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:	SEGURIDAD EN SISTEMAS INFORMÁTICOS
Código:	122
Tipo:	Obligatoria
Materia:	SEGURIDAD, AUDITORÍA Y CALIDAD EN SISTEMAS DE INFORMACIÓN
Módulo:	TECNOLOGÍAS INFORMÁTICAS
Experimentalidad:	
Idioma en el que se imparte:	Español
Curso:	1
Semestre:	2
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: INGENIERÍA TELEMÁTICA

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: FRANCISCO JAVIER LOPEZ MUÑOZ	fjlopezm@uma.es	952131327	-	Todo el curso: Lunes 08:45 - 10:45, Miércoles 09:00 - 12:00, Lunes 12:30 - 13:30
ISAAC AGUDO RUIZ	isaac@uma.es	952136315	3.2.44 - E.T.S.I. INFORMÁTICA	Primer cuatrimestre: Miércoles 09:30 - 12:30, Jueves 09:30 - 12:30 Segundo cuatrimestre: Lunes 11:30 - 13:30, Martes 09:30 - 11:30, Miércoles 09:30 - 11:30
MARIA CRISTINA ALCARAZ TELLO	alcaraz@uma.es	95951952915	3.2.50 - E.T.S.I. INFORMÁTICA	Primer cuatrimestre: Jueves 10:30 - 12:30, Martes 10:30 - 12:30, Lunes 13:00 - 15:00 Segundo cuatrimestre: Martes 12:00 - 14:00, Martes 11:00 - 12:00, Jueves 09:30 - 12:30

RECOMENDACIONES Y ORIENTACIONES

Es necesario que el alumno haya cursado y superado previamente alguna asignatura de Grado en la que haya aprendido los conceptos básicos relacionados con la seguridad de la información y la seguridad en redes.
Ejemplos de estas asignaturas dentro de la Universidad de Málaga son:

- Seguridad de la Información (Grado en Ingeniería Informática)
- Seguridad en Servicios y Aplicaciones (Grado en Ingeniería del Software)
- Seguridad en Redes Telemáticas (Grado en Ingeniería Telemática)

CONTEXTO

La asignatura 'Seguridad en Entornos Informáticos' es el complemento adecuado para aquellos alumnos que, habiendo cursado en el Grado alguna asignatura básica en la materia de seguridad, deseen conocer y profundizar en la realidad de esta temática desde un punto de vista más cercano al ámbito profesional y de la investigación a nivel europeo.
Además, esta asignatura sienta las bases para cursar posteriormente la asignatura optativa 'Técnicas y metodologías de intrusión y defensa en sistemas informáticos', impartida en este mismo Master.

COMPETENCIAS

1 Competencias generales y básicas

Competencias generales

1.4 CG4. Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.

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.

1.9 CG9. Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.

1.10 CG10. Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.

2 Competencias específicas

2.1 EDG1: Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.

2.5 ETI2: Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

2.7 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.

CONTENIDOS DE LA ASIGNATURA

Nombre Bloque Temático

Tema 1. SERVICIOS BÁSICOS DE SEGURIDAD

1.1 C.I.A

1.2 No-repudio

1.3 Control de Acceso

Tema 2. SERVICIOS AVANZADOS DE SEGURIDAD

2.1 Administración de Claves

2.2 Time-stamping

2.3 Gestión de Identidades

2.4 Administración de Confianza

2.5 Privacidad

Tema 3. SEGURIDAD EN APLICACIONES

3.1 Firma de Contratos

3.2 Pagos Electrónicos

3.3 Subastas Electrónicas

3.4 Escenarios Multiparte

Tema 4. SEGURIDAD EN REDES

4.1 Seguridad en Redes TCP/IP

4.2 Seguridad en Redes Inalámbricas

Tema 5. SEGURIDAD EN ESCENARIOS DE LA INTERNET DEL FUTURO

5.1 Seguridad en Internet de los Objetos

5.2 Seguridad en Cloud

ACTIVIDADES FORMATIVAS

Actividades Presenciales

Actividades expositivas

Lección magistral Impartición de clase magistral en el aula

Actividades No Presenciales

Actividades prácticas

Resolución de problemas
Estudios de casos
Estudios de casos

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluación No Presenciales

Actividades de evaluación No Presenciales

Actividades de evaluación del estudiante

Otras actidades no presenciales eval.estudiante

Actividades de evaluacion Presenciales

Actividades de evaluación del estudiante

Examen final

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

- Comprender y aplicar políticas y normativas de seguridad así como los procesos de certificación de seguridad.

- Aplicar tecnologías avanzadas de seguridad y evaluar el nivel de seguridad en función de tipo de tecnologías utilizadas.

- Conocer los retos y soluciones de seguridad en los escenarios de la internet del futuro.

- Conocer y aplicar técnicas forenses y de autoría informática.

PROCEDIMIENTO DE EVALUACIÓN

Se evaluarán los contenidos teóricos de la asignatura mediante un examen final que supondrán hasta un 70% de la calificación global de la misma. Eventualmente, podría haber un examen parcial eliminatorio según se desarrolle la impartición de la asignatura. La asistencia a ciertas clases teóricas específicas, previamente anunciadas por el profesor, será obligatoria.

Además, se evaluarán los contenidos prácticos de la asignatura mediante la entrega de prácticas y/o trabajos obligatorios, que supondrán el restante 30% de la calificación final. Los estudiantes a tiempo parcial habrán de entregar estas prácticas también, que podrán desarrollar fuera del Centro.

En la convocatoria de Septiembre y Diciembre se realizará un sólo examen final que abarcará todos los conocimientos teórico-practicos impartidos en la asignatura.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Applied Cryptography: Protocols, Algorithms, and Source Code in C¿, Bruce Schneier, Wiley, 1996

Cryptography and Network Security: Principles and Practic, William Stallings, Prentice Hall, 2014

Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, 1996

User's Guide To Cryptography And Standards, Alex W. Dent, Chris J. Mitchell, Artech House, 2004

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral Impartición de clase magistral en el aula	33,8	☑	☐
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**33,8**		

ACTIVIDAD FORMATIVA NO PRESENCIAL

Descripción	Horas
Estudios de casos	20
Resolución de problemas	20
Estudios de casos	20
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**67,45**
TOTAL HORAS ACTIVIDAD EVALUACIÓN	**11,25**
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	**112,5**