (CCISO) Certified Job. Teresa Tina. (Microsoft)

CISSP (ISC) 2 Certified Information Systems Security Professional Official Study Guide. James M. Stewart, Mike Chapple, Darril Gibson (Sybex)

Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Yuri Diogenes, Erdal Ozkaya (Packt)

Security Patterns in Practice: Designing Secure Architectures Using Software Patterns. Eduardo Fernandez-Buglioni (Wiley)

Threat Modeling: Designing for Security 1st Edition. Adam Shostack (Wiley)

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	11	☑	☐
Prácticas en laboratorio	22,8	☑	☐
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**33,8**		
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**67,45**		
TOTAL HORAS ACTIVIDAD EVALUACIÓN	**11,25**		
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	**112,5**		