DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Graduado/a en Ingeniería del Software por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería Informática
Asignatura:	Seguridad en Servicios y Aplicaciones
Código:	307
Tipo:	Obligatoria
Materia:	Tecnologías de Desarrollo
Módulo:	Ingeniería del Software I
Experimentalidad:	69 % teórica y 31 % práctica
Idioma en el que se imparte:	Español
Curso:	3
Semestre:	2
Nº Créditos	6
Nº Horas de dedicación del estudiante:	150
Nº Horas presenciales:	60
Tamaño del Grupo Grande:	72
Tamaño del Grupo Reducido:	30
Página web de la asignatura:	

EQUIPO DOCENTE

Departamento: LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

Área: INGENIERÍA TELEMÁTICA

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: MARIA CRISTINA ALCARAZ TELLO	alcaraz@uma.es	951952915	3.2.50 - E.T.S.I. INFORMÁTICA	Primer cuatrimestre: Lunes 08:30 - 10:30, Martes 09:45 - 10:45, Lunes 15:15 - 17:15, Lunes 12:30 - 13:30
RODRIGO ROMAN CASTRO	rroman@uma.es	951952914	3.2.26 - E.T.S.I. INFORMÁTICA	Primer cuatrimestre: Lunes 08:30 - 10:30, Jueves 08:30 - 10:30, Martes 10:30 - 12:30

RECOMENDACIONES Y ORIENTACIONES

Se recomienda cursar la asignatura en el mismo curso que "Ingeniería de requisitos" y "Tencologías de Aplicaciones Web" debido a sus interrelaciones y haber superado las asginaturas: "Redes y Sistemas Distribuidos", "Programación Orientada a Objetos" y "Bases de Datos".

CONTEXTO

La asignatura de Seguridad en Servicios y Aplicaciones se centra en aquellos aspectos de la seguridad que deben considerarse durante el desarrollo del software y en el despliegue seguro de aplicaciones en Internet. Respecto al primer punto, se estudia la identificación de amenazas y vulnerabilidades, así como la gestión del riesgo. Esta información será utilizada como entrada al proceso de desarrollo del software seguro, que comienza con la obtención de los requisitos de seguridad y concluye, garantizando que el software implementado cumple dichos requisitos. En cuanto a la seguridad de aplicaciones en internet, la asignatura la aborda en dos frentes: primero cubriendo los servicios de seguridad de alto nivel que son necesarios para el despliegue exitoso de estas aplicaciones, y segundo mediante el estudio de los mecanismos que actualmente se utilizan para proporcionar seguridad a estas aplicaciones, tanto a nivel de transporte (SSL/TLS) como en la programación de dichas aplicaciones.

COMPETENCIAS

1 Competencias generales y básicas.

GENERALES

CG03 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.

CG04 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 básicas, comunes y específicas del título.

CG06 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 básicas, comunes y específicas del título.

CG08 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.

CG09 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

2 Competencias específicas.

Competencias de Tecnologia Especifica

CE-IS-03 Capacidad de dar solución a problemas de integración en función de las estrategias, estándares y tecnologías disponibles.

2 Competencias específicas.

Competencias de Tecnologia Especifica

CE-IS-05 Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

CONTENIDOS DE LA ASIGNATURA

Fundamentos de Seguridad

1.1 Introducción

1.2 Ciclo de vida del software de seguridad

1.3 Modelo de escenario básico de Seguridad

1.4 Servicios y mecanismos de seguridad

Técnicas criptográficas básicas y servicios de seguridad asociados

2.1 Introducción a la criptografía clásica

2.2 Algoritmos simétricos

2.3 Algoritmos asimétricos (o de clave pública)

2.4 Otras primitivas criptográficas

Esquemas, protocolos y mecanismos de soporte

3.3 Gestión de las claves

3.4 Mecanismos de control de acceso

3.5 Protocolos criptográficos avanzados

Herramientas de seguridad

4.1 Correo electrónico seguro

4.2 Sesión remota segura

4.3 Cifrado de datos

Seguridad en aplicaciones web

5.1 Seguridad a nivel de transporte

5.2 Control de acceso en la web y gestión de identidad

5.3 Vulnerabilidades web y pruebas de intrusión

5.4 Privacidad y anonimato

Seguridad en Sistemas Operativos

6.1 Seguridad en sistemas de escritorio

6.2 Seguridad en entornos virtualizados

6.3 Mecanismos de prevención

ACTIVIDADES FORMATIVAS

Actividades presenciales

Actividades expositivas
Lección magistral

Actividades prácticas en instalaciones específicas
Prácticas en laboratorio

Actividades no presenciales

Actividades de discusión, debate, etc.
Discusiones

Actividades de elaboración de documentos
Elaboración de memorias

Actividades prácticas
Desarrollo y evaluación de proyectos

Estudio personal
Estudio personal

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluación presenciales

Actividades de evaluación del estudiante

Examen final
Realización de trabajos y/o proyectos
Otras actividades eval.del estudiante

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

A partir de las actividades formativas y con el objetivo de alcanzar las competencias generales y específicas detalladas en cada materia, se pretenden los siguientes resultados de aprendizaje:

· Tener criterios para seleccionar los servicios y mecanismos de seguridad más adecuados en cada situación para conseguir los niveles de seguridad requeridos. Este resultado está relacionado con las siguientes competencias: CG03,CG04 y CE-IS-05.
· Integrar diferentes servicios de seguridad en las aplicaciones software. Este resultado está relacionado con las siguientes competencias: CG06,CG09 y CE-IS-03.
· Implementar servicios básicos de seguridad. Este resultado está relacionado con las siguientes competencias: CG08.

En un grano más fino podemos destacar los siguientes resultados de aprendizaje:

- Conocer y saber diferenciar los diferentes tipos de amenazas y vulnerabilidades de seguridad de los servicios y aplicaciones actuales.
- Ser capaz de evaluar la seguridad de un sistema mediante el análisis de cada uno de sus componentes y los mecanismos empleados.
- Conocer las normativas de seguridad de la información y ser capaz de ponerlas en práctica en entornos simulados.
- Conocer los servicios de seguridad básicos y avanzados así como los mecanismos con los que se implementan y saber implementarlos.
- Saber evaluar y utilizar los mecanismos y herramientas de seguridad disponibles.

PROCEDIMIENTO DE EVALUACIÓN

La evaluación en las convocatorias ordinarias se hace de la siguiente forma: un examen final (70% de la calificación) + evaluación continua (30% de la calificación). Se requiere superar por separado tanto el examen final (correspondiente al 70%) como la evaluación continua (correspondiente al 30%). La asistencia a ciertas clases teóricas específicas, previamente anunciadas por el profesorado, serán obligatorias.

Respecto a la evaluación continua, ésta se realizará en base a los contenidos prácticos y mediante la realización de actividades prácticas en laboratorio, como pueden ser: trabajos individuales o en grupos, desarrollos de informes técnicos específicos, actividades en foros, cuestionarios o actividades de control (a evaluar sólo en laboratorio - por lo que se recomienda su asistencia), etc. El tipo de práctica dependerá del tema a evaluar, y se estima un orden de una a dos prácticas por tema, dependiendo de la complejidad de la práctica y del tema en sí. Aquellas actividades prácticas que sean entregadas fuera del plazo o enviadas por otras fuentes diferentes a las establecidas por el profesorado serán descartadas.

Cabe mencionar que los estudiantes a tiempo parcial, deportistas universitarios de alto nivel, y alumnos/as de Erasmus realizando la asignatura a distancia en una universidad destino distinta de la UMA, dispondrán de un mayor plazo de entrega de las actividades prácticas, las cuales podrán ser realizadas fuera del centro docente. Respecto al examen final, estos grupos de estudiantes estarán sujetos a las mismas condiciones que el resto del alumnado, realizándolo de forma presencial.

Para la convocatoria de Septiembre y las convocatorias extraordinarias, el alumnado deberán someterse a un examen teórico-práctico con los mismos porcentajes: 70% la teoría + 30% la práctica. También para estas convocatorias se deberá superar por separado tanto la parte teórica como la parte práctica. Sin embargo, para la convocatoria de Septiembre, y en el caso de que el/la alumno/a haya superado la evaluación continua en la convocatoria ordinaria de Junio, éste tendrá la opción de utilizar para dicha convocatoria la calificación de la evaluación continua, presentándose así únicamente a la parte teórica del examen.

Para el proceso de evaluación se tendrá en cuenta también la aplicación de metodologías específicas de aprendizaje, como por ejemplo el aprendizaje basado en juegos serios (en inglés, gamification). Los alumnos que participen en los juegos serios deberán asistir a clase (por lo que se tendrá en cuenta la asistencia) y podrán conseguir hasta 0,5 puntos extra a su nota final, y siempre y cuando, hayan superado de forma satisfactoria la asignatura. Asimismo, se guardará la nota obtenida de los juegos ([0-0,5] puntos) hasta septiembre (pero no para las convocatorias extraordinarias).

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Dent, A. & Mitchell, C., User's Guide To Cryptography And Standards, Artech House, 2005.

Menezes A., Handbook of Applied Cryptography, CRC, 1996.

Pfleeger, C., Security in computing, Prentice Hall, 2007.

Stallings, W., Brown, L, Computer Security: Principles and Practice, Pearson, 2014.

Stallings, W., Cryptography and network security, principles and practices Practice Hall, 2006.

Stallings, W., Cryptography and network security, principles and practices Practice Hall, 2013.

Complementaria

Dent, A. & Mitchell, C., User's Guide To Cryptography And Standards, Artech House, 2005.

Menezes A., Handbook of Applied Cryptography, CRC, 1996.

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	41,4	☑	☐
Prácticas en laboratorio	18,6	☐	☑
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**60**		

ACTIVIDAD FORMATIVA NO PRESENCIAL

Descripción	Horas
Desarrollo y evaluación de proyectos	30
Elaboración de memorias	20
Discusiones	5
Estudio personal	20
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**75**
TOTAL HORAS ACTIVIDAD EVALUACIÓN	**15**
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	**150**